HP Web Jetadmin 10.4

User Guide

Copyright and License

The information contained herein is subject to change without notice.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Publication Date: 11/2017

Trademark Credits

Table of contents

1 Install and Set Up HP Web Jetadmin

When you install HP Web Jetadmin, you only need to install it on one hardware platform that meets the recommended minimum requirements (System Requirements on page 1) and is centrally accessible on the network. You may then access the software from any supported Windows desktop on the network and manage all supported network-connected peripherals.

HP Web Jetadmin offers several installation options. If you have installed a previous version of HP Web Jetadmin, you can choose to upgrade the previous version or install a new copy. Upgrading an older version preserves your settings for discovery options and groups and is most likely the best choice if you have already been using HP Web Jetadmin.

Every release of HP Web Jetadmin contains new features and improvements to existing features. In an environment where a previous release of HP Web Jetadmin is integrated into critical business operations, HP recommends that you fully test and qualify a new release before implementing that release into full production.

Read all of the support materials before you implement HP Web Jetadmin. For current information about HP Web Jetadmin, see the *Late Breaking News for HP Web Jetadmin 10.4* and the *HP Web Jetadmin 10.4 Supported Devices Readme*. These documents are available from the HP Web Jetadmin support page (click the flag icon on the bottom of the page, and then select your country/region).

System Requirements

HP Web Jetadmin includes network device communication protocols and internal components that manage application and device data. These components extend the capabilities of HP Web Jetadmin and improve usage and performance in device lists, columns, and filtering functions.

HP Web Jetadmin is supported on platforms that have Microsoft Windows and .NET Framework high-priority updates. During each development cycle, HP regularly tests HP Web Jetadmin on platforms that have the current Microsoft updates. HP investigates all post-release software issues that customers report. For more information about the current software issues, see the *Late Breaking News for HP Web Jetadmin 10.4*. This document is available from the HP Web Jetadmin support page (in English).

HP Web Jetadmin requires the Windows HTTP SSL service. HP Web Jetadmin uses SSL to communicate with newer HP devices through port 8050.

HP Web Jetadmin Server Application

Supported operating systems

- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10 (64-bit edition only)

- Microsoft Window 8.1 (64-bit edition only)
- Microsoft Window 8 (64-bit edition only)
- Microsoft Windows 7 SP1 (64-bit edition only)

For more information about a specific Microsoft operating system, go to www.microsoft.com.

Notes

- HP no longer supports or tests HP Web Jetadmin installations on Microsoft operating systems that were released prior to the operating systems that are supported for the current release.
- Beginning with HP Web Jetadmin 10.3 SR6, Microsoft .NET Framework 4.5 or later is required in addition to .NET Framework 3.5 SP1 because HP Web Jetadmin supports Transport Layer Security (TLS) 1.1 and 1.2. Some of the operating systems that are supported for the current release already ship with .NET Framework 4.5 or later.

  If the HP Web Jetadmin installer does not detect .NET Framework 3.5 SP1 and .NET Framework 4.5 or later, the installer provides the appropriate installation instructions and Microsoft URL to download .NET Framework.
- The operating systems that are supported for the current release include Windows Installer 4.5. If Windows Installer 4.5 is not already installed, the HP Web Jetadmin installer provides the appropriate Microsoft URL to download Windows Installer 4.5.
- Local administrator access is required to install or upgrade HP Web Jetadmin.
- Production HP Web Jetadmin installations are restricted to dedicated hosts. Running HP Web Jetadmin on systems that are also mail servers, DNS servers, domain controllers, and so on is not supported.

HP Web Jetadmin Client Application

Supported operating systems

- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows 10
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 SP1

For more information about a specific Microsoft operating system, go to www.microsoft.com.

Notes

- Beginning with HP Web Jetadmin 10.3 SR6, Microsoft .NET Framework 4.5 or later is required in addition to .NET Framework 3.5 SP1 because HP Web Jetadmin supports Transport Layer Security (TLS) 1.1 and 1.2. Some of the operating systems that are supported for the current release already ship with .NET Framework 4.5 or later.

If the HP Web Jetadmin installer does not detect .NET Framework 3.5 SP1 and .NET Framework 4.5 or later, the installer provides the appropriate installation instructions and Microsoft URL to download .NET Framework.

Virtual Machine (Optional Platform)

Recommended requirements

HP recommends the following virtualization solutions:

- VMware ESX
- Microsoft Hyper-V

Notes

- For a VMware server, the virtual machine network must be set to `bridged` to facilitate HP Web Jetadmin communications.
- It is very important to configure VMware so that its guest or virtual systems have enough resources to support HP Web Jetadmin and Microsoft SQL Server. To ensure that the appropriate resources are provisioned, see the support documentation for the version of VMware you are using.

Server Hardware

Recommended requirements

HP recommends the following hardware configuration for the server:

- 4 or more processor cores
- 2.8 GHz or higher processor speed
- 4 GB or more of RAM
- 4 GB of available storage

Minimum requirements

Although you can use the following hardware configuration for the server, HP does not recommend that you use it for production installations. HP does not test HP Web Jetadmin on this hardware configuration and, therefore, cannot guarantee the results.

- 2 processor cores
- 2.33 GHz processor speed
- 5 GB of RAM (2 GB is required for the HP Web Jetadmin Service, and 2 GB is the default SQL memory reservation)

  HP Web Jetadmin uses a value of 3,072 MB to qualify a system as having 3 GB of RAM.
- 4 GB of available storage

Notes

- Recent software improvements have increased resource capacity requirements. HP strongly recommends the 64-bit editions of Windows and 4 GB or more of RAM for production HP Web Jetadmin installations.
- Storage requirements vary depending on the implementation, database, and migration from previous versions.
- NTFS is the only supported file system.
- If the HP Web Jetadmin installer determines that less than 1 GB of RAM is installed, the installer displays a message stating that 3 GB of RAM is required.

Client Hardware

Recommended requirements

HP recommends the following hardware configuration for the client:

- PC with 2.4 GHz processor
- 64-bit system with 4 GB of RAM
- Client display with a minimum resolution of 1024 x 768
- Optimized for Normal font size
- Default DPI only

Minimum requirements

Although you can use the following hardware configuration for the client, HP does not recommend that you use it for production installations. HP does not test HP Web Jetadmin on this hardware configuration and, therefore, cannot guarantee the results.

- PC with 1.8 GHz processor
- 32-bit or 64-bit system with 2 GB of RAM
- Client display with a minimum resolution of 1024 x 768
- Optimized for Normal font size
- Default DPI only

Database

For new installations of HP Web Jetadmin 10.3 SR8 or later, the installation package contains and automatically installs the database for Microsoft SQL Server 2012 Express SP2 (product version 11.0.5058.0). Existing installations of HP Web Jetadmin prior to 10.3 SR8 and installations that have been upgraded to 10.3 SR8 or later use the database for Microsoft SQL Server 2008 Express (product version 10.00.2531.00).

NOTE: HP has successfully tested HP Web Jetadmin with Microsoft SQL Server 2014.

TIP: For more information about configuring HP Web Jetadmin to use a separate Microsoft SQL instance, see the *Using Microsoft SQL Server with HP Web Jetadmin* white paper. This white paper is available from the HP Web Jetadmin support page (in English).

Network

The HP Web Jetadmin installer requires one active IPv4 connection. If an active IPv4 connection is not available, the installer fails.

For firmware upgrades with HP Web Jetadmin, a minimum bandwidth of 1 MB/s is required. If there are multiple devices upgrading at the same time, then the minimum bandwidth of 1 MB/s will be equal to the number of concurrent firmware upgrades. For example, four simultaneous upgrades requires at least 4 MB/s.

Installations and Upgrades

Local administrator access is required to install or upgrade HP Web Jetadmin.

Client Application

The HP Web Jetadmin client application requires the following:

- Internet Explorer 8, 9, 10, or 11
- Display with a minimum resolution of 1024 x 768

Notes

- Internet Explorer is required to start the HP Web Jetadmin client application. For more information about Internet Explorer requirements and limitations, see the support documentation for the Windows operating system that you are using.
- Administrator access is not required to run the HP Web Jetadmin client application.
- A maximum of 15 concurrent client sessions are allowed.

Supported Devices

HP Web Jetadmin supports HP devices and third-party devices that are connected through HP Jetdirect print servers. HP Web Jetadmin also supports third-party devices that are standard printer MIB compliant and are connected to the network. For third-party devices, HP Web Jetadmin provides basic capabilities as well as more robust capabilities if the devices are used with HP-certified plug-ins for HP Web Jetadmin.

IMPORTANT: If the following devices use a Universal Plug-in (UPI), WS-Discovery must be enabled on the devices:

- HP LaserJet Pro
- HP Officejet Pro
- HP FutureSmart with a firmware version earlier than 3.2.3

If WS-Discovery is disabled on HP LaserJet Pro and HP Officejet Pro devices, HP Web Jetadmin uses the correct UPI and displays a status of **Device Communication Error** for the devices after a device discovery or full refresh is performed.

If WS-Discovery is disabled on HP FutureSmart devices with a firmware version earlier than 3.2.3, HP Web Jetadmin uses a generic device model instead of the correct UPI after a device discovery or full refresh is performed.

Host Access

For the application host, local administrator access is required to install or upgrade HP Web Jetadmin.

For the client host, local user access is required to access the HP Web Jetadmin client application and administrator access is required to install Microsoft .NET Framework.

Client/Server Security

Microsoft domain or locally managed Windows users and passwords are required.

Notes

- HP tests HP Web Jetadmin in Microsoft Active Directory domains.
- Users must be a member of an HP Web Jetadmin server administrator group or designated as one of the following in the HP Web Jetadmin User settings:
  - Windows local security group
  - Active Directory security group
  - Local individual user account
  - Active Directory domain user account

Install HP Web Jetadmin

To install HP Web Jetadmin, perform the following steps:

1. Go to www.hp.com/go/webjetadmin, and then download the HP Web Jetadmin software.
2. Double-click the EXE file.
3. Follow the instructions in the wizard.
4. If the installation stops with a warning that a reboot is required, reboot the host on which the HP Web Jetadmin installer is running. Then relaunch the installer to continue the installation.
5. When the installation is complete, click the **Finish** button.

IMPORTANT: If the HP Web Jetadmin installer does not install Microsoft SQL Server Express Edition, the most common reason for the failure is that Windows updates, such as service packs or hotfixes, were installed on the machine and the machine was not restarted after the updates completed. Restart the machine, and then install HP Web Jetadmin again.

Install HP Web Jetadmin from the Command Line

You can install HP Web Jetadmin from a command line, through a script, or through an automated process. The following is the command syntax:

```
<filename>.exe [/L"<LanguageID>"] [/S /v/qn] </V"[Property1=Value1]
[Property2=Value2] [...]">
```

Command-line parameters

- `<filename>.exe`

  Specifies the name of the EXE file that you downloaded from www.hp.com/go/webjetadmin.

- `/L"<LanguageID>"`

  Specifies the ID of the language the installer uses (Optional). If the language dialog is enabled and you specify a valid language ID, the installer automatically suppresses the language dialog. If you specify an invalid language ID or a language ID that the installer does not support, the installer ignores this parameter.

  The following are the language IDs. The default is the local system language.

Language	Language ID
Chinese (Simplified)	2052
Chinese (Traditional)	1028
English (Worldwide)	1033
French (European)	1036
German	1031
Italian	1040
Japanese	1041
Korean	1042
Portuguese (Brazilian)	1046
Russian	1049
Spanish (Mid-Atlantic)	1034

- `/S /v/qn`

  Performs a silent installation (Optional).

  To perform a silent installation, the following properties are required:

  - `WJA_EULA`
  - `ENABLE_ANONYMIZED_DATA_COLLECTION`

- `/V"[Property1=Value1] [Property2=Value2] [...]"`

  Specifies a list of properties the installer uses (Required). The following are the properties and values.

Property and Value	Description
`WJA_EULA=ACCEPT | REJECT`	Specifies whether you accept or reject the HP Web Jetadmin End User License Agreement (EULA). This property is required for silent installations.
`ENABLE_ANONYMIZED_DATA_COLLECTION=TRUE | FALSE`	Specifies whether the Data Collection feature is enabled or disabled. This feature collects data about your printers and implementation of HP Web Jetadmin and anonymizes the data. HP Web Jetadmin uses an Internet connection to transmit the anonymized data to HP. HP uses the anonymized data to improve products and services. This property is required for silent installations.

Property and Value	Description
	IMPORTANT: HP is committed to protecting your privacy and the integrity of your computer. You can enable and disable this feature at any time. Your name, address, email address, and other sensitive data are not sent to HP.
`WJA_BACKUP_CONFIRM=YES | NO`	Specifies whether a backup of HP Web Jetadmin was performed prior to the installation. This property is required for upgrade installations.
`WJA_SUPPLY_GROUP_REMOVAL_CONFIRM=YES | NO`	Specifies whether the existing Supplies Groups are removed. In HP Web Jetadmin 10.2, the Supplies Groups functionality was removed as a product feature. Regular device groups will not be removed or altered during the installation. This property is required when upgrading from all versions of HP Web Jetadmin 10.1 and earlier. `YES`—Confirms that you understand and agree that all Supplies Groups functionality as well as existing groups will be removed during the installation. `NO`—Causes the installation to terminate and end without the software being installed.
`WJA_COLUMN_CONFIRM=YES | NO`	Specifies whether the column data is upgraded, which might affect filters, groups with filters, and device list exporting. This property is required for silent upgrade installations prior to HP Web Jetadmin 10.2 SR 5.
`WJA_SKIP_DB_INSTALL=1 | 0`	Specifies whether the database installation is skipped. To skip the database installation, specify `1`. This property is required only if you want the installer to skip the database installation.
`INSTALLDIR=\"<Path>\"`	Specifies the HP Web Jetadmin installation path. The following is the default path: C:\Program Files\HP Inc\Web Jetadmin 10\ This property is optional for silent installations. The path must be enclosed with `\"`. In addition, the properties specified for the `/V` option must be enclosed with quotes. The following is an example of the correct syntax: `/V"WJA_EULA=ACCEPT INSTALLDIR=\"C:\Program Files\HP Inc\Web Jetadmin 10\""` CAUTION: If the path contains spaces and is not enclosed with `\"`, the installer fails.
`DATABASEDIR=\"<Path>\"`	Specifies the database installation path. The following is the default path: C:\Program Files\Microsoft SQL Server\ This property is optional for silent installations. If the directory name contains spaces, you must use the Windows short-path notation. To find the short-path notation, issue the following command: `Dir *. /x` The path must be enclosed with `\"`. In addition, the properties specified for the `/V` option must be enclosed with quotes. The following are examples of the correct syntax: – `/V"WJA_EULA=ACCEPT DATABASEDIR=\"C:\SQLServer\""`

Property and Value	Description
	– `/V"WJA_EULA=ACCEPT DATABASEDIR=\"C:\Program~1\SQLServer\""` CAUTION: If the path contains spaces and is not enclosed with `\"`, the installer fails.

Examples of the command-line syntax

The following examples assume that the name of the installation file is WjaSetup-x64.exe.

- To perform a basic silent installation, enter the following command:

  ```
  WjaSetup-x64.exe /S /v/qn /V"WJA_EULA=ACCEPT
  ENABLE_ANONYMIZED_DATA_COLLECTION=TRUE"
  ```

- To start the installer in Spanish, enter the following command:

  ```
  WjaSetup-x64.exe /L"1034"
  ```

- To perform a silent installation with HP Web Jetadmin installed on C:\WJA, enter the following command:

  ```
  WjaSetup-x64.exe /S /v/qn /V"WJA_EULA=ACCEPT
  ENABLE_ANONYMIZED_DATA_COLLECTION=TRUE INSTALLDIR=\"C:\WJA\""
  ```

- To perform a silent installation with HP Web Jetadmin installed on C:\WJA and the database installed on C:\WJADB, enter the following command:

  ```
  WjaSetup-x64.exe /S /v/qn /V"WJA_EULA=ACCEPT
  ENABLE_ANONYMIZED_DATA_COLLECTION=TRUE INSTALLDIR=\"C:\WJA\"
  DATABASEDIR=\"C:\WJADB\""
  ```

- To perform a silent upgrade, enter the following command:

  ```
  WjaSetup-x64.exe /S /v/qn /V"WJA_EULA=ACCEPT
  ENABLE_ANONYMIZED_DATA_COLLECTION=TRUE INSTALLDIR=\"C:\WJA\"
  DATABASEDIR=\"C:\WJADB\" WJA_BACKUP_CONFIRM=YES
  WJA_SUPPLY_GROUP_REMOVAL_CONFIRM=YES WJA_COLUMN_CONFIRM=YES"
  ```

Install HP Web Jetadmin in Blocking Mode

You can run a silent installation in blocking mode from the command line. The following is the command syntax:

```
start /wait <ProgramAndArguments>
```

The following examples assume that the name of the installation file is WjaSetup-x64.exe.

-
  ```
  start /wait WjaSetup-x64.exe /S /v/qn /V"WJA_EULA=ACCEPT INSTALLDIR=
  \"C:\wja\" DATABASEDIR=\"C:\wjadb\""
  ```

-
  ```
  start /wait "C:\temp\WjaSetup-x64.exe /S /v/qn /V"WJA_EULA=ACCEPT
  ENABLE_ANONYMIZED_DATA_COLLECTION=TRUE INSTALLDIR=\"C:\wja\"
  DATABASEDIR=\"C:\wjadb\"""
  ```

Post-installation Tasks

The HP Web Jetadmin server will start automatically as a Microsoft Service. The HP Web Jetadmin server cannot accept HP Web Jetadmin client connections until the HP Web Jetadmin server has fully loaded all services into memory. Dependent upon your HP Web Jetadmin server available system resources, it may take 1-2 minutes for all services to completely load after initial server installation or server reboot.

The first time you launch HP Web Jetadmin after installation, a pop-up dialog is displayed stating that no devices have been discovered. You can opt to launch discovery settings at this point.

Once the installation is complete, HP Web Jetadmin can be launched from a supported browser by entering the hostname or IP address of the computer on which it is installed, followed by the port number and path. Typical default port numbers for Web services have a value of 80. Since HP Web Jetadmin may be running simultaneously with another Web service on the same computer, HP Web Jetadmin uses a port number of 8000. If desired, the port value may be altered.

Here is an example of the URL used to activate HP Web Jetadmin on a supported Windows desktop:

```
http://myhost:8000
```

Recommended Initial Configuration Steps

After HP Web Jetadmin is installed, some of the initial steps that you should take to begin managing devices and the print environment include configuring the options that are shared throughout HP Web Jetadmin, running a discovery, and configuring various other features.

Shared configuration options include the database, network (for example, SNMP and HTTPS), discovery, server maintenance, and credentials. To configure these options, go to **Tools** > **Options** > **Shared**, and then navigate to the appropriate category. For more information about a specific option, see the online Help for that option.

Finding devices on the network might be as simple as enabling HP Web Jetadmin to passively listen for devices on the network. Finding devices might be as complex as working with the IT team to map the entire IP network, and then running an IP Range discovery to compile a complete inventory of network-connected devices. You can also use many of the same settings and techniques to discover PC-connected devices. Before you plan and implement a device discovery strategy, carefully review the information about discoveries in the HP Web Jetadmin documentation and white papers.

You should configure features such as Roles, Users, Alerts, and Device Groups before you begin using HP Web Jetadmin. For more information about a specific feature, see the appropriate section in the HP Web Jetadmin documentation and the HP Web Jetadmin white papers.

The HP Web Jetadmin documentation and white papers are available from the HP Web Jetadmin support page (click the flag icon on the bottom of the page, and then select your country/region).

Configure the HP Web Jetadmin Service to Restart Automatically

It is recommended to configure HP Web Jetadmin to restart automatically whenever the HP Web Jetadmin service fails. If, for example, the database is inaccessible, the HP Web Jetadmin service will be stopped and then automatically restarted. The HP Web Jetadmin service will wait for the database to become accessible and then the HP Web Jetadmin service becomes live.

HP Web Jetadmin installs an additional service named HPWSProAdapter. The HPWSProAdapter service facilitates communication with certain HP device models and must be left running. You must also perform the steps in this section for the HPWSProAdapter service.

To configure the HP Web Jetadmin service to restart automatically, follow these steps.

1. Access the **Windows Control Panel** and select **Administrative Tools**.
2. Select **Services** and then select **HPWJA Service**.
3. Right-click and select **Properties** from the menu.
4. Click the **Recovery** tab. For the **First failure**, **Second failure**, and **Subsequent failures**, select **Restart the service**.
5. Click **OK**.

Ports

HP Web Jetadmin listens continuously on several ports and opens other ports for specific functionality. The following table lists the ports that HP Web Jetadmin uses.

NOTE: HP Web Jetadmin uses Internet Control Message Protocol (ICMP) in the discovery process. HP Web Jetadmin sends an ICMP echo request to determine if the IP is active.

Port number	Type	Inbound (I) or Outbound (O)[1]	Description
69	UDP	I	TFTP Incoming Port: HP Web Jetadmin uses this port as a staging area for firmware images during HP Jetdirect firmware updates. Through SNMP, HP Web Jetadmin triggers HP Jetdirect to retrieve firmware through this port.
80	TCP	O	HP Web Jetadmin uses this port to qualify the link to the HP Embedded Web Server on the device and to retrieve the firmware images from the web.
161	UDP	O	SNMP: HP Web Jetadmin and other management applications use SNMP to communicate with and manage devices. HP Web Jetadmin uses this port on the printer to issue `Set` and `Get` commands to the SNMP agent.
427	UDP	I	SLP Listen: HP Jetdirect-connected devices use Service Location Protocol (SLP) to advertise their existence. When the passive SLP discovery feature is enabled on HP Web Jetadmin, devices send multicast packets to this port on the HP Web Jetadmin server.
443	TCP	O	HTTPS: The HP Web Jetadmin service and HPWSProAdapter service send device configurations and queries to this port over HTTPS. HPWSProAdapter uses this port to communicate with devices that do not support Web Services and are configured to redirect all of the network traffic to HTTPS.
843	TCP	O	HP Web Jetadmin uses this port to configure some settings, such as fax and digital sending, on some HP MFP device models.
1433	UDP	O	Microsoft SQL Server: By default, HP Web Jetadmin installs the SQL Server database on the same host. Optionally, you can configure HP Web Jetadmin to communicate with a SQL Server database on a different host. HP Web Jetadmin uses this port to facilitate communication with a remote SQL Server database.
2493	UDP	I/O	Build Monitor: This is an HP Web Jetadmin server port that is kept open. Other HP Web Jetadmin servers use this port to discover running instances of HP Web Jetadmin.
3702[2]	UDP	O	WS Discovery: HP Web Jetadmin uses this port to perform a Web Services discovery on newer HP devices.

Port number	Type	Inbound (I) or Outbound (O)[1]	Description
3910[2], 3911	TCP	O	WS Discovery: HP Web Jetadmin uses this port to retrieve details about the device Web Services during a discovery. HP Web Jetadmin uses these details to establish the WS communication paths that it needs to manage devices. HP Web Jetadmin uses port 3910 to retrieve print requests and uses port 3911 to retrieve the printer status.
4088	TCP	I	Remoting: HP Web Jetadmin uses this port as the primary communication channel between a started HP Web Jetadmin client and its corresponding HP Web Jetadmin server.
4089	TCP	I	Client Event Notification: HP Web Jetadmin uses this port to communicate change events from the HP Web Jetadmin server to the client. These events trigger the client to pull updates from the server through the Remoting interface. In previous releases of HP Web Jetadmin, Windows assigned this port.
7627[2]	TCP	O	Web Services (HTTPS): HP Web Jetadmin uses this port to communicate with HP FutureSmart devices and older laser devices for some operations, such as OXPd. For devices that do not support Web Services, the HPWSProAdapter Service acts as a gateway between HP Web Jetadmin and the devices. The HPWSProAdapter Service receives Web Services requests from HP Web Jetadmin, and then sends the translated requests to the devices over port 8080 (an unsecure connection, an HP Embedded Web Server password is not configured on the devices) or port 443 (a secure connection, an HP Embedded Web Server password is configured on the devices).
8000	UDP	O	HP Web Jetadmin Discovery Listen: HP Web Jetadmin uses this port on remote IP hosts to detect earlier versions of the HP Web Jetadmin software.
8000	TCP	I	Web Server: HP Web Jetadmin provides an HTTP listener for the initial client launch and online Help content.
8050	TCP	I	Device Eventing Callback (HTTPS): Newer HP devices use a WS eventing protocol for management communications.
8080	TCP	O	HPWSProAdapter: HPWSProAdapter uses this port to communicate with devices that do not support Web Services and are not configured to redirect all of the network traffic to HTTPS. HP Web Jetadmin sends device configurations and queries to this port.
8140	TCP	I	OXPm Web Services (HTTP): This is the communication port for HP Open Extensibility Platform (management operations).
8143	TCP	I	OXPm Web Services (HTTPS): This is a secure communication port for HP Open Extensibility Platform (management operations).
8443	TCP	I	Secure Web Server (HTTPS): HP Web Jetadmin provides a secure HTTPS listener for the initial client launch, Help content, and device file transfer operations.
9100	TCP	O	Printer Firmware Upgrade and Test File Operation: HP Web Jetadmin uses this printer port to transfer printer firmware files, test job files, and PJL configuration files.
27892	UDP	I	Traps Listener: HP Web Jetadmin uses this port for SNMP-based alerts and for By User Data Collections.
27893	UDP	I	WS Hello Listener: HP Web Jetadmin monitors this port for incoming WS Hello packets from the HP WS Pro Proxy Agent software that is installed on hosts in the enterprise. When HP Web Jetadmin detects a packet, it follows up to determine whether there are any printers to discover on the sending host. For

Port number	Type	Inbound (I) or Outbound (O)[1]	Description
			more information, see the *HP Web Jetadmin 10.4 Proxy Agents Readme*. This document is available from the HP Web Jetadmin support page (in English).
59113	TCP	O	Microsoft SQL Server: By default, HP Web Jetadmin installs the SQL Server database on the same host. Optionally, you can configure HP Web Jetadmin to communicate with a SQL Server database on a different host. HP Web Jetadmin uses this port to facilitate communication with a remote SQL Server database.

[1] The I/O column represents the communication direction with respect to the HP Web Jetadmin server host. HP Web Jetadmin uses random source ports when communicating with ports on remote IP addresses.

[2] HP Web Jetadmin uses ports 7627, 3702, and 3910 internally to communicate with devices. To ensure proper communication, these ports must be kept open for communication directly with the device and with the internal HPWSProAdapter service.

When using WMI discovery (discovering PC-connected printers without an HP proxy installed on the PC), several ports have to be opened for the WMI communication (DCOM ports, WMI ports, and WMI connection applications (UnsecApp or WMI_OUT)). For more information, see: https://msdn.microsoft.com/en-us/library/aa822854.aspx

Open the ports in the Windows firewall by using a batch file

HP Web Jetadmin opens the ports listed in the table to communicate with devices. However, the firewall that you are using might block the connection and prevent HP Web Jetadmin from communicating with the network.

Instead of adding firewall rules for these ports one at a time, you can create a batch file that opens all of the ports that HP Web Jetadmin requires for the Windows firewall at one time. For instructions, see the Create a Batch File to Open HP Web Jetadmin Required Ports in the Windows Firewall white paper. This white paper is available from the HP Web Jetadmin support page.

Implement SSL

By default, the HP Web Jetadmin HTTP service runs without certificates. If you add a certificate, the HTTP server runs in HTTPS mode and Secure Sockets Layer (SSL) communication is enforced. In HTTPS mode, the user and the HTTP server are authenticated to one another and the traffic between them is encrypted. This adds an extra layer of security to the Smart Client download and other HTTP transactions.

HP Web Jetadmin does not self-generate certificates. You must obtain a certificate from a certificate authority (CA). CAs can exist inside or outside of an organization. Many companies have their own CAs. The HP Web Jetadmin Signing Request feature generates a file that you can send to the CA. When the CA sends you a certificate, use the Install Certificate feature to enable HTTPS.

IMPORTANT: For new server certificates, you must install 2048-bit certificates. Any previously installed 1024-bit server certificates continue to function correctly.

Enable Secure Sockets Layer (SSL)

HP Web Jetadmin administrators enable SSL by adding a certificate to the HP Web Jetadmin application. This certificate forces the browser to use the more secure HTTPS protocol when a user accesses the client logon page. The administrator must enable SSL from the console or host that runs the application by using the procedure in Configure HTTPS (Server Certificates or SSL) on page 14. When a remote administrator accesses **Tools** > **Options** > **Shared** > **Network** > **HTTPS**, a message appears stating that certificates can only be installed from an HP Web Jetadmin client that runs on the console or server that hosts HP Web Jetadmin.

In some environments, SSL is required when an HTTP interface or service is used for communication. In these cases, SSL can be enabled and enforced by HP Web Jetadmin. SSL provides a high level of assurance regarding the authentication and encryption of HTTP communication. That is, a user who requests access to the HP Web Jetadmin Smart Client download can be reasonably assured that the system hosting HP Web Jetadmin is authentic and the communication between the two systems is encrypted so that it cannot be easily read by eavesdroppers.

The SSL protocol uses certificates to accommodate both authentication and encryption. HP Web Jetadmin can generate a signing request that can be used by a certificate authority (CA) to generate a certificate. Using **Tools** > **Options** > **Shared** > **Network** > **HTTPS**, the user can generate a **Signing Request**.

Once the request has been fulfilled by the CA, the certificate is ready to be installed on HP Web Jetadmin. Remember, you must be at the application console to use **Tools** > **Options** > **Shared** > **Network** > **HTTPS**. Use **Install Certificate** to browse and upload the certificate file.

Once the certificate is installed, the HTTP service enforces SSL. Any browser contact with HP Web Jetadmin should indicate HTTPS on the URL when a certificate is installed. Using **Remove Certificate** uninstalls the certificate and SSL is no longer enforced.

Important Points to Remember When Implementing SSL

Client communication with SSL enforced requires one or more of the following considerations.

- For new server certificates, you must install 2048-bit certificates. Any previously installed 1024-bit server certificates continue to function correctly.
- When SSL has been implemented on HP Web Jetadmin with an internal certificate authority (CA), the CA's authorizing certificate must be installed in the client browser. If this certificate is not installed in the client browser the HP Web Jetadmin Smart Client page will fail to load up in SSL mode.
- Proxy servers tend to use the standard SSL port 443. If the HP Web Jetadmin Smart Client page is being called through a proxy server, a redirect error may occur. This is due to the URL being redirected to 443 rather than 8443 which is the port used by the HP Web Jetadmin SSL. The workaround for this is to place the HP Web Jetadmin fully qualified domain name (FQDN) into the browsers exceptions list under **Tools** > **Internet Options** > **Connections** > **LAN Settings** > **Advanced**. This causes the browser to pull HTTP and HTTPS content directly from the HP Web Jetadmin server.

  TIP: HP Web Jetadmin HTTP and HTTPS port numbers can be customized to something other than 8000 and 8443.

- When you have implemented SSL on HP Web Jetadmin, a redirect occurs when the browser URL uses port 8000. Here is an example:

  The known URL prior to SSL implementation is `http://servername.domain.xxx:8000`.

  After SSL implementation, HP Web Jetadmin will redirect this to a new URL: `https://servername.domain.xxx:8443`.

  The URLs shown here use FQDN. In most cases the certificate issued and installed in the HP Web Jetadmin SSL implementation will contain an FQDN for the host on which HP Web Jetadmin is installed. If a non FQDN is used in the browser, certificate failure will occur. As a general rule, form the HP Web Jetadmin URL with FQDN when HP Web Jetadmin is implemented with SSL.

To configure HTTPS, access **Tools** > **Options** > **Shared** > **Network** > **HTTPS**.

Configure HTTPS (Server Certificates or SSL)

1. To configure HTTPS, access **Tools** > **Options** > **Shared** > **Network** > **HTTPS**.
2. To associate a certificate with the HP Web Jetadmin server and enable HTTPS, select **Install Certificate**.

   IMPORTANT: When using the HP Web Jetadmin client to install a certificate on a Vista host with UAC enabled, you must launch the client from the installer (just after install is finished and from the checkbox that enables client launch) or from an IE that was **Run as Administrator**.

   -or-

   To remove the installed certificate from the server and disable HTTPS, select **Remove Certificate**.

   -or-

   To generate a certificate request that can be sent to a signing authority to generate a certificate that can be installed to enable HTTPS, select **Signing Request**.

   IMPORTANT: For new server certificates, you must install 2048-bit certificates. Any previously installed 1024-bit server certificates continue to function correctly.

3. To save these settings and continue setting other options, click **Apply**. Then click the next option to configure in the left menu bar. To save these settings and close this window, click **OK**.

Use a Separate Instance of Microsoft SQL Server

By default, HP Web Jetadmin installs and uses a database that runs under Microsoft SQL Server Express. An existing installation of HP Web Jetadmin can be configured to use the full version of SQL Server instead of SQL Server Express. However, HP does not support or test HP Web Jetadmin installations with SQL Server databases other than the version listed in Database on page 4 and, therefore, cannot guarantee the results.

For more information about configuring HP Web Jetadmin to use a separate Microsoft SQL instance, see the *Using Microsoft SQL Server with HP Web Jetadmin* white paper. This white paper is available from the HP Web Jetadmin support page (in English).

Deploy the Smart Client

HP Web Jetadmin uses the Microsoft ClickOnce Smart Client technology. This technology runs a Microsoft .NET Framework application by automatically downloading and starting the application through a web browser. The Smart Client application runs as a local .NET Framework application on the host and uses .NET Remoting to communicate with the HP Web Jetadmin service. The following describes the interaction between the HP Web Jetadmin server and the Smart Client application:

- The Smart Client application uses HTTP or HTTPS to initially contact the HP Web Jetadmin server. The default HTTP port is 8000. The default HTTPS port is 8443. For instructions on changing the default ports, see Change the Default HTTP or HTTPS Port for the HP Web Jetadmin Smart Client Application on page 16.
- The HP Web Jetadmin server transfers approximately 2 MB of files for the Smart Client application to the client.
- The Smart Client application runs on the client as the user who is logged in to the computer, executes commands that download approximately 50 MB of HP Web Jetadmin client files, and starts the graphical user interface for the HP Web Jetadmin client application. The web browser is now inactive.

After the Smart Client application starts, the web browser is no longer required. Although HP Web Jetadmin also uses the web browser to deliver online Help and proactive Product Update notifications, the HP Web Jetadmin client application runs locally on the computer.

- The HP Web Jetadmin server downloads all of the relevant information to the client. When new information is available, the HP Web Jetadmin server contacts the client and downloads the new information.

The HP Web Jetadmin installer builds a shortcut on the installation host to http://*<ip_address>*:8000/, where *<ip_address>* is the host where HP Web Jetadmin is installed. Use this URL to access HP Web Jetadmin remotely from anywhere on the company's intranet or WAN.

To start the Smart Client session, only a web browser is required. Administrator rights are not required to run Smart Client applications. However, .NET Framework must be installed. Local administrator rights might be required to install .NET Framework.

In most cases, the Smart Client session starts automatically. However, the local security settings on the workstation might prevent the application from starting automatically. For more information about manually starting the Smart Client, see Start an HP Web Jetadmin Client Session on page 17. For more information about changing the local security settings, see the Microsoft documentation.

Change the Default HTTP or HTTPS Port for the HP Web Jetadmin Smart Client Application

Use the following steps to change the default HTTP or HTTPS port that is used to start the HP Web Jetadmin Smart Client application:

1. Use Notepad or a similar text editor to open the HP.Imaging.Wjp.Core.WebServer.config.xml file. This configuration file is available in the following directory:

   C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config

2. Update the `<value>` attribute for the HTTP or HTTPS port in the following entries:

```
<property name="HttpsPort">
  <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
  </type>
  <value>8443</value>
</property>
<property name="HttpPort">
  <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
  </type>
  <value>8000</value>
</property>
```

3. Close and save the file.

Run the Smart Client Application in a Workgroup

Use the following steps to change the Microsoft security settings:

TIP: For more information about the security policy settings, see the Microsoft documentation.

1. On the HP Web Jetadmin server, go to **Start** > **Control Panel** > **System and Security** > **Administrative Tools**, and then double-click **Local Security Policy**.

2. In the left navigation pane, expand **Local Policies**, and then select **Security Options**.

3. In the right pane, double-click **Network access: Sharing and security model for local accounts**.
4. From the list, select the **Classic - local users authenticate as themselves** option.
5. Click the **OK** button.

Start an HP Web Jetadmin Client Session

After the HP Web Jetadmin installation is complete, use one of the following methods to start an HP Web Jetadmin client session:

- On the host where HP Web Jetadmin is installed, go to **Start** > **All Programs** > **HP Web Jetadmin 10**, and then select **HP Web Jetadmin**.
- In Internet Explorer, browse to the following URL on the host where HP Web Jetadmin is installed:

  http://*<ip_address>*:8000
- From the command line, issue the following command:

  ```
  rundll32 dfshim.dll, ShOpenVerbApplication http://<ip_address>:
  8000/wja/wja.application?InternalErrorDetails=true
  ```

  To start the HP Web Jetadmin client session in a specific language, use the following URLs. If the corresponding Windows language pack is installed, the HP Web Jetadmin client session displays in that language. If the corresponding Windows language pack is not installed, the HP Web Jetadmin client session displays in a mixture of English and the specified language.

Language	URL
Chinese (Simplified)	http://*<ip_address>*:8000/wja/wja.application?lang=zh-cn
Chinese (Traditional)	http://*<ip_address>*:8000/wja/wja.application?lang=zh-tw
English (Worldwide)	http://*<ip_address>*:8000/wja/wja.application?lang=en-us
French (European)	http://*<ip_address>*:8000/wja/wja.application?lang=fr-fr
German	http://*<ip_address>*:8000/wja/wja.application?lang=de-de
Italian	http://*<ip_address>*:8000/wja/wja.application?lang=it-it
Japanese	http://*<ip_address>*:8000/wja/wja.application?lang=ja-jp
Korean	http://*<ip_address>*:8000/wja/wja.application?lang=ko-kr
Portuguese (Brazilian)	http://*<ip_address>*:8000/wja/wja.application?lang=pt-pt
Russian	http://*<ip_address>*:8000/wja/wja.application?lang=ru-ru
Spanish (Mid-Atlantic)	http://*<ip_address>*:8000/wja/wja.application?lang=es-es

In some cases, you might need to add the URL for HP Web Jetadmin to the trusted security zone in the Web browser.

Configure HP Web Jetadmin to Bind to a Specific NIC

HP Web Jetadmin can run on a multi-homed server or on a server that has multiple network interfaces. In many cases, a multi-homed server is connected to more than one network and has multiple IP addresses. A multi-homed server with multiple IP addresses can cause problems because HP Web Jetadmin tends to use only one address for various reasons.

HP Web Jetadmin is a collection of features that administrators can use to manage devices. Each of these features might require communications on the network or convey the IP address through which communications should take place to other features either on or off the HP Web Jetadmin server. These features facilitate learning the HP Web Jetadmin server IP address when the HPWJA service starts. These features do so in isolation and might not select the correct IP address. The following sections describe situations where features might not detect and select the correct IP address and provide a workaround that forces HP Web Jetadmin to select the correct IP address.

HP Web Jetadmin Client Connection

The HP Web Jetadmin client startup is initiated from Internet Explorer using HTTP. Immediately after the startup sequence, the HP Web Jetadmin client sends an HTTP message to the client host. The HTTP message points to a Microsoft .NET Framework remote connection. The client host then initiates a relatively secure connection to the HP Web Jetadmin server based on the HTTP message.

If HP Web Jetadmin is installed on a multihomed server and the HP Web Jetadmin (HPWJA) service selects an incorrect IP address, the .NET Framework remote connection fails because the system that hosts the client cannot communicate by using the IP address provided. Use the following steps to force the HPWJA service to use the correct IP address:

1. Stop the HPWJA service by using Windows Service Manager.

   ⚠ CAUTION: Be careful when stopping the HPWJA service. Critical tasks might be running and clients might be logged in to HP Web Jetadmin. To view the running tasks, go to **Application Management** > **Overview** > **Application Management - Active Tasks**. To view the clients that are logged in, go to **Application Management** > **Overview** > **Client Management - Active Clients**.

2. Use Notepad or a similar editor to open the System.Remoting.config file. This configuration file is available in the following directory:

   C:\Program Files\HP Inc\Web Jetadmin 10\config\WjaService

   IMPORTANT: Make sure that Notepad is running with sufficient privileges to update and save the file.

3. Find the following code in the System.Remoting.config file:

```
<application>
  <channels>
   <channel ref="tcp" port="4088" name="CMRemotingChannel"
     rejectRemoteRequests="false"
     tokenImpersonationLevel="Impersonation" secure="true"
     protectionLevel="EncryptAndSign" impersonate="false">
```

4. Add the `machineName="xxx.xxx.xxx.xxx"` entry, changing the value to the IP address of the HP Web Jetadmin server that facilitates client communication. The following is an example of the edited code:

```
<application>
  <channels>
   <channel ref="tcp" port="4088" name="CMRemotingChannel"
     rejectRemoteRequests="false"
     tokenImpersonationLevel="Impersonation" secure="true"
     protectionLevel="EncryptAndSign" impersonate="false"
     machineName="xxx.xxx.xxx.xxx">
```

> ⚠ CAUTION: Make sure that the new entry and value are entered exactly as shown here. Use the quotes that the editor generates. Do not copy and paste this text because incorrect characters, such as quotes, cause the HPWJA service to fail at startup. Observe all of the rules for editing XML. If the file is incorrectly formatted, the HP Web Jetadmin XML parser fails.

5. Close and save the file.

6. Start the HPWJA service by using Windows Service Manager.

HP Web Jetadmin Alerts and SNMP Traps Registration

In rare cases, HP Web Jetadmin detects and uses an incorrect IP address for SNMP traps registration at the device. When HP Web Jetadmin alert subscriptions are created, HP Web Jetadmin registers its IP address in the SNMP traps destination table on the HP device. This registration causes the device to send a notification in the form of SNMP trap packets back to the HP Web Jetadmin server. HP Web Jetadmin uses these notifications to trigger alerts for device conditions such as toner out or paper jam.

If an HP Web Jetadmin instance on a multi-homed server populates the SNMP traps destination table with the incorrect IP address, follow these steps to force HP Web Jetadmin to select and use the correct IP address:

1. Stop the HPWJA service by using Windows Service Manager.

> ⚠ CAUTION: Be careful when stopping the HPWJA service. There might be critical tasks running. To view the running tasks in HP Web Jetadmin, go to **Application Management** > **Overview** > **Application Management - Active Tasks**. To view the client logins in HP Web Jetadmin, go to **Application Management** > **Overview** > **Client Management - Active Clients**.

2. Open Notepad or a similar text editor that has the appropriate create and edit permissions.

3. Enter the following text:

```
<ipmc:configuration
xmlns:ipmc="www.hp.com/schemas/imaging/ipmc/config/2004/02/24">
  <property name="LocalIPV4Address">
   <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
   </type>
   <value>xxx.xxx.xxx.xxx</value>
  </property>
</ipmc:configuration>
```

> ⚠ CAUTION: Make sure that the new field and values are entered exactly as shown here. Use the quote marks that the editor generates. Do not copy and paste from this document because incorrect characters cause the HPWJA service to fail at startup. Observe all the rules regarding XML editing. If the files are incorrectly formatted, the HP Web Jetadmin XML parser fails.

4. Change the `<value>xxx.xxx.xxx.xxx</value>` entry to the correct HP Web Jetadmin server IP address through which the device can communicate.

5. Select **File** > **Save As**.

6. On the **Save as** window, navigate to the following directory on the HP Web Jetadmin server host:

   C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config

7. In the **File name** text box, enter `HP.Imaging.Wjp.Alerts.Library.AlertsHelpers.config.xml`.

8. From the **Save as type** drop-down list, select **All Files (*.*)**.

9. Click **Save**.

10. Start the HPWJA service by using Windows Service Manager.

HP Web Jetadmin now uses the IP address specified during SNMP traps registration. You must update any SNMP traps registrations created prior to this procedure by using the HP Web Jetadmin Configuration feature or by creating additional alerts subscriptions.

HP Web Jetadmin Web Service

The HP Web Jetadmin web or HTTP service uses the server IP addresses for various reasons, including communicating with other processes, nodes, services, and the IP address of the actual HTTP server. In rare cases, HP Web Jetadmin detects the incorrect IP address on multi-homed systems. A configuration file that includes the HP Web Jetadmin IP address is built during the first HPWJA service startup. Follow these steps to correct the IP address value in the configuration file:

1. Stop the HPWJA service by using Windows Service Manager.

   ⚠ CAUTION: Be careful when stopping the HPWJA service. There might be critical tasks running. To view the running tasks in HP Web Jetadmin, go to **Application Management** > **Overview** > **Application Management - Active Tasks**. To view the client logins in HP Web Jetadmin, go to **Application Management** > **Overview** > **Client Management - Active Clients**.

2. Open Notepad or a similar text editor that has the appropriate create and edit permissions.

3. Select **File** > **Open**.

4. On the **Open** window, navigate to the following directory:

   C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config

5. Open the HP.Imaging.Wjp.Core.WebServer.config.xml file.

6. Find the following portion of the file:

```
<property name="HostIPv4Address">
  <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
  </type>
  <value>xxx.xxx.xxx.xxx</value>
</property>
```

7. Change the `<value>xxx.xxx.xxx.xxx</value>` entry to the correct server IP address.

8. Select **File** > **Save**.

9. Start the HPWJA service by using Windows Service Control Manager.

HP Web Jetadmin now uses the specified IP address with reference to the HTTP or web services.

Configure the Port for Event Notifications

HP Web Jetadmin directs clients to a TCP connection to receive event notifications. After the client establishes the TCP connection, HP Web Jetadmin sends event notifications that prompt the client to update itself via the standard Microsoft .NET Remoting channel on port 4088. The HP Web Jetadmin server communicates the port number that is established for event notifications to the client when the client first establishes a connection to the HP Web Jetadmin server. The port number that HP Web Jetadmin communicates to the client is somewhat random, which might cause a problem if a firewall is configured on the HP Web Jetadmin server.

If a firewall is configured on the HP Web Jetadmin server, the event notification port must be set to **static** and the firewall must be configured to accept connections through this port. If a firewall is configured on the client, the firewall on the client does not have to be configured to launch the client.

Use the following steps to configure a static port for event notifications:

⚠ CAUTION: Be careful when restarting the HP Web Jetadmin service. Critical tasks might be running and clients might be logged in to HP Web Jetadmin. To view the running tasks, go to **Application Management** > **Overview** > **Application Management - Active Tasks**. To view the clients that are logged in, go to **Application Management** > **Overview** > **Client Management - Active Clients**.

1. Use Notepad or a similar editor to create a file that contains the following XML section:

   ```
   <ipmc:configuration
   xmlns:ipmc="www.hp.com/schemas/imaging/ipmc/config/2004/02/24">
     <property name="ClientEventRouter.ServerPort">
      <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
      </type>
      <value>8099</value>
     </property>
   </ipmc:configuration>
   ```

   The port number specified for the `<value>` attribute can be any unused port.

2. From the **File** menu, select **Save**.

3. On the **Save As** window, navigate to the following directory on the HP Web Jetadmin server:

   C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config

4. In the **File name** box, enter `Global.config.xml`, and then click the **Save** button.

5. Restart the HP Web Jetadmin service (HPWJAService). For instructions, see Restart the HP Web Jetadmin Service Manually on page 21.

6. Use any firewall application or a similar application to open the port.

Configure the Firewall Software

You must configure the firewall on the HP Web Jetadmin server host to allow client traffic and other traffic to pass through the correct ports. The firewall monitors HP Web Jetadmin for the ports that it uses and allows traffic.

In some firewall applications, such as Microsoft Firewall, you can specify a program or executable file as a firewall exception. In these cases, you can define the following file as an exception:

C:\Program Files\HP Inc\Web Jetadmin 10\bin\HPWJAService.exe

The firewall on the client system does not require any special consideration because the client application does not listen to a specific port.

Restart the HP Web Jetadmin Service Manually

It may be necessary to stop and restart the HP Web Jetadmin service. An example of this would be when a network is switched from hard-wired to wireless. Once the network is switched, HP Web Jetadmin must be restarted in order for the application to realize the change.

⚠ CAUTION: Restarting HP Web Jetadmin services may interrupt background tasks and user sessions. Always check the application before restarting.

To script the stop of all HP Web Jetadmin services, use these command strings in this order:

- Net stop HPWSProAdapter
- Net stop HPWJAService
- Net stop mssql$HPWJA

To script the start of all HP Web Jetadmin services, use these command strings in this order:

- Net start mssql$HPWJA
- Net start HPWJAService
- Net start HPWSProAdapter

1. Uninstall HP Web Jetadmin.
2. Use Windows Service Manager to set the older HP Web Jetadmin service (listed as **HP Web Jetadmin** in the Services MMC) to **activate** and to also start the service.

Back Up and Restore HP Web Jetadmin

Scripts for backing up and restoring HP Web Jetadmin are available. These scripts provide examples of the recommended method for backing up and restoring the HP Web Jetadmin settings and data, including the Microsoft SQL Server database. The WJABackupRestoreInstructions_<*language_code*>.txt file provides instructions for running the scripts. The scripts and instructions are available in the following directory:

C:\Program Files\HP Inc\Web Jetadmin 10\WJABackupRestore

Upgrade HP Web Jetadmin

The current HP Web Jetadmin installation must be backed up before an upgrade is started. The WJABackupRestoreInstructions_<*language_code*>.txt file provides instructions for backing up HP Web Jetadmin. This file is located in the following directory on the HP Web Jetadmin server:

C:\Program Files\HP Inc\Web Jetadmin 10\WJABackupRestore

In HP Web Jetadmin, go to **Help** > **About**, and then write down the current version as 10.4. *nnnnn*, where *nnnnn* is the build number. This version of the installer is required to perform a recovery.

Before you begin an upgrade, go to **Application Management** > **Overview** > **Application Management – Active Tasks**, and then check for any paused or pending tasks. You must stop or resolve these tasks before you run the installer.

To upgrade HP Web Jetadmin, obtain the HP Web Jetadmin installation executable from www.hp.com/go/webjetadmin. Then run the executable on the system that hosts HP Web Jetadmin.

Import Feature Packs

Feature Packs provide support for dynamically adding new configuration options and new device images to HP Web Jetadmin. Feature Packs are imported and applied on an existing installation of HP Web Jetadmin. This means that you can gain access to the new functionality without installing and qualifying a new version of the full HP Web Jetadmin application. HP Web Jetadmin Administrator rights are required to apply Feature Packs.

Feature Packs are cumulative. A new Feature Pack includes the new functionality that is being released and all of the functionality that was released in previous Feature Packs.

Each Feature Pack has a minimum version of HP Web Jetadmin that must be installed before the Feature Pack can be imported and applied. If you import a Feature Pack on a version of HP Web Jetadmin that is earlier than the minimum required version, HP Web Jetadmin displays a message that specifies the minimum required version.

Feature Packs are available from www.hp.com/go/webjetadmin as signed HP Binary (HPb) files. After you download an HPb file, you must import the HPb file into the existing installation of HP Web Jetadmin, and then apply the HPb file. You must restart the HP Web Jetadmin service before the new functionality is available in HP Web Jetadmin.

⚠ CAUTION: After a Feature Pack is applied, it cannot be removed from HP Web Jetadmin. HP recommends that you back up HP Web Jetadmin before you apply a Feature Pack.

When a Feature Pack is initially released, the software and online Help for the new features are available only in English. The localized software and online Help for the new features will be provided at a later time, either in a new Feature Pack or a new version of HP Web Jetadmin.

Import and apply a Feature Pack

⚠ CAUTION: After a Feature Pack is applied, it cannot be removed from HP Web Jetadmin. HP recommends that you back up HP Web Jetadmin before you apply a Feature Pack.

1. Go to www.hp.com/go/webjetadmin, and then download the HP Web Jetadmin Feature Pack file.
2. Go to **Tools** > **Feature Packs**.
3. Click the **Import** button.
4. On the **Open** window, browse to and select the HPb file, and then click the **Open** button.
5. On the **Success** window, click the **OK** button. The HPb file is listed on the **Feature Packs** window with a status of **Imported (Apply Pending)**.

   -or-

   If a Feature Pack has already been imported, but has not been applied yet, HP Web Jetadmin displays the **Warning** window.

   To overwrite the existing Feature Pack, click the **Yes** button.

   To cancel the import process, click the **No** button.
6. Select the Feature Pack from the list, and then click the **Apply** button.

   The status of the selected Feature Pack must be **Imported**.
7. On the **Confirm Feature Pack apply** window, click the **OK** button.
8. On the **Success** window, click the **OK** button. The Feature Pack is listed on the **Feature Packs** window with a status of **Applied (Service Restart Required)**.
9. Restart the HP Web Jetadmin service (HPWJAService).

⚠ CAUTION: Restarting the HP Web Jetadmin service can interrupt critical processes. Before you restart the HP Web Jetadmin service, use the HP Web Jetadmin Broadcast Message feature to notify the active users, and then make sure that all of the users are logged off and that there are no active tasks running on the HP Web Jetadmin server.

Delete an imported Feature Pack

1. Go to **Tools** > **Feature Packs**.
2. Select the Feature Pack from the list, and then click the **Delete** button.

   The status of the selected Feature Pack must be **Imported**.
3. On the **Delete Feature Pack** window, click the **OK** button.
4. On the **Success** window, click the **OK** button.

Display the Release Notes for a Feature Pack

The Release Notes for Feature Packs are provided only in English.

1. Go to **Tools** > **Feature Packs**.
2. Select the Feature Pack from the list, and then click the **Details** button. The Release Notes are displayed in Notepad.

Enable FIPS on the HP Web Jetadmin Server

Federal Information Processing Standard (FIPS) can be enabled only after you upgrade to HP Web Jetadmin 10.4 or later. This topic provides instructions for upgrading HP Web Jetadmin, making the required changes to the settings in HP Web Jetadmin, and then enabling FIPS. These instructions must be followed in the order provided.

The MD5 and DES protocols are blocked after FIPS is enabled. Communication over SNMPv1/SNMPv2 is still possible after FIPS is enabled.

Upgrade to HP Web Jetadmin 10.4 or later

1. On the HP Web Jetadmin server, go to www.hp.com/go/webjetadmin, and then download the HP Web Jetadmin software.
2. Double-click the EXE file.
3. Follow the instructions in the wizard.
4. If the installation stops with a warning that a reboot is required, reboot the HP Web Jetadmin server. Launch the installer again to continue the installation.
5. When the installation is complete, click the **Finish** button.

Make the required changes to the settings in HP Web Jetadmin and on the devices

If you omit the following steps, HP Web Jetadmin might not be able to communicate with the devices after FIPS is enabled. HP Web Jetadmin displays a status of **Device Communication Error** for these devices.

1. If HP Web Jetadmin has already discovered devices by using an SNMPv3 credential that specifies the MD5 and DES protocols, SNMP communication with those devices will not work after FIPS is enabled. The SNMPv3 credential for these devices must be changed to the SHA-1 and AES-128 protocols. However, you

cannot use HP Web Jetadmin to determine if the SNMPv3 credential for the devices uses the MD5 and DES protocols.

Use the following steps to update the SNMPv3 credential on all of the devices that use SNMPv3:

a. In the **Device Management** navigation pane, right-click **Configuration**, and then select **Create configuration template**. The **Create Device Configuration Template** wizard starts.

b. On the **Select Template Models** page, select the device models to configure, and then click the right arrow button.

c. Select the network cards to configure, and then click the right arrow button.

d. Click the **Next** button.

e. On the **Specify template options** page, enter a name for the template in the **Name** box (up to 48 characters).

f. In the **Device settings** navigation pane, go to **Security** > **SNMP Version Access Control**.

g. Select the **Modify SNMPv3** option.

h. In the **Current SNMPv3 Credential** section, enter the user name, authentication protocol, authentication passphrase, privacy protocol, and privacy passphrase that are currently configured for SNMPv3. The current SNMPv3 credentials are required.

i. In the **New SNMPv3 Credential** section, select **SHA-1** from the **Authentication Protocol** list, and select **AES-128** from the **Privacy Protocol** list.

j. If required, enter the new values for the user name, authentication passphrase, and privacy passphrase.

⚠ CAUTION: To change the authentication and privacy passphrases, the current passphrases must be specified in the device configuration template even if global SNMPv3 credentials are stored in HP Web Jetadmin. If the current passphrases are not specified, the configuration fails.

k. Click the **Next** button.

l. On the **Confirm** page, verify that the information is correct, and then click the **Create Template** button.

m. On the **Results** page, click the **Done** button.

n. In the **Device Management** navigation pane, right-click **Configuration**, and then select **Apply configuration template**. The **Apply Device Configuration Template** wizard starts.

o. Select the device configuration template that you just created from the list, and then click the **Next** button.

p. On the **Select devices** page, select the devices to configure from the **Available devices** list, and then click the **>** button.

q. Click the **Next** button.

r. On the **Confirm** page, verify that the information is correct, and then click the **Apply Template** button.

s. On the **Results** page, click the **Done** button.

2. Use the following steps to delete the SNMPv3 global credentials that use the MD5 and DES protocols:

   a. Go to **Tools** > **Options** > **Shared** > **Credentials** > **Device** > **SNMPv3**.

   b. Select the SNMPv3 credential that uses the MD5 and DES protocols from the list, and then click the **Remove** button.

c. On the **Confirm Delete** window, click the **Yes** button.

d. Repeat steps b through c for each SNMPv3 credential that uses the MD5 and DES protocols.

3. Run a discovery to rediscover all of the SNMPv3-configured devices.

4. Trap forwarding that is configured to use SNMPv3 credentials with the MD5 and DES protocols does not work after FIPS is enabled. Use one of the following procedures to update the alert subscriptions that are configured to forward SNMP traps to a server using SNMPv3 credentials with the SHA-1 and AES-128 protocols.

NOTE: Alert subscriptions that are configured to only write alerts to the alert history log or to send email notifications when alerts occur do not need to be updated.

Update the alert subscriptions that were created by using an alert subscription template that is configured to forward SNMP traps

a. In the **Device Management** navigation pane, go to **Alerts** > **All Subscriptions**.

b. At the top of the **All Subscriptions** pane, click the **Expand all** button to display the details for each alert subscription.

c. To identify the alert subscription templates that must be updated, look for alerts that have **SNMPv3 Trap Forwarding** in the **Notification Type** column and have **Linked** in the **Linked to Template** column. The name of the alert subscription template is shown in the **Subscription Name** column.

d. In the **Device Management** navigation pane, go to **Alerts** > **Templates**.

e. In the **Alerts - Subscription Templates** pane, select the alert subscription template from the list, and then click the **Edit** button. The **Edit Subscription Template** wizard starts.

f. Click the **Next** button until the **Specify notification settings** page appears.

g. In the **SNMPv3 credential** section, select **SHA-1** from the **Authentication protocol** list, and select **AES-128** from the **Privacy protocol** list.

h. If required, enter the new values for the user name, authentication passphrase, and privacy passphrase.

i. Click the **Next** button until the **Confirm** page appears.

j. On the **Confirm** page, verify that the information is correct, and then click the **Save Template** button.

k. On the **Results** page, click the **Done** button.

All of the alert subscriptions that are linked to this alert subscription template are automatically updated with the new SNMPv3 credentials.

l. Repeat steps c through k for each of the alert subscription templates.

Update the alert subscriptions that were created without using an alert subscription template and are configured to forward SNMP traps

a. In the **Device Management** navigation pane, go to **Alerts** > **All Subscriptions**.

b. In the **All Subscriptions** pane, select the alert subscription from the list, and then click the **Edit Subscription** button. The **Edit Subscription** wizard starts.

c. Click the **Next** button until the **Specify notification settings** page appears.

d. In the **SNMPv3 credential** section, select **SHA-1** from the **Authentication protocol** list, and select **AES-128** from the **Privacy protocol** list.

e. If required, enter the new values for the user name, authentication passphrase, and privacy passphrase.

f. Click the **Next** button until the **Confirm** page appears.

g. On the **Confirm** page, verify that the information is correct, and then click the **Edit Subscription** button.

h. On the **Results** page, click the **Done** button.

i. Repeat steps b through h for each alert subscription that was created without using an alert subscription template.

-or-

If any future changes are made to the alert subscriptions, all of the alert subscriptions must be changed. To prevent this in the future, HP recommends that you use the following steps to create new alert subscriptions that are linked to alert subscription templates:

a. In the **Device Management** navigation pane, go to **Alerts** > **All Subscriptions**.

b. In the **All Subscriptions** pane, select the alert subscription from the list, and then click the **Unsubscribe** button. The **Delete Alert Subscriptions** wizard starts.

c. On the **Confirm** page, click the **Unsubscribe** button.

d. On the **Results** page, click the **Done** button.

e. In the **Device Management** navigation pane, go to **Alerts** > **Templates**.

f. In the **Alerts - Subscription Templates** pane, select the alert subscription template from the list, and then click the **Apply** button. The **Apply Alert Subscription Template** wizard starts.

NOTE: If an alert subscription template is not available, create an alert subscription template that meets your specific needs.

g. On the **Select devices** page, select the devices from the **Available devices** list, and then click the **>** button.

h. Click the **Next** button.

i. To link the selected alert subscription template to this alert subscription, select the **Link template to subscription** option. Changes that are made to the selected alert subscription template are automatically applied to the devices that are associated with this alert subscription.

   -or-

   To create an alert subscription that is not linked to the selected alert subscription template, select the **Do NOT link template to subscription** option, and then enter a name for this alert subscription in the **Subscription name** box. Changes that are made to the alert subscription template are not applied to the devices that were previously configured with this alert subscription template.

j. Click the **Next** button.

k. On the **Confirm** page, verify that the information is correct, and then click the **Apply Template** button.

l. On the **Results** page, click the **Done** button.

m. Repeat steps b through l for each of the alert subscriptions that were created without using an alert subscription template.

5. On the client machines where the HP Web Jetadmin client is launched, use the following steps to enable the TLS protocol:

a. Open an Internet Explorer browser.

b. Go to **Tools** > **Internet options**, and then click the **Advanced** tab.

c. Scroll down to the **Security** section, and then select the checkboxes for one or more of the TLS versions (TLS 1.0, TLS 1.1, and TLS 1.2).

6. Use the following steps to verify that the devices are configured to communicate with the TLS protocol:

   a. Select the device from any device list.

   b. On the **Config** tab, go to **Network** > **Mgmt Protocol**.

   c. Verify that any version of TLS (TLS 1.0, TLS 1.1, and TLS 1.2) is enabled.

   d. Repeat steps a through c for each device.

7. Use the following steps to enable FIPS-140 mode on the devices. Enabling FIPS-140 mode affects only the following device configuration options:

   - **SNMP Version Access Control** configuration option: The SHA-1 authentication protocol and AES-128 privacy protocol must be configured.

   - **Mgmt Protocol** configuration option: The TLS 1.0, TLS 1.1, or TLS 1.2 protocol must be enabled.

   TIP: The following steps are not required. However, you can use these steps to troubleshoot any FIPS-related problems.

   a. Select the device from any device list.

   b. On the **Config** tab, go to **Security** > **FIPS-140 Mode**.

   c. Select the **Enabled** option.

   d. Click the **Apply** button.

   e. Repeat steps a through d for each device.

   If any of the following device configuration options are configured on a device, enabling FIPS-140 mode fails for that device:

   - **SNMP Version Access Control** configuration option: The MD5 authentication and DES privacy protocols must not be specified.

   - **IPsec/Firewall Policy** configuration option: The DES-CBC-MD5 algorithm must not be specified for the **Kerberos** setting.

   - **Upload Jetdirect Certificate** configuration option: Certificates must not be signed by using MD5 or earlier (MD2 or MD4).

   - **Upload CA Certificate** configuration option: Certificates must not be signed by using MD5 or earlier (MD2 or MD4).

   - **Mgmt Protocol** configuration option: The SSL 3.0 or earlier protocol must not be enabled.

   HP Web Jetadmin does not report the exact reason for the failure. However, if you enable FIPS-140 mode by using the device HP Embedded Web Server (EWS), the EWS does report the exact reason for the failure. The FIPS-140 mode setting is available in the EWS from the **Networking** tab > **Security** link > **Settings** page.

Enable FIPS on the HP Web Jetadmin server

1. Stop the following services. These services must be stopped in the specified order.

   a. HPWSProAdapter

   b. HPWJAService

   c. mssql$HPWJA

2. Use the following steps to enable FIPS on the HP Web Jetadmin server as a local security policy:

   TIP: For more information about the **System cryptography** setting, see the *"System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" security setting effects in Windows XP and in later versions of Windows* document. This document is available from the Microsoft support page.

   a. Go to **Control Panel** > **Administrative Tools** > **Local Security Policy** > **Local Policies** > **Security Options**.

   b. Right-click **System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing**, and then select **Properties**.

   c. On the **Local Security Setting** tab, select the **Enabled** option, and then click the **OK** button.

3. Start the following services. These services must be started in the specified order.

   a. mssql$HPWJA

   b. HPWJAService

   c. HPWSProAdapter

4. Use the following steps to verify that HP Web Jetadmin can communicate with all of the devices:

   a. In the **All Devices** list, look for any devices that have **Device Communication Error** in the **Status** column.

   b. Verify that you can configure a device by using HP Web Jetadmin.

   c. In the **All Devices** list, right-click a device, and then select **Refresh Selection (Full)**. Verify that the refresh completed.

   If there are any devices that have a status of **Device Communication Error** or you cannot complete step b or c, access the device EWS, and then verify the following settings:

   - Click the **Networking** tab, and then click the **Network Settings** link. If SNMPv3 is enabled, verify that the authentication protocol is SHA *x* and the privacy protocol is AES.

   - Click the **Security** tab, and then click the **Certificate Management** link. Select a certificate, and then click the **View Details** button. Verify that the self-signed certificate uses a signature algorithm other than MD5. Repeat this step for each self-signed certificate.

Uninstall HP Web Jetadmin

When you uninstall HP Web Jetadmin, the Microsoft SQL Server Express Edition instance of the HP Web Jetadmin database is also removed. You can restore the HP Web Jetadmin database if you ran the appropriate backup procedures and stored the backup files in a secure location.

To uninstall HP Web Jetadmin, perform the following steps:

1. Go to **Start** > **Control Panel** > **Uninstall a program**.

2. Right-click **HP Web Jetadmin 10.4**, and then select **Change**. The **HP Web Jetadmin 10.4 - InstallShield Wizard** starts.

3. Click the **Next** button.

4. Select the **Remove** option, and then click the **Next** button.

5. Follow the instructions in the wizard.

6. Review the MSI <*xxxxx*>.LOG file, where <*xxxxx*> is a randomly generated string. The log file is available in the following directory:

   C:\Users\<*username*>\AppData\Local\Temp

TIP: You can uninstall HP Web Jetadmin from the command line. For instructions, see the *Uninstall HP Web Jetadmin from the Command Line* white paper. This white paper is available from the HP Web Jetadmin support page (in English).

Manage Licenses

There are some features for HP Web Jetadmin that require a license. After you obtain the license for a feature, you must install the license to enable the functionality.

To manage the licenses, perform the following steps:

1. Go to **Start** > **All Programs** > **HP Web Jetadmin 10**, and then select **HP Web Jetadmin License Manager**.

2. To install a license, perform the following steps:

   a. Click the **Add** button.

   b. On the **Enter License** window, enter the license key, and then click the **Apply** button.

3. To delete a license, select the license from the list, and then click the **Remove** button.

4. To refresh the list of licenses, click the **Refresh** button.

5. Click the **Exit** button.

6. Restart the HP Web Jetadmin service (HPWJA Service).

2 Introduction to HP Web Jetadmin

HP Web Jetadmin increases business productivity by helping you proactively address potential printing problems, automatically configure peripheral drivers, and update firmware. HP Web Jetadmin provides all of the peripheral management capabilities you need in one easy-to-use Web browser interface. It is a is a free utility that you can download from www.hp.com/go/webjetadmin.

Product Support

This section provides information about obtaining support for HP Web Jetadmin.

Print the HP Web Jetadmin Guides

If you need to print the *HP Web Jetadmin 10.4 Installation and Setup Guide* and the *HP Web Jetadmin 10.4 User Guide*, PDFs are available from the HP Web Jetadmin support page (click the flag icon on the bottom of the page, and then select your country/region).

To view PDF files, Adobe Acrobat Reader must be installed on your computer. To download the latest Adobe Acrobat Reader, go to www.adobe.com/products/acrobat/readstep2.html.

Online Help

The HP Web Jetadmin online Help provides detailed information about using the software to configure and manage devices on the network. Use the **Contents**, **Index**, and **Search** tabs to navigate the online Help.

Each page in HP Web Jetadmin has a help icon (?) on the content toolbar. When you click the help icon and then click somewhere on the user interface, HP Web Jetadmin displays the context-sensitive help for that specific portion of the user interface.

To access external links, the browser must have access to the Internet. If you are behind an Internet firewall, you might need to configure proxy servers. Contact the network administrator to determine the appropriate settings for the browser.

Technical Support

HP maintains an extensive Web presence to provide information and assistance. To obtain technical support for HP Web Jetadmin, use the following links:

- www.hp.com/go/webjetadmin

  Provides access to Premium Support, Consulting Services, and a variety of self-help information, such as support documentation and white papers.

- http://support.hp.com

  Provides access to 24/7 online support for your country/region.

Getting Around in HP Web Jetadmin

The user interface for HP Web Jetadmin is designed to be efficient and intuitive, limiting the number of steps required to complete a task and streamlining software operation.

Application Views in HP Web Jetadmin

HP Web Jetadmin can be separated into three views accessible through the lower portion of the left navigation pane:

- Device Management on page 84 for managing all device-related functions.
- Print Management on page 269 for managing print queues and drivers on remote servers and workstations.
- Application Management on page 277 for managing application functionality such as users and roles, security, and software updates.

Top Menu Bar

The features that are available from the top menu bar change depending on the application view, plug-ins that are installed, and version of HP Web Jetadmin. The top menu bar can be used to quickly access product functionality.

The following menus are available from the top menu bar:

- **File** menu—Use this menu to perform tasks such as adding new items (for example, roles, groups, and templates), displaying a print preview or printing the device list that is currently displayed, and exiting HP Web Jetadmin.
- **View** menu—Use this menu to perform tasks such as specifying the columns that are displayed in the device lists, refreshing the device list, specifying which predefined device lists are displayed in the **Device Management** navigation pane, and specifying which columns are included in device lists to identify devices.
- **Tools** menu—Use this menu to perform tasks such as exporting device list information, managing Feature Packs, discovering devices, and managing the global settings for HP Web Jetadmin.
- **Help** menu—Use this menu to perform tasks such as displaying the context help, accessing the HP Web Jetadmin support page, and displaying information about HP Web Jetadmin (for example, version installed, End-User License Agreement, copyright information, and installed licenses).

Preferences

Preferences for lists (in Device Lists on page 105 and Groups on page 121) lets you manage data displayed in those lists. The top menu bar changes depending on the application view, presence of plug-ins, and the version of HP Web Jetadmin.

Device Filters

You can select which device lists or filters are displayed in the left navigation pane.

To configure device filters, perform the following steps:

1. From the top menu bar, select **View** > **Preferences** > **Device Filters**. The **Preferences** page is displayed with fields for device filters.
2. To display device filters in the left navigation pane under **All Devices**, move the filters from **Available filters** to **Selected filters**.

   To remove filters from the left navigation pane, select them in **Selected filters** and move them to **Available filters**.
3. To save these settings and continue setting other options, click **Apply**. Then click the next option to configure in the left menu bar. To save these settings and close this window, click **OK**.

Device Identification

Individual users can customize device tools to reflect only the device information that is most important to them. Space on device lists can be limited, so you should carefully choose the columns to be displayed. You can select columns to identify the devices on the **Select Devices** page, on the device list pages in **Device Lists** (Device Lists on page 105) and in **Device Groups** (Groups on page 121) and in the **Status** tab (Status Tab on page 85).

To configure how devices are identified, perform the following steps:

1. From the top menu bar, select **View** > **Preferences** > **Device Identification**. The **Preferences** page is displayed with fields for device identification.
2. To display fields as columns on device lists throughout HP Web Jetadmin, move them from **Available fields** to **Selected fields**.

   To remove columns from device lists, move the fields from **Selected Fields** to **Available Fields**.
3. To save these settings and continue setting other options, click **Apply**. Then click the next option to configure in the left menu bar. To save these settings and close this window, click **OK**.

Application Log

The application log records all of the transactions that occur. The application log includes the following information:

- The transaction that occurred.
- The details of the transaction.
- How the transaction was triggered, such as a user or group policy.
- The user who triggered the transaction.
- The date and time the transaction was triggered. If a time is not specified, the transaction was just triggered.

View the application log

1. Go to **Tools** > **Application Log**. The **Application Log** window opens.
2. To display a specific range of log entries, select the start date from the calendar in the **Show log entries from** field, select the end date from the calendar in the **to** field, and then click the **Apply Time Range** button.
3. To sort the application log entries, click a column header.

Refresh the log entries

▲ Click the **Refresh** button.

Edit the application log settings

▲ To configure how long the application log entries are saved, maximum number of log entries that are saved, and whether the log entries are archived, click the **Edit Log Settings** button. The **Options** window opens with the **Application Log** option selected. For more information, see Configure the Settings for the Application Log on page 59.

Clear the application log

1. Click the **Clear Log** button.
2. On the **Clear Application Log** window, click the **OK** button.

Status Bar Features

The status bar spans the bottom of the page and includes information about:

- **Activity indicator**: indicates the status of HP Web Jetadmin. If HP Web Jetadmin is processing a background activity (for example, refreshing a device or getting updated data about a device), it is displayed in this area (the area includes the icon/menu and the status message). If more than one activity is underway, the user can see the list of what is happening by clicking on the activity indicator. They can select an entry from the list to see the status message associated with that activity. If a new activity starts it will change what is shown (otherwise the selected activity message will continue to show until the activity completes).

  If multiple activities are in progress, you can see the list of all of those activities by clicking on the **Activity indicator**. You can select an entry from the list to see the status message associated with that activity.
- **Device counts**: when in device lists, this indicates the device you have highlighted and a count of all devices in the displayed list.
- **Layout**: when in device lists, displays the type of layout being shown.
- **Filter**: when in device lists, states whether or not filters are in use.
- **Map**: identifies the item on the map. This information is included in the activity/status message area and is not a separate area on the status bar.

Page Layout in HP Web Jetadmin

Each page in HP Web Jetadmin has the following features:

- A left navigation pane that lists all functions for each separate view (Left Navigation Pane on page 34).
- An area on the right that displays content or task modules providing access to related features or tasks (Task Modules on page 35).
- A work space that changes depending on the view and the feature selected (Workspace on page 35).

You can resize columns for most lists by clicking and dragging the column headers.

Left Navigation Pane

HP Web Jetadmin has a navigation pane on the left side of the user interface that displays a tree for the current view (**Device Management**, **Print Management**, or **Application Management**). The tree provides an organized display of the functionality of the view. The **Device Management** view contains most of the functionality of HP Web Jetadmin and, therefore, has the most complex tree.

Many parts of the navigation tree have right-click functionality. An example of this is Discovery on page 134, where you can select an item from the **Discover devices** right-click menu.

Other parts of the tree, such as Device Groups (Groups on page 121), have drag-and-drop functionality enabled. Devices can be selected in device lists within the workspace and dragged into Device Groups. The selected devices are added as group members. Many top-level nodes can invoke summary functionality in the workspace. By selecting a top-level node, such as Alerts, the workspace in the right-hand portion of the interface contains a summary of the Alerts features. The task modules that are specific to a feature (such as Alerts) are then displayed in the work space. You can alter the feature summary by selecting or deselecting the task modules that are important to you. (See Task Modules on page 35.)

Task Modules

Task modules are flexible blocks of specific or targeted functionality designed to help a you perform a task or obtain feature information. You can find task modules in many of the workspace pages or in the docking area (see Docking Task Modules and Maps on page 35). In either case, you can enable or disable task modules on a per-user basis. You can hide or display task modules, and you can move them within the content area.

A **Current Task** task module is initially included in the task module docking for each section. For example, in Device Groups, the Current Tasks - Device Groups task module lists all tasks within **Groups**.

Docking Task Modules and Maps

The docking feature in HP Web Jetadmin enables you to dock task modules and maps. You can:

- Specify a map or a user-specific collection of task modules in HP Web Jetadmin to be docked.
- View the collection of task modules regardless of the current focus of the application.
- Undock the maps or collection of task modules to maximize application space.
- Dock maps or task modules to any one of four sides of the work space.
- Hide maps or the collection of task modules beneath a tabbed control that enables access at any time.
- View a Current Tasks task module, which changes depending on the focus (context) of the application.

To display the **Task Module** docking area, click **View** > **Task Modules** > **Task Module docking area**. To display the **Map** docking area, click **View** > **Device Modules** > **Map**. The **Map** menu item is available when you have selected a group; the group does not have to have to a map associated with it. The **Map** module is visible if the **Map** menu item has been selected to show the module and if the selected group has a map associated with it. Note here that the map module may not be visible even if it is “displayed” because it is only visible when you are on a group that has a map attached to it.

Workspace

The large area on the right side of the navigation tree is the HP Web Jetadmin workspace. This area changes depending on the View and Navigation tree elements selected. In many cases, the focus of this area can be a summary of a feature space. You can obtain this summary by selecting any top-level element within the navigation tree. Elements with the + symbol next to them are top-level elements that invoke a summary focus. An exception to this is the **All Devices** list. When **All Devices** is selected in the left navigation pane, the device list is displayed in the workspace. The workspace can also reflect specific feature functionality. Whenever a sub-level element (generally one that has no + symbol next to it) is selected, the workspace reflects specific functionality. For an example, see View Discovery History on page 165.

Wizards

Wizards provide a collection of steps in the required order for a user to accomplish a task successfully. Every wizard is launched in a window separate from the main application by using many different controls including right-click menu items and task modules. Many of the wizards in HP Web Jetadmin are launched from multiple controls in different parts of the application. An example of a wizard is **Create Group** (Create a New Device Group on page 126). After your start the wizard, you are prompted for the group type, the group name, and the group members; after you identify that information, you can continue with the displayed steps until the task is successfully completed. Confirmation and results pages provide both a safeguard and additional details about the task.

Need Info Wizard

The **Need Info** wizard is displayed when you try to perform a device configuration but provide incorrect sensitive configuration information.

Some configuration items require additional information, such as an existing password, before setting the new configuration. If you fail to enter this required information correctly, the **Need Info** wizard is displayed, providing an opportunity to enter the correct information. The wizard displays one or more devices on the left, and prompts you for the required information on the right. You can only change the required information. All other information remains the same as originally entered.

For each device and each set of required information, you must click either **Set** or **Skip** to complete the wizard. You can select one or more devices in the list, enter the required information, and click **Set**. If you do not know the existing passwords or required information, you can click **Skip**. If you click **Skip**, that configuration item will not be set on that device.

When you click **Finish**, HP Web Jetadmin tries to complete the device configuration again. If additional information is required, the **Need Info** wizard is displayed again.

Other Features

- **Drag-and-drop**: You can drag-and-drop various items (for example, devices) onto functionality (reports, groups, and more) to save time and increase accuracy.
- **Errors Encountered within HP Web Jetadmin**: If the user interface has an error or cannot understand the input, it displays “error on page”. You can hover the mouse over the error icon to see information about the problem that exists on that page.
- **Identification of the HP Web Jetadmin Server**: The title bar on the HP Web Jetadmin client window always indicates the name of the computer system where HP Web Jetadmin is installed.
- **Determining the Software Version**: By using **Help > About**, an HP Web Jetadmin logo page can be launched. This contains the exact revision of the software in the xx.x.xxxxx format which represents MajorApplicationVersion.MinorApplicationVersion.Buildnumber number.

- **Client performance**: The client application performs many tasks locally to reduce traffic to the HP Web Jetadmin server and improve performance on the client. HP Web Jetadmin leverages the client application in the following ways to maximize performance:
  - The client application is built on Microsoft .NET Framework technology. The client application does not need to contact the HP Web Jetadmin server to complete user actions.
  - The client application stores and manages all of the graphics.
  - The HP Web Jetadmin server sends event notifications to the client application only on an as-needed basis.
  - The client application performs most of the list operations instead of the HP Web Jetadmin server.
  - Virtualization improves client performance because the HP Web Jetadmin server passes only the data that is required for display to the local host.
  - All of the clients share the update traffic from a single data set on the HP Web Jetadmin server.
  - Sometimes the settings for the network and HP Web Jetadmin can impact client performance. HP Web Jetadmin uses an economical polling pattern to gather information from devices. If a feature that causes HP Web Jetadmin to gather information from devices is added, the result might be less than optimal.
- **Running Multiple Clients**: You can run more than one HP Web Jetadmin client application on a single host, and you might also have multiple client sessions communicating simultaneously to different HP Web Jetadmin server applications. On a single host, you may also run multiple client sessions that are connected to the same HP Web Jetadmin server application.
- **Smart Client file cache**: The files for the Smart Client application and other Microsoft .NET Framework applications are stored in this file cache. The Smart Client file cache has the following characteristics:
  - Files are stored in the following directory:

    C:\Users\<*username*>\AppData\Local\Apps\2.0
  - Administrative access on the local machine is not required to install and remove the files and directories.
  - Microsoft .NET Framework imposes a 200 MB limit for the Smart Client file cache.
  - The Smart Client file cache contains the client debug control file and trace log. To manually clear these files, use the following Smart Client cache tool. The files are reloaded during the next run.

    ```
    Mage.exe -cc Del *.*
    ```
- **Copy and Paste**: In **Device Lists** , device information can be copied and pasted into other applications. Select one or more rows, click Ctrl-C or right-click on a device and then select **Copy**. When pasted, this information is formatted the same way a device list export would be: the first row is column headers and the subsequent rows are the selected devices.

  In the **Status** tab, you can select fields from the device information section and click Ctrl-C.

HP Web Jetadmin Server

HP Web Jetadmin runs on a server host allowing remote access from HP Web Jetadmin host clients. The following sections outline features and information about the HP Web Jetadmin server application.

HP Web Jetadmin and Distributed Environments

HP Web Jetadmin is scalable client/server software designed to support distributed environments. HP Web Jetadmin can be installed on either a server or on a user's desktop. It can be installed on multiple servers and the user desktop can support multiple instances of the HP Web Jetadmin client application running simultaneously.

The HP Web Jetadmin server performs many background tasks including discovery and configuration of devices, firmware retrieval, and application security. HP Web Jetadmin has a robust client application that runs on Microsoft Windows desktops. The client application displays device lists and groups and provides all the control interfaces needed for device management. Due to changes in the allocation of tasks between the client and server, HP Web Jetadmin offers significant performance improvements over earlier releases of the software.

Characteristics of the HP Web Jetadmin server-based application include:

- Can run on remote server-host or locally on client-host.
- Supports multiple clients (up to 15 or more) accessing a single HP Web Jetadmin server.
- Supports multiple client sessions on a single desktop accessing separate HP Web Jetadmin servers.
- Provides secure downloads of client application through a Microsoft Smart Client connection that is established through Internet Explorer.
- Communications through Microsoft .NET Remoting.
- Provides change event mechanism for the server to efficiently update application details at clients.
- Retrieves information from www.hp.com facilitating updates to software, firmware, and more.
- Offers update service for obtaining application patches, plug-ins, and more from www.hp.com.
- Automatically updates clients whenever newer server-based client components exist.
- Ensures that device credentials and user/roles details are securely stored by the server.
- Provides HTML online help content to clients.
- Communicates to devices, both network and PC-connected, from the server.
- Communicates from the server to other hosts (email, print queue, Active Directory, SNMP traps, and more).

How the HP Web Jetadmin Service Works

HP Web Jetadmin provides a variety of features that support the client, application, and device communication. HP Web Jetadmin runs on the server as a service. The HP Web Jetadmin service (HPWJA Service) contains a simple HTTP server that downloads the Smart Client application and provides the online Help. For more information about the Smart Client application, see Deploy the Smart Client on page 15.

The HP Web Jetadmin service also handles the client-driven requests. HP Web Jetadmin communicates with devices in ways that are both user-driven and automated as background activities. Background activities include the following:

- **Slow polling**: Keeps network traffic to a minimum even when multiple client sessions are running.
- **User-scheduled activities**: Includes discovery, firmware upgrades, and device configuration.

  A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

The HP Web Jetadmin service has the following characteristics:

- The HP Web Jetadmin service runs in the background.
- The HP Web Jetadmin service supports the following communication interfaces:
  - HTTP
  - HTTPS
  - TFTP
  - SNMP
  - Microsoft .NET Remoting
  - .NET Listen
  - TFTP send/receive
  - SLP
- The client application is first downloaded through a Smart Client connection that is launched through Internet Explorer.
- Client communication works through .NET Remoting, which provides both authentication and encryption.
- HP Web Jetadmin communicates with devices and other hosts through user-driven requests or automated background activities.

Overview of Directories and Files

Resources for HP Web Jetadmin are available in the following directories on the server:

- C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin
- C:\Program Files\HP Inc\Web Jetadmin 10
- C:\Program Files\Microsoft SQL Server\MSSQL.10.HPWJA

  This is the Microsoft SQL Server database instance for HP Web Jetadmin.

HP Web Jetadmin includes the following services:

- HP Web Jetadmin Core Service:

  C:\Program Files\HP Inc\Web Jetadmin 10\bin\HPWJAService.exe

  Display name: HPWJAService
- MSSQL$HPWJA (must be started before HPWJAService):

  C:\Program Files\Microsoft SQL Server\MSSQL.10.HPWJA\MSSQL\Binn\sqlserver.exe

  Display name: SQL Server (HPWJA)

The following table provides a list of the files that are typically found in the directories.

Directory	Files
C:\Program Files	• Core application components, DLLs, and more • HP Web Jetadmin service executable • Files downloaded through Smart Client application install • Universal Print Driver

Directory	Files
	- Certificates - End User License Agreements (EULAs) - Other documents such as the release notes and online user documentation.
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin	- All application settings (file-based) - Trace control file for debug mode - Trace file when debug mode (server) is enabled

The user settings and data that are stored in the HP Web Jetadmin database can be backed up and restored. For more information, see the *Back up, Restore, and Clone an HP Web Jetadmin Installation* white paper. This white paper is available from the HP Web Jetadmin support page (in English). The user settings and data that are not stored in the HP Web Jetadmin database are stored in files that are available in the following directory:

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin

Microsoft SQL Database Overview

HP Web Jetadmin uses a Microsoft SQL Server database instance to store and manage the captured device data. SQL Server Express Edition is embedded in HP Web Jetadmin. SQL Server Express Edition requires Microsoft .NET Framework, has a 4 GB limitation on the size of the database, and can exist on a host with any other SQL Server implementation.

If SQL Server Express Edition is not already installed, it is installed during the initial HP Web Jetadmin installation. HP Web Jetadmin can coexist with other versions of SQL Server if they are installed on the same host.

During the installation, HP Web Jetadmin executes OSQL commands that install the database components, including the HP Web Jetadmin database instance and data structures. There are no user-specified attributes for any of the SQL elements during the installation.

HP Web Jetadmin creates a named Microsoft SQL Server Express Edition database instance during the installation. The database instance is a service that runs in Windows Service Manager MMC and has a dependency on the HP Web Jetadmin service (HPWJA Service). You can also observe the HPWJA Service in Windows Service Manager MMC. You must stop the HPWJA Service before you can stop the Microsoft SQL service.

HP Web Jetadmin manages the proprietary HP Web Jetadmin database. HP Web Jetadmin must be the only entity that connects to the database. The database does not contain user-accessible details and cannot be used as a source of raw content for other user processes.

The HP Web Jetadmin database contains the following data:

- Application logs (Application Log on page 33)
- User and role associations (User Security on page 278)
- User preferences (Users on page 283)
- Role permissions (Roles on page 280)
- Credentials (Add Credentials for Devices on page 119)
- Device groups (Groups on page 121)
- Tasks (throughout HP Web Jetadmin)

- Templates (throughout HP Web Jetadmin)
- Devices and supported device objects (Device Lists on page 105)
- Data collections (Data Collection on page 225)

Low-privilege Service Account

The HPWJA Service and Microsoft SQL Server (HPWJA) service run under the NT AUTHORITY\Network Service account, which is a low-privilege account on the local system. Using this account for both of these services is a critical security feature for HP Web Jetadmin. The NT AUTHORITY\Network Service account must have access to the following locations.

Location	Rights required
C:\Program Files\HP Inc\Web Jetadmin 10 (including all subdirectories and files in the directory structure)	Read & execute, List folder contents, and Read access
Registry key: HKEY_LOCAL_MACHINE\SOFTWARE\HP Inc.\HPWebJetadmin\WjaService (including all subkeys)	Full control and Read access
Registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Hewlett-Packard\WJAUpdateService (including all subkeys) IMPORTANT: This registry key applies only to HP Web Jetadmin 10.2 (10.2.59093) through HP Web Jetadmin 10.4 (10.4.98174). Previous versions do not use this registry key.	Full control and Read access
Registry key: HKEY_LOCAL_MACHINE\SOFTWARE\HP Inc.\WJAUpdateService (including all subkeys) IMPORTANT: This registry key applies only to HP Web Jetadmin 10.4 SR1 and later. Previous versions do not use this registry key.	Full control and Read access
Microsoft SQL directory and file structure	Full control and Read access
C:\Windows\ServiceProfiles\NetworkService (including all subdirectories and files in the directory structure)	Full control and Read access

Although you can run both of the HPWJA services under a different account, HP does not provide support to assist with this configuration. Changing the Microsoft Windows account that the HPWJA Service or SQL Server (HPWJA) service runs under might cause unexpected behavior in HP Web Jetadmin or cause both of these services to not start. In this case, HP Web Jetadmin will not run at all.

⚠ CAUTION: If you run HP Web Jetadmin under any account other than the NT AUTHORITY\Network Service account, you do so at your own risk.

To verify which account a service is running under, perform the following steps:

1. Use one of the following methods to open the Microsoft Windows Services window:

   - **Start** > **Programs** > **Administrative Tools** > **Services**
   - **Start** > **Run** > `Services.msc`

2. Double-click the service.
3. On the **Properties** screen, click the **Log On** tab.
4. Verify that the NT AUTHORITY\Network Service account is listed in the **This account** field.

HTTP Service

HP Web Jetadmin contains a small and embedded HTTP/HTTPS service. This service exists for three reasons:

- Smart Client application delivery (initial client access).
- Help content delivery (during client session).
- Device application file hosting (devices get jar file when directed by **Device Management** features).

A few key points about this HTTP service include:

- The integrated HTTP service is simple and only exists for the purpose of distributing files.
- The service contains no script execution interpreters or cgi-bin capability.
- The service does not allow file navigation.
- The service does not execute read/write calls to the HP Web Jetadmin database.
- The HTTP/HTTPS server is integrated into the HP Web Jetadmin service, which runs as a low-privilege account on the local host.
- The HTTP service does not run in kernel mode.

The HTTP service can be configured to run default HTTPS and uses certificates that are obtained through a local certificate-authority. When HTTPS is enabled, it enforces authentication between the users IE browser and the local HTTP service. This provides tighter security for initial HP Web Jetadmin client launch than is provided by HTTP. Some environments may require that all HTTP servers enforce and run default HTTPS.

Characteristics of the HTTPS service are:

- HTTPS can be enabled as part of a post-install procedure with HP Web Jetadmin security settings.
- HTTPS requires that the user obtain a certificate from a certificate authority.
- HTTPS can only be enabled through a client running on the local system hosting HP Web Jetadmin software.

The default port for HTTP is 8000. The default port for HTTPS is 8443. If the HP Web Jetadmin installation requires a different port on the HTTP server that is embedded in HP Web Jetadmin, change the `HttpPort` and `HttpsPort` entries in the HP.Imaging.Wjp.Core.WebServer.config.xml file. This file is available in the following directory:

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config

If you change the port entries, you must restart HP Web Jetadmin.

To change the program link, go to **Start** > **All Programs** > **HP Web Jetadmin 10**. Right-click **HP Web Jetadmin**, and then select **Properties**. Change the port number in the link variable to the new port number.

Localization

HP Web Jetadmin is localized in several languages. All the available languages are automatically implemented when you install HP Web Jetadmin. There are no additional steps required after the installation to enable the language support.

The Windows Region and Language settings on the client used to access HP Web Jetadmin determine the language in which the HP Web Jetadmin software and online Help are displayed. For more information about specifying the Region and Language settings, see the Microsoft documentation for the version of Windows that is running on the client.

If the Region and Language settings on the client specify a language that HP Web Jetadmin does not support, the software and online Help are displayed in English.

HP Web Jetadmin might not be localized at every software release. If a software release is not localized, some of the new content in the software and online Help for that release might be displayed in English while other content is displayed in the language specified by the Region and Language settings.

When you use the Export feature, the exported content might contain information based on the Region and Language settings specified on the server where HP Web Jetadmin is installed instead of the Region and Language settings specified on the client.

Localized versions of the *HP Web Jetadmin 10.4 Installation and Setup Guide* and the *HP Web Jetadmin 10.4 User Guide* are available from the HP Web Jetadmin support page (click the flag icon on the bottom of the page, and then select your country/region).

HP Web Jetadmin Network Traffic and Behavior

The HP Web Jetadmin server application performs a number of actions including:

- **Client event notifications**: When a user logs in to HP Web Jetadmin, a separate client application runs on the local desktop host. The HP Web Jetadmin server uses a TCP connection to notify the client application when changes occur. The client application then connects to the Microsoft .NET Remoting channel on the HP Web Jetadmin server and requests the updated information. The HP Web Jetadmin server sends event notifications only when the following events occur:
  - Updated data for the client application is available
  - The HP Web Jetadmin server has not received any communication from the client application for a predetermined period of time
- **Supplies Alerts Polling**: When devices exist in supplies groups, Supplies Alerts are enabled (Alerts on page 188). The Alerts features affect both user alerts (by email or a log) and other supplies-related reports. All of the alerts are based on user-selected threshold values. When the supply level value for a device is not close to the specified supply threshold, HP Web Jetadmin polls that device more slowly, taking up less network bandwidth. When the supply level value for a device is close to the specified supply threshold, HP Web Jetadmin polls that device more often. This smart-polling mechanism ensures that the supply level alert is delivered in a timely manner while limiting the polling that is done on the network. Supplies Alerts polling is integrated with other kinds of polling within the HP Web Jetadmin system which means that polling is performed only when stale information is detected.
- **Slow Polling**: HP Web Jetadmin uses a slow-polling mechanism that queries for device information. This mechanism is user-configurable; faster settings put a larger load on the network (see documentation on application settings and the training module on application maintenance). This slow-polling mechanism is used for a variety of tasks including:

  - Users are viewing lists and one or more displayed information attributes has become stale.
  - Automatic Device Groups exist (Groups on page 121).
- **Background Tasks**: Many features in HP Web Jetadmin can be launched automatically or manually by a user logged into a client application session. In either case, these can become background tasks that can be run without a user being logged into a client application session. Background tasks are managed centrally by HP Web Jetadmin software and the user can display them at any time through a task manager interface. The **Active Tasks** task module is one way users can view running tasks.

HP Web Jetadmin Client

Users gain access to HP Web Jetadmin through a local Microsoft .NET Framework client application. The client application runs on any supported client desktop. The first time a client application accesses the HP Web Jetadmin server, HP Web Jetadmin installs client files and launches a Windows client session. The client session communicates with HP Web Jetadmin on the server. Client application files are left in the users' Local Settings directory and updated as needed. The server and client applications can run on the same host or on different hosts.

ClickOnce Software Installation and Launch

The following events occur when you start the Smart Client installation and launch:

1. Client using Internet Explorer browses HTTP service (URL: http://server:8000).
   - The server detects Microsoft .NET Framework on the browser client.
   - Browser is redirected to HP Web Jetadmin.
   - The browser passes the application to .NET Framework.
   - .NET Framework verifies the signature, reads the XML, and launches Smart Client.
2. Smart Client is launched.
   - For the first run, an Application Run dialog box is displayed to client.
   - 2MB files are downloaded through the HTTP service.
   - UIExec.exe is launched on client host.
3. Microsoft .NET Framework Remoting begins and uses port 4088.
   - For the first run, 50 MB files downloaded.
   - The HP logo page is visible.
   - The client files are updated if a newer version is detected.
4. HP Web Jetadmin Client application is started.
   - The client begins detecting events, executing calls, and more.
   - The help content traverses the HTTP service.
   - All other client communication uses .NET Framework Remoting.

Notification that Microsoft .NET Framework Is Required

The HP Web Jetadmin server detects whether or not Microsoft .NET Framework is installed on the host. If .NET Framework is not installed on the host, HP Web Jetadmin displays a message that provides instructions to install .NET Framework or start HP Web Jetadmin.

Admin privileges are required to install .NET Framework. The **Start HP Web Jetadmin** link launches the client after .NET Framework is installed.

HP Web Jetadmin Client's Sleep State

When the HP Web Jetadmin client is started and then goes into a sleep or power-save state, it may fail with an Unexpected Error when the client system is brought back up to a “run” or “on” state. This is due to the HP Web Jetadmin server host losing regular contact with the client host. The server host, once it loses regular contact, will break the connection with the client session. Once the client system is out of the sleep state and tries to contact the server, access is denied and the client stops causing an Unexpected Error. You need to then restart the client.

Shared Configuration Options for all Views

The following sections describe the configuration options that are shared among all the views in HP Web Jetadmin. To access these shared configuration options, go to **Tools** > **Options** > **Shared**.

General Shared Configuration Options

General settings are those settings that do not fit into any other category for shared configuration options.

Configure the Database Settings

This option allows you to select the memory size for the database.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools > Options > Shared > General > Database**.
2. Select the memory size from the drop-down list.

   NOTE: This feature is not available when HP Web Jetadmin is using a remote database.

3. Select database query timeout from the drop-down list.
4. Click the **Apply** button.

Configure the Data Collection Option

The Data Collection feature collects data about your printers and implementation of HP Web Jetadmin and anonymizes the data. HP Web Jetadmin uses an Internet connection to transmit the anonymized data to HP. HP uses the anonymized data to improve products and services.

IMPORTANT: HP is committed to protecting your privacy and the integrity of your computer. You can enable and disable this feature at any time. Your name, address, email address, and other sensitive data are not sent to HP.

To configure this feature, perform the following steps:

1. Go to **Tools** > **Options** > **Shared** > **General** > **Data Collection**.

2. For more information about this feature, click the **Data Collection and Use Statement** and **HP Privacy Statement Online** links.

3. To enable the collection of anonymized data, select the **Enable data collection** checkbox.

   -or-

   To disable the collection of anonymized data, clear the **Enable data collection** checkbox.

Shared Configuration Options for Network

Network settings impact how HP Web Jetadmin behaves on your network and how it performs for functions like discovery.

Configure the SNMP Settings

HP Web Jetadmin uses the SNMP protocol to gather information from the devices. You can configure the SNMP timeout value and SNMP retries. On some networks, SNMP timeouts and retries should be increased because of low bandwidth or slow links. Also, decreasing SNMP timeouts and retries might improve discovery performance on some networks.

Your network topology might cause slow response times; if so, increase the timeout value. Or, you might want to set the number of retries to a higher number to protect against packet loss.

⚠ CAUTION: Increasing SNMP values can increase the time required to perform a discovery.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools > Options > Shared > Network** and select **SNMP**.

2. Configure the desired settings:

   - **SNMPv1 timeout value**: Specify how long HP Web Jetadmin waits for a reply from a network query that is sent to SNMPv1 devices. The default is 500 ms.

   - **SNMPv3 timeout value**: Specify how long HP Web Jetadmin waits for a reply from a network query that is sent to SNMPv3 devices. The default is 1000 ms.

   - **SNMP retries**: Specify how many times HP Web Jetadmin retries an SNMP communication with devices after a timeout occurs. The default is 3.

3. Click the **Apply** button.

Configure the HTTP Settings

HTTP options enable you to specify a web proxy server and port number from which a client can access the proxy server. A security barrier is enabled on your internal network when accessing external web sites that are required by HP Web Jetadmin.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools** > **Options** > **Shared** > **Network** and select **HTTP**.
2. Configure the desired settings:
   - **HTTP proxy address settings**: If your environment includes a proxy server, enter the **HTTP proxy address settings**. Identify the address and the port number HP Web Jetadmin should use to communicate through the proxy server.
   - **HTTP proxy user settings**: Check **Use HTTP proxy credentials** to use HTTP proxy credentials and then enter the user and password.
   - **Download settings**: Check **Allow download** to allow downloads.
   - **HTTP timeout**: Specify the number of seconds that an HTTP connection can be idle before a timeout occurs. The default is 30. On networks that have a low bandwidth or slow links, you can increase the HTTP timeout period. On some networks, decreasing the HTTP timeout period might improve the performance of discoveries.

     The HTTP timeout also impacts the ClickOnce Smart Client start-up.
3. Click the **Apply** button.

Configure the HTTPS Settings

The HP Web Jetadmin HTTP service runs without certificates. If you add a certificate, the HTTP server runs in HTTPS mode, which means that secure sockets layer (SSL) communication is enforced. For more information about running in HTTPS mode, see Implement SSL on page 13.

IMPORTANT: For new server certificates, you must install 2048-bit certificates. Any previously installed 1024-bit server certificates continue to function correctly.

Configure the DNS Settings

By default, HP Web Jetadmin enables DNS lookups. You can turn them off if desired.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools** > **Options** > **Shared** > **Network** and select **DNS**.
2. Configure the desired settings:
   - **Enable DNS lookups**: Check this box to enable HP Web Jetadmin to perform DNS lookups.
3. Click the **Apply** button.

Shared Configuration Options for Email

Options in Email provide a way to configure settings to enable email communications from HP Web Jetadmin and also to manage email addresses.

Configure the SMTP Gateway Settings

Server, user, and email settings must be configured for the SMTP gateway that HP Web Jetadmin uses to send email messages to users. These email messages contain information about alert events, reports, exported report data, exported device list data, and so on.

Configure the SMTP server settings

1. Go to **Tools** > **Options** > **Shared** > **Email** > **SMTP**.
2. In the **SMTP server settings** section, enter the IP address or hostname, the port for the SMTP gateway, and click the box next to Use SSL.

NOTE: To configure smtp.office365.com server, enable Use SSL and enter port 587.

3. To verify that the SMTP server settings are valid, click the **Verify** button. If the SMTP server is valid, the IP address or hostname is underlined.
4. If the SMTP server requires authentication, perform the following steps:

TIP: To test whether the SMTP server requires authentication, send a test email message without specifying the SMTP user settings. If the test is successful, the SMTP user settings are not required.

   a. In the **SMTP user settings** section, enter the user name, password, and domain that are required for authentication on the SMTP server.

   b. In the **Default 'from' address** box, enter the email address that is included in each email that HP Web Jetadmin sends. The default is wja@hp.com.

5. Click the **Apply** button.

Send a test email message

Before you send a test email message, you must configure the SMTP gateway settings.

1. Click the **Test** button.
2. On the **Test Email Settings** window, enter the email address for the recipient of the test message in the **'To' address** box.
3. Click the **OK** button.

Manage the Shared Email Addresses

This option allows email addresses to be added and maintained for use in Reports on page 215, Alerts on page 188, and Device Lists on page 105.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools > Options > Shared > Email > Addresses**.
2. Configure the desired settings:
   - **New**: Type the new email address and select the preferred language. Then click **OK**.
   - **Remove**: Select an existing email address and click **Remove**. When prompted, confirm the action.
   - **Edit**: Select an existing email address and click **Edit**. Make changes to the email address and click **OK**.

Shared Configuration Options for Discovery

You can search for devices located within a range of IP addresses (multiple IP ranges can be designated).

Configure Large Subnets for IP Range Discoveries

You can choose to specify a large subnet range using the larger subnet address feature (**Tools** > **Options** > **Shared** > **Discovery** > **Methods** > **IP Range** > **General**). Large networks are considered any network bigger than a Class B network, which has up to 65,000 nodes.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools > Options > Shared > Discovery > Methods > IP Range > General**.
2. To search for subnets larger than Class B (65,000 nodes), click **Allow large subnet discoveries**.
3. Click the **Apply** button.

To define the IP ranges, see Manage the IP Ranges for Discoveries on page 49.

Manage the IP Ranges for Discoveries

HP Web Jetadmin can search for devices located within a range of IP addresses (multiple IP ranges can be designated) (IP Range Discovery on page 142).

Use the following steps to configure this option:

1. On the top menu bar, access **Tools > Options > Shared > Discovery > Methods > IP Range > IP Ranges**.
2. Choose the action to take:
   - Select an IP range.
   - **Add**: Add an IP range. Type the range in **First address** and **Last address**; then type a description (if desired) in **Description**. Click **Add**.

     Calculate range: To calculate a range, click **Calculate range**. The **Calculate IP Range** page is displayed:

     – **Subnet from my computer**: Automatically use IP address ranges currently found on the local subnet of your computer. You can add a description in **Description** if desired.

     – **Subnet from WJA server**: Automatically use IP address ranges currently found on the subnet of the HP Web Jetadmin server. You can add a description in **Description** if desired.

     – **Subnet from network address**: Type a known IP address and subnet mask. You can add a description in **Description** if desired.
   - **Edit**: Make changes to IP ranges. Follow the steps in the bulleted item above for adding an IP range.
   - **Delete**: Remove addresses from the list by highlighting the address and clicking **Delete**.
   - **Import**: If desired, import a range list by clicking **Import**; then browse for the range list.
   - **Export**: If desired, export a range list by clicking **Export**; then browse for the location where you want to store the range list.

Manage the Address Lists for Specified Address Discoveries

The **Specified Address** option lets you manage lists of specified addresses for discoveries. The addresses and groups managed through this option can be selected while launching or scheduling discoveries through the **Device Discovery** wizard (see Discover Devices on page 160).

Use the following steps to configure this option:

1. On the top menu bar, access **Tools** > **Options** > **Shared** > **Discovery** > **Methods** > **Specified Address**.
2. Add a new address group:
   a. Click **New**. The **Add a specified address group** page is displayed.
   b. Type the name of the address group.
   c. To add an IP address to the group, click **Add**.
   d. The **Add specified address** dialog is displayed. Type the IP address or hostname.
   e. Click **Add**. To continue adding IP addresses or hostnames, repeat these steps.
   f. When all IP addresses or hostnames have been added, click **Close**.
   g. Click **OK** two times.
3. Edit a specified address group name:
   a. Highlight the group and click **Edit**. The **Add specified address group** page is displayed.
   b. Change the group name.
   c. Click **OK** two times.
4. Remove a specified address from a group:
   a. Highlight the group and click **Edit**. The **Add specified address group** page is displayed.
   b. Highlight the IP address or hostname and click **Remove**.
   c. Click **OK** two times.
5. Delete a specified address group:
   a. Highlight the group and click **Delete**.
   b. Click **OK**.

Shared Configuration Options for Server Maintenance

Server Maintenance settings help you automatically maintain your server.

Configure the Schedule for Server Maintenance

Your server is automatically cleaned up daily, but you can specify the time of day that the cleanup should occur. This is when the HP Web Jetadmin service performs routine clean-up tasks. These tasks are better performed when the HP Web Jetadmin service is not busy doing other processor intensive tasks such as **Discovery**, **Reports Data Collection**, exporting **Device List** data, and more. Select a time that you know the HP Web Jetadmin service is not doing other processor intensive tasks.

The scheduled **Server Maintenance** task removes unneeded data from the HP Web Jetadmin database tables. This is temporary data used in normal HP Web Jetadmin processes throughout the day. No user or device-related information is removed from the system.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools** > **Options** > **Shared** > **Server Maintenance** and select **Schedule**.
2. Enter the time you want the server cleaned up every day.
3. Click the **Apply** button.

Manage the Discovery History

Use this option to configure the number of days that HP Web Jetadmin retains the discovery history, clear the entries in the discovery history, archive the expired entries in the discovery history, and clear the discovery history archive file.

Configure the retention period for the discovery history

1. Go to **Tools** > **Options** > **Shared** > **Server Maintenance** > **Discovery**.
2. From the **Retention time** list, select the number of days that HP Web Jetadmin retains the discovery history. The default is 90 days.
3. Click the **Apply** button.

Clear the discovery history

1. Go to **Tools** > **Options** > **Shared** > **Server Maintenance** > **Discovery**.
2. Click the **Clear History** button.

Archive the expired entries in the discovery history

1. Go to **Tools** > **Options** > **Shared** > **Server Maintenance** > **Discovery**.
2. Select the **Archive expired entries to file** checkbox.
3. Click the **Apply** button.

Clear the discovery history archive file

1. Go to **Tools** > **Options** > **Shared** > **Server Maintenance** > **Discovery**.
2. Click the **Clear Archive** button.

Configure the Retention Period for the Configuration History

This option allows you to select the number of days to retain configuration history.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools** > **Options** > **Shared** > **Server Maintenance** > **Configuration**.
2. In the **Retention time** box, specify the number of days that the configuration history is retained. The default is 30.
3. Click the **Apply** button.

To clear all previous configuration history, click **Clear History**.

Configure the Retention Period for the Alerts History

This option allows you to select the memory size for the database.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools** > **Options** > **Shared** > **Server Maintenance** > **Alerts**.
2. In the **Retention time** box, specify the number of days that the entries in the alerts log are retained. The default is 30.
3. Click the **Apply** button.

To clear the log, select **Clear History**.

Manage the Report Data

As data is collected for reports, it is stored in tables within the HP Web Jetadmin database. You can specify how long to retain data for reporting purposes and delete data that has been retained by HP Web Jetadmin for reporting purposes. Data retention is set to one year beyond the initial collection date. You can change this value to a maximum of five years through this option.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Shared** > **Server Maintenance** > **Reports**.
2. Select the type of data to delete:
   - **All data**: Delete all data that has been collected to-date, as though no data collections had ever been done.
   - **User data**: You will be asked to identify the user and then confirm your request.
   - **Device data**: Delete device data that has been collected to-date, as though no data collections had ever been done.
3. Click **Delete Data**. Confirm the delete request by clicking **Yes**.
4. In the **Retention time** box, specify the number of years that the report data is retained. The default is 1.
5. Click the **Apply** button.

Shared Configuration Options for Credentials

HP Web Jetadmin can configure many devices simultaneously. This saves device administrators from having to contact every device separately for the purpose of assigning configuration items like passwords and other credentials. Many environments have password policies that make the device administrator have to reconfigure security credentials periodically. The power of HP Web Jetadmin fleet management lends itself to configuration of many devices simultaneously.

Credentials Store

The concept of a Credentials Store is not new to HP Web Jetadmin. Older versions of HP Web Jetadmin stored credentials onto the devices as they were used and configured. This feature keeps HP Web Jetadmin users from having to provide a credential every time a device is configured that requires one.

The Credentials Store is a portion of the HP Web Jetadmin database that securely encrypts and stores device credentials when ever a correct credential value is authenticated at the device. These values are stored on a per credential and per device basis.

Here is a list of HP device credentials used by HP Web Jetadmin:

- EWS Password: Blocks unauthorized access to the device-embedded HTTP interface. It is also synchronized with the HP Jetdirect telnet password.
- File System Password: Protects the printer disk and other storage facilities from unauthorized access.
- SNMPv3 Credentials: Consists of user name, passphrase1, and passphrase2 which are all used when SNMPv3 is enabled. This version of SNMP secures and authenticates communication between management applications like HP Web Jetadmin and the device. This protocol is used when strong security is required.
- SNMP Set Community Name: A grouping mechanism for SNMPv1/v2 used as a security mechanism by many customers. Device configuration is not possible without knowledge of the Set name value. The Set name value traverses the network in clear text and can be “sniffed” by eavesdroppers.
- SNMP Get Community Name: Sometimes used to prevent device discovery from other HP Web Jetadmin installations. Devices only respond to Get packets that have the correct value. The Get name value traverses the network in clear text and can be “sniffed” by eavesdroppers.

Two actions cause the value of any credential to be stored:

- Configuration: The credential becomes stored once it has been configured onto the device.
- Use: The credential value, when used successfully, becomes stored.

HP Web Jetadmin reuses stored credentials any time it encounters the requirement for them. When configuring a device that has had a credential stored, you are not required to re-enter the credential into HP Web Jetadmin. The application uses the credential in the background. In fact, you are not even required to know the credential because HP Web Jetadmin is using stored values.

Credentials Delegation

With credentials stored in the Credentials Store, HP Web Jetadmin can apply them transparently any time the need arises. This is known as credentials delegation. While configuring devices, you do not have to remember or even know the credential to perform the configuration. You just need access to HP Web Jetadmin and device configuration features. Characteristics of credentials delegation are:

- Only one or a few device administrators know the device credentials.
- Some HP Web Jetadmin users are allowed configuration access to the devices via Roles and User Security.
- Users can be added or removed from this delegation through Roles and User Security (User Security on page 278).
- Other HP Web Jetadmin users can be restricted from device configuration.
- Knowledge about device passwords is required before you can change any password value.

Credentials delegation is used to allow configuration of devices without having to share the credential “secrets” across a large distribution. Staffs can control and configure devices while administrators control and configure passwords. Any user with access to devices and configuration features has delegated access to the **Credential Store**.

Credentials Needed

When HP Web Jetadmin, during an action such as device configuration, encounters a device with a credential such as SNMP Set Community Name, it follows a specific sequence. Here is a simplified example showing how HP Web Jetadmin attempts to resolve a credential:

- HP Web Jetadmin checks the Credential Store for a credential.
- If a credential exists, HP Web Jetadmin attempts the configuration using the credential value.

  If a credential does not exist, HP Web Jetadmin checks Global Credentials.
- If the configuration is successful, the credential check is resolved and complete.

  If it fails, HP Web Jetadmin checks Global Credentials.

During a user-attended configuration session, HP Web Jetadmin prompts for credentials. If the user does not supply the credential or the session is not live, the device is flagged as **Credentials Required** and listed in the **Credentials Required** column that can be enabled in any device list (Columns for Device Lists on page 106). You can right-click the device and add the needed credential to the system in order to resolve this state.

HP Jetdirect Device Password

HP Web Jetadmin enables device security by providing management over appropriate, device-based security settings. The HP Jetdirect password that was used by HP Web Jetadmin in the past is a software security solution and not a device-based security solution. That is, the password itself had to be recognized and authenticated by earlier revisions of HP Web Jetadmin software. Other applications did not recognize this password and did not force users to prove knowledge of the password.

As security features have become more sophisticated and device based security has improved, HP Web Jetadmin developers have opted out of using the HP Jetdirect device password as a protective mechanism for device authentication. Instead, HP recommends that you choose one of the following two recommendations providing device security:

- **SNMP Set Community Name**: Devices will not allow an SNMP Set from any application without the Set Community Name correctly embedded in the SNMP packet. If the Set name in the packet is “public” and the Set name on the device is “George”, the device will not accept or acknowledge the packet. Set Community Names traverse the network in clear text and, therefore, can be “sniffed” or viewed by eavesdroppers. In most environments, security provided a Set Community Name may provide adequate security.
- **SNMPv3**: Devices configured via SNMPv3 offer significant security benefits. First, SNMPv3 configures a user account and two pass-phrases onto the device that the user (or application) must authenticate. This blocks unauthorized management of devices, and the account/pass-phrase details do not traverse the network in clear text which makes it difficult for eavesdroppers to learn the “secrets”. Second, the communication between the management application and the device is encrypted using the SNMP credentials so information about the device is protected. SNMPv3 is recommended in security-sensitive environments.

Restricting Configuration by Device Group

Within the model of device credential delegation, restriction to specific device configuration can be further defined in **User Security** using the Restriction type **Groups** (Restrict Roles to Device Groups on page 281).

Consider the following layers of security:

- Access to device credential values: Credential Store/selected device administrators (Credentials Store on page 52).
- Access to HP Web Jetadmin: **Users** and **Roles** (User Security on page 278).
- Access to device credentials store: Roles/Feature Permissions (Roles on page 280).
- Access to specific devices: Roles/Device Group Membership/Device Feature Permissions (Roles on page 280).

Each layer uses HP Web Jetadmin security to protect against unauthorized access:

1. First, device passwords are protected by one administrator or a few select administrators.
2. Second, **Users** and **Roles** allow only authorized users to log onto HP Web Jetadmin.
3. Third, **Roles** and **Feature Permissions** allow only authorized users access to configuration access to all devices.
4. Finally, **Roles**, **Device Group Membership**, and **Device Feature Permissions** allow authorized users to specific devices based on device group membership and specified device configuration features.

All devices and configuration options outside of the **Group Restriction Type** are secured from unauthorized access.

Clear the Credentials

Global credentials are credentials that HP Web Jetadmin uses for any device; they are an easy way for you to enter common credentials up front. Global credentials can be set for SNMPv1 Get Community Name, SNMPv1 Set Community Name, SNMPv3 Credentials, and EWS Password. If these credentials have been set, and device operations (for example, device configuration) require credentials, then the global credential will be tried. If the operation succeeds for the devices with the global credential, that global credential will be stored with the device. It still remains a global credential for other devices, but now that specific device has a working credential stored with it.

For example: User “A” enters global credentials for SNMPv1 Get Community Name as “mine” and “yours”. User “B” tries to interact with device “X”, which has a community name already set. HP Web Jetadmin first tries global credentials “yours” and “mine”; “yours” works. “Yours” is the stored as a regular credential for device “X”. The next time any user tries to interact with device “X”, HP Web Jetadmin will use the regular credential for that device (which is now “yours”) and will ignore any global credentials. However, if the regular credential “yours” becomes out of date, this process starts over again.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools** > **Options** > **Shared** > **Credentials** > **General**.
2. Configure the desired settings:
   - **Clear global credentials**: Clears every temporary, global, device-specific credential.
   - **Clear all stored credentials**: Clears every temporary, global, device-specific credential.
3. You must then confirm or cancel your request.

Manage the Global SNMPv1 Get Community Names

The SNMP Get Community Name object is configurable from within security settings. It can actually cause a device to disappear. For example:

User A is running an instance of HP Web Jetadmin known as Web Jetadmin A. This user is managing a set of devices that are also being managed by User B. User B is running another copy of HP Web Jetadmin known as Web Jetadmin B. This B copy of HP Web Jetadmin is being used at the help desk.

User B tries to provide a measure of security by changing the default Get Community Name on the set of devices from `public` to `private` using HP Web Jetadmin. User A opens HP Web Jetadmin and notices that all the devices have become non-responsive and show only a `device communication error`. **Quick Device Discovery** does not help. Upon checking the printer itself, User A finds it to be powered on. User A can also reach the printer web server interface through a browser.

⚠ CAUTION: Changing the Get Community Name can cause devices to become unresponsive to management applications such as HP Web Jetadmin. The SNMP protocol will no longer respond to `public` queries and other management applications on the network will not be able to communicate with these devices.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools** > **Options** > **Shared** > **Credentials** > **Device** > **SNMPv1 Get Community Name**.
2. To add a community name, click **Add** and type the community name. Enter an associated (or easier) name in **Remember credential as** and click **OK**.
3. To remove a Get Community Name, click **Remove**.

Manage the Global SNMPv1 Set Community Names

The SNMP Set Community Name is a grouping mechanism for SNMPv1/v2 that has been adopted as a security mechanism by many customers. Device configuration is not possible without knowledge of the Set name value. The Set name value traverses the network in clear text and can be easily detected by eavesdroppers.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools** > **Options** > **Shared** > **Credentials** > **Device** > **SNMPv1 Set Community Name**.
2. To add a community name, click **Add** and type the community name. Enter an associated (or easier) name in **Remember credential as** and click **OK**.
3. To remove a Set Community Name, click **Remove**.

Manage the Global SNMPv3 Credentials

SNMPv3 secures and authenticates communication between management applications, such as HP Web Jetadmin, and devices. SNMPv3 is used when strong security is a requirement.

SNMPv3 credentials consist of a user name, authentication protocol, authentication passphrase, private protocol, and privacy passphrase. HP Web Jetadmin uses these credentials when SNMPv3 is enabled.

IMPORTANT: SNMPv3 does not support the No Authentication Protocol and No Privacy Protocol modes.

HP Web Jetadmin can discover devices that have SNMPv3 fully enabled. However, you must configure HP Web Jetadmin to discover SNMPv3-enabled devices. For more information, see Configure the General Settings for Device Discoveries on page 64.

To discover SNMPv3-enabled devices, HP Web Jetadmin requires the SNMPv3 credentials for the devices. HP Web Jetadmin detects SNMPv3 credentials for devices in the following ways:

- SNMPv3 is enabled in HP Web Jetadmin and SNMPv3 credentials are configured on the devices. In this case, HP Web Jetadmin stores the credentials in its credentials store, and then uses these credentials when communicating with the devices.
- SNMPv3 credentials are added to the HP Web Jetadmin global credentials store and these global credentials match the credentials on the devices. In this case, when HP Web Jetadmin communicates with an SNMPv3-enabled device, it tries the values in the global credentials store. If the global credential values are valid and HP Web Jetadmin can communicate with the device, the credential values are stored on each device.

Devices that HP Web Jetadmin discovers through SNMPv1 and have SNMPv3 enabled through some other method, such as the HP Embedded Web Server or another instance of HP Web Jetadmin, have a Device Communication Error status when HP Web Jetadmin attempts to re-establish communication. To reset these devices to SNMPv3-enabled, use the **Refresh Selection** command in the device list.

Add SNMPv3 credentials

1. Go to **Tools** > **Options** > **Shared** > **Credentials** > **Device** > **SNMPv3**.
2. Click the **Add** button.
3. In the **User name** box, enter the user name.
4. From the **Authentication Protocol** list, select the protocol.

   For third-party devices, the authentication protocol must be MD5 or SHA-1. HP Web Jetadmin cannot discover third-party devices that do not use these protocols.
5. In the **Authenticated passphrase** and **Confirm authenticated passphrase** boxes, enter the authenticated passphrase (minimum of 8 characters).

   For third-party devices, the authentication passphrase must be in the format of a passphrase with a minimum length of 8 characters. HP Web Jetadmin cannot discover third-party devices that have an authentication passphrase that is in the format of a key or that is less than 8 characters.
6. From the **Privacy Protocol** list, select the protocol.

   For third-party devices, the privacy protocol must be DES or AES-128. HP Web Jetadmin cannot discover third-party devices that do not use these protocols.
7. In the **Private passphrase** and **Confirm private passphrase** boxes, enter the private passphrase (minimum of 8 characters).
8. For HP devices, select the **HP Device** checkbox. HP Web Jetadmin uses *Jetdirect* for the context name.

   -or-

   For third-party devices, clear the **HP Device** checkbox, and then enter a context name in the box next to the **HP Device** checkbox. The context name can be left blank.
9. In the **Remember credential as** box, enter a name for this credential that is easy to remember.
10. Click the **OK** button.

Delete SNMPv3 credentials

1. Go to **Tools** > **Options** > **Shared** > **Credentials** > **Device** > **SNMPv3**.
2. Select the credential from the list, and then click the **Remove** button.
3. On the **Confirm Delete** window, click the **Yes** button.

Manage the Global EWS Passwords

The EWS password blocks unauthorized access to the device-embedded HTTP interface. Also, it is synchronized with the HP Jetdirect telnet password.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools > Options > Shared > Credentials > Device > EWS**.
2. To add an EWS password, click **Add** and type the username and password. Then enter an associated (or easier) name in **Remember credential as** and click **OK**.

   NOTE: Enter either the EWS credentials or the Domain credentials. Enter Domain credentials as: `FullyQualifiedDomainName\Username`

3. To remove an EWS password, click **Remove**.

Manage the Global File System Passwords

The File system password protects the printer disk and other storage facilities from unauthorized access.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools > Options > Shared > Credentials > Device > File System**.
2. To add a file system password, click **Add** and type the password. Then enter an associated (or easier) name in **Remember password as** and click **OK**.
3. To remove a file system password, click **Remove**.

Manage the Domain Credentials

This option allows you to enter domain credentials when needed.

Use the following steps to configure this option:

1. On the top menu bar, access **Tools > Options > Shared > Credentials > Domain Browsing**.
2. Configure the desired settings:
   - **Add Domain**: Add a domain. The **Add Domain** dialog is displayed. Type the domain or browse for it. If you browse, you might be prompted for credentials.
   - **Set Credential**: Enter the username and password. In the **Stored** column, set credentials for any domain with **Yes**.
   - **Remove**: Delete a domain; select a domain listed and click **Remove**.
   - **Test**: Test the domain. Credentials might be required.

Application Management Configuration Options

The following sections describe the configuration options for functional areas in the **Application Management** view. To access these configuration options, go to **Tools** > **Options** > **Application Management**.

Configure the Settings for the Application Log

Use this option to specify how long the application log entries are saved, the maximum number of log entries that are saved, and whether older log entries are archived. For more information about viewing the application log, see Application Log on page 33.

Configure the log settings

1. Go to **Tools** > **Options** > **Application Management** > **Application Log**.
2. From the **Save log entries for** list, select the number of days that the log entries are saved. The default is 60.
3. In the **Maximum number of entries** box, specify the maximum number of entries that are saved in the log. Any log entries that exceed this number are stored in the archive file. The default is 20,000.
4. Click the **Apply** button.

Clear the log entries

1. Click the **Clear Log** button.
2. On the **Clear Application Log** window, click the **OK** button.

Archive the log entries

Log file entries that are older than the limit specified for the **Save log entries for** setting can be archived to a file. The archive log file is written to the HP Web Jetadmin server in the location displayed in the **Log archive** section. The operating system on the server determines this location.

TIP: The NetworkService folder is typically a hidden system folder in Microsoft operating systems. For instructions on how to make this folder visible, see the Microsoft Windows documentation for the operating system on the HP Web Jetadmin server.

1. Select the **Archive expired entries to file** check box.
2. Click the **Apply** button.

Clear the archived log entries

⚠ CAUTION: The log archive file will continue to grow indefinitely. You must manage the size of this file.

▲ Click the **Clear Archive** button.

Restore the Default Roles

You can use this option to restore the default user roles. For more information, see Roles on page 280.

To restore the default roles, perform the following steps:

1. Go to **Tools** > **Options** > **Application Management** > **User Security**.
2. Click the **Restore** button.

Device Management Configuration Options

The following sections describe the configuration options for functional areas in the **Device Management** view. To access these configuration options, go to **Tools** > **Options** > **Device Management**.

Device Polling Configuration Options

There are several configuration options that can be set to affect how device polling is performed in HP Web Jetadmin.

Configure the Background Polling Options

Whenever you access a device list in HP Web Jetadmin, the devices on the network are polled. You can determine how many devices and how often devices are polled by setting the rate on the **Background** polling page. You can reduce network traffic by setting a polling rate appropriate for your own environment.

HP Web Jetadmin performs a slow-poll when users access device lists. Slow polling means that HP Web Jetadmin queries only a certain number of devices every X seconds and only for specified columns. The columns polled are based on the union of all columns in the layouts currently displayed on Device List pages on all currently connected clients. This polling rate can be changed through **Tools > Options > Device Management > Device Polling > Device List**. List performance can be improved by changing the polling rate; network traffic will increase.

TIP: Another way to refresh the list more quickly is to highlight any or all devices where fast data is desired. Selected devices in the currently visible portion of the device list are always polled at a faster rate than non-selected devices.

Polling always occurs across all devices at the specified rate regardless of whether or not anyone is accessing a device list. Accessing a device list only affects the columns which are polled for when the polling does occur. Selecting devices within the visible portion of the list causes those devices to be polled for at a higher rate.

Polling is also affected by thresholds that specify how long the value for a specific column is considered valid. These thresholds are predefined in HP Web Jetadmin. You cannot change the predefined thresholds. Before HP Web Jetadmin polls a device for column values, it performs the following steps:

1. If HP Web Jetadmin does not have a value for a column, it polls the device. If HP Web Jetadmin can obtain a value from the device, it displays the value in the device lists.
2. If HP Web Jetadmin cannot obtain a value from the device, it checks the age of the value it has. If the age of the value is within the predefined threshold for the column, HP Web Jetadmin considers the value valid.
3. If the age of the value exceeds the predefined threshold for the column, HP Web Jetadmin polls the device to obtain the current value. If HP Web Jetadmin can obtain a value from the device, it displays the value in the device lists. If HP Web Jetadmin cannot obtain a value from the device, it displays **<Unknown>** in the device lists.

The predefined thresholds are based on the stability of the value for each column. For example, the **Severity** column is considered out-of-date after 15 seconds because the status of devices changes frequently. The

System Contact column is considered out-of-date after 24 hours because the contact does not change frequently. The **Model** column is never considered out-of-date because the device model never changes.

If you use HP Web Jetadmin to update the **System Contact** value for a device, the 24-hour polling threshold is not valid. HP Web Jetadmin immediately updates the **System Contact** column in the device lists. If you use another mechanism, such as HP Embedded Web Server, to change the **System Contact** value, HP Web Jetadmin does not display the updated value in the device lists for 24 hours. However, you can refresh the information in the device lists at any time to reflect the current values for the devices. For instructions, see **Refresh device selection** in Top Menu Bar on page 32.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Device Polling** > **Background**
2. Configure the desired settings:
   - **Polling interval**: Specify the number of seconds during which HP Web Jetadmin sends device requests to the network. The default is 2.
   - **Time between polling intervals**: Specify the number of seconds that HP Web Jetadmin remains idle between polling intervals. The default is 10.
   - **Number of devices per poll**: Specify the number of devices that HP Web Jetadmin can query concurrently. The default is 2.

     HP Web Jetadmin sends device requests for the specified number of devices to the network in a poll burst and waits for the responses. When HP Web Jetadmin receives the response packets, it sends another burst of device requests. HP Web Jetadmin continues to send device requests until the specified polling interval expires, and then waits until the specified number of devices per poll is satisfied before sending new device requests.
3. Click the **Apply** button.

To reset all of the values to the defaults, click the **Reset to Default Values** button.

Configure the Polling Options for Device Lists

Device List polling polls devices that are in view across all clients. The information polled from the device varies based on what columns the clients are viewing in the Device List.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Device Polling** > **Device List**.
2. Configure the desired settings:
   - **Polling interval**: Specify the number of seconds during which HP Web Jetadmin sends device requests to the network. The default is 5.
   - **Time between polling intervals**: Specify the number of seconds that HP Web Jetadmin remains idle between polling intervals. The default is 7.
   - **Number of devices per poll**: Specify the number of devices that HP Web Jetadmin can query concurrently. The default is 2.

     HP Web Jetadmin sends device requests for the specified number of devices to the network in a poll burst and waits for the responses. When HP Web Jetadmin receives the response packets, it sends another burst of device requests. HP Web Jetadmin continues to send device requests until the specified polling interval expires, and then waits until the specified number of devices per poll is satisfied before sending new device requests.

3. Click the **Apply** button.

To reset all of the values to the defaults, click the **Reset to Default Values** button.

Configure the Polling Options for Device Tabs

Device Tab polling polls device information needed to drive the device-related information on the selected device tabs across all clients.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Device Polling** > **Device Tabs**.
2. Configure the desired settings:
   - **Polling interval**: Specify the number of seconds during which HP Web Jetadmin sends device requests to the network. The default is 5.
   - **Time between polling intervals**: Specify the number of seconds that HP Web Jetadmin remains idle between polling intervals. The default is 2.
   - **Number of devices per poll**: Specify the number of devices that HP Web Jetadmin can query concurrently. The default is 3.

     HP Web Jetadmin sends device requests for the specified number of devices to the network in a poll burst and waits for the responses. When HP Web Jetadmin receives the response packets, it sends another burst of device requests. HP Web Jetadmin continues to send device requests until the specified polling interval expires, and then waits until the specified number of devices per poll is satisfied before sending new device requests.
3. Click the **Apply** button.

To reset all of the values to the defaults, click the **Reset to Default Values** button.

Configure the Polling Options for Device Alerts and Supplies Alerts

You can define how often devices should be checked to see if they warrant alerts. Frequent polling can increase network traffic; infrequent polling might cause some device alerts to go unnoticed and, therefore, unattended. You can also specify how long an alert event stays in the alert history log, or you can clear the alerts log at any time.

You can configure static polling rates for supplies alerts subscriptions. This feature helps prevent missing alerts by keeping supplies alerts subscriptions in a static polling interval. If you enable this feature, supplies alerts subscriptions that exceed the specified threshold are placed in static polling. These supplies alerts subscriptions remain in static polling until you disable static polling or replenish the supplies. Supplies alerts subscriptions move to the static poller on the next polling cycle of the poller the subscription is in. If you disable this feature, qualifying supplies alerts subscriptions move from the static poller to the most appropriate poller, which is determined by the rate of use for the supply, on the next polling cycle of the poller the subscription is in.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Device Polling** > **Alerts**.
2. To configure polling for devices, specify the following settings:

- **Maximum communication interval**: Specify the number of hours during which no device communication occurs. The default is 24.
- **Critical alert interval**: Specify how often devices are polled for critical alerts. The default is 5 minutes.

3. To configure static polling for supplies alerts, specify the following settings:
   - **Enable static polling**: Select this checkbox to enable static polling for supplies alerts.
   - **Polling interval**: Specify the polling interval in hours.
   - **Apply at % above alert threshold**: Specify the percentage above the alert threshold the supply level must reach before the supplies alerts subscription is placed in static polling.
   - **Number of devices per poll**: Specify the number of devices HP Web Jetadmin polls in each polling burst.
4. Click the **Apply** button.

Configure the Polling Options for Supplies

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Device Polling** > **Supplies**.
2. Configure the desired settings:
   - **Polling interval**: Specify the number of seconds during which HP Web Jetadmin sends device requests to the network. The default is 5.
   - **Time between polling intervals**: Specify the number of seconds that HP Web Jetadmin remains idle between polling intervals. The default is 10.
   - **Number of devices per poll**: Specify the number of devices that HP Web Jetadmin can query concurrently. The default is 2.

     HP Web Jetadmin sends device requests for the specified number of devices to the network in a poll burst and waits for the responses. When HP Web Jetadmin receives the response packets, it sends another burst of device requests. HP Web Jetadmin continues to send device requests until the specified polling interval expires, and then waits until the specified number of devices per poll is satisfied before sending new device requests.
3. Click the **Apply** button.

To reset all of the values to the defaults, click the **Reset to Default Values** button.

Devices Configuration Options

Configuration options for Devices help determine which devices will be displayed or not displayed in **Device Lists**.

Manage Hidden Devices

If communication with a device has not occurred within a specified number of days, you can configure HP Web Jetadmin to automatically list the device on the **Hidden Devices** list so that it will not show up in other **Device** lists throughout the product. The number of days specified is counted starting at midnight after the policy has been set **and** the device has not been communicated with.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Devices** > **Hidden Devices**.
2. Configure the desired settings:
   - **Automatically hide devices in communication error after**: Specify how many days should pass with a device before that device should be hidden.
   - **Hidden devices**: To show a device in the device lists even though it has not been communicated with, highlight it in the **Hidden devices** list and click **Show**.
3. Click the **Apply** button.

Manage Blocked Devices

The **Blocked Devices** list contains device addresses for which device discoveries are blocked. You can add devices to this list in one of two ways:

- Devices can be deleted from the **All Device** list with the “Delete and Block” option; the devices are then added to the **Blocked Devices** list.
- Devices can be added to (or removed from) the **Blocked Devices** list in **Tools** > **Options** > **Device Management** > **Devices** > **Blocked Devices** (see steps below).

If a device is on the **Blocked Devices** list, HP Web Jetadmin cannot discover it. If you add a device to this list through **Tools** > **Options** > **Device Management** > **Devices** > **Blocked Devices**, the device will still be included on the **All Devices** list. Devices can be identified by IP Address or Hostname. Hostname is the preferred method, since IP Addresses on devices can change.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Devices** > **Blocked Devices**.
2. To add a device to the Blocked Devices list so that it will not be found during a discovery, click **Add**.
3. To remove a device from the Blocked Devices list so that it can be found during a discovery, click **Remove**.

Device Discovery Configuration Options

Global settings for discovery can be set here.

Configure the General Settings for Device Discoveries

General discovery settings include SLP listen, SNMPv3, and WS-Discovery listen.

IMPORTANT: HP Jetdirect firmware version x.06.00 or greater is required to support the Multicast and SLP discovery method.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Device Discovery** > **General**.
2. Configure the desired settings:

- **SLP listen**: Select this option to use passive discovery on port 427 for SLP signals propagated at HP Jetdirect power-on. The default for this field is off or unselected.
- **SNMPv3**: Select this option to enable SNMPv3 credential entry fields in HP Web Jetadmin discovery settings. When these credentials are added for discovery settings or global credentials, HP Web Jetadmin attempts SNMPv3 queries on devices. The default for this field is off or unselected.

  ⚠ CAUTION: SNMPv3 discoveries can be slow if not properly set. These should be targeted only at parts of the network that are known to have SNMPv3-enabled devices. Also, SNMPv3 devices **require** that SNMPv3 credentials are entered.

- **WS-Discovery listen**: Select this option to use passive discovery on port 3702 for WS-Discovery signals propagated at HP Jetdirect power-on. The default for this field is off or unselected.

3. Click the **Apply** button.

Device Filters Configuration Options

Configuration options for Device Filters help determine which devices will be displayed or not displayed in **Device Lists**.

Configure the Number of Days that Devices are Considered New

You can specify how long a device is considered new in HP Web Jetadmin. “New” devices are displayed on the **New (Time Period)** device list.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Device Filters** > **New Devices Filter**.
2. Configure the desired settings:
   - **Time period for device to remain “New”**: Specify the number of days that HP Web Jetadmin considers devices new. The default is 14.
3. Click the **Apply** button.

Device Tabs Configuration Options

Configuration options for Device Tabs help determine how many devices will be displayed at one time in multiple device view.

Configure the General Options for Device Tabs

For multiple device view, this configuration option determines the maximum number of devices per page for which status should be shown.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Device Tabs** > **General**.
2. In the **Devices to allow in multi-view** box, specify the maximum number of devices that are displayed in the tabs when multiple devices are selected in a device list. The default is 10.
3. Click the **Apply** button.

Configuration Options for Fleet Configurations

Global settings can be set here for fleet configurations.

Configure the Retry Settings for Device Configuration Schedules

Device configurations can be run on an immediate or scheduled basis. The settings on this page apply to scheduled configurations. When a device fails to respond to a scheduled configuration operation, it is added to a list of devices to which the configuration operation will be retried. The settings determine how often the configuration operation will be retried, and how many times it will be retried before the configuration operation gives up and marks the configuration as having failed overall. If the device responds successfully during a retry attempt, it is removed from the list. If all devices are removed from the list before the number of retries is exhausted, the configuration operation is deemed successful.

If the device cannot be configured, an entry noting the failed operation is logged in the **Application Log** and in the **Configuration History**.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Configuration** > **General**.
2. Configure the desired settings:
   - **Number of configuration retries**: Select the number of times that HP Web Jetadmin tries to configure a device before stopping. The default is 0.
   - **Hours between configuration retries**: Specify the number of hours that HP Web Jetadmin waits before trying to configure a device again. The default is 8.
3. Click the **Apply** button.

Restore the Default Configuration Templates

You can choose to restore default templates with this setting.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Configuration** > **Templates**.
2. Configure the desired settings:
   - **Restore default templates**: Restores all templates shipped with HP Web Jetadmin.

   The changes are applied automatically.

Manage the User-defined Device Configuration Settings

You can create custom device configuration settings that provide additional information about a device that is not available by using the device's existing configuration options. You can then apply the user-defined settings to devices. The following are examples of user-defined settings:

- Warranty expiration dates
- Lease start and stop dates
- Service maintenance dates
- Location of the device

User-defined settings are available on the **Config** tab, device configuration wizards, device list columns, and reports.

You can export user-defined settings from one HP Web Jetadmin installation to an XML file. Then you can import the XML file into a different HP Web Jetadmin installation.

Changes that are made to the user-defined settings might not take effect for all of the HP Web Jetadmin features until HP Web Jetadmin is restarted.

⚠ CAUTION: Actions that are performed on the **User Defined** window are effective immediately and cannot be canceled.

Create user-defined settings

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **User Defined**.
2. Click the **New** button.
3. On the **Create User Defined Setting** window, enter a name for the user-defined setting in the **Setting name** box.
4. To disable the user-defined setting when configuring multiple devices, select the **Hide when configuring multiple devices** checkbox.

   IMPORTANT: Select this checkbox if the value of the user-defined setting must be unique for each device, such as an identification number. This user-defined setting cannot be used to configure multiple devices or in device configuration templates.

   -or-

   To allow the user-defined setting to be used when configuring multiple devices, clear the **Hide when configuring multiple devices** checkbox.
5. Click the **OK** button.

Edit user-defined settings

Changing the name of a user-defined setting does not affect any current or historical data that was saved for that setting. The new name should still reflect the purpose of the setting.

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **User Defined**.
2. Select the user-defined setting from the list, and then click the **Edit** button.
3. On the **Edit User Defined Setting** window, enter a new name for the user-defined setting in the **Setting name** box.
4. To disable the user-defined setting when configuring multiple devices, select the **Hide when configuring multiple devices** checkbox.

IMPORTANT: Select this checkbox if the value of the user-defined setting must be unique for each device, such as an identification number. This user-defined setting cannot be used to configure multiple devices or in device configuration templates.

-or-

To allow the user-defined setting to be used when configuring multiple devices, clear the **Hide when configuring multiple devices** checkbox.

5. Click the **OK** button.
6. On the message window, click the **OK** button.

Delete user-defined settings

After a user-defined setting is deleted, all of the current and historical data that was saved for the setting is lost and the user-defined setting is removed from any templates and scheduled tasks.

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **User Defined**.
2. Select the user-defined settings from the list, and then click the **Delete** button.
3. On the **Delete User Defined Setting** window, verify that the correct user-defined settings are listed, and then click the **OK** button.
4. On the message window, click the **OK** button.

Import user-defined settings

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **User Defined**.
2. Click the **Import** button. The **Import User-Defined Settings** wizard starts.
3. On the **Select file** page, click the **Browse** button.
4. On the **Open** window, navigate to and select the file, and then click the **Open** button.
5. To replace duplicate user-defined settings with the user-defined settings in the XML file, select the **Overwrite duplicate user-defined settings** checkbox.

IMPORTANT: If a user-defined setting that already exists in HP Web Jetadmin is overwritten by a user-defined setting in the XML file that has the same name, note the following issues:

- Templates and user-defined data for the devices lose the values for the overwritten user-defined settings.
- To display the overwritten user-defined settings correctly, the HP Web Jetadmin service must be restarted.
- The columns for the overwritten user-defined settings in HP Web Jetadmin must be reselected.

-or-

To prevent duplicate user-defined settings from being imported into HP Web Jetadmin, clear the **Overwrite duplicate user-defined settings** checkbox.

6. Click the **Next** button.
7. On the **Confirm** page, verify that the correct XML file is selected, and then click the **Import** button.
8. On the **Results** page, click the **Done** button.

Export user-defined settings

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **User Defined**.
2. Select the user-defined settings from the list.

   -or-

   Select the **Select all** checkbox.
3. Click the **Export** button. The **Export User-Defined Settings** wizard starts.
4. On the **Confirm** page, verify that the correct user-defined settings are listed, and then click the **Export** button.
5. On the **Save As** window, navigate to and select the directory where you want to save the XML file.
6. In the **File name** box, enter a name for the XML file, and then click the **Save** button.
7. On the **Results** page, click the **Done** button.

Manage the PJL Repository

You can send a file or test file with PJL configuration options to one or more printers. You can choose to have the file sent immediately or you can schedule it.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Configuration** > **PJL Repository**. The **PJL File Repository** page is displayed showing current file names and descriptions.
2. To add a file to the repository, click **Add File**. The **Add File** dialog is displayed.
   a. Type a unique file name or browse to the file.
   b. Type a description and then click **OK**.
3. To delete a file:
   a. Select the files from the list, and then click the **Remove** button.
   b. On the **Remove Files** window, click the **OK** button.

Manage the Certificate Repository

Printers might need certificates to access some external web sites. You can store certificates in the certificate repository, and then install those certificates on one or more printers. You can view detailed information for a certificate, delete certificates, and include certificates in device configuration templates.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Configuration** > **Certificate Repository**. The **Certificate Repository** page is displayed showing the certificates stored in the repository.
2. To import a certificate, click **Import**. The **Open** dialog is displayed. Browse to the certificate file, and then click **Open**.
3. To delete a certificate, select the certificate, and then click **Delete**. A confirmation message is displayed. Click **OK**.
4. To view a certificate, select the certificate, and then click **View Details**.

Manage the OXPd Device Function Repository

A device function file defines the name and functionality of a button that can be displayed on a printer control panel. You can import device function files into the device function repository, and then use the device function files to configure one or more printers. You can edit device function files, delete device function files, and include device function files in device configuration templates.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Device Functions**. The **OXPd Device Function Repository** page is displayed showing the device function files stored in the repository.
2. To import a device function file, click **Import**. The **Open** dialog is displayed. Browse to the device function file, and then click **Open**.
3. To delete a device function file, select the file, and then click **Delete**. A confirmation message is displayed. Click **OK**.
4. To edit a device function file, select the file, and then click **Edit**. Change the settings, and then click **OK**.

Manage the OXPd Accessory Record Repository

An accessory record file defines how third-party applications access device accessories. You can import accessory record files into the accessory record repository, and then use the accessory record files to configure one or more printers. You can edit accessory record files, delete accessory record files, and include accessory record files in device configuration templates.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Accessory Records**. The **OXPd Accessory Record Repository** page is displayed showing the accessory record files stored in the repository.
2. To import an accessory record file, click **Import**. The **Open** dialog is displayed. Browse to the accessory record file, and then click **Open**.
3. To delete an accessory record file, select the file, and then click **Delete**. A confirmation message is displayed. Click **OK**.
4. To edit an accessory record file, select the file, and then click **Edit**. Change the settings, and then click **OK**.

   For a shared accessory record file, you can only edit the name of the accessory.

Manage the OXPd Authentication Agent Repository

When a user signs in on an OXPd-enabled device to access secure features, the device initiates an authentication process by invoking a proxy from a third-party solution. The proxy, which is called an OXPd authentication agent, contacts the authentication server and authenticates the user before the user is allowed to gain access to the secure features. OXPd authentication agent files contain the information that devices require to contact authentication servers and authenticate users.

Import OXPd authentication agent files

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Authentication Agents**.
2. Click the **Import** button.
3. On the **Open** window, navigate to and select the OXPd authentication agent files, and then click the **Open** button.

Edit OXPd authentication agent files

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Authentication Agents**.
2. Select the OXPd authentication agent file from the list, and then click the **Edit** button.
3. In the **Name** box, enter the unlocalized name for the OXPd authentication agent (maximum of 100 characters).
4. In the **Web application** section, perform the following steps:
   a. In the **URI** box, enter the URI of the OXPd authentication server (maximum of 256 characters). The URI is case-sensitive and must begin with one of the following protocols:
      - http://
      - https://
      - file://
      - ftp://

   b. If network credentials are required to access the OXPd authentication server, select the **Use credentials** checkbox. Enter the network credentials in the **User name** (maximum of 128 characters), **Password** (maximum of 128 characters), and **Confirm password** boxes.

   c. In the **Connection timeout** box, enter the maximum number of seconds that the device has to establish a connection to the OXPd authentication server before a timeout occurs.

   d. In the **Response timeout** box, enter the maximum number of seconds that the device has to receive a response from the OXPd authentication server before a timeout occurs.

   e. To enable the device to contact the OXPd authentication server before launching the Web browser, select the **Enable pre-prompt check** checkbox.
5. In the **Prompt info** section, perform the following steps:
   a. In the **Post-query format string** box, enter the string that the device uses to construct the body of the initial HTTP POST request (maximum of 1,024 characters). The device sends this request to the specified URI. The string can contain extended characters.

   b. In the **URI** box, enter the URI that the device contacts to validate and perform the functionality from the third-party solution (maximum of 256 characters). The URI is case-sensitive and must begin with one of the following protocols:
      - http://
      - https://
      - file://
      - ftp://

NOTE: OXPd does not allow URIs that contain embedded authentication credentials, such as ftp://username:password@domain/path, by explicitly prohibiting the use of the at (@) symbol in the domain name.

c. If credentials are required to access the URI, select the **Use pre-prompt credentials** checkbox. Enter the credentials in the **User name** (maximum of 128 characters), **Password** (maximum of 128 characters), and **Confirm password** boxes.

6. To notify the OXPd authentication server when users sign out, select the **Enable signout notification** checkbox.

7. In the **Signout notification max retries** box, enter the maximum number of times that the device can retry sending a notification to the OXPd authentication server when users sign out.

8. In the **Signout notification retry intervals** box, enter the minimum number of seconds that the device must wait before sending another notification to the OXPd authentication server when users sign out.

9. Click the **OK** button.

Delete OXPd authentication agent files

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Authentication Agents**.
2. Select the OXPd authentication agent file from the list, and then click the **Delete** button.
3. On the confirmation window, click the **OK** button.

Manage the OXPd Authorization Proxy Configuration Repository

The built-in authorization proxy on a device provides access to a Web-based service that authorizes users to access the device. OXPd authorization proxy files contain the information that devices require to access authorization agents from third-party solutions. You can use OXPd authorization proxy files to override the built-in authorization proxies on OXPd-enabled devices with OXPd authorization agents from third-party solutions.

Import OXPd authorization proxy files

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Authorization Proxy Configuration**.
2. Click the **Import** button.
3. On the **Open** window, navigate to and select the OXPd authorization proxy files, and then click the **Open** button.

Delete OXPd authorization proxy files

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Authorization Proxy Configuration**.
2. Select the OXPd authorization proxy configuration file from the list, and then click the **Delete** button.
3. On the confirmation window, click the **OK** button.

Edit OXPd authorization proxy files

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Authorization Proxy Configuration**.
2. Select the OXPd authorization proxy file from the list, and then click the **Edit** button.
3. In the **Name** box, enter the unlocalized name for the OXPd authorization proxy (maximum of 100 characters).

4. In the **URI** box, enter the URI of the OXPd authorization agent (maximum of 256 characters). The URI is case-sensitive and must begin with one of the following protocols:

   - http://
   - https://
   - file://
   - ftp://

   This text box can use static data or custom variables supported in the following formats:

   - Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

     %%<custom variable>%% (where "<custom variable>" is the name of the user defined field)

     Example: `%%var_URI%%`

   - Variable data along with a combination of static content before or after the variable

     <static value>%%<custom variable>%%<static value>

     Example: `http://%%var_URI%%`

     Example: `http://%%var_URI%%/myapp`

TIP: By starting the variable data name with var_, it's easier to find and identify user defined fields in HP Web Jetadmin.

TIP: For more information on variable data, see Create and Use Variable Data on page 183.

5. If network credentials are required to access the URI, select the **Use credentials** checkbox. Enter the network credentials in the **User name** (maximum of 128 characters), **Password** (maximum of 128 characters), and **Confirm password** boxes.

6. In the **Connection timeout** box, enter the maximum number of seconds that the device has to establish a connection to the authorization agent before a timeout occurs.

7. In the **Response timeout** box, enter the maximum number of seconds that the device has to receive a response from the authorization agent before a timeout occurs.

8. To allow users to choose an alternate sign-in method when more than one method is enabled on the device, select the **Enable sign in choice** checkbox. An Advanced button is available on the sign-in screen on the device control panel. When the user touches the Advanced button, a list of the alternate sign-in methods that the user can select opens.

NOTE: Some devices do not support alternate sign-in methods. These devices do not display the Advanced button if this checkbox is selected.

9. To notify the authorization agent each time the permissions or proxy configuration on the device changes, select the **Enable change notification** checkbox.

10. To enable the authorization proxy to automatically add new permissions to the guest permission set, select the **Add new permission to guest permission set** checkbox.

IMPORTANT: If this checkbox is cleared, guest users for new permissions are denied access to the device.

11. To view the fax and email settings that the device uses for guest users, click the **View guest user overrides** button.

12. Click the **OK** button.

Manage the OXPd Statistics Agents Repository

Devices collect statistics about each job that they process. The job statistics include the device ID, job ID, user who initiated the job, and details about the job.

A statistics agent is a server-based solution that receives job statistics from devices. When a job is completed, the device sends the job statistics to the statistics agent. The statistics agent sends an acknowledgement to the device when the job statistics are received.

An OXPd statistics agent record defines the information that devices require to send job statistics to the server where the statistics agent is installed. An OXPd statistics agent record also defines when the device sends job statistics to the OXPd statistics agent server and whether the device automatically deletes the oldest job statistics when the storage media on the device is full. The OXPd statistics agent record must be registered on every device that sends job statistics to the specified OXPd statistics agent server.

During normal operation, if the storage media on the device is full when a new job starts, the device automatically deletes the oldest job statistics from the storage media to make room for the new job statistics. The device deletes the oldest job statistics even if all of the registered OXPd statistics agents have not received the job statistics and sent an acknowledgement to the device. However, you can configure a device to prevent the job statistics from being deleted from the storage media if the device has not received an acknowledgement from the OXPd statistics agent server. In this case, if the storage media is full when a job starts, the device is locked and does not start any new print or scan jobs. Use one of the following methods to unlock the device:

- Allow the device to continue resending an unacknowledged notification until the OXPd statistics agent server acknowledges that the job statistics have been received. After the device receives an acknowledgement for all of the outstanding notifications, the lock is cleared from the device.
- Remove the OXPd statistics agents that have not successfully received the notifications from the device. The device no longer sends notifications to these OXPd statistics agents.
- Use the Administration app or menu on the device control panel or the device HP Embedded Web Server (EWS) to remove all of the OXPd statistics agents from the device. The device no longer sends notifications to any OXPd statistics agents.

After an OXPd statistics agent record is imported into the OXPd Statistics Agents Repository, use the **OXPd Statistics Agents** configuration option to add that OXPd statistics agent record to a device. OXPd statistics agent records can be edited, deleted, and included in device configuration templates.

Import OXPd statistics agent records

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Statistics Agents**.
2. Click the **Import** button.
3. On the **Open** window, navigate to and select the OXPd statistics agent records, and then click the **Open** button.

Delete an OXPd statistics agent record

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Statistics Agents**.
2. Select the OXPd statistics agent record from the list, and then click the **Delete** button.
3. On the **File Delete** window, click the **OK** button.

Edit an OXPd statistics agent record

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Statistics Agents**.
2. Select the OXPd statistics agent record from the list, and then click the **Edit** button.
3. In the **Name** box, enter the unlocalized name for the OXPd statistics agent (maximum of 100 characters).
4. To prevent the device from automatically deleting the oldest job statistics to make room for the new job statistics when the storage media on the device is full, select the **Critical agent (acknowledgement required for delete)** check box. The device deletes the job statistics only when it receives an acknowledgement from the OXPd statistics agent server. If the device runs out of storage space for unacknowledged job statistics, the device is locked and does not print or scan any new jobs.

   -or-

   To allow the device to automatically delete the oldest job statistics to make room for the new job statistics when the storage media on the device is full, clear the **Critical agent (acknowledgement required for delete)** check box.
5. From the **Data persistence frequency** list, select one of the following options:
   - **Job**—The device commits the job statistics to its storage media only when each job is completed. If a power failure occurs while the device is processing a job, all of the statistics for that job are lost.
   - **Job and sheet**—The device commits the job statistics to its storage media when each job is completed and when each scanned or printed page is delivered to its destination. If a power failure occurs while the device is processing a job, the recovered job statistics contain accurate values up to the time of the power failure. Only the job statistics that the device was actively processing at the time of the power failure are lost.
6. In the **URI** box, enter the URI of the OXPd statistics agent server (maximum of 256 characters). The URI is case-sensitive and must begin with one of the following protocols:
   - http://
   - https://
   - file://
   - ftp://

   This text box can use static data or custom variables supported in the following formats:
   - Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

     %%<custom variable>%% (where “<custom variable>” is the name of the user defined field)

     Example: `%%var_URI%%`
   - Variable data along with a combination of static content before or after the variable

     <static value>%%<custom variable>%%<static value>

     Example: `https://%%var_URI%%`

     Example: `https://pull.%%var_URI%%.MyCompany.com:8443/MyCompanyAuthentication/services/AuthenticationService`

TIP: By starting the variable data name with var_, it’s easier to find and identify user defined fields in HP Web Jetadmin.

TIP: For more information on variable data, see Create and Use Variable Data on page 183.

7. If network credentials are required to access the OXPd statistics agent server, select the **Use credentials** check box. Enter the network credentials in the **User name** (maximum of 128 characters), **Password** (maximum of 128 characters), and **Confirm password** boxes.
8. In the **Connection timeout** box, enter the maximum number of seconds that the device has to establish a connection to the OXPd statistics agent server before a timeout occurs.
9. In the **Response timeout** box, enter the maximum number of seconds that the device has to receive a response from the OXPd statistics agent server before a timeout occurs.
10. In the **Retry interval** box, specify the number of seconds that the device waits before trying to connect to the OXPd statistics agent server again.
11. In the **Max consecutive retries** box, enter the maximum number of times that the device tries to connect to the OXPd statistics agent server.
12. Click the **OK** button.

Manage the OXPd Quota Record Repository

A quota solution, such as Pcounter for HP, is installed on a server and used to specify the amount of various device resources that each user is allowed to use. These device resources include the number of sheets of paper printed, the amount of toner used, and so on. The following are examples of how quotas can be defined:

- Quotas can be based on time. The quota balance can be automatically reset on a recurring basis, such as each week or once a month.
- Quotas can be based on a credit or debit amount. Users can pay into their quota account by using a payment product, such as a web-based pay-for-print application or a debit/credit card machine attached to the device.

An OXPd quota agent record contains the information that devices require to access the server where the quota solution is installed. An OXPd quota agent record can also define web resources that are displayed when users initiate a job on the device, such as a request for credentials, and when a quota limit is reached, such as a warning message.

After an OXPd quota agent record is imported into the OXPd Quota Record Repository, use the **OXPd Quota Agents** configuration option to add that OXPd quota agent record to a device. OXPd quota agent records can be edited, deleted, and included in device configuration templates.

Import OXPd quota agent records

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Quota Agents**.
2. Click the **Import** button.
3. On the **Open** window, navigate to and select the OXPd quota agent records, and then click the **Open** button.

Delete an OXPd quota agent record

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Quota Agents**.
2. Select the OXPd quota agent record from the list, and then click the **Delete** button.
3. On the **File Delete** window, click the **OK** button.

Edit an OXPd quota agent record

1. Go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Quota Agents**.
2. Select the OXPd quota agent record from the list, and then click the **Edit** button. The **Quota Agent Details** window opens.
3. In the **Name** box, enter an unlocalized name for the OXPd quota agent record (maximum of 100 characters).
4. In the **Quota agent** section, use the following steps to specify the settings that the device requires to access the OXPd quota server:
   a. In the **URI** box, enter the URI of the OXPd quota server (maximum of 256 characters). The URI is case-sensitive and must begin with one of the following protocols:
      - http://
      - https://
      - file://
      - ftp://

      This text box can use static data or custom variables supported in the following formats:
      - Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

        %%<custom variable>%% (where "<custom variable>" is the name of the user defined field)

        Example: `%%var_URI%%`
      - Variable data along with a combination of static content before or after the variable

        <static value>%%<custom variable>%%<static value>

        Example: `https://%%var_URI%%`

        Example: `https://%%var_URI%%/myApp`

   TIP: By starting the variable data name with var_, it's easier to find and identify user defined fields in HP Web Jetadmin.

   TIP: For more information on variable data, see Create and Use Variable Data on page 183.

   b. If network credentials are required to access the OXPd quota server, select the **Use credentials** check box. Enter the network credentials in the **User name** (maximum of 128 characters), **Password** (maximum of 128 characters), and **Confirm password** boxes.
   c. In the **Connection timeout** box, enter the maximum number of seconds that the device has to establish a connection to the OXPd quota server before a timeout occurs.
   d. In the **Response timeout** box, enter the maximum number of seconds that the device has to receive a response from the OXPd quota server before a timeout occurs.
   e. In the **Retry interval** box, specify the number of seconds that the device waits before trying to connect to the OXPd quota server again.
   f. In the **Max consecutive retries** box, enter the maximum number of times that the device tries to connect to the OXPd quota server.
5. In the **Quota StartJob User Prompt Target** section, use the following steps to specify the settings for the web resource that is displayed in a web browser when a user initiates a job on the device:

a. In the **URI** box, enter the URI of the web resource (maximum of 256 characters). The URI is case-sensitive and must begin with one of the following protocols:

   - http://
   - https://
   - file://
   - ftp://

b. If network credentials are required to access the URI of the web resource, select the **Use credentials** check box. Enter the network credentials in the **User name** (maximum of 128 characters), **Password** (maximum of 128 characters), and **Confirm password** boxes.

6. In the **Quota Limit Reached User Prompt Target** section, use the following steps to specify the settings for the web resource that is displayed in a web browser when a quota limit is reached:

   a. In the **URI** box, enter the URI of the web resource (maximum of 256 characters). The URI is case-sensitive and must begin with one of the following protocols:

      - http://
      - https://
      - file://
      - ftp://

   b. If network credentials are required to access the URI of the web resource, select the **Use credentials** check box. Enter the network credentials in the **User name** (maximum of 128 characters), **Password** (maximum of 128 characters), and **Confirm password** boxes.

7. Click the **OK** button.

Alerts Configuration Options

Global settings for alerts can be set here.

Attach the Supplies Report to the Email Notifications for Supply Alerts

The **General** option for **Alerts** provides the capability to include or exclude the supplies report as an email attachment when the email notification is selected for alert subscriptions. Other notification options in HP Web Jetadmin include **Email Templates**, **Subscription Templates**, **Log to File**, and **SNMP Trap Generator**. For more information about **Alerts**, see Alerts on page 188.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Alerts** > **General**.
2. To restrict who receives detailed supply report attachments to emails, check **Attach supplies report to supply alert email notifications**.
3. Click the **Apply** button.

Manage the Custom Email Templates

You can create custom email templates or reset the default alert subscription template back to its original state. This is convenient if changes have been made to the template that you no longer want.

NOTE: Email clients may or may not make the web browser the active window when a device URL is selected in an alerts email.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Alerts** > **Email Templates**.
2. Select one of the actions:
   - **Create**: Click **Create** and complete the page displayed.
     - Complete **Subject** and **Body**.
     - Add a macro to **Subject** by selecting the macro and clicking **Insert Field** or drag-and-drop the macro into the content area.

       Macros are added at the current cursor position within **Subject**.
     - Add a macro to **Body** by selecting the macro and clicking **Insert Field** or drag-and-drop the macro into the content area.

       Macros are added at the current cursor position within **Body**.
     - To save the template, click **OK**.
   - **Edit**: Select the template and click **Edit**. You can then make changes to it. (You cannot edit the default email templates: **Concise** and **Verbose**.)
   - **Delete**: Select the template and click **Delete**. (You cannot delete the default email templates: **Concise** and **Verbose**.)
   - **Copy**: Select the template and click **Copy**. You can then name the new template and make changes to it.

Manage the Templates for Alert Subscriptions

You can reset the default alert subscription template back to its original state. This is convenient if changes have been made to the template that you no longer want applied.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Alerts** > **Subscription Templates**.
2. To reset the alert subscription template to factory settings (its state when first installed), click **Restore**.

Configure the Settings for the Alerts Log

This option enables an entry to be created in a log file each time HP Web Jetadmin processes an alert. You can control the format of the log file entry, the maximum size of the log file, and turn the logging on and off. This file has a pre-defined path and filename on the server, and that path is shown in **Log file path**.

The maximum logfile size is enforced by removing the oldest entries whenever new ones are added. New entries are added to the beginning of the logfile and the oldest entries are removed from the end of the logfile.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Alerts** > **Log to File**.
2. After you select **Enable**, specify the maximum file size for the log.

   To clear the log, select **Clear**.
3. Select the language for the log.
4. To make changes to the log file, click **Edit**. The **Edit Alert Log to File Template** page is displayed.
5. Type the field directly into the **Body**.

   Or, you can insert fields:

   - Select the source for available fields in **Source**.
   - Highlight the field in **Available Fields** (at the left of this page) and then click **Insert Field** (at the right of this page).
6. Click the **Apply** button.
7. To reset the format to factory settings (its state when first installed), click **Restore**.

Configure the Format for SNMP Traps

The SNMP Trap Generator provides an easy way to integrate HP Web Jetadmin with another management application. You can create alert subscriptions in HP Web Jetadmin for the device alerts that you want forwarded to the management application. The alert subscription specifies information about the server where the SNMP traps are sent and the format for the SNMP traps. When HP Web Jetadmin processes one of these device alerts, it forwards the SNMP trap to the specified server and port.

The SNMP Trap Generator supports only one format for the SNMP traps. If you change the format, all of the existing and future alert subscriptions that generate SNMP traps use the new format.

To handle an SNMP trap from the SNMP Trap Generator, load the MIB file (webjet.mib) or HP System Insight Manager CFG file (webjet.cfg) into the management application that receives the SNMP traps. After you direct the MIB or CFG file to read the trap variable, you can view the formatted SNMP trap. The MIB and CFG files are available in the following directory:

C:\Program Files\HP Inc\Web Jetadmin 10\views\dav\bin

To configure the format for SNMP traps, perform the following steps:

NOTE: HP Web Jetadmin uses the displayed format for all of the forwarded SNMP traps.

1. Go to **Tools** > **Options** > **Device Management** > **Alerts** > **SNMP Trap Generator**.
2. To change the format, perform the following steps:
   a. Click the **Edit** button.
   b. On the **Edit SNMP Trap Template** window, make the changes to the format.
   c. Click the **OK** button.
3. To reset the format to the default, click the **Restore** button.

Firmware Configuration Options

Global settings can be stored here for managing firmware images and how devices are updated.

Configure the Settings for Firmware Upgrades

Use this option to specify the number of concurrent firmware upgrades that HP Web Jetadmin can perform, the number of times that HP Web Jetadmin tries a firmware upgrade again if the upgrade fails, and how long HP Web Jetadmin waits before trying a firmware upgrade again.

Configure the firmware upgrade settings

1. Go to **Tools** > **Options** > **Device Management** > **Firmware** > **General**.
2. In the **Maximum concurrent upgrades** box, enter the maximum number of concurrent firmware upgrades that HP Web Jetadmin can perform. The default is 8.

   IMPORTANT: If the maximum number of concurrent firmware upgrades is set to 11 or higher, you must also change the value in the `FirmwareUpgradeThreadsize` section in the PerfomanceTuning.config.xml file to match the value specified in the **Maximum concurrent upgrades** box. For instructions on changing the `FirmwareUpgradeThreadsize` section, see Increase the size of the firmware upgrade thread pool on page 81.

   IMPORTANT: Upgrading the firmware on a large number of devices simultaneously is a resource-intensive operation and requires a high-end server. Even if HP Web Jetadmin is installed on a high-end server, HP recommends that you keep the other HP Web Jetadmin tasks to a minimum while the firmware upgrades run.

3. In the **Retries** box, enter the number of times that HP Web Jetadmin tries a firmware upgrade again if the upgrade fails. The default is 0.
4. In the **Time between retries** boxes, enter the number of hours that HP Web Jetadmin waits before trying a firmware upgrade again. The default is 3.
5. Click the **Apply** button.

Increase the size of the firmware upgrade thread pool

The maximum number of concurrent firmware upgrades is defined by the size of the firmware upgrade thread pool. The value specified for the size of the firmware upgrade thread pool must match the value specified in the **Maximum concurrent upgrades** box.

1. Make a backup copy of the PerfomanceTuning.config.xml file. This file is available in the following directory on the HP Web Jetadmin server:

   C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config

2. Open the PerfomanceTuning.config.xml file in Notepad or a similar editor.
3. Change the `<value>`*`xx`*`</value>` attribute in the `FirmwareUpgradeThreadsize` section. For example, specify `30`.

   ```
   <property name="FirmwareComponent.FirmwareUpgradeThreadsize">
    <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
    </type>
    <value>xx</value>
   </property>
   ```

IMPORTANT: The `FirmwareUpgradeThreadsize` section is available in the PerfomanceTuning.config.xml file only for new installations of HP Web Jetadmin 10.3 SR8 or later. For installations that have been upgraded to HP Web Jetadmin 10.3 SR8 or later, this section must be manually added to the PerfomanceTuning.config.xml file.

4. Close and save the file.
5. Restart the HP Web Jetadmin service (HPWJAService).
6. Launch the HP Web Jetadmin client.
7. Change the value of the maximum number of concurrent firmware upgrades. For instructions on changing the value, see Configure the firmware upgrade settings on page 81.

Reports Configuration Options

Global settings for Reports can be set here.

Manage the General Settings for Reports

You can use this option to define the calendar quarters for your company and restore the report templates to the defaults. The specified calendar quarters are reflected in a generated report if the data for that report is separated into quarters.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Reports** > **General**.
2. Select the date for the first day of the first quarter of the year (for your company).
3. To restore all of the Report templates that came with HP Web Jetadmin, click **Restore**.
4. You will be asked to confirm your request. Click **OK** in the dialog box.
5. Click the **Apply** button.

Configure the Data Collection Times for Reports

You can set the default time for all data collections.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Reports** > **Data Collection Times**.
2. For each type of data collection, specify the time that the collection occurs. The default for each type of data collection is 12:00 A.M.
3. Click the **Apply** button.

Supplies Configuration Options

Global settings can be set here for **Supplies**.

Configure the Threshold for Low Supplies

The **General** option controls the supply threshold at which devices are placed in the “supply needed” state.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Supplies** > **General**.
2. In the **Supply level** box, specify the percentage of remaining supplies that triggers the device to send a notification that the supply is low. The default is 25.
3. Click the **Apply** button.

Configure the Shop for Supplies Link in Reports

The **Supplies Reordering** option lets you select whether or not to display a **Shop for Supplies** link on the **Supplies Ordering** report; this is a direct link to the HP SureSupply web site.

Use the following steps:

1. On the top menu bar, access **Tools** > **Options** > **Device Management** > **Supplies** > **Supplies Reordering**.
2. Check the box **Include shop for supplies link in reports** to allow the administrator to enable or disable ordering from SureSupply for the application.
3. Click the **Apply** button.

3 Device Management

The **Device Management** view provides many features for configuring and managing the devices on the network. The left navigation pane and the task modules on the **Overview** pane provide access to these features.

Devices - Common Tasks Task Module

The **Devices - Common Tasks** task module provides links that initiate the following tasks for devices:

- Discover devices on the network
- Create a device group
- Configure the settings on devices
- Subscribe to alerts for devices
- Upgrade the firmware on devices
- Add devices to a data collection
- Generate a report

Devices - Summary Task Module

The **Devices - Summary** task module provides links that display the device lists.

Devices - Active Tasks Task Module

The **Devices - Active Tasks** task module provides a list of the device tasks that are running. Use this task module to stop or view the details of an active task.

Devices - Scheduled Tasks Task Module

The **Devices - Scheduled Tasks** task module provides a list of the device tasks that are scheduled to run. Use this task module to delete or edit a task schedule.

Device Management Options

Configuration options can be set for many functional areas within the **Device Management** view. For more information, see Device Management Configuration Options on page 60.

Device Tabs

When you select a device list or device group, tabs are available in the lower portion of the device list. These device tabs provide additional information and functionality for the devices that are selected in the device list.

Showing and Hiding Device Tabs

The device tabs are displayed in the lower portion of any device list page to provide you with more detailed information about the devices. The device tabs are enabled by default but can be disabled at any time. The advantage of displaying the device tabs is to enable quick access to all device data by simply selecting the device in the device list and then clicking on the desired tab.

To hide the device tabs, use the **Hide Device Tabs** tool (the up/down arrow button on the toolbar on any device list page). This offers more room to display the device list itself. Hiding device tabs can also reduce network traffic and improve performance while working with large lists of devices.

Status Tab

Device status can appear for a single device or multiple devices depending on list selection. Device status polling rates can be altered for both multiple and single status modes. The number of devices that can concurrently display status through **Status** tab is limited to ten by default but can be increased or decreased (Configure the Polling Options for Device Lists on page 61). These settings can be accessed in **Tools** > **Options** > **Device Management** > **Status**.

The **Status** tab shows real-time status messages and graphics that indicate device issues for the selected device or devices. While the status tab is being shown, the device status is updated regularly. Use the **Status** tab to quickly assess the current status of one or more devices.

The polling rate of the devices is set in **Tools** > **Options** > **Device Management** > **Device Polling** (Device Polling Configuration Options on page 60).

The **Status** tab has three possible views:

- **Single device view** (most common): When a single device is selected, the single device view is shown. The toolbar on the **Status** tab links to the Embedded Web Server for the selected device (if the device supports this feature). Device identification information such as device model, host name, IP address, and system contact information is also displayed (as requested through the top menu bar on **View** > **Preferences** > **Device Identification**). Current supply and reserve levels, including the name of the consumable and a percentage level are shown. Additional information on all supplies is available on the device's **Supplies** tab at the bottom of any device list.

- **Multiple device view**: When between 2 and 10 devices are selected, the multiple tiled view is shown. Device identification information such as device model, host name, and IP address is also displayed. Current supplies and reserve levels are shown. Additional information on all supplies is available on the device **Supplies** tab.

  The number of devices shown is determined by the configuration setting in **Tools** > **Options** > **Device Management** > **Device Tabs** > **General** (Configure the General Options for Device Tabs on page 65). If the multiple device view limit is set to 5, and you have more than 5 devices selected, the view changes from individual statuses (for each device) to a status summary for all selected devices.

- **Composite device view**: When more than 10 devices are selected, the composite view is shown. The number of selected devices is shown along with how many are in an **OK**, **Error**, or **Caution** state on the device **Status** tab at the bottom of any device list.

In the **Status** tab, you can select fields from the device information section and click Ctrl-C.

Options on the **Status** tab page include:

- For single device view:
  - **Embedded Web Server** (only enabled in Single device view): Brings up a web browser that takes you to the device's Embedded Web Server, if the device has one.
  - **Configure Page**: Shows the **Config** tab; you can change or add configuration information for devices.
  - **Online** or **Offline** (only enabled in Single device view): Shows whether the selected device is online or offline. You can actually change the status for the device remotely using this option.
- For multiple device view (2-10 devices):
  - **Configure Page**: Shows the **Config** tab; you can change or add configuration information for devices. From the **Customize Status Tab** page, you can select multiple options to be displayed. While it is convenient to have the configuration information displayed, selecting a lot of the options could potentially impact polling time.
- For composite device view (over 10 devices):
  - **Configure Page**: Shows the **Config** tab; you can change or add configuration information for devices. From the **Customize Status Tab** page, you can select multiple options to be displayed. While it is convenient to have the configuration information displayed, selecting a lot of the options could potentially impact polling time.

Parts of the **Status** tab page include:

- **Single device view** (one selected device):
  - **Status**: Shows the status of the selected device.
  - **Information**: Shows device identification information as requested through the top menu bar on **View** > **Preferences** > **Device Identification**.
  - **Front Panel Messages**: Shows the front panel message currently displayed on the selected device.
  - **Supply levels**: Shows the supply and reserve levels that remain for the selected device.
- **Multiple device view** (2-10 selected devices):
  - **Status**: Shows the status of the selected devices.
  - **Information**: Shows device identification information as requested through the top menu bar on **View** > **Preferences** > **Device Identification**.

  - **Front Panel Messages**: Shows the front panel message currently displayed on the selected devices.
  - **Supply levels**: Shows the supply and reserve levels that remain for the selected devices.
- **Composite device view** (11 or more selected devices):
  - **Status summary**: The number of selected devices is shown along with how many are in an **OK**, **Error**, or **Caution** state.

The following configuration options can be set for polling devices.

- Configure the Background Polling Options on page 60
- Configure the Polling Options for Device Lists on page 61
- Configure the Polling Options for Device Tabs on page 62

Config Tab

The **Config** tab allows device configuration for the selected device or devices. A list of configuration items is displayed and is based on the configuration items supported for the devices selected. If one has the correct permissions, they can change one or more configuration items and apply the settings to the device or devices selected. If one does not have the correct permissions, they can only view the configuration items.

If a single device is selected, the configuration items in the tab are shown with the current device settings. If multiple devices are selected, configuration items in the tab are shown with unspecified or blank settings. The list of configurable options varies by the devices selected. With multiple devices selected, all configurable items will probably not apply to all devices. Only settings that apply to a device will be set on that device. Some options may be repeated multiple times because different settings are supported on different devices. If it is not clear which device or device model a particular setting applies to, holding the mouse over the name in the configuration settings displays a tooltip with additional information.

Features on the **Config** tab page include:

- **Apply Template**: Select a previously created configuration template to apply to the currently selected devices.
- **View History**: Displays a list of recent configurations that have occurred on one or more of the selected devices (View the Configuration History on page 177).
- **Customize** button: Starts the **Edit My Settings List** wizard. Use this wizard to create a personalized list of favorite configuration options that are available from the **My Settings** category.

  My Settings allow you to group commonly used configuration items in one place, so they are easy to work with. You can configure, edit, or delete options from **My Settings**. You can access **My Settings** from the **Config** tab in any **Device List** (and then click **Customize**), by right-clicking on any configurable item (for example, in the **Create Configuration Template** wizard).

  After the **Edit My Settings List** is displayed, select the configuration option by highlighting it and clicking the arrow buttons between the two lists. To display the options in **My Settings**, check the **Show 'My Settings'** box. To save your changes, click **OK**.
- **Refresh**: Gets the current settings from a single device, or the unspecified settings for multiple devices. Any pending changes which have not been applied will be lost.
- Category tree: Organizes the configuration options into categories to make them easier to find. The configuration options are listed alphabetically in each category.
- Configuration options: Changes the settings on the devices. The changes that are made to these settings do not take effect until they are applied and confirmed.

- **Save as Template**: Captures the selected configuration in an HP Web Jetadmin configuration template. You can use templates for the following reasons:
  - A backup of the device configuration is needed to manage maintenance and risk.
  - A device configuration is deemed as “release accepted” and a template is needed to configure other devices with like-settings.

  The configuration template only captures configuration options that are selected.
- **Schedule**: Schedule this configuration for later (Schedule Device Configurations on page 178).
- **Apply**: Apply all of the settings to the device or devices now.

Alerts Tab

The **Alerts** tab allows easy access to alerts settings for a particular device or set of devices. Device alerts provide the ability for the device to proactively notify you when a problem occurs with the device.

You can set alerts using the **Alerts** tab or by selecting **Alerts** from the menu at the left. Using the **Alerts** tab can be faster since you have already selected the device or devices.

The **Alerts** tab has two possible views:

- **Single device view**: The current set of subscribed alerts is displayed. You can subscribe to alerts, change alert subscriptions, or remove alert subscriptions.
- **Multiple device view**: A summary view of how many devices have alerts subscriptions and how many do not. The same quick access to alerts subscriptions, change alert subscriptions, or remove alert subscriptions is provided.

Options on the **Alerts** tab page include:

- **Group By**: The different ways you can choose to group alerts:
  - **Device**: Displays devices that can be individually expanded to show each applied subscription and corresponding Alerts detail.
  - **Subscription**: Displays subscriptions by name that can be individually expanded to show devices to which the subscription has been applied.
  - **Solution Type**: Displays one or any of the three types of Alerts that have been configured. These can be expanded to show individual subscriptions and devices to which the subscription has been applied.
- **+** (Expand All): View detail.
- **-** (Collapse All): View summary information only and no detail.
- **Subscribe**: Create an alert subscription.
- **Apply Subscription Template**: Use alert subscription settings to apply to additional devices. The **Alert History** option allows you to view the alerts history for the selected set of devices.
- **Alert History**: View alerts history; can group by device or by alert.

Parts of the **Alerts** tab page include:

- **Device Model**
- **IP Hostname**
- **IP Address**

- Advanced Settings

  There are two threshold settings that can be set through **Advanced Settings**; **Count threshold** and **Percent threshold**. When **Count threshold** is enabled, the Alert will trigger as the increasing device counter matches the value (number) applied here. This is only visible when Page Count Alerting is enabled.

  Percent threshold supplies a common threshold value (percentage) that can apply to threshold Alerts. This is a decreasing percentage and is set on an integer value. This is a percentage based on decreasing supplies. This setting is only applicable to supplies that are depleting or depleted and need replacing.

- Notification Type
- Subscription Type
- Linked to Template

This page displayed is identical to the page displayed when you select **Alerts - All Subscriptions** in the left navigation pane (View All Alert Subscriptions on page 209).

Features on the **Alerts** tab page include:

- **Save As Template**: Save the current settings as an alerts template (Create Alert Subscription Templates on page 200).
- **Unsubscribe**: Remove devices from this alerts template (Edit Alert Subscription Templates on page 205).
- **Edit Subscription**: Make changes to an alerts subscription (Edit Alert Subscription Templates on page 205).

Troubleshoot Tab

The **Troubleshoot** tab provides features that are used to remotely manage and troubleshoot devices. The features that are available vary depending on the devices that are selected in the device list. Some of the features are available only if a single device is selected in the device list.

The following features are available on the **Troubleshoot** tab:

- **Embedded Web Server** button—Opens the device Embedded Web Server (EWS). The EWS provides options to remotely manage the device.
- **Online** or **Offline** button—Sets the device status to online or offline.
- **HP Support** button—Opens the product support page for the device.
- **Reset Device** button—Starts the **Device Reset Options** wizard. Use the following steps to reset the devices:

  1. From any device list, select one or more devices.
  2. Click the **Reset Device** button.
  3. On the **Select a reset option** page, select one of the following options:

     NOTE: The options that are available vary depending on the selected devices.

     ○ **Power Cycle**—Sends a power cycle command to the devices.

     ○ **Reset to Factory Defaults**—Resets the devices to the factory defaults.
  4. To schedule the power cycle to occur at a specific time, select the **Schedule** checkbox.
  5. Click the **Next** button.
  6. On the **Schedule device reset** page, use the following steps to create a schedule:

        a. In the **Name** box, enter a name for the schedule.

        b. From the **Start time** lists, select the date and time that the power cycle occurs.

        c. In the **Recurrence** section, select the option that specifies how often the power cycle occurs, and then specify any associated settings.

        d. Click the **Next** button.

    7. On the **Success** page, click the **Done** button.

- **Print Test Page** button—Sends a test page or file to the device. The file must be in a file format that the device can print. The file formats that are valid vary depending on the device. For example, most devices can print TXT and PJL files. Some devices can print only PDF files.

- **Remote Control Panel** button—Opens the **Remote Control-Panel** page for the device. This page is used to remotely interact with the device control panel. If an administrator password is configured on the device, HP Web Jetadmin displays a page where you must enter the administrator password.

- **Restore Device** button—Launches the Restore Device wizard. Use the following steps to restore the devices:

    NOTE: This option is only supported with FutureSmart devices. If this function is greyed out for FutureSmart devices, click on the Config tab, and then go back to the Troubleshoot tab.

    1. Click **Browse**, and select the backup file from the system (compressed ZIP format).

        The Encryption Key field should match the restore file key provided at the time of taking the backup.

    2. Click the **Restore settings from a different product** box. Once this option is enabled, devices of the same class can be restored.

        NOTE: There is no option to get the backup file from HP Web Jetadmin. Use the device EWS page to get the backup file by navigating to **General**, and then **Backup and Restore**.

        The current configuration settings change once the file is restored, and the device will restart.

        If an invalid encryption key is entered, HP Web Jetadmin displays a success message after the file has been successfully transferred to the printer. With the current firmware implementation, the printer will start processing the file, and HP Web Jetadmin will not know if the file could be decoded/decrypted correctly.

- **Detailed status** section—If a single device is selected, displays a list of the status messages that occurred for the device. If multiple devices are selected, displays the number of each status message that occurred for the devices.

- **Troubleshooting tools** section—Provides historical information for one or more selected devices. Select one of the following options:

    – **Recent Alerts**—Displays a list of the recent alerts.

    To displays more information about all of the alerts in the list, click the **View History** button.

    – **Recent Configurations**—Displays a list of the recent device configurations.

    To display more information about a device configuration, select the configuration from the list, and then click the **Details** button.

    To display more information about all of the device configurations in the list, click the **View History** button.

    – **Firmware Updates**—Displays a list of the firmware updates that are available.

Groups Tab

This tab reflects the group or groups to which a device has membership, when a single device is selected. The tab re-displays all selected devices from any device list showing all columns specified in **View** > **Preferences** > **Device Identification**, and the **Groups** column when multiple devices are selected.

These devices will be added to any group created from the **Groups** tab, **Add devices to group**, or **Add devices to new group**. In the single device mode, **Remove From Group** can be used to remove the selected device from any manual group.

Parts on the **Groups** tab page include:

- **Add devices to group**: Easily add devices to an existing group.
- **Add devices to new group**: Conveniently create a group and immediately add devices to it.

Columns on the **Groups** tab page include:

- **Group**: Lists the name of the group for the selected devices.
- **Description**: Shows the description of the corresponding group as entered while creating a group with the **Create new device group** Wizard or while editing a group with the **Edit device group** wizard.
- **Contact**: Shows contact information of the corresponding group as entered while creating a group with the **Create new device group** Wizard or while editing a group with the **Edit device group** wizard.

Features on this page include:

- **Remove From Group**: Remove a device from the selected group (Remove Devices from a Manual Group on page 130).
- **View**: View the devices in the selected group (View a Device Group on page 134).

  You must select a group before clicking **View**. If you are in a group and click **View** in the **Groups** tab, you must have a row selected with a group other than the one you are in.

Reports Tab

The **Reports** tab allows easy access to report functionality for a device or set of devices.

The two main areas of this feature allow you to access the two main reporting tasks:

- **Data Collection**: Must be enabled for devices to ensure the raw data is present to generate reports. Turning on data collection (by checking the check box and clicking **Apply**) enables this process. The **Job Data** collection option enables the **Jobs by user: color/mono** report. The **Device Data** collection enables the **Device pages: color/mono** report.
- **Report Generation**: Select the type of report to generate.

Parts on the **Reports** tab page include:

- **Group By**: The different ways you can choose to group data:
  - **Device**: Orders the tab-list by each device displayed in the list selection. Expanding the list shows each device and its collection state for each data collection type.
  - **Data Collection**: Orders the tab-list by data collection type and shows devices beneath each.

  - **Enabled**: Shows two groups of devices. One is **Enabled** which are devices that have by-user data collection enabled. The other one is **Disabled**, which are devices that do not have by-user data collection enabled.
  - **None**: Shows a tab-list of all devices selected with their data collection states appearing within columns.
- **+** (Expand All) or **-** (Collapse All): show all details or show only summary information.
- **Add devices to data collection**: Add devices to a data collection that have been defined (Add Devices to Data Collection on page 227).
- **Apply data collection template**: Apply a data collection template (Apply a Data Collection Template on page 229).
- **Generate report**: Produce a report after data collection has completed (Generate Reports on page 235).
- **Schedule report**: Schedule this report to be generated at a specific time (Schedule a Report on page 247).

Supplies Tab

The following tasks can be performed on the **Supplies** tab for the devices selected in a device list:

- Quickly check the status of the supplies and its reserve levels that are installed on the selected devices
- Print a report that shows the status of the supplies
- Access the HP SureSupply website to purchase supplies

The following features are available on the **Supplies** tab:

- **Group by** list—Specifies how the supplies information is grouped and displayed in the list. Select one of the following options:
  - **Device**—Groups the information by the device model name.
  - **Urgency**—Groups the information by the level of the supply, such as **Low**, **Empty**, and **OK**.
  - **Part number**—Groups the information by the part number of the supply.
  - **None**—Displays one line for each supply that is installed on the selected devices.
- **Refresh Sort** button—Updates the sorted information.
- **View** list—Specifies how much information about the supplies is included in the list. Select one of the following options:
  - **Default**—Displays the device model, IP hostname, IP address, supply level, reserve level, pages remaining, part number, and so on.
  - **Details**—Displays all of the information that the **Default** option displays and also displays information such as the capacity, manufactured date, and serial number of the supply.
- **+ (Expand all rows)** button—Expands each row to display the detailed information.
- **- (Collapse all rows)** button—Collapses each row to display only the summary information.
- **Show all** and **Show only needed** buttons—Specifies which supplies are displayed in the list. These buttons toggle between the two features.
  - **Show all** button—Displays all of the supplies that are available for the selected devices.
  - **Show only needed** button—Displays only the supplies that are in a low or very low state.

- **Refresh Supplies** button—Updates the levels of the supplies and its reserve state.
- **Shop for supplies online** button—Opens the **Order Supplies** window where you must choose whether HP Web Jetadmin automatically sends information about the selected printers to HP. Select the appropriate option, and then click the **OK** button. The HP SureSupply website opens where supplies for the devices can be purchased.
- **Print shopping list** button—Generates a print preview of the information that is currently displayed in the list.

Storage Tab

Storage management functionality is used to manage fonts, macros, and objects on device storage facilities such as disk or flash devices. This functionality can be viewed from any device list with one or more devices selected and then choosing the **Storage** tab.

All selected devices are displayed in the **Storage** tab list with **Device Model**, **IP Hostname**, and **IP Address** defined. Used space and Read/Write accessibility are displayed for each device in the list. In addition, grouping controls exist for multiple devices enabling a variety of storage analysis and storage configuration access.

The following features are available on the **Storage** tab:

- **View** list: To change the information that is displayed on the **Storage** tab, select one of the following options from the list:
  - **Media**: This option lists the storage media on the selected devices. If the **Storage Device count** is **1** or greater, the mouse-over tool tip displays a table of all the storage media on the device. The following options are available in this view:
    - **Secure Storage Erase**: Starts the devices secure storage erase action. One of three secure modes can be set for the storage erase action. These modes are **Non-secure Fast Erase**, **Secure Fast Erase**, and **Secure Sanitizing Erase**. The extent of security in the secure erase feature on the device will depend on device model and firmware. See device documentation regarding Secure Storage erase features for more details. An option to enable write-protect can be set to leave the device in read-only mode once secure storage erase has completed. This feature can be scheduled as a one time or recurring operation.
    - **Initialize File System**: Causes the device user-directory structure to initialize. The file system will vary depending on device or storage type; please see device-specific documentation. This feature can be scheduled as a one-time or recurring operation.
    - **Write Protection**: Enables or disables write functionality on the selected storage facility. This makes a device read-only or read-write capable.
    - **Erase Customer Data**: Starts the **Erase Customer Data** wizard. This wizard removes any job information that is stored on the device, but does not remove any device configuration settings. The device cannot be used while the erase operation is in progress. The erase operation can be scheduled to occur at a specified time.

      The erase operation runs in one of the following modes:

      - **Non-secure fast erase**
      - **Secure fast erase**
      - **Secure sanitizing erase**—This erase mode overwrites the data three times. The erase operation might take several hours to complete for a large hard disk that has numerous jobs.

    HP Web Jetadmin monitors the erase operation for one hour. If the erase operation takes more than one hour to complete, HP Web Jetadmin displays an error message on the **Results** page of the **Erase Customer Data** wizard. However, the device continues the erase operation until it is complete.

    - Secure cryptographic erase

  For more information about HP FutureSmart devices and hard disk security, see the *HP FutureSmart Firmware Device Hard Disk Security* white paper. This white paper is available from the HP support page (in English).

  - **Use Drive**: If a device has more than one drive installed, enables you to select the drive where configuration files, stored jobs, and temporary files are stored, and move existing customer data to that drive. You cannot move configuration data to a RAM drive because all data on a RAM drive is lost when the drive is turned off and then turned on. You can create a schedule to run the Use Drive operation one time or on a recurring basis.

  - **Erase Drive**: Enables you to completely erase a drive. This process does not preserve any data. You can erase only one drive at a time. The **Secure Erase** option selects the most secure erase method available for the selected drive. The **Cryptographically Erase** option is performed only on secure drives. This option resets the encryption key, prevents access to the data, turns the drive off and then on, and re-encrypts the drive with new keys. You can create a schedule to run the Erase Drive operation one time or on a recurring basis.

  - **Set Encryption to AES_128**: Erases all of the data on the SSD drive. The device automatically turns off and then turns on. When the device turns on, the encryption level is set to AES-128.

  - **Set Encryption to AES_256**: Erases all of the data on the SSD drive. The device automatically turns off and then turns on. When the device turns on, the encryption level is set to AES-256.

- **Fonts and Macros**: This option displays the number of fonts and macros installed on the device. The mouse-over tool tip displays a table of all the fonts and macros installed on the device. The following options are available in this view:

  - **Repository** button: Displays the **Repository** pane with a list of all of the fonts and macros that are stored in the repository. For more information about managing the storage repository, see Storage Repository on page 256.

  - **Install**: Installs a font or macro on the selected device. (See Install Fonts and Macros on Devices on page 258.)

  - **Remove**: Removes the selected fonts and macros from the device, but does not remove them from the **Storage Repository**. (See Remove Font and Macro Files from Devices on page 258.)

  - **Print Font/Macro**: Prints the selected fonts and macros. (See Print Font/Macro on page 258.)

- **Resident Fonts**: This option displays the number of resident fonts on the device. The mouse-over tool tip displays a table of all the resident fonts on the device.

- **Disk Jobs**: This option displays the number of stored jobs currently on the device. The mouse-over tool tip displays a table of the stored jobs on the device. The following options are available in this view:

  - **Delete**: Deletes the selected print job.

  - **Print Disk Job**: Prints the selected print job. If the print job is secured by a PIN, you must type the correct PIN in order to print the job. You can enter only one PIN. If you select more than one PIN-protected job and the jobs have different PIN values, you can print only one. HP recommends that you select only one private print job at a time to avoid this restriction.

- **Templates** button: Displays the **Templates** pane with a list of all of the storage templates that have been created. For more information about storage templates, see Storage Templates on page 259.

Solutions Tab

The **Solutions** tab displays the following information about the devices that are selected in the device list:

- The number of applications, such as chailets and Microsoft .NET Framework applications, that are installed on the device
- The number of solutions that are installed on the device
- Whether Application Manager and Solution Manager are installed on the device

  Application Manager and Solution Manager are required to install chailets and .NET Framework applications. Application Manager is required to install solutions.

The following features are available on the **Solutions** tab:

- **Repository** button—Accesses the Solutions Repository where you can manage the solutions. For more information, see Solutions Repository on page 263.
- **Apply Template** button—Starts the **Apply Solution Template** wizard. For more information about this wizard, see Applying a Solutions Template on page 268.
- **Install Managers** button—Starts the **Install Manager** wizard. For more information about this wizard, see Install Solutions on page 96.
- **Remove** button—Starts the **Uninstall Solution** wizard. For more information about this wizard, see Uninstalling Solutions on page 265.
- **Edit** button—Starts the **Edit Solution** wizard. For more information about this wizard, see Editing Solutions on page 95.
- **Install** button—Starts the **Install Solutions** wizard. For more information about this wizard, see Installing Solutions on page 264.

Editing Solutions

- **Description**: custom description of the solution.
- **Application URL**: specifies where the solution is located, and identifies a credential that can be applied to access the location.
- **Configuration URL**: specifies where a configuration file is located, and identifies a credential that can be applied to access the location. The configuration file is used to configure the solution.
- **License URL**: specifies where a license file is located, and identifies a credential that can be applied to access the location. The license file is used to grant access to various functionality within the solution.

You can edit the **Configuration URL** and **License URL** properties for one or more solutions using the **Edit Solution** wizard.

1. From the **Solutions** tab, select a device and click **Edit**. The **Edit Solution** wizard is started with the **Select options** page displayed.
2. Select an existing template or manually specify options.
3. To edit the solution immediately, click **Next**.

   -or-

   To schedule the edit for another time, click **Schedule** and then **Next**.
4. Select at least one solution and click **Next**. The **Edit settings** page is displayed with a list of solutions that have been selected.
5. If you select one of the displayed solutions, its **Configuration URL** and **License URL** settings are displayed in the **Settings** group box on the right side of the wizard page.
6. Specify new **Configuration URL** and **License URL** settings and then click **Activate Choice for Solution**. The selected solution will have its associated **State** column changed to **Modified**. Click **Next**.
7. If you are installing the solution now, the **Confirm** page is displayed.

   If you chose to schedule the edit of the solution, the **Specify schedule options** page is displayed. Assign a name and then specify a date, time, and recurrence for the edit.

   Click **Next**. The **Confirm** page is displayed.
8. Click **Edit**. The **Results** page is displayed.
9. Click **Done**.

Install Solutions

The **Install Solutions** wizard installs the **Application Manager**, or the **Solution Manager**, and the solution. Follow these steps:

1. Select a device or devices within the **Solutions** tab.
2. On the **Solutions** tab page at the bottom of any device list, click **Install**. The **Install Solutions** wizard is started with the **Select** page displayed.
3. Select the **Install Solution Manager** check box for FutureSmart devices, or **Install Application Manager** depending upon the device (FutureSmart devices or other devices), and then select the solution.
4. Click **Next**. The **Confirm** page is displayed.
5. Click **Install**.

Capabilities Tab

The **Capabilities** tab page shows a list of capabilities information for either a single device or multiple devices, depending on the devices selected in the device list. Device capabilities are displayed in two columns: capabilities name and capabilities value. An alphabetic sort can be done on the capabilities name.

Firmware Tab

The **Firmware** tab provides information about the device firmware and HP Jetdirect firmware that are currently installed on the selected devices and information about the newer firmware versions that are available in the Firmware Repository. The following features are available on the **Firmware** tab:

- **View** list—To change the information that is displayed on the **Firmware** tab, select one of the following options from the list:
  - **Summary**—Displays the status of the firmware that is installed on the selected devices, indicates if newer versions of the firmware are available, and indicates the number of selected devices that are currently in a short stack condition.

NOTE: When the HP Jetdirect firmware is upgraded, a device might be left in a short stack condition if the device is disconnected during the upgrade process or a fatal error occurs. HP Web Jetadmin detects this error condition and tries the upgrade again to make sure that the device is not left in an incomplete upgrade state.

– **Printer Firmware**—Displays detailed information about the device firmware on the selected devices.

  The **Printer Firmware - Severity** column can be used to verify that the device firmware is up-to-date. A green icon indicates that the latest version of the device firmware in the Firmware Repository is installed on the device. A yellow icon indicates that a newer version of the device firmware is available in the Firmware Repository. The **Up-to-date** icon is displayed in this column if the firmware version on the device is newer than the firmware versions that are available in the Firmware Repository or if the firmware version on the device is the same as the latest firmware version that is available in the Firmware Repository.

  By default, HP Web Jetadmin checks for newer firmware versions in the HP Web Jetadmin Firmware Repository. Instead of checking all firmware files in the HP Web Jetadmin firmware repository, it can validate if newer qualified images are available in the HP Web Jetadmin repository by changing the value for ConsiderQualifiedFirmwareAsLatest in the FirmwareUpgrade.config.xml to True. If this setting is not available in the FirmwareUpgrade.config.xml file, then add the full section:

```
<property name="ConsiderQualifiedFirmwareAsLatest">
   <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
   </type>
   <value>True</value>
</property>
```

  After changing the value in the xml file, restart HP Web Jetadmin. If the value for ConsiderQualifiedFirmwareAsLatest in the FirmwareUpgrade.config.xml is set to True, HP Web Jetadmin will only consider the qualified firmware image as the latest image, even if there is a non-qualified image with a later firmware datecode and version available in the HP Web Jetadmin repository. If none of the firmware images are set as qualified, then it will always show the existing device firmware as up-to-date.

  By default, the FirmwareUpgrade.config.xml can be found in:

  C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config

  The **Printer Firmware - Available in WJA Repository** column displays the number of device firmware files in the Firmware Repository that are available to install or reinstall on the device. This number includes the current device firmware file and all of the new firmware files in the Firmware Repository that can be installed or reinstalled on the device. The **Up-to-date** icon is displayed in this column if the firmware version on the device is newer than the firmware versions that are available in the Firmware Repository.

– **Jetdirect Firmware**—Displays detailed information about the HP Jetdirect firmware on the selected devices.

  The **Jetdirect Firmware - Severity** column can be used to verify that the HP Jetdirect firmware is up-to-date. A green icon indicates that the latest version of the HP Jetdirect firmware in the Firmware Repository is installed on the device. A yellow icon indicates that a newer version of the HP Jetdirect firmware is available in the Firmware Repository. The **Up-to-date** icon is displayed in this column if the firmware version on the device is newer than the firmware versions that are available in the Firmware Repository or if the firmware version on the device is the same as the latest firmware version that is available in the Firmware Repository.

  The **Jetdirect Firmware - Available** column displays the number of HP Jetdirect firmware files in the Firmware Repository that are available to install or reinstall on the device. This number includes the current HP Jetdirect firmware file and all of the new HP Jetdirect firmware files that can be installed or reinstalled on the device. The **Up-to-date** icon is displayed in this column if the firmware version on the device is newer than the firmware versions that are available in the Firmware Repository.

NOTE: HP Web Jetadmin can consider only qualified **Jetdirect Firmware**. The ConsiderQualifiedFirmwareAsLatest option mentioned under **Printer Firmware** also applies to**Jetdirect Firmware**.

- **Repository** button—Displays the **Firmware Repository** pane. For more information about managing the repository, see Firmware Repository on page 213.
- **Upgrade** button—Starts the **Firmware Upgrade** wizard. This button is available only if the same version or a newer version of the device firmware or HP Jetdirect firmware is available for the selected devices.

Copy Template Wizard

Throughout **Device Management** view, templates can be created and managed to save you time and provide consistency. Templates contain configuration preferences (that vary by template type) and can be applied to devices or groups. Templates are available in **Configuration**, **Alerts**, **Discovery**, **Data Collection**, and **Report Generation**. Templates with a locked icon next to them are system templates that cannot be edited; these templates can be copied if you want a template with similar settings.

NOTE: In the **Application Management** view, templates can be created for **Role Templates** (Role Templates on page 283).

After a template has been created, it can be copied to create a new template and then changes can be made. This is useful if you need a template similar to an existing one.

To copy templates, perform the following steps:

1. In the left navigation pane, right-click the area for the template (**Configuration**, **Alerts**, **Discovery**, **Data Collection**, and **Report Generation**) and select **Copy template**. The **Copy Template** wizard is started with the **Specify template name** page displayed.
2. Select the template to copy from the **Template** drop-down list.
3. In the **New template name** field, type the name of the new template.

   The original template will remain unchanged.
4. Click **Next**. The **Confirm** page is displayed showing the original template name and the new template name just created.
5. If the new template name is correct, click **Copy Template**. The template will be copied to its new name.
6. The **Results** page is shown. Click **Done**.
7. Make changes to the new template by following the appropriate steps:
   - Edit Configuration Templates on page 185.
   - Edit Alert Subscription Templates on page 205.
   - Edit Discovery Templates on page 168.
   - Edit a Data Collection Template on page 230.
   - Edit a Report Template on page 253.

Export and Import Device Configuration Templates

In an environment that has multiple instances of HP Web Jetadmin, you can create device configuration templates in one instance, and then import them into the instances that are running on different servers. However, to import device configuration templates, each server must run the same version of HP Web Jetadmin.

Export device configuration templates

1. In the **Device Management** navigation pane, expand **Configuration**.
2. To export multiple templates, right-click **Templates**, and then select **Export configuration templates**. The **Export Templates** wizard starts. On the **Select template** page, select the templates, and then click the **Next** button.

   -or-

   To export one template, expand **Templates**, right-click the template, and then select **Export**. The **Export Templates** wizard starts.
3. On the **Specify export options** page, enter a password in the **File encryption password** box. This password prevents unauthorized access to any sensitive data in the template.
4. In the **Confirm password** box, enter the password again, and then click the **Next** button.
5. On the **Confirm** page, verify that the correct templates are listed, and then click the **Export** button.
6. On the **Save as** window, navigate to the location to save the template file, enter a name in the **File name** box, and then click the **Save** button.
7. On the **Results** page, click the **Done** button.

Import device configuration templates

1. In the **Device Management** navigation pane, expand **Configuration**.
2. Right-click **Templates**, and then select **Import configuration templates**. The **Import Templates** wizard starts.
3. On the **Select file** page, click the **Browse** button, navigate to and select the template file, and then click the **Open** button.
4. In the **File password** box, enter the password that was assigned to the template file when it was exported.
5. To overwrite an existing template that has the same name, select the **Overwrite duplicate templates** checkbox. If you select this checkbox, a warning message appears on the **Confirm** page.
6. Click the **Next** button.
7. On the **Confirm** page, verify that the file name is correct, and then click the **Import** button.
8. On the **Results** page, click the **Done** button.

Edit Schedule Wizard

After a schedule has been completed, it can be edited.

To edit schedules, perform the following steps:

1. In **Device Management**, access the **Scheduled Tasks** task module. Then highlight the task and **Edit**.

   In **Application Management**, access the **Application Management - Schedule Tasks** task module or the **Web Jetadmin - All Active Tasks** task module.

2. Highlight the task and click **Edit**.
3. Click **Next**. The **Confirm** page is displayed.
4. The **Results** page is shown. Click **Done**.

Mapping

Mapping lets you identify the physical location of devices, device groups, and URLs on a map. You can also set up navigation shortcuts to key items.

There are three general steps to follow to use the **Map** features:

1. Activating the Maps Feature on page 102
2. Adding a Map Graphic to a Device Group on page 102
3. Placing Devices and Subgroups on a Map on page 103

When all three of these steps have been completed, you can use the **Map** docking feature and begin interacting with maps (Docking Task Modules and Maps on page 35).

Devices and Groups

Devices in groups and sub-groups have specific behaviors that should be considered:

Devices in Automatic Groups

- If a device that has been placed on the map for an automatic group is automatically removed from an auto group (because it no longer meets the auto group criteria) it is removed from the map but the information that is on the map and where it is placed is maintained in case the device is automatically added back into the group in the future. The mapping information will be maintained until the map for the group is removed, the group is removed, or the device is deleted from HP Web Jetadmin.
- If a device is automatically added to an automatic group (because it meets the auto group criteria) the behavior depends upon whether or not it was previously on the map. If it was not previously on the map, then it will not be on the map after it is added. If it was on the map when it was automatically removed earlier, then it will be placed back on the map in the same location. If the map has been changed in between and the location is now off the map, the map item will be removed from the map.

For more information about automatic and manual groups, see Manual versus Automatic Groups on page 122.

Devices in Sub-groups

- If you remove a sub-group that has been placed on its parent's map, then the sub-group is removed from the map and all map information about that sub-group on that map is permanently deleted from

HP Web Jetadmin. For information about sub-groups, see Placing Devices and Subgroups on a Map on page 103.

- If you change a sub-group that has been placed on its parent's map to have a different parent group, then the sub-group is removed from the original parent group's map and all map information about that sub-group on that map is permanently deleted from HP Web Jetadmin.

Hidden Devices and Mapping

Hidden devices in HP Web Jetadmin will not be displayed on any map. However, HP Web Jetadmin will continue to remember that the device is on those maps and where it was placed unless the map or group with the device is deleted from HP Web Jetadmin.

When you reactivate a hidden device, it reappears on any maps that contained it when it was hidden. It is placed in the same location on each map on which it appeared. If the map for the group has changed and the location where the device is to be placed is no longer on the map, then the device is permanently deleted from that group's map. For automatic groups, the device only reappears on the map if it also reappears in the group because it still meets the auto grouping criteria for the group.

Activating the Maps Feature

The **Map** module must be activated before you can use it.

1. From the top menu bar, select **View** > **Device Modules** > **Map**.
2. If **Map** is grayed out, it is already active. If it is not grayed out, select it to activate maps.

   If you are in a device group with a map, activating it causes the map for that group to appear. If not, then there are no visible changes when this feature activated.

Adding a Map Graphic to a Device Group

Any graphic can be added to a device group. File types must be supported by Microsoft Windows.

1. From the left navigation pane, select **All Devices** or a group under **Groups**.
2. Click **Configure map** in the toolbar. The **Configure map** dialog is displayed.
3. To add a map to the group, follow the steps on the page. You can also drag-and-drop a graphic onto the right-hand portion of the window to use it as your map graphic.

Changing a Graphic Image for a Map

A graphic image for a map can be changed to a different image. File types must be supported by Microsoft Windows.

1. Click **Configure Map** on any device list page. If the group already has a map and the map module is showing the map for the group, you can access **Configure Map** by clicking on the **Configure Map** tool on the **Map** toolbar.
2. Click **New map**. The **File Open** dialog is displayed.

3. Specify the new graphic file

4. Drag a graphic image and drop it on the picture area of the **Configure map** dialog.

Placing Devices and Subgroups on a Map

Before you can place devices on a group map, there must be devices in the group (Add Devices to a Group on page 129). In order to place sub-groups on a group map, the group must have sub-groups.

The device image is the same image used for that device in device lists. It is centered on the point where you drop it on the map.

If selecting more than one device, devices are placed on the map at the point where you drop them with each image being positioned slightly down and to the right of the previous one. If the automatic positioning places an image off of the map, the cascading continues in the upper left corner of the map.

A device or a subgroup may only appear on the map once. Once it is on the map, it no longer appears in the list on the left. Devices may appear on multiple maps. Subgroups can only appear on the map for their parent group.

1. Click **Configure Map** on any device list page. If the group already has a map and the map module is showing the map for the group, you can access **Configure Map** by clicking on the **Configure Map** tool on the **Map** toolbar.

2. Select **Device** or **Group** from **Map Item Type**. The devices in the device group are listed.

3. Select one or more devices in the list and drag and drop them on the map where you want them.

4. To move the device or subgroup to a different location on the map, click on it and drag and drop it on its new location.

Placing URLs on a Map

1. Click **Configure Map** on any device list page. If the group already has a map and the map module is showing the map for the group, you can access **Configure Map** by clicking on the **Configure Map** tool on the **Map** toolbar.

2. Select **URL** from **Map Item Type**. The devices in the device group are listed.

3. Type a name and Web address for the URL.

4. Click on the URL and drag and drop it onto the map where you want it. The item image is placed centered on the point where you drop it.

5. To move the URL to a different location on the map, click on it and drag and drop it on its new location.

Viewing Device or Group Status

The **View** mode provides various functionality for maps.

- Device status: The status of a device or a group is only displayed on the map in **View** mode; it is not visible in **Configure Map**. The status is shown on the device icon on the map.

- Selecting devices on a map: Selecting a device on a map also selects it in the device list. If a device is on a map, selecting it in the device list will also select it on the map. Multiple devices can be selected on the map by holding down Ctrl.

- Accessing devices in sub-groups: Selecting a group on the map also selects it in the left navigation pane and displays its device list. If the new group has a map, it is displayed in the map module; if it does not have a map, the map module is hidden.

- Move up to a parent group: Use **Map** to move to the parent group by clicking **View parent group** item on the map module's toolbar. This selects the parent group in the left navigation pane and switches to that group's device list. If the parent group has a map it is displayed in the map module; if it does not have a map the map module is hidden.

- Go to a URL: Select a URL on the map to launch the browser and take you to that URL.

- Filter device list: Any filter applied to the device list is also applied to the map. For example, if you apply the **Color devices** filter to the device list, the map no longer shows monochrome devices that have been placed on the map. Clearing the filter causes the mono devices to reappear on the map.

Sizing a Map

A map can be resized using one of three methods.

In **Edit** mode, resize the **Configure Map** dialog by clicking and dragging a corner of the map graphic.

In **View** mode, use the drop-down in the **Map** module and select one of three methods. The images for the devices, groups, or URLs on the map will move appropriately as the map is scaled to continue to center on the same point on the map.

- **Fit to screen**: The map image will fit exactly within the available space of the **Map** window.

- **100%**: The map image is displayed as the actual size of the graphic image that is being used for the map. Depending upon the current size of the map module window, the resulting image may be smaller or larger than the window.

- **Custom**: You can select the size of the map between 10% of actual size to 200%. Select **Custom** and then use the “minus” and “plus” signs to decrease or increase the size of the map. These buttons change the zoom by 10% each time they are clicked until the limit is reached (at which time the button will be disabled).

Removing Items from a Map

You can remove items from a map without removing the entire map.

1. Click **Configure Map** on any device list page. If the group already has a map and the map module is showing the map for the group, you can access **Configure Map** by clicking on the **Configure Map** tool on the **Map** toolbar.

2. Remove items using one of these methods:

   - Click the item to remove and drag it off the map.

   - Right-click on the item to remove and select **Remove item**.

Removing a Map from a Group

You can remove a map from a group with one of the following methods:

- Use **Remove map** on the toolbar.
- Right-click on the map to remove and select **Remove map**.

Device Lists

HP Web Jetadmin **Device Lists** and related features such as sorting and filtering lets you easily locate, manage, and analyze device fleets. Batch configuration, fleet upgrades, reporting and other powerful HP Web Jetadmin features all start with the basic list of devices.

For example, Pete is an HP Web Jetadmin user who understands that all devices of a certain model and in a certain geographical location require firmware updates. These updates are required to enhance the device functionality and increase performance. Using advanced filtering, Pete can get a list of devices that match both the model and geographical location criteria. Pete can then export the details from this list and use the contact information to begin communicating a time frame in which the firmware updates will occur. After a time, the contacts are all aware of the firmware update activity that will happen after hours when most devices are not in use. Then, using a device list and firmware updating, Pete can schedule the fleet updates for these devices. Later, again using HP Web Jetadmin lists, Pete can view all of the devices that have or have not completed the firmware update process. A common theme in this scenario is device lists and filtering. (See Filters and Device Lists on page 110.)

Pre-Defined Device Lists

The following pre-defined device lists show devices on your network that are not marked as hidden:

- **All Devices**: Displays a list of all discovered devices.
- **Color Devices**: Displays a list of discovered devices that support color.
- **Error Devices**: Displays a list of discovered devices that are in an error state.
- **Information Devices**: Displays a list of discovered devices that are in an information state.
- **New (Last Discovery)**: Displays a list of devices that were discovered for the first time by the last discovery.
- **New (Manual)**: Displays a list of discovered devices that are considered new. Devices are considered new when they are first discovered. The devices remain in this state until you explicitly acknowledge them. Acknowledging devices can be done by right-clicking any selection of devices in any devices list.
- **New (Time Period)**: Displays a list of devices that were discovered for the first time within the last 14 days. You can set the number of days in **Tools** > **Options** > **Device Management** > **Device Filters** > **New Devices Filter**. For more information, see Configure the Number of Days that Devices are Considered New on page 65.
- **Non-unique Devices**: Displays a list of discovered devices that cannot be uniquely identified.

  HP Web Jetadmin uses a combination of the device serial number, model name, and model number to create a unique identification for each device it discovers and adds to the **All Devices** list. If a device cannot supply any of these attributes, HP Web Jetadmin adds the device to the **All Devices** list, but marks the device as non-unique. Some features, such as Device Utilization Data Collections, do not function with non-unique devices.
- **PC-Connected Devices**: Displays a list of discovered devices that are connected to a PC rather than connected directly to the network.
- **Ready Devices**: Displays a list of discovered devices that are in a ready state.

- **Ungrouped Devices**: Displays a list of discovered devices that are not assigned to any group.
- **Warning Devices**: Displays a list of discovered devices that are in a warning state.

If the **Device Model** column is blank, that device has a model name that HP Web Jetadmin does not recognize. If **Unknown (Disconnected)** appears in the **Device Model** column, the HP Jetdirect print server does not have a printer connected to it.

Groups lists are the **Device Lists** that display when a group is selected. These lists can be searched or filtered just as the **All Devices** list can be searched or filtered (Search Device Lists on page 114 or Filters and Device Lists on page 110). For more information about Groups, see Groups on page 121.

Columns for Device Lists

The columns in device lists contain simple data or complex data. HP Web Jetadmin obtains most of the data that appears in these columns by querying the devices, but some of the data is specific to HP Web Jetadmin. You can use the columns to sort and customize the device lists.

There are numerous columns in HP Web Jetadmin. This number continually increases as new devices, functionality, and plug-ins are released.

Use the following steps to add or remove columns in device lists:

1. Access any **Device List**. Right-click in any column header and select **Customize**. The **Select Columns** wizard is started.
2. To specify the columns displayed on this page, select one of the following options from the **Category** drop-down list:
   - **Favorites**: Displays the most commonly used columns.
   - **All**: Displays all of the available columns, except obsolete columns. To display only a specific category of columns, expand **All**, and then select the category.
   - **Obsolete**: Displays columns that are still available in HP Web Jetadmin, but have been replaced by new columns or will not be supported in the future.
3. Select the column by highlighting it and clicking the arrow buttons between the two lists. To select multiple columns, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons.

   Some complex columns support displaying portions of their detailed information as individual columns. These complex columns display the detailed items as children in a tree structure in the column selection control. To see the detailed information that can also be used as columns, expand the complex column. When you move a detailed item to the other list, the name of the item is displayed followed by the name of its parent in parentheses.
4. Click **OK**. The changes should be reflected on the **Device Lists**.

Complex Data in Device Lists

A complex column contains a summary of the data in a grid format. The heading of a complex column contains an icon (a magnifier over a sheet of paper) that indicates an advanced tooltip is available. Hold the cursor over the underlined data in the grid to activate the advanced tooltip feature and display more information about the data in a grid format. You can also display the data for a complex column as separate columns.

The data in the complex column is not a combination of all of the column's subitems. The data in the complex column is one of the following values:

- The value of only one of the column's subitems that are displayed when the cursor is held over the data in the complex column, such as the **Print Usage Counters** complex column
- A unique value, such as the **Proxy Server** complex column

The advanced tooltip displays for 1 minute or until you move the cursor outside of the tooltip. Every time you move the cursor within the tooltip, the 1 minute starts over. The information in the tooltip can also be complex. In this case, the tooltip displays a summary of the data and an icon that indicates more data is available. Hold the cursor over the data in the tooltip to activate another advanced tooltip that displays the next level of data.

Columns Dependent on HP Web Jetadmin Data

Some column data is internal to HP Web Jetadmin and is not obtained from the device, such as device status or other data specific to the local application. Examples of these columns dependent on HP Web Jetadmin data are:

- **User Defined Settings**: Custom columns that can be created by users and then populated with data that is only resident on the application. (In previous versions of HP Web Jetadmin, this used to be called custom fields or custom settings.)
- **Acknowledged**: Shows if you have defined the device as **Acknowledged**. Acknowledging devices can be done by right-clicking any selection of devices in any devices list.
- **Credentials Required**: Shows requests for required credentials that were not met.
- **Discovery Date/Time**: Time and date of the last discovery.
- **Last Communication**: Time and date of the last communication.
- **Last Discovered**: Time and date of the last discovery that found this device.
- **PC-Connected**: If a device is locally connected to a PC.
- **Status**: HP Web Jetadmin status message about the device.
- **Severity**: Severity rating of status for the device.
- **Groups**: Shows the group membership for a device, listing ether a single group or the word "multiple". If you hover-over it with your mouse a listing of all groups is displayed.

You can enable two different columns that help track discovery and communication and represent internal device date/time tracking: **Last Communication** and **Last Discovered**. These time stamps are updated whenever a discovery has occurred in which the device was discovered or re-discovered.

Columns Dependent on HP Jetdirect Data

Some columns displayed in device lists in HP Web Jetadmin are dependent on data retrieved from HP Jetdirect devices:

- **Jetdirect Model**
- **Jetdirect Port**
- **Jetdirect Revision**

IP Hostname and **System Name** can both be enabled in HP Web Jetadmin device lists. The **IP Hostname** is enabled in the **Default HP Web Jetadmin** device list layout. These two items can be useful but can also be confusing.

IP Hostname is an element that is populated with a name retrieved from network DNS (Domain Name Service). HP Web Jetadmin uses the device IP address and performs what is known as a reverse-lookup; DNS responds with a name value if one is registered within the service for that particular IP address. Two requirements exist for HP Web Jetadmin to be able to get a device's **IP Hostname**: DNS provides reverse name lookup based on the IP address, and the device IP address must have a name registered in DNS. If HP Web Jetadmin performs a name lookup for a device's IP address and DNS is unable to deliver a result, the value **Unknown** is displayed in the device list's **IP Hostname** column. HP Web Jetadmin will only show resolvable names in the **IP Hostname** column.

The **IP Hostname** column is enabled by default. To populate this column, HP Web Jetadmin must perform DNS lookups. To enable DNS lookups, go to **Tools** > **Options** > **Shared** > **Network** > **DNS**. For security and performance reasons, you can disable DNS lookups.

System Name is an object that is bound to the HP Jetdirect print server. The **System Name** appears as **Host Name** in the Embedded Web Server (EWS) interfaces for many devices in the networking configuration area. This device bound name, in and of itself, is not resolvable through DNS. When a device's **System Name** is changed to something like "PRTR445" and the DNS name value for a device's IP address is "lab412", the IP Hostname column in HP Web Jetadmin will reflect "lab412". **System Name** is simply a device bound object that can be changed using HP Web Jetadmin and the device's EWS but there are cases when it can also be registered into DNS.

HP Jetdirect print servers have a few different features that can allow the **System Name** value to become registered into a device's DNS. In many cases, when devices have their IP address parameters DHCP configured, a registration with DNS is possible. This is dependant on both the DHCP system on the network, the HP Jetdirect print server model and firmware revision, and the system name being populated on the HP Jetdirect print server. For more information about DHCP/DNS name registration, see the technical documentation for HP Jetdirect print servers. WINS is another network service that can be used to make HP Jetdirect print server system names visible through DNS. Many HP Jetdirect print servers are capable of exposing the **System Name** via WINS and WINS/DNS linkages can cause these names to be DNS visible and also appear in the **IP Hostname** column in HP Web Jetadmin. For more information about **IP Hostname** and DNS registration, see the technical documentation for HP Jetdirect print servers.

Statuses on Device Lists in HP Web Jetadmin

You can select columns to view on **Device Lists** from a static list of columns. The various statuses might be displayed in those columns include:

- **Unavailable**: The device does not support the column.
- **Undefined**: For the HP Jetdirect version when the device is incapable of reporting that attribute.
- **Missing**: Usually a temporary status until the device communicates its data to HP Web Jetadmin.

Manipulating Columns in Device Lists

You can manipulate columns on the device lists in HP Web Jetadmin:

- **Selecting Devices**: Selecting a device means performing some action that causes the device to become selected which sets up the device or devices for some further action. Click to select one device or Shift +Click to select multiple devices.
- **Resize columns**: To set the width of a column, click and drag the column marker in the list header to the desired width. Or, to resize the column to the broadest width required to display the data, double-click on the column header.
- **Sort columns**:

- To sort the entire device list by a specific column, click in the header for that column. Click again to reverse the sort.
- To perform a secondary sort on a list, use Shift+Click on a different column after the initial sort.
- To perform additional sorts, hold down Shift while clicking on different column headers.

- **Display or hide columns**: To display or hide columns, right-click on the column header. The columns that are currently displayed have a check mark next to them; the ones that are not displayed (or hidden) have nothing next to them. Click on the columns to display or hide.
- **Right-click menus**: Various kinds of right-click menus are displayed based on whether something is selected and what list is displayed. For example, if a device is selected on a device list, right-clicking within the device list causes different menu options to be displayed than right-clicking when no devices are selected.
- **Re-order columns**: Move columns around in device lists by dragging-and-dropping them in the header to where you want them.

Customizing Layouts for Device Lists

In addition to the **Default** layout which is always available (it cannot be deleted), you can create different layouts to apply to any **Device List**. At the top of each **Device List** is a **Layouts** field with a drop-down list from which you can select any custom layout or default layout or create a layout. The layouts can be:

- **Shared**: Any user can access them.
- **Private**: Cannot be accessed by other users.

Add custom device lists

1. In the toolbar, click **View** > **Column Layouts**. The **Column Layout Manager** page is displayed.
2. Click **New**. The **Column Layout Editor** page is displayed.
3. Type the name of the custom view in **Name**.
4. To specify the columns displayed on this page, select an option from the **Category** drop-down list.
5. Select the column to display on the device lists by highlighting it and clicking the arrow buttons between the two lists.

TIP: To select multiple columns, use either Ctrl+Click or Shift+Click. To move the order of the visible columns, use the up/down arrows.

6. If this view can be seen or used by other users, check the box for **Shared** (or public).
7. Click **OK**. The **Column Layout Manager** page is displayed. Click **Close**. The view you just edited is available to select on the device lists.

Edit custom device lists

1. In the toolbar, click **View** > **Column Layouts**. The **Column Layout Manager** page is displayed.

   Highlight the view to edit and then click **Edit**. The **Column Layout Editor** page is displayed.
2. To specify the columns displayed on this page, select an option from the **Category** drop-down list.
3. Select the column to display or remove from the device lists by highlighting it and clicking the arrow buttons between the two lists.

TIP: To select multiple columns, use either Ctrl+Click or Shift+Click. To move the order of the visible columns, use the up/down arrows.

4. If this view can be seen or used by other users, check the box for **Shared** (or public).

5. Click **OK**. The **Column Layout Manager** page is displayed. Click **Close**. The view you just added is now available to select on the device lists.

Filters and Device Lists

You can use filters to limit the content of any device list based on specific criteria. You can also apply filters to other features, such as automatic device groups.

Characteristics of filters are:

- Multiple layers of filtering can be created by using AND/OR operators.
- Filters can be stored and also shared with other users.
- Some built-in filters are available when HP Web Jetadmin is installed.
- Filters can be added as filtered lists in the left navigation pane.

Available actions for filters listed on the **Filters** menu (accessible from the toolbar) are:

- **Built-in**: Apply a built-in filter, such as **Color Devices** or **Error Devices**, to the displayed device list.
- **Shared**: Apply a filter that is designated as **Shared** in the Filter Editor.
- **Private**: Apply a filter that is not designated as **Shared** in the Filter Editor.
- **Clear**: Clear the filter from the selected devices in the device list.
- **New**: Use the Filter Editor to create a filter.
- **Edit**: Use the Filter Editor to edit a filter.
- **Save As**: Save a filter with another name.
- **Manage**: Use the Filter Manager to create, edit, and delete filters.

Built-in Filters

The following built-in filters are available from the **Filter** menu:

- **Color Devices**: Any devices with color capability.
- **Error Devices**: Any devices with a severity of "Error".
- **Information Devices**: Any devices with a severity of "Information".
- **New (Last Discovery)**: Any devices that were added to the **All Devices** list since last discovery.
- **Non-Unique Devices**: Any devices that do not have a unique serial number.
- **PC-Connected Devices**: Any devices that were discovered through PC-Connected device discoveries.
- **Ready Devices**: Any devices that are in a ready state.
- **Ungrouped Devices**: Any devices that are not a member of a group.
- **Warning Devices**: Any devices with a severity of "Warning".

Filter Manager and Filter Editor

The Filter Manager and Filter Editor features are used to create, edit, copy, and delete the device list filters.

HP Web Jetadmin supports Microsoft Global Input Method Editors (IMEs). An IME is a program that can be used to enter complex characters and symbols, such as Japanese characters, by using a standard keyboard. For more information, see the Microsoft technical documentation.

Building a Compound Filter

If you create a basic filter and do not get the results you need, you can create a compound filter. After you create a basic filter in the **Filter Editor**, you can select **Advanced** to view its layers. For example:

```
GT([IP Address], [192.168.40.0]) AND LT([IP Address], [192.168.47.255])
AND EQ([Device Name], [HP LaserJet 4100 MFP]) OR EQ([Device Model],
[HP Color LaserJet 4730 MFP])
```

The **Advanced** feature can be used to change the filter into two sub-filters that are compounded. Use the **AND** function and add some open and closed parentheses:

```
(GT([IP Address], [192.168.40.0]) AND LT([IP Address], [192.168.47.255]))
AND (EQ([Device Name], [HP LaserJet 4100 MFP]) OR EQ([Device Model],
[HP Color LaserJet 4730 MFP]))
```

TIP: For backward compatibility with previous releases, HP Web Jetadmin still supports alternate symbols, such as quotes (") and apostrophes ('), to enclose parameters for filter functions. HP Web Jetadmin automatically changes alternate symbols to brackets when you exit the **Advanced** editor.

After this compound filter is added to the **Specify filter criteria** page, the Basic feature can no longer be used (you will receive an error message).

Create Filters

1. Access a device list. In the toolbar, click **Filters**, and then click **Manage**. The **Filter Manager** page is displayed.
2. Click **New**. The **Filter Editor** page is displayed.
3. Type the name for this new filter in **Name**.
4. To make this filter visible to other users, select **Shared**. If the filter is not shared, it is only visible to the user who created it.
5. If the filter is shared, you can choose to have it display in the left navigation pane under the **All Devices** list by selecting **Available Under All Devices**.
6. If you select **Advanced**, a text field is displayed where you can manipulate filter attributes that are expressed in explicit text rather than through a graphical interface. An example of this content is show here: `Contains([Asset Number], [2]) AND Contains([Asset Number], [1], [Match Case])`

   An invalid string should be blocked from being applied to settings. An Insert feature is provided to place operators and functions into the advanced filter content. A Validate feature is provided to report problems with the advanced filter content if any exist.
7. If you select **Basic**, click **Add**. Now you can specify:

- **Category**: Specifies the columns that are displayed in the **Device Property** drop-down list.
- **Device Property**: Device and system attributes, which are the same as HP Web Jetadmin columns.
- **Not**: Check box that invokes “not” filtering. When an attribute matches the filter functions, the device will NOT be shown in the list.
- **Filter Function**: A set of standard operators that give flexibility to the device property definition. These operators will change depending on the **Device Property** selected.

  Once multiple selections are chosen and displayed in **Filter Function**, you can choose “AND” or “OR” (the default is “AND”).
- **Value**: Provides an entry point to define the **Filter Function** and **Device Property** value. This can either be a free text field or a pre-populated drop-down menu depending on the **Device Property** selected.
- **Options**: Contains features that further describe the content of free text. Examples are “Match Case” and “Ignore Case”. This feature is only active when free text fields are available.

8. When done, click **OK**. The **Filter Editor** is displayed with your selections.
9. When done, click **Close**. The device list is displayed.

Edit Filters

1. Access a device list. In the toolbar click **Filters** and then click **Manage**. The **Filter Manager** is displayed.
2. Select the filter you want to edit, and then click **Edit**. The **Filter Editor** page is displayed.
3. Make the changes to the existing filter.
4. When done, click **OK**. The **Filter Manager** page is displayed.
5. When done, click **Close**. The device list is displayed.

“Save As” Filters

1. Access a device list. In the toolbar click **Filters** and then select **Save As**. The **Save Filter As** is displayed.
2. Apply the filter you want to copy to the new filter.
3. In the toolbar, click **Filters**, and then select **Save As**. The **Save Filter As** page is displayed.
4. Specify the name of the new filter, and then click **OK**. You can now edit the filter definitions of the new filter.

Managing Filters

1. Access a device list. In the toolbar click **Filters** and then select **Manage**. The **Filter Manager** is displayed.
2. Select the filter and then click:
   - **New**: Create a filter.
   - **Edit**: Edit a filter.

- **Copy**: Copy an existing filter to create a new filter.
- **Remove**: Delete a filter.

3. Follow the steps for the action requested.

Apply Filters to Device Lists

1. Display the device list on which you want to apply the filter.
2. In the toolbar click **Filters** and then click one of the following:
   - **Built-in**: Apply a built-in filter, such as **Color Devices** or **Error Devices**, to the displayed device list.
   - **Shared**: (If there are shared filters); Lists any filter that has been designated as “shared” in the **Filter Editor**.
   - **Private**: Access all filters that are not shared (as specified in the **Filter Editor**).
3. Select the filter from the list. The device list will automatically display only those devices that match the criteria in the selected filter.
4. To view all devices again, click **Filters** and then select **Clear**.

Filtering On Special Column Types

Some device list columns show a summary value rather than the actual data stored on the device or in the HP Web Jetadmin database. This is because the actual data is too complex to be represented in a column cell. These columns are treated differently for the display and filter features. The display feature shows an indicator in the column cell. The filter feature can act on the actual underlying data. Examples of columns like these are the **Device Groups** column and the **SNMP Trap Destination Table** column.

Two examples of how these columns work and how filtering can be used are:

- The **Device Groups** column for a device belonging to just one group shows the actual name of that group. The **Device Groups** column for a device belonging to more than one device group shows the indicator value **<Multiple>**. The **Device Groups** column for a device belonging to no device groups will show the indicator value **<None>**.

  Filtering can be used to filter devices that belong to a particular device group by using the **Device Groups** filter property and the value of the device group name. An example taken from the **Advanced** edit mode of HP Web Jetadmin filtering is shown here:

  ```
  Contains([Device Groups], [Test])
  ```

- The **SNMP Trap Destination Table** column always uses the summary rather than the actual data from the device’s trap destination table. This is because the data on the device trap destination table is too complex to be displayed properly within a column cell. The summary used in the **SNMP Trap Destination Table** column cell is <*number1*> of <*number2*>, where *number1* is the actual number of entries in the trap destination table and *number2* is the maximum number of possible entries in the trap destination table.

  For example, a device having a potential for three trap destination table entries with only one of those being used will appear **1 of 3** in the **SNMP Trap Destination Table** column. Tooltip functionality (which is a text message resulting by hovering your mouse over the column cell) can be used to reveal the contents of a device trap destination table. For example, the following tooltip could appear when activated for a cell:

  ```
  2 of 3

  Slot, Trap Destination, Port, Version, Community
  ```

```
1,192.168.0.254,27892, v2c, wja

2,192.168.0.6,27892, v2c, wja
```

Further, HP Web Jetadmin filtering features can be utilized to find devices that do or don’t have specific trap table entries. For example, filtering can be used to see if a list of devices has a certain IP address present in any of their trap destination tables. Here is an example take from the **Advanced** edit mode of HP Web Jetadmin:

```
AnyItem([SNMP Trap Destination Table (obsolete).Trap Table Entries], [EQ(\
[Trap Table Entry.IP Address\], \[192.168.0.254\])])
```

Another example of using HP Web Jetadmin filter features on the **SNMP Trap Destination Table** uses regular expression. Taken from the **Advanced** edit mode of HP Web Jetadmin:

```
RegEx([SNMP Trap Destination Table (obsolete)], [(?<entries>[0-9]+) of
\k<entries>\r])
```

This example shows a filter that will filter the list to only devices with full trap destination tables.

Some complex columns do not support filtering on the individual subitems. For these columns, the filter compares the filter value to the export text for the item that represents the subitems as nested XML tags. For more information about filtering in complex columns, see the white papers that are available from the HP Web Jetadmin support page (click the flag icon on the bottom of the page, and then select your country/region).

Search Device Lists

You can use the Search feature to search all of the visible columns in a device list for devices that meet specific criteria. A Quick Search feature and a more complex Advanced Search feature are available. The first time that you search a device list, the search takes longer than subsequent searches.

Quick device list searches

The **Search Text** box is available on the toolbar that appears above device lists. The **Search Text** box provides a simple entry point for searching device lists.

1. In the **Search Text** box, enter the search criteria, and then press the Enter key. The first occurrence of the search criteria is highlighted.
2. To display the next occurrence, press F3.

   -or-

   To display the previous occurrence, press Shift+F3.

Advanced device list searches

The Advanced Search feature provides more flexible searches. For example, you can use regular expressions in the search criteria to specify a search pattern instead of exact text to match.

1. On the toolbar above the device list, click the **Advanced Search** (binoculars) icon. The **Advanced Search** window opens.
2. In the **Find what** box, enter the search criteria.
3. Click the **+** button next to the **Find options** option.
4. To find only occurrences of the search criteria that match the specified uppercase and lowercase exactly, select the **Match case** checkbox.

5. To select the next occurrence of the search criteria and retain the selection of any previously located occurrences, select the **Add to selection** checkbox.

   If this checkbox is cleared, the next matching entry is selected, but any previously selected entries are cleared.

6. To enable the use of regular expressions as part of the search criteria, select the **Use regular expression** checkbox.

   The content of the search string must follow the Microsoft .NET Framework standard for a regular expression pattern. For example, if you specify `gr(a|e)y` as the search criteria, the search finds occurrences of both *gray* and *grey* without having to perform two searches.

   TIP: For more information about regular expressions, go to the MSDN Library, and then search for *regular expressions*.

7. To continue the search at the beginning of the device list when it reaches the end of the device list, select the **Wrap at end of list** checkbox.

   -or-

   To stop the search when it reaches the end of the device list, clear the **Wrap at end of list** checkbox.

8. To search a specific column in the device list, select the column from the **Search column** list.

9. To find the first occurrence of the search criteria, click the **Find** button.

   -or-

   To find the next occurrence of the search criteria, click the **Find** button again.

   -or-

   To find and highlight all of the occurrences of the search criteria, click the **Find All** button.

Exporting Device Data

Data representing device attributes can be exported to a file and then stored on a disk or sent via email through SMTP. Export data is the same as column data. Many data elements exist within HP Web Jetadmin but the data that is actually available on devices will vary depending on model and device firmware revision.

You can also copy and paste data from Device Lists to any other application. Select one or more rows, click Ctrl-C or right-click on a device and then select **Copy**. When pasting this information, it is formatted the same way a device list export would be: the first row will be column headers and the subsequent rows will be the selected devices.

To export device data, perform the following steps:

1. Access any device list. Then right-click anywhere within the list and select **Export**. The **Export Devices** wizard is started with the **Select columns** page displayed.

2. Select the **Device Interaction Settings**:

   - **Threshold**: Specify the age or type of data that HP Web Jetadmin will get from the devices selected:

     - **Database only**: HP Web Jetadmin will always get data from the database.

     - **Missing items only**: HP Web Jetadmin will get data directly from the device if that data is not already in the database.

     - **From device only**: HP Web Jetadmin will always get data from the device.

    - **1 Hour**: HP Web Jetadmin will always get data that is one hour old or older.
    - **3 Hours**: HP Web Jetadmin will always get data that is three hours old or older.
    - **6 Hours**: HP Web Jetadmin will always get data that is six hours old or older.
    - **24 Hours**: HP Web Jetadmin will always get data that is 24 hours old or older.
  - **Do not prompt for credentials**: Select this if you want to export data from devices but you do not want to prompt for credentials from each device that is exporting data.

3. To specify the columns displayed on this page, select one of the following options from the **Category** drop-down list:
   - **Favorites**: Displays the most commonly used columns.
   - **All**: Displays all of the available columns, except obsolete columns. To display only a specific category of columns, expand **All**, and then select the category.
   - **Obsolete**: Displays columns that are still available in HP Web Jetadmin, but have been replaced by new columns or will not be supported in the future.
4. Select the column by highlighting it and clicking the arrow buttons between the two lists. To select multiple columns, use either Ctrl+Click or Shift+Click. To move the order of the visible columns, use the up/down arrow buttons.
5. To schedule the export for a later time, click **Schedule device list export**.

   A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

   NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.
6. Click **Next**. If devices were not selected prior to starting this wizard, the **Select devices** page is displayed. If devices were selected, skip the next step.
7. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.
8. Click **Next**. The **Specify destination settings** page is displayed. You can configure the filename of the exported file, the destination, and the file format.
9. Specify the destination:
   - **Local file**: Select this to save the export to a local file. You will be prompted for a filename and location after the export has begun.
   - **Email**: Send the data to an email address. Type the email address on this page or browse for the correct email address.
   - **Server file**: The server filename and path are specific to the HP Web Jetadmin host installation. The provided path describes where the file will be located after the export has completed. If a file of the same name exists in the location, the filename of the export file will have a time stamp appended to it to make it unique. If you want to replace the default filename, type the new name in the input box.
   - **Database**: Select this to save to a database view. Provide the view name and language for header information. The export will create a view located under **Views** in the HP Web Jetadmin database. The

view can be accessed with any SQL Server tool or reporting tool. (This option is only available after a license is purchased and installed.)

10. Select the file format (CSV or XML).

11. Click **Next**; the **Confirm** page is displayed.

12. Click **Start Export**. The **Results** page is displayed listing the status of the export.

For complex columns, HP Web Jetadmin exports only the summary data displayed in the device list grid. To display the details, select each of the individual subitems you want to export. If an item contains a list of elements, the item typically has a subitem that represents the list. You can select the subitem to export the entire list. In this case, the output is an XML fragment that contains an item tag for each element in the list. If the individual items are also complex, the XML fragment includes *all* of the item details. You cannot select the level of detail exported for each item. Some complex items do not support the selection of individual subitems for export. In this case, the exported content is an XML fragment that includes all of the subitems rather than the summary displayed in the device list.

Related Application Options for Device Lists

The following configuration options exist for **Device Lists**:

- Manage Hidden Devices on page 63
- Manage Blocked Devices on page 64
- Configure the Background Polling Options on page 60
- Configure the Number of Days that Devices are Considered New on page 65
- Configure the General Options for Device Tabs on page 65

The column **IP Hostname** is dependent on Configure the DNS Settings on page 47 lookups, which are enabled by default. For security and performance reasons, you can turn them off (Columns for Device Lists on page 106).

Printing Device Lists

You can print any device list. You can select specific devices or print the entire list.

To print device lists, perform the following steps:

1. From the left navigation pane, access any device list.

2. You can either print the entire list or just selected devices:

   - To print the entire device list, you can choose to print the whole list or certain pages of it. Go to the next step.

   - To print specific devices on the list, highlight those devices and then go to the next step.

3. To preview the list as requested, click **File** > **Print** > **Preview** > **Device List**.

4. On the device list page, in the toolbar click **File** > **Print** > **Device List**. The **Print** page is displayed.

5. Select your printer and the page range (**All**, **Selection**, or **Pages** to identify certain page numbers).

6. Click **Print**. The selected list will print to the specified printer.

Deleting Devices from Device Lists

You can delete any device from a device list.

If you delete a device from a device list, HP Web Jetadmin removes the device from all of the maps and permanently deletes all of the map information about that device.

To delete devices from device lists, perform the following steps:

1. From the left navigation pane, access any device list.
2. Highlight the device or devices to delete and right-click to select **Delete**.
3. Select one of the following options:

Function	Removes devices from device lists	Removes historical and task data	Will be rediscovered the next time a discovery is performed
Hide	Yes	No	Yes
Delete	Yes	Yes	Yes
Delete and block	Yes	Yes	No. If you delete devices from the Blocked Devices list, HP Web Jetadmin discovers the devices again the next time a discovery runs.

4. Click **OK**.

Refreshing Devices

From any device list, you can refresh devices or the display of a device.

Refresh Selection: This device list feature is available for either single or multiple devices. Right-click your selection or use F5 to activate this feature. When **Refresh Selection** is activated, HP Web Jetadmin client will request all device data the client is currently tracking for those devices directly from the devices even if the data within the database is not expired. There may be a short delay in the data change on your device list depending on number of devices in the selection. After **Refresh Selection** is finished, all of the data within your device list should appear very close to data that actually exists on the devices that were selected when the feature was activated. Data on devices, such as page counts, can change quickly so there is really never a guarantee that data is absolutely accurate. After the refresh is finished, normal polling and data threshold behavior will continue.

Refresh Selection (Full): This device list feature is only available on a single device selection. Right-click your selection and choose **Refresh Selection (Full)** to activate this feature. When **Refresh Selection (Full)** is activated, HP Web Jetadmin effectively clears all device based data and then re-retrieves those data elements important to Discovery. If the device is the same device, all data elements used to identify the device are kept the same and the device uniqueness attributes that are internal to this copy of HP Web Jetadmin are also kept the same. After this discovery action has finished (for either a changed or existing device) the same refresh action is performed as the **Refresh Selection** feature. In other words, all of the device data that the client is currently tracking for those devices which be requested directly from the devices because the data has been invalidated in the HP Web Jetadmin database tables. If the device is not the same (it does not have the same uniqueness identifiers) HP Web Jetadmin will do exactly what occurs during a new device discovery; HP Web Jetadmin will register a new unique device into device data tables. The old device will remain as well, but the new device will be activated, leaving the old device in **Communication Error** state. The old device, should it be found on a new IP address, can be activated again once HP Web Jetadmin begins to communicate with it.

TIP: At this time, the **Refresh Selection (Full)** feature is restricted to a single device for performance reasons. To get the desired result, a full discovery should be done on your network or maybe only on a specific list of IP addresses using the **Specified addresses** discovery option.

Find More Devices

On the **All Devices** page (select **All Devices** from the left navigation menu) in the upper right corner is a **Start discovery** button. When you click that button, the **Device Discovery** wizard starts to walk you through the steps needed for a successful device discovery.

You will want to use this feature after you initially install HP Web Jetadmin and then afterwards to find additional devices. When you first install HP Web Jetadmin, no discovery has been run which means the **All Devices** list will be empty.

Add Credentials for Devices

Some devices use credentials, which must be entered into HP Web Jetadmin for a user to access that device. If the credentials entered by the user (when trying to access a device) do not match the credentials entered HP Web Jetadmin, the device denies access.

The **All Devices** list has a **Credentials Required** column that shows which devices need credentials. **Yes** in this column indicates that the corresponding device requires credentials; **No** indicates that it does not need credentials. If a device requires credentials, you must add them before users access that device. The **Needed Credentials** wizard will walk you through the steps to add credentials. The pages displayed by the wizard will vary based on the specific credentials required by the device or devices.

To add credentials for devices, perform the following steps:

1. In the **All Devices** list, highlight the device or devices requiring credentials (those with a **Yes** in the **Credentials Required** column).
2. Right-click and select **Update Credentials**.
3. Use the **Needed Credentials** wizard to enter the credential information for the device or devices. Depending upon the credentials required by the device or devices, one or more of the following pages will be displayed for you to complete:

   TIP: Throughout the **Needed Credentials** wizard there is a **Skip** button that can be used to **not** enter credentials for devices if, for example, you are unsure of the required value for the device.

   - **Enter SNMPv1 Get Community Name** page: Select the device for the credential, supply the Get Community Name (can be up to 256 characters), and click **Set**. Then click **Finish**, or click **Next** and follow instructions in the wizard.
   - **Enter SNMPv1 Set Community Name** page: Select the device for the credential, supply the Set Community Name (can be up to 256 characters), and click **Set**. Then click **Finish**, or click **Next** and follow instructions in the wizard.
   - **Enter EWS or Domain Password** page: Select the device for the password, type the username and password, and click **Set**. Then click **Finish**, or click **Next** and follow instructions in the wizard.
   - **Enter SNMPv3 Credential** page: Select the device for the password and type the username, the authenticated password, and the private password. Click **Set** and then click **Finish**.

   NOTE: Enter either the EWS credentials or the Domain credentials. Enter Domain credentials as: `FullyQualifiedDomainName\Username`

Resolve Communication Errors for Devices That Have a New IP Address

Devices can be in a communication error status for several reasons, such as the device is turned off or the IP address assigned to the device has changed. If devices are in a communication error status because the IP addresses assigned to the devices have changed, you can use the Resolve IP Addresses wizard to rediscover these devices and resolve the status.

The Resolve IP Addresses wizard retrieves a list of all the devices that are currently in a communication error status, regardless of the reason for the communication error. For each of these devices, the wizard retrieves the hostname assigned to the device, and then looks up the hostname in the Domain Name System (DNS) to determine if the corresponding IP address has changed. If a new IP address has been assigned to the device, the wizard adds that device to a list of devices to be rediscovered. The wizard then runs a Specified Addresses discovery using this list of devices to be rediscovered. If there are PC-connected devices and network-connected devices in a communication error status, the wizard runs a separate discovery for each group of devices.

If you know that the IP addresses assigned to some of the devices on the network have changed, you can run the Resolve IP Addresses wizard one time to resolve the status of those devices. If the IP addresses assigned to the devices on the network change frequently, you can create a schedule to run the wizard on a recurring basis, such as daily, weekly, or monthly.

To resolve devices that are in a communication error status, perform the following steps:

1. Go to **Tools** > **Resolve Device Communication Failures**. The **Resolve IP Addresses** wizard starts.
2. To run the discovery immediately, leave the **Schedule** checkbox cleared.

   -or-

   To create a schedule for the discovery, select the **Schedule** checkbox.

   A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.
3. Click the **Next** button. The **Specify credentials** page appears.
4. If credentials are required to discover the devices, select the **Specify credentials to use for this discovery** option, and then perform the following steps:

   a. If the devices on the network have an SNMPv1 Get Community Name other than public defined, select the **SNMPv1 Get Community Name** checkbox, and then enter the SNMPv1 Get Community Name in the box.

   b. If HP Web Jetadmin is configured to discover SNMPv3 devices, select the **SNMPv3 Credentials** checkbox, and then enter the user name, authentication password, and private password in the boxes.

   IMPORTANT: To enable HP Web Jetadmin to discover SNMPv3 devices, go to **Tools** > **Options** > **Device Management** > **Device Discovery** > **General**.

   c. If the devices are connected to the network through a PC, select the **WMI Credentials** checkbox, and then enter the administrator (local) credentials for the Windows host that HP Web Jetadmin queries during the discovery in the boxes.

   d. To use the global credentials, select the **Use global credentials** checkbox.

   TIP: To define the global credentials, go to **Tools** > **Options** > **Shared** > **Credentials**, and then select the appropriate option.

5. Click the **Next** button.

6. If you did not select the **Schedule** checkbox, the **Confirm** page appears. Perform the following steps:

   a. Click the **Start Resolving Devices** button.

   b. The **Results** page appears and shows the progress of the discovery. While the discovery is running, you can hide the **Resolve IP Addresses** wizard or cancel the discovery.

      This discovery is available in the **Devices – Scheduled Tasks** task module on the **Device Management** > **Overview** page. You can view the progress or stop the discovery from this task module.

   c. When the discovery is finished, the **Results** page indicates the status of the discovery and displays the number of devices that were found in a communication error status, the number of devices that were resolved, and the number of devices that were not resolved.

      If a device is in a communication error status, but the IP address assigned to the device has not changed or the Resolve IP Addresses wizard was unable to discover the new IP address found in the DNS, the wizard cannot resolve the status. The device remains in a communication error status.

   d. Click the **Done** button.

7. If you selected the **Schedule** checkbox, the **Specify schedule options** page appears. Perform the following steps:

   a. In the **Name** box, enter a name for this discovery schedule.

   b. In the **Start time** boxes, specify the date and time this discovery starts.

   c. In the **Recurrence** section, select the option that defines how often this discovery runs, and then specify the corresponding settings.

   d. Click the **Next** button.

   e. On the **Confirm** page, click the **Create Schedule** button.

   f. The **Results** page appears and displays the details about the discovery. Click the **Done** button.

   This discovery schedule is available in the **Devices – Scheduled Tasks** task module on the **Device Management** > **Overview** page. You can edit and delete the schedule from this task module.

Groups

Groups lets you separate devices into subsets (or device groups) so that you can easily manage them. You can add and delete groups, name and rename them, and add or remove devices from existing groups. Putting devices in groups lets you configure multiple devices at the same time.

You can organize groups in a hierarchy to make it easier to manage them. It might be best to mirror an existing structure you are using for groups of devices. For example, you can organize your groups by geography, by building and floor, or by functional area (accounting, marketing, and so forth). Groups can have the same name when they don’t exist within the same parent group.

Device groups can be either Manual, where you specify which devices belong to each group, or Automatic, where you define filter criteria and devices are automatically added to and removed from each group. You cannot manually change the membership of Automatic groups except by changing the filter criteria. You can have both manual and automatic groups at the same time. (See Manual versus Automatic Groups on page 122.)

Device groups can also be used to delegate device management responsibilities to specific users. A user can be granted device management permissions for devices only in specific groups.

You can do the following with **Groups**:

- Organize your devices into meaningful categories, for ease of management.
- Create a hierarchy of parent groups and subgroups.

  Subgrouping is where a group exists as a member or subgroup of a parent group. The top-level parent group in HP Web Jetadmin is simply “Groups.” This exists at the top-level node in the left navigation pane and can only contain other groups.
- Create Automatic groups, where membership is determined automatically according to defined filter criteria.
- Create Manual groups, where membership is determined manually.
- Create policies for automatically applying various types of operations on devices when they are added to and removed from a group.
- Schedule various operations to happen on a group, rather than specific devices.
- Apply security permissions for users, such that they can perform operations on some groups, but not others.
- Provide meaningful names up to 48 characters long.
- The same device can be included in more than one device group.

A few common examples of HP Web Jetadmin groups scenarios include:

- A geographic representation of your device fleet.
- Parent groups representing buildings within a campus could contain subgroups that represent floors or floor quadrants. This could ease finding devices within a campus setting.
- Parent groups reflecting how devices are dispersed among organizations.

Group Representation

In the **Device Management** navigation pane, group names are followed by a number enclosed with parentheses. This number is the number of devices in the group. For example, if the Finance group contains five devices and does not contain any subgroups, this group appears in the **Device Management** navigation pane as **Finance (5)**.

If a group contains subgroups, the parent group name is followed by a second number enclosed with parentheses. This number is the sum of the number of devices in the parent group and the number of devices in all the subgroups of the parent group. For example, the Building 1 group contains two devices and two subgroups. The 1st Floor subgroup contains 12 devices and does not contain any subgroups. The 2nd Floor subgroup contains 10 devices and does not contain any subgroups. In the **Device Management** navigation pane, these groups appear as **Building 1 (2)(24)**, **1st Floor (12)**, and **2nd Floor (10)**.

You can include the same device in multiple groups. If the same device is assigned to multiple subgroups of a parent group, that device is counted only once in the total number of devices for the parent group, and the total number of devices is followed by an asterisk (*). For example, if two devices are assigned to both the 1st Floor and 2nd Floor subgroups, the parent group appears in the **Device Management** navigation pane as **Building 1 (2) (22*)**.

Manual versus Automatic Groups

You can use groups to categorize devices based on common criteria. For example, you might use an IP addressing scheme to group devices based on the area where they are located. The ability to create manual device groups and the ability to use the Filter feature to create automatic device groups provide powerful tools for managing group membership.

In HP Web Jetadmin, groups can be set up with one of two different membership types:

- Manual group: Each device is assigned manually to the group and remains in the group until you remove it.
- Automatic group: Devices are automatically assigned based on specified filter criteria. You can create a variety of filters. For example, to understand how many color devices exist on a specific network, build the following filters. The first filter specifies the network. The second filter specifies the color capability.

Property	Function	Value
IP Address	Contains	15.5
Color	Equals	Yes

  You can also edit this filter in advanced mode using the HP Web Jetadmin filtering syntax. These strings can have functions and values added and modified to affect the outcome of the filtering action. Automatic group membership is updated when one or more of the following occur:

  – The Automatic Group has had a filter (or filter change) applied.

  – New devices enter the system running a device discovery.

  – Device changes are realized by the system that either match or don’t match the filter criteria.

  – Devices are removed from the system by hiding or deleting them from the **All Devices** list.

Group Policies

Policies are applied to groups for the purpose of applying a settings action (or actions) onto a device when it becomes a member of the group or when it is removed from a group.

Many combinations of policy settings can be applied to a group. Multiples of the same policy types can be applied to groups as well. A short definition for each policy type follows:

- **Enable data collection policy**: If you have already defined a reports data collection template, this policy will automatically apply that template to devices when they are added to the group, when they are removed from the group, or both.
- **Subscribe to alerts or unsubscribe to alerts policy**: If you have already defined an alert subscription template, this policy will automatically apply that template to devices when they are added to the group, when they are removed from the group, or both.
- **Configure devices policy**: If you have already defined a device configuration template, this policy will automatically apply that template to devices when they are added to the group, when they are removed from the group, or both.
- **Add or remove devices to supply group policy**: If you have already defined a supply group, this policy will automatically add devices to that supply group when they are added to the group, when they are removed from the group, or both.

Example for Group Policies

Following is a simple example of applying a configuration template to a group:

- An administrator is named Pat.
- Pat has an HP Web Jetadmin group named “Pat’s Devices”.
- One policy setting on the group is a configuration template that sets the **System Contact** to “Pat” and the **Device Location** to “Building 3”.

Change the Order in which HP Web Jetadmin Applies Policies

You can specify the order in which HP Web Jetadmin applies policies to devices that are added or removed from a device group. When HP Web Jetadmin finishes applying one policy, it begins applying the next policy in the list.

If a device does not respond while HP Web Jetadmin is applying a policy, the policy execution task never completes. In this case, HP Web Jetadmin does not apply the remaining policies in the list to the device. To avoid this situation, HP Web Jetadmin provides a timeout setting with a default value of 450 minutes for each policy execution task. If a policy execution task does not complete within this default timeout period, HP Web Jetadmin begins executing the next policy in the list.

You can increase or decrease the timeout value, depending on the types of policies you define for device groups and the number of devices to which HP Web Jetadmin applies these policies during an execution phase. If you only define policies that do not take a long time to execute, such as installing solutions or fonts, or only add a few devices to a device group at one time, you can decrease the timeout value. If you define policies that take a long time to execute, such as firmware upgrades, or add a large number of devices to a device group at one time, you can increase the timeout value.

For example, assume that you define a firmware upgrade policy and a subscribe to alerts policy for a device group, and specify that the firmware upgrade policy is applied first and the subscribe to alerts policy is applied second. If you add 100 devices to this device group, HP Web Jetadmin begins executing the firmware upgrade task for all the devices. If HP Web Jetadmin does not finish upgrading the firmware on all 100 devices within 450 minutes, it continues executing the firmware upgrade task on the remaining devices and begins executing the subscribe to alerts task for all the devices. HP Web Jetadmin is now executing both policy tasks at the same time. In this case, it is possible for HP Web Jetadmin to execute the subscribe to alerts policy on a device before it executes the firmware upgrade policy on that device. To ensure that the policies are applied to devices in the order you specified, you can increase the timeout value to allow additional time for HP Web Jetadmin to complete the firmware upgrade task.

To change the default timeout value, perform the following steps:

1. Use Notepad or a similar editor to open the PolicyOrdering.config.xml file. This file is available in the following directory on the HP Web Jetadmin server:

   C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config

2. Find the following entry:

   ```
   <ipmc:configuration xmlns:ipmc="www.hp.com/schemas/imaging/ipmc/
   config/2004/02/24">
     <property name="PolicyExecutionTaskTimeout">
      <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
      </type>
      <value>450</value>
     </property>
   </ipmc:configuration>
   ```

3. Change the `<value>` parameter to the number of minutes that are appropriate for the types of policy execution tasks you define and the number of devices you add to a device group at one time.

Security Restriction Settings for Groups

You can use a restricted role to specify which device groups a user can access and which management tasks the user can perform for the devices in those device groups. For more information about using roles, see Roles on page 280. For more information about managing users, see Users on page 283.

When a restricted role is assigned to a user, the user can view all of the device groups that are available. The names of the device groups that the user can access based on the restricted role are highlighted in bold text. For the devices in these device groups, the user can perform only the management tasks that are specified for the restricted role.

For example, use the following steps to give User A permission to access only the devices that are in Group 1 and permission to refresh and delete the devices that are in Group 1:

1. Create a restricted role. On the **Specify permission settings** page of the **Create Role** wizard, select **Device Groups** from the **Restriction type** list, and select the **Manage Devices** check box.

2. Assign the restricted role to User A. On the **Specify role settings** page of the **Assign User Role** wizard, add Group 1 to the **Restrict permissions by group** list.

When User A displays a list of all the available device groups, only Group 1 is highlighted in bold text. User A can access, refresh, and delete the devices that are in Group 1. If User A tries to delete a device in any other device group, HP Web Jetadmin displays an error message.

Groups - Common Tasks Task Module

The **Groups - Common Tasks** task module provides links that initiate the following tasks for device groups:

- Create a device group
- Add devices to a device group
- Remove devices from a device group
- Edit the settings for a device group
- Delete a device group
- Edit the policies for a device group

- Import device groups
- Export device groups

Groups – Summary Task Module

The **Groups – Summary** task module provides the following information about the device groups:

- The number of device groups that include devices that have an **Error** or **Warning** status
- The number of device groups that have been created
- The number of devices that are assigned to device groups
- The number of devices that are not assigned to device groups
- The number of discovered devices

Groups – Management Task Module

The **Groups – Management** task module provides a list of the device groups that have been created. Use this task module to perform the following tasks:

- Create a device group
- Edit the properties of a device group, including the group name
- Add devices to a device group
- Remove devices from a device group
- Delete a device group
- Display a list of the devices in a device group

Create a New Device Group

A device group is set of devices on your network. After you create a group, you can manipulate all of the devices in that group. You can set up device groups so that device membership is either determined manually by you (**Manual group**) or automatically based on criteria you specify (**Automatic group**).

Naming groups with meaningful descriptions makes it easier to find a specific device group in a list. For example, instead of assigning `Payroll` and `Receivables` as device group names, you could assign `Accounts Payroll` and `Accounts Receivables`. These two device groups would then appear together in a sorted list.

The **Manual group** feature allows you to add discovered devices to a device group, thereby giving you complete control over the group membership. This method can be cumbersome if you have a lot of devices, and membership may need to be reevaluated manually when new devices are discovered or added to the network. However, this method may be required in certain grouping strategies, where the criteria cannot be evaluated automatically (such as “Marketing,” “Payroll”, and “Sales” devices).

The **Automatic group** feature allows HP Web Jetadmin to automatically add newly discovered devices to a device group if the devices meet specific criteria. Specify the filters that HP Web Jetadmin uses to determine if a new device should be added to a device group. You can specify multiple filters for the device group. You can also use the filters to remove devices from a device group when filter criteria does not apply to a device. Automatic group membership is determined by filter settings; devices cannot be added to or removed from these groups manually.

Use the following steps to create a device group:

1. In the **Device Management** navigation pane, right-click **Groups**, and then select **New group**. The **Create Group** wizard starts.
2. On the **Specify group options** page, specify the following settings:
   - **Group name**: The following are characteristics of the group name:
     - Can be up to 48 characters.
     - Can have alphabetic characters.
     - Can have numeric characters.
     - Can have special characters, such as an apostrophe (‘) or hyphen (-).
     - Can have Unicode characters.
     - Cannot contain a forward slash or a backward slash.
     - Can have the same name as another group if the two groups with identical names are in different parent groups.
     - Naming is flexible and can be changed on existing groups.
   - **Parent group**: Click the **...** button, and then select the parent group. The following are characteristics of parent groups:
     - Can contain a subgroup that has the same name as another subgroup in a different parent group.
     - No known limits exist for the depth of parent groups and subgroups or the number of groups.

   IMPORTANT: All primary device group criteria applies to subgroups.

   - **Group membership type**: Determines how devices will be added to the group. Select:
     - **Manual group**: Each device is added to the group manually.
     - **Automatic group**: Devices are added to the group automatically depending upon the filters set for the group.
3. To set the properties for the group, select the **Configure group properties now** checkbox.
4. Click **Next**.
5. If you are creating a manual group and did not select the **Configure group properties now** checkbox, continue with step 9.

   -or-

   If you are creating a manual group or an automatic group and selected the **Configure group properties now** checkbox, continue with step 6.
6. To create a manual group, perform the following steps:

   a. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

b. Click **Next**.

To create an automatic group, perform the following steps:

a. On the **Specify filter criteria** page, define the criteria that determines which devices are automatically added to this group by using the **Basic** or **Advanced** editing option.

   Select the **Basic** option, and then click **Add**. On the **Function** page, specify the following settings, and then click **OK**:

   - **Device Property**: Select the property from the drop-down list.
   - **Not**: Check this if the devices should **not** match the filter criteria. Otherwise, devices matching the filter criteria will be assigned to this group.
   - **Filter Function**: Select the way in which the devices should match the filter criteria from the drop-down box (contains, ends with, equals, and so forth).
   - **Value**: Type the value for the filter criteria.
   - **Options**: Choose to ignore the case to determine a match or to match the case.
   - **Category**: Select **Favorites** (most commonly used filters), **All** (all the available filters, except obsolete filters), or **Obsolete** (filters that are still available, but have been replaced by new filters or will not be supported in the future).

   Select the **Advanced** option, and then define the filters as follows:

   i. Type your own formula using the **Insert** button to insert various expressions.

   ii. When you have finished, click **Validate** to ensure the formula for the filter is valid.

b. Click **Next**.

7. On the **Specify group properties** page, enter the description and contact information, and then click **Next**.

8. On the **Configure group policies** page, perform the following steps:

   NOTE: The **Policy** column lists policies based on the user's permissions. This list is blank if there are no user permissions configured (User Security on page 278).

   a. To add a policy to the device group, click **Add**. On the **Add Policy** page, select the appropriate options from the **Policy**, **Trigger**, and **Policy action** lists, and then click **Add**. When you are finished adding policies, click **Close**.

   b. To delete a policy from the device group, select the policy in the **Policies for devices added to group** or **Policies for devices removed from group** section, and then click **Remove**.

   c. To specify the order in which the policies are applied to devices in the device group, select the policy in the **Policies for devices added to group** or **Policies for devices removed from group** section, and then click the up or down arrow.

   d. When you are finished configuring the group policies, click **Next**.

9. On the **Confirm** page, verify that the information is correct, and then click **Create Group**.

10. On the **Results** page, select the **View group** checkbox if you want to open the group, and then click **Done**.

Building a Compound Filter (Groups)

If you have created a basic filter and are not getting the results you need, you can create a compound filter. Once you create a basic filter in the **Filter Editor**, you can click **Advanced** to view its layers. For example:

```
GT([IP Address], [192.168.40.0]) AND LT([IP Address], [192.168.47.255])
AND EQ([Device Name], [HP LaserJet 4100 MFP]) OR EQ(]Device Model],
[HP Color LaserJet 4730 MFP])
```

The **Advanced** feature can be used to change the filter into two sub-filters that are compounded. Use the **AND** function and add some open and closed parentheses:

```
(GT([IP Address], [192.168.40.0]) AND LT([IP Address], [192.168.47.255]))
AND (EQ(]Device Name], [HP LaserJet 4100 MFP]) OR EQ(]Device Model],
[HP Color LaserJet 4730 MFP]))
```

NOTE: For backward compatibility with previous releases, HP Web Jetadmin still supports alternate symbols, such as quotes (") and apostrophes ('), to enclose parameters for filter functions. HP Web Jetadmin automatically changes alternate symbols to brackets when you exit the **Advanced** editor.

After this compound filter is added to the **Specify filter criteria** page, the Basic feature can no longer be used (you will receive an error message).

Moving a Device Group

After a device group is created, you can move it to a different level within **Groups**. To move a device group, expand **Groups** in the left navigation menu; click on the group to move and drag it to the group that should be its parent. The **Move Group** wizard is displayed. Click **Move Group** and then click **Done**.

Add Devices to a Group

Managing a group of devices can be easier than managing individual devices. Adding devices to a group lets you manage all of the devices in that group at the same time. Removing devices from a group means to delete them from the group, but they will remain in the **All Devices** list. You can only add devices to a group that has been identified as a manual group; devices are automatically added to any group identified as an automatic group based on filter criteria (Manual versus Automatic Groups on page 122).

To add devices to groups, perform the following steps:

1. Select **Groups** in the left navigation pane. The **Groups** page is displayed.

   On the **Groups** page, click **Add devices to group**. The **Add Devices** wizard is started with the **Select group** page displayed.

2. Select the group to add devices to and click **Next**.

3. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

4. Click **Next**. A **Confirm** page is displayed.

   If changes need to be made, click **Back** and make corrections.

   If no changes need to be made, click **Add Devices**. The **Results** page is displayed. Click **Done** to display the **Groups** page.

Remove Devices from a Manual Group

You can delete any device from a device group that has been identified as a manual group (Manual versus Automatic Groups on page 122).

To remove devices from manual groups, perform the following steps:

1. Select **Groups** in the left navigation pane. The **Groups** page is displayed.

   On the **Groups** page, click **Remove devices from group**. The **Remove Devices** wizard is started with the **Select group** page displayed.

2. Select the manual group to remove devices from and click **Next**.

3. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

4. Click **Next**. A **Confirm** page is displayed.

   If changes need to be made, click **Back** and make corrections.

   If no changes need to be made, click **Remove Devices**. The **Results** page is displayed. Click **Done** to display the **Groups** page.

Edit a Device Group

After a device group has been created, you can change its name, the devices in the group, how the devices are assigned to that group (manually or automatically), or any of its properties.

To edit device groups, perform the following steps:

1. In the **Device Management** navigation pane, right-click **Groups**, and then select **Edit group**. The **Edit Group** wizard starts.

2. On the **Select group** page, click the **...** button, select the group, and then click **Next**.

3. On the **Specify group options** page, enter the new group name and parent group name. Select the **Manual group** or **Automatic group** option.

   NOTE: When you change a device group from Manual to Automatic, devices that meet the filter criteria for the automatic group will replace any devices that had been in the group when it was a manual group. Changing a device group from Automatic to Manual will not cause the device membership to change; the devices present in the group will be retained and manual modifications can be performed on those devices.

   If you rename the group, the group name must conform to the following specifications:

   - Must have a unique name within its parent group.
   - Can be up to 48 characters.
   - Can have alphabetic characters.
   - Can have numeric characters.
   - Can have special characters, such as an apostrophe (‘) or hyphen (-).

- Can have Unicode characters.
- Cannot contain a forward slash or a backward slash.

4. Click **Next**.

5. If you selected the **Manual group** option, perform the following steps:

   a. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

   b. Click **Next**.

   If you selected the **Automatic group** option, perform the following steps:

   a. On the **Specify filter criteria** page, define the criteria that determines which devices are automatically added to this group by using the **Basic** or **Advanced** editing option.

      Select the **Basic** option, and then click **Add**. On the **Function** page, specify the following settings, and then click **OK**:

      - **Device Property**: Select the property from the drop-down list.
      - **Not**: Check this if the devices should **not** match the filter criteria. Otherwise, devices matching the filter criteria will be assigned to this group.
      - **Filter Function**: Select the way in which the devices should match the filter criteria from the drop-down box (contains, ends with, equals, and so forth).
      - **Value**: Type the value for the filter criteria.
      - **Options**: Choose to ignore the case to determine a match or to match the case.
      - **Category**: Select **Favorites** (most commonly used filters), **All** (all the available filters, except obsolete filters), or **Obsolete** (filters that are still available, but have been replaced by new filters or will not be supported in the future).

      Select the **Advanced** option, and then define the filters as follows:

      i. Type your own formula using the **Insert** button to insert various expressions.

      ii. When you have finished, click **Validate** to ensure the formula for the filter is valid.

   b. Click **Next**.

6. On the **Specify group properties** page, enter the description and contact information, and then click **Next**.

7. On the **Configure group policies** page, perform the following steps:

   a. To add a policy to the device group, click **Add**. On the **Add Policy** page, select the appropriate options from the **Policy**, **Trigger**, and **Policy action** lists, and then click **Add**. When you are finished adding policies, click **Close**.

   b. To delete a policy from the device group, select the policy in the **Policies for devices added to group** or **Policies for devices removed from group** section, and then click **Remove**.

   c. To specify the order in which the policies are applied to devices in the device group, select the policy in the **Policies for devices added to group** or **Policies for devices removed from group** section, and then click the up or down arrow.

   d. When you are finished configuring the group policies, click **Next**.

8. On the **Confirm** page, verify that the information is correct, and then click **Save Group**.

NOTE: Automatic group membership is determined by filter settings; devices cannot be added to or removed from these groups manually.

9. On the **Results** page, select the **View group** checkbox if you want to open the group, and then click **Done**.

Delete a Device Group

You can keep your groups current by removing those groups that are no longer needed.

If you delete a device group with a map, all map information associated with that group is permanently deleted from HP Web Jetadmin. For more information about maps, see Mapping on page 101.

To delete device groups, perform the following steps:

1. Select **Groups** in the left navigation pane. The **Groups** page is displayed.

   On the **Groups** page, click **Delete device group**. The **Delete Group** wizard is started with the **Select groups** page displayed.

2. Highlight the group or groups (must be at the same level) to delete.

   NOTE: Multiple groups, if at the same level, can be selected; use either Ctrl+Click or Shift+Click.

3. Click **Next**. A **Confirm** page is displayed.

   If changes need to be made, click **Back** and make corrections.

   If no changes need to be made, click **Delete**. The **Results** page is displayed. Click **Done** to display the **Groups** page.

Edit Device Group Policies

You can make changes to device group policies.

To edit device group policies, perform the following steps:

1. In the **Device Management** navigation pane, right-click **Groups**, and then select **Edit group policies**. The **Edit Group Policies** wizard starts.
2. On the **Select group** page, click the **...** button, select the group, and then click **Next**.
3. On the **Configure group policies** page, perform the following steps:
   a. To add a policy to the device group, click **Add**. On the **Add Policy** page, select the appropriate options from the **Policy**, **Trigger**, and **Policy action** lists, and then click **Add**. When you are finished adding policies, click **Close**.
   b. To delete a policy from the device group, select the policy in the **Policies for devices added to group** or **Policies for devices removed from group** section, and then click **Remove**.
   c. To specify the order in which the policies are applied to devices in the device group, select the policy in the **Policies for devices added to group** or **Policies for devices removed from group** section, and then click the up or down arrow.
   d. When you are finished configuring the group policies, click **Next**.
4. On the **Confirm** page, verify that the information is correct, and then click **Save Policies**.
5. On the **Results** page, click **Done**.

Import Device Groups

You can import device groups from an XML file. The format of the XML file must match the format of the file created by **Export Group**.

NOTE: Group Policies are not part of the Groups Import/Export feature set. These policy settings must be created manually on the target HP Web Jetadmin instance where after Groups import has been completed.

To import device groups, perform the following steps:

1. In the left navigation pane, right-click **Groups** and then click **Import**. The **Import Groups** wizard is started with the **Select options** page displayed.
2. Specify the file to import and then identify the parent group (if any) for his imported device group. The parent group must already exist on HP Web Jetadmin.
3. Click **Next**. The **Confirm** page is displayed listing any device groups you are importing.
4. Click **Import Group**. The **Results** page is displayed.
5. Click **Done**.

Export Device Groups

You can export device groups to an XML file.

To export device groups, perform the following steps:

1. In the left navigation pane, right-click **Groups** and then click **Export**. The **Export Groups** wizard is started with the **Select groups** page displayed.
2. Select the group by highlighting it and clicking the arrow buttons between the two lists. To select multiple groups, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons.

   If a group is being added whose parent group has already been added, you will be prompted for the desired location of this group.
3. Click **Next**. The **Confirm** page is displayed listing any device groups you are exporting.
4. Click **Export Group** and choose a location on the client machine and a filename.
5. Click **Save**. The **Results** page is displayed.
6. Click **Done**.

Rename a Device Group

You can change the name of a group to give it a more meaningful name.

To rename device groups, perform the following steps:

1. In the left navigation pane, expand the **Groups** node and right-click on the specific group to rename; select **Rename**.
2. Type the new name and click **Enter**. A group name:

- Must have a unique name within its parent group.
- Can be up to 48 characters.
- Can have alphabetic characters.
- Can have numeric characters.
- Can have special characters (such as “‘” or “-”).
- Can have Unicode characters.
- Cannot contain a forward slash or a backward slash.

View a Device Group

You can view device groups that have been created.

To view device groups, perform the following steps:

1. In the left navigation pane, expand **Groups**.
2. Select the group you want to view.

Search for Groups

You can use the Groups Search feature to quickly find a group that meets specific criteria. The Groups Search feature supports regular expressions.

NOTE: For more information about regular expressions, go to the MSDN Library, and then search for *regular expressions*.

To search for a group, perform the following steps:

1. In the **Device Management** navigation pane, right-click **Groups**, and then select **Search**. The **Groups Search** window appears.
2. In the **Name** box, enter the search criteria. You can use the following special characters in the search criteria:
   - `*`: Matches the preceding character zero or more times. For example, if you specify `zo*`, group names that contain *z*, *zo*, or *zoo* are considered a match.
   - `?`: Matches the preceding character zero or one time. For example, if you specify `a?ve?`, group names that contain *v* or *ve* are considered a match.

   You can use these special characters together to specify the following searches:

   - `*?`: Repeats the search criteria any number of times, but as few times as possible.
   - `??`: Repeats the search criteria zero or one time, but as few times as possible.

   All other characters are treated as normal characters.
3. Click the **Search** button. A list of all the groups that meet the search criteria appears.
4. Select the group that you want to display, and then click the **OK** button.

Discovery

Discovery features enable HP Web Jetadmin to find devices and then add them to the HP Web Jetadmin device lists. You might have information about the network that can be used in HP Web Jetadmin discovery settings, but some discovery features enable you to search for devices without networking details.

A powerful discovery engine exists within HP Web Jetadmin enabling you to locate most devices on both small and large networks. HP Web Jetadmin includes a new discovery for printers located in Active Directories (Active Directory Discovery on page 149). Scheduling and discovery templates allow you to tailor HP Web Jetadmin features to any topology or geographically deployed printer fleet. (See also Schedule Discoveries on page 163 and Create Discovery Templates on page 166.)

Discovery features in HP Web Jetadmin include:

- Active Directory Discovery on page 149.
- Import and Export Features of IP Range Files on page 145.
- IP Range calculator (Setting Realistic Ranges on page 143).
- View Discovery History on page 165.
- Discovery Templates (Create Discovery Templates on page 166).
- Manage Blocked Devices on page 64.
- Integrated PC-Connected device discovery (PC-Connected Device Discoveries on page 137).

Network devices can be automatically discovered on multiple subnets and then managed. The following types of discovery are currently supported:

- SLP Multicast Discovery on page 140: An SLP Multicast request is sent out on the network to evoke a response from devices connected to HP Jetdirect print servers.
- IP Broadcast Discovery on page 141: An SNMP Broadcast is sent to the specified Broadcast address. SNMP Devices respond.
- IP Range Discovery on page 142: Searches for devices within a range of IP addresses.
- Specified Device Address Discovery on page 147: You can add address lists of known devices to HP Web Jetadmin to query only specific end nodes.
- Active Directory Discovery on page 149: Queries Microsoft Active Directory using an Active Directory starting point such as domain, organization units (OUs), or other Active Directory containers.
- Domain Discovery on page 151: For PC-Connected devices, the domain is browsed to identify Windows hosts on the network.
- WS-Discovery on page 152: A Web Services request is sent out on the network to evoke a response from network-connected and PC-connected devices that support the Web Services protocol.
- Quick Device Discovery on page 139 is also available to discover devices when you add the hostname or IP address information to this feature anywhere in **Device Management**. Plus, HP Web Jetadmin can listen for SLP announcements that are propagated from HP Jetdirect-connected devices. This passive mechanism requires no additional settings and only generates network traffic when HP Web Jetadmin receives an SLP announcement.

In addition to gathering devices that are directly connected to the network, HP Web Jetadmin can find PC-Connected devices. These are devices that are connected through USB or parallel connectors to either desktops or servers on the network (Discovery Types and Methods on page 136).

When you initially install HP Web Jetadmin, you will be asked if you want to run a discovery immediately. You can request to discover devices at any time. By default, HP Web Jetadmin does not listen for SLP broadcasts; when passive SLP is enabled, some devices may be found by this type of discovery even if you do not initiate a discovery.

Discovering Devices with HP Web Jetadmin through Firewalls

Although firewalls provide a secure perimeter for business resources, they can also present a barrier to software products. HP Web Jetadmin provides the ability to discover and manage devices throughout a business network.

HP Web Jetadmin uses Multicast and SLP techniques to discover devices on your network. Using standard firewall configurations, multicasts are typically blocked because the communication port on which it relies is blocked. To facilitate a broadcast discovery such as Multicast and SLP, HP Web Jetadmin uses the well-known static port, UDP port number 427. To enable this discovery technique, the machine running HP Web Jetadmin must unblock the port used from within the firewall settings.

Discovery Types and Methods

HP Web Jetadmin performs the following types of discoveries:

- Network-connected device discoveries—HP Web Jetadmin finds a network node and then sends SNMP queries to discover the devices that are connected directly to that network node. After the SNMP query resolves a device, the device is displayed in the **All Devices** list. Resolved devices can include HP Jetdirect-connected devices, third-party devices, HP network scanners, HP network projectors, and so on. For more information, see Network-Connected Device Discoveries on page 136.
- PC-connected device discoveries—HP Web Jetadmin finds PCs and then discovers the devices that are connected to an LPT port or USB port on those PCs. HP SNMP Proxy Agent is a small software package that facilitates communication between HP Web Jetadmin and the PC-connected devices. If HP SNMP Proxy Agent is installed on the PC, HP Web Jetadmin gathers detailed information about the connected devices. If HP SNMP Proxy Agent is not installed on the PC, HP Web Jetadmin gathers only a minimal amount of device information about the connected devices. For more information, see PC-Connected Device Discoveries on page 137.

Most of the discovery methods are available for both network-connected discoveries and PC-connected discoveries. The following table identifies whether a discovery method can be selected for each discovery type.

Discovery method	Network-connected device discoveries	PC-connected device discoveries
Quick Device Discovery on page 139	Yes	No
SLP Multicast Discovery on page 140	Yes	No
IP Broadcast Discovery on page 141	Yes	Yes
IP Range Discovery on page 142	Yes	Yes
Specified Device Address Discovery on page 147	Yes	Yes
Active Directory Discovery on page 149	Yes	Yes
Domain Discovery on page 151	No	Yes
WS-Discovery on page 152	Yes	Yes

Network-Connected Device Discoveries

HP Web Jetadmin uses several methods to find devices that are connected directly to the network. Regardless of the method used, HP Web Jetadmin first finds nodes on the network. Then HP Web Jetadmin determines if the nodes are qualified printing or imaging devices by using the SNMP protocol to query the nodes for specific SNMP objects. HP Web Jetadmin adds the qualified devices to the database and displays them in the **All Devices** list.

In most cases, the IP addresses for devices are static. However, IP addresses can change in some situations, such as when the device is moved or DHCP is used to assign device addresses. In these cases, HP Web Jetadmin automatically changes a device's IP address in the database when it detects a change in that IP address.

PC-Connected Device Discoveries

HP Web Jetadmin can discover printers that are connected directly to PCs. A PC-connected device discovery queries the local PCs to find devices that are connected to an LPT port or USB port on the local PC. HP SNMP Proxy Agent is a small software package that facilitates the communication between HP Web Jetadmin and the PC-connected devices. If HP SNMP Proxy Agent is installed on a PC, HP Web Jetadmin gathers detailed information about the connected devices. If HP SNMP Proxy Agent is not installed on a PC, HP Web Jetadmin gathers only a minimal amount of device information about the connected devices.

When a PC-connected device discovery runs, HP Web Jetadmin communicates directly with the local PC in one of the following ways:

- HP SNMP Proxy Agent—HP Web Jetadmin looks for HP SNMP Proxy Agent on the PC. If HP SNMP Proxy Agent is installed, HP Web Jetadmin queries the device through the proxy agent in much the same way as it queries devices that are connected directly to the network. Many pieces of information about the devices are available, such as the status, page count, and supply levels.
- Windows Management Instrumentation (WMI)—WMI is a Microsoft service that runs on most Windows operating systems. Remote management applications use WMI to gather information. HP Web Jetadmin performs a query through WMI on the PCs that are found by using the various discovery methods. This query attempts to resolve Windows printer model details for devices that are plug-and-play compatible. The WMI PC-connected discovery solution does not gather the status or other details from the device. The WMI PC-connected discovery requires administrator (local) credentials on each host queried.

PC-connected device discoveries use different query protocols depending on the discovery method. The following table shows the primary and secondary protocols for each discovery method. If communication is possible by using the primary protocol, HP Web Jetadmin queries the devices. If communication is not possible by using the primary protocol, HP Web Jetadmin uses the secondary protocol to query the devices.

PC-connected device discovery method	Primary protocol	Secondary protocol
IP Broadcast	SNMP	WMI[1]
IP Range	SNMP	WMI
Specified Addresses	SNMP	WMI
Active Directory	SNMP	WMI
Domain	SNMP	WMI

[1] IP Broadcast discoveries send an SNMP query to a broadcast address. IP Broadcast discoveries find devices through WMI only if the PC is capable of responding to SNMP queries. The SNMP service must be enabled on the PC for it to respond to SNMP queries.

Discoveries that use the WMI protocol require administrative access to the PC that is being queried. The local administrator password can be used. However, in many environments a domain user is granted administrative privileges on the local Windows hosts. Administrative credentials are entered when the discovery is initiated by using the **Specify credentials to use for this discovery** option.

Network-connected and PC-connected devices are added to the **All Devices** list. To identify devices that are discovered by PC-connected device discoveries, add the **PC Connected** column to the device lists.

HP SNMP Proxy Agent

HP SNMP Proxy Agent is software that is installed on a desktop client PC. HP Web Jetadmin uses HP SNMP Proxy Agent to discover and manage locally connected (for example, USB-connected) HP printers and scanners. HP SNMP Proxy Agent exposes management objects through the Microsoft SNMP service on the client PC. A simple PC-connected device discovery in HP Web Jetadmin discovers the locally attached devices. HP Web Jetadmin then uses the proxy to gather additional information about the devices, such as remaining toner levels, page counts, and status. HP SNMP Proxy Agent is available from www.hp.com/go/webjetadmin. For more information about the requirements and important support details, see the *HP SNMP Proxy Agent Readme*. This Readme is available from the HP Web Jetadmin support page (in English).

Troubleshoot PC-connected Device Discoveries

Administrators can use the log files in HP Web Jetadmin to troubleshoot PC-connected device discoveries. The log files are useful when running Windows Management Instrumentation (WMI) or HP SNMP Proxy Agent discoveries. The log files do not capture details about network-connected device discoveries.

To enable logging, perform the following steps:

1. Use Notepad or a similar editor to open the DiscoveryManager.config.xml file. This file is available in the following directory:

   C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config

2. Find the following property:

   ```
   <property name="DiscoveryLogEnabled”>
     <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
     </type>
     <value>False</value>
   </property>
   ```

3. Change the `<value>` entry to `True`.

4. Find the following property:

   ```
   <property name="NumDiscoveryLogs">
     <type>HP.Imaging.Wjp.Sdk.Core.Framework.ConfigurationItemString
     </type>
     <value>2</value>
   </property>
   ```

   This property is useful when PC-connected device discoveries are performed over a long period of time. The default setting causes HP Web Jetadmin to overwrite a second log file for each new discovery.

5. To increase the number of log files that HP Web Jetadmin creates, change the `<value>` entry to the required number of log files.

6. Close and save the DiscoveryManager.config.xml file.

7. Restart the HP Web Jetadmin service (HPWJA Service). For instructions, see Restart the HP Web Jetadmin Service Manually on page 21.

⚠ CAUTION: Be careful when restarting the HP Web Jetadmin service. Conflicts with existing operations, such as firmware upgrades, alerts, and data collection, might occur.

Each time HP Web Jetadmin contacts an address to determine if a PC-connected device is present, HP Web Jetadmin adds an entry to the log files in the following directory:

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin\WjaService\config \FileStore\Discovery\Specified

The following are examples of log entries:

- `An SNMP error occurred when trying to contact remote server`

  An SNMP-related error occurred.

- `An SNMP Credentials error has occurred`

  SNMP credentials are required for the device.

- `An SNMP Timeout error has occurred`

  SNMP did not respond within the specified HP Web Jetadmin timeout settings. For more information about the SNMP timeout settings, see Configure the SNMP Settings on page 46.

- `The remote server machine does not exist or is unavailable`

  The remote host does not qualify as a PC-connected host.

- `A Timeout occurred trying to contact Remote Host`

  A timeout occurred while trying to start a WMI session with the host.

- `The Remote host could not be contacted`

  A WMI session could not be started.

- `Access is denied`

  The remote host denied access to a WMI session.

Quick Device Discovery

If you know the IP address or hostname of a network-connected device, you can use the Quick Device Discovery feature to find the device instead of running a full network discovery. To use the IP hostname for the Quick Device Discovery feature, DNS lookups must be enabled. For instructions on enabling DNS lookups, see Configure the DNS Settings on page 47.

You can only use the Quick Device Discovery feature to find PC-connected devices if the devices are already in the HP Web Jetadmin database. To find a PC-connected device that is not in the database, you must run a device discovery and use the **PC connected devices** option. For more information about PC-connected device discoveries, see PC-Connected Device Discoveries on page 137.

To find a network-connected device, the Quick Device Discovery feature searches the device addresses in the HP Web Jetadmin database. If the device address is in the database, HP Web Jetadmin highlights the device in the **All Devices** list. If the device address is not in the database, HP Web Jetadmin performs a network query only for network-connected devices. If the device address is found on the network, HP Web Jetadmin adds the device to the database and highlights the device in the **All Devices** list.

The Quick Device Discovery feature does not search the device lists. For instructions on searching the visible columns in device lists, see Search Device Lists on page 114.

To perform a Quick Device Discovery, perform the following steps:

1. In the **Device Management** navigation pane, enter the IP address or hostname for the device in the **Quick Device Discovery** box, and then click the **Go** button.
2. If the device is not found, perform the following steps:
   a. Click the **Credentials may be required to locate the device** link.
   b. On the **Enter Credentials** window, select the **Use** checkbox, enter the SNMPv1 Get Community Name for the device, and then click the **OK** button.
   c. If the device is found, continue with step 3.

      -or-

      If the device is not found, click the **Cancel** button, and then click the **OK** button on the **Quick Device Discovery** window. Verify that the device is connected to the network, verify the device address and credentials, and then repeat the Quick Device Discovery.
3. On the **Quick Device Discovery** window, click the **OK** button.

SLP Multicast Discovery

(For network device discoveries only.)

A discovery using SLP multicast requires minimal settings to launch. SLP (service location protocol) is used to cast a query onto the network for the purpose of finding HP Jetdirect devices. After initial device response, SNMP follow-up queries are performed to learn more about devices and add them to the **All Device** list in HP Web Jetadmin. This discovery mechanism finds HP Jetdirect devices on both local and remote subnets.

Characteristics of an SLP Multicast discovery for network devices include:

- Multicast packets are sent to the HP Jetdirect-specific multicast address: 224.0.1.60.
- Packets contain a router hop-counter (IP time to live attribute) that can be set from within HP Web Jetadmin (default 4 hops).
- Packets expire when router hop-counter reaches zero.
- The discovery mechanism is fast.
- The discovery presents low network traffic.
- HP Jetdirect firmware must be at least x.06.00 or greater.
- Only HP Jetdirect-connected printers will be discovered.

The reach of SLP multicast discovery will depend upon the:

- Setting for **Routers to cross (hops)** (a configuration option for Discovery; see Configure the General Settings for Device Discoveries on page 64).
- Configuration of the network routers; if the router is configured to pass multicast requests on to other sections of your network, then a discovery could potentially discover devices on your entire network.

The other option to control the reach of the discoveries is to configure the multicast request to span a certain number of routers (Configure the General Settings for Device Discoveries on page 64). Spanning routers will require the routers to be configured to allow multicast request to be forwarded.

The discovery could also be affected by the configuration of your local firewall (Discovering Devices with HP Web Jetadmin through Firewalls on page 136).

If the router is configured to pass multicast requests on to other sections of the network, and **Discovery** is configured to cross multiple routers, then a discovery could potentially discover devices across multiple subnets and perhaps your entire network.

Details About Running an SLP Multicast Discovery

(For network device discoveries only.)

If one of the discovery methods you choose is **SLP multicast** (while creating templates (Create Discovery Templates on page 166), editing templates (Edit Discovery Templates on page 168), or scheduling (Schedule Discoveries on page 163)), then the **Choose SLP multicast settings** page is displayed. On this page, select the number of routers to cross (or hops) for the discovery. Increasing the number of hops might increase the amount of time for the discovery to complete; plus, it generates more network traffic than a discovery with fewer routers to cross.

HP Web Jetadmin does not add devices that cannot be resolved and managed via SNMP, which might be due to insufficient credentials, to the device list. HP Web Jetadmin enforces device manageability through SNMP before adding devices to the device list.

IP Broadcast Discovery

IP Broadcast discoveries send SNMP query packets (in the form of IP broadcasts) to one or more IP network(s). These are used in both PC-Connected and network device discoveries.

IP Broadcast Discoveries for Network Devices

An IP Broadcast discovery enables you to find devices or HP Web Jetadmin installations when IP broadcast addressees are known. IP broadcast discoveries send SNMP query packets (in the form of IP broadcasts) to one or more IP network(s). One network-specific broadcast address exists for each IP subnet on an IP intranet. IP subnets are determined by the IP network number and the IP subnet mask. IP calculators, available free on the Internet, are a great way to determine IP broadcast addresses. An all 1s IP broadcast can also be used to query the entire intranet. Broadcasting is typically blocked by routers due to traffic spike concerns.

Characteristics of IP broadcast discoveries for network devices include:

- Sends SNMP queries over one or more IP broadcasts.
- Listens for replies and then qualifies network connected devices.
- Default broadcast is the Global Broadcast Address (255.255.255.255).
- Can use one or more known IP broadcast addresses with optional address descriptions.
- Limited checking is performed to determine if the broadcast address is valid.
- Fast and thorough, especially on a local segment.
- Most modern networks block broadcast traffic.

IP Broadcast Discoveries for PC-Connected Devices

IP broadcast discoveries for PC-Connected devices send an SNMP query to the IP broadcast address specified. An all 1s broadcast is the default. Systems with the SNMP Proxy Agent first answer with the operating system. HP Web Jetadmin follows up with queries to both host and to printer specific objects. IP Broadcast discovery does not attempt WMI queries when no SNMP proxy agent exists.

Characteristics of IP broadcast discoveries for PC-Connected devices include:

- Settings are the same as network device.
- SNMP queries are attempted on discovered nodes.
- If no SNMP Proxy Agent response, WMI queries are performed when credentials exist in settings.

NOTE: Legacy editions of Microsoft Windows Server that have HP SNMP Proxy Agent or HP WS Pro Proxy Agent do not always respond to IP broadcasts from the HP Web Jetadmin server. HP recommends that you use alternate discovery methods to find PC-connected devices on legacy editions of Microsoft Windows Server.

Details About Running an IP Broadcast Discovery

1. In the left navigation pane, click **Discovery** and then click **Discover devices on my network** (in the **Discovery - Current Tasks** task module). The **Device Discovery** wizard is started with the **Specify discovery options** page displayed.
2. Select **Specify settings** and then select **IP broadcast**. Click **Next**. The **Select IP broadcast address** page is displayed.
3. You can:
   - Select a broadcast address.
   - **Add**: Add a broadcast. Type the address in **Address** and type a description (if desired) in **Description**. Then click **Add**.
   - **Show favorites only**: View only the broadcast addresses you have added by clicking **Show favorites only** (at the bottom of the page).
   - **Remove**: Remove addresses from the list by highlighting the address and clicking **Remove**.
   - **Customize**: Add or remove addresses to favorites by clicking **Customize**. Then select an address and click **Add Favorite** or **Remove Favorite**. When done, click **OK** (Customizing IP Ranges for Discoveries on page 146).
4. Click **Next**.

IP Range Discovery

In contrast to running a broadcast discovery (where all devices or HP Web Jetadmin installations in the subnet are queried), you can choose to discover a specified IP range or a number of IP ranges. This reduces network traffic and eliminates the possibility of having unwanted devices. HP Web Jetadmin installations show up in the database. IP Range discovery searches for devices or HP Web Jetadmin installations within a range of IP addresses. This type of discovery is accurate and thorough but can be slow for large ranges.

IP Range Discovery is effective when the administrator has knowledge of IP segments. Administrators use IP Range Discovery settings to map IP segments or groups of IP segments into HP Web Jetadmin discovery. This method efficiently sweeps selected portions of the network or WAN. IP Range address pairs consist of beginning and ending IP addresses. IP Range discoveries first ping specific IP addresses as defined by range address pairs. If the device responds, HP Web Jetadmin follows with SNMP queries. Multiple ranges can be specified in IP Range discoveries. HP Web Jetadmin pings in bursts of 30 queries to the first set of addresses from the first range and then waits one second before sending the next burst of 30 queries.

Setting Realistic Ranges

Most networks are divided up into subnets, which can be used to describe a network IP addressing scheme and are sometimes referred to as IP maps. A subnet within a large network can be described with a network number and a subnet mask. This is an example of one subnet with an IP range of 15.5.188.1 through 15.5.191.254:

- Network number example: 15.5.188.0
- Subnet mask example: 255.255.252.0

There are 1,022 possible addresses on this subnet. It may take HP Web Jetadmin only about 10 minutes to discover devices on this network depending on the network, the number of devices on that network, and the host on which HP Web Jetadmin is installed.

NOTE: IP address calculators are an easy way to analyze IP networks. Many free versions of IP calculators exist and can be obtained on the Internet.

IP Range discovery can perform to expectations when the range data has been correctly developed. It is easy to configure ranges that are larger than needed and actually cause the discovery to take a long time and perhaps even yield little in the way of devices. For example, a class A range could easily be developed for the HP intranet but would literally take weeks to complete. On most large networks, the majority of the IP addresses won't answer the HP Web Jetadmin query and will cause timeouts to occur; these translate into very long discovery times.

If you specify an IP range that is very large, your network might crash if that IP range is for a class A or class B network (when the first two octets of the IP range are not the same). HP Web Jetadmin will display a warning message stating that a large range might cause a large amount of network traffic; you can choose to continue or change the range.

You can choose to specify a large subnet range using the larger subnet address feature (**Tools** > **Options** > **Shared** > **Discovery** > **Methods** > **IP Range** > **General**). Large networks are considered any network bigger than a Class B network, which has up to 65,000 nodes.

Setting Ranges Based on Subnets or Contiguous Subnets

Since large IP ranges can cause HP Web Jetadmin discovery to take long periods of time to complete, it can be useful to use subnet ranges rather than the entire network for a discovery. These subnets, when put together into one list, represent an IP map. This type of a map can be obtained from an IT or Network Infrastructure team. It is also a good idea to work with these teams to discuss plans for implementing HP Web Jetadmin discoveries.

NOTE: HP strongly recommends that you discuss HP Web Jetadmin discoveries with your information technology or network administration team.

Here is an example of IP range planning. Assume we have 27 subnets on our hypothetical network. All of these subnets use the same subnet mask of 255.255.255.0. Here are the network numbers that represent our 27 subnets:

15.0.1.0, 15.0.2.0, 15.0.3.0, 15.0.4.0, 15.0.5.0, 15.0.30.0, 15.0.31.0, 15.0.32.0, 15.0.33.0, 15.0.34.0, 15.0.35.0, 15.0.36.0, 15.0.37.0, 15.0.38.0, 15.0.39.0, 15.0.55.0, 15.0.64.0, 15.0.65.0, 15.0.66.0, 15.0.67.0, 15.0.68.0, 15.0.69.0, 15.0.70.0, 15.0.71.0, 15.0.72.0, 15.0.73.0, 15.0.74.0

From this information, we can formulate the following IP address ranges and import them into HP Web Jetadmin:

- 15.0.1.1-15.0.1.254
- 15.0.2.1-15.0.2.254
- 15.0.3.1-15.0.3.254
- 15.0.4.1-15.0.4.254
- 15.0.5.1-15.0.5.254
- 15.0.30.1-15.0.30.254
- 15.0.31.1-15.0.31.254
- 15.0.32.1-15.0.32.254
- 15.0.33.1-15.0.33.254
- 15.0.34.1-15.0.34.254
- 15.0.35.1-15.0.35.254
- 15.0.36.1-15.0.36.254
- 15.0.37.1-15.0.37.254
- 15.0.38.1-15.0.38.254
- 15.0.39.1-15.0.39.254
- 15.0.55.1-15.0.55.254
- 15.0.64.1-15.0.64.254
- 15.0.65.1-15.0.65.254
- 15.0.66.1-15.0.66.254
- 15.0.67.1-15.0.67.254
- 15.0.68.1-15.0.68.254
- 15.0.69.1-15.0.69.254
- 15.0.70.1-15.0.70.254
- 15.0.71.1-15.0.71.254
- 15.0.72.1-15.0.72.254
- 15.0.73.1-15.0.73.254
- 15.0.74.1-15.0.74.254

We can take the formulation one step further and simplify things. Some of the IP ranges are contiguous. These contiguously-addressed subnets are one after the other, in order, making it easy to combine them. The final result would look like this:

- 15.0.1.1-15.0.5.254
- 15.0.30.1-15.0.39.254
- 15.0.55.1-15.0.55.254
- 15.0.64.1-15.0.74.254

This has reduced the number of IP ranges from 27 to 4. We can build this into a form that is easily imported into HP Web Jetadmin and also reflects descriptions. Here is an example of data that can be imported via a text file:

- 15.0.1.1-15.0.5.254 = subnet range for western area
- 15.0.30.1-15.0.39.254 = subnet range for central area
- 15.0.55.1-15.0.55.254 = subnet range for branch office
- 15.0.64.1-15.0.74.254 = subnet range for eastern area

Consolidating ranges makes dealing with large quantities of data simpler but may not help when descriptions are needed for the purpose of cataloging ranges.

Import and Export Features of IP Range Files

IP range data can be developed in other tools and imported through text files. In fact, HP Web Jetadmin can export IP range data to text files. This makes it easier to deal with large numbers of IP ranges, manipulate complex data and archive data for use in multiple instances. Tile format for IP Range import and export file format can be broken down as follows:

- 1 range per line
- Each IP address is separated by a hyphen character (-)
- Comment or description strings can be appended to the IP range by using an equal character (=)

Here is an example of 1 IP range with a comment: xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx=descriptive text string (where xxx represents an octet in the IP address).

There is no known limit to the number of IP ranges manageable within HP Web Jetadmin software. IP ranges are also used by other features like PC-Connected printer discovery and HP Web Jetadmin Installations discovery. All IP ranges entered into HP Web Jetadmin can also be managed globally from within **Tools** > **Options** > **Shared** > **Discovery** > **Methods** > **IP Range** > **IP Ranges**.

IP Range Discoveries for Network Devices

IP Range discoveries for network devices or HP Web Jetadmin installations first send an SNMP query to all addresses within the range. When nodes are discovered, HP Web Jetadmin performs queries to determine qualified devices. These qualified devices, when found, are added to the device lists.

Characteristics of IP range discoveries for network devices or HP Web Jetadmin installations include:

- IP ranges are simply two addresses that represent range begin and end points.
- Multiple ranges can be specified in an IP Range discovery.
- IP range data can be manually added through the user interface.
- IP ranges can be imported to HP Web Jetadmin from text files.
- Multiple IP ranges can be added and with optional, descriptive tags.

- HP Web Jetadmin sends 1 query to each address represented by the range.
- HP Web Jetadmin pings the device ranges in bursts of 30.
- HP Web Jetadmin has features to calculate IP ranges based on:
  - Local client host
  - HP Web Jetadmin server host
  - Device
- HP Web Jetadmin IP Range discoveries have proven to be effective, accurate and thorough.
- HP Web Jetadmin IP Range discoveries can be very slow if not configured properly.
- HP Web Jetadmin IP Range discoveries can draw security attention due to their scanning action.

Customizing IP Ranges for Discoveries

To customize the IP ranges for discoveries, perform the following steps:

1. In the **Device Management** navigation pane, right-click **Discovery**, and then select **Discover devices**. The **Device Discovery** wizard starts.
2. On the **Specify discovery options** page, select the **IP Range** option, and then click **Next**.
3. On the **Select IP ranges** page, click **Customize**.
4. To add an address to the favorites list, select the address, and then click **Add Favorite**.
5. To delete an address from the favorites list, select the address, and then click **Remove Favorite**.
6. Click **OK**, and then continue with the **Device Discovery** wizard.

IP Range Discoveries for PC-Connected Devices

IP Range discoveries for PC-Connected devices first send an SNMP query to all addresses within the range. If SNMP communication is possible on a device, the discovery attempts to find a locally connected printer. If no SNMP communication is possible and if the user provided administrative credentials, the discovery will attempt to find a locally connected printer on the device.

Characteristics of IP range discoveries for PC-Connected devices include:

- IP Range scanning is same as network connected.
- Nodes representing hosts are detected.
- SNMP queries are attempted on discovered nodes.
- If no SNMP Proxy Agent response, WMI queries are performed when credentials exist in settings.

Details About Running an IP Range Discovery

The **Select IP ranges** page is displayed when you choose **IP range** as the discovery method while:

- Creating discovery templates (Create Discovery Templates on page 166)
- Editing discovery templates (Edit Discovery Templates on page 168)

- Scheduling a discovery (Schedule Discoveries on page 163)
- Running a Web Jetadmin discovery (Discover Remote Installations of HP Web Jetadmin on page 288)

On the **Select IP ranges** page, you can select the IP address ranges displayed or you can edit the ranges.

1. Choose the action to take:
   - Select an IP range.
   - **Add**: Add an IP range by clicking **Add**. Type the range in **First address** and **Last address**; then type a description (if desired) in **Description**. Click **Add**.

     To calculate a range, click **Calculate range**. The **Calculate IP Range** page is displayed:

     - **Subnet from my computer**: Automatically use IP address ranges currently found on the local subnet of your computer. You can add a description in **Description** if desired.
     - **Subnet from WJA server**: Automatically use IP address ranges currently found on the subnet of the HP Web Jetadmin server. You can add a description in **Description** if desired.
     - **Subnet from network address**: Type a known IP address and subnet mask. You can add a description in **Description** if desired.
   - **Edit**: Make changes to IP ranges by clicking **Edit**. Follow the steps in the bullet above for “Add”.
   - **Delete**: Remove addresses from the list by highlighting the address and clicking **Delete**.
   - **Import**: If desired, import a range list by clicking **Import** and then browse for the range list.
   - **Export**: If desired, export a range list by clicking **Export** and then browse for location you want to store the range list.
   - **Show favorites only**: View only the IP ranges you have added by clicking **Show favorites only** (at the bottom of the page).
   - **Customize**: Add or remove addresses to favorites by clicking **Customize**. Then select an address and click **Add Favorite** or **Remove Favorite**. When done, click **OK**.
2. Click **OK**.

Specified Device Address Discovery

Sometimes there is enough information about your device fleet that enables building a base of device addresses. These addresses can be added to HP Web Jetadmin through the **Specified Address** option (see Manage the Address Lists for Specified Address Discoveries on page 49).

Specified Device Address discoveries use an explicit list of device addresses. These addresses can be IP hostnames or IP addresses. IP hostnames can have fully qualified domain information appended. Address information can be both imported from and exported to text files. Specified Device Address discovery works similarly to IP Range discovery; HP Web Jetadmin simply moves down a list of addresses, performing queries and adding qualified devices to the all devices list.

Here is an example of a small specified address base:

- 15.5.2.1
- 15.5.62.4
- 15.5.8.3
- 15.5.8.7

- BP005a.yourco.com
- BP065
- BP076.yourco.com

NOTE: For PC-Connected device discoveries, HP Web Jetadmin follows SNMP queries with WMI queries when no SNMP Proxy Agent has been detected on the remote host.

Specified Device Address Discoveries for Network Devices

Network device discovery queries each address in the list specified. Devices qualified through these queries are added to the **All Devices** list.

Characteristics of Specified Device Address discoveries for network devices include:

- Specified device address discoveries find devices based on user supplied addresses.
- IP address or hostnames are valid address forms.
- HP Web Jetadmin initially qualifies the device by using an SNMP query.
- Follow-up queries through SNMP qualify the device and place it into the **All Devices** list if appropriate.
- This discovery is very fast and only hits the addresses specified by the user.
- This discovery is only as accurate as the address base specified by the user.
- Addresses can be entered into HP Web Jetadmin one by one or they can be imported from text file.
- In HP Web Jetadmin, addresses can be exported to text file.

Specified Device Address Discoveries for PC-Connected Devices

Specified Address discoveries for PC-Connected devices first send an SNMP query to all addresses within the list of addresses. If SNMP communication is possible on a device, the discovery attempts to find a locally connected printer. If no SNMP communication is possible and if the user provided administrative credentials, the discovery will attempt to find a locally connected printer on the device using WMI protocol.

Characteristics of Specified Device Address discoveries for PC-Connected devices include:

- Specified address scan is the same as network connected.
- Nodes representing hosts are detected.
- SNMP queries are attempted on discovered nodes.
- If no SNMP Proxy Agent response, WMI queries are performed when credentials exist in settings.

Details About Running a Specified Device Addresses Discovery

If one of the discovery methods you choose is **Specified address** (while creating templates (Create Discovery Templates on page 166), editing templates (Edit Discovery Templates on page 168), or scheduling (Schedule Discoveries on page 163)), then the **Select addresses** page is displayed. On this page, you can select the IP address ranges displayed or you can edit the addresses:

1. In the left navigation pane, click **Discovery** and then click **Discover devices on my network** (in the **Discovery - Current Tasks** task module). The **Device Discovery** wizard is started with the **Specify discovery options** page displayed.
2. Select **Specify settings** and then select **Specified addresses**. Click **Next**. The **Select addresses** page is displayed.
3. Click **Edit Addresses**. The **Specified Addresses** page is displayed.
4. Type the network address in **Network address** and click **Add Address**; the address is displayed below in the box. Repeat this until you have entered all network addresses.
5. Check **Show For Me** next to each IP address you want to include on the **Select IP ranges** page (the previous page).
6. If desired, remove any ranges by highlighting it and clicking **Remove Address**.
7. If desired, import a range list by clicking **Import Addresses** and then browse for the range list.
8. If desired, export a range list by clicking **Export Addresses** and then browse for location you want to store the range list.
9. Click **OK** and then click **Next**. The **Confirm** page is displayed.
10. Click **Start**. The **Results** page is displayed. Click **Done**.

Active Directory Discovery

Active Directory Discovery requires your knowledge about the Active Directory domain. HP Web Jetadmin provides a new discovery feature that queries Microsoft Active Directory using an Active Directory starting point such as domain, organization unit (OU), or other Active Directory containers. In the case of network devices, HP Web Jetadmin scans the Active Directory for published shared printers. In the case of PC-Connected device discovery, HP Web Jetadmin scans the active directory for Windows hosts. From these initially discovered lists of nodes, HP Web Jetadmin finds and qualifies devices and then adds them to the **All Devices** list.

Active Directory Discoveries for Network Devices

Active Directory (AD) discovery requires your knowledge about the AD domain. Once the AD discovery is started, the LDAP protocol is used to query AD for published print shares. From print shares discovered, the **Port Name** field is checked for the default name forms which are all case-sensitive and include:

- `IP_<ip-addr>`
- `mt:<ip-addr>`
- `***ip_<ip-addr>` (*** can be anything not containing "ip_")
- `ip_<ip-addr>:***` (colon between the IP address and ***)
- `ip_<ip-addr> ***` (space between the IP address and ***)
- `ip_<ip-addr>-***` (dash between the IP address and ***)
- `ip_<ip-addr>_***` (underscore between the IP address and ***)

If any of these are found during the Node Discovery, the address is stored. Then, during the Node Resolve, the IP addresses are queried through SNMP to detect network connected printers. When network connected devices are discovered, they are added to the HP Web Jetadmin **All Devices** list. No special user credentials are needed other than device based SNMP Get Community strings (normally not used). In fact, HP Web Jetadmin, running under the low privilege account, Network Service, takes the credentials of the user logged in through the HP Web Jetadmin client and uses these to query the Active Directory.

You can choose to perform recursive queries meaning any sub-units below the specified path will be searched. The administrator can also perform discovery on multiple Active Directory locations. And, the discovery can also be filtered on both location and description strings if these are published to the Active Directory.

Characteristics of Active Directory discoveries for network devices include:

- You can activate Active Directory discovery by specifying AD location(s).
- You can optionally set location and/or description filtering to narrow Active Directory discovery.
- You can optionally specify Active Directory recursion searching to one or all levels below the specified AD location or locations.
- Active Directory discovery scans the directory for printer shares.
- IP addresses that are resolved from printer shares are queried using SNMP.
- Printers that are qualified are populated into the HP Web Jetadmin **All Devices** list.
- Discovery is fast.
- Discovery does not require any special privileges and relies on public Active Directory search.
- Discovery is accurate to the extent that network printers are shared and published through Active Directory.
- Discovery relies on the fact that a default port name in the Active Directory share actually contains the printer’s IP address.

  Active Directory Discovery discovers published print queues in a network’s Active Directory. To find the IP address of the network device to which the print queue is attached, AD discovery parses the print queue’s port. An IP address can only be detected from those print queues with ports with the default format of IP_www.xxx.yyy.zzz.

Active Directory Discoveries for PC-Connected Devices

Active Directory discoveries for PC-Connected devices use the LDAP protocol to identify Windows hosts on the network. Each host identified is queried using the WMI protocol. Administrative credentials are required for this discovery. Once a connection is established through WMI, the host is queried for a locally connected printer.

Characteristics of Active Directory discoveries for PC-Connected devices include:

- Settings are identical to discoveries for network devices.
- Discoveries for PC-Connected devices scan Active Directory for Windows hosts.
- SNMP queries are attempted on discovered nodes.
- If no SNMP Proxy Agent response, WMI queries are performed when credentials exist in settings.
- Local administrator credentials are required to perform this discovery.

Details About Running an Active Directory Discovery

Start here if one of the discovery methods you choose is **Active Directory** (while creating templates (Create Discovery Templates on page 166), editing templates (Edit Discovery Templates on page 168), or scheduling

(Schedule Discoveries on page 163)), then the **Specify Active Directory options** page is displayed. On this page, you can define options for Active Directory discoveries:

1. Type the path for the Active Directory location or browse to it. Then click **Add**; it will be displayed in the list below.
2. Check next to any location you want included in the discovery.
3. If desired, remove any ranges by highlighting it and clicking **Remove**.
4. Select the recursion level:
   - **Current level**: discoveries check the container specified by the path and the contents of any containers in the path.
   - **All levels**: discoveries check the container specified by the path plus the contents of all containers and sub-containers in the path.
5. Specify the print queue filter to use in **Filter**.
6. Click **Next**.

Passive SLP Discovery

(For network device discoveries only.)

When HP Jetdirect-connected devices are power-cycled, they propagate SLP (service location protocol) multicast packets. When HP Web Jetadmin detects an HP Jetdirect SLP multicast (recognized by the source 124.0.1.60), it performs follow-up SNMP queries and adds the device to the **All Devices** list.

Characteristics of Passive SLP discoveries for network devices include:

- Passive SLP discovery is quiet; HP Web Jetadmin does not propagate traffic unless a previously undetected device announces itself.
- HP Web Jetadmin listens for UDP traffic on port 427.
- Devices, including new devices, are discovered as they are powered on.
- Router filtering may inhibit multicast packets.
- Can be disabled on HP Jetdirect print servers.
- Will only discover HP Jetdirect-connected print servers.

Domain Discovery

(For PC-Connected device discoveries only.)

For Domain discoveries for PC-Connected devices, the domain is browsed to identify Windows hosts on the network. Each host identified is queried using the SNMP or WMI protocol. Administrative credentials are required for WMI. For WMI, once a connection is established the host is queried for a locally connected printer.

Characteristics of domain discoveries for PC-Connected devices include:

- SNMP queries are attempted on discovered nodes.
- If no SNMP Proxy Agent response, WMI queries are performed when credentials exist in settings.

- Might be slow on large domains.
- Local administrator credentials are needed to perform this discovery.

Details About Running a Discovery Using Domains

Start here if one of the discovery methods you choose is **Domain** (while creating templates (Create Discovery Templates on page 166), editing templates (Edit Discovery Templates on page 168), or scheduling (Schedule Discoveries on page 163)), then the **Select domains** page is displayed. On this page, you can select the domains to include in the discoveries:

1. Type the domain in **Domain** or browse for the domain. Then click **Add**. The domain is displayed in the **Domain** box below.

   To remove any domains from the **Domain** box, highlight the domain and click **Remove**.

2. Click **Next**.

WS-Discovery

A discovery that uses the Web Services protocol requires minimal settings to launch. HP Web Jetadmin uses the Web Services protocol to query the network to find network-connected and PC-connected devices. After an initial device response, HP Web Jetadmin performs additional SNMP queries to learn more about the devices and add them to the **All Devices** list. This discovery mechanism finds devices on both local and remote subnets.

Characteristics of a Web Services discovery for network devices include the following:

- Packets contain a router hop-counter (IP time to live attribute) that can be set from within HP Web Jetadmin. The default is 4 hops.
- Packets expire when the router hop-counter reaches zero.
- The discovery mechanism is fast.
- The discovery presents low network traffic.

The reach of a Web Services discovery depends on the following:

- The setting for the **Routers to cross (hops)** configuration option for the discovery (see Configure the General Settings for Device Discoveries on page 64).
- The configuration of the network routers. If the router is configured to pass Web Services requests on to other sections of the network, then a discovery might discover devices on the entire network.

You can also control the reach of discoveries by configuring the Web Services request to span a certain number of routers (see Configure the General Settings for Device Discoveries on page 64). The routers must be configured to allow the Web Services request to be forwarded.

The discovery can also be affected by the configuration of the local firewall (see Discovering Devices with HP Web Jetadmin through Firewalls on page 136).

If the router is configured to pass Web Services requests on to other sections of the network and the discovery is configured to cross multiple routers, then the discovery might discover devices across multiple subnets and perhaps the entire network.

Details About Running a WS-Discovery

If you choose the WS-Discovery method while creating templates (see Create Discovery Templates on page 166), editing templates (see Edit Discovery Templates on page 168), or scheduling discoveries (see Schedule Discoveries on page 163), then the **Choose WS-Discovery settings** page is displayed. On this page, select the number of routers to cross (or hops) for the discovery. Increasing the number of hops might increase the amount of time for the discovery to complete. In addition, the discovery generates more network traffic than a discovery with fewer routers to cross.

Managing Third-Party Printers in HP Web Jetadmin

During device discoveries, HP Web Jetadmin uses SNMP queries to gather information from the device. If HP Web Jetadmin concludes that the device is a peripheral such as a printer, plotter, or multifunction device, it displays the device in the list of discovered devices. For HP Web Jetadmin to conclude that a device is a peripheral, the device must be able to answer a set of industry-standard questions.

A Management Information Base (MIB) is a set of objects that defines the types of SNMP queries that can be asked of a device. For example, the Standard Printer MIB (RFC 1759) is a generic set of objects to which most peripherals should be able to provide answers when queried. The Standard Printer MIB consists of objects that describe functionality and capabilities of the printer such as page counts and media types. Other common MIBs include MIB2 (RFC 1213) and the Host Resources MIB (RFC 1514). Device vendors also have a set of proprietary MIBs that contain information unique to their devices. HP Web Jetadmin must have knowledge of MIB objects in device plug-ins before it can send queries to devices using those MIB objects.

Devices must be able to answer queries defined in the common industry-standard MIBs for HP Web Jetadmin to discover the devices. Otherwise, there is not enough information about the device to warrant displaying it in the list of discovered devices. HP Web Jetadmin focuses on printer management, and it would be increasingly difficult to distinguish devices as printers unless they can answer a standard set of questions such as those defined in the Standard Printer MIB.

After HP Web Jetadmin discovers a device, the level of support that can be provided depends on the depth of queries defined in the respective device plug-ins.

Support

Support in HP Web Jetadmin can be quite extensive if the device can answer industry-standard queries. Quite a bit of HP Web Jetadmin functionality can be supported through standard queries such as basic status, configuration, alerts, reporting, and page counting. HP Web Jetadmin attempts to support the following functionality for third-party devices using standard queries for basic support.

Device Page — Status Tab

- **Device** and **Information** categories
  - Picture of a generic device, possibly vendor specific
  - **Device Model**, **IP Hostname**, **IP Address**, **System Contact**
- **Status** category
  - Basic status (online/offline, toner low, toner out, media low, media out, paper jam, cover open, service requested)
  - Front panel display
- **Supply levels** category

  - Input tray remaining levels
  - Supplies remaining levels

Device Page — Config tab

- **Device** category
  - **Contact Person**
  - **Control Panel Language**
  - **PJL Configuration**
  - **Company Name**
- **Network**
  - **System Name**
  - **Proxy Server**

Device Page — Alerts tab

- General alerts only, polling only of SNMP Alert table and status OIDs

Device Page — Troubleshoot tab

- **Reset Device** button
- **Embedded Web Server** button

Device Page — Supplies tab

- Input tray levels
- Supplies levels

Device Page — Capabilities

- Installed components such as input tray capacities, interpreter languages, duplexer, hard disk, total memory

Alerts

- Polling only, no traps
- Limited set of events
  - Service (online, offline, error, disconnected)
  - Supplies (paper out, toner low, toner out, other supplies low/out/replace)
  - Media Path (paper jam, cover open, output full)

Reports

- **Device Inventory**
- **Supply Utilization**

Columns

- **Serial Number**
- **Contact Person**
- **System Contact**

- System Location
- System Name
- System Up Time

Functionality Definitions

This section provides definitions for many of the supported features for third-party devices and the objects used for obtaining the information. The feature is supported if the device can answer the industry-standard query defined in these definitions.

- **Alerts**: Polling at a specified interval is used to provide alerts that support the following types of events based on status queries that match certain conditions or prtAlerts table objects. Standard status queries can typically determine the following types of alert conditions:

  - Cover Open
  - Offline
  - Paper Jam
  - Printer Error

  Certified devices can process traps for real-time alerts when events occur for most events under the General category. Polling of remaining supplies levels to provide Supplies alerts at desired thresholds is also available for certified devices.

- **Bitmap and Icon**: HP Web Jetadmin displays any predefined bitmaps and icons that were created in a device plug-in. Certified devices have a unique picture that matches the device, while basic support provides one generic picture per third-party vendor.

- **Capabilities**: Capabilities such as installed languages, trays, and accessories are displayed on the **Capabilities** tab as supported by the device using objects such as prtInterpreterDescription and prtInputDescription.

- **Configuration**: The following items are provided at a minimum for configuration, assuming that the device supports the following objects:

  - **System Contact** (sysContact)
  - **System Location** (sysLocation)
  - **Control Panel Language** (prtConsoleLocalization)
  - **Contact Person** (prtGeneralServicePerson)
  - **System Name** (sysName)

  Certified devices can provide extended configuration items using vendor-specific objects.

- **Control Panel Display**: The current message on the printer front panel is displayed using prtConsoleDisplayBufferText.

- **Description**: A description is displayed from the response to sysLocation.

- **Engine Cycle Count**: Engine Cycle Count is a value stored on the printer that represents a cumulative total of pages printed for the life of the printer. Engine Cycle Count is displayed if a printer supports prtMarkerLifeCount. Page counts for mono, color, simplex duplex, fax, copy, and scan are only obtainable via proprietary queries and require advanced support such as qualified or certified.

- **IP Hostname**: The IP hostname is displayed if the operating system can resolve an IP address to a hostname from a name server such as DNS or WINS using a GetHostByAddr call. System Name, which can be the hostname if the NIC registers it with a name server, is displayed if the device answers the sysName MIB2 object.
- **Model**: The printer model name is displayed according to the response to hrDeviceDescr.
- **Serial Number**: The serial number is a unique manufacturing identifier for the device. The serial number is a critical identifier item that HP Web Jetadmin uses to determine the uniqueness of a device along with other items such as the MAC address and IP address. Some functionality, such as Reports, is blocked in HP Web Jetadmin if the serial number cannot be obtained. Therefore, HP Web Jetadmin makes a strong effort to obtain the serial number from third-party devices. The most typical and widely supported object to extract for obtaining the serial number is prtGeneralSerialNumber.
- **Status**: Device status, which indicates the current state of the printer (for example, online or paper jam), is displayed based on responses to standard objects such as hrPrinterDetectedErrorState.
- **System Contact**: The system contact is displayed from the response to sysContact.
- **Storage**: The presence of storage media such as a hard disk, flash disk, RAM disk, and installed RAM can be detected using hrDiskStorage objects. Additional storage information is provided on the **Storage** tab for certified devices.
- **Remaining Input Tray Levels**: The approximate amount of paper remaining in a particular tray can be displayed by calculating a percentage based on responses to the Standard MIB objects prtInputCurrentLevel and prtInputMaxCapacity.
- **Remaining Toner Levels**: The approximate amount of toner or ink remaining in the cartridge cavity is determined by calculating a percentage based on prtMarkerSuppliesLevel and prtMarkerSuppliesMaxCapacity.
- **Reports**: Basic support includes only the **Device Inventory** report. Advanced support may include reports that make use of the various supported page count values, such as **Accessories Inventory** (capabilities), **Supply Utilization** (marker supply information), **Device Utilization** (page counters), and **Hourly Peak Usage** (hourly page counters).

Troubleshooting

Determining why a particular non-HP device supports the features that it does is usually a result of the device's ability to answer the queries HP Web Jetadmin sends. Certified devices have known objects written in their device plug-ins and those objects have already been tested, so issues rarely occur on those devices. However, for qualified devices and those requiring basic support, HP Web Jetadmin is dependent on the device to answer industry-standard queries. Some devices support more gauges than others. You cannot always assume that all devices from a particular vendor support the same features. For example, one Xerox model may support the control panel display, while another Xerox model does not. The following are common explanations for why particular items may not appear for devices.

Issue	Resolution
A gauge may be present for a consumable, but the gauge is hashed out instead of containing a remaining percentage.	If a devices answers prtMarkerSuppliesDescription correctly, the gauge is present because HP Web Jetadmin knows the consumable exists. However, if the device cannot answer either prtMarkerSuppliesMaxCapacity or prtMarkerSuppliesLevel correctly, the percentage cannot be calculated and HP Web Jetadmin displays hashes instead to indicate an unknown level.
A paper tray gauge does not indicate a remaining percentage.	While a device answers the prtInputType query to indicate a tray is present, the device may respond to the prtInputMaxCapacity and

Issue	Resolution
	prtInputCurrentLevel queries with either valid values or an indication that at least one sheet remains. If the device returns valid values, a calculation is presented. If the device does not provide valid values, HP Web Jetadmin displays either **Empty** or **Not Empty**, depending on whether the device indicates at least one sheet remains.
The control panel displays **Not Supported** or **Unknown**.	**Not Supported** indicates the device did not respond to the prtConsoleDisplayBufferText object. **Unknown** may indicate that the devices recognizes the prtConsoleDisplayBufferText object, but did respond with any text.
The model name for the device appears to be a much longer name than the true name of the device.	HP Web Jetadmin relies on hrDeviceDescr to display the model name. Properly truncated model names are generally provided in proprietary objects. HP Web Jetadmin does not know how to truncate a response to hrDeveiceDescr if it contains too many characters. For example, if a Lexmark printer responds with **Lexmark X652de 7932M8R LJ.MN.P092**, HP Web Jetadmin does not know where to truncate the string.
No consumable gauges are present for items such as toner and fuser.	A device must answer prtMarkerSuppliesDescription correctly, otherwise HP Web Jetadmin does not know that the consumable exists and cannot display a gauge.

Discovery - Common Tasks Task Module

The **Discovery - Common Tasks** task module provides links that initiate the following tasks for discoveries:

- Discover devices on the network
- Schedule a discovery
- Create a discovery template
- Run a discovery by using a discovery template
- Edit a discovery template
- Delete a discovery template
- Copy a discovery template to create a new template

Discovery - Quick Monitor Task Module

The **Discovery - Quick Monitor** task module can be used to quickly discover a device and display the device status.

Discover a device

1. Enter an IP address or hostname in the **Device** box.
2. Click the **Go** button. The device information and status is displayed in the task module.
3. If the device is not found, use the following steps to specify the device credentials:

a. Click the **Credentials may be required to locate this device** link. The **Enter Credentials** window opens.

b. To use SNMPv1 credentials to discover the device, select the **Use** check box, and then enter the SNMPv1 Get Community Name for the device in the box.

   -or-

   To use SNMPv3 credentials to discover the device, use the following steps:

   i. In the **User name** box, enter the user name.

   ii. From the **Authentication Protocol** list, select the protocol.

      For third-party devices, the authentication protocol must be MD5 or SHA-1. HP Web Jetadmin cannot discover third-party devices that do not use these protocols.

   iii. In the **Authenticated password** and **Confirm authenticated password** boxes, enter the authenticated password (minimum of 8 characters).

      For third-party devices, the authentication password must be in the format of a passphrase with a minimum length of 8 characters. HP Web Jetadmin cannot discover third-party devices that have an authentication password that is in the format of a key or that is less than 8 characters.

   iv. From the **Privacy Protocol** list, select the protocol.

      For third-party devices, the privacy protocol must be DES or AES-128. HP Web Jetadmin cannot discover third-party devices that do not use these protocols.

   v. In the **Private password** and **Confirm private password** boxes, enter the private password (minimum of 8 characters).

   vi. For HP devices, select the **HP Device** checkbox. HP Web Jetadmin uses *Jetdirect* for the context name.

      -or-

      For third-party devices, clear the **HP Device** checkbox, and then enter a context name in the box next to the **HP Device** checkbox. The context name can be left blank.

   vii. Click the **OK** button.

Clear the information from the task module

▲ Click the **Clear** button.

Display the device in the All Devices list

This feature is available only when the **Device - Quick Monitor** task module is accessed from the **Device Management** > **Overview** pane.

▲ Click the **Open** button.

Discovery - Summary Task Module

The **Discovery - Summary** task module provides a list of the discoveries that have run. Use this task module to view the discovery history or run a discovery.

Discovery – Active Discoveries Task Module

The **Discovery – Active Discoveries** task module provides a list of the discoveries that are running. Use this task module to stop or view the progress of an active discovery.

Discovery – Scheduled Discoveries Task Module

The **Discovery – Scheduled Discoveries** task module provides a list of the discoveries that are scheduled to run. Use this task module to delete or edit a discovery schedule.

Discovery – Templates Task Module

The **Discovery – Templates** task module provides a list of the discovery templates that have been created. Use this task module to perform the following tasks:

- Create a discovery template
- Run a discovery by using a discovery template
- Edit a discovery template
- Delete a discovery template
- Copy a discovery template to create a new template
- View the settings for a discovery template

Related Application Options for Discovery

Discovery settings refine the way HP Web Jetadmin performs a discovery in your own environment. Configuration options for **Discovery** include:

- Configure the General Settings for Device Discoveries on page 64 (**Tools** > **Options** > **Device Management** > **Device Discovery** > **General**)
- **IP Range** (**Tools** > **Options** > **Shared** > **Discovery** > **Methods** > **IP Range** > **General** > Configure Large Subnets for IP Range Discoveries on page 49)
- **IP Range** (**Tools** > **Options** > **Shared** > **Discovery** > **Methods** > **IP Range** > Manage the IP Ranges for Discoveries on page 49)

SNMPv3 Enabled Devices

Devices that have SNMPv3 fully enabled can be discovered by HP Web Jetadmin. To discover these devices, enable **Discover SNMP v3 devices** in **Tools** > **Options** > **Device Management** > **Device Discovery** > **General**.

HP Web Jetadmin requires SNMPv3 credentials for these devices in order for them to be discovered. There are two ways HP Web Jetadmin can become aware of device SNMPv3 credentials:

- HP Web Jetadmin is used to enable SNMPv3 and also configure the SNMPv3 credentials onto the devices. In this case, HP Web Jetadmin stores the credentials into its credential store and uses them whenever device communication is required. HP Web Jetadmin also marks these devices as SNMPv3-enabled and remembers to use the credentials and SNMPv3 whenever communication is required.

- HP Web Jetadmin has had SNMPv3 credentials added to the Global credentials store and these credentials match those credential values on the devices. In this case, HP Web Jetadmin is being made aware of credential values that work for devices that are SNMPv3-enabled. When one of these devices is encountered, HP Web Jetadmin will try the credential values that are configured using the option **SNMPv3 Credentials** in **Tools** > **Options** > **Shared** > **Credentials**. If the credential values work and HP Web Jetadmin is able to communicate with the devices, the credential values will be stored individually for each device.

Devices that were discovered through SNMPv1 and have had SNMPv3 enabled through some other means such as Embedded Web Server or another instance of HP Web Jetadmin will indicate a communication failure when HP Web Jetadmin attempts to re-establish communication. The **Refresh Selection (Full)** command can be used on these devices to cause HP Web Jetadmin to reset them to SNMPv3-enabled devices.

NOTE: If SNMPv3 communication was established outside of HP Web Jetadmin, the global discovery setting for **Discover SNMPv3 Devices** must be configured in **Tools** > **Options** > **Device Management** > **Discovery** > **General**. No new SNMPv3 devices will be added to the database unless this option is enabled.

Network Options for Discoveries

Related options that can be set in HP Web Jetadmin through **Tools** > **Options** > **Shared** > **Network** include:

- Configure the SNMP Settings on page 46:
  - **SNMPv1 timeout value**: Specify how long HP Web Jetadmin waits for a reply from a network query that is sent to SNMPv1 devices. The default is 500 ms.
  - **SNMPv3 timeout value**: Specify how long HP Web Jetadmin waits for a reply from a network query that is sent to SNMPv3 devices. The default is 1000 ms.
  - **SNMP retries**: Specify how many times HP Web Jetadmin retries an SNMP communication with devices after a timeout occurs. The default is 3.
- Configure the DNS Settings on page 47 (**Enable DNS lookups**): Forces HP Web Jetadmin to query name services for each device discovered. This setting is sometimes disabled in environments where DNS responses are slow or are not functioning. (The default is on.)
- Manage the IP Ranges for Discoveries on page 49: Global store for IP Range settings used by network device discovery, PC-Connected device discovery and HP Web Jetadmin application discovery.
- Shared Configuration Options for Credentials on page 52: In some cases, credentials like Manage the Global SNMPv1 Get Community Names on page 55 or Manage the Global SNMPv3 Credentials on page 56 are being used. Use **Credentials** to set well known device credentials. These will be tried during discovery when devices don’t respond to queries that use default credentials.

Discover Devices

The **Device Discovery** wizard can be used to launch a discovery immediately or schedule a discovery to run at a later time.

Use the following steps to discover devices:

1. In the **Device Management** navigation pane, right-click **Discovery**, and then select **Discover devices**. The **Device Discovery** wizard starts

2. To use a discovery template, select the **Use template** option, and then select the template from the list.

   -or-

   To specify the discovery settings, use the following steps:

   NOTE: For more information about the discovery types and methods, see Discovery Types and Methods on page 136.

   a. Select the **Specify settings** option.

   b. To discover only devices that are connected directly to the network, select the **Network connected devices** option.

      -or-

      To discover only devices that are connected to the PCs that are on the network, select the **PC connected devices** option.

   c. Select the check boxes for the discovery methods to use. At least one discovery method must be specified.

3. To run the discovery immediately, leave the **Schedule discovery** check box cleared.

   -or-

   To schedule the discovery to run at a later time, select the **Schedule discovery** check box.

   NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

   NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

4. Click the **Next** button.

5. On the settings page, specify the settings for the discovery method, and then click the **Next** button.

   If more than one discovery method is selected, the wizard displays a separate settings page for each discovery method.

6. If credentials are not required to discover the devices, select the **Do not use credentials** option.

   -or-

   If credentials are required to discover the devices, use the following steps to specify the credentials:

   NOTE: The credentials options that are available vary depending on the discovery methods selected.

   a. Select the **Specify credentials to use for this discovery** option.

   b. If the devices on the network have an SNMPv1 Get Community Name other than public defined, select the **SNMPv1 Get Community Name** checkbox, and then enter the SNMPv1 Get Community Name in the box.

c. If HP Web Jetadmin is configured to discover SNMPv3 devices, use the following steps to specify the SNMPv3 credentials:

> TIP: To enable HP Web Jetadmin to discover SNMPv3 devices, go to **Tools** > **Options** > **Device Management** > **Device Discovery** > **General**.

i. Select the **SNMPv3 Credentials** check box.

ii. In the **User name** box, enter the user name.

iii. From the **Authentication Protocol** list, select the protocol.

For third-party devices, the authentication protocol must be MD5 or SHA-1. HP Web Jetadmin cannot discover third-party devices that do not use these protocols.

iv. In the **Authenticated passphrase** and **Confirm authenticated passphrase** boxes, enter the authenticated passphrase (minimum of 8 characters).

For third-party devices, the authentication passphrase must be in the format of a passphrase with a minimum length of 8 characters. HP Web Jetadmin cannot discover third-party devices that have an authentication passphrase that is in the format of a key or that is less than 8 characters.

v. From the **Privacy Protocol** list, select the protocol.

For third-party devices, the privacy protocol must be DES or AES-128. HP Web Jetadmin cannot discover third-party devices that do not use these protocols.

vi. In the **Private passphrase** and **Confirm private passphrase** boxes, enter the private passphrase (minimum of 8 characters).

vii. For HP devices, select the **HP Device** checkbox. HP Web Jetadmin uses *Jetdirect* for the context name.

-or-

For third-party devices, clear the **HP Device** checkbox, and then enter a context name in the box next to the **HP Device** checkbox. The context name can be left blank.

d. If Active Directory credentials are required, select the **Active Directory Credentials** check box, and then enter the user name, password, and domain in the boxes.

e. To use the global credentials, select the **Use global credentials** checkbox.

> TIP: To define the global credentials, go to **Tools** > **Options** > **Shared** > **Credentials**, and then select the appropriate option.

7. Click the **Next** button.

8. Use the following steps to schedule the discovery:

> NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

a. In the **Name** box, enter a name for this discovery schedule.

b. In the **Start time** boxes, specify the date and time that this discovery starts.

   c. In the **Recurrence** section, select the option that defines how often this discovery runs, and then specify the corresponding settings.

   d. Click the **Next** button.

9. On the **Confirm** page, verify that the settings are correct, and then click the **Start** button.

10. On the **Progress** page, click the **Details** button. Review the information for each discovery method, and then click the **Close** button.

11. On the **Results** page, select the **View all devices** check box to display a list of the discovered devices.

12. Click the **Done** button.

Schedule Discoveries

Discoveries can be scheduled to run once on a specific date and time or run on a recurring basis. Discoveries can be scheduled for network-connected devices or PC-connected devices. Multiple schedules can be created with different settings, such as discovery type, discovery methods, and date and time to run.

The settings for a discovery schedule can be changed at any time. The next time the scheduled discovery runs, the updated settings are used.

For example, assume that the administrator wants to run an IP Range discovery on the subnets in Asia and Europe every Wednesday at 11:00 a.m. in the time zone where the subnets are located. Each location has five subnets. Most of the employees turn off the devices at night to save energy. The HP Web Jetadmin server is in the North American Central Time Zone. The following table provides the settings for the discovery schedules that are required to accomplish this task.

Schedule name	Time discovery runs in Central Time Zone	Recurrence	IP ranges searched
Asia	9:00 p.m.	Every week on Tuesday	15.62.40.1-15.62.47.254
Europe	4:00 a.m.	Every week on Wednesday	15.5.188.2-15.5.188.254

Use the following steps to schedule a discovery:

IMPORTANT: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

1. In the **Device Management** navigation pane, right-click **Discovery**, and then select **Schedule discovery**. The **Device Discovery** wizard starts.

2. To use a discovery template, select the **Use template** option, and then select the template from the list.

   NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

   -or-

   To specify the discovery settings, use the following steps:

   NOTE: For more information about the discovery types and methods, see Discovery Types and Methods on page 136.

a. Select the **Specify settings** option.

b. To discover only devices that are connected directly to the network, select the **Network connected devices** option.

   -or-

   To discover only devices that are connected to the PCs that are on the network, select the **PC connected devices** option.

c. Select the check boxes for the discovery methods to use. At least one discovery method must be specified.

3. Click the **Next** button.

4. On the settings page, specify the settings for the discovery method, and then click the **Next** button.

   If more than one discovery method is selected, the wizard displays a separate settings page for each discovery method.

5. If credentials are not required to discover the devices, select the **Do not use credentials** option.

   -or-

   If credentials are required to discover the devices, use the following steps to specify the credentials:

   NOTE: The credentials options that are available vary depending on the discovery methods selected.

   a. Select the **Specify credentials to use for this discovery** option.

   b. If the devices on the network have an SNMPv1 Get Community Name other than public defined, select the **SNMPv1 Get Community Name** checkbox, and then enter the SNMPv1 Get Community Name in the box.

   c. If HP Web Jetadmin is configured to discover SNMPv3 devices, use the following steps to specify the SNMPv3 credentials:

      TIP: To enable HP Web Jetadmin to discover SNMPv3 devices, go to **Tools** > **Options** > **Device Management** > **Device Discovery** > **General**.

      i. Select the **SNMPv3 Credentials** check box.

      ii. In the **User name** box, enter the user name.

      iii. From the **Authentication Protocol** list, select the protocol.

      For third-party devices, the authentication protocol must be MD5 or SHA-1. HP Web Jetadmin cannot discover third-party devices that do not use these protocols.

      iv. In the **Authenticated password** and **Confirm authenticated password** boxes, enter the authenticated password (minimum of 8 characters).

      For third-party devices, the authentication password must be in the format of a passphrase with a minimum length of 8 characters. HP Web Jetadmin cannot discover third-party devices that have an authentication password that is in the format of a key or that is less than 8 characters.

      v. From the **Privacy Protocol** list, select the protocol.

      For third-party devices, the privacy protocol must be DES or AES-128. HP Web Jetadmin cannot discover third-party devices that do not use these protocols.

vi. In the **Private password** and **Confirm private password** boxes, enter the private password (minimum of 8 characters).

vii. For HP devices, select the **HP Device** checkbox. HP Web Jetadmin uses *Jetdirect* for the context name.

-or-

For third-party devices, clear the **HP Device** checkbox, and then enter a context name in the box next to the **HP Device** checkbox. The context name can be left blank.

d. If Active Directory credentials are required, select the **Active Directory Credentials** check box, and then enter the user name, password, and domain in the boxes.

e. To use the global credentials, select the **Use global credentials** checkbox.

> TIP: To define the global credentials, go to **Tools** > **Options** > **Shared** > **Credentials**, and then select the appropriate option.

6. Click the **Next** button.

7. Use the following steps to specify the schedule settings:

a. In the **Name** box, enter a name for this discovery schedule.

b. In the **Start time** boxes, specify the date and time that this discovery starts.

c. In the **Recurrence** section, select the option that defines how often this discovery runs, and then specify the corresponding settings.

d. Click the **Next** button.

8. On the **Confirm** page, verify that the settings are correct, and then click the **Start** button.

9. On the **Results** page, click the **Done** button.

View Discovery History

After discoveries run, use the discovery history to evaluate the effectiveness of the discoveries and adjust future discoveries to better meet your needs.

Use the following steps to view the discovery history:

1. In the **Device Management** navigation pane, expand **Discovery**, and then select **History**.

2. To display the detailed data for a discovery, click the **+** button.

   -or-

   To hide the detailed data for a discovery, click the **-** button.

Summary discovery data (first-level fields)

The first-level fields provide the overall results of each discovery. With the exception of the **New Devices Found** column, these statistics pertain only to a specific discovery. The device count in the **New Devices Found** column is only the number of new devices found since the previous discovery ran.

The following are the first-level fields:

- **Date**: the date and time the discovery ran.
- **User**: the user who requested the discovery.

- **Duration**: how long it took for the discovery to complete.
- **Type**: type of discovery ran (PC-Connected devices or network devices).
- **Total Devices Found**: the number of network and PC-Connected devices found **for this discovery**.
- **New Devices Found**: the number of “New” devices found (network and PC-Connected) **for this discovery**.
- **Hidden Devices**: devices that have been removed from the Device View list. This can happen if a device has been rediscovered with a new network card causing the previous entry to be invalidated but still kept in the database as an inactive device.
- **Reactivated Devices**: Hidden devices that are placed back in the **Device View** list. This can happen when a previously hidden device is rediscovered under a previously discovered connection.

Detailed discovery data (second-level fields)

The second-level fields provide detailed data about each discovery. Use this data to evaluate and compare the effectiveness of the discovery methods. For example, use the **Devices Found** and **Unique Devices** columns to determine the strength of a particular discovery method.

The following are the second-level fields:

- **Method**: the type of discovery that was run. The statistics collected on each discovery method row are specific to that method. Each of the following fields listed are specific to the method listed here.
- **Devices Found**: the number of devices found by this discovery method and possibly by other methods as well.
- **Unique Devices**: the number of devices found by only this discovery method. Not found within any other discovery method.
- **New Devices**: the number of new devices found by this discovery method. New devices are not cumulative across methods if found by multiple methods. For example, if multiple methods were used for a discovery and one new device was found by multiple methods, that one device will be listed under each method that found it.
- **Node Count**: the number of active nodes or network devices (printer and non-print devices) that were discovered using this discovery method. This discovery represents a listing of IP addresses that could be resolved into printers and added to the **All Devices** list.
- **Blocked Devices**: the number of blocked devices found by this discovery method.
- **New Unique Devices**: the number of new devices found by only this discovery method.

Discovery Templates

Discovery templates can be accessed from the **Device Management** navigation pane or the **Discovery – Templates** task module.

Create Discovery Templates

A discovery template contains the settings to run a network-connected device discovery or PC-connected device discovery. A discovery template can be used to launch a discovery or create a discovery schedule. The **Discovery – Templates** task module can be used to manage the discovery templates.

Use the following steps to create a discovery template:

NOTE: For more information about the discovery types and methods, see Discovery Types and Methods on page 136.

1. In the **Device Management** navigation pane, right-click **Discovery**, and then select **Create discovery template**. The **Create Discovery Template** starts.
2. To discover only devices that are connected directly to the network, select the **Network connected devices** option.

   -or-

   To discover only devices that are connected to the PCs that are on the network, select the **PC connected devices** option.
3. Select the check boxes for the discovery methods to use. At least one discovery method must be specified.
4. Click the **Next** button.
5. On the settings page, specify the settings for the discovery method, and then click the **Next** button.

   If more than one discovery method is selected, the wizard displays a separate settings page for each discovery method.
6. If credentials are not required to discover the devices, select the **Do not use credentials** option.

   -or-

   If credentials are required to discover the devices, use the following steps to specify the credentials:

   NOTE: The credentials options that are available vary depending on the discovery methods selected.

   a. Select the **Specify credentials to use for this discovery** option.

   b. If the devices on the network have an SNMPv1 Get Community Name other than public defined, select the **SNMPv1 Get Community Name** checkbox, and then enter the SNMPv1 Get Community Name in the box.

   c. If HP Web Jetadmin is configured to discover SNMPv3 devices, use the following steps to specify the SNMPv3 credentials:

      TIP: To enable HP Web Jetadmin to discover SNMPv3 devices, go to **Tools** > **Options** > **Device Management** > **Device Discovery** > **General**.

      i. Select the **SNMPv3 Credentials** check box.

      ii. In the **User name** box, enter the user name.

      iii. From the **Authentication Protocol** list, select the protocol.

      For third-party devices, the authentication protocol must be MD5 or SHA-1. HP Web Jetadmin cannot discover third-party devices that do not use these protocols.

      iv. In the **Authenticated password** and **Confirm authenticated password** boxes, enter the authenticated password (minimum of 8 characters).

      For third-party devices, the authentication password must be in the format of a passphrase with a minimum length of 8 characters. HP Web Jetadmin cannot discover third-party devices that have an authentication password that is in the format of a key or that is less than 8 characters.

v. From the **Privacy Protocol** list, select the protocol.

   For third-party devices, the privacy protocol must be DES or AES-128. HP Web Jetadmin cannot discover third-party devices that do not use these protocols.

vi. In the **Private password** and **Confirm private password** boxes, enter the private password (minimum of 8 characters).

vii. For HP devices, select the **HP Device** checkbox. HP Web Jetadmin uses *Jetdirect* for the context name.

   -or-

   For third-party devices, clear the **HP Device** checkbox, and then enter a context name in the box next to the **HP Device** checkbox. The context name can be left blank.

d. If Active Directory credentials are required, select the **Active Directory Credentials** check box, and then enter the user name, password, and domain in the boxes.

e. To use the global credentials, select the **Use global credentials** checkbox.

TIP: To define the global credentials, go to **Tools** > **Options** > **Shared** > **Credentials**, and then select the appropriate option.

7. Click the **Next** button.
8. On the **Specify template name** page, enter a name for this template, and then click the **Next** button.
9. On the **Confirm** page, verify that the information is correct, and then click the **Create Template** button.
10. On the **Results** page, click the **Done** button.

Run Discoveries by Applying Discovery Templates

Use the following steps to run a discovery by applying a discovery template:

1. In the **Device Management** navigation pane, right-click **Discovery**, and then select **Run discovery template**. The **Device Discovery** wizard starts.
2. Select the template to use and click **Next**. The **Confirm** page is displayed.
3. The template summary information is displayed. Review your selection and if it is correct click **Start**. The **Progress** page is displayed. (You can hide the **Progress** page to do other functions in HP Web Jetadmin while the discovery is in progress, or you can stop the discovery from this page.)
4. When the discovery is complete, the **Results** page is displayed.

   To view the discovered devices on the **All Devices** list, check **View all devices**.

   To return to the **Discovery** page, click **Done**.

Edit Discovery Templates

The settings for a discovery template can be changed at any time. After the settings are changed, any discovery that runs by applying the updated discovery template uses the updated settings.

Use the following steps to edit a discovery template:

1. In the **Device Management** navigation pane, expand the **Discovery** option, and then select **Templates**.
2. In the **Discovery Templates** pane, select the template from the list, and then click the **Edit** button. The **Edit Discovery Template** wizard starts.
3. To discover only devices that are connected directly to the network, select the **Network connected devices** option.

   -or-

   To discover only devices that are connected to the PCs that are on the network, select the **PC connected devices** option.

   NOTE: For more information about the discovery types and methods, see Discovery Types and Methods on page 136.

4. Select the check boxes for the discovery methods to use. At least one discovery method must be specified.
5. Click the **Next** button.
6. On the settings page, specify the settings for the discovery method, and then click the **Next** button.

   If more than one discovery method is selected, the wizard displays a separate settings page for each discovery method.

7. If credentials are not required to discover the devices, select the **Do not use credentials** option.

   -or-

   If credentials are required to discover the devices, use the following steps to specify the credentials:

   NOTE: The credentials options that are available vary depending on the discovery methods selected.

   a. Select the **Specify credentials to use for this discovery** option.

   b. If the devices on the network have an SNMPv1 Get Community Name other than public defined, select the **SNMPv1 Get Community Name** checkbox, and then enter the SNMPv1 Get Community Name in the box.

   c. If HP Web Jetadmin is configured to discover SNMPv3 devices, use the following steps to specify the SNMPv3 credentials:

      TIP: To enable HP Web Jetadmin to discover SNMPv3 devices, go to **Tools** > **Options** > **Device Management** > **Device Discovery** > **General**.

      i. Select the **SNMPv3 Credentials** check box.

      ii. In the **User name** box, enter the user name.

      iii. From the **Authentication Protocol** list, select the protocol.

      For third-party devices, the authentication protocol must be MD5 or SHA-1. HP Web Jetadmin cannot discover third-party devices that do not use these protocols.

      iv. In the **Authenticated password** and **Confirm authenticated password** boxes, enter the authenticated password (minimum of 8 characters).

      For third-party devices, the authentication password must be in the format of a passphrase with a minimum length of 8 characters. HP Web Jetadmin cannot discover third-party devices that have an authentication password that is in the format of a key or that is less than 8 characters.

v. From the **Privacy Protocol** list, select the protocol.

For third-party devices, the privacy protocol must be DES or AES-128. HP Web Jetadmin cannot discover third-party devices that do not use these protocols.

vi. In the **Private password** and **Confirm private password** boxes, enter the private password (minimum of 8 characters).

vii. For HP devices, select the **HP Device** checkbox. HP Web Jetadmin uses *Jetdirect* for the context name.

-or-

For third-party devices, clear the **HP Device** checkbox, and then enter a context name in the box next to the **HP Device** checkbox. The context name can be left blank.

d. If Active Directory credentials are required, select the **Active Directory Credentials** check box, and then enter the user name, password, and domain in the boxes.

e. To use the global credentials, select the **Use global credentials** checkbox.

TIP: To define the global credentials, go to **Tools** > **Options** > **Shared** > **Credentials**, and then select the appropriate option.

8. Click the **Next** button.

9. In the **Specify template name** box, enter a new name for the discovery template, and then click the **Next** button.

10. On the **Confirm** page, verify that the settings are correct, and then click the **Save Template** button.

11. On the **Results** page, select the **Run discovery** check box to launch a discovery.

12. Click the **Done** button.

Copy Discovery Templates

Use the following steps to copy a discovery template and create a new template:

1. In the **Device Management** navigation pane, expand **Discovery**, and then expand **Templates**.

2. Right-click the template to be copied, and then select **Copy**. The **Copy Template** wizard starts.

3. On the **Specify template name** page, enter a name for the new discovery template, and then click the **Next** button.

4. On the **Confirm** page, verify that the information is correct, and then click the **Copy Template** button.

5. On the **Results** page, click the **Done** button.

Delete Discovery Templates

Use the following steps to delete a discovery template:

1. In the **Device Management** navigation pane, expand the **Discovery** option, and then select **Templates**.

2. In the **Discovery Templates** pane, select the template from the list, and then click the **Delete** button. The **Delete Discovery Templates** wizard starts.

3. On the **Confirm** page, verify that the information is correct, and then click the **Delete Template** button.

4. On the **Results** page, click the **Done** button.

View Discovery Templates

Use the following steps to view a discovery template:

1. In the **Device Management** navigation pane, expand the **Discovery** option, and then select **Templates**.

2. In the **Discovery Templates** pane, select the discovery template from the list, and then click the **View** button.

Configuration

Many device settings can be viewed and configured through HP Web Jetadmin. Device configuration works differently depending on whether a single device or multiple devices are selected.

If a single device is selected, the configuration items in the tab are shown with the current device settings. If multiple devices are selected, configuration items in the tab are shown with unspecified or blank settings. The list of configurable options varies by the devices selected. With multiple devices selected, all configurable items will probably not apply to all devices. Only settings that apply to a device will be set on that device. Some options may be repeated multiple times because different settings are supported on different devices. If it is not clear which device or device model a particular setting applies to, holding the mouse over the name in the configuration settings displays a tooltip with additional information.

Configuration option availability depends on device model, network card and firmware revision. One model of device may support a configuration option for digital send functionality where another model, probably a single-function one, does not support that same configuration option. Again, in fleet scenarios, any configuration option that is set in HP Web Jetadmin will only be applied to device models for which it is supported.

Complex Data in the Confirm, Results, and Configuration History Pages

When configuring devices, the **Confirm** and **Results** pages display the options you are configuring and the values for those options in a simple grid. If the value of the configuration option is complex, the first column in the grid contains an icon. Hold the mouse anywhere over the line for that configuration option to activate the advanced tool tip feature and display details of the configuration option.

The advanced tool tip displays for one minute or until you move the mouse out of the tool tip. Every time you move the mouse within the tool tip the one minute starts over. The information displayed in the tool tip can also be complex. In this case, the tool tip displays only a summary similar to the device list grid and displays an icon that indicates more data is available. Holding the mouse over the data in the tool tip activates another advanced tool tip that displays the next level of details. This allows you to display multiple levels of details.

Credentials Required for Device Configuration

When HP Web Jetadmin encounters a device configuration that requires credentials, it looks in the device-specific credentials store first. If there are credentials for that device in the store, HP Web Jetadmin uses those credentials for the configuration. If the credentials are valid, HP Web Jetadmin configures the device and does not change the credentials in the store. If there are no credentials for the device in the store or the credentials are not valid, HP Web Jetadmin uses the global credentials. If the global credentials are valid and the configuration is successful, HP Web Jetadmin adds the credentials for that device to the store. If a device credential failure occurs, HP Web Jetadmin displays the Needed Credentials wizard and you can add the device credentials to HP Web Jetadmin. After you add the required credentials, the device configuration should succeed.

This state can also be detected in post-configuration in either **Configuration History** or in the **Credentials Required** column. After the required credential values exist in the **Credentials Store**, prompting from HP Web Jetadmin should not occur unless the values on the device change.

Device File System Password

If a file system password exists on the device and if it is not captured in HP Web Jetadmin's **Credential Store**, you will be prompted for the password when attempting to perform any configuration action. Device file system passwords can be configured on the devices from HP Web Jetadmin. When these are configured, they are also placed into the **Credential Store**. Global file system credentials can be added to HP Web Jetadmin through **Tools** > **Options** > **Shared** > **Credentials** > **Device** > **File System** (Manage the Global File System Passwords on page 58). These are used when no password exists in the store and one is required by the device.

Sensitive Device Information

In some cases, HP Web Jetadmin sends sensitive information to the device. This information can include user and password detail such as device **Digital Send** features or other device security features that require credentials. In this case HP Web Jetadmin is sending the information using the SSL/TLS protocol. This protocol allows HP Web Jetadmin to send encrypted information to the device and prevents clear-text information from being 'sniffed' through a network trace utility. When communicating with the device through the SSL/TLS protocol, HP Web Jetadmin uses certificates stored on the printer's HP Jetdirect network interface. These certificates can be self-signed or they can be signed by a verifiable certificate authority. At this time, HP Web Jetadmin does not check the authenticity of certificates stored on the device; it simply uses the certificate when communicating with the device through the SSL/TLS protocol. This security limitation could be exploited, allowing unauthorized individuals access to sensitive information like user and password detail. Administrators should keep this in mind when managing sensitive device information using HP Web Jetadmin software.

Importing a Configuration from a File

A CSV (comma separated value) file can be created and then imported into HP Web Jetadmin for the purpose of device configuration. This provides a way to configure a fleet of devices with unique parameters that would otherwise have to be configured one device at a time. CSV files can easily be created by exporting data from a spreadsheet or word processing program.

Here is an example of a device configuration scenario:

- 30 devices exist: 16.24.1.26-16.24.1.56
- Asset number assignments are required: Abc10040-Abc10070
- Assignments are made respective to IP address sequence

The following table is an example of the CSV file for this device configuration scenario.

IP Addr	Port	Asset Number
16.24.1.26	1	Abc10040

IP Addr	Port	Asset Number
16.24.1.27	1	Abc10041
16.24.1.28	1	Abc10042
16.24.1.29	1	Abc10043
16.24.1.30	1	Abc10044

NOTE: The first column is always the device identification, which can be an IP address, MAC address, or IP hostname. The second column is always the port. For HP devices, the port is 1, unless a device is attached to a multiport print server. For third-party devices, the port must be <Not supported>, which is case-sensitive. If you specify anything else for third-party devices, the import fails.

Once the file is created and stored to disk on the client desktop; the user can import the file contents into HP Web Jetadmin using **Configure Devices**.

The CSV file contains header text for each device property to be configured. Once the user has browsed and uploaded the file a Map Headers control appears. The customer specific header text can be matched with the corresponding device property.

The following are the columns headers for a CSV file. The first two columns identify the devices to configure. If HP Web Jetadmin did not discover these devices before the CSV file is imported, the devices are not configured.

- Column 1: Device Identifier (either IP address, hardware address (MAC address), or IP hostname)
- Column 2: Port (always just “Port”)
- Column 3 through *nn*: User-specified device settings. The following device settings can be imported:
  - Access Control List
  - Asset Number
  - Company Name
  - Default Copier Copies
  - Default Printer Copies
  - Device Location
  - Device Name
  - Get Community Name
  - Job Timeout
  - Set Community Name
  - System Contact
  - System Location
  - System Name
  - TCP Idle Timeout
  - HTTP Idle Timeout
  - Any user-defined settings that are specified by using the **Tools** > **Options** > **Device Management** > **Configuration** > **User Defined** option.

Once the mapping is configured, HP Web Jetadmin displays the data headers and device status. Devices which were previously discovered and successfully matched are shown in the list; any devices in the file which were not successfully matched are counted as “Unresolved devices”.

Only the settings listed above can be imported from a file. If a setting contains a comma, quotations must be used around that particular setting. For example, the following line can be used to set values of "Chicago, IL, USA" and "Building 5, Floor 3":

```
16.24.1.26,1,“Chicago, IL, USA”,“Building 5, Floor 3”
```

Configuration - Common Tasks Task Module

The **Configuration - Common Tasks** task module provides links that initiate the following configuration tasks:

- Configure the settings on devices
- Schedule a device configuration
- Create a device configuration template
- Apply a device configuration template to devices
- Edit the settings for a device configuration template
- Delete a device configuration template
- Copy a device configuration template to create a new template
- View the device configuration history

Configuration - Recent Configurations Task Module

The **Configuration - Recent Configurations** task module provides a list of the device configurations that have run. Use this task module to view the details for a device configuration or the device configuration history.

Configuration - Active Configurations Task Module

The **Configuration - Active Configurations** task module provides a list of the device configuration tasks that are running. Use this task module to stop or view the status of an active task.

Configuration - Scheduled Configurations Task Module

The **Configuration - Scheduled Configurations** task module provides a list of the device configurations that are scheduled to run. Use this task module to delete or edit a configuration schedule.

Configuration - Templates Task Module

The **Configuration - Templates** task module provides a list of the default device configuration templates and the custom device configuration templates that have been created. Use this task module to perform the following tasks:

- Create a device configuration template
- Apply a device configuration template to devices
- Edit the settings for a device configuration template
- Delete a device configuration template
- Copy a device configuration template to create a new template
- View the settings for a device configuration template

Related Application Options for Configuration Management

Global settings can be set here for fleet configurations:

- Configure the Retry Settings for Device Configuration Schedules on page 66
- Restore the Default Configuration Templates on page 66
- Manage the User-defined Device Configuration Settings on page 66

Configure Devices

Use the following steps to configure devices without using a configuration template:

1. In the left **Device Management** navigation pane, right-click **Configuration**, and then select **Configure devices**. The **Configure Devices** wizard starts.
2. Select one of the options:
   - **Use template**: Devices will be configured by applying settings from a template. Select a configuration template from the drop-down box and go to Step 3.
   - **Specify settings**: Devices will be configured by specifying settings in the wizard. Go to Step 3.
   - **Import from file**: Devices will be configured by importing settings from a CSV file. (See Importing a Configuration from a File on page 172.)
     - Click **Next**. The **Select CSV file** page is displayed.
     - Type the path and name of the CSV file to import, or browse for the file. Click **Next**. If successful, it shows you the headers from the CSV file.

       NOTE: If any errors are found in the CSV file, you will need to correct them and then try this import procedure again.
     - Select the comparable device setting for each header. Click **Next**. The **Confirm** page is displayed.
     - Click **Configure devices**. The **Results** page is displayed. Click **Done** to display the **Configuration** page.

   NOTE: For more information about the **Confirm** and **Results** pages, see Complex Data in the Confirm, Results, and Configuration History Pages on page 171.
3. To schedule the configuration for a later time, click **Schedule configuration**.

NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

4. Click **Next**. The **Select devices** page is displayed.

5. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

   To select an entire group instead of individual devices, change the selection method to **Groups**. Tasks can be performed on a single group or a group and all of its subgroups.

   NOTE: If subgroups are included, the task might take longer to complete and network traffic might increase significantly. HP recommends that you include subgroups only when necessary.

   If a task is scheduled for a group, the task uses the devices that are in the group when the task starts. If the devices that are in the group are changed, you do not have to delete the scheduled task and create a new scheduled task.

   Click **Next**. If you chose to specify settings, the **Specify device settings** page is displayed.

6. The settings displayed are the ones supported by the devices selected in Step 5. Settings are organized alphabetically within each category. You can also use the personalized **My Settings** category to easily find your favorite settings. If **My Settings** is not visible, then right-click and select **Show 'My Settings'**. Select the configuration options and then click **Next**.

   NOTE: For information about specific configuration options that might not work properly in a batch mode, see Captured Configurable Options and Configuration Templates on page 182.

   If you chose to schedule this configuration, the **Specify schedule options** page is displayed.

   If you did not choose to schedule this configuration, go to Step 8.

7. Select the start date and time for your configuration, specify how often it should run, and give it a name. Configuration schedules can have the following flexible settings applied:

   - **Name**: Enter a name for this scheduled task, for easier identification in the task modules and the configuration history.
   - **Start time**: Specifies when the configuration will launch.
   - **Recurrence, Once**: Launches only once in the specified schedule.
   - **Recurrence, Daily**: Task will recur daily once per day or once per weekday depending on the selected setting.
   - **Recurrence, Weekly**: Task will recur once every X weeks on the day specified depending on the setting.
   - **Recurrence, Monthly**: Task will recur once every X months on XX day depending on setting; or, task will recur on specified day pattern depending on setting.

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

NOTE: For more information about the **Confirm** page, see Complex Data in the Confirm, Results, and Configuration History Pages on page 171.

8. Review the settings selected. If you did not choose to schedule this configuration, go to step 10.

9. Click **Create Schedule**. The **Results** page is displayed.

   NOTE: For more information about the **Results** page, see Complex Data in the Confirm, Results, and Configuration History Pages on page 171.

   At this point, the schedule has been created but the devices have not yet been configured. You may want to run the configuration once to make sure there are no problems, such as devices needing credentials in order to be configured. This will increase the chances of the scheduled configuration completing successfully. If you do not want to run the configuration now, uncheck the option **Run configuration now (recommended)** and click **Done** to display the **Configuration** page. Otherwise, you will be taken to a second **Configuration** page.

10. Click **Configure Devices**. The **Results** page is displayed. To see details of the configuration, click **Details**. Then click **Close**.

    NOTE: For more information about the **Results** page, see Complex Data in the Confirm, Results, and Configuration History Pages on page 171.

    Click **Done** to display the **Configuration** page.

View the Configuration History

When HP Web Jetadmin configures a device, information about the device, settings configured, and results is stored in the configuration history. The configuration history can be exported to a comma-separated values (CSV) file.

View the configuration history

1. In the **Device Management** navigation pane, expand **Configuration**, and then select **History**.

   NOTE: For more information about how to display complex data on the **Configuration History** pane, see Complex Data in the Confirm, Results, and Configuration History Pages on page 171.

2. On the **Configuration History** pane, select one of the following options from the **Group By** list:

   - **None**—Displays the configuration history as a simple list. To sort the list by a column, click the column heading.
   - **Task**—Groups the configuration history by the task.
   - **Device**—Groups the configuration history by the device model.
   - **Initiator**—Groups the configuration history by the user who initiated the device configuration.
   - **Start time**—Groups the configuration history by the date and time that the device configuration started.
   - **Device result**—Groups the configuration history by the results of the device configuration.
   - **Task result**—Groups the configuration history by the results of the task.

3. To display the details for a group or device configuration, click the **+** button next to the group or device configuration.

   -or-

   To hide the details for a group or device configuration, click the **-** button next to the group or device configuration.

4. To display the details for all of the configuration history, click the **+** (**Expand All**) button at the top of the **Configuration History** pane.

   -or-

   To hide the details for all of the configuration history, click the **-** (**Collapse All**) button at the top of the **Configuration History** pane.

5. To refresh the configuration history, click the **Refresh** button.

Export the configuration history

1. In the **Device Management** navigation pane, expand **Configuration**, and then select **History**.
2. Click the **Export** button.
3. On the **Save As** window, navigate to and select the folder where the CSV file is saved.
4. In the **File name** box, enter a name for the CSV file.
5. Click the **Save** button.

Schedule Device Configurations

Configurations can be scheduled to occur at the time and day you specify. Like other scheduling within HP Web Jetadmin, configuration schedules can have the following flexible settings applied:

NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

- **Name**: Allows flexible naming of scheduled tasks.
- **Start time**: Specifies when the configuration will launch.
- **Recurrence**, **Once**: Launches only once in the specified schedule.
- **Recurrence**, **Daily**: Will recur daily once per day or once per weekday depending on setting.
- **Recurrence**, **Weekly**: Will recur every X weeks depending on setting.
- **Recurrence**, **Monthly**: Will recur once every X months on XX day depending on setting; or, task will recur on specified day pattern depending on setting.

Once a configuration task is scheduled it can be viewed in the **Configuration - Scheduled Configurations** task module. Running tasks can be viewed in **Configuration - Active Configurations** task module.

Use the following steps to schedule a device configuration:

NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

1. In the **Device Management** navigation pane, right-click **Configuration**, and then select **Schedule configuration**. The **Schedule Device Configuration** wizard starts.

2. Select one of the options:

   - **Use template**: Devices will be configured by applying settings from a template. Select a configuration template from the drop-down box and go to Step 3.

   - **Specify settings**: Devices will be configured by specifying settings in the wizard. Go to Step 3.

   - **Import from file**: Devices will be configured by importing settings from a CSV file. (See Importing a Configuration from a File on page 172.)

     – Click **Next**. The **Select CSV file** page is displayed.

     – Type the path and name of the CSV file to import, or browse for the file. Click **Next**. If successful, it shows you the headers from the CSV file.

     NOTE: If any errors are found in the CSV file, you will need to correct them and then try this import procedure again.

     – Select the comparable device setting for each header. Click **Next**. The **Confirm** page is displayed.

     – Click **Configure devices**. The **Results** page is displayed. Click **Done** to display the **Configuration** page.

3. Click **Next**. The **Select devices** page is displayed.

4. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

   To select an entire group instead of individual devices, change the selection method to **Groups**. Tasks can be performed on a single group or a group and all of its subgroups.

   NOTE: If subgroups are included, the task might take longer to complete and network traffic might increase significantly. HP recommends that you include subgroups only when necessary.

   If a task is scheduled for a group, the task uses the devices that are in the group when the task starts. If the devices that are in the group are changed, you do not have to delete the scheduled task and create a new scheduled task.

   Click **Next**. If you chose to specify settings, the **Specify device settings** page is displayed.

5. The settings displayed are the ones supported by the devices selected in Step 4. Settings are organized alphabetically within each category. You can also use the personalized **My Settings** category to easily find your favorite settings. If **My Settings** is not visible, then right-click and select **Show 'My Settings'**. Select the configuration options and then click **Next**.

   NOTE: For information about specific configuration options that might not work properly in a batch mode, see Captured Configurable Options and Configuration Templates on page 182.

6. Select the start date and time for your configuration, specify how often it should run, and give it a name. Configuration schedules can have the following flexible settings applied:

- **Name**: Enter a name for this scheduled task, for easier identification in the task modules and the configuration history.
- **Start time**: Specifies when the configuration will launch.
- **Recurrence, Once**: Launches only once in the specified schedule.
- **Recurrence, Daily**: Task will recur daily once per day or once per weekday depending on the selected setting
- **Recurrence, Weekly**: Task will recur once every X weeks on the day specified depending on the setting.
- **Recurrence, Monthly**: Task will recur once every X months on XX day depending on setting; or, task will recur on specified day pattern depending on setting.

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

7. Review the settings selected.
8. Click **Create Schedule**. The **Results** page is displayed.

   At this point, the schedule has been created but the devices have not yet been configured. You may want to run the configuration once to make sure there are no problems, such as devices needing credentials in order to be configured. This will increase the chances of the scheduled configuration completing successfully. If you do not want to run the configuration now, uncheck the option **Run configuration now (recommended)** and click **Done** to display the **Configuration** page. Otherwise, you will be taken to a second **Configuration** page.
9. Click **Configure Devices**. The **Results** page is displayed. To see details of the configuration, click **Details**. Then click **Close**.

   Click **Done** to display the **Configuration** page.

Configuration Templates

Configuration templates are used to store device settings and apply those settings to one or more devices. This can be done to keep device configurations consistent and to make it easy to apply a common set of settings on a regular basis. Templates are an easy way to change the settings for regularly scheduled configurations, without having to recreate the entire schedule. Templates can also be used to save many settings from a device, either for backup purposes or to apply to similar devices.

You can create and manage configuration templates:

- **Create configuration template**: Create a configuration template (Create Configuration Templates on page 182).
- **Apply configuration template to devices**: Apply the selected configuration template to devices (Apply Configuration Templates to Devices on page 186).
- **Edit configuration template**: Make changes to an existing configuration template (Edit Configuration Templates on page 185).
- **Delete configuration template**: Delete a configuration template (Delete Configuration Templates on page 186).
- **Copy configuration template**: Copy a configuration template and rename the new template and make changes to it (Copy Template Wizard on page 99).

- **Export configuration templates**: Export a configuration template to a file and then import it into a different instance of HP Web Jetadmin running on a different server (Export and Import Device Configuration Templates on page 99).
- **Import configuration templates**: After a configuration template has been exported, you can then import it to use it on a different instance of HP Web Jetadmin running on a different server (Export and Import Device Configuration Templates on page 99).

Volatile Configuration and HP Web Jetadmin Configuration Templates

Some actions performed remotely on devices can cause the device to automatically power cycle or change in some other way that can impact the success of further configuration. Consider the case where you are attempting to configure several device parameters, including one parameter that causes the device to reset itself, which also causes HP Web Jetadmin to lose communication with the device for a time. Changing a device's IP parameters is a good example. The device (in many cases) re-initializes and stops communicating for a time.

HP Web Jetadmin has several configuration elements that are known to cause device interrupts and, therefore, cause a configuration to become volatile or unstable. These items are programmatically marked in such a way that HP Web Jetadmin always uses them last in a configuration. These configuration items are:

- **Security** > **LDAP - Accessing the Server**
- **Digital Sending** > **Activity Log**
- **Fax** > **Fax Reports and Logs** (print or clear activity log)
- **Security** > **Disable Direct Ports**
- **Network** > **Protocol Stacks**
- **Network** > **IPv4 Information**, which includes **Subnet Mask** and **Gateway** (both single and batch configurations)
- **Wireless** > **802.11 a/b/g**
- **Network** > **Link Setting**
- **File System** > **File System Password**
- **Security** > **Get Community Name**
- **Security** > **Set Community Name**
- **Security** > **SNMP Version Access Control**

In any configuration, whether it is performed for a single device, for multiple devices, or with a configuration template, these settings are always sent to the device last to improve the chance of successful configurations. The following considerations should be made with these settings:

- The chances of a configuration failure increase when these settings are used in the same configuration.
- HP Web Jetadmin only marks these items to run last. HP Web Jetadmin does not put these items in any order relative to the other items listed here.
- Device behaviors, while sometimes predictable, are not fully documented with these known configuration items.

In summary, not all of the HP Web Jetadmin configurations can guarantee a positive and stable result at the physical device. You might need to test individual configuration options to understand the effects on various HP device models and determine if an HP Web Jetadmin configuration is successful. HP will continue best effort practices in documenting these and other known configuration characteristics.

Adding Configuration Templates to a Group Policy

Configuration templates can be added to Group policies. Group policies are a powerful new automation tool that can save you a great deal of time configuring devices and HP Web Jetadmin settings. Any device group can have a property known as Group Policy. One type of group policy is Configure Devices, which uses a selected configuration template from the list of existing templates. The configuration template can be applied either as the device is added into the group or as the device is removed from the group. Multiple Configure Devices Group Policies using different templates can exist on a single device group.

Captured Configurable Options and Configuration Templates

Some configuration options behave differently for single-device configuration than they do for multiple-device configuration. When capturing device settings into a configuration template via the **Save As Template** feature, some configuration options will fail when the template is used to configure multiple devices. The configuration options that will fail when used to configure multiple devices via a stored configuration template are the following:

- Tray Administration
- Authentication Manager
- Control Panel Language
- Default Media Type
- SNMP Trap Destination Table
- Access Control List
- IPv6 Options
- Asset Number
- System Name
- IP Address
- LAA Address Configuration

When capturing device settings via the **Save As Template** feature, these items should remain unchecked. If it is desired to have these configuration options as part of the template, an edit can be performed on the template after it has been saved and the desired configuration option can be selected and configured appropriately. Once the modified template is saved, a version of the configuration option that supports multiple configuration will be used and the operation should succeed. This situation will not occur during normal use of multiple device configuration or when a configuration template is created independently from a device.

Create Configuration Templates

Configuration templates are used to store device settings and apply those settings to one or more devices. This can be done to keep device configurations consistent and to make it easy to apply a common set of settings on a regular basis. Templates are an easy way to change the settings for regularly scheduled configurations, without having to recreate the entire schedule. Templates can also be used to save many settings from a device, either for backup purposes or to apply to similar devices.

Use the following steps to create a configuration template:

1. In the **Device Management** navigation pane, right-click **Configuration**, and then select **Create configuration template**. The **Create Device Configuration Template** wizard starts.
2. On the **Select Template Models** page, select the device models to configure, and then click the right arrow button.
3. Select the network cards to configure, and then click the right arrow button.
4. Click **Next**. The **Specify template options** page appears, listing only the configuration options that apply to the device models and network cards you selected.
5. Enter the name of the template (up to 48 characters).
6. Specify the settings for the configuration options to include in the template, and then click **Next**.

   NOTE: If you click **Back**, any configuration settings you already specified might be lost when you return to the **Specify template options** page. If you remove any device models or network cards on the **Select Template Models** page, some configuration options might not be available when you return to the **Specify template options** page. If you add device models or network cards on the **Select Template Models** page, new configuration options might be available when you return to the **Specify template options** page.

   NOTE: For information about specific configuration options that might not work properly in a batch mode, see Captured Configurable Options and Configuration Templates on page 182.

   NOTE: The configuration options selected for this template will only be applied to those devices that support the options.
7. On the **Confirm** page, verify that the configuration option settings are correct, and then click **Create Template**.
8. On the **Results** page, click the **Done** button.

Create and Use Variable Data

With HP Web Jetadmin 10.4 SR2 or later, templates and OXPd files support variable data.

When creating a configuration template, the following configuration options support variable data:

- Asset Number
- Quick Sets
- LDAP Sign in Setup
- Fax Archiving
- Fax Header Settings
- Outgoing Servers
- Email Address/Message Setting

If the value field for the configuration item displays a blue colored background, then that configuration item can use variable data.

Create user defined fields to store your variable data

If you want to use variable data, you need to create user defined fields to store your variable data. The user defined field can have any name. Use the following steps to create user defined fields:

1. Click **Tools**, and then **Options**.
2. Click **Device Management**, and then click the plus sign to expand **Configuration**, and then click **User Defined**.
3. Click **New** to create a new user defined field.
4. On the **Create User Defined Settings** screen, in the Setting Name field, enter a name.

   For example: `var_DefaultFrom` or `var_DefaultDisplayName`.

   TIP: By starting the variable data name with var_, it's easier to find and identify user defined fields in HP Web Jetadmin.

5. Click **OK**, and then repeat these steps for all the variable fields.

NOTE: Every user defined field uses a unique number in the HP Web Jetadmin database which is invisible to users. If you delete a user defined field and create a new user defined field with the same name, another unique number will be associated with the user defined field. Therefore, you must create the user defined field on one HP Web Jetadmin server, export the user defined field, and then import it on other HP Web Jetadmin servers.

Import the variable data into HP Web Jetadmin

Use the following steps to import variable data:

1. Create a CSV file with the following syntax on the first line:

   ```
   IP Addr,Port,UserDefinedFieldName1,UserDefinedFieldName2
   ```

2. On the lines after that, list the actual values. The Port option is always 1 for network-connected devices.

   ```
   IP Addr,Port,var_DefaultFrom,var_DefaultDisplayName

   10.10.10.10,1,Pfxe.fser@company.com,Peter

   10.10.10.11,1,sdf.cxe@company.com,Sandra
   ```

   NOTE: Instead of IP Addr, you can also use Mac Address or IP Hostname. For more information, see Importing a Configuration from a File on page 172.

   NOTE: HP Web Jetadmin stores the user defined values only in its own database. Nothing gets configured on the device itself.

3. In HP Web Jetadmin, right-click **Configuration** and then select **Configure Devices**.
4. Select **File**, and then **Import**, and then follow the wizard.

Create a template with variables

After identifying the variable configuration options and creating the corresponding user defined fields, create a template and refer to the user defined field as variable data by using one of the following conventions:

- Variable data (a variable in a template always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

  %%<custom variable>%% (where "<custom variable>" is the name of the user defined field)

- Variable data along with a combination of static content before or after the variable

  <static value>%%<custom variable>%%<static value>

-or-

<static value>%%<custom variable>%%

For more information on creating a template, see Create Configuration Templates on page 182.

Using variable data with OXPd files

You can use variable data in the following OXPd files:

- OXPd Device Functions
- OXPd Accessory Records
- OXPd Authentication Agents
- OXPd Statistics Agents
- OXPd Quota Agents

In the following fields:

- Server context ID
- URI
- User name
- Vendor ID (only for OXPd Accessory Records)
- Product ID (only for OXPd Accessory Records)

After creating user defined variables, refer to the user defined fields inside the OXPd file using the following format:

%%<custom variable>%% (where “<custom variable>” is the name of the user defined field)

Example: %%ServerContextID%%

Edit Configuration Templates

Use the following steps to edit a configuration template:

1. In the **Device Management** navigation pane, right-click **Configuration**, and then select **Edit configuration template**. The **Edit Device Configuration Template** wizard starts.
2. On the **Select template** page, select the template, and then click **Next**.
3. On the **Select Template Models** page, change the device models and network cards included in the template, and then click **Next**.

   NOTE: If you change the device models and network cards included in the template, any configuration settings you already specified for the template might be lost. If you remove any device models or network cards, some configuration options might no longer be available. If you add device models or network cards, new configuration options might now be available.

4. On the **Specify template options** page, enter a new name for the template (up to 48 characters).
5. Specify the settings for the configuration options to include in the template, and then click **Next**.

   NOTE: For information about specific configuration options that might not work properly in a batch mode, see Captured Configurable Options and Configuration Templates on page 182.

NOTE: The configuration options selected for this template will only be applied to those devices that support the options.

6. On the **Confirm** page, verify that the configuration option settings are correct, and then click **Save Template**.

7. On the **Results** page, click the **Done** button.

Delete Configuration Templates

Use the following steps to delete a configuration template:

1. In the **Device Management** navigation pane, right-click **Configuration**, and then select **Delete configuration template**. The **Delete Device Configuration Template** wizard starts.

2. Select the template to delete and click **Next**. The **Confirm** page is displayed.

3. Click **Delete Template**. The **Results** page is displayed.

   Click **Done** to display the **Configuration** page.

Copy a Configuration Template

Throughout **Device Management** view, templates can be created and managed to save you time and provide consistency. Templates contain configuration preferences (that vary by template type) and can be applied to devices or groups. Templates are available in **Configuration**, **Alerts**, **Discovery**, **Data Collection**, and **Report Generation**. For more information, see Copy Template Wizard on page 99.

View Configuration Templates

Use the following steps to view a configuration template:

1. In the **Device Management** navigation pane, expand **Configuration**, expand **Templates**, and then select the template. The information about the template is displayed in the workspace.

2. You can view all of the settings for the template. You can also:

   - **Apply**: Apply the selected configuration template to devices (Apply Configuration Templates to Devices on page 186).
   - **Edit**: Make changes to an existing configuration template (Edit Configuration Templates on page 185).
   - **New**: Create a configuration template (Create Configuration Templates on page 182).
   - **Delete**: Delete a configuration template (Delete Configuration Templates on page 186).

Apply Configuration Templates to Devices

When you apply a configuration template, HP Web Jetadmin configures the devices with the settings stored in the template.

The following are the results you can expect when applying a template:

- The template contains configuration options for a single device model or network card.

If you apply the template to a device model or network card that is specified in the template, all the configuration options are valid and HP Web Jetadmin applies the configuration options to the device.

If you apply the template to a device model or network card that is not specified in the template, the results are not guaranteed. Other device models and network cards might not support the configuration options specified in the template. If the device model or network card supports a configuration option specified in the template, HP Web Jetadmin applies that configuration option to the device. If the device model or network card does not support a configuration option specified in the template, HP Web Jetadmin does not apply that configuration option to the device and displays **Not Supported** for that configuration option on the **Results** page.

- The template contains configuration settings for multiple device models and network cards.

  When you apply the template, the results depend on the configuration options specified in the template and the device models and network cards to which you apply the template.

  If the configuration options specified in the template are common to all the device models and network cards specified in the template, HP Web Jetadmin applies all the configuration options when you apply the template to those device models and network cards.

  However, all the configuration options might not be valid for all the device models and network cards specified in the template. For example, assume that the template includes one device model that supports the fax functionality and one device model does not support the fax functionality. If you apply the template to the device model that supports the fax functionality, HP Web Jetadmin applies the fax configuration options specified in the template to the device. If you apply the template to the device model that does not support the fax functionality, HP Web Jetadmin does not apply the fax configuration options specified in the template to the device and displays **Not Supported** for those configuration options on the **Results** page.

To determine if a device model or network card supports the configuration options specified in the template, edit the template. For instructions, see Edit Configuration Templates on page 185. For each configuration option in the template, hold the cursor over the configuration option title. A list of device models and network cards that support that configuration option appears.

Use the following steps to apply a configuration template to devices:

1. In the **Device Management** navigation pane, right-click **Configuration**, and then select **Apply configuration template**. The **Apply Device Configuration Template** wizard starts.

2. Select the configuration template from the drop-down box.

3. If you want to schedule this configuration to run at a later time, select **Schedule configuration**. Click **Next**; the **Select devices** page is displayed.

   NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

   NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

   NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

4. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double

arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

To select an entire group instead of individual devices, change the selection method to **Groups**. Tasks can be performed on a single group or a group and all of its subgroups.

NOTE: If subgroups are included, the task might take longer to complete and network traffic might increase significantly. HP recommends that you include subgroups only when necessary.

If a task is scheduled for a group, the task uses the devices that are in the group when the task starts. If the devices that are in the group are changed, you do not have to delete the scheduled task and create a new scheduled task.

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

5. Review the settings selected. Click **Apply Template**. The **Results** page is displayed.
6. To see details of the configuration, click **Details**. Then click **Close**.

   Click **Done** to display the **Configuration** page.

Alerts

HP Web Jetadmin can detect different events occurring on devices and then relay detailed messages about those events, device states, and other important specifics. These messages can be sent to email addresses or to **Alerts History** within HP Web Jetadmin. For example, error or warning conditions on printers, such as paper out or toner low, can trigger email messages to be sent by HP Web Jetadmin that contain detailed information pertaining to the condition, allowing the recipient to act upon that condition immediately

The advantage of alerts is that you can receive proactive, real-time warnings via email for events that occur on networked printers. Receiving early notification of printer events allows administrators to correct the problems before they impact end user productivity, saving time for both the administrator and the end user. Helpdesks might use alerts to proactively troubleshoot issues with printers before end users detect them. Individuals responsible for ordering consumables, such as toner cartridges, might enable toner low alerts so they can be warned of toner low conditions in order to proactively order toner before it runs out.

Alerts and HP Web Jetadmin

HP Web Jetadmin sends proactive alerts when it detects an event on a device. HP Web Jetadmin determines the appropriate action to take for that event, and then sends a notification through a specified method.
HP Web Jetadmin detects device-based events in one of the following ways:

- Device polling—HP Web Jetadmin always uses polling for the Supplies and Critical alerts.

  HP Web Jetadmin polls devices for Supplies alerts in adaptive intervals based on the rate that the supplies are used.

  HP Web Jetadmin polls devices for Critical alerts at the rate specified for the **Alerts** option. For more information about this option, see Configure the Polling Options for Device Alerts and Supplies Alerts on page 62.

- Traps—Devices send trap packets to HP Web Jetadmin when an event occurs.

  When an alert subscription is created for a device, the IP address for HP Web Jetadmin is configured as the trap destination on the device.

HP Web Jetadmin supports the SNMPv1/SNMPv2c traps and SNMPv3 traps that devices send. There are significant differences in the way that HP Web Jetadmin handles the trap tables for SNMPv1/SNMPv2c and SNMPv3. For more information about these differences, see the *Using Proactive Alerts with HP Web Jetadmin* white paper. This white paper is available from the HP Web Jetadmin support page (in English).

The following features are available for alerts in HP Web Jetadmin:

- An intuitive, easy-to-use interface for subscribing to alerts
- Multiple options for specifying alert subscriptions
- A default template for alert subscriptions
- Alerts for supply events
- Adaptive polling for supply events
- Backup polling
- An alerts history interface

What You Can Do With Alerts

You can use Alerts to have immediate or real-time notification that an event has occurred. A common scenario is a print maintenance or support team. These people would like to know when a problem happens rather than to wait for a customer complaint. In this way, they can proactively handle trouble perhaps even prior to the customer experiencing downtime.

In HP Web Jetadmin, you actually **subscribe** to Alerts to get information about devices. When you subscribe to an Alert, you are requesting information from a device (or devices) about specific settings on that device (or devices) including events, email address notification, and more. (See Create Alert Subscriptions on page 192.)

Types of Alerts

There are three types of Alerts:

- **General alerts (detailed)**: Include most non-supply device events and rely on traps. Polling is established when traps destinations cannot be configured.
- **Supplies alerts**: Monitor device supply status and levels through polling. The polling mechanism uses a combination of slow-polling and sliding time interval depending on the level of the supply being monitored.
- **Critical alerts**: Events are monitored by polling every five minutes. The polling interval is configurable within the range of 5 to 360 minutes. Because of the frequent polling nature of this solution, it is important to use it sparingly and only for devices that need immediate attention. All General Alerts are available.

Examples of Alerts

Following are some examples of alerts you might want to configure:

- An alert that is set to add an event to the alert history when a specific printer error occurs.

NOTE: Alerts now support more detailed printer errors such as “Subsystem 72 -- Service Error” and more.

- An alert set to notify a recipient through email about a Toner Low condition.
- An alert set to notify a recipient through email about a specific supply threshold.
- An alert set to propagate an SNMP trap directed at a listener process on another application such as HP OpenView.

Alerts Traps Listener Port

HP Web Jetadmin uses UDP port 27892 as the traps listener port for alerts and any reports that are based on by-user collections.

Alerts - Common Tasks Task Module

The **Alerts - Common Tasks** task module provides links that initiate the following tasks for alerts:

- Subscribe to alerts for devices
- Create an alert subscription template
- Apply an alert subscription template to devices
- Edit an alert subscription template
- Delete an alert subscription template
- Copy an alert subscription template to create a new template

Alerts - Recent Alerts Task Module

The **Alerts - Recent Alerts** task module provides a list of the alerts that have occurred. Use this task module to view the alerts history.

Alerts - Alert Subscriptions Task Module

The **Alerts - Alert Subscriptions** task module provides the following information:

- The number of devices that are subscribed for alerts
- The number of devices that are not subscribed for alerts
- The number of discovered devices

Use this task module to display a list of the alert subscriptions that have been created or subscribe to alerts for devices.

Alerts - Subscription Templates Task Module

The **Alerts - Subscription Templates** task module provides a list of the default alert subscription templates and the custom alert subscription templates that have been created. Use this task module to perform the following tasks:

- Create an alert subscription template
- Apply an alert subscription template to devices
- Edit the settings for an alert subscription template
- Delete an alert subscription template
- Copy an alert subscription template to create a new template
- View the settings for an alert subscription template

Alerts - Active Tasks Task Module

The **Alerts - Active Tasks** task module provides a list of the alert tasks that are running. Use this task module to stop or view the status of an active alert task.

Related Application Options for Alerts

Configuration settings can be stored here for managing alerts:

- Attach the Supplies Report to the Email Notifications for Supply Alerts on page 78
- Configure the Polling Options for Device Alerts and Supplies Alerts on page 62
- Manage the Custom Email Templates on page 78
- Manage the Templates for Alert Subscriptions on page 79
- Configure the Format for SNMP Traps on page 80

Managing Device Alerts

When alerts have been configured for a device, they are entered on a **Trap Table**. (Traps are set only on General alerts, see Create Alert Subscriptions on page 192). Depending on the device, the trap table will contain up to 3, 6, or 12 for that device. HP Web Jetadmin will not automatically overwrite any traps in the table. When a **Trap Table** is full, the **Edit trap table settings** dialog box is displayed, which lets you manage the alerts for that device. You can:

- **Remove all trap table settings**: Removes all traps from the table and allows new ones to be added.
- **Remove selected trap table settings**: Removes selected traps from the table and allows new ones to be added.
- **Skip this device**: Leaves the trap table full so new alerts will not be added for this device.

The **Edit trap table settings** dialog box will be displayed within HP Web Jetadmin as soon as the **Trap Table** for the device becomes full. If alerts were set up with a schedule, with a Group Policies on page 123, or for Device Utilization by User and Data Collections on page 226, the **Edit trap table settings** dialog box will be accessible through the Alerts - Active Tasks Task Module on page 191 so that you can take action on them at your convenience.

Create Alert Subscriptions

An alert subscription defines the following information:

- The type of alerts that HP Web Jetadmin monitors
- The devices that HP Web Jetadmin monitors for the alerts
- The specific events that HP Web Jetadmin monitors
- The type of notifications that HP Web Jetadmin sends when the events occur

HP Web Jetadmin always displays alerts in the alert history. When the **Log to File** option is enabled, HP Web Jetadmin also writes alerts to the alerts log file. For more information about the alerts log file, see Configure the Settings for the Alerts Log on page 79.

Create an alert subscription by using an alert subscription template

1. In the **Device Management** navigation pane, right-click **Alerts**, and then select **Subscribe**. The **Create Alert Subscription** wizard starts.

2. On the **Specify alerts subscription type** page, select the **Use Template** option, select the alert subscription template from the list, and then click the **Next** button.

3. To select individual devices, use the following steps:

   a. Select the **Devices** option.

   b. To change the list of devices, click the **...** button next to the **Source** box, and then select the device list.

   c. Select the devices from the list, and then click the **>** button.

   d. Click the **Next** button. Continue with step 4.

   -or-

   To select a group of devices, use the following steps:

   a. Select the **Groups** option.

   b. Click the **...** button next to the **Group** box, and then select the group.

   c. To include the subgroups that are in the selected group, select the **Include subgroups** checkbox.

   IMPORTANT: If subgroups are included, network traffic might increase significantly. HP recommends that you include subgroups only when necessary.

   d. Click the **Next** button. Continue with step 4.

4. To link the selected alert subscription template to this alert subscription, select the **Link template to subscription** option. Changes that are made to the selected alert subscription template are automatically applied to the devices that are associated with this alert subscription.

   -or-

   To create an alert subscription that is not linked to the selected alert subscription template, select the **Do NOT link template to subscription** option, and then enter a name for this alert subscription in the **Subscription name** box. Changes that are made to the alert subscription template are not applied to the devices that were previously configured with this alert subscription template.

5. Click the **Next** button.

6. On the **Confirm** page, verify that the information is correct, and then click the **Apply Template** button.

7. On the **Progress** page, click the **Details** button. Review the alerts for each device, and then click the **Close** button.

8. If HP Web Jetadmin has stored the maximum number of alerts for any of the selected devices, the **Edit trap table settings** window opens. For more information about this window, see Manage the trap table on page 196.

9. On the **Results** page, click the **Done** button.

Create an alert subscription by specifying the alert settings

1. In the **Device Management** navigation pane, right-click **Alerts**, and then select **Subscribe**. The **Create Alert Subscription** wizard starts.

2. On the **Specify alerts subscription type** page, select the **Specify Settings** option.

3. Select one of the following options, and then click the **Next** button:

   - **General alerts (detailed)**—HP Web Jetadmin monitors the devices for non-supply events and relies on SNMP traps. HP Web Jetadmin establishes polling when the SNMP trap destination cannot be configured.

   - **Supplies alerts**—HP Web Jetadmin monitors the devices for supply statuses and levels and relies on polling. The polling mechanism uses a combination of slow-polling and a sliding-time interval depending on the level of the supply being monitored.

   - **Critical alerts**—HP Web Jetadmin monitors the devices for specific events by polling the devices every 5 minutes. The polling interval can be configured in the range of 5 to 360 minutes. HP recommends that you use this option sparingly and only for devices that need immediate attention because the polling frequency can significantly increase network traffic.

   NOTE: HP Web Jetadmin establishes polling when the SNMP trap destination cannot be configured. This polling rate is configurable, For more information see: Configure the Polling Options for Device Alerts and Supplies Alerts on page 62.

4. To select individual devices, use the following steps:

   a. Select the **Devices** option.

   b. To change the list of devices, click the **...** button next to the **Source** box, and then select the device list.

   c. Select the devices from the list, and then click the **>** button.

   d. Click the **Next** button. Continue with step 5.

   -or-

   To select a group of devices, use the following steps:

   a. Select the **Groups** option.

   b. Click the **...** button next to the **Group** box, and then select the group.

   c. To include the subgroups that are in the selected group, select the **Include subgroups** checkbox.

      IMPORTANT: If subgroups are included, network traffic might increase significantly. HP recommends that you include subgroups only when necessary.

   d. Click the **Next** button. Continue with step 5.

5. If the **General alerts (detailed)** or **Critical alerts** option was selected, use the following steps:

   a. On the **Select alerts** page, select the checkboxes for the alerts to monitor, and then click the **Next** button.

   b. To choose not to configure the advanced settings, select the **No advanced settings** option.

      -or-

      To prevent HP Web Jetadmin from sending duplicate alerts for a specific period of time, use the following steps:

      i. Select the **Time to ignore duplicate alerts** option. This setting applies only to this alert subscription.

      ii. In the **Ignore duplicates for** boxes, enter the amount of time that HP Web Jetadmin waits before sending a duplicate alert.

      iii. To specify that HP Web Jetadmin ignores the first occurrence of the time period configured for the **Ignore duplicates for** option, select the **Ignore first time period** checkbox.

      -or-

      To send alerts when a threshold is exceeded, select the **Count threshold (if applicable)** option, and then enter the threshold value in the **Send alert when value exceeds** box. For example, if a threshold of `5000` is specified for the **Page Count** alert, HP Web Jetadmin sends an alert from each monitored device when it prints page 5,001.

   c. Click the **Next** button. Continue with step 6.

   -or-

   If the **Supplies alerts** option was selected, use the following steps:

   a. On the **Select supplies categories** page, select the check boxes for the supply alerts to monitor, and then click the **Next** button.

   b. To specify a supply threshold, select the **Threshold value (early warning, low, very low)** option, and then enter the threshold value in the box. The threshold is a decrementing value. When a supply reaches the threshold, HP Web Jetadmin sends an alert.

      -or-

      To specify that HP Web Jetadmin sends an alert when the supply level increases significantly from the current level, select the **Replaced** option.

   c. Click the **Next** button. Continue with step 6.

6. To only write alerts to the alert history log, select the **Alert history only** option, and then click the **Next** button. Continue with step 7.

   -or-

   To send email notifications when alerts occur, use the following steps:

   IMPORTANT: SMTP must be configured to send email notifications. For more information, see Configure the SMTP Gateway Settings on page 47.

a. Select the **Email** option, and then click the **Next** button.

b. In the **Send to** box, enter the email addresses of the recipients separated with a semi-colon (;).

-or-

Click the **Browse** button. On the **Select Email Address** window, select the email addresses from the **Available addresses** list, and then click the **>** button. Click the **OK** button.

TIP: To manage the list of email addresses, click the **Manage list** button. The **Options** window opens with the **Addresses** option selected. For more information, see Manage the Shared Email Addresses on page 48.

c. To include a short description of the alert in the message, select the **Concise** option.

-or-

To include a more detailed description of the alert in the message, select the **Verbose** option.

-or-

To use an email template for the message, select the **Custom** option, and then select the template from the list.

TIP: To create an email template, click the **New** button. The **Options** window opens with the **Email Templates** option selected. For more information, see Manage the Custom Email Templates on page 78.

d. To send the alert information in the body of the email and as an attachment to the email, select the **Also send the email body as an attachment** checkbox.

e. Click the **Next** button. Continue with step 7.

-or-

To forward SNMP traps to a server when alerts occur, use the following steps:

a. Select the **SNMP trap generator** option, and then click the **Next** button.

b. In the **Trap destination** box, enter the IP address or fully qualified domain name of the server where HP Web Jetadmin forwards the SNMP traps.

c. In the **Listen port** box, enter the port on which the server listens for SNMP traps.

d. From the **SNMP version** list, select the version of SNMP that HP Web Jetadmin uses for the traps.

e. If **SNMPv1** or **SNMP v2** is selected from the **SNMP version** list, enter a community name for the trap in the **Community** box.

-or-

If **SNMPv3** is selected from the **SNMP version** list, use the following steps:

NOTE: For SNMPv3, HP Web Jetadmin sends an inform notification to the server instead of a trap notification. The server sends an acknowledgement to HP Web Jetadmin when the inform notification is received. If HP Web Jetadmin does not receive an acknowledgement within a specified timeout interval, HP Web Jetadmin resends the inform notification. For more information about configuring the SNMPv3 timeout interval and number of retries, see Configure the SNMP Settings on page 46.

i. In the **User name** box, enter the user name.

ii. In the **Context name** box, enter a context name, such as *public*.

iii. From the **Authentication protocol** list, select the protocol.

iv. In the **Authentication password** and **Confirm authentication password** boxes, enter the authentication password.

v. From the **Privacy protocol** list, select the protocol.

vi. In the **Privacy password** and **Confirm privacy password** boxes, enter the privacy password.

f. From the **Preferred language** list, select the language that HP Web Jetadmin uses for the SNMP traps.

g. To change the format for the SNMP traps, click the **Edit** button. The **Options** window opens with the **SNMP Trap Generator** option selected. For more information about the SNMP trap format, see Configure the Format for SNMP Traps on page 80.

h. Click the **Next** button. Continue with step 7.

7. On the **Specify subscription name** page, enter a name for the alert subscription, and then click the **Next** button.
8. On the **Confirm** page, verify that the information is correct, and then click the **Subscribe** button.
9. On the **Progress** page, click the **Details** button. Review the alerts for each device, and then click the **Close** button.
10. If HP Web Jetadmin has stored the maximum number of alerts for any of the selected devices, the **Edit trap table settings** window opens. For more information about this window, see Manage the trap table on page 196.
11. On the **Results** page, click the **Done** button.

Manage the trap table

1. On the **Edit trap table settings** window, select a device from the list.
2. To remove all of the traps from the table, select the **Remove all trap table settings** option. HP Web Jetadmin can add new traps to the table for this device.

   -or-

   To remove a specific trap from the table, select the trap from the **Trap table settings** section, and then select the **Remove selected trap table settings** option. HP Web Jetadmin can add new traps to the table for this device.

   -or-

   To leave all of the traps in the table, select the **Skip this device** option. HP Web Jetadmin cannot add new traps to the table for this device.
3. Click the **Activate Choice for Device** button.
4. Repeat steps 1 through 3 for each device in the list.
5. Click the **Finish** button.

Edit Alert Subscriptions

The settings for an alert subscription can be changed, including the name of the alert subscription.

Edit an alert subscription

1. In the **Device Management** navigation pane, expand the **Alerts** option, and then select **All Subscriptions**.

2. In the **All Subscriptions** pane, select the alert subscription from the list, and then click the **Edit Subscription** button. The **Edit Subscription** wizard starts.

3. If the alert subscription is configured for **General alerts (detailed)** or **Critical alerts**, use the following steps:

   a. On the **Progress** page, select or clear the check boxes for the alerts to monitor, and then click the **Next** button.

   b. To choose not to configure the advanced settings, select the **No advanced settings** option.

      -or-

      To prevent HP Web Jetadmin from sending duplicate alerts for a specific period of time, use the following steps:

      i. Select the **Time to ignore duplicate alerts** option. This setting applies only to this alert subscription.

      ii. In the **Ignore duplicates for** boxes, enter the amount of time that HP Web Jetadmin waits before sending a duplicate alert.

      iii. To specify that HP Web Jetadmin ignores the first occurrence of the time period configured for the **Ignore duplicates for** option, select the **Ignore first time period** checkbox.

      -or-

      To send alerts when a threshold is exceeded, select the **Count threshold (if applicable)** option, and then enter the threshold value in the **Send alert when value exceeds** box. For example, if a threshold of `5000` is specified for the **Page Count** alert, HP Web Jetadmin sends an alert from each monitored device when it prints page 5,001.

   c. Click the **Next** button. Continue with step 4.

   -or-

   If the alert subscription is configured for **Supplies alerts**, use the following steps:

   a. On the **Progress** page, select or clear the check boxes for the supply alerts to monitor, and then click the **Next** button.

   b. To specify a supply threshold, select the **Threshold value (early warning, low, very low)** option, and then enter the threshold value in the box. The threshold is a decrementing value. When a supply reaches the threshold, HP Web Jetadmin sends an alert.

      -or-

      To specify that HP Web Jetadmin sends an alert when the supply level increases significantly from the current level, select the **Replaced** option.

   c. Click the **Next** button. Continue with step 4.

4. To only write alerts to the alert history log, select the **Alert history only** option, and then click the **Next** button. Continue with step 5.

   -or-

   To send email notifications when alerts occur, use the following steps:

   IMPORTANT: SMTP must be configured to send email notifications. For more information, see Configure the SMTP Gateway Settings on page 47.

a. Select the **Email** option, and then click the **Next** button.

b. In the **Send to** box, enter the email addresses of the recipients separated with a semi-colon (;).

-or-

Click the **Browse** button. On the **Select Email Address** window, select the email addresses from the **Available addresses** list, and then click the **>** button. Click the **OK** button.

TIP: To manage the list of email addresses, click the **Manage list** button. The **Options** window opens with the **Addresses** option selected. For more information, see Manage the Shared Email Addresses on page 48.

c. To include a short description of the alert in the message, select the **Concise** option.

-or-

To include a more detailed description of the alert in the message, select the **Verbose** option.

-or-

To use an email template for the message, select the **Custom** option, and then select the template from the list.

TIP: To create an email template, click the **New** button. The **Options** window opens with the **Email Templates** option selected. For more information, see Manage the Custom Email Templates on page 78.

d. To send the alert information in the body of the email and as an attachment to the email, select the **Also send the email body as an attachment** checkbox.

e. Click the **Next** button. Continue with step 5.

-or-

To forward SNMP traps to a server when alerts occur, use the following steps:

a. Select the **SNMP trap generator** option, and then click the **Next** button.

b. In the **Trap destination** box, enter the IP address or fully qualified domain name of the server where HP Web Jetadmin forwards the SNMP traps.

c. In the **Listen port** box, enter the port on which the server listens for SNMP traps.

d. From the **SNMP version** list, select the version of SNMP that HP Web Jetadmin uses for the traps.

e. If **SNMPv1** or **SNMP v2** is selected from the **SNMP version** list, enter a community name for the trap in the **Community** box.

-or-

If **SNMPv3** is selected from the **SNMP version** list, use the following steps:

NOTE: For SNMPv3, HP Web Jetadmin sends an inform notification to the server instead of a trap notification. The server sends an acknowledgement to HP Web Jetadmin when the inform notification is received. If HP Web Jetadmin does not receive an acknowledgement within a specified timeout interval, HP Web Jetadmin resends the inform notification. For more information about configuring the SNMPv3 timeout interval and number of retries, see Configure the SNMP Settings on page 46.

i. In the **User name** box, enter the user name.

ii. In the **Context name** box, enter a context name, such as *public*.

iii. From the **Authentication protocol** list, select the protocol.

        iv. In the **Authentication password** and **Confirm authentication password** boxes, enter the authentication password.

        v. From the **Privacy protocol** list, select the protocol.

        vi. In the **Privacy password** and **Confirm privacy password** boxes, enter the privacy password.

    f. From the **Preferred language** list, select the language that HP Web Jetadmin uses for the SNMP traps.

    g. To change the format for the SNMP traps, click the **Edit** button. The **Options** window opens with the **SNMP Trap Generator** option selected. For more information about the SNMP trap format, see Configure the Format for SNMP Traps on page 80.

    h. Click the **Next** button. Continue with step 5.

5. On the **Specify subscription name** page, enter a new name for the alert subscription, and then click the **Next** button.
6. On the **Confirm** page, verify that the information is correct, and then click the **Edit Subscription** button.
7. On the **Progress** page, click the **Details** button. Review the alerts for each device, and then click the **Close** button.
8. If HP Web Jetadmin has stored the maximum number of alerts for any of the selected devices, the **Edit trap table settings** window opens. For more information about this window, see Manage the trap table on page 199.
9. On the **Results** page, click the **Done** button.

Manage the trap table

1. On the **Edit trap table settings** window, select a device from the list.
2. To remove all of the traps from the table, select the **Remove all trap table settings** option. HP Web Jetadmin can add new traps to the table for this device.

   -or-

   To remove a specific trap from the table, select the trap from the **Trap table settings** section, and then select the **Remove selected trap table settings** option. HP Web Jetadmin can add new traps to the table for this device.

   -or-

   To leave all of the traps in the table, select the **Skip this device** option. HP Web Jetadmin cannot add new traps to the table for this device.
3. Click the **Activate Choice for Device** button.
4. Repeat steps 1 through 3 for each device in the list.
5. Click the **Finish** button.

Copy an Alert Subscription Template

Throughout **Device Management** view, templates can be created and managed to save you time and provide consistency. Templates contain configuration preferences (that vary by template type) and can be applied to devices or groups. Templates are available in **Configuration**, **Alerts**, **Discovery**, **Data Collection**, and **Report Generation**. For more information, see Copy Template Wizard on page 99.

Alert History

The following information is available in the alert history:

- **Time Received**—The time that the device received the alert.
- **Alert**—The name of the alert.

NOTE: Job Completed alerts are not saved in the database and displayed in the **Alert** column because these alerts consume too much space in the database.

- **Device Model**—The model of the device that received the alert.
- **IP Hostname**—The IP hostname of the device that received the alert.
- **IP Address**—The IP address of the device that received the alert.

Use the following steps to view the alert history:

1. In the **Device Management** navigation pane, right-click **Alerts**, and then select **View alerts history**.
2. Click the **Close** button.

Alert Subscription Templates

You can view Alert templates (including the default template) and also do any of the following actions:

- Apply an Alert Subscription Template on page 204
- Create Alert Subscription Templates on page 200
- Delete an Alert Subscription Template on page 208
- Edit Alert Subscription Templates on page 205

Use the following steps to view an alert subscription:

1. Expand the **Alerts** tree in the left navigation pane and then expand **Templates** to list all Alert templates. Click on the template you want to view. The specific template detail is displayed.
2. You can do any of the following:
   - **Apply**: Apply the template to devices (Apply an Alert Subscription Template on page 204).
   - **Edit**: Make changes to the template (Edit Alert Subscription Templates on page 205).

Alert Templates in Group Policies

The **Groups Policy** features is a powerful new automation tool that saves users a great deal of time configuring devices and HP Web Jetadmin settings. Both Automatic and Manual type groups can have the Group Policy property. One policy that can be added to any device group's properties is Alerts. Both Subscribe and Unsubscribe using Alert templates can be applied to devices in the group either as they are populated into group membership or as they are removed from group membership. In this way, devices can have specific Alerts applied or de-applied without impact to other Alerts settings. (See Group Policies on page 123.)

Create Alert Subscription Templates

An alert subscription template defines the following information:

- The type of alerts that HP Web Jetadmin monitors
- The devices that HP Web Jetadmin monitors for the alerts
- The specific events that HP Web Jetadmin monitors
- The type of notifications that HP Web Jetadmin sends when the events occur

Alert subscription templates can be used to apply the same setting to multiple alert subscriptions. If an alert subscription template is linked to an alert subscription, any changes that are made to the alert subscription template are automatically applied to the devices that are associated with the alert subscription

The Default Alert Template is preconfigured when HP Web Jetadmin is installed. The Default Alert Template specifies several alerts in the Media Path, Service, and Supplies categories

HP Web Jetadmin always displays alerts in the alert history. When the **Log to File** option is enabled, HP Web Jetadmin also writes alerts to the alerts log file. For more information about the alerts log file, see Configure the Settings for the Alerts Log on page 79.

Use the following steps to create an alert subscription template:

1. In the **Device Management** navigation pane, right-click **Alerts**, and then select **Create subscription template**. The **Create Alert Subscription Template** wizard starts.
2. On the **Specify alerts subscription type** page, select one of the following options, and then click the **Next** button:
   - **General alerts (detailed)**—HP Web Jetadmin monitors the devices for non-supply events and relies on SNMP traps. HP Web Jetadmin establishes polling when the SNMP trap destination cannot be configured.
   - **Supplies alerts**—HP Web Jetadmin monitors the devices for supply statuses and levels and relies on polling. The polling mechanism uses a combination of slow-polling and a sliding-time interval depending on the level of the supply being monitored.
   - **Critical alerts**—HP Web Jetadmin monitors the devices for specific events by polling the devices every 5 minutes. The polling interval can be configured in the range of 5 to 360 minutes. HP recommends that you use this option sparingly and only for devices that need immediate attention because the polling frequency can significantly increase network traffic.
3. If the **General alerts (detailed)** or **Critical alerts** option was selected, use the following steps:
   a. On the **Select alerts** page, select the checkboxes for the alerts to monitor, and then click the **Next** button.

   b. To choose not to configure the advanced settings, select the **No advanced settings** option.

   -or-

   To prevent HP Web Jetadmin from sending duplicate alerts for a specific period of time, use the following steps:

i. Select the **Time to ignore duplicate alerts** option. This setting applies only to this alert subscription template.

ii. In the **Ignore duplicates for** boxes, enter the amount of time that HP Web Jetadmin waits before sending a duplicate alert.

iii. To specify that HP Web Jetadmin ignores the first occurrence of the time period configured for the **Ignore duplicates for** option, select the **Ignore first time period** checkbox.

-or-

To send alerts when a threshold is exceeded, select the **Count threshold (if applicable)** option, and then enter the threshold value in the **Send alert when value exceeds** box. For example, if a threshold of `5000` is specified for the **Page Count** alert, HP Web Jetadmin sends an alert from each monitored device when it prints page 5,001.

c. Click the **Next** button. Continue with step 4.

-or-

If the **Supplies alerts** option was selected, use the following steps:

a. On the **Select supplies categories** page, select the check boxes for the supply alerts to monitor, and then click the **Next** button.

b. To specify a supply threshold, select the **Threshold value (early warning, low, very low)** option, and then enter the threshold value in the box. The threshold is a decrementing value. When a supply reaches the threshold, HP Web Jetadmin sends an alert.

-or-

To specify that HP Web Jetadmin sends an alert when the supply level increases significantly from the current level, select the **Replaced** option.

c. Click the **Next** button. Continue with step 4.

4. To only write alerts to the alert history log, select the **Alert history only** option, and then click the **Next** button. Continue with step 5.

-or-

To send email notifications when alerts occur, use the following steps:

IMPORTANT: SMTP must be configured to send email notifications. For more information, see Configure the SMTP Gateway Settings on page 47.

a. Select the **Email** option, and then click the **Next** button.

b. In the **Send to** box, enter the email addresses of the recipients separated with a semi-colon (;).

-or-

Click the **Browse** button. On the **Select Email Address** window, select the email addresses from the **Available addresses** list, and then click the **>** button. Click the **OK** button.

TIP: To manage the list of email addresses, click the **Manage list** button. The **Options** window opens with the **Addresses** option selected. For more information, see Manage the Shared Email Addresses on page 48.

c. To include a short description of the alert in the message, select the **Concise** option.

-or-

To include a more detailed description of the alert in the message, select the **Verbose** option.

-or-

To use an email template for the message, select the **Custom** option, and then select the template from the list.

> 💡 TIP: To create an email template, click the **New** button. The **Options** window opens with the **Email Templates** option selected. For more information, see Manage the Custom Email Templates on page 78.

d. To send the alert information in the body of the email and as an attachment to the email, select the **Also send the email body as an attachment** checkbox.

e. Click the **Next** button. Continue with step 5.

-or-

To forward SNMP traps to a server when alerts occur, use the following steps:

a. Select the **SNMP trap generator** option, and then click the **Next** button.

b. In the **Trap destination** box, enter the IP address or fully qualified domain name of the server where HP Web Jetadmin forwards the SNMP traps.

c. In the **Listen port** box, enter the port on which the server listens for SNMP traps.

d. From the **SNMP version** list, select the version of SNMP that HP Web Jetadmin uses for the traps.

e. If **SNMPv1** or **SNMP v2** is selected from the **SNMP version** list, enter a community name for the trap in the **Community** box.

-or-

If **SNMPv3** is selected from the **SNMP version** list, use the following steps:

> 📝 NOTE: For SNMPv3, HP Web Jetadmin sends an inform notification to the server instead of a trap notification. The server sends an acknowledgement to HP Web Jetadmin when the inform notification is received. If HP Web Jetadmin does not receive an acknowledgement within a specified timeout interval, HP Web Jetadmin resends the inform notification. For more information about configuring the SNMPv3 timeout interval and number of retries, see Configure the SNMP Settings on page 46.

i. In the **User name** box, enter the user name.

ii. In the **Context name** box, enter a context name, such as *public*.

iii. From the **Authentication protocol** list, select the protocol.

iv. In the **Authentication password** and **Confirm authentication password** boxes, enter the authentication password.

v. From the **Privacy protocol** list, select the protocol.

vi. In the **Privacy password** and **Confirm privacy password** boxes, enter the privacy password.

f. From the **Preferred language** list, select the language that HP Web Jetadmin uses for the SNMP traps.

g. To change the format for the SNMP traps, click the **Edit** button. The **Options** window opens with the **SNMP Trap Generator** option selected. For more information about the SNMP trap format, see Configure the Format for SNMP Traps on page 80.

h. Click the **Next** button. Continue with step 5.

5. On the **Alerts template name** page, enter a name for the alert subscription template, and then click the **Next** button.

6. On the **Confirm** page, verify that the information is correct, and then click the **Create Template** button.

7. On the **Results** page, click the **Done** button.

Apply an Alert Subscription Template

After an alert template has been created, you can specify devices to use it with (Create Alert Subscription Templates on page 200). When applying a template to devices, you can choose to have the devices:

- **Link template to subscription**: Any changes made to the template will automatically affect any devices associated with this template.

- **Do NOT link template to subscription**: Changes made to this template will not affect the devices associated with it. This is used to apply the template settings as a new subscription without linking that subscription in any way to the original template.

Alert templates create an alerts subscription on the devices to which they were applied. Any time a new template is applied, a new alerts subscription is created on those devices.

Use the following steps to apply an alert subscription template:

1. Expand the **Alerts** tree in the left navigation pane. In the **Alerts - Common Tasks** task module, select **Apply subscription template**. The **Select template** page is displayed with all alert subscription templates in alphabetical order.

2. Highlight the template and click **Next**. The **Select devices** page displayed.

3. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

   To select an entire group instead of individual devices, change the selection method to **Groups**. Tasks can be performed on a single group or a group and all of its subgroups.

   NOTE: If subgroups are included, the task might take longer to complete and network traffic might increase significantly. HP recommends that you include subgroups only when necessary.

   If a task is scheduled for a group, the task uses the devices that are in the group when the task starts. If the devices that are in the group are changed, you do not have to delete the scheduled task and create a new scheduled task.

   Click **Next**. The **Specify link options** page is displayed.

4. Select the way you want to be notified about alerts:

   - **Link template to subscription**: Any changes made to the template will automatically affect any devices associated with this template.

   - **Do NOT link template to subscription**: Changes made to this template will not affect the devices associated with it. In effect, you are just using the settings from the template and then saving them under a different name for the device just added. You must enter that different name for the subscription.

   Click **Next**.

5. The **Confirm** page is displayed. Click **Apply Template**.

6. To see details about the alerts, click **Details**; to see details about the alerts for each device, click **Expand All**. When done, click **Close**; the **Results** page is displayed.

7. Click **Done**.

Edit Alert Subscription Templates

The settings for an alert subscription template can be changed, including the name of the alert subscription template.

If an alert subscription template is linked to an alert subscription, any changes that are made to the alert subscription template are automatically applied to the devices that are associated with that alert subscription.

HP Web Jetadmin always displays alerts in the alert history. When the **Log to File** option is enabled, HP Web Jetadmin also writes alerts to the alerts log file. For more information about the alerts log file, see Configure the Settings for the Alerts Log on page 79.

Use the following steps to edit an alert subscription template:

1. In the **Device Management** navigation pane, expand the **Alerts** option, and then select **Templates**.

2. In the **Alerts - Subscription Templates** pane, select the alert subscription template from the list, and then click the **Edit** button. The **Edit Subscription Template** wizard starts.

3. If the alert subscription template is configured for **General alerts (detailed)** or **Critical alerts**, use the following steps:

   a. On the **Select alerts** page, select or clear the check boxes for the alerts to monitor, and then click the **Next** button.

   b. To choose not to configure the advanced settings, select the **No advanced settings** option.

      -or-

      To prevent HP Web Jetadmin from sending duplicate alerts for a specific period of time, use the following steps:

      i. Select the **Time to ignore duplicate alerts** option. This setting applies only to this alert subscription.

      ii. In the **Ignore duplicates for** boxes, enter the amount of time that HP Web Jetadmin waits before sending a duplicate alert.

      iii. To specify that HP Web Jetadmin ignores the first occurrence of the time period configured for the **Ignore duplicates for** option, select the **Ignore first time period** checkbox.

      -or-

      To send alerts when a threshold is exceeded, select the **Count threshold (if applicable)** option, and then enter the threshold value in the **Send alert when value exceeds** box. For example, if a threshold of `5000` is specified for the **Page Count** alert, HP Web Jetadmin sends an alert from each monitored device when it prints page 5,001.

   c. Click the **Next** button. Continue with step 4.

   -or-

   If the alert subscription template is configured for **Supplies alerts**, use the following steps:

a. On the **Select supplies categories** page, select or clear the check boxes for the supply alerts to monitor, and then click the **Next** button.

b. To specify a supply threshold, select the **Threshold value (early warning, low, very low)** option, and then enter the threshold value in the box. The threshold is a decrementing value. When a supply reaches the threshold, HP Web Jetadmin sends an alert.

   -or-

   To specify that HP Web Jetadmin sends an alert when the supply level increases significantly from the current level, select the **Replaced** option.

c. Click the **Next** button. Continue with step 4.

4. To only write alerts to the alert history log, select the **Alert history only** option, and then click the **Next** button. Continue with step 5.

   -or-

   To send email notifications when alerts occur, use the following steps:

   IMPORTANT: SMTP must be configured to send email notifications. For more information, see Configure the SMTP Gateway Settings on page 47.

   a. Select the **Email** option, and then click the **Next** button.

   b. In the **Send to** box, enter the email addresses of the recipients separated with a semi-colon (;).

      -or-

      Click the **Browse** button. On the **Select Email Address** window, select the email addresses from the **Available addresses** list, and then click the **>** button. Click the **OK** button.

      TIP: To manage the list of email addresses, click the **Manage list** button. The **Options** window opens with the **Addresses** option selected. For more information, see Manage the Shared Email Addresses on page 48.

   c. To include a short description of the alert in the message, select the **Concise** option.

      -or-

      To include a more detailed description of the alert in the message, select the **Verbose** option.

      -or-

      To use an email template for the message, select the **Custom** option, and then select the template from the list.

      TIP: To create an email template, click the **New** button. The **Options** window opens with the **Email Templates** option selected. For more information, see Manage the Custom Email Templates on page 78.

   d. To send the alert information in the body of the email and as an attachment to the email, select the **Also send the email body as an attachment** checkbox.

   e. Click the **Next** button. Continue with step 5.

   -or-

   To forward SNMP traps to a server when alerts occur, use the following steps:

a. Select the **SNMP trap generator** option, and then click the **Next** button.

b. In the **Trap destination** box, enter the IP address or fully qualified domain name of the server where HP Web Jetadmin forwards the SNMP traps.

c. In the **Listen port** box, enter the port on which the server listens for SNMP traps.

d. From the **SNMP version** list, select the version of SNMP that HP Web Jetadmin uses for the traps.

e. If **SNMPv1** or **SNMP v2** is selected from the **SNMP version** list, enter a community name for the trap in the **Community** box.

   -or-

   If **SNMPv3** is selected from the **SNMP version** list, use the following steps:

   NOTE: For SNMPv3, HP Web Jetadmin sends an inform notification to the server instead of a trap notification. The server sends an acknowledgement to HP Web Jetadmin when the inform notification is received. If HP Web Jetadmin does not receive an acknowledgement within a specified timeout interval, HP Web Jetadmin resends the inform notification. For more information about configuring the SNMPv3 timeout interval and number of retries, see Configure the SNMP Settings on page 46.

   i. In the **User name** box, enter the user name.

   ii. In the **Context name** box, enter a context name, such as *public*.

   iii. From the **Authentication protocol** list, select the protocol.

   iv. In the **Authentication password** and **Confirm authentication password** boxes, enter the authentication password.

   v. From the **Privacy protocol** list, select the protocol.

   vi. In the **Privacy password** and **Confirm privacy password** boxes, enter the privacy password.

f. From the **Preferred language** list, select the language that HP Web Jetadmin uses for the SNMP traps.

g. To change the format for the SNMP traps, click the **Edit** button. The **Options** window opens with the **SNMP Trap Generator** option selected. For more information about the SNMP trap format, see Configure the Format for SNMP Traps on page 80.

h. Click the **Next** button. Continue with step 5.

5. On the **Specify name** page, enter a new name for the alert subscription template, and then click the **Next** button.

6. On the **Confirm** page, verify that the information is correct, and then click the **Save Template** button.

7. On the **Results** page, click the **Done** button.

Import and Export Alert Templates

In an environment that has multiple instances of HP Web Jetadmin, you can create device alert templates in one instance, and then import them into the instances that are running on different servers. However, to import device alert templates, each server must run the same version of HP Web Jetadmin.

Use the following steps to export device alert templates:

1. In the **Device Management** navigation pane, expand the **Alerts** option.
2. To export multiple templates, right-click **Templates**, and then select **Export alert templates**. The Export Templates wizard starts. On the **Select template** page, select the templates, and then click the **Next** button.

   -or-

   To export one template, expand Templates, right-click the template, and then select Export. The Export Templates wizard starts.
3. On the Specify export options page, enter a password in the **File encryption password** box. This password prevents unauthorized access to any sensitive data in the template.
4. In the **Confirm password** box, enter the password again, and then click the **Next** button.
5. On the Confirm page, verify that the correct templates are listed, and then click the **Export** button.
6. On the **Save as** window, navigate to the location to save the template file, enter a name in the **File name** box, and then click the **Save** button.
7. On the Results page, click the **Done** button.

Use the following steps to import device alert templates:

1. In the **Device Management** navigation pane, expand **Alerts**.
2. Right-click **Templates**, and then select **Import alert templates**. The Import Templates wizard starts.
3. On the Select file page, click the **Browse** button, navigate to and select the template file, and then click the **Open** button.
4. In the **File password** box, enter the password that was assigned to the template file when it was exported.
5. To overwrite an existing template that has the same name, select the **Overwrite duplicate templates** check box. If you select this check box, a warning message appears on the Confirm page.
6. Click the **Next** button.
7. On the Confirm page, verify that the file name is correct, and then click the **Import** button.
8. On the Results page, click the **Done** button.

Delete an Alert Subscription Template

Use the following steps to delete an alert subscription template:

1. Expand the **Alerts** tree in the left navigation pane. In the **Alerts - Common Tasks** task module, select **Delete subscription template**. The **Delete Alert Template** wizard is started with the **Select template** page displayed.
2. Highlight the template you want to delete and click **Next**. If the template is linked to devices, specify the options to remove:

   - **Remove template but save linked subscriptions**: Delete the template but do not delete any occurrences of this template that have been saved by other names with devices associated with it (unlinked, see Apply an Alert Subscription Template on page 204).
   - **Remove subscriptions for all linked devices (listed below)**: Delete the template and any subscriptions to the template for all of the devices listed on this page.

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

3. Click **Delete Template**; the **Results** page is displayed.

4. Click **Done**.

View All Alert Subscriptions

On the **All Subscriptions** page, you can view the following information about alerts:

- **Device Model**: The model of the device that received the alert.
- **IP Hostname**: The IP Hostname of the device that received the alert.
- **IP Address**: The IP Address of the device that received the alert.
- **Advanced Settings**: Any advanced settings for the device.
- **Notification Type**: How you are notified about the alert (logging or email and logging).
- **Subscription Type**: **General alerts (detailed)**, **Supplies solution**, and **Mission critical solution**.
- **Linked to Template**: If the device is linked to a template (any future changes to that template will affect the alert settings for the device).

Use the following steps to view all of the alert subscriptions:

1. Expand the **Alerts** tree in the left navigation pane and select **All Subscriptions**. The **All Subscriptions** page is displayed.

2. A summary is displayed with all alert subscription templates in alphabetical order. To view details, click **+** next to the device. To show details for all subscriptions click **+** (Expand All) at the top of the page, or click **-** (Collapse All) to minimize all subscriptions.

3. To group Alerts, select **Group By** at the top of the page. You can group alerts by:

   - **Device**: Displays devices that can be individually expanded to show each applied subscription and corresponding Alerts detail.
   - **Subscription**: Displays subscriptions by name that can be individually expanded to show devices to which the subscription has been applied.
   - **Solution Type**: Displays one or any of the three types of Alerts that have been configured. These can be expanded to show individual subscriptions and devices to which the subscription has been applied.

4. With **All Subscriptions**, you can do any of the following:

   - **Save as Template**: Starts the **Create Alert Subscription Template** wizard, with the subscription settings that were selected; see Create Alert Subscription Templates on page 200.
   - **Unsubscribe**: Stop subscribing to the alerts currently set for this device.
   - **Edit Subscription**: Make changes to the alerts for this subscription; see Edit Alert Subscriptions on page 196.

Firmware

Both printer and HP Jetdirect device firmware can be updated from HP Web Jetadmin. A firmware image file can be downloaded from www.hp.com and put on the client system. It can then be imported into the **Firmware Repository**. If the version of this image is greater than the version on the device, an upgrade is possible. HP Web Jetadmin cannot be used to downgrade firmware to an older revision level. Firmware updates can be scheduled to occur at any time. Firmware update retry is also available in cases where an update failed or a device was not on the network.

Qualifying Firmware

Qualifying firmware images ensures that firmware images are tested by individuals with permissions to qualify images before installing and implementing them in your workplace. When firmware images are marked as **Qualified**, they are listed with the column **Qualified** in the **Firmware Repository**. With appropriate permission, you can require firmware images to be qualified by clicking **Edit Properties** in the **Firmware Repository**. If you do not have permission, you can only install firmware images that have been **Qualified**. Permissions are set in **Application Management** > **User Security** > **Roles**; for permissions settings, select **Device Management** > **Firmware** > **Manage Repository**.

Firmware Repository and Qualifying Firmware

The **Firmware Repository** can be accessed from the navigation pane under **Firmware** (Firmware Repository on page 213). HP Jetdirect and printer firmware images exist on www.hp.com and can be accessed in two ways:

- HP Web Jetadmin can contact www.hp.com and display available images to users (using the **Get Images** feature). The images can then be imported to the client using the **Import** feature.
- Image files can be manually obtained and imported to HP Web Jetadmin by the user.

In both cases, the goal is to get the desired image(s) onto HP Web Jetadmin so that they can be used for updating.

Qualify Feature

Images that are imported into HP Web Jetadmin can be marked as **Qualified**. This allows administrative control over firmware images as they are downloaded from the Web.

Users assigned to **Roles** having **Upgrade Device** permission enabled, but who do not have **Manage Repository** enabled are able to upgrade only with firmware images that are qualified (those marked as **Yes** in the **Qualified** column). Images that are not qualified, will not appear in the list.

Administrators assigned to **Roles** having **Manage Repository** enabled, have the ability to see non-qualified images (those marked as **No**) and qualified images (those marked as **Yes**). These administrators can use upgrade devices with this firmware for test and qualification purposes. Once the firmware is qualified, these same administrators can use the **Edit Properties** feature in the **Firmware Repository** to mark the firmware as qualified. This action allows other users to begin performing upgrades with tested/qualified firmware.

Finding Images

HP Jetdirect firmware can be obtained through www.hp.com/go/webjetadmin_firmware. HP Printer firmware images can be obtained by visiting the device specific Software and Drivers Downloads pages at www.hp.com/go/webjetadmin_software. Devices that have firmware update capability will offer a self extracting executable. The file required for HP Jetdirect printer firmware updates has an rfu extension. This file can be extracted and then imported into HP Jetdirect by using **Import**.

Firmware - Common Tasks Task Module

The **Firmware - Common Tasks** task module provides links that initiate the following tasks for firmware:

- Upgrade the firmware on devices
- View the Firmware Repository

Firmware - Active Tasks Task Module

The **Firmware - Active Tasks** task module provides a list of the firmware tasks that are running. Use this task module to stop or view the status of an active task.

Firmware - Scheduled Tasks Task Module

The **Firmware - Scheduled Tasks** task module provides a list of the firmware tasks that are scheduled to run. Use this task module to delete or edit the settings for a scheduled task.

Firmware - Device Summary Task Module

The **Firmware - Device Summary** task module provides the following information:

- The number of devices that have the most current device and HP Jetdirect firmware versions installed
- The number of newer versions of the device and HP Jetdirect firmware that are available in the Firmware Repository and the number of each type that is available
- The number of devices that are currently in a short stack condition

NOTE: When the HP Jetdirect firmware is upgraded, a device might be left in a short stack condition if the device is disconnected during the upgrade process or a fatal error occurs. HP Web Jetadmin detects this error condition and tries the upgrade again to make sure that the device is not left in an incomplete upgrade state.

Related Application Options for Firmware

Global settings can be stored here for managing firmware images and how devices are updated.

- Configure the Settings for Firmware Upgrades on page 81

Upgrade Firmware

Once the firmware images exist on HP Web Jetadmin host, they can be applied as upgrades to devices.

If you chose to only use qualified firmware images, then you must certify firmware images before upgrading the firmware. Use **Edit Properties** on the **Firmware Repository**.

Use the following steps to upgrade the firmware:

1. In the left navigation pane, expand **Firmware**. In the **Firmware - Common Tasks** task module, select **Upgrade firmware**. The **Upgrade Firmware** wizard is started with the **Select upgrade type** page displayed.

2. Select the type of firmware to upgrade (device or HP Jetdirect).

3. To schedule the firmware upgrade for later, select **Schedule firmware upgrade**. Click **Next**. The **Select devices** page is displayed.

   NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

   NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

   NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

4. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

   To select an entire group instead of individual devices, change the selection method to **Groups**. Tasks can be performed on a single group or a group and all of its subgroups.

   NOTE: If subgroups are included, the task might take longer to complete and network traffic might increase significantly. HP recommends that you include subgroups only when necessary.

   If a task is scheduled for a group, the task uses the devices that are in the group when the task starts. If the devices that are in the group are changed, you do not have to delete the scheduled task and create a new scheduled task.

   Click **Next**. The **Select firmware version** page is displayed.

   If you chose to only use qualified firmware images (in **Edit Properties**), a **Qualified** column is displayed showing whether or not each image listed is qualified. You can select any of the qualified images to upgrade. If you need to qualify an image and you have the appropriate permissions (**Manage Firmware Images** set through User Security on page 278), select the image and click **Edit Properties**.

   NOTE: Some images with the same version and models will be listed as one option on the drop-down list.

   Click **Next**.

5. If one or more of the selected devices support Boot Language, the **Select boot language** page is displayed. Select the boot language that will be sent to the printer before the upgrade begins. Then click **Next**.

   If none of the selected devices support Boot Language, this page will not be displayed.

6. If you are scheduling this upgrade for a later time, the **Specify schedule options** page is displayed. Select the start date and time. Then click **Next**.

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

8. The **Results** page is displayed. If a device does not support boot language or for HP Jetdirect upgrades, **N/A** will be displayed.

9. Click **Done**.

Upgrading Firmware for HP Jetdirect Devices versus Printer Devices

Upgrading firmware on HP Jetdirect devices versus printing devices is similar but not identical. HP Jetdirect firmware updates are done by contacting the device through SNMP and directing it to perform an update by obtaining the updated firmware from a TFTP service that is started on the HP Web Jetadmin server. HP Web Jetadmin uses the standard port number for the TFTP server (port 69) that may get blocked by firewall software on the system hosting HP Web Jetadmin software. Once the update action is started, the device performs actions against the image file on the TFTP server until the whole image file is obtained. The actual update action is performed by the HP Jetdirect device itself.

Printer firmware updates are done by HP Web Jetadmin sending the RFU image file to the printer in the same way a print job would be sent. This print-file action is done via port 9100 on the printer. Once the printer receives the job, it recognizes it as an update and then launches internal processes that perform the actual update. HP Web Jetadmin is used strictly as a file send agent in the case of printer firmware updates.

NOTE: If an HP Jetdirect firmware upgrade is launched during a large print job, the job will not finish processing and will need to be restarted by the user.

Firmware Repository

The first step in firmware updates is to find available images. Images exist on www.hp.com and can be accessed in two ways:

- HP Web Jetadmin can contact www.hp.com and display available images for you.
- You can manually obtain and import image files to HP Web Jetadmin.

In both cases, the goal is to get the desired image onto the HP Web Jetadmin host so that it can be used for updating. This image will be shown on the **Firmware Repository** page.

NOTE: For more information about qualifying firmware and the **Firmware Repository**, see Qualifying Firmware on page 210.

View the Firmware Repository

You can view the firmware images that HP Web Jetadmin uses on the **Firmware** > **Repository** page. This page displays the following:

- Version of the firmware.
- Date of the version.
- Whether or not the image is local.
- Languages that the firmware supports. **All available** is displayed for images that do not support languages packs.
- Device models that the firmware upgrade supports.

Use the following steps to view the Firmware Repository:

1. In the left navigation pane, expand **Firmware** and click **Firmware Repository**.
2. The available firmware upgrades are listed on the **Firmware Repository** page.

From the **Firmware** > **Repository** page, you can choose to do the following:

- Get Images on page 214
- Import Images on page 214
- Edit Properties for Firmware Images on page 214
- Delete Images on page 215
- Upgrade Firmware on page 211

Get Images

Get Images is used to download selected images from www.hp.com onto the client. They can then be imported into the **Firmware Repository** and then installed from the **Firmware Repository** onto the HP Web Jetadmin device using the **Import** feature.

Use the following steps to obtain the firmware images:

1. In the left navigation pane, expand **Firmware** and click **Firmware Repository**. The **Firmware Repository** page is displayed with the firmware images already available.
2. Click **Get Images**. The **Get Firmware Images** wizard is started with the **Select images** page displayed.
3. Select the images to get from www.hp.com and click **Next**. The **Select destination** page is displayed.
4. Select the destination for the image to be stored and click **Next**. The **Confirm** page is displayed.
5. Click **Get Images**. The image is downloaded to HP Web Jetadmin and the **Results** page is displayed.
6. To get the images onto the HP Web Jetadmin server, check the box for **Import firmware images** and then click **Done**. The firmware images are then imported to the server and will appear in the Firmware Repository on page 213. (For more information about importing firmware images, see Import Images on page 214.)
7. Click **Done**.

Import Images

Use the following steps to import images in the Firmware Repository onto devices:

1. In the left navigation pane, expand **Firmware** and click **Firmware Repository**.

   The firmware upgrades are displayed on the **Firmware Repository** page. Click **Import**. The **Import Firmware Images** wizard is started with the **Select firmware file** page displayed.
2. Enter or browse to the file with the firmware image and click **Next**. The image is imported to devices and the **Results** page is displayed.
3. Click **Done**.

Edit Properties for Firmware Images

Use the following steps to edit the description of a firmware image or mark a firmware image as qualified:

1. In the left navigation pane, expand **Firmware** and click **Firmware Repository**.
2. Highlight the image to be edited and click **Edit**. The **Edit Image Properties** dialog is displayed.
3. Change the description of the qualified image setting and click **OK**.

Delete Images

Use the following steps to delete a firmware image from the Firmware Repository:

1. In the left navigation pane, click **Firmware** and then click **Firmware Repository**. The **Firmware Repository** page is displayed.
2. Select the firmware image you want to delete and click **Delete**.
3. A confirmation message is displayed. Click **Yes**.
4. The firmware will be deleted from the **Firmware Repository**.

Edit Scheduled Upgrades

Use the following steps to edit a scheduled firmware upgrade task:

1. In the **Firmware - Scheduled Tasks** task module, select the task and click **Edit Properties**.
2. Make any changes to the scheduled upgrade task and click **Next**. The **Confirm** page is displayed.
3. Click **Next**. The schedule for upgrading the firmware will be changed.

Delete Scheduled Upgrades

Use the following steps to delete a scheduled firmware upgrade task:

1. In the left navigation pane, click **Firmware**. Access the **Firmware - Scheduled Tasks** task module.

   Select the schedule to delete and then click **Delete**.
2. A confirmation message is displayed. Click **OK**. The schedule is deleted from HP Web Jetadmin.

Reports

HP Web Jetadmin provides a rich set of data collection and reporting features. These features enable data collections that are stored in a database and that are used in generating reports at a later time. After data is collected about a device or group of devices, you can display the data in a report, save the data for future use, or save the report.

There are two steps to producing a report:

1. **Collecting the data**: request which devices to collect information about for the report. Since this process causes network traffic and database space, you must turn on data collection when you want a report.

NOTE: If the data collection is not turned on, then the data will not be included in the report when it is run.

2. **Generating the report**: specify the report type, the device or group or devices to include in the report (which could be all or a subset of the devices you specified in Step 1), and the time frame for the data to be included in the report. This must be done each time you want the report to run.

Reporting in HP Web Jetadmin shows data change over time. A very simple report could be simple device page count on a single device (Device Utilization, see Device Utilization on page 221). After data collection has been established and multiple page counts exist in the database, a report can be displayed that shows the page count change (if any) in a selected time interval.

For more information about producing a report for the first time, see Getting Started with Reports on page 224.

Types of Data Collection and Reports That Are Available

The following table identifies the reports that can be generated for each type of data collection.

Data collection type	Report generated
Accessories Inventory Collects information about the accessories that are installed on devices, such as a duplexer or paper tray. Accessory information is collected once every 24 hours.	Accessory Inventory Reports information about the device accessories that are installed, have been uninstalled, and have been changed.
Device Inventory Collects information about the device status, other device details, and attribute changes, such as the first and last communication. Device information is collected once every 24 hours.	Device Inventory Reports the devices that HP Web Jetadmin discovered, devices that have been lost, and any IP address changes. This information includes the number of each device model that is installed on the network.
Device Utilization Collects the following information: ● Page counts for the color, mono (black and white), simplex, duplex, and total pages printed ● Page counts for the copy, scan, digital send, and fax pages printed Data is collected once every 24 hours.	Device Utilization Reports the page counts for the media and page types that the devices processed during a specific time interval or reporting period.
Device Utilization by User Collects information about the jobs that each user printed, including the application used to print each job. Data is collected when job traps are sent from a device to the HP Web Jetadmin host. For devices that do not support job traps, the data in the device job table is collected once every 24 hours.	Device Utilization by User Reports the jobs that have been printed and the user who printed the jobs.
Event Log History Collects information from the error log on the devices.	Event Log History Reports the frequency of occurrence for each error type.
Hourly Peak Usage Collects the following information: ● Page counts for the color, mono (black and white), simplex, duplex, and total pages printed	Hourly Peak Usage Reports the page counts for the media and page types that the devices processed on an hourly basis and displays them as charts or summary reports.

Data collection type	Report generated
- Page counts for the copy, scan, digital send, and fax pages printed Data is collected once every hour.	
Supply Utilization Collects information about the supplies that are about to run out and consumption rates based on the current usage. These supplies include cartridges, maintenance kits, and drum kits. Data is collected once every 24 hours.	Supply Ordering (HP SureSupply) Reports the requirements for ordering supplies based on a percentage or threshold. This report provides an option to automatically place orders by using HP SureSupply.
	Supply Replacement Forecast Reports the estimated date when each supply will need to be replaced by using the supply usage history. This report includes the percentage of confidence, part number details, current supply levels, and so on.
	Supply Usage Reports the supply consumption rates in specific environments. For each supply, this report shows the consumption to-date, last installation date, serial number, and so on. NOTE: This report includes information only about devices that have cartridges with serial numbers installed.

Examples of Reports

Reporting in HP Web Jetadmin shows data change over time. A very simple report could be simple device page count on a single device. After data collection has been established and multiple page counts exist in the database, a report can be displayed that shows the page count change (if any) in a selected time interval. (See Device Utilization on page 221).

Following is an example of data collection for page counts for a device for seven days:

Day 1: 20 pages	Day 8: 35
Day 2: 25 pages	Day 9: 40
Day 3: 26 pages	Day 10: 44
Day 4: 26 pages	Day 11: 44
Day 5: 26 pages	Day 12: 44
Day 6: 26 pages	Day 13: 44
Day 7: 31 pages	Day 14: 47

On days where page counts remain the same (in the example above, Days 3, 4, 5, and 6), HP Web Jetadmin stores the unchanged value.

Based on the above example, a simple report totaling pages printed in one week intervals might look like this:

Device 1.1.0.1

Week 1: 11 (31 - 20 = 11)
Week 2: 16 (47 - 31 = 16)
Total: 27 (11 + 16 = 27)

Another report totaling pages printed in daily intervals might look like this:

Day 1: 0	Day 8: 4
Day 2: 5	Day 9: 5
Day 3: 1	Day 10: 4
Day 4: 0	Day 11: 0
Day 5: 0	Day 12: 0
Day 6: 0	Day 13: 0
Day 7: 5	Day 14: 3
Device 1.1.0.1 Total = 27	

Complex reporting features exist and facilitate much more than simple counts. Data collected over time and reported in some interval is the general basis for most reporting features.

Report Management - Common Tasks Task Module

The **Report Management - Common Tasks** task module provides links that initiate the following tasks for reports:

- Display an overview of the main steps required to produce reports
- Add devices to a data collection
- Remove devices from a data collection
- Generate a report
- Schedule a report
- View an archived report

Data Collection - Common Tasks Task Module

The **Data Collection - Common Tasks** task module provides links that initiate the following tasks for data collections:

- Add devices to a data collection
- Remove devices from a data collection
- Create a data collection template
- Apply a data collection template to devices
- Edit a data collection template
- Delete a data collection template
- Copy a data collection template to create a new template

Data Collection - Management Task Module

The **Data Collection - Management** task module provides a list of the data collection types and the number of devices that have been added to each data collection. Use this task module to perform the following tasks:

- Add devices to a data collection
- Remove devices from a data collection
- View the settings and devices for a data collection
- View the **Data Collection Anomalies** window where you can reconcile or resolve the anomalies

Data Collection - Templates Task Module

The **Data Collection - Templates** task module provides a list of the data collection templates that have been created. Use this task module to perform the following tasks:

- Create a data collection template
- Apply a data collection template to devices
- Edit a data collection template
- Delete a data collection template
- Copy a data collection template to create a new template
- View the settings for a data collection template

Reports - Scheduled Reports Task Module

The **Reports - Scheduled Reports** task module provides a list of the reports that are scheduled to run. Use this task module to delete or edit the settings for a report schedule.

Reports - Report Templates Task Module

The **Reports - Report Templates** task module provides a list of the default report templates and the custom report templates that have been created. Use this task module to perform the following tasks:

- Create a report template
- Apply a report template to devices
- Edit a custom report template
- Delete a report template
- Copy a report template to create a new template
- View the settings for a report template

Reports - Report Generation Task Module

The **Reports - Report Generation** task module provides a list of the default reports that can be generated. Use this task module to perform the following tasks:

- Generate a report
- Schedule a report to run at a later time
- Generate a sample of a report

Reports - Archived Reports Task Module

The **Reports - Archived Reports** task module provides a list of the reports that have been archived. Use this task module to perform the following tasks:

- View an archived report
- Send an archived report to an email address
- Save an archived report as a comma-separated values (CSV) or HTML file
- Delete an archived report

Related Application Options for Reports

Global settings can be stored here for managing report data.

- Manage the General Settings for Reports on page 82
- Configure the Data Collection Times for Reports on page 82

Available Reports

Reports are generated through a combination of user-defined settings and collected data that is stored in the database. There are many report types that correspond directly to data collection types. Completed reports can be displayed through the HP Web Jetadmin client host. Reports are stored in an archive and can be sent to email through SMTP.

Reports can be generated in a summary format or in a reporting period format. Reports can be scheduled to occur at a specified time automatically or immediately.

NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

Accessory Inventory

The **Accessory Inventory** report can be used to inventory and track changes in device accessories.

Available report subtypes are:

- **Time Interval**: reports changes in accessories on devices over the specified time interval.
- **Last Known Status**: reports the last known status of each accessory on the device.

Available columns for this report include but are not limited to:

- Accessory Name
- Accessory Status
- Collection Date

For more information, see Types of Data Collection and Reports That Are Available on page 216.

NOTE: You might need to power cycle your devices to reflect accessory changes.

Device Inventory

The **Device Inventory** report captures device status and device communication states. This report can be used to track devices that are missing or have been known to be missing in some time frame.

Available report subtypes are:

- **Time Interval**: reports changes in statuses on devices over the specified time interval.
- **Last Known Status (Details)**: reports the last known status and communication state of each device.
- **Last Known Status (Summary)**: categorizes devices into the different statuses.

Available columns for this report include but are not limited to:

- Inventory Status
- Inventory Date

For more information, see Types of Data Collection and Reports That Are Available on page 216.

Device Utilization

The Device Utilization report tracks the media usage and page counts for a specific time period. The following report subtypes are available:

- **Time Interval (Job Type)**: Displays the page counts for the specified job type (for example, mono, color, or copy jobs).
- **Time Interval (Media Size)**: Displays the page counts for the specified media size.
- **Job Type (Details)**: Displays the page counts for the specified job type and media sizes.

The report data that is available for job types includes, but is not limited to, the following:

- Total
- Total Accent Color
- Total Color
- Total Duplex
- Total General Office Color
- Total Mono
- Total Other Color
- Total Simplex

For more information, see Types of Data Collection and Reports That Are Available on page 216.

Device Utilization by User

The **Device Utilization by User** reports by-user page counts based on job tables captured at the device.

Available report subtypes are:

- **Time Interval**: reports pages printed by user (application page count, color page counts, mono page counts, and others) over a time period.
- **Time Interval (Media Size)**: reports pages printed by user of media sizes (letter, legal, and others) over a time period.

Available columns for this report include but are not limited to:

- Total
- MS Word
- Total Color
- Total Mono

For more information, see Types of Data Collection and Reports That Are Available on page 216.

Event Log History

The **Event Log History** report shows device errors and error categories.

Available report subtypes are:

- **Time Interval**: reports pages printed on an hourly interval over a time period.
- **Summary (Event Type)**: reports the number of events in each category for each device, by report interval (daily, weekly, monthly, and others).

Available columns for this report include but are not limited to:

- Event Code (Hex)
- Event Description
- Event Log Page Count
- Event Type

For more information, see Types of Data Collection and Reports That Are Available on page 216.

Hourly Peak Usage

The **Hourly Peak Usage** report tracks hourly page and media counts.

Available report subtypes are:

- **Time Interval**: reports pages printed on an hourly interval over a time period.

Available columns for this report include but are not limited to:

- Total Mono
- Total
- Total Simplex
- Total Duplex
- Total Simplex

For more information, see Types of Data Collection and Reports That Are Available on page 216.

Supply Ordering

The **Supply Ordering** report provides a list of needed supplies based on your specified percentage and threshold. Also included is an HP SureSupply order option.

Available report subtypes are:

- **Details**: shows how many supplies per device are needed based on the specified threshold.
- **Summary**: shows a consolidated list of totals needed per supply part number across all devices based on the specified threshold.

Available columns for this report include but are not limited to:

- Supply
- Supply Part Number
- Installation Date
- Estimated Supply Level (%)

For more information, see Types of Data Collection and Reports That Are Available on page 216.

Supply Replacement Forecast

The **Supply Replacement Forecast** report is a predictive report showing replacement needs for specific supplies. The device supplies metrics that exist in your database will be analyzed, a prediction about needed supplies will be made, and the **Supply Replacement Forecast** will be generated. This prediction is based on details that include supplies levels, percentage coverage, and other historic data relegated to supplies and printing. The report will include a percentage confidence rating to give you an indication of how much data existed and was used in the analysis. If very little data existed, the percentage confidence should indicate a low value. If you have been tracking supplies on devices for a long period of time, the report would show a higher percentage of confidence.

Available report subtypes are:

- **Details**: shows estimated forecasted replacement date per device per supply as well as quantity of supply needed in the specified time period.
- **Summary**: shows the quantity of supply needed by part number across all devices based on specified time period.

Available columns for this report include but are not limited to:

- **Supply**
- **Supply Part Number**
- **Estimated Remaining**

For more information, see Types of Data Collection and Reports That Are Available on page 216.

Supply Usage

The **Supply Usage** report shows usage based on page count over supply lifetime, including many supply details including install dates and serial numbers. This report only includes information about devices with serial numbers on their toner cartridges.

Available report subtypes are:

- **Details**: shows supplies that are installed (active) and/or uninstalled (removed) on the device and provides usage information (installation date, estimated percentage remaining, and more).
- **Inventory**: tracks a specific supply instance between devices (the supply must have a valid serial number).

Available columns for this report include but are not limited to:

- **Supply Part Number**
- **Supply Status**
- **Supply Installation Date**
- **Average Supply Coverage (%)**
- **Average Supply Coverage (%)** (default)

For more information, see Types of Data Collection and Reports That Are Available on page 216.

Getting Started with Reports

The following steps are required to generate a report:

1. **Collect the data**: Specify the devices for which HP Web Jetadmin collects data. The data collection process causes network traffic and requires database space, so you must enable data collection when you want a report. You can specify which reports HP Web Jetadmin generates based on the type of data collection you select.
2. **Generate the report**: Specify the following options:
   - The type of report to generate. The type of data collection specified in step 1 determines which reports HP Web Jetadmin can generate.
   - The device group or individual devices to include in the report, which might be all of the devices or a subset of the devices specified in step 1.

     NOTE: You can only select devices for which data has been collected.
   - The time frame for the data to be included in the report.

   This must be done each time you want the report to run.

Data Collection

Data collections are groups of devices that have specific collection types enabled. You can apply a data collection type such as **Device Utilization** to a single device, to multiple devices, or to a device group. When a data collection is first applied to a device or devices, HP Web Jetadmin launches a data collection immediately establishing a data baseline. Once the device is populated under a specific data collection type, data collections occur at some interval or by way of some trigger.

NOTE: Applying data collection to a device group is done through Group Policies on page 123.

As data is collected, it is stored in tables within the HP Web Jetadmin database. Data retention is set to one year beyond the initial collection date. This value can be changed in **Tools** > **Options** > **Shared** > **Server Maintenance** > **Reports** (Manage the Report Data on page 52). Data collections for Reports can be retained for up to 5 years.

Data Collection Cycle

Data collection types all have a specific collection cycle that may or may not be dependent on a schedule. The **Device Utilization by User** data collections are triggered when printers send job-trap packets into the HP Web Jetadmin host. All other types are schedule-triggered. All data collections collect data every 24 hours except for the **Hourly Peak Usage** data collection which is collected once every hour to provide greater reporting resolution.

The default start time for the data collection 24 hour cycle is set at 12:00AM at the HP Web Jetadmin host. This can be configured for each data collection in **Tools** > **Options** > **Device Management** > **Reports** > **Data Collection Times**. When subscribing a device to a data collection, you can choose the time of collection if you prefer a different time. The 24 hour cycle is designed to ensure reporting accuracy. Data within reports will be marked if the data collected did not represent a full 24 hour cycle.

Initial Data Collection

Activating data collection always launches the specific data collection type on selected devices. This is done to gather initial or baseline data that is then stored in the database. This is not a user-selectable action. The result of this initial data collection can be observed in the **Results** display for any completed data collection.

Data Collection Custom Collection Time

HP Web Jetadmin has a custom collection time feature that allows you to specify the time zone of the devices you are collecting for and the hour to perform the collection. The data collection start time is 12:00AM local server time. The default collection time for the Web Jetadmin server can be altered through **Tools** > **Options** > **Device Management** > **Reports** > **Data Collection Times** (see Configure the Data Collection Times for Reports on page 82). You can specify the time zone and custom hour when setting up data collection (see Add Devices to Data Collection on page 227) or when creating data collection templates (Create a Data Collection Template on page 228), For example:

Joy has devices in the Pacific time zone. Her HP Web Jetadmin server is in the mountain time zone. The devices that Joy manages are not turned on until 8AM. Pacific time. Data collection at 12AM Mountain time would not capture any data for the devices since they are turned off at the end of the business day. When Joy sets up data collection for the devices, Joy can specify that she would like the collection to run in the Pacific time zone and at 9:00AM. The data collection would start on the HP Web Jetadmin server at 10AM Mountain time which is 9AM Pacific time.

HP Web Jetadmin will continue to use a 24 hour data collection cycle for all devices.

Device Utilization by User and Data Collections

The **Device Utilization by User** data collection type uses SNMP traps to trigger the HP Web Jetadmin host data collection. Every time a print job is completed by the device, a trap is sent and HP Web Jetadmin runs a complete query of the device's job table. Any new entries in the job table are stored in the HP Web Jetadmin database; all old entries that were previously stored are discarded.

HP Web Jetadmin uses UDP port 27892 as the traps listener port for alerts and any reports that are based on by-user collections.

Device Utilization by User accuracy may be limited by two things:

- the device's ability to store only a limited number of jobs in the job table.
- the device's ability to trap when multiple print jobs are queued.

Both of these are dependant on device printer model and firmware. **Device Utilization by User** and Reporting should never be used as a substitute for job accounting. HP Web Jetadmin **Reports** features are designed for trending and analysis purposes.

NOTE: For devices that don't support job-traps, HP Web Jetadmin will collect the device's job table once every 24 hours.

Device and Printer Driver Support for Device Utilization by User

Job logging features are not available on all HP printers. Check your printer documentation to be sure these device-based features exist.

End of job trapping is not supported on all HP printers. In the case where end of job trapping is not supported, HP Web Jetadmin will query the job tables once per collection period (24 hours). This may impact the accuracy of by-user reporting due to the limited size of the device job log.

Windows print drivers supplied by HP are known to support device job log entries. Windows print drivers available through Microsoft Windows operating systems may not support job log entries. Be sure to use HP model-specific drivers or the HP Universal Print Driver (UPD) when by-user tracking is required.

Using Group Policies to Set Data Collection

The **Group Policies** feature is a powerful new automation tool that can save you a lot of time configuring devices and HP Web Jetadmin settings. Any device group has a property known as a **Group Policies**. One policy that can be added to any device group's properties is **Enable Data Collection**. When activating the **Enable Data Collection** to a device group, you must define a data collection template from the list of existing templates. Also, a trigger is specified that enables the configuration to take place either as the device is populated into the group or as the device is de-populated from the group. Multiple **Enable Data Collection** settings can exist on a single device group. See Group Policies on page 123.

Add Devices to Data Collection

Use the following steps to add devices to a data collection:

NOTE: If you access this feature through the Data Collection - Management Task Module on page 219, then you will skip the first page of the **Add Devices to Data Collection** Wizard.

1. Expand the **Reports** tree in the left navigation pane and then click **Data Collection**.

   In the **Data Collection - Common Tasks** task module, select **Add devices to data collection**. The **Add Devices to Data Collection** wizard is started with the **Select data collection** page displayed.

2. Select the template to use, if any and then select the type of data collection(s) to perform.

3. Select the time zone and the time to start data collection. The click **Next**; the **Select devices** page is displayed.

   NOTE: For more information about Data Collection offset hours, see Data Collection Custom Collection Time on page 225.

4. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

   To select an entire group instead of individual devices, change the selection method to **Groups**. Tasks can be performed on a single group or a group and all of its subgroups.

   NOTE: If subgroups are included, the task might take longer to complete and network traffic might increase significantly. HP recommends that you include subgroups only when necessary.

   If a task is scheduled for a group, the task uses the devices that are in the group when the task starts. If the devices that are in the group are changed, you do not have to delete the scheduled task and create a new scheduled task.

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

6. Click **Add Devices**. The **Results** page is displayed.

   Click **Details** to view the types of data collection for that device. When done, click **Close**; the **Results** page is displayed again.

7. Click **Done** to display the **Data Collection** page.

8. Now you are ready to generate a report.

Remove Devices from Data Collection

Use the following steps to remove devices from a data collection:

1. Expand the **Reports** tree in the left navigation pane and then click **Data Collection**.

   In the **Data Collection - Common Tasks** task module, select **Remove devices from data collection**. The **Remove Devices from Data Collection** wizard is started with the **Select data collection type** page displayed.

2. Select the type of data collection that you want to remove devices from and click **Next**. The **Select devices** page is displayed.

3. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

4. Click **Next**. The **Confirm** page is displayed showing you the devices to be deleted from this type of data collection.

5. Click **Next**. The **Results** page is displayed.

6. Click **Done** to display the **Data Collection** page.

Data Collection Templates

In **Data Collection Templates**, you can:

- Create new templates (Create a Data Collection Template on page 228).
- View existing templates (Data Collection Templates on page 228).
- Edit existing templates (Edit a Data Collection Template on page 230).
- Apply existing templates (Apply a Data Collection Template on page 229).
- Delete existing templates (Delete a Data Collection Template on page 230).
- Copy existing templates (Copy Template Wizard on page 99).

You can also add devices to or remove devices from this type of data collection.

Create a Data Collection Template

For more information, see Types of Data Collection and Reports That Are Available on page 216.

Data Collection Templates are designed to help you enable more than one data collection type. In summary, you can create a data collection template by opening the **Create Data Collection Template** wizard, select one or more data collection types, name the template, and then confirm the settings.

After the template has been created, it can be applied to devices in the same ways as individual data collection types. By applying data collection templates, you are actually configuring the individual data collection types without having to activate controls multiple times.

For scheduling information, see Data Collection Custom Collection Time on page 225.

Use the following steps to create a data collection template:

1. Expand the **Reports** tree in the left navigation pane and then click **Data Collection**.

   In the **Data Collection - Common Tasks** task module, select **Create data collection template**. The **Create Data Collection Template** wizard is started with the **Choose data collection type** page displayed.

2. Select the type of data collection for this template and specify the time zone and collection time and then click **Next**. The **Select collection time** page is displayed.

3. Select the time zone and the time to start data collection. The click **Next**; the **Specify name** page is displayed.

   NOTE: For more information about Data Collection offset hours, see Data Collection Custom Collection Time on page 225.

4. Type the name for the template and then click **Next**. The **Confirm** page is displayed.

5. Click **Next**. The **Results** page is displayed.

6. Click **Done** to display the **Data Collection** page.

7. Now you are ready to apply the template to devices and to generate a report.

Apply a Data Collection Template

You can apply a **Data Collection** template that has already been created to a device or group of devices. You can also turn data collection on and off; this is useful if you need to control the network traffic generated to communicate with the devices and also because the data is stored in database tables which, over time, can become quite large. By selecting the data to include, you have great flexibility as to what you want to include in your reports.

Use the following steps to apply a data collection template:

1. Expand the **Reports** tree in the left navigation pane and then click **Data Collection**.

   In the **Data Collection - Common Tasks** task module, select **Apply data collection template**. The **Apply Data Collection Template** wizard is started with the **Select data collection** page displayed.

2. Select a template and click **Next**. The **Select devices** page is displayed.

3. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

   To select an entire group instead of individual devices, change the selection method to **Groups**. Tasks can be performed on a single group or a group and all of its subgroups.

   NOTE: If subgroups are included, the task might take longer to complete and network traffic might increase significantly. HP recommends that you include subgroups only when necessary.

   If a task is scheduled for a group, the task uses the devices that are in the group when the task starts. If the devices that are in the group are changed, you do not have to delete the scheduled task and create a new scheduled task.

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

5. Click **Next**. The **Results** page is displayed.

   Click **Details** to view the types of data collection for that device. To expand the details for all devices, click **Expand All**. When done, click **Close**; the **Results** page is displayed again.

6. Click **Done** to display the **Data Collection** page.

7. Now you are ready to generate a report.

Edit a Data Collection Template

Use the following steps to edit a data collection template:

1. Expand the **Reports** tree in the left navigation pane and then click **Data Collection**.

   In the **Data Collection - Common Tasks** task module, select **Edit data collection template**. The **Edit Data Collection Template** wizard is started with the **Select template** page displayed.

2. Select a template and click **Next**. The **Choose data collection type** page is displayed.

3. To change the type of data collection for this template, check the type or types to include and uncheck those that should not be included. Then click **Next**. The **Select collection time** page is displayed.

4. Select the time zone and the time to start data collection. The click **Next**; the **Specify name** page is displayed.

NOTE: For more information about Data Collection offset hours, see Data Collection Custom Collection Time on page 225.

5. To change the name for this template, type the new name in **Template name** (or you can leave the name as it was). Then click **Next**. The **Confirm** page is displayed showing you the old settings and the new settings for this template.

6. Click **Next**. The **Results** page is displayed.

7. Click **Done** to display the **Data Collection** page.

8. Now you are ready to generate a report.

Delete a Data Collection Template

Use the following steps to delete a data collection template:

1. Expand the **Reports** tree in the left navigation pane and then click **Data Collection**.

   In the **Data Collection - Common Tasks** task module, select **Delete data collection template**. The **Delete Data Collection Templates** wizard is started with the **Select templates** page displayed.

2. Select the data collection template or templates to delete and click **Next**. The **Confirm** page is displayed.

3. Click **Next**. The **Results** page is displayed.

4. Click **Done** to display the **Data Collection** page.

Copy a Data Collection Template

Throughout **Device Management** view, templates can be created and managed to save you time and provide consistency. Templates contain configuration preferences (that vary by template type) and can be applied to devices or groups. Templates are available in **Configuration**, **Alerts**, **Discovery**, **Data Collection**, and **Report Generation**. For more information, see Copy Template Wizard on page 99.

View Data Collection Templates

Use the following steps to view a data collection template:

1. Expand the **Reports** tree in the left navigation pane; then expand the **Data Collection** tree and click **Templates**.
2. Select the template from the list, and then click the **View** button.

Data Collection Summaries

You can view which devices have been added to any type of data collection. The following information is displayed:

- **Name**: name of the data collection.
- **Traffic impact**: how this data collection, while running, affects network traffic (high, medium, or low).
- **Collection time**: how often this data collection is run.
- **# Devices**: how many devices are included in this data collection. (More devices included might negatively impact network traffic).
- **Reports supported**: shows all of the reports you could generate with this particular type of data collection.

Use the following steps to view a summary of a data collection:

1. Expand the **Reports** tree in the left navigation pane and then expand **Data Collection**. Below **Data Collection**, click on any type of data collection. The summary page for that type of data collection is displayed.
2. View the summary data displayed.
3. To collect data now, highlight one or more devices listed and click **Collect Now** (at the bottom of the page). The data collection for the selected device or devices is started immediately.
4. To add devices from this type of data collection:

   a. Click **Add Devices** (at the bottom of the page). The **Add Devices to Data Collection** wizard is started with the **Select devices** page displayed. Click **Next**.

   b. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

   To select an entire group instead of individual devices, change the selection method to **Groups**. Tasks can be performed on a single group or a group and all of its subgroups.

   NOTE: If subgroups are included, the task might take longer to complete and network traffic might increase significantly. HP recommends that you include subgroups only when necessary.

   If a task is scheduled for a group, the task uses the devices that are in the group when the task starts. If the devices that are in the group are changed, you do not have to delete the scheduled task and create a new scheduled task.

   c. Click **Next**. The **Confirm** page is displayed showing you the devices to be added to this type of data collection.

   d. Click **Add Devices**. The **Results** page is displayed.

   e. Click **Done** to display the summary data page.

5. To remove devices from this type of data collection:

   a. Select the devices you want to remove and click **Remove Devices** (at the bottom of the page). The **Remove Devices from Data Collection** wizard is started with the **Confirm** page displayed.

   b. Click **Remove Devices**. The **Results** page is displayed.

   c. Click **Done** to display the summary data page.

6. To generate a report now, see Generate Reports on page 235.

Data Collection Statuses

Following are the various Data Collection statuses that will be displayed on Data Collection pages.

Status	Definition	Resolution
Communication Error	Data Collection was not possible because HP Web Jetadmin was not able to communicate with the device.	Make sure the device is connected to the network and that it is turned on
Device Change Error	A different device exists at this IP address. The Data Collection feature checks the device for unique attributes. Devices that don't match this criteria fail with this error.	The new device should be discovered through any discovery mechanism and then added into the data collection. Anomaly is informational only.
Device Error	Data Collection was not possible due to a device error.	Check the device.
Failure	Data Collection was not successful.	This could indicate ether an internal or external failure. Check the device if these recur.
In Process	Data Collection is in progress.	N/A
Need Credentials	Data Collection was not possible because credentials are required.	To locate the devices requiring credentials, use the HP Web Jetadmin **Device List** column titled **Credentials Required**. To add credentials, right-click on each device requiring credentials and select **Update Credentials**. After the credentials are updated, the Data Collection should succeed the next time it is attempted.
Not Valid For Device	Data Collection type is not valid for this device model.	Select a different device. If the device isn't capable, consider removing it from the data collection.
Success	Data Collection was successful.	N/A

Data Collection Anomalies

Use the following steps to view the data collection anomalies:

1. In the **Reports - Data Collection - Management** task module, highlight the type of data collection to review and click **Anomalies**. The **Data Collection Anomalies** page is displayed.
2. Select the anomaly to view and click **Reconcile**.

   You can choose to **Ignore the anomaly**.
3. To export the anomalies listed to an spreadsheet report, click **Export** and then specify the location to save the file.
4. When done, click **Close**.

The following table provides a description of the data collection anomalies.

Anomaly	Type	Description	Reset	Ignore	Adjust
Device at IP Address changed	All data collections	The device is a different device than what was subscribed to.	Deletes all data stored for the device.	Ignores this anomaly and removes it from the open anomalies list.	N/A
Suspect Serial Number	All data collections	The serial number is not unique (for example, serial numbers with xxx). This often occurs when swapping one formatter for another.	N/A	Ignores this anomaly and removes it from the open anomalies list.	N/A
Inconsistent Totals	Data collections for **Device Utilization** and **Hourly Peak Usage**	The page counts do not reconcile (for example, the page count total is different from the sum of color and mono page counts).	Deletes all the Collection data collected on the device for the given collection period. Future collections during that time will continue as normal.	Ignores this anomaly and removes it from the open anomalies list.	N/A
Abnormal Increasing Page Counts	Data collections for **Device Utilization** and **Hourly Peak Usage**	The page counts collected were over 10,000 pages for a given collection period.	Deletes the Collection data collected on the device for the given collection period. Future collections during that time will continue as normal.	Ignores this anomaly and removes it from the open anomalies list.	Adjusts the current values for the anomalous collection, subtracting the abnormally large number of pages from the count.
Descending Page Counts	Data collections for **Device Utilization** and **Hourly Peak Usage**	The collected page count has decreased; and will be treated as if no pages were printed on the device.	Deletes the Collection data collected on the device for the given collection period. Future collections during that time will continue as normal.	Ignores this anomaly and removes it from the open anomalies list.	Adjusts the current values for the anomalous collection, subtracting the actual negative pages from the collection.
Possibly missing job data	Data collections for **By User**	HP Web Jetadmin has detected that print jobs may have been missed because the device didn't send traps for the jobs.	N/A	Ignores this anomaly and removes it from the open anomalies list.	N/A

Anomaly	Type	Description	Reset	Ignore	Adjust
Removed from trap table	Data collections for By User	The HP Web Jetadmin server was removed from the device's trap table. Traps for completed jobs will not be received.	N/A	Ignores this anomaly and removes it from the open anomalies list.	Altering this anomaly adds the HP Web Jetadmin server to the **Trap Table**.
Device is not unique	All data collections	HP Web Jetadmin was not able to obtain sufficient data to uniquely identify the device.	N/A	Ignores this anomaly and removes it from the open anomalies list.	N/A
Not supported by device	All data collections	The device does not support the requirements of the data collection.	N/A	Ignores this anomaly and removes it from the open anomalies list.	N/A
Device is under contract	All data collections	HP Web Jetadmin could not complete the report subscription for the device because it is under contract.	N/A	Ignores this anomaly and removes it from the open anomalies list.	N/A
Failed to connect to device	All data collections	HP Web Jetadmin was unable to communicate with the device.	N/A	Ignores this anomaly and removes it from the open anomalies list.	N/A
SNMP trap table is full on device	All data collections	HP Web Jetadmin could not complete the collection subscription for the device because the device's trap table is full	N/A	Ignores this anomaly and removes it from the open anomalies list.	N/A
Device does not support required SNMP trap	All data collections	HP Web Jetadmin could not complete the collection subscription for the device because the device does not support the required SNMP trap	N/A	Ignores this anomaly and removes it from the open anomalies list.	N/A
Credentials are required to subscribe to device	All data collections	HP Web Jetadmin needs credentials for the device before the report subscription can be completed.	N/A	Ignores this anomaly and removes it from the open anomalies list.	N/A
Subscription was skipped for device	All data collections	During upgrade, the collection subscription request for this device was skipped by the user.	N/A	Ignores this anomaly and removes it from the open anomalies list.	N/A

Report Generation

After data collection has been performed, you can generate reports. The type of reports that can be generated is dependent upon the type of data collection that you ran.

Reports - Common Tasks Task Module

The **Reports - Common Tasks** task module provides links that initiate the following tasks for reports:

- Generate a report
- Schedule a report
- Create a report template
- Apply a report template to devices
- Edit a report template
- Delete a report template
- Copy a report template to create a new template
- View an archived report
- Send an archived report to an email address
- Save an archived report as a comma-separated values (CSV) or HTML file
- Delete an archived report

Generate Reports

Before you can generate a report, you must specify the report type, devices or device groups included in the report, device information included in the report, time period for the report, and if the report is archived or sent to an email address. You can generate the report immediately or schedule the report to run on a recurring basis.

You can select the device information that is included in the report from the **Available columns** list in the **Generate Report** wizard. Because there are so many columns available, the list provides three categories of columns—**Favorites**, **All**, and **Obsolete**. Each category contains a list of columns and additional categories that you can select.

When generating and displaying reports, HP Web Jetadmin uses either a period (.) or comma (,) as the decimal separator depending on the display language that is configured on the HP Web Jetadmin client. For example, the decimal separator is a period if the display language is English and the decimal separator is a comma if the display language is German. To change the display language in Windows on the HP Web Jetadmin client, go to **Start** > **Control Panel** > **Clock, Language, and Region** > **Region and Language**, and then click the **Keyboard and Languages** tab. From the **Choose a display language** list, select the language. If the **Choose a display language** list is not available, an additional language must be installed first.

NOTE: When viewing device lists, the decimal separator might be different from the decimal separator that is used when generating and displaying reports. HP Web Jetadmin uses either a period (.) or comma (,) as the decimal separator in device list columns depending on the settings that are configured on the **Formats** tab in the **Region and Language** dialog.

When reports are generated and sent to shared email addresses, HP Web Jetadmin uses either a period (.) or comma (,) as the decimal separator depending on the preferred language that is configured for each shared email address. For example, the decimal separator is a period in English reports and a comma in German reports. For instructions on specifying the preferred language for shared email addresses, see Manage the Shared Email Addresses on page 48.

Use the following steps to generate a report:

1. In the **Device Management** navigation pane, right-click **Reports**, and then select **Generate report**. The **Generate Report** wizard starts.

2. To use a report template, select the **Use template** option, and then select a template from the list.

   -or-

   To create a custom report, select the **Custom** option, and then select the report type from the list.

   NOTE: Data collection must be enabled for the report type that is selected. For more information about configuring data collection, see Data Collection on page 225.

3. To schedule the report to run at a later time, select the **Schedule report** checkbox.

4. Click the **Next** button.

5. To specify the devices that are included in the report by selecting individual devices, use the following steps:

   a. Select the **Devices** option.

   b. To display only the devices that are in a specific device list, click the **...** button, and then select the device list.

   c. From the **Available devices** column, select the devices, and then click the **>** button.

      -or-

      To include all of the devices, click the **>>** button.

   -or-

   To specify the devices that are included in the report by selecting a device group, use the following steps:

   NOTE: If a report for a device group is scheduled, the report includes the devices that are in the device group when the scheduled task starts.

   a. Select the **Groups** option.

   b. Click the **...** button, and then select the device group.

   c. To include the subgroups in a device group, select the **Include subgroups** checkbox.

      CAUTION: If subgroups are included in the report, HP Web Jetadmin might take more time to generate the report and there might be a significant increase in network traffic.

6. Click the **Next** button.

7. If data collection has not been enabled for the selected devices, the **Enable data collection** page appears. Use the following steps to enable data collection:

   a. Click the **Start Data Collection** button. The **Add Devices to Data Collection** wizard starts.

   b. From the **Time zone** list, select the time zone that HP Web Jetadmin uses for the data collection.

   c. From the **Time** list, select the time when HP Web Jetadmin collects data from the devices.

   d. Click the **Next** button.

   e. On the **Confirm** page, verify that the information is correct, and then click the **Add Devices** button.

f. On the **Results** page, click the **Done** button.

g. On the **Enable data collection** page, click the **Next** button.

8. On the **Specify report settings** page, specify the settings for the report. For more information about the settings for a specific report, click one of the following links:

    - Accessory Inventory Report Settings on page 238
    - Device Inventory Report Settings on page 239
    - Device Utilization Report Settings on page 240
    - Device Utilization by User Report Settings on page 241
    - Event Log History Report Settings on page 243
    - Hourly Peak Usage Report Settings on page 244
    - Supply Ordering Report Settings on page 245
    - Supply Replacement Forecast Report Settings on page 246
    - Supply Usage Report Settings on page 246

9. Click the **Next** button.

10. To only archive the report, select the **Archive only** option.

    -or-

    To send the report to email recipients, use the following steps:

    a. Select the **Email** option.

    b. In the **Send to** box, enter the email addresses of the recipients separated by a semi-colon (;).

    -or-

    Click the **Browse** button. On the **Select Email Address** window, select the email addresses from the **Available addresses** list, and then click the **>** button. Click the **OK** button.

    NOTE: When reports are generated and sent to shared email addresses, HP Web Jetadmin uses either a period (.) or comma (,) as the decimal separator depending on the preferred language that is configured for each shared email address. For example, the decimal separator is a period in English reports and a comma in German reports. For instructions on specifying the preferred language for shared email addresses, see Manage the Shared Email Addresses on page 48.

    c. To send the report as an HTML file, select the **HTML** option.

    -or-

    To send the report as a comma-separated values (CSV) file, select the **CSV** option.

11. Click the **Next** button.

12. In the **Report name** box, enter a name for the report.

13. In the **Archive report for** box, enter the number of days that HP Web Jetadmin keeps the archived report.

14. Click the **Next** button.

15. If the **Specify schedule options** page appears, use the following steps:

a. From the **Start time** lists, select the date and time that the scheduled report is generated.

b. In the **Recurrence** section, select the option that specifies how often the scheduled report is generated, and then specify any associated settings.

c. Click the **Next** button.

16. On the **Confirm** page, verify that the information is correct, and then click the **Create Schedule** button.

17. On the **Report Generation Complete** page, click the **Done** button.

Accessory Inventory Report Settings

Following are steps to complete the **Specify report settings** page for the **Accessory Inventory** report in the **Generate Report** wizard.

1. In the **Formatting (General)** section:

   - Select the subtype for this report.

   - Select how to group the data. Each group will be a separate section of the report. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example of this is **Device Model**. If chosen, HP Web Jetadmin groups all of the same device models next to each other in the report.

   - Select how to sort the data. Data within each group (as specified above) will be sorted this way. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example is **IP Address**: when chosen, HP Web Jetadmin orders the devices within the report by their IP addresses. Of course, the ordering occurs within the Group by subsets.

   - To exclude any device that has no data collected for it, select **Exclude devices with no collected data**.

2. In the **Formatting (Detailed)** section, select whether or not to show all accessories.

   - To show all accessories, click **Show all accessories**.

   - To show only some accessories, leave **Show all accessories** unchecked. Then select the accessories to show from **Available accessories**. and click the arrow buttons between the two lists to move them to **Selected accessories**.

3. In the **Date range** section:

   - **Previous time period**:

     This option lets you request data from a specified number of previous days, weeks, months, and years. TO base this from today, select **From today**; for example, if today is April 4, then previous month would be March 4 to April 4. If you request for the last month, that would be April 1 to April 30.

     NOTE: This option is not available if you are scheduling this report for a later time.

   - **Previous quarter**: This option lets you request data based on company quarters.

   - **Custom range**: To specify a custom date range, specify the date range for the data to be included on the report.

NOTE: Even though data can be collected for a period of time, not all of that data has to be included on the report. You can determine a smaller time frame for the data that is actually included in the report.

NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

4. In the **Device Information** section, select the column category (**Favorites**, **All**, or **Obsolete**) from the **Source** list.

   Select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

5. In the **Report data** section, select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

6. Click the **Next** button. For more information about the remaining pages in the **Generate Report** wizard, return to the task in Generate Reports on page 235.

Device Inventory Report Settings

Following are steps to complete the **Specify report settings** page for the **Device Inventory** report in the **Generate Report** wizard.

1. In the **Formatting (General)** section:

   - Select the subtype for this report.

   - Select how to group the data. Each group will be a separate section of the report. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example of this is **Device Model**. If chosen, HP Web Jetadmin groups all of the same device models next to each other in the report.

   - Select how to sort the data. Data within each group (as specified above) will be sorted this way. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example is **IP Address**: when chosen, HP Web Jetadmin orders the devices within the report by their IP addresses. Of course, the ordering occurs within the Group by subsets.

   - To exclude any device that has no data collected for it, select **Exclude devices with no collected data**.

2. In the **Date range** section:

   - **Previous time period**:

     This option lets you request data from a specified number of previous days, weeks, months, and years. TO base this from today, select **From today**; for example, if today is April 4, then previous month would be March 4 to April 4. If you request for the last month, that would be April 1 to April 30.

NOTE: This option is not available if you are scheduling this report for a later time.

- **Previous quarter**: This option lets you request data based on company quarters.

- **Custom range**: To specify a custom date range, specify the date range for the data to be included on the report.

NOTE: Even though data can be collected for a period of time, not all of that data has to be included on the report. You can determine a smaller time frame for the data that is actually included in the report.

NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

3. In the **Device Information** section, select the column category (**Favorites**, **All**, or **Obsolete**) from the **Source** list.

   Select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

4. In the **Report data** section, select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

5. Click the **Next** button. For more information about the remaining pages in the **Generate Report** wizard, return to the task in Generate Reports on page 235.

Device Utilization Report Settings

Following are steps to complete the **Specify report settings** page for the **Device Utilization** report in the **Generate Report** wizard.

1. In the **Formatting (General)** section:

   - Select the subtype for this report.

   - Select how to group the data. Each group will be a separate section of the report. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example of this is **Device Model**. If chosen, HP Web Jetadmin groups all of the same device models next to each other in the report.

   - Select how to sort the data. Data within each group (as specified above) will be sorted this way. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example is **IP Address**: when chosen, HP Web Jetadmin orders the devices within the report by their IP addresses. Of course, the ordering occurs within the Group by subsets.

   - Select the **Report Interval** (Daily, Weekly, Monthly, or None).

- To include totals for any specific column, select **Show totals**.
- To exclude any device that has no data collected for it, select **Exclude devices with no collected data**.

2. In the **Formatting (Detailed)** section (only applicable for the **Job Type (Details)** subtype), select whether or not to show all media sizes.

    - To show all media sizes, click **Show all media sizes**.
    - To show only some media sizes, leave **Show all media sizes** unchecked. Then select the media sizes to show from **Available media sizes**. and click the arrow buttons between the two lists to move them to **Selected media sizes**.

3. In the **Date range** section:

    - **Previous time period**:

      This option lets you request data from a specified number of previous days, weeks, months, and years. TO base this from today, select **From today**; for example, if today is April 4, then previous month would be March 4 to April 4. If you request for the last month, that would be April 1 to April 30.

      NOTE: This option is not available if you are scheduling this report for a later time.

    - **Previous quarter**: This option lets you request data based on company quarters.
    - **Custom range**: To specify a custom date range, specify the date range for the data to be included on the report.

   NOTE: Even though data can be collected for a period of time, not all of that data has to be included on the report. You can determine a smaller time frame for the data that is actually included in the report.

   NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

   NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

   NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

4. In the **Device Information** section, select the column category (**Favorites**, **All**, or **Obsolete**) from the **Source** list.

   Select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

5. In the **Report data** section, select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

6. Click the **Next** button. For more information about the remaining pages in the **Generate Report** wizard, return to the task in Generate Reports on page 235.

Device Utilization by User Report Settings

Following are steps to complete the **Specify report settings** page for the **Device Utilization by User** report in the **Generate Report** wizard.

1. In the **Formatting (General)** section:

   - Select the subtype for this report.
   - Select how to group the data. Each group will be a separate section of the report. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example of this is **Device Model**. If chosen, HP Web Jetadmin groups all of the same device models next to each other in the report.
   - Select how to sort the data. Data within each group (as specified above) will be sorted this way. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example is **IP Address**: when chosen, HP Web Jetadmin orders the devices within the report by their IP addresses. Of course, the ordering occurs within the Group by subsets.
   - To include totals for any specific column, select **Show totals**.
   - To exclude any device that has no data collected for it, select **Exclude devices with no collected data**.

2. In the **Date range** section:

   - **Previous time period**:

     This option lets you request data from a specified number of previous days, weeks, months, and years. TO base this from today, select **From today**; for example, if today is April 4, then previous month would be March 4 to April 4. If you request for the last month, that would be April 1 to April 30.

     NOTE: This option is not available if you are scheduling this report for a later time.
   - **Previous quarter**: This option lets you request data based on company quarters.
   - **Custom range**: To specify a custom date range, specify the date range for the data to be included on the report.

   NOTE: Even though data can be collected for a period of time, not all of that data has to be included on the report. You can determine a smaller time frame for the data that is actually included in the report.

   NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

   NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

   NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

3. In the **Device Information** section, select the column category (**Favorites**, **All**, or **Obsolete**) from the **Source** list.

   Select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

4. In the **Report data** section, select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

5. Click the **Next** button. For more information about the remaining pages in the **Generate Report** wizard, return to the task in Generate Reports on page 235.

Event Log History Report Settings

Following are steps to complete the **Specify report settings** page for the **Event Log History** report in the **Generate Report** wizard.

1. In the **Formatting (General)** section:
   - Select the subtype for this report.
   - Select how to group the data. Each group will be a separate section of the report. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example of this is **Device Model**. If chosen, HP Web Jetadmin groups all of the same device models next to each other in the report.
   - Select how to sort the data. Data within each group (as specified above) will be sorted this way. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example is **IP Address**: when chosen, HP Web Jetadmin orders the devices within the report by their IP addresses. Of course, the ordering occurs within the Group by subsets.
   - To include totals for any specific column, select **Show totals**.
   - To exclude any device that has no data collected for it, select **Exclude devices with no collected data**.
2. In the **Date range** section:
   - **Previous time period**:

     This option lets you request data from a specified number of previous days, weeks, months, and years. TO base this from today, select **From today**; for example, if today is April 4, then previous month would be March 4 to April 4. If you request for the last month, that would be April 1 to April 30.

     NOTE: This option is not available if you are scheduling this report for a later time.
   - **Previous quarter**: This option lets you request data based on company quarters.
   - **Custom range**: To specify a custom date range, specify the date range for the data to be included on the report.

   NOTE: Even though data can be collected for a period of time, not all of that data has to be included on the report. You can determine a smaller time frame for the data that is actually included in the report.

   NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

   NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

   NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

3. In the **Device Information** section, select the column category (**Favorites**, **All**, or **Obsolete**) from the **Source** list.

   Select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

4. In the **Report data** section, select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

5. Click the **Next** button. For more information about the remaining pages in the **Generate Report** wizard, return to the task in Generate Reports on page 235.

Hourly Peak Usage Report Settings

Following are steps to complete the **Specify report settings** page for the **Hourly Peak Usage** report in the **Generate Report** wizard.

1. In the **Formatting (General)** section:

   - Select the subtype for this report.

   - Select how to group the data. Each group will be a separate section of the report. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example of this is **Device Model**. If chosen, HP Web Jetadmin groups all of the same device models next to each other in the report.

   - Select how to sort the data. Data within each group (as specified above) will be sorted this way. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example is **IP Address**: when chosen, HP Web Jetadmin orders the devices within the report by their IP addresses. Of course, the ordering occurs within the Group by subsets.

   - To exclude any device that has no data collected for it, select **Exclude devices with no collected data**.

2. In the **Formatting (Detailed)** section, select the time range. You can select the entire day or a start and end time.

3. In the **Date range** section:

   - **Previous time period**:

     This option lets you request data from a specified number of previous days, weeks, months, and years. TO base this from today, select **From today**; for example, if today is April 4, then previous month would be March 4 to April 4. If you request for the last month, that would be April 1 to April 30.

     NOTE: This option is not available if you are scheduling this report for a later time.

   - **Previous quarter**: This option lets you request data based on company quarters.

   - **Custom range**: To specify a custom date range, specify the date range for the data to be included on the report.

   NOTE: Even though data can be collected for a period of time, not all of that data has to be included on the report. You can determine a smaller time frame for the data that is actually included in the report.

   NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

4. In the **Device Information** section, select the column category (**Favorites**, **All**, or **Obsolete**) from the **Source** list.

   Select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

5. In the **Report data** section, select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

6. Click the **Next** button. For more information about the remaining pages in the **Generate Report** wizard, return to the task in Generate Reports on page 235.

Supply Ordering Report Settings

Following are steps to complete the **Specify report settings** page for the **Supply Ordering** report in the **Generate Report** wizard.

1. In the **Formatting (General)** section:

   - Select the subtype for this report.
   - Select how to group the data. Each group will be a separate section of the report. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example of this is **Device Model**. If chosen, HP Web Jetadmin groups all of the same device models next to each other in the report.
   - Select how to sort the data. Data within each group (as specified above) will be sorted this way. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example is **IP Address**: when chosen, HP Web Jetadmin orders the devices within the report by their IP addresses. Of course, the ordering occurs within the Group by subsets.
   - To exclude any device that has no data collected for it, select **Exclude devices with no collected data**.

2. In the **Formatting (Detailed)** section, select the **Threshold** for the supplies to be included in the report. You can also choose to include the **Order Supplies** button which provides easy access to the HP SureSupply website.

NOTE: This option to order supplies is only displayed if you have enabled **Shop for Supplies** in **Tools > Options > Device Management > Supplies > Supplies Reordering**, see Configure the Shop for Supplies Link in Reports on page 83)

3. In the **Device Information** section, select the column category (**Favorites**, **All**, or **Obsolete**) from the **Source** list.

   Select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.

4. In the **Report data** section, select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.
5. Click the **Next** button. For more information about the remaining pages in the **Generate Report** wizard, return to the task in Generate Reports on page 235.

Supply Replacement Forecast Report Settings

Following are steps to complete the **Specify report settings** page for the **Supply Replacement Forecast** report in the **Generate Report** wizard.

1. In the **Formatting (General)** section:
   - Select the subtype for this report.
   - Select how to group the data. Each group will be a separate section of the report. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example of this is **Device Model**. If chosen, HP Web Jetadmin groups all of the same device models next to each other in the report.
   - Select how to sort the data. Data within each group (as specified above) will be sorted this way. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

     An example is **IP Address**: when chosen, HP Web Jetadmin orders the devices within the report by their IP addresses. Of course, the ordering occurs within the Group by subsets.
   - To exclude any device that has no data collected for it, select **Exclude devices with no collected data**.
2. In the **Formatting (Detailed)** section, the **Forecast period**. You can also choose to include the **Order Supplies** button which provides easy access to the HP SureSupply website.

   NOTE: This option to order supplies is only displayed if you have enabled **Shop for Supplies** in **Tools > Options > Device Management > Supplies > Supplies Reordering**, see Configure the Shop for Supplies Link in Reports on page 83)
3. In the **Device Information** section, select the column category (**Favorites**, **All**, or **Obsolete**) from the **Source** list.

   Select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.
4. In the **Report data** section, select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.
5. Click the **Next** button. For more information about the remaining pages in the **Generate Report** wizard, return to the task in Generate Reports on page 235.

Supply Usage Report Settings

Following are steps to complete the **Specify report settings** page for the **Supply Usage** report in the **Generate Report** wizard.

1. In the **Formatting (General)** section:

- Select the subtype for this report.
- Select how to group the data. Each group will be a separate section of the report. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

  An example of this is **Device Model**. If chosen, HP Web Jetadmin groups all of the same device models next to each other in the report.
- Select how to sort the data. Data within each group (as specified above) will be sorted this way. You can also select a primary and a secondary sort. To have the data sorted in ascending order, select **Ascending**.

  An example is **IP Address**: when chosen, HP Web Jetadmin orders the devices within the report by their IP addresses. Of course, the ordering occurs within the Group by subsets.
- To exclude any device that has no data collected for it, select **Exclude devices with no collected data**.

2. In the **Formatting (Detailed)** section, specify the **Usage period** and the installation state:
   - **Active Only**: installed in the printer.
   - **Removed Only**: removed from the printer.
3. In the **Device Information** section, select the column category (**Favorites**, **All**, or **Obsolete**) from the **Source** list.

   Select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.
4. In the **Report data** section, select the columns to be displayed from **Available columns** and click **>** to move them to **Selected columns**.
5. Click the **Next** button. For more information about the remaining pages in the **Generate Report** wizard, return to the task in Generate Reports on page 235.

Schedule a Report

Reports can be generated as you request them (if data collection has been enabled) or they can be scheduled to be generated at a future time. This might reduce network traffic at particular heavy times, or it might give the data collection process time to collect the data necessary to make the report meaningful.

NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

Use the following steps to schedule a report:

1. Select **Reports** from the left navigation pane. The **Reports** page is displayed.

   In the **Report Management - Common Tasks** task module click **Generate report**. The **Generate Report** wizard is started with the **Choose report options** page displayed.

2. If templates have been created, you can select an existing template from the **Use template** drop-down box.

   If there are no existing templates or if you want to request a custom report, select the report type from the drop down under **Custom**.

   NOTE: Be sure and select a report that matches the type of data collection you specified in Data Collection on page 225. If you find you need a different report, you might have to go back to Data Collection on page 225 and select a different type of data collection.

   Click **Next**. If any of the devices you selected have not been added to the corresponding data collection, the **Enable data collection** page is displayed. You can choose to add those devices to the data collection by clicking **Start Data Collection**. This will launch the **Add Devices to Data Collection** wizard (see Add Devices to Data Collection on page 227). You can add those devices at a later time.

3. Click **Next**. The **Select devices** page is displayed.

4. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

   To select an entire group instead of individual devices, change the selection method to **Groups**. Tasks can be performed on a single group or a group and all of its subgroups.

   NOTE: If subgroups are included, the task might take longer to complete and network traffic might increase significantly. HP recommends that you include subgroups only when necessary.

   If a task is scheduled for a group, the task uses the devices that are in the group when the task starts. If the devices that are in the group are changed, you do not have to delete the scheduled task and create a new scheduled task.

   Click **Next**. The **Specify report settings** page is displayed. For detailed information about this page for a specific report, select one of the following:

   - Accessory Inventory Report Settings on page 238
   - Device Inventory Report Settings on page 239
   - Device Utilization Report Settings on page 240
   - Device Utilization by User Report Settings on page 241
   - Event Log History Report Settings on page 243
   - Hourly Peak Usage Report Settings on page 244
   - Supply Ordering Report Settings on page 245
   - Supply Replacement Forecast Report Settings on page 246
   - Supply Usage Report Settings on page 246

5. After you have completed the **Specify report settings** page, click **Next**; the **Specify report name** page is displayed.

6. Enter the name for this report and specify how long you want to keep this report.

NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

7. If you are scheduling this report for a later time, the **Specify schedule options** page is displayed. Select the start date and time for your report and also how often it should run:

   - **Start time**: Specifies when the configuration will launch.
   - **Recurrence**, **Once**: launches only once in the specified schedule.
   - **Recurrence**, **Daily**: task will recur daily once per day or once per weekday depending on the selected setting.
   - **Recurrence**, **Weekly**: task will recur once every X weeks on the day specified depending on the setting.
   - **Recurrence**, **Monthly**: task will recur once every X months on XX day depending on setting; or, task will recur on specified day pattern depending on setting.

8. Click **Next**. The **Confirm** page is displayed, summarizing all of the report format options you have selected for this report.

9. Click **Create Schedule**. The **Report Generation Complete** page is displayed showing the actual report generation.

10. Click **Done** to display the **Reports** page.

Deleting Scheduled Reports

You can delete a report after it has been scheduled, if it has not been generated, through the **Reports - Scheduled Reports** task module.

1. In **Reports**, display the **Reports - Scheduled Reports** task module.

2. Highlight the report to delete and click **Delete**. The **Confirm Delete** message is displayed.

3. Click **Yes**. The previous page is displayed again.

Editing the Schedule for a Report

You can edit the schedule for a report, if the report has not been generated yet, through the **Reports - Scheduled Reports** task module.

NOTE: If a task is scheduled by using a template, the task uses the settings that are defined in the template when the task starts. If the template is updated, the updated settings are used the next time the task runs.

NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

NOTE: Scheduled tasks are displayed in the **Scheduled Tasks** task module on the **Device**, **Discovery**, **Configuration**, **Firmware**, **Reports**, **Storage**, **Solutions**, and **Application Management** pages. You can also display any task module on the **Overview** page.

1. Select **Reports** from the left navigation pane. The **Reports** page is displayed.

   Display the **Reports - Scheduled Reports** task module. The reports that have been scheduled are listed.

2. Highlight the report click **Edit**. The **Edit Schedule (Report Generation Task)** wizard is displayed.

3. Make changes to the schedule that had been created for the report. When done, click **Next**. The **Confirm** page is displayed.

4. Review your selections and then click **Next**. The **Progress** page is displayed. When done, click **Done**.

Email Reports

HP Web Jetadmin can attach reports to an email as an HTML or comma-separated values (CSV) file and send the email to a recipient. The SMTP gateway must be configured before HP Web Jetadmin can send reports to an email recipient. For more information about configuring the SMTP gateway, see Configure the SMTP Gateway Settings on page 47.

When new email addresses are added to the shared email addresses in HP Web Jetadmin, the preferred language for each email address is specified. The decimal separator that HP Web Jetadmin uses in the reports is either a comma (,) or a period (.) depending on the preferred language that is specified for each shared email address.

To send a report to a shared email address in a different language, the preferred language for that shared email address must be changed first. For more information about specifying the preferred language for a shared email address, see Manage the Shared Email Addresses on page 48.

Save Archived Reports

You can request that a report be saved as an HTML document anywhere on your network. When you select **Save As**, you can type the filename and location or browse for the location. The report will automatically be saved in HTML format.

You can request that a report be exported in comma-separated value (CSV) file format. CSV is a file type that stores tabular data (like in an Excel sheet) and is common on all computer platforms. CSV is one implementation of a delimited text file, which uses a comma to separate values. However, CSV differs from other delimiter separated file formats in using a " (double quote) character around fields that contain reserved characters (such as commas or newlines). Most other delimiter formats either use an escape character such as a backslash, or have no support for reserved characters. In computer science terms, this type of format is called a flat file because only one table can be stored in a CSV file. Most systems use a series of tables to store their information, which must be flattened into a single table often with information repeated over several rows to create a delimited text file.

Report Templates

In **Report Templates**, you can:

- Create a Report Template on page 251
- Apply a Report Template on page 253

- Edit a Report Template on page 253
- Delete a Report Template on page 254
- Copy a Report Template on page 255
- **View**: view a report template that has been previously created (see View Report Templates on page 251).

View Report Templates

1. Expand the **Reports** menu in the left navigation pane and then expand **Report Generation**. Then click **Templates**.
2. Click on the template to view.

Create a Report Template

A report template contains a set of criteria including the report type, devices, and the report format. After a report template is created, you can apply it to generate a report easily.

Any number of templates can be added to the twenty pre-existing templates that come with HP Web Jetadmin:

- By User - Application
- By User - Color/Mono
- By User - Print Server
- By User - Simplex/Duplex
- Device Utilization - Color/Mono
- Device Utilization - Job Type
- Device Utilization - Media Size
- Device Utilization - Simplex/Duplex
- Event Log - History
- Hourly Peak Usage - After Hours Printing
- Hourly Peak Usage - Business Hours
- Supplies - Current Status
- Supplies - Detailed Forecast
- Supplies - Inventory
- Supplies - Ordering Details
- Supplies - Purchasing Planning
- Supplies - Replacement Efficiency
- Supplies - Replacement Plan
- Supplies - Shopping List
- Supplies - Supply Efficiency

NOTE: These templates are default templates and cannot be edited or renamed. If you would like to alter the functionality of the default template, you can copy the default template and edit the saved copy (see Copy Template Wizard on page 99). You can delete the default templates. If you choose to restore them this is performed by going to **Tools** > **Options** > **Device Management** > **Report** > **General** and clicking **Restore**. This restores all report generation default templates.

Create Report Template is the wizard used to customize and store reports settings. Once the wizard is launched, you can select any one of the available **Report types** and then select settings for this template, including Report Format, Report Columns, Destination Settings, and more.

Use the following steps to create a report template:

1. Expand the **Reports** menu in the left navigation pane and then select **Report Generation**.

   In the **Reports - Common Tasks** task module, select **Create report template**. The **Create Report Template** wizard is started with the **Select report type** page displayed.

2. Highlight the report type and click **Next**. (Only one report type may be selected at a time.) The **Specify report settings** page is displayed.

3. For detailed information about this page for a specific report, select one of the following:

   - Accessory Inventory Report Settings on page 238
   - Device Inventory Report Settings on page 239
   - Device Utilization Report Settings on page 240
   - Device Utilization by User Report Settings on page 241
   - Event Log History Report Settings on page 243
   - Hourly Peak Usage Report Settings on page 244
   - Supply Ordering Report Settings on page 245
   - Supply Replacement Forecast Report Settings on page 246
   - Supply Usage Report Settings on page 246

4. After you have defined the report format, click **Next**. The **Specify destination options** page is displayed.

5. Select how you want the report displayed (either on the page or directly to email). If sending the report to email addresses, you can either browse for those addresses or you can enter them manually. Separate each address with a semi-colon.

6. Specify the report destination:

   - **Archive only**: saves the report on the HP Web Jetadmin server.
   - **Email**: send the report to an email address (Email Reports on page 250). Type the email address on this page or browse for the correct email address.

7. Specify the file format:

   - **HTML**: save the file as an HTML document (Save Archived Reports on page 250).
   - **CSV**: export the report as a CSV document (Email Reports on page 250).

   Click **Next**; the **Specify name** page is displayed.

8. Type the name for this report template and then click **Next**.

9. The **Confirm** page is displayed, summarizing all of the report format options you have selected for this report. Click **Create Template**.

10. The **Results** page is displayed.

11. Click **Done** to display the **Report Generation** page.

Apply a Report Template

A report template contains a set of criteria including the report type, devices, and the report format. After a report template is created, you can apply it to generate a report easily.

Use the following steps to apply a report template:

1. Expand the **Reports** menu in the left navigation pane and select **Report Generation**.

   In the **Reports - Common Tasks** task module, click **Apply report template**. The **Generate Report** wizard is started with the **Choose report options** page displayed.

2. In the **Use template** drop-down box, highlight the template you want to use and click **Next**. The **Specify date range for report** page is displayed.

3. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

   To select an entire group instead of individual devices, change the selection method to **Groups**. Tasks can be performed on a single group or a group and all of its subgroups.

   NOTE: If subgroups are included, the task might take longer to complete and network traffic might increase significantly. HP recommends that you include subgroups only when necessary.

   If a task is scheduled for a group, the task uses the devices that are in the group when the task starts. If the devices that are in the group are changed, you do not have to delete the scheduled task and create a new scheduled task.

4. Click **Next**; the **Specify report name** page is displayed. Type the name for this report template and then click **Next**.

5. The **Confirm** page is displayed, summarizing all of the report format options you have selected for this report. Click **Next**.

6. The **Report Generation Complete** page is displayed showing the actual report generation.

7. Click **Done** to display the **Reports** page.

Edit a Report Template

Use the following steps to edit a report template:

1. Expand the **Reports** menu in the left navigation pane and then select **Report Generation**.

   In the **Reports - Common Tasks** task module, select **Edit report template**. The **Edit Report Template** wizard is started with the **Select template** page displayed.

2. Highlight the template to edit and click **Next**. (Only one template may be selected at a time.) The **Specify report settings** page is displayed.

3. For detailed information about this page for a specific report, select one of the following:

- Accessory Inventory Report Settings on page 238
- Device Inventory Report Settings on page 239
- Device Utilization Report Settings on page 240
- Device Utilization by User Report Settings on page 241
- Event Log History Report Settings on page 243
- Hourly Peak Usage Report Settings on page 244
- Supply Ordering Report Settings on page 245
- Supply Replacement Forecast Report Settings on page 246
- Supply Usage Report Settings on page 246

4. After you have defined the report format, click **Next**. The **Specify destination options** page is displayed.
5. Select how you want the report displayed (either on the page or directly to email). If sending the report to email addresses, you can either browse for those addresses or you can enter them manually. Separate each address with a semi-colon.
6. Specify the report destination:
   - **Archive only**: saves the report on the HP Web Jetadmin server.
   - **Email**: send the report to an email address (Email Reports on page 250). Type the email address on this page or browse for the correct email address.
7. Specify the file format:
   - **HTML**: save the file as an HTML document (Save Archived Reports on page 250).
   - **CSV**: export the report as a CSV document (Email Reports on page 250).

   Click **Next**; the **Specify name** page is displayed.
8. Type the name for this report template and then click **Next**.
9. The **Confirm** page is displayed, summarizing all of the report format options you have selected for this report. Click **Next**.
10. The **Results** page is displayed showing the actual report generation.
11. Click **Done** to display the **Report Generation** page.

Delete a Report Template

Use the following steps to delete a report template:

1. Expand the **Reports** menu in the left navigation pane and then select **Report Generation**.

   In the **Reports - Common Tasks** task module, select **Delete report template**. The **Delete Report Templates** wizard is started with the **Select template** page displayed.
2. Highlight the template to delete and click **Next**. (Only one template may be selected at a time.) The **Confirm** page is displayed.
3. Click **Next**. The **Results** page is displayed.
4. Click **Done** to display the **Report Generation** page.

Copy a Report Template

Throughout **Device Management** view, templates can be created and managed to save you time and provide consistency. Templates contain configuration preferences (that vary by template type) and can be applied to devices or groups. Templates are available in **Configuration**, **Alerts**, **Discovery**, **Data Collection**, and **Report Generation**. For more information, see Copy Template Wizard on page 99.

Archived Reports

Archived Reports stores all previously-generated reports and gives you a way to display them. You can view archived reports, export them to CSV format, or delete them. An adjustable 90 day time-to-live (TTL) setting erases these reports as they age. Once the report has reached this value, HP Web Jetadmin automatically clears it from the archive.

View Archived Reports

You can view any report that has already been generated through **View archived reports**. All reports that have been generated are stored in **Archived Reports**.

Use the following steps to view an archived report:

1. In the left navigation pane, expand **Reports**.

   Select **Archived Reports**. The **Archived Reports** page is displayed.
2. Highlight the report to view and click **View**.
3. Now you can:
   - Email Reports on page 250.
   - Save Archived Reports on page 250.
   - **Print**: select **Print** and then select the printer to send the report to.
4. Click **Close**. The **Archived Reports** page is displayed.

Delete Archived Reports

Use the following steps to delete an archived report:

1. In the left navigation pane, expand **Reports** and then click **Archived Reports**. The **Archived Reports** page is displayed.
2. Highlight the archived report you want to delete and click **Delete**. The **Delete Archived Report** wizard is started with the **Confirm** page displayed.
3. If you need to make changes, click **Back**. If this is the correct report to delete, click **Next**. The **Results** page is displayed.
4. The report you deleted is displayed. Click **Done**.

Storage

Storage provides the capability to download and manage font and macro files on devices.

Storage - Common Tasks Task Module

The **Storage - Common Tasks** task module provides links that initiate the following tasks for storage:

- Import fonts and macros into the Storage Repository
- Delete fonts and macros from the Storage Repository
- Create a storage template
- Apply a storage template to devices
- Edit a storage template
- Delete a storage template
- Copy a storage template to create a new template

Storage - Active Tasks Task Module

The **Storage - Active Tasks** task module provides a list of the storage tasks that are running. Use this task module to stop or display the status of an active task. If a storage task is stopped, any devices that have not been configured yet are not configured.

Storage - Scheduled Tasks Task Module

The **Storage - Scheduled Tasks** task module provides a list of the storage tasks that are scheduled to run. Use this task module to delete or edit the settings for a task schedule.

Storage Repository

The **Storage Repository** lets you store fonts and macros.

Import Fonts and Macros

To import font and macro files into the Storage Repository, perform the following steps:

1. In the **Device Management** navigation pane, right-click **Storage**, and then select **Import fonts and macros**. The **Import Fonts and Macros** wizard starts.
2. On the **Select fonts and macros to import** page, click **Browse**.
3. On the **Open** dialog, browse to and select the font and macro files, and then click **Open**.
4. To remove any font and macro files that currently reside in the repository from the import list, select the **Exclude fonts and macros already in the repository** checkbox. Selecting this checkbox prevents HP Web Jetadmin from overwriting any files that are already in the Storage Repository.

5. Click **Next**.
6. On the **Confirm** page, verify that the list of fonts and macros is correct, and then click **Import**.
7. On the **Results** page, click the **Done** button.

Delete Fonts and Macros

You can delete fonts and macros from the **Storage Repository**. If they have been added to devices, this does not delete them from those devices.

1. In the left navigation pane, right-click on **Storage** and then click **Delete fonts and macros**. The **Delete Fonts and Macros** wizard is started with the **Select fonts and macros** page displayed.
2. Highlight the fonts and macros you want to delete from the repository and then click **Next**. The **Confirmation** page is displayed.
3. Click **Next**. The **Results** page is displayed.
4. Click **Done**.

Edit Properties for Storage

You can configure the ID associated with each font or macro file. By default, the font and macro installation process will start assigning IDs starting with '1'. If you need specific fonts and macros to have specific ID values, then you can define those values with **Edit Properties** so that they will always get installed with those ID values.

A font and a macro may have the same ID but all fonts must have unique IDs and all macros must have unique IDs.

1. In the left navigation pane, click **Storage** and then click **Repository**. The **Storage Repository** is displayed.
2. Select the font or macro whose ID you want to change. Then click **Edit Properties**. The **Edit Resource Properties** dialog is displayed.
3. Type the new ID number and click **OK**.

Save to File

You can save fonts and macro files to a file outside of HP Web Jetadmin. This would be useful if you want to install them on a PC-connected printer at a later time.

1. In the left navigation pane, click **Storage** and then click **Repository**. On the **Repository** page, click **Save to File**. The **Save to File** wizard is started with the **Source** page displayed.
2. Choose which font and macro files you want to save by selecting **Use template** or **Select from list**; then click **Next**.
3. If you chose:
   - **Use template**:
     - The **Select template** page is displayed.
     - Select the template to use and click **Next**.
   - **Select from list**:

  - The **Select fonts and macros** page is displayed.
  - Select the font and macro files to save and click **Next**.

4. The **Confirm** page is displayed.
5. Click **Save**. The **Save as** page is displayed. Select the location and name for this file and click **Save**. The **Results** page is displayed.
6. Click **Done**.

Install Fonts and Macros on Devices

After a font or macro file has been imported into the **Storage Repository**, it can be installed on a device.

1. Access any device list.
2. Highlight the device or devices and click the **Storage** tab at the bottom portion of page. On the **View** menu, select **Fonts and Macros**.
3. Highlight the device or devices in the **Storage** tab and click **Install**. The **Install Fonts and Macros** wizard is started with the **Select fonts and macros** page displayed.
4. Select the font and macro files you want to install on the device and click **Next**. The **Specify destination** page is displayed.
5. Select the destination for the chosen font and macro files and then click **Next**. The **Options** page is displayed.
6. Make your selections and then click **Next**.
7. The **Confirm** page is displayed.
8. Click **Install**. The **Results** page is displayed.
9. Click **Done**.

Remove Font and Macro Files from Devices

After a font or macro file has been installed on a device, it can be removed from that device. It is not deleted from the **Storage Repository**.

1. Access any device list.
2. Highlight the device or devices and click the **Storage** tab at the bottom portion of page. On the **View** menu, select **Fonts and Macros**.
3. Highlight the device or devices in the **Storage** tab and click **Remove**. The **Remove Fonts and Macros** wizard is started with the **Select device resources** page displayed.
4. Select the font and macro files you want to remove from the device and click **Next**. The **Confirm** page is displayed.
5. Click **Remove**. The **Results** page is displayed.
6. Click **Done**.

Print Font/Macro

This option prints a test page of the selected font or macro.

1. Access any device list.
2. Highlight the device or devices and click the **Storage** tab at the bottom portion of page. On the **View** menu, select **Fonts and Macros**.
3. Highlight the device or devices in the **Storage** tab and click **Print Font/Macro**. The **Print Fonts and Macros** wizard is started with the **Select fonts and macros** page displayed.
4. Select the font and macro files you want to print and click **OK**.

Storage Templates

Storage templates allow a number of selected font and macro files to be installed on a group of devices or a single device, allowing any number of these files to be installed with a single command. You can:

- Create Storage Templates on page 259
- Apply a Storage Template on page 260
- Edit Storage Templates on page 260
- Delete a Storage Template on page 261.
- Copy a Storage Template on page 261
- View Storage Templates on page 261.

Create Storage Templates

Use the following steps to create a storage template:

1. In the **Device Management** navigation pane, right-click **Storage**, and then select **Create storage template**. The **Create Storage Template** wizard starts.
2. To download fonts and macros to the devices, select the **Download fonts and macros to the device(s)** option.

   -or-

   To delete fonts and macros from the devices, select the **Delete fonts and macros from the device(s)** option.
3. On the **Select fonts and macros** page, select the fonts and macros from the list, and then click the **Next** button.
4. On the **Specify destination** page, select the option that specifies where the fonts and macros are stored on the device from the **Destination** list, and then click the **Next** button.

   TIP: A device might recognize some USB devices as flash media. To determine if you should select **USB Storage** or **Flash** from the **Destination** list, select the device in any device list, and then click the **Storage** tab. Hold the cursor over the number displayed in the **Storage Media** column. In the table that opens, the **Media Type** column identifies the option that must be selected from the **Destination** list. You can use these steps to verify the destination for other media types, such as RAM disks and flash disks.
5. On the **Options** page, use the following steps to specify the overwrite options:

a. To replace the existing fonts and macros on the device with the fonts and macros in this storage template, select the **Overwrite existing fonts and macros** checkbox.

b. To replace the IDs of the existing fonts and macros on the device with the IDs of the fonts and macros in this storage template, select the **Overwrite existing fonts and macro IDs** checkbox.

c. Click the **Next** button.

6. On the **Specify name** page, enter a name for the storage template in the **Name** box, and then click the **Next** button.
7. On the **Confirm** page, verify that the information is correct, and then click the **Create** button.
8. On the **Results** page, click the **Done** button.

Apply a Storage Template

You can install storage within a template to a single device, multiple devices, or a group.

1. In the left navigation pane, click **Storage** and then click **Templates**. On the Storage **Templates** overview page, click **Apply**. The **Apply Storage Template** wizard is started with the **Select devices** page displayed.
2. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers. Then click **Next**.
3. The **Confirm** page is displayed.
4. Review the selections and click **Apply Template**. The **Results** page is displayed.
5. Click **Done**.

Edit Storage Templates

Use the following steps to edit a storage template:

1. In the **Device Management** navigation pane, expand the **Storage** option, and then select the **Templates** option.
2. In the **Templates** pane, select the storage template from the list, and then click the **Edit** button. The **Edit Storage Template** wizard starts.
3. To download fonts and macros to the devices, select the **Download fonts and macros to the device(s)** option.

   -or-

   To delete fonts and macros from the devices, select the **Delete fonts and macros from the device(s)** option.
4. Click the **Next** button.
5. On the **Select fonts and macros** page, select the fonts and macros from the list, and then click the **Next** button.
6. On the **Specify destination** page, select the option that specifies where the fonts and macros are stored on the device from the **Destination** list, and then click the **Next** button.

TIP: A device might recognize some USB devices as flash media. To determine if you should select **USB Storage** or **Flash** from the **Destination** list, select the device in any device list, and then click the **Storage** tab. Hold the cursor over the number displayed in the **Storage Media** column. In the table that opens, the **Media Type** column identifies the option that must be selected from the **Destination** list. You can use these steps to verify the destination for other media types, such as RAM disks and flash disks.

7. On the **Options** page, use the following steps to specify the overwrite options:
   a. To replace the existing fonts and macros on the device with the fonts and macros in this storage template, select the **Overwrite existing fonts and macros** checkbox.
   b. To replace the IDs of the existing fonts and macros on the device with the IDs of the fonts and macros in this storage template, select the **Overwrite existing fonts and macro IDs** checkbox.
   c. Click the **Next** button.
8. On the **Specify name** page, enter a name for the storage template in the **Name** box, and then click the **Next** button.
9. On the **Confirm** page, verify that the information is correct, and then click the **Save** button.
10. On the **Edit template results** page, click the **Done** button.

Delete a Storage Template

Delete any storage templates that are not being used.

1. In the left navigation pane, click **Storage** and then click **Templates**. The Storage **Templates** overview page is displayed.
2. Select the template to delete and click **Delete**. The **Delete Template** wizard is started with the **Confirm** page displayed.
3. Review the selection and click **Delete Template**. The **Results** page is displayed.
4. Click **Done**.

Copy a Storage Template

You can copy storage templates to create a new template. The copied template is added to the list of existing templates and the original template is unchanged.

1. In the left navigation pane, click **Storage** and then click **Templates**. The Storage **Templates** overview page is displayed.
2. Select the template to copy and click **Copy**. The **Copy Template** wizard is started with the **Specify template name** page displayed.
3. Type the name for the new template. The original template's name will not be changed.
4. Click **Next**. The **Confirm** page is displayed.
5. Review the selection and click **Copy Template**. The **Results** page is displayed.
6. Click **Done**. The new template will now be listed under **Templates** left navigation pane.

View Storage Templates

Use the following steps to view a storage template:

1. In the **Device Management** navigation pane, expand **Storage**, and then select **Templates**.
2. On the **Templates** pane, select the storage template from the list, and then click the **View** button.

Solutions

Solutions extends HP Web Jetadmin support to include new licensable and configurable solutions supplied through third parties.

HP Web Jetadmin provides functionality to manage programs that can be installed on devices. Central to the process of solution management is a **Solution Repository**, which is a collection of programs that can be installed on managed devices. Three different types of programs can be contained within the repository:

- Chailets
- Microsoft .NET Framework solutions
- Solutions

For simplicity, these program types will simply be referred to as **Solutions**.

Solutions are imported into the **Solution Repository**. Then they can be installed on a device or a group of devices. Solutions within the repository may have their properties edited or, if they are no longer needed, solutions can be removed from the repository.

On device lists, a **Solutions Tab** is provided to allow you to manage solutions that are installed on a device. You can quickly see which solutions are installed on a device and then take action to either install new solutions or remove solutions that are no longer needed.

Solutions within the repository may be combined together to create **Solution Templates**. These templates may be applied to a device or a group of devices to install one or more solutions. Functionality is provided to manage templates that have been created. Templates may be edited, copied, or removed. Applying a template means that the solutions identified within the template are installed on the device or group of devices.

Templates may also be applied as part of a **Group Policy**. A **Group Policy** is an action that is performed when a device is added to a group or removed from a group. Group policies can also be used to create workflows that define multiple actions needed to be performed on a group of devices that meet specific criteria.

Solutions - Common Tasks Task Module

The **Solutions - Common Tasks** task module provides links that initiate the following tasks for solutions:

- Import a solution
- Install a solution on devices
- Uninstall a solution from devices
- Edit the settings for a solution
- Create a solution template
- Apply a solution template to devices

Solutions - Active Tasks Task Module

The **Solutions - Active Tasks** task module provides a list of the solutions tasks that are running. Use this task module to stop or display the status of an active task. If a solutions task is stopped, any devices that have not been configured yet are not configured.

Solutions - Scheduled Tasks Task Module

The **Solutions - Scheduled Tasks** task module provides a list of the solutions tasks that are scheduled to run. Use this task module to delete or edit the settings for a solutions schedule.

Solutions Repository

The available solutions are listed on the **Solutions Repository** page. From this page you can:

- **Import solution**: import solutions into the **Solutions Repository** (Importing Solutions on page 263).
- **Edit solution**: edit solutions that have already been imported (Editing Solution Settings on page 263).
- **Remove solution**: remove solutions that have already been imported (Removing Solutions on page 264).
- **Install solution**: install solutions on devices or groups of devices (Installing Solutions on page 264).

The **Solutions Repository** can contain different types of solutions:

- Pre-installed solutions: cannot be removed.
- Added solutions: all added solutions can be edited to facilitate solution management. They include:
  - Chailets (Java-based applications)
  - Microsoft .NET Framework applications
  - Solutions

Importing Solutions

You can import solutions and then install them later on devices or groups of devices.

1. In the left navigation pane, click on **Solutions** and then click **Repository**. The **Repository** page is displayed.
2. Click **Import**. The **Import Solutions** wizard is started with the **Select files** page displayed.
3. Select a solution to import or click **Browse** to find the desired solution.
4. To import the solution, click **Import**.

Editing Solution Settings

You can make changes to solutions that have already been imported.

1. In the left navigation pane, click on **Solutions** and then click **Repository**. The **Repository** page is displayed.
2. Select a solution and click **Edit**. The **Edit Solution Settings** wizard is started.
3. If you are editing a:

- Chailet or Microsoft .NET Framework application:
  - **Description**: custom description of the application.
- **Solution**: you can edit the:
  - **Description**: custom description of the solution.
  - **Application URL**: the URL path to the location of the solution on the application depot that the device will use when obtaining the solution from that depot.

    User name and **Password** (Depot Credential): a user name and password credential used to gain access to the depot where the **Application URL** is located. The user name and password credential can be left blank, or both values must be provided.
  - **Configuration URL**: specifies where a configuration file can be retrieved to properly configure the solution.

    User name and **Password** (Depot Credential): a user name and password credential used to gain access to the depot where the **Configuration URL** is located. The user name and password credential can be left blank, or both values must be provided.
  - **License URL**: specifies where a license file can be retrieved. The license associated with the file will identify which features you have that are licensed to use within the solution.

    User name and **Password** (Depot Credential): a user name and password credential used to gain access to the depot where the **License URL** is located. The user name and password credential can be left blank, or both values must be provided.

4. After you make your edits, click **OK**.

Removing Solutions

You can remove solutions that have already been imported. All solutions can be removed except for pre-installed solutions.

1. In the left navigation pane, click on **Solutions** and then click **Repository**. The **Repository** page is displayed.
2. Select the solution to remove and click **Remove**. The **Remove Repository Solution** wizard is started with the **Confirm** page displayed.
3. To remove the solution, click **Remove**. The **Results** page is displayed.
4. Click **Done**.

Installing Solutions

You can identify a solution and then install it on one or more devices or groups of devices. You can also specify properties for the solution.

1. In the left navigation pane, click on **Solutions** and then click **Repository**. The **Repository** page is displayed.
2. Click **Install**. The **Install Solutions** wizard is started with the **Select options** page displayed.
3. Select an existing template or manually specify options.
4. To install the solution immediately, click **Next**.

   To schedule the installation for another time, click **Schedule** and then click **Next**.

NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

The **Select devices** page is displayed.

5. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers. Then click **Next**. The **Edit settings** page is displayed with the list of solutions that may be installed.

6. Select at least one solution and click **Next**. The **Edit settings** page is displayed with the list of solutions that have been selected to be installed. This page also indicates whether or not configuration settings have been supplied for the solution.

7. Depending on the type of solution, you can edit its properties. If you're editing a:

   - Solution: you can edit the:
     - **Description**: custom description of the solution.
     - **Application URL**: specifies where the solution is located. This is used to retrieve the application.
     - **Configuration URL**: specifies where a configuration file can be retrieved to properly configure the solution.
     - **License URL**: specifies where a license file can be retrieved. The license associated with the file will identify which features you have that are licensed to use within the solution.
   - Chailet or Microsoft .NET Framework application:
     - **Description**: custom description of the solution.

   Click **OK**.

8. If you are installing the solution now, the **Confirm** page is displayed.

   If you chose to schedule the installation of the solution, the **Specify schedule options** page is displayed. Assign a name and then define the date and time for the installation.

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

10. Click **Install**. The **Progress** or **Results** page is displayed.

11. Click **Done**.

Uninstalling Solutions

You can uninstall solutions from one or more devices.

1. In the left navigation pane, click on **Solutions**. From the **Common Tasks** task module, click **Uninstall solution**. The **Uninstall Solutions** wizard is started with the **Select devices** page displayed.

2. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers.

3. Click **Next**. The **Select solutions** page is displayed with the list of solutions that may be uninstalled.

4. Select at least one solution to uninstall from the selected devices and click **Next**. The **Confirm** page is displayed with the list of solutions that have been selected to be uninstalled from which devices.
5. Click **Uninstall**. The **Progress** or **Results** page is displayed.

Solutions Templates

Solution templates allow a number of selected solutions to be installed on a group of devices or a single device, allowing any number of solutions to be installed with a single command. You can:

- **Create solutions template**: Create a solutions template (Creating a Solutions Template on page 266).
- **Edit solution template**: Make changes to an existing solutions template (Editing a Solutions Template on page 267).
- **Remove solutions template**: Delete a solutions template (Deleting a Solutions Template on page 267).
- **Copy solutions template**: Copy a solutions configuration template and rename the new template and make changes to it (Copying a Solutions Template on page 267).
- **Apply solutions template**: Install solutions within a template to a single device, multiple devices, or a group (Applying a Solutions Template on page 268).

Specific Solution Templates Overviews

Each solution template has a specific page that shows the template name, the solutions, and the settings for each solution. From these pages, you can:

- **Apply solutions template**: Install solutions within a template to a single device, multiple devices, or a group (Applying a Solutions Template on page 268).
- **Edit solution template**: Make changes to an existing solutions template (Editing a Solutions Template on page 267).
- **Delete solutions template**: Delete a solutions template (Deleting a Solutions Template on page 267).
- **Copy solutions template**: Copy a solutions configuration template and rename the new template and make changes to it (Copying a Solutions Template on page 267).

Creating a Solutions Template

You can create a new solutions template.

1. In the left navigation pane, click **Solutions** and then click **Templates**. On the **Solutions Template Overview** page, click **Create**. The **Create Solution Template** wizard is started with the **Select solutions** page displayed.
2. Select the solutions to include with the template. To install solution managers, click **Install managers if needed**.
3. Click **Next**. The **Edit settings** page is displayed.
4. The solutions that have been selected to be installed are displayed. To change configuration settings, click **Edit** and make changes as necessary.
5. Click **Next**. The **Specify template name** page is displayed.
6. Type the name and click **Next**. The **Confirm** page is displayed.

7. Review the template and click **Create template**. The **Results** page is displayed.
8. Click **Done**.

Deleting a Solutions Template

Delete any solutions templates that are not being used.

1. In the left navigation pane, expand **Solutions**, and then click **Templates**.
2. On the **Templates** page, select the template to delete, and then click **Delete**. The **Delete Solution Templates** wizard starts.
3. On the **Confirm** page, review the selection, and then click **Delete Templates**. The **Results** page displays.
4. Click **Done**.

Editing a Solutions Template

You can make changes to a solutions template.

1. In the left navigation pane, click **Solutions** and then click **Templates**. On the **Solutions Template Overview** page, click **Edit**. The **Edit Solution Template** wizard is started with the **Select solutions** page displayed.
2. Select the solution to edit and click **Next**. The **Edit settings** page is displayed.
3. To modify the template, click **Edit** and make the necessary changes.
4. Click **Next**. The **Specify template name** page is displayed.
5. You can change the name of the template if desired and the click **Next**. The **Confirm** page is displayed.

NOTE: If you change the name of the template, the original template will now have this new name. If you want to copy an existing template and maintain the original template and its name, you must use the **Copy** option on the **Solutions Template Overview** page (Copying a Solutions Template on page 267.

6. Review the selection and click **Edit Template**. The **Results** page is displayed.
7. Click **Done**.

Copying a Solutions Template

You can copy solutions templates to create a new template. The copied template is added to the list of existing templates and the original template is unchanged.

1. In the left navigation pane, click **Solutions** and then click **Templates**. On the **Solutions Template Overview** page, click **Copy**. The **Copy Solution Template** wizard is started with the **Template Specification** page displayed.
2. Select the template to copy and specify the name for the new template. The original template's name will not be changed.
3. Click **Next**. The **Confirm** page is displayed.
4. Review the selection and click **Copy Template**. The **Results** page is displayed.
5. Click **Done**. The new template will now be listed under **Templates** left navigation pane.

Applying a Solutions Template

You can install solutions within a template to a single device, multiple devices, or a group.

1. In the left navigation pane, click **Solutions** and then click **Templates**. On the **Solutions Template Overview** page, click **Apply**. The **Apply Solution Template** wizard is started with the **Select devices** page displayed.

2. Select the solution options to apply. If you want to apply the solutions later, click **Schedule**. Then click **Next**. The **Select devices** page is displayed.

3. Select the device by highlighting it and clicking the arrow buttons between the two lists. To select multiple devices, use either Ctrl+Click or Shift+Click. To move all devices from one list to the other, use the double arrow buttons. You can sort the list of available devices by clicking the column headers, or view more columns by right-clicking the column headers. Then click **Next**.

   If you are applying the template now, the **Results** page is displayed.

   If you chose to schedule this for later, the **Specify schedule options** page is displayed with the list of solutions that may be installed. Specify when you want the solutions to be applied.

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

5. Review the selections and click **Apply Template**. The **Results** page is displayed.

6. Click **Done**.

4 Print Management

The **Print Management** view gives you control over remote print queues and drivers. These features can be used to create, edit, and delete existing queues as well as to install or update printer drivers. HP Web Jetadmin can act as a driver repository for deploying new HP drivers onto remote systems. And, HP Web Jetadmin **Print Management** features use HP's Universal Print Drivers (UPDs).

For example, you can use HP Web Jetadmin **Print Management** to locate a workstation or server on the network. Once this host is found, you can add administrative credentials and begin to manage the print queue and drivers on the remote host. Existing queues on the host can have a number of settings and/or the driver changed. Queues can be added or removed. You must have local administrator rights on these remote systems when performing this management activity.

File and printer sharing must be enabled at the remote host where the print queue is to be created.

Fleet Management of Print Queues

Within the **Print Management** view, HP Web Jetadmin has the capability of installing queues and drivers onto multiple remote hosts. This fleet queue creation can be done remotely from the HP Web Jetadmin client interface and in a configuration session.

Users of the **Print Management** feature could be IT personnel in school districts. These personnel may have responsibility over desktop print functionality and print devices in remote and wide geographic distribution. On top of the remote distribution problem, large numbers of workstations and different restrictions apply. Consider this problem:

- Each school in the district has obtained a color MFP.
- A dozen to several hundred student workstations could exist in each school.
- Staff are allowed to print color but students are not.
- IT has full administrative access to all of the workstations.

HP Web Jetadmin could be used in attaining substantial savings in an environment like this one. Pre-configuration could be used on drivers deployed to student workstations. All drivers and queues could be deployed through the **Create Print Queue** tool (Create Print Queue on page 271) and in very few configuration sessions. Travel to each of the schools could then be reduced to a bare minimum.

Driver Management

HP Web Jetadmin facilitates driver management. Drivers can be added to the HP Web Jetadmin host which acts like a driver repository. These drivers are installed on remote hosts where queue management is being performed. Some of these features can be locked.

Driver management in HP Web Jetadmin includes the following:

- **Pre-configure driver** (Pre-configure Driver on page 274).
- **Upload driver to available drivers** (Upload Drivers to HP Web Jetadmin on page 274).

- **Delete driver from available drivers** (Delete a Driver on page 275).
- **Retrieve driver from available drivers** (Retrieve a Driver on page 275).

Supported drivers include:

- HP device specific drivers
- .INF install

HP’s Universal Print Driver

The HP Universal Print Driver Postscript (UPD-PS) is bundled with HP Web Jetadmin software and can be installed from any create or edit queue interface (Create Print Queue on page 271 or Edit Print Queue on page 273). Universal Print Drivers PCL5 and PCL6 can be added to HP Web Jetadmin through a .INF installation

The HP Universal Print Driver has pre-configure capability which enables you to specify print defaults such as duplex or grayscale. Some of these defaults can be locked so that users must always use certain features such as duplex.

When HP Web Jetadmin creates a queue using the HP Universal Print Driver, the driver and printer (specified in HP Web Jetadmin) are installed in traditional mode, which means that the printer and driver have none of the special HP Universal Print Driver features that are available when this driver is installed from install.exe when downloaded from www.hp.com.

Print Management and Credentials

HP Web Jetadmin requests and utilizes Windows user credentials during print management operations. These credentials are needed for viewing, adding or removing print queues, or for modifying print queue driver or queue settings on remote systems. The credentials used during print management must provide local administrator access on the Windows system being managed by HP Web Jetadmin. These credentials are stored securely by HP Web Jetadmin and are re-used when the same Windows user requests further print management operations. These credentials are not reused for other Windows users requesting print management operations; credentials for different Windows users are stored separately and securely for each user requesting print management operations. These credentials can be cleared from the HP Web Jetadmin credential-store by using the **Clear all stored credentials** feature within **Tools** > **Options** > **Shared** > **Credentials** > **General**.

⚠ CAUTION: **Clear all Credentials** removes all stored credentials including all device credentials. Use caution when performing this operation.

Print Management - Common Tasks Task Module

The **Print Management - Common Tasks** task module provides links that initiate the following tasks for print queues and print drivers:

- Create a print queue
- Edit a print queue
- Delete a print queue

- Preconfigure the settings for a print driver
- Upload a print driver to HP Web Jetadmin
- Delete a print driver from HP Web Jetadmin
- Copy a print driver to any destination

Print Management - Print Queues Task Module

The **Print Management - Print Queues** task module provides a list of the print queues that have been created. Use this task module to perform the following tasks:

- Find a remote host on the network and specify the user credentials that provide administrative access to that host
- Create a print queue
- Delete a print queue
- Edit the settings for a print queue
- Send a test page to a print queue

Print Management - Available Drivers Task Module

The **Print Management - Available Drivers** task module provides a list of the print drivers that have been uploaded to HP Web Jetadmin. Use this task module to perform the following tasks:

- Upload a print driver to HP Web Jetadmin
- Delete a print driver from HP Web Jetadmin
- Preconfigure the settings for a print driver
- Copy a print driver to any destination

Print Management - Active Tasks Task Module

The **Print Management - Active Tasks** task module provides a list of the print management tasks that are running. Use this task module to stop or display the status of an active task.

Print Management Options

There are no configuration options for **Print Management** at this time.

Create Print Queue

Local administrator credentials are required on hosts managed by HP Web Jetadmin **Print Management** features. You can have these rights in a number of ways.

- You are a domain administrator.
- Your user domain account exists in the local Administrator group on the remote host.
- You belong to a domain group that exists in the local Administrator group on the remote host.

File and printer sharing must be enabled at the remote host where the print queue is to be created.

It is possible to create queues on many remote hosts in one working session (Fleet Management of Print Queues on page 269).

Use the following steps to create a print queue:

NOTE: When creating print queues on Windows Server 2003, you may be prompted for credentials repeatedly if there are no shared printers already on that host. In this case, you may have to add a shared printer locally. See Microsoft documentation about enabling the RPC endpoint for the print spooler.

NOTE: Print Management features allow the use of HP drivers regardless of the specific printer model selected. In many cases, a printer may only be supported with host-based print drivers or other types of print drivers. In the case where a driver is used in creating a print queue for a device that does not support that driver type, printing may or may not succeed when using that print queue. Always be sure that a supported driver is being used and matches the device for which the print queue is being created.

1. In the left navigation pane, click **Print Management** at the bottom of the screen.

   In the **Print Management - Print Queues** task module, click **New**. The **Create Queue** wizard is started with the **Select device** page displayed.

2. Select a device from the list (only one device can be selected). Click **Next**. The **Select server** page is displayed.

3. Select a computer name and a domain. Select **Add** (more than one computer name can be selected). Click **Next**. The **Select driver** page is displayed.

4. The **Credentials** wizard is started if there is only one server selected, if the **Show drivers on server in Available Drivers** is checked, and if you have not entered credentials for that server already. Select the print server and then type your credentials and password. Click **Set** and then click **Finish**. The **Select driver** page is displayed.

5. Select the driver:

   NOTE: The drivers on the print server are displayed in the **Available Drivers** list if **Show drivers on server in Available Drivers** is selected on the **Select server** page. Plus, if this feature is selected, all drivers are listed, some of which are not supported.

   NOTE: If creating a print queue on multiple servers, only the drivers on the HP Web Jetadmin server and the UPD drivers are available.

   - **Universal Print Driver PS**: The Universal Print Driver PostScript is available (HP's Universal Print Driver on page 270); other Universal Print Drivers can be obtained and installed through an .INF installation.
   - **Known Drivers**: Drivers that are already installed on the remote host or drivers that exist on the HP Web Jetadmin server (INF driver install base). These drivers, when identified for use with the print queue, are added to the queue as it is being installed (Create Print Queue on page 271).

   To display all drivers (not just the ones that are specific to the selected device), click **Show all drivers**.

Click **Next**. The **Specify print queue options** page is displayed.

6. Type the printer name using Windows naming conventions for print queues. This name must be a unique name on the server.

7. Type the port name. This defaults to the printer's IP Address preceded by **IP**; it is recommended to leave this as the default but you can change it if desired.

8. If you want to share this printer click **Share this printer**.

9. The share name defaults to the printer name but you can change it if desired.

10. You can add a location and any comments. Then click **Next**. The **Confirm** page is displayed.

11. Click **Next**. The **Results** page is displayed.

    If the printer was shared, you can print a test page.

12. Click **Done**. The **Print Management** page is displayed.

Edit Print Queue

Any existing print queue can be edited to change the driver associated with it, whether or not it is shared.

Use the following steps to edit a print queue:

NOTE: Print Management features allow the use of HP drivers regardless of the specific printer model selected. In many cases, a printer may only be supported with host-based print drivers or other types of print drivers. In the case where a driver is used in creating a print queue for a device that does not support that driver type, printing may or may not succeed when using that print queue. Always be sure that a supported driver is being used and matches the device for which the print queue is being created.

1. In the left navigation pane, click **Print Management** at the bottom of the screen.

   In the **Print Management - Print Queues** task module, select the print queue and click **Edit**. The **Edit Print Queue** wizard is started with the **Select driver** page displayed.

2. Select the driver:

   - **Universal Print Driver PS**: The Universal Print Driver PostScript is available (HP's Universal Print Driver on page 270); other Universal Print Drivers can be obtained and installed through an .INF installation.

   - **Known Drivers**: Drivers that are already installed on the remote host or drivers that exist on the HP Web Jetadmin server (INF driver install base). These drivers, when identified for use with the print queue, are added to the queue as it is being installed (Create Print Queue on page 271).

   To display all drivers (not just the ones that are specific to the selected device), click **Show all drivers**.

   Click **Next**. The **Specify print queue options** page is displayed.

3. If you want to share this printer click **Share this printer**.

4. Click **Next**. The **Results** page is displayed.

5. Click **Done**. The **Print Management** page is displayed.

Delete Print Queue

Use the following steps to delete a print queue:

1. In the left navigation pane, click **Print Management** at the bottom of the screen.

   In the **Print Management - Print Queues** task module, click **Delete**. The **Delete Print Queue** wizard is started.

2. Select the print queue to delete.
3. Click **Next**. The **Confirm** page is displayed.
4. Click **Next**. The **Results** page is displayed. Click **Done** to display the **Print Management** page.

Pre-configure Driver

After drivers are listed in **Available Drivers**, they can be pre-configured to contain settings such as duplex-on or grayscale. Many HP drivers can be pre-configured. Typically, PCL5 and PCL6 HP drivers for newer HP devices can be pre-configured in a variety of ways. Some settings can be locked.

Setting	Lockable or Not Lockable
Duplex/Simplex	Lockable
Orientation: Portrait/Landscape	Not Lockable
Print in grayscale	Lockable
Print quality	Not Lockable

After a pre-configuration has been added for a driver to HP Web Jetadmin, whenever that driver is selected you will be asked to select the default or the pre-configured driver.

Use the following steps to preconfigure a driver:

NOTE: Users who are not members of the local administrators group on the HP Web Jetadmin server host are not able to create driver pre-configuration settings. The **Printing Preferences** tab and the **Device Settings** tab are not displayed for those users not in the local administrators group.

1. In the left navigation pane, click **Print Management** at the bottom of the screen.

   In the **Print Management - Common Tasks** task module, click **Pre-configure driver**. The **Driver Pre-configuration** wizard is started with the **Select driver** page displayed.

2. Select the driver and click **Next**. The **Specify Configuration Options** page is displayed.
3. Configure the driver settings and name the pre-configuration for the driver; notice that some might be locked in which cases you cannot adjust them. Click **Next**. The **Confirm** page is displayed.
4. Click **Save Configuration**. The **Results** page is displayed.
5. Click **Done**. The **Print Management** page is displayed.

   The new pre-configuration and the default configuration now exist and can either be exported to an INF driver install file set or used in managing print queues.

Upload Drivers to HP Web Jetadmin

INF install file sets for drivers can be uploaded into the HP Web Jetadmin host. These drivers can then be installed onto remote hosts (Edit Print Queue on page 273 or Create Print Queue on page 271).

All of the files in the directory with the INF file and all files in subdirectories of that directory are copied to the HP Web Jetadmin server as part of the upload process. Extra files not related to that driver should not be in that directory or its subdirectories.

Use the following steps to upload a driver:

1. In the left navigation pane, click **Print Management** at the bottom of the screen.

   In the **Print Management - Available Drivers** task module, click **Upload**. The **Upload Driver** wizard is started with the **Select INF File** page displayed.

2. Select an INF file and click **Next**. The **Confirm** page is displayed.
3. Click **Start**. The selected driver is copied to the destination specified in the preceding step.
4. Click **Done**. The **Print Management** page is displayed.

Delete a Driver

Drivers can be removed from HP Web Jetadmin if there is a more current version available or if they are no longer needed.

Use the following steps to delete a driver:

1. In the left navigation pane, click **Print Management** at the bottom of the screen.

   In the **Print Management - Available Drivers** task module, click **Delete**. The **Delete Driver** wizard is started with the **Confirm** page displayed.

2. Click **Next**. The **Results** page is displayed. Click **Done** to display the **Print Management** page.

Retrieve a Driver

Use the following steps to copy a driver to any destination:

1. In the left navigation pane, click **Print Management** at the bottom of the screen.

   In the **Print Management - Available Drivers** task module, click **Retrieve**. The **Get Driver** wizard is started with the **Select driver** page displayed.

2. Select the driver:

   - **Universal Print Driver PS**: The Universal Print Driver PostScript is available (HP’s Universal Print Driver on page 270); other Universal Print Drivers can be obtained and installed through an .INF installation.
   - **Known Drivers**: Drivers that are already installed on the remote host or drivers that exist on the HP Web Jetadmin server (INF driver install base). These drivers, when identified for use with the print queue, are added to the queue as it is being installed (Create Print Queue on page 271).

   To display all drivers (not just the ones that are specific to the selected device), click **Show all drivers**.

   Click **Next**.

3. Select the driver and the pre-configuration for the driver and click **Next**. The **Specify destination settings** page is displayed.
4. Select a folder for the driver and click **Next**. The **Confirm** page is displayed.
5. Click **Start**. The selected driver is copied to the destination specified in the preceding step.
6. Click **Done**. The **Print Management** page is displayed.

5 Application Management

You can use the features in the Application Management view to configure and manage devices on the network. The task modules on the **Overview** page provide access to these features.

The following are some important things to note about HP Web Jetadmin:

- **Low-privilege service account**: HP Web Jetadmin runs under the Network Service account, which is a low-privilege account on the local system. Many environments require that applications such as HP Web Jetadmin do not have administrative access to the operating system.
- **Database access and authentication**: HP Web Jetadmin uses Windows credentials to access the database instance that was created in Microsoft SQL Server Express Edition when the software was installed.
- **File permissions and NTFS**: HP Web Jetadmin uses Windows credentials to access the database instance that was created in SQL Server Express Edition when the software was installed.

Network Ports

HP Web Jetadmin opens a number of ports for various reasons. See the Installation and Setup Guide for detailed information about Ports on page 11.

Application Management Options

Configuration options can be set for many functional area within the **Application Management** view. For more information, see Application Management Configuration Options on page 58.

Application Management – Common Tasks Task Module

The **Application Management – Common Tasks** task module provides links that initiate the following tasks for managing HP Web Jetadmin:

- Create a role
- Assign a role to users
- Find remote installations of HP Web Jetadmin

Application Management – Active Tasks Task Module

The **Application Management – Active Tasks** task module provides a list of the application management tasks that are running. Use this task module to stop or view the status of an active task.

Application Management - Scheduled Tasks Task Module

The **Application Management - Scheduled Tasks** task module provides a list of the application management tasks that are scheduled to run. Use this task module to delete or edit the settings for an active task.

HP Web Jetadmin - All Active Tasks Task Module

The **HP Web Jetadmin - All Active Tasks** task module provides a list of the HP Web Jetadmin tasks that are running. Use this task module to stop or display the status of an active task.

HP Web Jetadmin - All Scheduled Tasks Task Module

The **HP Web Jetadmin - All Scheduled Tasks** task module provides a list of the HP Web Jetadmin tasks that are scheduled to run. Use this task module to delete or edit an HP Web Jetadmin task.

Client Management - Active Clients Task Module

The **Client Management - Active Clients** task module provides a list of the clients that are connected to the HP Web Jetadmin server.

User Security

A role is a set of permissions for HP Web Jetadmin features. HP Web Jetadmin administrators can assign local or domain users to user roles. After a user is assigned to a role, that user can access the features specified for that role.

The following are the security features in HP Web Jetadmin:

- Advanced security technologies on the Microsoft .NET Framework platform provide authentication and encryption of client/server communications.
- Windows Active Directory integrated role-based user authentication secures the application against unauthorized usage.
- Optional SSL (Secure Sockets Layer) communication between client browser and application server ensure data security for application file download.
- Optional Simple Network Management Protocol v3 (SNMPv3) used on devices provides authentication and encryption.
- IPsec plug-in; using HP Web Jetadmin, you can configure an IPsec policy and then apply it to one or more selected HP Jetdirect devices.
- Running under a low-privilege service account reducing risk of privilege escalation attacks.
- Secure online update features allow a safe easy way to get online patches updates and new features.

You can manage access to HP Web Jetadmin in **User Security**. You can control who has access and what they have access to. In **User Security**, you can manage:

- **Role templates**: Two exist to allow you to create one set of access levels and then apply that template when adding users. You can create, view, edit, and delete role templates.
- **Users**: Allows you to assign users to a role template. You can create, view, edit, and delete users.

Initial User Security

HP Web Jetadmin is a multi-user application that can be accessed from remote client-workstations. Users and user-permissions can be administered to control access to the application and specific features within the application. An example of this would be a helpdesk scenario where many users may not require or should not have access to features like, discovery, user permissions or, global application settings.

HP Web Jetadmin uses Windows domain identities to authenticate users and grant access to the application or to specified features. HP Web Jetadmin provides single-sign-on which means the user is authenticated by virtue of being logged into their client host. They do not have to provide their credentials again when logging into HP Web Jetadmin.

The HP Web Jetadmin Administrator Role

The HP Web Jetadmin administrator has full rights to all application settings and features. The person installing HP Web Jetadmin software must have local administrative privileges on the install-host and therefore will have initial administrative access to the software. Any identity that is a member of the local administrators group on the local host also has administrative access to the software. The identity must have local administrative privileges on the install-host and therefore will have initial administrative access to the software.

Alternate Log-in Method for User Security

HP Web Jetadmin uses the single sign-on functionality to pass the identity of the user who is currently logged into Windows on the client to the server where HP Web Jetadmin is installed. HP Web Jetadmin authenticates this identity through the local Windows users on the server or through the Windows domain identities. In some cases, the client and server might not reside on the same Windows security domain or on any Windows security domain. If HP Web Jetadmin fails to authenticate this identity for any reason, it displays an alternate log-in prompt. Users can then enter log-in credentials other than the credentials for the current Windows session on the client.

The alternate log-in prompt is useful in a variety of situations, such as the following:

- An authorized HP Web Jetadmin user needs to access HP Web Jetadmin from the desktop of an unauthorized user.
- The HP Web Jetadmin server is on a security domain. The user has a log-in identity on the security domain that has been given access rights in HP Web Jetadmin through the Users and Roles features. However, the user's desktop is not on the security domain.

User Security - Common Tasks Task Module

The **User Security - Common Tasks** task module provides links that initiate the following tasks for roles and users:

- Create a role
- Assign a role to users
- Copy a role template to create a new template

User Security - Roles Task Module

The **User Security - Roles** task module provides a list of the roles that have been created. Use this task module to perform the following tasks:

- Create a role
- Edit a role
- Delete a role
- View the settings for a role
- Copy a role to create a new role

User Security - Users Task Module

The **User Security - Users** task module provides a list of the users and the roles that are assigned to the users. Use this task module to perform the following tasks:

- Assign a role to users
- Edit the settings for a user
- Delete a user
- Display the **User Security - Diagnostics** pane for a user
- Refresh the list of users

Roles

A role is a set of permissions for specific HP Web Jetadmin features. A permission set can apply to all of the features in HP Web Jetadmin or be restricted to only the device management features for a device group. For more information about restricting permission sets to device groups, see Restrict Roles to Device Groups on page 281.

After you assign a role to a user, the user can access only the HP Web Jetadmin features that are enabled for that role. You can create multiple roles to allow different levels of access to HP Web Jetadmin features for different users. You can assign multiple roles to one user.

The permission sets for roles are cumulative. If you assign one role to a user, you can grant additional permissions to that user by assigning another role that has a different permission set. Users never lose permissions when multiple roles are assigned to them. For example, assume that Role A enables permission to update the device firmware and Role B disables permission to update the device firmware. If you assign Role A to a user, the user can update the device firmware. If you then assign Role B to the user, the user retains permission to update the device firmware.

You can use the Diagnostics feature to view the roles that are assigned to a user and the features that are enabled or disabled for each of those roles. For more information about the Diagnostics feature, see User Security Diagnostics on page 286.

Restrict Roles to Device Groups

When you create a role, you can restrict the role to device groups and limit the permission set to specific device management features, such as configuring devices, running discoveries, and updating the device firmware. To limit the permission set to device groups from the **Create Role** wizard, you must select the **Device Groups** option from the **Restriction type** list on the **Specify permission settings** page. Then you can enable or disable each device management feature. For instructions on creating roles, see Create Roles on page 281.

After you create a role that is limited to the device management features, you can assign the role to a user. During the process of assigning the role to a user, you must specify the device groups to which the role is restricted. The user can access the device management features that are enabled for the role only on the devices that are members of the specified device groups. The user cannot access the device management features on devices that are not members of the specified device groups. For instructions on assigning roles, see Assign Roles to Users on page 284.

Create Roles

If you have permission to manage users, you can create roles by using the **Create Role** wizard.

To create roles, perform the following steps:

1. In the **Application Management** navigation pane, right-click **Roles**, and then select **Create**. The **Create Role** wizard starts.

   NOTE: You can assign more than one role to a user. The permission sets for roles are cumulative. If you assign one role to a user, you can grant additional permissions to that user by assigning another role that has a different permission set. Users never lose permissions when multiple roles are assigned to them. For example, assume that Role A enables permission to update the device firmware and Role B disables permission to update the device firmware. If you assign Role A to a user, the user can update the device firmware. If you then assign Role B to the user, the user retains permission to update the device firmware.

2. On the **Specify permission settings** page, select one of the following options from the **Restriction type** list:

   - **None**: The permission set for this role applies to all areas of HP Web Jetadmin.
   - **Device Groups**: The permission set for this role is limited to the device management features.

     NOTE: If the **Device Groups** option is selected, you must also specify the device groups to which the role is restricted when you assign the role to a user. For instructions on assigning roles, see Assign Roles to Users on page 284.

3. Select the checkbox next to each permission that you want to enable for the role, and then click the **Next** button.

   NOTE: You must enable at least one permission.

4. On the **Specify role name** page, enter a name for the role in the **Role name** box, and then click the **Next** button.

   NOTE: Each role must have a unique name.

5. On the **Confirm** page, verify that the information is correct, and then click the **Create Role** button.

6. To start the **Assign User Role** wizard, select the **Assign to users now** checkbox. For more information about the **Assign User Role** wizard, see Assign Roles to Users on page 284.

7. On the **Results** page, click the **Done** button.

Edit Roles

You can change the permissions that are enabled for a role, but you cannot change the restriction type that is defined for that role. You cannot edit the Administrator role.

NOTE: If a user is logged in to HP Web Jetadmin when you change the permissions for the role to which that user is assigned, the changed permissions do not take effect until that user logs out and then logs back in. However, if the user continues working after you change the permissions and tries to access a feature that is no longer allowed, HP Web Jetadmin displays a message that the user no longer has permission to perform that action.

Roles can be edited by multiple clients simultaneously. The last saved user settings are the ones that will be stored for that role template.

To edit roles, perform the following steps:

1. In the **Application Management** navigation pane, expand the **Roles** option, right-click the role, and then select **Edit**. The **Edit Role** wizard starts.

2. To enable a permission, select the checkbox next to the permission.

   -or-

   To disable a permission, clear the checkbox next to the permission.

3. Click the **Next** button.

4. On the **Specify role name** page, enter a new name for the role in the **Role name** box, and then click the **Next** button.

   NOTE: Each role must have a unique name.

5. On the **Confirm** page, verify that the information is correct, and then click the **Save Role** button.

6. On the **Results** page, click the **Done** button.

Delete Roles

You can delete any role except the Administrator role.

NOTE: If a user is logged in to HP Web Jetadmin when you delete the role to which that user is assigned, the client for that user is shut down and a message displays stating that the user no longer has permission.

To delete roles, perform the following steps:

1. In the **Application Management** navigation pane, expand the **Roles** option, right-click the role, and then select **Delete**. The **Delete Role** wizard starts.

2. On the **Confirm** page, verify that the information is correct, and then click the **Delete Role** button.

3. On the **Results** page, click the **Done** button.

View Roles

1. In the left navigation pane, click on **User Security**.

   In the **User Security - Roles** task module, select the role to change and click **View**. The role is displayed showing the type of restriction and any permissions set.

2. From this page, you can:

   - Edit Roles on page 282 (if it is not the Administrator role).
   - Delete Roles on page 282 (if it is not the Administrator role).
   - **Add User** (Assign Roles to Users on page 284).
   - **Remove User** (Remove Roles on page 286).

Role Templates

Two role templates come with HP Web Jetadmin:

- **Default Device Admin Role**: has limited device management permissions and no application management permissions. You can open this template, rename it, and then change permissions as necessary.
- **HP Web Jetadmin Administrator Role**: a read-only role. Users assigned to this role have full rights to HP Web Jetadmin. Both users and user-groups can be added to this role. User groups that are added can be either local or domain groups.

For information about assigning a role template or a role to users, see Assign Roles to Users on page 284.

NOTE: Even though you can create, edit, and view role templates, you cannot edit or delete the **HP Web Jetadmin Administrator (Read-Only)** role template.

Copy a Role Template

Role templates can be created and managed to save you time and provide consistency. Templates contain configuration preferences (that vary by template type) and can be applied to users or user groups. For more information, see Copy Template Wizard on page 99.

NOTE: Templates are also available in the **Device Management** view for **Configuration**, **Alerts**, **Discovery**, **Data Collection**, and **Report Generation**.

Users

If you have permission to manage users in HP Web Jetadmin you can add users to a role. A user can be added to a role with all of its permissions, or that user can be added to a role with only a subset of its permissions.

Managing Users within User Groups

Either domain or local user groups can be assigned to an HP Web Jetadmin **Role**. Once the assignment is made, the users contained within the user group have privileges that are defined within by the role. Here are some examples of user groups and Role assignment.

- **Example 1**: a domain user group contains users who belong to the Support team. The company adds and removes users as needed when staff changes occur. The Support team's user-group is associated with an HP Web Jetadmin Role named HELPDESK.

  Domain User Group-Support:

  AMERICAS\ralphj

  EMEA\rjiminez

  ASIAPACIFIC\chansen

  The following are the assignments.

User	Role
AMERICA\Support	HELPDESK

- **Example 2**: a local group on the system that hosts HP Web Jetadmin includes a group named WJAUsers. This group is managed by the HP Web Jetadmin administrator who's name is Chester. Chester keeps a few people in the group who help him administer the application. The group is associated with the built-in Role named HP Web Jetadmin Administrator (read only).

  Local User Group-WJAUsers:

  EMEA\Wendt

  EMEA\Pacj

  ASIAPACIFIC\Hae

  The following are the assignments.

User	Role
`WJA-SYSTEM\WJAUsers`	HP Web Jetadmin Administrator (read only)

Assign Roles to Users

You can assign roles to users to manage the HP Web Jetadmin features that the users can access. After you assign a role to a user, the user can access only the HP Web Jetadmin features that are enabled for that role. You can create multiple roles to allow different levels of access to HP Web Jetadmin features for different users. You can assign multiple roles to one user.

The permission sets for roles are cumulative. If you assign one role to a user, you can grant additional permissions to that user by assigning another role that has a different permission set. Users never lose permissions when multiple roles are assigned to them. For example, assume that Role A enables permission to update the device firmware and Role B disables permission to update the device firmware. If you assign Role A to a user, the user can update the device firmware. If you then assign Role B to the user, the user retains permission to update the device firmware.

To assign roles to users, perform the following steps:

1. In the **Application Management** navigation pane, right-click **User Security**, and then select **Assign roles to users**. The **Assign User Role** wizard starts.
2. On the **Select users or user groups** page, click the **Add** button.

3. On the **Add User** page, enter the user name and domain where the user is defined.

   -or-

   To search for the user, perform the following steps:

   a. Click the **Browse** button.

   b. To change the location, click the **Locations** button. In the **Locations** window, select the HP Web Jetadmin or Windows domain, and then click the **OK** button.

   c. Enter the user name. To display examples of the format for entering user names, hold the cursor over the **Enter the object name to select (examples)** link.

   d. To validate the user name, click the **Check Names** button.

   e. If the user name is not valid, the wizard displays an error message. Click the **OK** button, and then repeat steps b through d.

   f. Click the **OK** button.

4. Click the **Add** button.

5. To add additional users, repeat steps 3 and 4.

6. Click the **Close** button.

7. On the **Select users or user groups** page, verify that the information is correct, and then click the **Next** button.

8. To create a role from the **Specify role settings** page, click the **New** button. The **Create Role** wizard starts. For instructions on using the **Create Role** wizard, see Create Roles on page 281.

9. Select the role from the **Role** list.

10. If the selected role cannot be restricted to device groups, the **Add** button is not available. Continue with step 11.

    -or-

    If the selected role can be restricted to device groups, the **Add** button is available. Perform the following steps:

    a. Click the **Add** button.

    b. On the **Select Group** window, click the **...** button, and then select the device group.

    c. Click the **OK** button.

    d. To add additional device groups, repeat steps a through c.

11. Click the **Next** button.

12. On the **Confirm** page, verify that the information is correct, and then click the **Add** button.

13. On the **Results** page, click the **Done** button.

To assign multiple roles to a user, repeat this procedure for each role that you want to assign to the user.

Edit Users

You can change the user and role for an existing assignment.

Use the following steps to edit a user role:

1. Select **Application Management** from the bottom of the left navigation pane.

   Expand **User Security** and click on **Users**. The **User Security - Users** page is displayed.

2. Select the user or group and click **Edit**. The **Edit User Roles** wizard is started with the **Users** page displayed.

3. To change the user for the role check **Change User** and then type the User name and domain.

   If you click **Browse**, the **Select User** page is displayed. Type the **Object Type** and **Location** and click **Next**. If necessary, you can browse for locations.

4. The information will be validated. If the user is found, it will be listed in the **Selected Users** box at the bottom of this page. If the user is not found, verify the user name and domain and re-enter that information.

5. Review the users assigned to this role shown in **Selected Users**.

   If any should be removed, click **Remove**.

   If the users assigned to this role template are correct, click **Next**. The **User Security - Users** page is displayed again.

6. Select the role from the **Role** drop-down box.

7. If any groups have permissions associated with them, they are listed in the **Restrict Permissions by Group** box at the bottom of this page.

   If any of the sets of permissions should apply to this user, click **Add**. This means the user will only be allowed to perform actions on the group listed.

   If any of the sets of permissions listed should be removed so that the user has access to more groups, click **Remove**.

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

8. Review the selections. If they are correct, click **Next**. The **Results** page is displayed. Click **Done**.

Remove Roles

Use the following steps to remove a role:

1. Select **Application Management** from the bottom of the left navigation pane.

   Expand **User Security** and click on **Users**. The **User Security - Users** page is displayed.

2. Select the user or group and click **Remove Role**. The **Remove User Role** wizard is started with the **Confirm** page displayed.

3. If this is the correct user to delete, click **Next**. The **Results** page is displayed.

4. Click **Done**. The **User Security - Users** page is displayed.

User Security Diagnostics

User Security - Diagnostics provides analysis of permissions as they exist for an individual user or group. Any domain or local user or group can be chosen and then examined for existing permissions on HP Web Jetadmin.

Use the following steps to view the roles and permissions for a user or group:

1. Select **Application Management** from the bottom of the left navigation pane.

   Expand **User Security** and click on **Diagnostics**. The **User Security - Diagnostics** page is displayed.

2. Browse for or enter the user name and domain and then click **View Roles**.

3. If desired, select a restriction to filter the list displayed.

4. The role or roles and permissions for the user are displayed.

HP Web Jetadmin Management

HP Web Jetadmin provides the ability to discover most versions of other HP Web Jetadmin installations. HP Web Jetadmin can perform a unidirectional synchronization with another HP Web Jetadmin **All Devices List** (Device Lists on page 105). This makes it easy to discover devices that have already been discovered by other installations of HP Web Jetadmin. Both of these features, synchronization and application discovery are valuable for a variety of reasons:

- An administrator detects others using HP Web Jetadmin software to attain understanding of printer management on the network.
- An administrator detects other HP Web Jetadmin installations as a matter of security or management policy.
- An administrator is responsible for finding all devices in a distributed environment where others are responsible for managing them in multiple areas.

HP Web Jetadmin - Common Tasks Task Module

The **HP Web Jetadmin - Common Tasks** task module provides links that initiate the following tasks for HP Web Jetadmin:

- Find remote installations of HP Web Jetadmin
- Display a list of the remote HP Web Jetadmin installations that have been found

HP Web Jetadmin - Management Task Module

The **HP Web Jetadmin - Management** task module provides a list of the remote HP Web Jetadmin installations that have been found. Use this task module to perform the following tasks:

- Discover remote installations of HP Web Jetadmin
- Launch a remote installation of HP Web Jetadmin
- Quickly discover a remote installation of HP Web Jetadmin by using the IP address or hostname of the remote HP Web Jetadmin server

HP Web Jetadmin - Summary Task Module

The **HP Web Jetadmin - Summary** task module provides the number of remote installations of each version of HP Web Jetadmin that were found on the network.

Remote Installations of HP Web Jetadmin on the Network

Sometimes it is advantageous to find other HP Web Jetadmin application installations on the network. HP Web Jetadmin provides the ability to discover most revisions of the HP Web Jetadmin software and then synchronize with those other installations.

Using synchronization and application discovery enables you to:

- Detect others using HP Web Jetadmin software to attain understanding of printer management on the network.
- Detect other HP Web Jetadmin installations as a matter of security or management policy.
- Schedule the discovery of other HP Web Jetadmin installations.
- Find all devices in a distributed environment (others might manage them in multiple areas).

Discover Remote Installations of HP Web Jetadmin

HP Web Jetadmin instances can be listed for discovery, user viewing, removing, and even launching.

HP Web Jetadmin instances can be found on both local and remote networks. The settings for IP Range and IP Broadcast are identical to HP Web Jetadmin Discovery settings. In fact, these settings are shared between the two features.

- HP Web Jetadmin can discover other instances of HP Web Jetadmin.
- IP Range and IP Broadcast discoveries share stored setting with other discovery features.
- HP Web Jetadmin instances can be launched directly from the discovery listing.
- The listing can be modified by performing further discoveries or by manually removing the instances.
- Address, URL, hostname, and version information are included in the listing.

You can schedule application discovery. If an application discovery is currently running and you try and start another application discovery, you will receive a dialog asking if you want to view the current discovery or schedule a new one.

Use the following steps to discover remote installations of HP Web Jetadmin on the network:

1. In the **Application Management** navigation pane, right-click **HP Web Jetadmin Management**, and then select **Find More Applications**. The **HP Web Jetadmin Discovery** wizard starts.
2. On the **Choose discovery options** page, select the discovery methods to use for the discovery. For more information about the discovery methods that can be used, see the following topics:
   - WS-Discovery on page 152
   - IP Broadcast Discovery on page 141
   - IP Range Discovery on page 142

3. To run the discovery immediately, leave the **Schedule discovery** checkbox cleared.

   -or-

   To schedule the discovery to run at a later time, select the **Schedule discovery** checkbox.

4. Click the **Next** button.

5. On the settings page, specify the settings for the discovery method, and then click the **Next** button.

   NOTE: If more than one discovery method is selected, the wizard displays a separate settings page for each discovery method.

6. If the **Specify schedule options** page appears, use the following steps:

   a. From the **Start time** lists, select the date and time that the discovery runs.

   b. In the **Recurrence** section, select the options that specify how often the discovery runs.

   c. In the **Name** box, enter a name for the discovery schedule.

   d. Click the **Next** button.

7. On the **Confirm** page, verify that the information is correct, and then click the **Start** button.

8. On the **Progress** page, click the **Done** button.

Launch Remote Installations of HP Web Jetadmin

Use the following steps to launch a remote installation of HP Web Jetadmin:

1. In the **Application Management** navigation pane, expand the **HP Web Jetadmin Management** option, and then select **HP Web Jetadmin Installations**.

2. On the **HP Web Jetadmin Installations** pane, select the remote installation from the list, and then click the **Launch** button.

Remove Remote Installations of HP Web Jetadmin

Use the following steps to remove remote installations of HP Web Jetadmin from the list of discovered installations:

1. In the **Applications Management** navigation pane, expand the **HP Web Jetadmin Management** option, and then select **HP Web Jetadmin Installations**. The **HP Web Jetadmin Installations** pane appears.

2. To remove one or more remote installations from the list, select the installations, and then click the **Remove** button.

   -or-

   To remove all of the remote installations from the list, click the **Remove All** button.

3. On the **Confirm** page of the **Remove Applications From List** wizard, verify that the information is correct, and then click the **Next** button.

4. On the **Results** page, click the **Done** button.

Data Synchronization

Data synchronization pulls information about the devices that have been discovered on a remote HP Web Jetadmin server, and then adds the devices to the local HP Web Jetadmin server and displays them in the **All Devices** list. Data synchronization occurs even if the local HP Web Jetadmin server has already discovered the devices that are on the remote HP Web Jetadmin server.

Data synchronization is not a two-way process. The devices on the local HP Web Jetadmin server are not pushed to the remote HP Web Jetadmin server. Therefore, the number of devices on the remote HP Web Jetadmin server typically does not match the number of devices on the local HP Web Jetadmin server.

The following is an example of data synchronization. Server A is the local server and has 50 discovered devices. Server B is the remote server and has 100 discovered devices. There are 10 devices on Server A that are not on Server B. There are 75 devices on Server B that are not on Server A. After data synchronization is initiated on Server A, Server A has 125 devices—the original 50 devices plus the 75 devices that are pulled from Server B. Server B still has only 100 devices because the 10 devices from Server A are not pushed to Server B.

A user on the local HP Web Jetadmin server initiates data synchronization. The local user must have domain user credentials that are associated with a role on the remote HP Web Jetadmin server or administrative rights on the remote HP Web Jetadmin server. The local user must be in one of the following groups:

- The user group on the local HP Web Jetadmin server. A data synchronization role on that server must also be assigned to the local user.
- The user group on the remote HP Web Jetadmin Smart Client.
- The admin group on the local HP Web Jetadmin server.

Synchronize data between HP Web Jetadmin servers

1. If there are no user-defined settings configured on the remote HP Web Jetadmin server, continue with step 2.

   -or-

   If there are user-defined settings configured on the remote HP Web Jetadmin server, the user-defined settings must exist on both the local and remote HP Web Jetadmin servers before the values of the user-defined settings on the remote HP Web Jetadmin server can be synchronized. The user-defined settings must be exported from the remote HP Web Jetadmin server, and then imported into the local HP Web Jetadmin server. For more information about exporting and importing user-defined settings, see Manage the User-defined Device Configuration Settings on page 66.

   ⚠ CAUTION: When a user-defined setting is created, HP Web Jetadmin generates a random number that is used as a unique identifier for that user-defined setting. Therefore, to maintain the same unique identifier for each user-defined setting, the user-defined settings must be exported from the remote HP Web Jetadmin server, and then imported into the local HP Web Jetadmin server.

2. Go to **Tools** > **Data Synchronization**. The **Data Synchronization** window opens.
3. If the list of remote HP Web Jetadmin servers is empty or the remote HP Web Jetadmin server is not in the list, use one of the following options to add remote HP Web Jetadmin servers to the list:
   - In the **WJA Quick Discovery** box, enter the IP address or hostname of the remote HP Web Jetadmin server, and then click the **Go** button.
   - Discover the remote HP Web Jetadmin servers. For more information about discovering HP Web Jetadmin servers, see Discover Remote Installations of HP Web Jetadmin on page 288.
4. Select the remote HP Web Jetadmin server from the list.

5. To synchronize the HP Web Jetadmin servers immediately, click the **Synchronize** button.

   -or-

   To schedule the synchronization for a later time, click the **Schedule** button. The **Synchronize Data** wizard starts. Use the following steps to schedule the synchronization:

   a. On the **Specify user** page, enter your password in the **Password** box, and then click the **Verify link** button.

   b. After the link is successfully verified, click the **Next** button.

   c. On the **Select device data** page, select the checkboxes next to the device data to include in the data synchronization, and then click the **Next** button.

   NOTE: The checkboxes for the device data that must be synchronized are already selected and cannot be cleared.

   d. On the **Specify schedule** page, select the date and time that the data synchronization runs.

   NOTE: A scheduled task uses the date and time on the server where HP Web Jetadmin is installed. The location where the scheduled task runs might not be in the same time zone as the location where the HP Web Jetadmin server is installed. Consider the potential for date and time differences when scheduling tasks.

   e. In the **Recurrence** section, select the option that specifies how often the data synchronization runs, and then specify any associated settings.

   f. Click the **Next** button.

   g. On the **Confirm** page, verify that the schedule information is correct, and then click the **Start Synchronization** button.

   h. On the **Progress** page, click the **Done** button.

6. On the **Data Synchronization** window, click the **OK** button.

Delete data synchronization schedules

1. Go to **Tools** > **Data Synchronization**. The **Data Synchronization** window opens.
2. Select the remote HP Web Jetadmin server, and then click the **Clear Schedule** button.
3. On the **Confirm Schedule Removal** window, click the **Yes** button.

Delete servers from the list of remote servers

1. Go to **Tools** > **Data Synchronization**. The **Data Synchronization** window opens.
2. Select the remote HP Web Jetadmin server, and then click the **Delete** button.
3. On the **Confirm Entry Removal** window, click the **Yes** button.

6 Device Configuration Options

Following are the various configuration options for devices. Your device might or might not support all of the options.

Device Configuration Options for Copier

Configuration options for Copiers define functions for the copiers including default copy settings.

Auto Include Margins

Use this option to specify whether content close to the edges on an original scanned document is automatically included on the copy.

To include the entire image on an original scanned document, including any content that is close to the edges, select the **On** option. If necessary, the device reduces the image slightly on the copy, depending on the size of the printable area on the paper.

To leave a margin of unscanned space on the copy, select the **Off** option. The device might not be able to fit the entire original image on the copy.

Color Copy Mode and Color Copy Mode With Auto

Use this option to set the device to the desired copy mode.

To set this option, select the desired setting from the drop-down box.

Color Copy Option

The **Color Copy Option** provides an effective way to limit color copying which can serve as a cost control option for you. To provide an option to disable color copies and limit the color copy costs.

Use the following steps to configure this option:

1. To allow color copies, select **Enable**.
2. To disable color copies, select **Disable**. The corresponding option will disappear from the Embedded Web Server. The disability to make color copies is applied after a timeout period.

Copier Fit To Page

This option enables the device with local copier capability to fit the input image size automatically onto the output sheet size. This object allows you to scale to the output size without knowing the scaling percentage.

Use the following steps to configure this option:

1. To set the Fit to page, select the Off or On radio button.
2. Click **Apply**.

Copier Reduce/Enlarge

This option enables you to specify reduction/enlargement for copies. The number is represented as a percentage of the original. A value of 100 will make copies with no reduction or enlargement; higher values will make enlargements, while lower values cause a reduction. It is often useful to be able to make reductions or enlargements if the paper size being copied to is different from the size of the source document. Some useful values for copying from one size to another would be:

- Legal to Letter (78%)
- Letter to A4 (97%)
- A4 to Letter (94%)
- Legal to A4 (83%)

To set this option, enter a number for the percentage of the reduction or enlargement.

Copy - Alternative Letterhead Mode

When printing using duplex mode, this option defines the first side of the page as having letterhead and the other side having no letterhead.

To configure this option, select **On** or **Off**.

Copy Background Cleanup

Use this option to set the default amount of background to be removed from the original document being scanned. For example, if a higher value is set then more of the background is removed from the original.

To configure this option, select a default value for the amount of background to remove from scanned images.

Copy Content Orientation

Use this option to specify the default orientation for the scan job and binding format of the original document and the print job. If the setting is:

- **Book-Style**: The original document has book-style (long edge) binding and the printed document has book-style binding.
- **Book-style original; Flip-style Copy**: The original document has book-style (long-edge) binding and the printed document has flip-style binding.
- **Flip-style**: The original document has flip-style (short edge) binding and the printed document has flip-style binding.
- **Flip-style original; Book-style Copy**: The original document has flip-style binding and the printed document has book-style binding.

Use the following steps to configure this option:

1. In **Orientation**, select the orientation for the scan job.
2. In **2-Sided Format**, select the desired binding format for the scan job.

Copy Contrast

Use this option to specify the default contrast (brightness) that the device uses to make copies. The device can make copies that are lighter or darker than the original. To take advantage of the one-touch copying feature, change the default contrast to the value that users typically select when making copies.

To specify the contrast that the device uses to make copies, select the contrast value from the list. For the lightest contrast (maximum brightness), select **8** or **125**. For the darkest contrast (minimum brightness), select **0** or **-125**.

Copy Darkness

Use this option to specify the default amount of exposure that is applied to the scanned document. For example, a lower setting will cause the printed output to be lightened; a higher setting will cause the printed output to be darkened.

To configure this option, select a default value for the darkness to be applied to scanned images.

Copy Fold

Use this feature to fold sheets of paper in half or into thirds. Folding is supported only for Letter-sized and A4-sized paper.

- Select **None** if no fold is necessary.
- Select **C-Fold** to fold the page into thirds towards the first side with the top or right side of the paper on the outside.

  When C-Fold is selected, Sheets Folded Together accepts 1 to 3 values.
- Select **V-Fold** to fold the page in half towards the first side of the paper.

  When V-Fold is selected , Sheets Folded Together accepts 1 to 5 values.
- Select **Advanced fold Options** to show more folding options or to change the location of the printed content in relation to the fold.

Copy Heavy Originals

Use this option to specify the weight of the original scanned documents.

When heavy paper is used, the device adjusts the tension and moves the paper through the scanning area at a slower rate. For paper that weighs more than 100 g/m^2, the quality of the output might improve if you select the **Heavy** option.

To specify the weight of the original scanned documents, select the **Normal** or **Heavy** option.

Copy Job Auto Interrupt

The auto job interrupt feature allows the product to automatically interrupt an active network print job between complete sets to print a new copy job. This option lets you specify if the auto job interrupt feature is enabled or disabled. If you enable the auto job interrupt feature, users do not have to wait for large, multi-copy network print jobs to finish printing before they can print a new copy job.

Use the following steps to configure this option:

1. To enable the auto job interrupt feature, select **On**.
2. To disable the auto job interrupt feature, select **Off**.

Copy Job Build

Use this option to enable by default combining multiple scanned jobs into a single printed document. If this option is enabled, then multiple scan jobs will be combined into one print job and no other network print jobs will interrupt the copy. If it is disabled, the scan jobs will remain separate scan jobs.

To set this option, select **Enabled** or **Disabled**.

Copy Job Scan Ahead

The walk-up copying feature allows you to walk up to the product and start making a copy while the product is busy printing a network print job. If the walk-up copying feature is enabled and a user initiates a copy job while the product is printing a network print job, the product scans and holds the copy job until it finishes printing the network print job. If the walk-up copying feature is disabled and a user initiates a copy job while the product is printing a network print job, the product waits until it finishes printing the network print job to start scanning the copy job. The product displays a message on the control panel saying that the copy job is blocked and will be processed as soon as the current job finishes printing. The user can choose to cancel the copy job or leave the originals in the automatic document feeder (ADF) or on the scanner glass.

Use the following steps to configure this option:

1. To enable this feature, select **On**.
2. To disable this feature, select **Off**.

Copy Manage Booklet

Use this option to copy two or more pages onto one sheet of paper so you can fold the sheets in the center to form a booklet. The product arranges the pages so that when multiple sheets are folded together, the pages are in the correct order.

To enable these features, select the check box next to them.

- **Booklet Format**: assembles sequential pages into the correct order for a booklet.
- **Borders on each page**: prints a border around each page.
- **Fold and Stitch**: automatically staples and folds the booklet pages.

NOTE: Set the Staple and Hole punch option to None to enable the Booklet option.

Copy Optimize Text/Picture

Use this option to optimize the quality of copy output based on the content of typical copy jobs. You can choose to optimize for text, photographs, printed pictures, or a mix of text and pictures.

Select the image type that is most commonly copied from the **Optimize Text/Picture** drop-down list.

If you select **Manually Adjust** from the **Optimize Text/Picture** drop-down list, the **Optimize For** drop-down list is available. To specify whether the copy output is optimized more for text or more for pictures by default, select the appropriate option from the **Optimize For** drop-down list.

Copy Output Bin

This option lets you specify the default output bin where the printed copies are delivered. The output bins that you can select depend on the output device that is configured with the product. If you want to take advantage of the one-touch copying feature, you should change the default to the output bin where the users typically send printed copies. This eliminates the need for the users to specify the output bin at the control panel each time they make copies.

To specify the default output bin for copies, select the output bin from the drop-down list.

Copy Pages Per Sheet

Use this option to specify the default number of pages to print on one physical piece of paper and how those pages are ordered on the paper.

Use the following steps to configure this option:

1. In **Pages per Sheet**, select the number of pages to be placed on one physical piece of paper.
2. In **Page order**, select how those pages should be placed on the paper.
3. To print page borders, select **Print page borders**.

Copy Paper Tray Selection

Use this option to specify the default input paper tray the device should use for a copy job.

To set this option, select the default paper tray that will be used for copy jobs.

Copy Reduce/Enlarge

Use this option to specify the default reduction and enlargement configurable settings for scanned jobs.

To set this option, specify the scaling within the given range or select **Auto Scale**.

Copy Sharpness

Use this option to specify the default amount of sharpness to be applied to the original document being scanned. A higher value produces sharper copies.

To set this option, select the default sharpness value. The higher the value, the greater the default sharpness.

Copy Stamps

Use this option to change custom Copy Stamps or use the pre-defined Copy Stamps text.

Select up to six preset positions for a stamp and configure the content that will be printed there.

- **Text Font**: Changes the font.
- **Text Size**: Changes the text size.
- **Text Color**: Changes the text color.
- **White Background**: Enables white background.

Copy Stamps (Custom)

Use these options to change the Custom Copy Stamps text or use the pre-defined Copy Stamps text.

Enable **Custom Copy Stamps Text** to use user-defined text.

Enable **Pre-defined Copy Stamps Text** to use pre-defined text.

Copy Stamps (Enforced)

Use this option to use the features of both Copy Stamps and Copy Stamps (Custom).

NOTE: Once changes are made in Copy Stamp (Enforced), further changes can not be made in Copy Stamps or Copy Stamps (Custom).

Select the stamp content by selecting the check boxes.

Select up to six preset positions for a stamp and configure the content that will be printed there.

- **Starting Number**: Sets the starting page number in pre-defined stamps.
- **Text Font**: Changes the font.
- **Text Size**: Changes the text size.
- **Text Color**: Changes the text color.
- **White Background**: Enables white background.

Copy Staple

Use this option to specify the default staple placement for copy jobs. This setting is only available if a stapler is attached to the device.

To set this option, select the staple placement for copy jobs.

Copy Staple/Hole Punch

Use this option to specify the default staple/hole punch placement for copy jobs. These settings are only available if a stapler/finisher is attached to the device.

To set these options, select the staple/hole punch placement for copy jobs.

Copy Watermark

Use this option to change the watermark text and the following options:

- **Watermark Type**: Set text either as None, Text, or Secure. Text is placed at the center of the page.
- **Secure Watermark Text**: Background text and pattern that is barely visible on the first copy of a document. Any future copies of the document display the watermark more visibly.
- **First Page Only**: Prints watermark only on the first page.
- **Rotate text 45 degrees**: Rotates text 45 degrees.
- **Text Font**: Changes the font.
- **Text Size**: Changes the size of the font to 30, 40, or 60 point.
- **Background Color**: Changes the color of the background.
- **Background Pattern**: Changes the pattern of the background.
- **Darkness**: Changes the darkness of the font.

Copy Watermark (Custom)

Use these options to change the Custom Watermark text or to use the pre-defined Watermark text.

Enable **Custom Watermark Text** to use user-defined text.

Enable **Pre-defined Watermark Text** to use pre-defined text.

Default Copier Copies

This option allows you to select the default number of copies that will be generated on each copy job initiated from the control panel.

To select the default number of copies, type the number of copies (between 1 and 99) in the edit box.

Default Copy Collation

This option lets you specify collation behavior. Since collation does consume additional resources on the device, turning this feature off can sometimes allow the device to complete jobs which otherwise may have failed to complete.

Use the following steps to configure this option:

1. To enable this feature, select **On** or **Enabled**.
2. To disable this feature, select **Off** or **Disabled**.

Default Edge-to-Edge Setting

Use this option to specify whether copies are printed as close to the edge of the page as possible or printed with the normal unprinted border.

Use the following steps to configure this option:

1. For a 1 mm (0.04 inch) unprintable border, select the **Edge-to-Edge Output** option.
2. For a 6.35 mm (0.25 inch) unprintable border, select the **Normal** option.

Default Image Quality

This option lets you select the default copy quality either for maximum performance, or for more economic operation when the best performance is not needed.

To configure this option, select the desired quality level.

Default Number of Copies

This option lets you specify the default number of copies that are printed for each copy job. If you want to take advantage of the one-touch copying feature, change the default to the number of copies that the users typically print. This eliminates the need for the users to specify the number of copies at the control panel each time they make copies.

To specify the default number of copies, type the quantity in the text box.

Default Number of Sides

This option lets you specify if one side or both sides of the original or the copy document are copied.

To configure this option, select the desired default number of sides from the drop-down box.

Default Original Content

This option lets you specify the default type of information that is on the original document (**Text**, **Graphics**, or **Mixed**). If you want to take advantage of the one-touch copying feature and the users typically copy originals that have only graphics or only text, change the default to the appropriate type of information. This eliminates the need for the users to specify the page content at the control panel each time they make copies.

To configure this option, select the information type (**Text**, **Graphics**, or **Mixed**) from the drop-down box.

Default Original Media Size

This option lets you specify the default original media size of copied documents. The paper sensors override the default. If the paper sensors cannot detect the size of the original, the product uses the default. If you want to take advantage of the one-touch copying feature, change the default copy media size to the size of the originals that the users typically copy. This eliminates the need for the users to specify the media size at the control panel each time they make copies.

To specify the media size of the originals, select the media size from the drop-down list.

First Copy Speed

This option lets the device handle the speed for the first copy. If you do not use the copying functionality frequently, you may take advantages to enable the fast first copy feature.

To disable this option, select **No early warm up** (default). The copying process might be slower for the first copy.

To enable this option, select **Early warm up**. The copying process will be faster but it might cause excessive wear on the device.

Hold Off Print Jobs During Copy

Use this option to prevent network print jobs from starting until after the product finishes printing a copy job. You can specify if the hold off print job feature is enabled or disabled. Enabling this option will give walk-up copying users priority over network print jobs, and the product will not start printing any network print jobs as long as a user is interacting with the control panel.

Some products support the Hold Off Time on page 300 option. The device will wait for the amount of time that you specify for the Hold Off Time on page 300 option after a copy job finishes printing before starting to print any network print jobs.

NOTE: If you enable the hold off print job feature, you must also specify a value for the Hold Off Time on page 300 option.

Use the following steps to configure this option:

1. To enable this feature, select **On**.
2. To disable the hold off print job feature, select **Off**.

Hold Off Time

This option lets you specify the default amount of time that network print jobs must wait before starting to print if the Hold Off Print Jobs During Copy on page 300 option is enabled. If you want to give walk-up copying users priority over network print jobs, you should configure the Hold Off Print Jobs During Copy on page 300 option. HP Web Jetadmin will not start printing any network print jobs as long as a user is interacting with the control panel. In addition, the product will wait for the amount of time that you specify for the **Hold Off Time** option after a copy job finishes printing before starting to print any network print jobs.

NOTE: If the Hold Off Print Jobs During Copy on page 300 option is not enabled, HP Web Jetadmin ignores the **Hold Off Time** value entered for this feature.

To specify how long HP Web Jetadmin waits before starting network print jobs, type the number of seconds in the text box.

Interrupt Copy Jobs

This feature lets you interrupt an active copy job between complete sets to print a new copy job. This option lets you specify if the copy job interrupt feature is enabled or disabled. If you enable the copy job interrupt feature, users do not have to wait for large, multi-copy copy jobs to finish printing before they can print a new copy job.

Use the following steps to configure this option:

1. To enable this feature, select **On**.
2. To disable the interrupt copy job feature, select **Off**.

Paper Path

Use this option to configure the paper path.

- Select **Automatically Select** to automatically copy.
- Select **Face–up (straightest path)** to copy face-up.
- Select **Face–down (correct order)** to copy face-down.

Device Configuration Options for Device

Configuration options for Devices define general administrative functions for the device including Power Save, Tray Administration, and print defaults.

Alternative Letterhead Mode

When printing using duplex mode, this option defines the first side of the page as having letterhead and the other side having no letterhead.

To configure this option, select **On** or **Off**.

Anonymous Usage Information Transmission

Use this option to enable or disable the transmission of anonymous information about the printer to HP. The printer sends the following types of information to HP:

- The country/region, language, and local time zone where the printer is installed
- The printer model number
- Information about how the printer is used, such as the number of pages printed, print mode used, media printed, brand of cartridges installed, file types printed, and applications used to print jobs
- The events that occur, such as low supply alerts
- The printer features that are used, such as photo card slots, fax, scan, and HP Embedded Web Server
- Additional technical information that varies depending on the printer

HP uses this information to design future printers that better meet customers' needs.

IMPORTANT: HP is committed to protecting your privacy and the integrity of your devices. Your name, address, email address, and other sensitive data are not sent to HP.

To enable the transmission of anonymous usage information, select the **Enable** option.

-or-

To disable the transmission of anonymous usage information, select the **Disable** option.

Asset Number

Use this option to assign an asset number to the device. The asset number can be based on any user-defined schema, such as an organization's accounting system.

NOTE: You can only apply this configuration option to a single device. You cannot use this configuration option to configure multiple devices with the same static value in a template.

Use the following steps to configure this option:

1. Enter the device asset number in the box. Most devices support a maximum of 1,024 characters.

   This text box can use static data or custom variables supported in the following formats:

   - Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

     %%<custom variable>%% (where “<custom variable>” is the name of the user defined field)

     Example: `%%var_AssetNumber%%`

   - Variable data along with a combination of static content before or after the variable

     <static value>%%<custom variable>%%<static value>

     Example: `CityName%%var_AssetNumber%%`

     Example: `CityName%%var_AssetNumber%%Building`

   TIP: By starting the variable data name with var_, it’s easier to find and identify user defined fields in HP Web Jetadmin.

   TIP: In HP Web Jetadmin, text boxes that support variable data are highlighted blue. For more information on variable data, see Create and Use Variable Data on page 183.

2. To apply the asset number to the device immediately, click the **Apply** button.

   -or-

   To apply the asset number to the device later, click the **Schedule** button. The **Schedule Device Configuration** wizard starts. For more information about using the **Schedule Device Configuration** wizard, see Schedule Device Configurations on page 178.

Auto Cleaning Page

This option enables and disables the automatic cleaning page. You can specify how often you want to print the automatic cleaning page. If the printer is in the middle of a print job when it reaches the page count that you specify, the printer finishes printing that print job before it starts the cleaning process. The cleaning process takes approximately 2.5 minutes to complete. You can either discard or recycle the cleaning page after it is printed.

Use the following steps to configure this option:

1. To enable **Auto Cleaning Page**, select **Auto cleaning page enabled**.
2. Select the cleaning frequency.
3. Select the page size (Letter or A4). You must use plain paper.

NOTE: To ensure that the cleaning process runs automatically and without intervention, make sure that the paper size you specify is always available in the printer.

Auto Continue

Choose to have a non-critical error message appear for ten seconds before the device resumes operation. Select **Off** for **Auto Continue** to require you to acknowledge non-critical error messages by pressing **Continue** on the device before the device resumes operation.

Use the following steps to configure this option:

1. To enable **Auto Continue**, select **On**.
2. To disable **Auto Continue**, select **Off**. You will have to acknowledge non-critical error messages by pressing **Continue** on the device before the device resumes operation.

Auto Recovery

Use this option to enable or disable the Auto Recovery feature on the device. If this option is enabled and an unrecoverable error occurs in the device firmware, the device automatically turns off and turns on to recover from the error.

To enable the Auto Recovery feature on the device, select the **Enabled** option.

To disable the Auto Recovery feature on the device, select the **Disabled** option.

Auto Sense Mode

Use this option to optimize device settings for certain media types that can be detected automatically by the printer. Not all printers will support all of the sensing methods, or sensing from every tray. Sensing options may include:

- **Full Sensing**: For each sheet of paper that is picked up from the tray, the product detects light paper, plain paper, heavy paper, glossy paper, tough paper, and transparencies.
- **Expanded Sensing**: For the first few sheets of paper that is picked up from the tray, the product detects light paper, plain paper, heavy paper, glossy paper, tough paper, and transparencies. The product assumes the rest of the pages are of the same type.
- **Transparency Only**: The product distinguishes between transparencies and non-transparencies.

Use the following steps to configure this option:

1. Select the setting for **Tray 1 Sensing** to configure how the device detects media in Tray 1.

2. Select the setting for **Tray N Sensing** (if available) to configure how the device detects media in trays 2 through N.

AutoSend

Use this option to enable the device to periodically send usage information about the device's configurations and supplies to a list of recipients.

Use the following steps to configure this option:

1. Check the **Enable AutoSend** box to enable this feature.

2. Select the frequency to send configuration and supplies information in **Send every**.

3. If you have a relationship with HP that provides you with services such as proactive cartridge replacement, pay per page contracts, support agreements, or usage tracking, enable the **Send to HP using HTTPS** feature. Information is always sent to HP securely using HTTPS POST, if possible. Otherwise, you can choose to allow this information to be sent using email if HTTPS fails or is unavailable.

4. If you want to send the same information to a custom list of web addresses or email addresses, enable those features and enter the appropriate addresses.

AutoStore

AutoStore is an automated document and content capture solution for HP MFP devices. The **AutoStore** product consists of a server-based application, **AutoStore Server**, and an installable embedded Web server application, **AutoStore ChaiService**.

The **AutoStore ChaiService** contacts the **AutoStore Server** on a regular basis to determine whether there is a new set of **AutoStore** menus to download and display on the front panel of a device. To do this, it must be configured with the **AutoStore Server** information. You can also configure how frequently the **AutoStore ChaiService** will contact the **AutoStore Server**.

NOTE: To protect the **AutoStore** menus, use a device's authentication feature. If authentication is used, configure the **AutoStore ChaiService** to revoke authentication when certain events occur.

NOTE: For convenience, configure the **AutoStore ChaiService** to contact the **AutoStore Server** immediately for new **AutoStore** menus, especially when the administrator is testing a newly designed set of **AutoStore** menus.

After **AutoStore** is installed and configured, the front panel on a device or group of devices displays the **AutoStore** menus. These menus allow users to easily scan, process, and route documents to pre-programmed destinations. For example, an MFP device scans the documents, and then the **AutoStore Server** processes and then routes the documents to a destination.

NOTE: If the **AutoStore ChaiService** is installed on a device(s), you must configure the **AutoStore ChaiService** to use the service.

NOTE: HP Web Jetadmin does not display the current configuration settings in this section. You can use HP Web Jetadmin to change the configuration settings. To view the configuration settings, you must use HP Web Jetadmin to browse to the device embedded Web server.

Use the following steps to configure this option:

1. Select either **IP Address** or **Hostname** and then type the IP address or hostname in the corresponding text box.
2. Type the network port value in **Port** (1 to 9999).
3. To specify how often to poll the **AutoStore Server**, type the interval (in minutes) in **Interval**.
4. If displayed, set the **Authentication timeout**.
5. If displayed and if desired, select **Revoke authentication on reentry**.
6. Click **Apply**.

Browser

Use this option to configure specific settings for the web browser on the device (for example, enabling OXPd 1.6 support). The web browser settings that can be configured include connection timeout, response timeout, and a list of trusted sites.

Use the following steps to configure this option:

1. To set the connection timeout, select an option from the drop-down list.
2. To set the response time, select an option from the drop-down list.
3. Enter trusted sites in the **Trusted sites** text box. For multiple sites, use a semicolon to separate each entry.

Calibration Timing

Use this option to control when calibrations are performed. You can set the timer (in hours) to turn on or off calibration. If a time is set, the calibration takes place after the timer expires and the next job is finished printing.

To set this option, select a time from the dropdown box and click **Apply**.

Cartridge Low Action

This option lets you specify how the printer responds when a toner-low condition exists. Set the printer to continue normal operations or set it to stop printing. In either case, HP Web Jetadmin displays a Toner Low message on the Device Status page. Allowing the printer to continue printing when the toner is low lets the current print job finish printing and gives the user who is responsible for the printer time to change the toner cartridge. However, this might result in poor print quality.

Use the following steps to configure this option:

1. To let the printer continue printing when the toner is low, select **Continue**.
2. To stop the printer from printing until the toner is replaced, select **Stop**.

Cartridge Out Action

This option lets you specify how the printer responds when a toner-out condition exists. Set the printer to continue normal operations or set it to stop printing. In either case, HP Web Jetadmin displays a **Toner Out** message on the Device Status page. Allowing the printer to continue printing when the toner is out lets the current print job finish printing and gives the user who is responsible for the printer time to change the toner cartridge. However, this might result in poor print quality.

Use the following steps to configure this option:

1. To let the printer continue printing when the toner is out, select **Continue**.
2. To stop the printer from printing until the toner is replaced, select **Stop**.

Clearable Warnings

This option lets you determine whether a warning is cleared on the control panel or when another job is sent.

Use the following steps to configure this option:

1. Select **On** to display a warning until GO is pressed.
2. Select **Job** to display a warning until the end of the job in which it was generated.

If **On** is selected, a warning is displayed until GO is pressed. If **Job** is selected, a warning is displayed until the end of the job in which it was generated.

Cold Reset Media Size

This option returns or sets the media size that is used as the **Default Media Size** when a cold reset occurs. Different countries/regions require different default media sizes. The factory uses this option to select the default media size.

Use the following steps to configure this option:

1. To set the **Cold Reset Media Size** option, select the option for the media size.
2. Click **Apply**.

Color Control Setting

Use this option to control the color settings.

- **Drying Time**: Change the drying time to Normal, Most, or More, by selecting the drop down menu.

  The drying time is a period of time inserted between pages to reduce the chance that a page will smear the one below it in the output tray. Printing will pause temporarily if more time is needed.

  NOTE: The time it takes for pages to dry varies greatly depending on paper type, printer driver settings, humidity, and temperature. In addition, the paper type and printer driver settings might affect the printing speed.

- **Black Spread**: Change the black spread to Normal, Less, or Least, by selecting the drop down menu.

  Black spread can appear as blurriness where light and dark colors meet, making edges less sharp and defined.

- **Saturation**: Move the slider to adjust the amount of saturation.

  Saturation is the amount of color used during the printing process. Certain coated paper (such as photo paper) can absorb larger quantities than other types of paper (such as plain paper).

NOTE: If you notice smearing on printed documents or images, use a lower saturation setting.

- **Hue Correction**: Move the slider to adjust the color levels used in documents and images.
- **Ignore Driver Settings**: If selected, only the device's settings apply.
- **Restore Factory Defaults**: Restores the default settings in the drop down menus.

Color Supply Out

This option lets you specify how the printer responds when one of the color toners is empty. You can choose to set the printer to continue printing with black toner (for a certain number of pages) or set it to stop printing altogether. In both cases, HP Web Jetadmin displays a **Toner Out** message on the device lists.

Use the following steps to configure this option:

1. To stop the printer from printing until the toner is replaced, select **Stop**.
2. To let the printer continue printing with black toner, when one or more of the color toners is out, select **Auto Continue Black**.

Color/Black Mix

This option optimizes the performance or cost per page depending on the expected color content of typical print jobs. This feature allows you to set printer behavior for printing mostly color or mostly black (monochrome) print jobs.

NOTE: Selecting the **Print In Grayscale** feature from the printer driver overrides these settings for a specific print job.

Use the following steps to configure this option:

1. **Auto**: (Default) best choice for most conditions; it behaves the same as **Mostly Color Pages**.
2. **Mostly Color Pages**: Provides the best performance for most conditions, especially when mostly color pages are printed. Under normal usage, there is minimal or no cost per page impact from this selection.
3. **Mostly Black Pages**: Provides the best cost per page for users printing mostly monochrome pages on color printers.

Company Name

The company contact is the name of the organization that owns or is responsible for the device.
HP Web Jetadmin displays the company contact on the **Status** page for the device and on several of the device lists. You can also search for and display a list of all of the devices for which a specific organization is responsible.

Contact Person

Use this option to specify the name of the person who should be contacted if there are any problems with the device or if you need support.

To set this option, type the name of the contact person.

Control Panel Display

This option lets you make specific items appear on the Control Panel Display on the device. The items include IP Address, Hostname, Serial Number, Asset Number, Device Name, System Location, System Contact, Device Location and a short text string that you can define.

One option can be selected.

Select the desired option. If you select **Other**, enter the message to display on the control panel.

Control Panel Language

This option lets you specify the language that is displayed on the printer control panel. The drop-down list contains all of the languages that the printer supports. If you have a multilingual workforce, set the control panel language to the one language that your employees prefer.

Choose the desired language from the drop-down list.

Courier Font Type

This option allows you to choose whether the regular courier font or a dark font is used. This setting does not affect fax or copy jobs, but does apply to the internal reports which contain a Courier font. The regular TrueType Courier font prints somewhat lighter than the bitmap fonts for the same.

To specify the courier font type, select **Regular** or **Dark**.

Date and Time

This option allows you to remotely specify the time and date for a device or group of devices. When the correct time and date is set on a device, the device can complete time or date dependant operations and add time and date stamps on documents, such as a diagnostic report.

To specify the time and date on a device, type the current year, month, and day in the corresponding fields. Use the 12-hour system. For example, 1 PM is 1 PM.

Date/Time Format

Use this option to specify the format for dates and times as displayed on the device. Specifying the format allows you to comply with the formats used by your organization.

To specify the date format, select a format from **Date format**. To specify the time format, select a time format from **Time format**.

Daylight Savings Time

Use this option to specify the date range for daylight saving time (summer time), which should match the daylight saving time schedule for the location of the device.

Use the following steps to configure this option:

1. To specify the start date and end date for daylight saving time, perform the following steps:
   a. In the **Start Date** and **End Date** columns, select the appropriate values from the **Occurrence**, **Week Day**, **Month**, and **Hour** drop-down lists.
   b. Type the number of minutes for the daylight saving time offset in the **DST Offset** text box.
2. To use the default start date and end date for daylight saving time, select the **Use Defaults** option.

Default Input Paper Tray

This option lets you specify which tray the device should first get paper from as a default (upper paper tray or lower paper tray).

Select the paper tray you want to use for a default.

Default Media Size

This option lets you specify the default media size. The drop-down list contains all of the media sizes that the printer supports. This option is useful if the people who use the printer typically print on a specific size of media. For example, if the printer is dedicated to the legal department and those users typically print on Legal paper, set the default media size to Legal.

The media size setting that you might select when printing a job overrides the setting specified here.

To specify the default media size, select the media size from the drop-down list labeled **Default Media Size**.

Default Media Type

This option specifies the default media type. The drop-down list contains all of the media types that the printer supports. This option is useful if the people who use the printer typically print on specific media. For example, if the printer is dedicated to the human resources department and they typically print on three-hole punched paper, set the default media type to **Prepunched**.

NOTE: For this option to work, you must specify the media type for each tray under the **Media Type Administration** category on the **Device Configuration** page.

The media type setting that a user selects when printing a job overrides the setting specified here.

To specify the default media type, select the media type from the drop-down list.

Default Print Density

This option lets you select the default density for print jobs, which affects all pages printed on the device (host print jobs, received faxes, copies, and internal reports).

To select this option, select a density from the drop-down box (5 is the darkest, or highest density). For color, select the desired print density for each color. If applicable, you can also select the print density for highlights, midtones, and shadows.

Default Printer Copies

This option lets you specify the default number of copies that are printed for each print job. This option is useful if the people who use the printer typically print a specific number of copies. For example, if the printer is dedicated to the legal department and those users always print three copies of their documents, set the default number of copies to three.

NOTE: The copies setting that you select when printing a job overrides the setting specified here.

To specify the default number of printer copies, type the number of copies into **Default Printer Copies**.

Delay Calibration at Wake/Power On

Use this option to control the timing of the calibration when the printer wakes up or is turned on.

Use the following steps to configure this option:

1. To set the printer to calibrate immediately when it wakes up or is turned on, select **Off**. The device will not print any jobs until it finishes calibrating.
2. To enable a device that is asleep to accept print jobs before it calibrates, select **On**. The device only accepts new jobs for a short time. It may start calibrating before it has printed all the jobs it has received.

NOTE: For best results, allow the device to calibrate before printing. Print jobs performed before calibration might not be of the highest quality.

CA Certificates

Devices use certificate authority (CA) certificates, which are also called public keys, to browse to external websites. For example, devices might require a CA certificate to enable OXPd 1.6 support. If there are no CA certificates in the device's certificate store, the device uses the HP Jetdirect CA certificate if one is available.

Use this option to install or remove the Secure Sockets Layer (SSL) trusted CA certificates on the device.

Install or remove CA certificates on the device

When CA certificates are removed from the device, the CA certificates remain in the HP Web Jetadmin Certificate Repository.

CAUTION: If an intermediate CA certificate is installed, the scope of authentication is limited.

1. If you are configuring multiple devices, select one of the following options in the **Overwrite options** section:
   - **Replace/overwrite existing Certificates**
   - **Append to existing Certificates**
   - **Remove Certificates**
2. Click the **Add** button. The **Add Device Certificate** window opens with a list of all of the CA certificates that are stored in the HP Web Jetadmin Certificate Repository.

   TIP: To manage the list of CA certificates, click the **Edit** button. The **Options** window opens with the **Certificate Repository** option selected. For more information about the Certificate Repository, see Manage the Certificate Repository on page 69.
3. Select the CA certificates from the list, and then click the **OK** button.

Delete CA certificates from the list of available CA certificates

▲ From the **Certificates** list, select the CA certificates, and then click the **Remove** button.

Device Location

This option identifies the device based on its location. You can use the **Device Location** to search for and display a list of all of the devices that have specific text in their device locations (for example, North Bldg, 3rd Floor).

HP Web Jetadmin displays the **Device Location** on the device lists if you configured this option to be listed (Device Identification on page 33 and Columns for Device Lists on page 106). You can also choose to have this column display in any custom view (Customizing Layouts for Device Lists on page 109).

To configure this option, enter a description of the location in the text box. The maximum number of characters is 1,024.

NOTE: Some devices do not support a maximum of 1,024 characters.

Device Name

This option identifies the device based on its name. You can use the **Device Name** to search for and display a list of all of the devices that have specific text in their device names (for example, Color LaserJet Marketing).

HP Web Jetadmin displays the **Device Name** on the device lists if you configured this option to be listed (Device Identification on page 33 and Columns for Device Lists on page 106). You can also choose to have this column display in any custom view (Customizing Layouts for Device Lists on page 109).

To set the device name, type or change the device name in **Device Name**.

Device Volumes

This group of options selects the volumes of certain sounds emitted by the device:

NOTE: Some of the volume options may not be displayed depending on available features of the device being configured.

- **Line monitor**: Allows you to set the volume level used during the fax machine to fax machine negotiation for each sent and received fax.
- **Alarm**: Allows you to set the volume level used by the device for the beep to indicate an error condition.
- **Ring**: Allows you to set the volume level used to indicate an incoming call on the connected phone line.
- **Key press**: Allows you to set the volume level used when control panel keys are pressed.

To select the volume options, select **Off**, **Soft**, **Medium**, or **Loud**.

Duplex Binding

Use this option to specify the default duplex option and orientation that is used when a print job does not specify these settings. System administrators can use this option to implement a policy for duplex printing when print jobs do not specify a setting.

To specify the default duplex option for the device, select one of the following options:

- **Long Edge**—This option is recommended for portrait print jobs.
- **None (1-sided)**
- **Short Edge**—This option is recommended for landscape print jobs.

Duplex Blank Pages

This option lets you optimize the duplex printing performance.

Select **Auto** to enable enhanced print speed in some circumstances by often not taking the time to print blank sides. For paper types that need to print the blank side (like letterhead), **Auto** is smart enough to do so.

Select **Yes** to always print blank sides in duplex jobs. The image will always be on the correct side.

Duplex Impressions

This option lets you define how a device counts pages. This option also includes an **Opt in** agreement to make the user aware that once enabled, this setting cannot be disabled. Each user is required to opt-in before they will be able to set this configuration.

Use the following steps to configure this option:

1. Click **"Opt In" to enable**.
2. The **HP Print Tracker Usage Change** agreement is displayed. Carefully review the document. If you accept the terms, select **I accept**. If you do not accept the terms, this option cannot be enabled.
3. To enable this option, check the box **Enable duplex impression counting**.

Dust Detection

Use this feature to receive notifications when the product detects dust on the document feeder scan assembly. Dust can reduce scan quality.

- **Dust Detection Error Messaging**

To enable Dust Detection Error Messaging, select the **Enabled** option.

To disable Dust Detection Error Messaging, select the **Disabled** option.

- **Dust Detection Feature**

To enable the Dust Detection Feature, select the **Enabled** option.

To disable the Dust Detection Feature, select the **Disabled** option.

- **Dust Detection Sensitivity**

To configure Dust Detection Sensitivity, select either **Low**, **Medium**, or **High** from the drop-down box.

Economode

This option allows you to select the **Economode** (toner saving) default for jobs that do not specify an Economode value. This allows the printer to behave in a consistent manner for print jobs which do not specify the Economode setting.

To specify the default Economode value, select the radio button for the desired Economode (**On** or **Off**).

Enable Retrieve/Print from USB

Use this option to enable or disable the ability to print documents from a USB flash device.

To enable USB printing, select the **Enabled** option.

-or-

To disable USB printing, select the **Disabled** option.

Energy Settings

Use this option to change Sleep and Shutdown settings after inactivity.

- **Sleep/Auto Off After**: Changes when the device sleeps after inactivity.
- **Shut Down After Inactivity**: Changes when the device shuts down after inactivity.
- **Delay when ports are active**: Delays these energy settings if any ports are in use.

Fuser Modes

Use this option to specify the fuser temperature mode for all the media types that the device supports. You can associate a different fuser temperature mode with each media type. If your environment experiences variable humidity conditions, changing the fuser temperature mode can maximize the print quality.

To configure the fuser mode for a media type, select the fuser mode from the drop-down list. For more information about the appropriate fuser modes for a specific device, see the device documentation.

NOTE: When configuring this option in batch mode, a list of all the media types and fuser modes that are available on all the supported devices displays. If you specify a media type or fuser mode that a selected device does not support, the setting is ignored for that device.

FutureSmart Level

Each version of the HP FutureSmart firmware can include multiple levels of functionality. HP Web Jetadmin displays the range of firmware levels that are available in the HP FutureSmart firmware that is installed on the device.

Use this option to specify the level of the HP FutureSmart firmware version that the device uses.

NOTE: This configuration option is available for HP FutureSmart 3 or later.

NOTE: For more information about HP FutureSmart, see the HP FutureSmart Solution Web site.

To configure this option, enter the firmware level in the box. If the firmware level is outside of the range of levels that are available on the device, HP Web Jetadmin automatically changes the firmware level to the nearest minimum or maximum level that the device supports.

After HP Web Jetadmin applies the firmware level to the device, the device automatically restarts.

High Capacity Output Mode

This option lets you specify which high-capacity output accessory the printer directs output to. Directing output to various high-capacity output accessories can help reduce how much time you spend going to the printer and removing output from full bins. This is particularly useful for very large print jobs or busy printers.

To set the high-capacity output mode, select one of the output accessory options.

High Capacity Output Names

Use this option to assign unique names to the printer multibin mailboxes. After you assign a name to a mailbox, users can direct their output to a specific mailbox. For example, you might want to name mailboxes after departments or individuals within a department.

NOTE: You can only apply this configuration option to a single device. You cannot use this configuration option to configure multiple devices at one time or include this configuration option in a template.

To configure this option, type the name in the text box next to the mailbox.

Home Screen Applications - FutureSmart 3

Use this option to specify which applications are displayed on the device control panel for devices that have FutureSmart 3 or earlier. Specify the order in which the applications are displayed, and move applications into and out of the Quick Sets folder.

Third-party applications might be included in the list of applications. However, other tools might control whether these applications are displayed or hidden on the device control panel.

The Quick Sets folder appears in the main list of applications. Only one Quick Sets folder is allowed. Quick Sets applications can reside in the main list of applications or in the Quick Sets folder. Applications in the Quick Sets folder are displayed immediately after the folder, and the application names are indented. You can move applications in the Quick Sets folder up or down in the list or move them out of the folder into the main application list. However, you can only move Quick Sets applications from the main application list into the Quick Sets folder.

Each application has a corresponding checkbox that specifies if the application is displayed or hidden on the device control panel. The first row of the table contains a master checkbox that controls the checkboxes for all the applications. If you select the master checkbox, the checkboxes for all the applications are selected. If you clear the master checkbox, the checkboxes for all the applications are cleared. Selecting or clearing the checkbox for an application does not affect the status of the master checkbox. The following describes how the checkboxes for the Quick Sets folder and the applications in the folder behave:

- If you select the checkbox for the Quick Sets folder, the status of the checkboxes for all the applications in the folder remains unchanged.
- If you clear the checkbox for the Quick Sets folder, the checkboxes for all the applications in the folder are also cleared.

- If you select the checkbox for an application in the Quick Sets folder, the checkbox for the Quick Sets folder is also selected. The Quick Sets folder must be displayed on the device control panel if any of the applications in the folder are to be displayed.
- If you clear the checkbox for an application in the Quick Sets folder, the status of the checkbox for the Quick Sets folder remains unchanged.

For batch configurations and templates, the checkboxes initially contain a blue square. When you select a checkbox with a blue square, the checkbox is cleared. In a batch configuration or template, the **Home Screen Applications** configuration option is not valid if all the checkboxes contain a blue square. At least one checkbox must be cleared or selected.

The applications are displayed on the device control panel in the order in which they appear in the table. You can move applications up or down relative to one another. You can also move Quick Sets applications into and out of the Quick Sets folder. The buttons to the right of the table are enabled or disabled depending on which application you select.

Use the following steps to configure this option:

1. To display all the applications on the device control panel, select the master checkbox in the **Show/Hide** column.

   -or-

   To hide all the applications on the device control panel, clear the master checkbox in the **Show/Hide** column.
2. To display an application on the device control panel, select the corresponding checkbox in the **Show/Hide** column.
3. To hide an application on the device control panel, clear the corresponding checkbox in the **Show/Hide** column.
4. To change the order in which the applications are displayed on the device control panel, select an application in the main application list or in the list of applications in the Quick Sets folder, and then click one of the following buttons:
   - **Move to top**: Moves the selected application to the first row in the appropriate list.
   - **Move up**: Moves the selected application up one position in the appropriate list.
   - **Move down**: Moves the selected application down one position in the appropriate list.
   - **Move to bottom**: Moves the selected application to the last row in the appropriate list.
5. To move a Quick Sets application from the main application list into the Quick Sets folder, use the **Move up** and **Move down** buttons to position the application immediately after the Quick Sets folder. Select the application, and then click the **Move in** button. The selected application is positioned at the end of the list of applications in the folder.
6. To move a Quick Sets application from the Quick Sets folder into the main application list, select the application, and then click the **Move out** button. The selected application is positioned in the main application list immediately after the Quick Sets folder.
7. To restore the order of all the applications to the order that they were in when you accessed this configuration option, click the **Reset** button.

Home Screen Applications - FutureSmart 4

Use this option to specify which applications are displayed on the device control panel for devices which have at least FutureSmart 4, devices with older firmware should be configured with the **Home Screen Applications (-FutureSmart 3)**. With the **Home Screen Applications - FutureSmart 4** option, you specify the tree order in which the applications are displayed, the page on which the applications are displayed, and you can move applications into and out of the Quick Sets folder. The first page in HP Web Jetadmin is the default screen on the device. The second page in HP Web Jetadmin can be seen on the device after scrolling to the next/second page.

Third-party applications might be included in the list of applications.

The Quick Sets folder appears in the main list of applications. Only one Quick Sets folder is allowed. Quick Sets applications can reside in the main list of applications (basically, the top tree level) or in the Quick Sets folder. Applications in the Quick Sets folder are displayed immediately after the folder, and the application names are indented. You can move applications in the Quick Sets folder up or down in the list or move them out of the folder into the main application list. However, you can only move Quick Sets applications from the main application list into the Quick Sets folder.

Each application has a corresponding checkbox that specifies if the application is displayed or hidden on the device control panel. The first row of the table contains a master checkbox that controls the checkboxes for all the applications. If you select the master checkbox, the checkboxes for all the applications are selected. If you clear the master checkbox, the checkboxes for all the applications are cleared. Selecting or clearing the checkbox for an application does not affect the status of the master checkbox. The following describes how the checkboxes for the Quick Sets folder and the applications in the folder behave:

- If you select the checkbox for the Quick Sets folder, the status of the checkboxes for all the applications in the folder remains unchanged.
- If you clear the checkbox for the Quick Sets folder, the checkboxes for all the applications in the folder are also cleared.
- If you select the checkbox for an application in the Quick Sets folder, the checkbox for the Quick Sets folder is also selected. The Quick Sets folder must be displayed on the device control panel if any of the applications in the folder are to be displayed.
- If you clear the checkbox for an application in the Quick Sets folder, the status of the checkbox for the Quick Sets folder remains unchanged.

When creating a template in template mode, the checkboxes initially contain a blue square. A blue square means that the current configuration for this item on a device will not be changed. When you select a checkbox with a blue square, the checkbox is cleared. In a batch configuration or template, the **Home Screen Applications** configuration option is not valid if all the checkboxes contain a blue square. At least one checkbox must be cleared or selected.

The applications are displayed on the device control panel in the order in which they appear in the table. You can move applications up or down relative to one another. You can also move Quick Sets applications into and out of the Quick Sets folder. The buttons to the right of the table are enabled or disabled depending on which application you select.

Use the following steps to configure this option:

1. To display all the applications on the device control panel, select the master checkbox in the **Show/Hide** column.

   -or-

To hide all the applications on the device control panel, clear the master checkbox in the **Show/Hide** column.

2. To display an application on the device control panel, select the corresponding checkbox in the **Show/Hide** column.
3. To hide an application on the device control panel, clear the corresponding checkbox in the **Show/Hide** column.
4. To change the order in which the applications are displayed on the device control panel, select an application in the main application list or in the list of applications in the Quick Sets folder, right-click and then click one of the following buttons:
   - **Move In**: Moves the selected application to the appropriate folder. It will list the applicable folders.
   - **Move Out**: Moves the selected application out of the folder (this will move the application to the top level).
   - **Move to top**: Moves the selected application to the first row in the appropriate list.
   - **Move up**: Moves the selected application up one position within the current folder.
   - **Move down**: Moves the selected application down one position within the current folder.
   - **Move to bottom**: Moves the selected application to the last row within the current folder.
   - **New Folder**: Use this option to create a new folder.
   - **Edit Folder**: Use this option to rename an existing folder.
   - **Delete Folder**: Use this option to delete a folder.
   - **Restore All**: Cancel/restore all the applications to the order that they were in when you accessed this configuration option.
5. To change the page number of the application (the scrolling location on the screen), click the drop down box under the Page Number column. If the page number can’t be assigned, the closest possible page number will be selected.

Home Screen Language Selection

Use this option to enable or disable the Language Selection button on the device control panel. If you enable the Language Selection button, users can select a different language for the control-panel display during their session.

For some devices, if you enable the Language Selection button, you can specify up to four alternate languages for the control-panel display and the default keyboard layout for each alternate language.

For some devices, you can specify the default keyboard layout for all the available languages. You can also enable or disable the alternate keyboard layout button on the keyboard screens. If you enable the alternate keyboard layout button, you can specify which keyboard layouts are available.

Use the following steps to configure this option:

1. To enable the Language Selection button on the control panel, select the **Show the language Selection button** checkbox.

NOTE: Depending on the device you are configuring, perform step 2 *or* step 3. To display a list of devices that support the settings, hold the cursor over the **Home Screen Language Selection** title bar above the settings.

2. To specify the alternate languages and keyboard layouts, perform the following steps:

   a. Select the alternate language from the list.

   b. Select the default keyboard layout for the language from the corresponding list.

3. To specify the keyboard layouts for all the available languages and any alternate keyboard layouts, perform the following steps:

   a. Select the keyboard layout for each language from the corresponding list.

   b. To enable the alternate keyboard layouts, select the **Display the alternate keyboard button** checkbox.

   NOTE: If you select the **Display the alternate keyboard button** checkbox, you must also select at least one of the available keyboard layouts.

   c. To enable all the available keyboard layouts, select the **All Keyboard Layouts** checkbox.

   -or-

   To enable specific keyboard layouts, clear the **All Keyboard Layouts** checkbox, and then select the checkbox next to each keyboard layout you want to enable.

Home Screen Wallpaper Customization

Use this option to add or remove a wallpaper to the background.

Click **Browse** to select the image file.

Click **Clear Wallpaper** to remove the wallpaper.

- Only image files (.jpeg, .png, .gif, .bmp) can be used as wallpapers.
- The maximum supported size is 800x484 pixels in FutureSmart 4.5.

I/O Timeout to End Print Jobs

This option lets you select the amount of time the device should wait between packets of data on a print job before canceling that job.

To configure this option, select how long the printer waits from the drop-down list.

Inactivity Timeout

Use this option to specify the number of seconds that the device can remain inactive before automatically reverting to the Home screen. This timeout setting applies only when a user accesses a screen other than the Home screen, and then no further action occurs on that screen for the specified number of seconds.

To configure this option, enter the number of seconds in the box. Valid values are from 10 to 300.

Input Auto Continue

This option lets you specify the default action that the printer takes when the specified media size or type is not available. It also lets you specify how long the printer waits before performing the default action. Specifying a default action for the printer to take when the specified media size or type is not available allows the printer to finish printing the current job without user intervention.

To specify the action for the printer if the specified media size or type is not available, select the desired action from the **Input Auto Continue** drop-down list.

Input Auto Continue Timeout

This option lets you specify how long the printer waits before performing the default action when the specified media size or type is not available. Specifying how long the printer should wait before taking the default action when the specified media size or type is not available allows you time to manually correct the issue.

To specify the action for the printer if the specified media size or type is not available, select how long the printer waits from the drop-down box.

Instant Lamp On

Enable this option to keep the scanner lamp warm when the scanner is turned on. Disabling this option saves energy when the scanner is not in use but the scanner lamp turns off after a period of inactivity and will need to warm up before scanning again.

To configure this option, select:

- **Enabled**: the scanner lamp remains warm and ready to scan when not in use, but uses more energy.
- **Disabled**: the scanner lamp saves energy when not in use, and will need to warm up before scanning again.

Invalid Personality Reports

Use this option to determine whether invalid personality reports are enabled or disabled for a product.

To configure this setting, select **Enabled** or **Disabled**.

Jam Recovery

This option allows you to select the default device reprint behavior after a paper jam is cleared on a fax receive, copy, or print job. The settings include:

- **Disabled**: The device will never reprint a page after clearing a paper jam.
- **Enabled**: The device will always reprint a page after clearing a paper jam.
- **Auto**: The device will reprint a page after clearing a paper jam, if the installed memory is greater than 7 MB.

To select the jam recovery behavior, select the desired setting (**Disabled**, **Enabled**, or **Auto**).

Stored Jobs (Delete Temporary Jobs After)

This option lets you specify how long the printer holds a print job that has not printed before automatically deleting the print job.

⚠ CAUTION: Selecting **Never Delete** could cause the printer's hard disk to fill up with print jobs that were held but never released for printing.

Select the timeout value from the **Stored Jobs (Delete Temporary Jobs After)** drop-down list.

Stored Jobs (Allow on this device)

This option lets you enable and disable the job retention feature. The Stored Jobs (Allow on this device) feature is available on some printers that have mass storage capability. This allows you to store print jobs in the flash memory on a printer. The Stored Jobs (Allow on this device) feature allows you to complete the following tasks:

- Store a print job on the printer. You can then call the print job from the printer control panel as needed. This feature is useful for storing forms and other commonly shared documents.
- Store secure private copies to hold a print job until a user releases it by entering a personal identification number. Print one copy of a multiple-copy print job for proofing. The user can then release the remaining copies for printing or cancel them.

⚠ CAUTION: If the Stored Jobs (Allow on this device) feature is disabled, the option appears on the printer driver user interface but does not store the print job on the printer.

Use the following steps to configure this option:

1. To enable the Stored Jobs (Allow on this device) feature, click **Enable**.
2. To disable the Stored Jobs (Allow on this device) feature, click **Disable**. If the Stored Jobs (Allow on this device) feature is disabled, the option appears on the printer driver user interface but does not store the print job on the printer.

Stored Jobs (Temporary Storage Limit)

This option lets you specify how many jobs can be stored on the printer hard disk at the same time.

Key Press Sound

Use this option to specify whether or not the printer emits a sound when a key is pressed in its control panel.

To configure this option, select **On** or **Off**.

Keyboard Layout

Use this feature to set the keyboard layout on your device's control panel to your language.

To use this option, select your language.

Manage Stapler/Stacker

Use this option to specify the default Staple, Job Offset and Hole Punch placement for print jobs.

This setting is only available if a stapler is attached to the device.

Manually Feed Prompt

Use this feature to specify whether **Manual Feed Prompt** will be displayed always, or only if the tray is not loaded.

If you select **Always** (default), the system always generates a prompt before pulling from the multipurpose tray.

If you select **Unless loaded**, the system generates the prompt only if the multipurpose tray is empty or if it is configured for a different type or size.

Media Administration

This option allows you to enable or disable the media types that the printer uses. You can also define your own media types.

Use the following steps to configure this option:

1. To enable a media type, select the check box next to the media type.
2. To disable a media type, clear the check box next to the media type.
3. To define a new media type, type the media name in **Media Types**. Select the check box next to the media type to activate it.

Online Solutions

The Online Solutions feature provides access to cloud-based solution pages for device events, such as paper jams. When the Online Solutions feature is enabled on a device, the following options are available for device events:

- QR codes can be displayed on the device control panel.
- Web links can be displayed in the Event Log in the device HP Embedded Web Server (EWS).

When a user scans a QR code with a smartphone or tablet or clicks a web link in the Event Log, the device sends information to the HP Solution Finding Web Service. The HP Solution Finding Web Service identifies the most relevant, up-to-date information or video available for the device event, and then returns the solution to the user.

IMPORTANT: The information that the device sends to HP includes the event details, device model, and product serial number. For more information about HP's privacy practices, review the HP Online Privacy Statement.

Use this option to enable or disable the Online Solutions feature and configure the settings. You can restrict access to the Online Solutions feature to only the device administrator.

Enable and configure the Online Solutions feature

1. Select the **Enable Online Solutions** checkbox.
2. To enable QR codes on the device control panel, select the **Show QR code in control panel event details** checkbox. An information (i) icon is displayed on the control panel for an event. When a user presses the information (i) icon, the QR code for that event is displayed on the control panel.

   -or-

   To disable QR codes on the device control panel, clear the **Show QR code in control panel event details** checkbox.
3. To enable web links for event codes in the Event Log, select the **Show links in the EWS Event Log** checkbox.

   -or-

   To disable web links for event codes in the Event Log, clear the **Show links in the EWS Event Log** checkbox.
4. To allow only users who are signed in as an administrator to see the QR codes and Event Log links, select the **Restrict Online Solutions to Administrator** checkbox.

   NOTE: This setting does not prevent users who are not signed in as an administrator from viewing the Event Log. This setting only prevents these users from seeing the web links in the Event Log.

   -or-

   To allow all users to see the QR codes and Event Log links and view solutions from a smartphone or tablet, clear the **Restrict Online Solutions to Administrator** checkbox.

Disable the Online Solutions feature

▲ Clear the **Enable Online Solutions** checkbox.

Optimum Speed/Cost

This option optimizes the performance or cost per page depending on the expected color content of typical print jobs. You can choose whether print quality is more important or whether speed of the print job is more important.

To specify the optimum speed or cost per page, select one of the options (**Auto**, **Speed**, or **Cost Per Page**).

Optimum Speed/Energy Usage

Use this option to configure the optimum speed and energy usage for the device. This setting controls the fuser cooling behavior on the device.

To configure this option, select one of the following options from the list:

- **Faster First Page**: Power to the fuser is not turned off between jobs. This option has no impact on the first page out time.
- **Save Energy**: Power to the fuser is turned off after the device has been idle for 55 minutes. This option has a minimal impact on the first page out time because it affects only the first print job the device sends after it has been idle for 55 minutes or longer.
- **Save Most Energy**: Power to the fuser is turned off after each job. This option has the most impact on the first page out time because it affects every print job the device sends, regardless of how long the device has been idle.

Order Supplies % Level

Use this option to configure the low threshold for supplies.

To set this option, type the desired value in the text box (0-100).

Original Orientation

This option lets you specify the default orientation of the information on the printed page. This is useful if the people who use the printer typically print with a specific orientation. For example, if the printer is dedicated to the accounting department and those users typically print spreadsheets with many columns, set the default orientation to Landscape to show as many columns as possible on one page.

NOTE: The orientation setting that you select when printing a job overrides the setting specified here.

Use the following steps to configure this option:

1. To print across the narrow side of the media, select **Portrait**.
2. To print across the wide side of the media, select **Landscape**.

Outgoing Servers

Use this option to configure the SMTP servers that the device uses to send outgoing emails for the following functions:

NOTE: The functions that are available vary depending on the device.

- **Email**
- **Internet Fax**
- **Alerts**
- **AutoSend**

Use the following steps to configure this option:

NOTE: Some devices do not support all of the following configuration options.

1. If you are configuring multiple devices, select one of the following options in the **Overwrite options** section:

- **Replace/overwrite existing lists**: Any existing SMTP servers on the device are replaced with the lists shown here. Any existing servers that are not defined here are deleted.
- **Append to existing lists**:

  If **Overwrite any existing items with the same name** is not selected, existing servers on the device are not changed. Any servers defined here are added to the device, unless a server already exists with the same name for the same function.

  If **Overwrite any existing items with the same name** is selected, existing servers on the device are not changed, unless a server is defined here with the same name. Any servers defined here are added to the device, and if the name matches an existing server for a particular function, its values is changed to those defined here.

2. To add an SMTP server, perform the following steps:

   a. Click the **Add** button.

   b. On the **Add Server** window, enter the hostname or IP address of the SMTP server in the **Server name or address** box. The SMTP server name must be unique.

   -or-

   To search for the available SMTP servers, click the **Find Servers** button. On the **Find Servers** window, select the SMTP server from the list, and then click the **OK** button.

   NOTE: The **Find Servers** button is available only if you are configuring a single device.

   c. In the **Port number** box, enter the port number. The default is port 25.

   d. From the **Split emails if larger than** list, select the maximum size for emails. The device splits multiple-page scanned documents that are larger than this value into multiple emails based on the page boundaries.

   e. To enable SMTP server authentication, select the **Server requires authentication** checkbox, and then select one of the following options:

   - **Use credentials of user after sign in at control panel**: The device uses the credentials of the user who is signed in on the device to access the SMTP server.
   - **Use credentials defined below**: The device uses the specified credentials to access the SMTP server. Enter the credentials in the **User name** (maximum of 128 characters) and **Password** (maximum of 128 characters) boxes.

     The User name text box can use static data or custom variables supported in the following formats:

     – Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

     %%<custom variable>%% (where “<custom variable>” is the name of the user defined field)

     Example: `%%var_UserName%%`

     – Variable data along with a combination of static content before or after the variable

     <static value>%%<custom variable>%%<static value>

     Example: `Sales%%var_UserName%%`

     Example: `Sales%%var_UserName%%@MyCompany.com`

TIP: By starting the variable data name with var_, it's easier to find and identify user defined fields in HP Web Jetadmin.

TIP: In HP Web Jetadmin, text boxes that support variable data are highlighted blue. For more information on variable data, see Create and Use Variable Data on page 183.

f. To test the SMTP server and credentials, enter an email address in the **Send test email to** box, and then click the **Test Server** button.

NOTE: The **Test Server** button is available only if you are configuring a single device.

g. In the **Server usage** section, select the checkboxes for the functions that use this SMTP server.

3. To edit an SMTP server, select the SMTP server from the list, and then click the **Edit** button. On the **Edit Server** window, edit the settings, and then click the **OK** button.

4. To delete a single SMTP server from all of the functions, select the SMTP server from the list, and then click the **Remove** button. On the **Confirm Remove** window, click the **OK** button.

5. To delete all of the SMTP servers from all of the functions, click the **Remove All** button. On the **Confirm Remove** window, click the **OK** button.

6. To change the order of the SMTP servers for a function, select the SMTP server from the list, and then click the up and down arrows to the right of the function. The device contacts the SMTP servers in the order in which they are listed.

Output Auto Continue

This option allows you to control the behavior of the device if a print job is submitted which lets you specify a paper tray and/or paper size which does not match the current device configuration. This allows the printer to behave in a consistent manner in case of a conflict between the print job specification and the printer configuration.

Use the following steps to configure this option:

NOTE: The options available are dependent upon the device.

1. **Output overflow command**: Specifies the default action to take when the output bin is full or when the stapler is empty.

2. **Output auto continue timeout**: Specifies how long before the device should wait before taking the action specified in the output overflow command.

3. **Output overflow bin**: Specifies what bin should be used if the primary bin is full.

Override A4/Letter

Use this option to print on letter-size paper when an A4 job is sent but no A4-size paper is loaded in the device, or to print on A4 paper when a letter-size job is sent but no letter-size paper is loaded).

To enable this option, select **Yes** and then click **Configure**.

OXPd Accessory Records

Use this option to add, delete, and list the OXPd accessory records on the device. Accessory records are either shared or owned. A shared accessory record describes an accessory that multiple web applications can use and contains a product ID, vendor ID, and serial number. An owned accessory record describes an accessory that only a single web application can use and contains the same fields as a shared accessory record as well as a callback URI, server context ID, optional network credential, connection timeout, and response timeout.

Use the following steps to configure this option:

1. If you are configuring this option for multiple devices at the same time, select one of the following overwrite options:
   - **Replace/overwrite existing OXPd accessory record**
   - **Append to existing OXPd accessory record**
   - **Remove OXPd accessory record**
2. To add OXPd accessory records to the device, click **Add**. The **Add OXPd Accessory Record** dialog is displayed listing all of the OXPd accessory records in the **OXPd Accessory Record Repository**. Highlight the OXPd accessory records you want to add, and then click **OK**.

   To manage the list of OXPd accessory records, click **Edit**. The **OXPd Accessory Record Repository** dialog is displayed. You can import, delete, and edit OXPd accessory records.
3. To delete OXPd accessory records from the device, highlight the OXPd accessory records, and then click **Remove**. The OXPd accessory records are deleted from the list of OXPd accessory records on the device.

NOTE: When you delete OXPd accessory records from the device, the OXPd accessory records remain in the HP Web Jetadmin **OXPd Accessory Record Repository**. To import, delete, and view OXPd accessory records, go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Accessory Records**.

NOTE: Server context ID, URI, User name, Vendor ID, and Product ID are custom variable data fields that support data in the following formats.

- Actual value to be configured
- Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

  %%<custom variable>%% (where “<custom variable>” is the name of the user defined field)
- Variable data along with a combination of static content before or after the variable

  <static value>%%<custom variable>%%<static value>

For more information on variable data, see Create and Use Variable Data on page 183.

OXPd Authentication Agents

OXPd authentication agent files contain the information that OXPd-enabled devices require to contact OXPd authentication servers and authenticate users who sign in on the device. For more information about OXPd authentication agents, see Manage the OXPd Authentication Agent Repository on page 70.

Use this option to manage the OXPd authentication agents that are stored on the device.

Add OXPd authentication agents on the device

1. If you are configuring multiple devices, select one of the following options:

- **Replace/overwrite existing OXPd authentication agents**: Replaces the existing OXPd authentication agents on the devices with the OXPd authentication agents on this list.
- **Append to existing OXPd authentication agents**: Adds the OXPd authentication agents on this list to the existing OXPd authentication agents on the devices.

2. Click the **Add** button. The **Add OXPd Authentication Agent Record** window opens with a list of the OXPd authentication agents that are in the repository.
3. To manage the OXPd authentication agents, click the **Edit** button. The **Options** window opens with the **OXPd Authentication Agents Repository** option selected. You can import, edit, and delete the OXPd authentication agents in the repository.
4. Select the OXPd authentication agents, and then click the **OK** button.

Delete OXPd authentication agents from the device

1. If you are configuring multiple devices, select the **Remove OXPd authentication agents** option.
2. Select the OXPd authentication agents, and then click the **Remove** button.

NOTE: Server context ID, URI, and User name are custom variable data fields that support data in the following formats.

- Actual value to be configured
- Variable data (a variable always starts and ends with %% with the name of the variable in between the starting and ending %% signs)

  %%<custom variable>%% (where “<custom variable>” is the name of the user defined field)
- Variable data along with a combination of static content before or after the variable

  <static value>%%<custom variable>%%<static value>

For more information on variable data, see Create and Use Variable Data on page 183.

OXPd Authorization Proxy Configuration

OXPd authorization proxy files contain the information that OXPd-enabled devices require to access OXPd authorization agents from third-party solutions. For more information about OXPd authorization proxies, see Manage the OXPd Authorization Proxy Configuration Repository on page 72.

Use this option to manage the OXPd authorization proxy that is stored on the device.

Add or replace an OXPd authorization proxy on the device

1. Select the **Add/replace OXPd authorization proxy configuration** option.
2. To add an OXPd authorization proxy, click the **Add** button.

   -or-

   To replace the existing OXPd authorization proxy, click the **Replace** button.

   The **Add OXPd Authorization Proxy Configuration** window opens with a list of the OXPd authorization proxy files that are in the repository.

3. To manage the OXPd authorization proxy files in the repository, click the **Edit** button. The **Options** window opens with the **OXPd Authorization Proxy Configuration Repository** option selected. You can import, edit, and delete the OXPd authorization proxy files in the repository.

4. Select the OXPd authorization proxy file, and then click the **OK** button.

Delete an OXPd authorization proxy from the device

▲ Select the **Remove OXPd authorization proxy configuration** option.

OXPd Device Functions

Use this option to add, delete, and list the OXPd device functions for a third-party device. An OXPd device function definition consists of a title list, description list, icon list, guide, requested button position, and browser target. The browser target consists of a URI, optional credentials, and optional initial post query form.

Use the following steps to configure this option:

1. If you are configuring this option for multiple devices at the same time, select one of the following overwrite options:

   - **Replace/overwrite existing OXPd device functions**
   - **Append to existing OXPd device functions**
   - **Remove OXPd device functions**

2. To add OXPd device functions to the device, click **Add**. The **Add OXPd Device Functions** dialog is displayed. Select the OXPd device functions you want to add, and then click **OK**.

   To manage the list of OXPd device functions, click **Edit**. The **OXPd Device Function Repository** dialog is displayed. You can import, edit, and delete OXPd device functions.

3. To delete OXPd device functions from the device, highlight the OXPd device functions, and then click **Remove**. The OXPd device functions are deleted from the list of OXPd device functions on the device.

NOTE: When you delete OXPd device functions from the device, the OXPd device functions remain in the HP Web Jetadmin **OXPd Device Function Repository**. To import, delete, and view OXPd device functions, go to **Tools** > **Options** > **Device Management** > **Configuration** > **OXPd Device Functions**.

NOTE: Server context ID, URI, and User name are custom variable data fields that support data in the following formats.

- Actual value to be configured
- Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

  %%<custom variable>%% (where “<custom variable>” is the name of the user defined field)

- Variable data along with a combination of static content before or after the variable

  <static value>%%<custom variable>%%<static value>

For more information on variable data, see Create and Use Variable Data on page 183.

OXPd Enabled

Use this option to enable OXPd.

To set this option, select **Enabled** or **Disabled**.

OXPd OPS Config Settings

Some devices have a limited amount of internal storage. For these devices, you can store OXPd services data on an external OXPd Pro Server (OPS) instead of the device's internal storage. The OXPd-enabled firmware in the device does not store OXPd services data. Before you can perform any OXPd services operations on the device, you must use this option to configure the OXPd Pro Server.

To configure the OPS information on the device, perform the following steps. After these steps are complete, the device firmware stores the OXPd services data on the OXPd Pro Server.

NOTE: The CA certificate for the OXPd Pro Server must be imported to the device before you can configure the OPS information on the device.

1. In the **URI** box, enter the URL for the OXPd Pro Server.
2. Select the **Use credentials** checkbox.
3. In the **Username** box, enter the user name that is required to access the OXPd Pro Server.
4. In the **Password** box, enter the password that is required to access the OXPd Pro Server.
5. In the **Confirm Password** box, enter the password again.

To remove the OPS information from the device, perform the following steps:

1. Select the **Use Credentials** checkbox.
2. Select the **Remove** checkbox.
3. In the **Password** box, enter the password that is required to access the OXPd Pro Server.
4. In the **Confirm Password** box, enter the password again.

OXPd Quota Agents

A quota solution, such as Pcounter for HP, is installed on a server and used to specify the amount of various device resources that each user is allowed to use. These device resources include the number of sheets of paper printed, the amount of toner used, and so on. The following are examples of how quotas can be defined:

- Quotas can be based on time. The quota balance can be automatically reset on a recurring basis, such as each week or once a month.
- Quotas can be based on a credit or debit amount. Users can pay into their quota account by using a payment product, such as a web-based pay-for-print application or a debit/credit card machine attached to the device.

An OXPd quota agent record contains the information that devices require to access the server where the quota solution is installed. An OXPd quota agent record can also define web resources that are displayed when users initiate a job on the device, such as a request for credentials, and when a quota limit is reached, such as a warning message.

Use this option to manage the OXPd quota agent records that are stored on the device.

Add OXPd quota agent records on the device

1. Click the **Add** button. The **Add OXPd Quota Agent Record** window opens with a list of the OXPd quota agent records that are available in the repository.

   TIP: To manage the list of OXPd quota agent records, click the **Edit** button. The **Options** window opens with the **OXPd Quota Agents** option selected. For more information, see Manage the OXPd Quota Record Repository on page 76.

2. Select the OXPd quota agent records from the list, and then click the **OK** button.

Delete OXPd quota agent records from the device

▲ Select the OXPd quota agent records from the list, and then click the **Remove** button.

OXPd Statistics Agents

Devices collect statistics about each job that they process. The job statistics include the device ID, job ID, user who initiated the job, and details about the job.

A statistics agent is a server-based solution that receives job statistics from devices. When a job is completed, the device sends the job statistics to the statistics agent. The statistics agent sends an acknowledgement to the device when the job statistics are received.

An OXPd statistics agent record defines the information that devices require to send job statistics to the server where the statistics agent is installed. An OXPd statistics agent record also defines when the device sends job statistics to the OXPd statistics agent server and whether the device automatically deletes the oldest job statistics when the storage media on the device is full. The OXPd statistics agent record must be registered on every device that sends job statistics to the specified OXPd statistics agent server.

Use this option to manage the OXPd statistics agent records that are stored on the device.

Add OXPd statistics agent records on the device

1. If you are configuring multiple devices, select one of the following options in the **Overwrite options** section:
   - **Replace/overwrite existing OXPd statistics agents**—Replaces the existing OXPd statistics agent records on the devices with the OXPd statistics agent records on this list.
   - **Append to existing OXPd statistics agents**—Adds the OXPd statistics agent records on this list to the existing OXPd statistics agent records on the devices.
2. Click the **Add** button. The **Add OXPd Statistics Agent Record** window opens with a list of the OXPd statistics agent records that are in the repository.

   TIP: To manage the list of OXPd statistics agent records, click the **Edit** button. The **Options** window opens with the **OXPd Statistics Agents** option selected. For more information, see Manage the OXPd Statistics Agents Repository on page 74.

3. Select the OXPd statistics agent records from the list, and then click the **OK** button.

Remove OXPd statistics agent records from the device

1. If you are configuring multiple devices, select the **Remove OXPd statistics agents** option.
2. Select the OXPd Statistics agent records from the list, and then click the **Remove** button.

Paper Tray Assignments

This option lets you assign media sizes and types to input trays. You can also see how much media is in each tray.

To configure this option, select the media size from the Size drop-down box for the default and for each tray.

PCL Form Length

Use this option to set the PCL form length on the device. You can specify 5 to 128 lines of text per page.

The device uses the PCL form length to set the spacing between lines. When the paper size is changed, the device automatically recalculates the form length based on the Vertical Motion Index (VMI).

PJL Configuration

This option lets you configure the ability to print PJL files. You can also add them to a configuration template or schedule them to print at a different time.

Use the following steps to configure this option:

1. Select the desired file from the displayed list.
2. To add a new file to the list, click **New**. The **PJL Repository** configuration page is displayed showing current files in the repository.

NOTE: This page is also accessible from **Tools** > **Options** > **Device Management** > **Configuration** > **PJL Repository**. For more information about the **PJL Repository** configuration option, see Manage the PJL Repository on page 69.

Power On Calibration

Use this option to help determine when a power on calibration occurs. Applications can use this object to control when calibrations are performed.

- **On**: Calibration occurs immediately following boot.
- **Off**: Calibration never occurs.
- **Delayed**: Calibration never occurs; for the delay interval. Setting this option to **Delayed** controls when a calibration occurs in relation to a power on event.

To configure this setting, select **Off**, **On**, or **Delayed**.

Print PDF Errors

You can choose to have a PDF error page print, which shows the error encountered and the stack at the time of the error. This is useful for debugging.

To configure this option, select **On** to print an error page or **Off** to not print an error page.

Print PS Errors

You can choose to have a PostScript error page print, which shows the error encountered and the stack at the time of the error. This is useful for debugging.

To configure this option, select **On** to print an error page or **Off** to not print an error page.

Printer Wakeup

Use this option to send a notification to the device that takes the device out of Sleep mode. When you enable this option and click **Apply**, the notification is sent immediately.

PS Defer Media

If the device uses non-HP PostScript drivers instead of HP drivers to print jobs, use this option to enable or disable the HP paper-handling model. Non-HP PostScript drivers do not recognize all the tray configurations and either print from a non-specified tray or do not print at all. The HP paper-handling model always prints jobs.

If the **Enabled** option is selected, non-HP PostScript drivers use the HP tray-selection method. This is the default.

If the **Disabled** option is selected, non-HP PostScript drivers use the non-HP PostScript tray-selection method.

Quick Sets

Quick Sets are shortcut jobs with predefined settings that help users complete their jobs quickly and reliably. Users can access Quick Sets on the device control panel from the Home screen or the Quick Sets application.

Use this option to create Quick Sets for Copy, Email, Fax, Save to Network/FTP Folder, Save to USB, and Save to SharePoint® jobs. Quick Sets are saved as unique jobs and do not impact the defaults that are set for the device.

Use the following steps to configure this option:

1. If you are configuring multiple devices or creating a device configuration template, select one of the following options:

   - **Replace/overwrite existing lists**: Replaces any existing Quick Sets on the device with the Quick Sets that are defined here. Any existing Quick Sets on the device that are not defined here are deleted.

   - **Append to existing lists**: Adds the Quick Sets that are defined here to the Quick Sets on the device. A Quick Set is added to the device only if a Quick Set that has the same name and type does not already exist on the device.

     – If the **Overwrite any existing items with the same name** checkbox is selected, an existing Quick Set on the device that has the same name and type as a Quick Set that is defined here is overwritten with the settings that are defined here.

     – If the **Overwrite any existing items with the same name** checkbox is not selected, an existing Quick Set on the device that has the same name and type as a Quick Set that is defined here is not changed.

2. To add a Quick Set, click the **Add** button. The **Add Quick Set** wizard starts.

   a. On the **Specify Quick Set type** page, select the type of Quick Set to create, and then click the **Next** button. The types of Quick Sets that are available vary depending on the device.

NOTE: You can create a Quick Set if the base application, such as Email or Save to Network/FTP Folder, is disabled. However, the Quick Set will not work or appear on the device control panel until the base application is enabled.

b. On the **Specify Quick Set options** page, specify the following settings, and then click the **Next** button:

- **Quick Set title**: Enter a name for the Quick Set. The name can be a maximum of 30 characters and can include any Unicode characters.
- **Button location**: Select the location where the button for the Quick Set appears.
- **Quick Set description**: Enter a description of the Quick Set. The description can be a maximum of 90 characters and can include any Unicode characters.
- **Quick Set start option**: Select the option that specifies how the user starts the Quick Set job.
- **Original sides prompt**: Select the option that specifies whether the Quick Set job uses the setting for original sides that is defined in the application or the user is prompted to specify whether the originals are one-sided or two-sided.

c. On the **Specify Settings** page, specify the appropriate settings for the Quick Set, and then click the **Next** button. The settings on the page vary depending on the device and Quick Set type.

- **Copy**: Specify the settings for the copy job.
- **Email**: Specify the email settings and specify whether users can edit each field on the device control panel. If any of the settings require that users sign in, go to the **Security** tab in the HP Embedded Web server (EWS) on the device, and then configure the base application to require signing in.

  To specify multiple email addresses for any of the fields, separate each address with a semicolon (;) or a comma (,).

  This text box can use static data or custom variables supported in the following formats:

  – Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

    %%<custom variable>%% (where “<custom variable>” is the name of the user defined field)

    Example: `%%var_EmailName%%`

  – Variable data along with a combination of static content before or after the variable

    <static value>%%<custom variable>%%<static value>

    Example: `Sales.%%var_EmailName%%`

    Example: `Sales.%%var_EmailName%%@MyCompany`

  TIP: By starting the variable data name with var_, it’s easier to find and identify user defined fields in HP Web Jetadmin.

  TIP: In HP Web Jetadmin, text boxes that support variable data are highlighted blue. For more information on variable data, see Create and Use Variable Data on page 183.

- **Fax**: Enter one or more fax numbers for the recipients of the fax job. If no fax recipients are specified, the user must enter the fax number on the device control panel.
- **Save to Network/FTP Folder**: In the **Network folder type** section, enter the path to the folder where the job is saved. The path for a standard shared folder is a simple UNC path without any variables. The path for a personal shared folder, such as the user's Home folder, is defined in

Microsoft Active Directory. To save a file to a user's personal shared folder, the user must sign in at the device and the device must be able to retrieve the information for the user's Home folder.

In the **Folder Access Settings** section, select the option that specifies the type of read and write access that must be defined for the folder where the job is stored. To verify the folder access before the job starts, select the **Verify folder access prior to job start** checkbox.

- **Save To USB**: Specify the default location where the job is saved on a USB flash drive that is inserted into the easy-access USB port on the device. Files can be saved at the root directory or in a specified folder on the USB flash drive.

  The folder path can be a maximum of 1,024 characters. Use a forward slash (/) to separate folder and subfolder names.

- **Save to SharePoint®**: Specify the path of the SharePoint site where the job is saved. To verify the access credentials for the SharePoint before the job starts, select the **Verify folder access prior to job start** checkbox.

  The path for a standard SharePoint site is a simple path without any variables. The path for a personal SharePoint site, such as a user's Home SharePoint site, is defined in Microsoft Active Directory. To save a file to a personal SharePoint site, the user must sign in at the device and the device must be able to retrieve the information for the user's Home SharePoint site.

  The SharePoint Path text box can use static data or custom variables supported in the following formats:

  – Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

    %%<custom variable>%% (where "<custom variable>" is the name of the user defined field)

    Example: `%%var_SharePointSite%%`

  – Variable data along with a combination of static content before or after the variable

    <static value>%%<custom variable>%%<static value>

    Example: `https://%%var_SharePointSite%%`

    Example: `https://%%var_SharePointSite%%Sales`

TIP: By starting the variable data name with var_, it's easier to find and identify user defined fields in HP Web Jetadmin.

TIP: In HP Web Jetadmin, text boxes that support variable data are highlighted blue. For more information on variable data, see Create and Use Variable Data on page 183.

d. On the **Specify Quick Set job settings** page, specify the default scan and file settings that are used for this Quick Set job, and then click the **Next** button. The settings that are available on this page vary depending on the device and Quick Set type.

e. On the **Confirm** page, verify that the information is correct, and then click the **Finish** button.

3. To edit a Quick Set, select the Quick Set from the list, and then click the **Edit** button. The **Edit Quick Set** wizard starts. The pages in the wizard vary depending on the Quick Set type. The settings on the pages are the same as the settings that are described for the **Add Quick Set** wizard in step 2.

4. To copy the settings of an existing Quick Set to a new Quick Set, select the Quick Set from the list, and then click the **Copy** button. The **Edit Quick Set** wizard starts. Enter a name for the new Quick Set, and then change the settings as required. The settings on the pages are the same as the settings that are described for the **Add Quick Set** wizard in step 2.

5. To delete a Quick Set, select the Quick Set from the list, and then click the **Remove** button. On the **Confirm Remove** window, click the **OK** button.

6. To change Quick Set order, select the Quick Set from the list, and then click the **Move Up** or **Move Down** buttons.

Quiet Mode

This option provides a quieter printing experience by slowing the printer down for office printing or increasing the speed to the full speed for large jobs. You can select the value as **On**, **Off**, **Auto Transition**. **Auto Transition** allows you to set a predetermined job size of 10 to 999 pages, and print jobs will print in the **Quiet Mode** for all print jobs up to the user's predetermined page size. Jobs that have pages above the predetermined size will print at the full speed.

To configure **Quiet Mode**, select **On**. If desired, specify the job size (10–999) in **Auto Transition**.

Replace Supplies

Use this option to specify the behavior of the device when a supply becomes low or is out.

NOTE: The **Override at Out** option is available only from the device control panel. If this option is selected, the device continues to print when the supply is out. HP Web Jetadmin displays this option only if it is selected on the device.

Use the following steps to configure this option:

NOTE: The following options are not available for all devices.

1. To stop printing when a supply becomes low, select the **Stop at Low** option.

2. To stop printing when a supply is out, select the **Stop at Very Low** option.

3. To allow the device to continue printing when a supply is out, select the **Stop At Maxlife** option. This option is available only for monochrome devices.

4. To stop printing and display a prompt when a supply is out, select the **Prompt to Continue** option.

5. To stop printing when a specific threshold is reached, select the **Stop after Very Low by** option, and then enter the number of pages that the device prints before stopping in the box.

Resolution

This option lets you select the default resolution for print jobs that do not specify a resolution. This allows the printer to behave in a consistent manner for print jobs which do not specify a resolution.

To configure this option, select the desired default resolution.

Resolution Enhancement

REt (Resolution Enhancement Technology) is a process that you can turn on and off. Turning on REt will sharpen the resolution but slow down printing. If the resolution selected is 1200 dpi, then REt will not be used regardless of this setting. This setting is not in effect when the resolution used is 1200 dpi.

Select whether to turn REt on or off.

Restore Modes

Use this option to restore all fuser modes to their default or factory settings.

To restore all fuser modes to their default or factory settings, select **Restore Modes**.

Rotate Offset

Use this to enable or disable **Rotate Offset**, which allows you to print multiple copies of a job in alternate orientations.

To set this option, select **Enable** or **Disable**.

Show Date and Time

Use this option to enable the printer to hide or display the date and time on the device control panel.

To show or hide the date and time, select **Hide** or **Display**.

Show Network Address

Use this option to enable the printer to display the **IP Address** or the **Network Address** button on its control panel (which button is displayed depends on the device). Enabling this feature makes it easier to see the device's IP address.

Use the following steps to configure this option:

1. To make the printer show the **Network address** button in the initial page of its control panel, select **Display**.
2. To make the printer hide its **Network address** button, select **Hide**.

Show Stop Button

Use this option to enable or disable the Show Stop Button in the control panel.

To enable the Show Stop Button, select the **Enabled** option.

-or-

To disable the Show Stop Button, select the **Disabled** option.

Click the **Apply** button.

Show Welcome Message

Use this option to specify a welcome message that is displayed on the device control panel. Users must read the welcome message, and then touch the OK button to continue.

Use the following steps to configure the welcome message:

1. Select the **Show Welcome Message** checkbox.
2. In the **Title** box, enter a title that displays in the banner of the welcome message (maximum of 40 characters).
3. In the **Text** box, enter the text for the welcome message (maximum of 1,500 characters).
4. From the **Border Color** list, select the color that is used for the border of the welcome message.

Size/Type Prompt

This option lets you specify what the control panel displays when a paper tray is opened and closed. Configure it to display or not display the message **To change size or type press check** on the control panel. In either case, HP Web Jetadmin displays a **Tray empty** message on the device's **Status** page.

Use the following steps to configure this option:

1. To turn on the display message, select **Display**.
2. To turn off the display message, select **Do Not Display**.

Sleep/Wake Time

This option specifies the time of day that you want the printer to automatically start waking (or warming) up and also sleeping.

You can save energy when the device is not in use for the time specified in **Sleep delay**. After **Sleep delay** is applied, **Sleep mode** is automatically enabled. It might take some time for the device to return to a **Ready** state once it is in **Sleep mode**. **Wake time** can only be set if the **Sleep delay** time is set.

Setting a **Wake time** is useful to ensure the device is ready at a certain time and not in **Sleep mode**. For example, to make sure the device is ready at 7:45, set the **Wake time** for 7:30, then set a **Sleep delay** of 30 minutes or longer so people have time to use the device before it re-enters **Sleep Mode**. **Wake time** can only be set if the **Sleep delay** time is enabled.

Some devices also support **Sleep time**. Use **Sleep time** to ensure the device enters **Power save mode** at the specified time, such as the end of the work day. **Sleep time** can only be set if you have enabled **Sleep delay**.

NOTE: Make sure you coordinate the **Wake time** with both **Sleep delay** and **Sleep time**.

To set this configuration option, select the desired settings from the lists displayed.

Sleep Delay (Minutes)

Use this option to specify the number of minutes the device must be idle before it automatically enters Sleep Mode. This option is useful for reducing the average power consumption when the device is not used often.

To configure this option, enter the number of minutes to delay in the text box.

Sleep Delay Time

This option, also referred to as **Power Save**, lets you specify how long the printer can be idle before automatically powering off. **Sleep Delay** mode reduces the printer average power consumption after it has been idle for a specific length of time. This is useful if the printer is not used often.

NOTE: If the printer has an MFP (scanner unit) installed, such as the HP Color LaserJet 8500 or the HP Color LaserJet 8550, the **Power Save Timeout** setting specified on the printer control panel might override the setting specified on this page.

To set the **Sleep Delay**, select the timeout value from the drop-down list.

Sleep Mode

Use this option to specify how the printer goes into sleep mode, and then how it warms up again.

Use the following steps to configure this option:

1. To disable **Sleep mode**, select **Off**. Disabling **Sleep mode** is not recommended, since energy saving procedures will no longer be running.

2. To set **Sleep mode**, select the desired value from the **Sleep mode** drop-down list.

3. To set **Sleep delay**, select the desired value from the **Sleep delay** drop-down list.

   Setting a **Sleep delay** is the most common set to put the printer into sleep mode, after a specific amount of idle time.

4. To set the **Sleep schedule**, it must first be selected from the **Sleep mode** drop-down list. Then select the corresponding checkbox for the **Wake time** and **Sleep time** for each **Weekday**. Select the corresponding time from the available fields.

   Setting a **Sleep schedule** is useful for ensuring that HP Web Jetadmin is **Ready** at a certain time and not in **Sleep mode**.

   For example, to make sure HP Web Jetadmin is **Ready** at 7:45, set the **Wake time** for 7:30 and then set a **Sleep delay** of 30 minutes or longer so people have time to use the product before it re-enters **Sleep mode**.

5. To set the **Maximize energy savings**, select it from the **Sleep mode** drop-down list.

   Selecting **Maximize energy savings** will let the printer itself determine which are the best sleep options to be set.

6. To set the **Custom energy savings**, select it from the **Sleep mode** drop-down list. To use **Custom energy savings**, select **Custom energy savings** and then select the desired values for **Sleep delay**. Select **Enable** for **Wake time** and **Sleep time** for each **Weekday**. Then select the corresponding time from the available fields.

   If multiple and concurrent sets are made, the **Custom energy savings** option will be automatically selected. If awakened during a set **Sleep schedule**, the device will return to **Sleep** after the **Sleep Delay** setting or 15 minutes of inactivity occurs, whichever is less time.

Sleep Schedule

Use this option to specify the time of day you want the device to automatically wake up (or warm up) and enter sleep mode. The wake up time ensures that the device is ready at a specific time each day. The sleep time ensures that the device enters its energy-saving sleep mode when it is not in use, such as in the evenings or on the weekend. You can specify a different sleep schedule for each day of the week. You can also add, edit, and delete sleep schedules for holidays.

To create a weekly sleep schedule, select the checkbox next to the **Wake Time** and **Sleep Time** fields for each day you want to schedule, and then enter the appropriate times.

To create a holiday sleep schedule, perform the following steps:

1. Click **Add**. The **Holiday Schedule - Add** dialog is displayed.
2. Type the name of the holiday in the **Event** field.
3. Enter the date and time you want the device to enter sleep mode in the **Start** field.
4. Enter the date and time you want the device to wake up in the **End** field.
5. Click **OK**.

To edit a holiday sleep schedule, select the schedule from the **Holiday Schedule** list, and then click **Edit**. Change the settings, and then click **OK**.

To delete a holiday sleep schedule, select the schedule from the **Holiday Schedule** list, and then click **Remove**.

Sleep Timer Settings

Use this option to configure the Sleep Mode/Auto Off feature on the device. When this feature is enabled, the device automatically enters Sleep mode or Auto Off mode after a specified period of inactivity and then wakes up when the specified events occur.

⚠ CAUTION: Configuring the **Sleep Timer Settings** configuration option for some devices might cause those devices to enter a deep sleep mode. USB-based solutions that are connected to these devices might be disabled. HP Web Jetadmin does not display a message or provide any indication that the USB-based solutions will be disabled.

To enable the Sleep Mode/Auto Off feature, perform the following steps:

1. Select the **Enable Sleep Mode/Auto Off Timer** checkbox.
2. Enter the number of minutes the device waits with no activity before entering Sleep mode in the **Sleep Mode/Auto off after** field. Valid values are `1` through `120`.
3. To specify which events wake up the device, select one of the following options:
   - **All events**: The device wakes up when any event occurs.
   - **Network port**: The device wakes up only when a network port event occurs.
   - **Power button only**: The device wakes up only when the power button on the device is pressed.

To disable the Sleep Mode/Auto Off feature, clear the **Enable Sleep Mode/Auto Off Timer** checkbox.

Stacker Staple Setting

Use this option to specify the number of staples put on each print job. The stacker staple setting specified in HP Web Jetadmin overrides the setting specified through the printer control panel.

To configure this option, select **No Stapling** or **One Staple**.

Stand by Fuser Mode

Use this option to set the temperature for a Fuser Mode when it is in standby mode. Turning this off means using less energy but warm up time for a print job will take longer.

To set this option, select the temperature from the drop-down box.

Stapler Offset Mode

If an HP 3-bin Stapler/Stacker accessory is installed on the device, use this option to specify whether each print job is offset in the output bin. Offsetting the print jobs makes it easier to separate multiple print jobs.

To disable this option, select the **Off** option.

To enable this option, select the **On** option.

Staples Out Override

Use this option to specify the default action that the printer takes when the output bin is full or when the stapler runs out of staples.

To configure this option, select **Stop** or **Continue**.

1. To send the rest of a job to a different output bin, from **Output Overflow Command**, select **Overflow Job**.
2. Select how long the printer waits from **Output auto continue timeout**.
3. Select the output bin from **Output Overflow Bin**.
4. To continue printing a job without stapling, select **Staples Out Override**.
5. Select how long the printer waits from the drop-down list labeled **Output auto continue timeout**.

Status Page Language

This option lets you specify the device personality (PCL, PostScript, Text, or HP-GL2) that the HP Jetdirect print server uses when it sends a status page to the device. You might need to change the status page language to accommodate a particular printing device. For example, a PostScript printer might not be able to understand the default PCL print page that an HP Jetdirect print server sends.

NOTE: This option only affects the test page output language, not the spooled print job language.

To set the status page language, select one of the status page language options.

Stored Jobs (Sort/List Order)

Use this option to specify the sort order of the stored print jobs on the device. You can sort stored print jobs by the date or the job name.

Supplies Status Messages on Control Panel

This option lets you control whether or not supplies-related status messages will be displayed on the control panel.

To display status messages on the device's control panel, select **Show**. To suppress status messages, select **Do Not Show**.

Suppress Blank Pages

This option lets you specify how the printer responds when a job with blank pages is printed. Allowing the printer to suppress printing blank pages can save you time, toner, and paper.

Use the following steps to configure this option:

1. To allow printing blank pages in a print job, select **No**.
2. To suppress printing blank pages in a print job, select **Yes**.

System Setup

This option lets you configure several settings. See the steps below for more information.

Use the following steps to configure this option:

1. **Clearable Warnings**: Control how the device tracks clearable warnings. If **On** is selected, a warning is displayed until GO is pressed. If **Job** is selected, a warning is displayed until the end of the job in which it was generated.
2. **Show IP Address**: Lets you specify whether the device IP address should be displayed along with the Ready Message.
3. **Tray Behavior**:
   - **Use Requested Tray**: Indicates if the device will automatically try to load media from the next input media tray in the auto-select sequence (defined by each device) when it cannot load media from the current tray.
   - **Manual feed prompt**: Lets you specify whether **Manual Feed Prompt** will be displayed always, or only if the tray is not loaded.
   - **Size/Type prompt**: Lets you specify what the control panel displays when a paper tray is opened and closed. Configure it to display or not display the message **To change size or type press check** on the control panel. In either case, HP Web Jetadmin displays a **Tray empty** message on the Device Status page.
   - **Use another tray**: When set to **Enabled**, this gives the user the ability to select another tray from which paper could be provided for the job. When set to **Disabled**, the user is forced to provide paper through the same tray, after the paper mount message is posted.
4. **Duplex Blank Pages**: Enables or disables smart duplexing.

System Setup Ram Disk

Use this option to turn off RAM Disk functionality or to set it to automatic. If **Auto**, a RAM disk is created whose size is determined by the printer as a percentage of the amount of installed memory.

To configure this option, select **Off** or **Auto**.

Time Zone

Use this option to specify the Greenwich Mean Time (GMT) by selecting the time zone the device is in and specify whether the clock for the device is automatically adjusted for daylight saving time (DST).

Use the following steps to configure this option:

1. Select the time zone for the device from the list.
2. To enable daylight saving time, select the **Automatically adjust clock for daylight saving changes** checkbox.

   NOTE: Some time zones do not support daylight saving time. For these time zones, if the **Automatically adjust clock for daylight saving changes** checkbox is selected, the **Automatically Adjust for DST** column in the device lists always displays **No**.

   -or-

   To disable daylight saving time, clear the **Automatically adjust clock for daylight saving changes** checkbox.

Time Zone/Daylight Saving

Use this option to specify the Greenwich Mean Time (GMT) by indicating which time zone the device is located in and whether the clock on the device is automatically adjusted for daylight saving time. You can also use this option to set the real time clock to the local time on the device. The device uses the real time clock to adjust the weekly timer mode, wake up at a particular time, enable time stamps on email alerts, and record internal event times. This feature provides the maximum flexibility for time configuration and management. When used with the local time on the device, the **Time zone settings** and **Daylight saving settings** options help indicate the GMT time. You can also use this option to specify the date range for daylight saving time, which should match the daylight saving time schedule for the location of the device.

Use the following steps to configure this option:

1. Select the time zone for the device from the **Time zone** drop-down list.
2. To enable the daylight saving setting, select the **Automatically adjust clock for daylight saving time (DST)** checkbox.
3. To specify the start date and end date for daylight saving time, perform the following steps:
   a. Select the appropriate values from the **Occurrence**, **Week Day**, **Month**, and **Hour** drop-down lists.
   b. Enter the number of minutes for the daylight saving time offset in the **DST offset** text box.
4. To use the default start date and end date for daylight saving time, click **Use Defaults**.

Tray 1 Mode / Manual Feed

This option lets you specify:

- **Cassette (Manual Feed Disabled)**: Let the device prioritize by paper size first.
- **First (Manual Feed Enabled)**: Means that the device will always try to use paper from that tray regardless of the media type or size specified.

Select the desired option: **Cassette (Manual Feed Disabled)** or **First (Manual Feed Enabled)**.

Tray Administration

This option lets you assign media sizes and types to input trays.

NOTE: The drop-down list of media types contains all of the media types that are enabled on the **Media Administration** page.

Use the following steps to configure this option:

1. To set the media size and type, select the media size from the **Size** drop-down list next to the tray.
2. Select the media type from the **Type** drop-down list next to the tray.

Tray Setup Media Type

This option lets you select the default paper type to be selected for each tray. The device is capable of using various fuser temperatures for the printing process that are suitable for different types of paper.

To configure this option, choose the desired paper type for each tray from the drop-down list box for that tray. The available options are:

- **Light** (Less than 60 g/m^2), for Transparencies and Thin Paper.
- **Midweight** (60 - 128 g/m^2), for Plain Paper, Plain Envelope, and Postcard.
- **Heavy** (128 - 225 g/m^2), for Bond Paper, Labels, Rough Paper, and Cardstock.
- **Extra Heavy** (More than 225 g/m^2).

Use Another Tray

Use this feature to set the device to use another tray if necessary.

NOTE: This setting may affect the configuration items in the **Digital Sending**, **Fax**, and **Security** categories. It is not recommended to set this option with other configuration items under those categories.

If you select **Enabled** (default), the printer prompts users to use another tray when the selected tray is unavailable.

If you select **Disabled**, the printer does not prompt the user.

Use Requested Tray

Use this feature to specify how the device handles jobs with a specific input tray.

To have the device use another tray when necessary, select **Enabled**.

To not direct the device to use another tray when necessary, select **Disabled**. You will then need to provide paper through the same tray.

Select **Exclusively** (default) to ensure that the printer will not automatically select another tray when you indicate that a specific tray should be used.

Select **First** to allow the printer to pull from a second tray if the specified tray is empty or contains a different media type or size.

Device Configuration Options for Digital Sending

Configuration options for Digital Sending devices define functions for the device including setup and default settings.

Activity Log

This option lets you view the logs for the digital send device. The logs contain digital sending job information and error events associated with the device. You can use this information to check the status of digital send jobs for the device. If there are any errors associated with the jobs, you can also view the specific error messages to begin troubleshooting any issues.

Use the following steps to configure this option:

1. To save the activity log, select **Save log**.

   NOTE: The log is saved when the settings for the digital send device are applied.

2. To clear the activity log, select **Clear log**.

Address Book Management

Use this option to import a predefined list of email addresses (500 maximum) from a comma separated value (CSV) file directly into the internal address book of the digital send device. The address book can store up to 2,000 addresses. Once an address file is imported to the digital send device, the addresses can be searched by alias. The alias can be a name or an email address. To ensure that searches are consistent in the digital send device address book, use the same format for all aliases. For example, type the first name and then the last name.

NOTE: The CSV file must have a header, which is always the first line of that file. If the CSV file does not have a header, the first line of addresses will be considered a header and that address will be lost.

Use the following steps to configure this option:

NOTE: A digital send device can store up to 2000 entries, but only up to 500 entries can be loaded at a time.

NOTE: The CSV file must have a pair of entries for each new address, where the first entry is the name of the person and the second entry is a valid email address. The CSV file also must have a header entry "name, emailaddress". Following is a sample of a CSV file:

```
name, emailaddress

taylor duggan, taylor.duggan@hp.com

kelly jacobson, kelly.jacobson@hp.com
```

1. To import an address file, select **Import address book**. Click **File** to browse to locate the CSV file using a dialog window.
2. To clear the address book on the digital send device, select **Clear device address book**.

Administrator Information

This option lets you specify the contact information for the administrator of the digital send device. In case of a problem with this device, this administrator should be contacted.

Use the following steps to configure this option:

1. Type the name of the person responsible for maintaining the digital sending features of this device in **Name**.
2. Type the email address of the person responsible for maintaining the digital sending features of this device in **Email address**.
3. Type the phone number of the person responsible for maintaining the digital sending features of this device in **Phone number (optional)**.
4. Type the physical location of the person responsible for maintaining the digital sending features of this device in **Location (optional)**.

Advanced Search Options

This option lets you specify the settings the digital send device uses to search the LDAP database for email addresses. LDAP servers with large email address databases can take a long time for the digital send device to search. Specify the most efficient search method for the device to ensure the fastest possible search results.

Use the following steps to configure this option:

1. Select the maximum number of addresses returned from an LDAP search from **Maximum LDAP addresses**.

   NOTE: Smaller values typically result in faster search times, but may not provide the user with all possible matching addresses.

2. Select the maximum amount of time that the digital send device waits for the LDAP search to complete from **Maximum search time**.

   NOTE: Smaller values typically result in faster search times, but may not provide the user with all possible matching addresses.

3. Optional: If the LDAP server supports additional search parameters, type a parameter into **LDAP filter condition**. This parameter must be in the form of a valid LDAP filter.
4. Select how thoroughly the search is performed from the **Find entries in the database**.
   - Select **fast mode** to search for only entries that begin with the search string. This option is faster, but may not return all matching entries.
   - Select **verbose mode** to search for any entries that contain the search string. This option is more thorough, but may take longer to complete.
5. If email entries in the LDAP database are alphabetized, select **Enabled** or **Disabled** from the **Entries in database are alphabetized** drop-down list. The digital send device searches the LDAP database more efficiently if this option is selected.

Clear All Network Folders

Use this configuration item to clear all folder entries from the devices' **Send to Network Folder** settings. This should be done in order to either remove settings or as a first step in modifying folder configuration settings.

NOTE: At this time, **Send to Network Folder**, **Send to Network Folder — MSeries or Later**, and **Network Folder Setup** configuration items can only be used to modify existing settings only on a single device. In order to modify settings on more than one device, the folder settings must be cleared using **Clear all Network Folders** can then be re-established through a second configuration.

Modification of existing folder settings must be performed in steps. It is advised that you use configuration templates to both store and modify device settings.

Following is an example of how both the **Clear all Network Folders** and the **Send to Network Folder — MSeries or Later** can be used together to modify existing settings on a group of devices. You will be able to effectively use this configuration option if you understand this example.

Example:

- Thirty LaserJet M4345 MFP devices have **Send to Network Folder** functionality enabled and also have the following three folders implemented identically.
  - HR: `\\server1\HRFolder`
  - Accounting: `\\server1\AccountingFolder`
  - Public: `\\server3\public\week1`
- Each week the folder `\public\week1` is changed to correspond to the current week in the year. At this time, we need to change the folder to be `\public\week2`.

Steps:

1. Create an HP Web Jetadmin configuration template with these settings:

   NOTE: For more information about configuration templates, see Configuration Templates on page 180.

   - HR: `\\server1\HRFolder`
   - Accounting: `\\server1\AccountingFolder`
   - Public: `\\server3\public\week2`

   This template can also be stored for longer term use; it can be modified each week that the configuration action is needed.

2. Once the configuration template is ready, use **Clear all Network Folders** to remove settings from the 30 devices.

3. After the 30 devices have been cleared of all **Send to Network Folder** settings, apply the template created in Step 1 to all 30 devices.

4. Before you clear settings on a device, it is important that you understand what those settings are for. Clearing the settings and then reapplying new settings may cause other device settings to be lost. Use the HP Web Jetadmin device list column **Digital Sending – Send to Network Folder** to verify that all devices successfully had the folder setting changed. The column detail can either be copied and pasted into an application like Notepad or exported to a CSV file in order to view the folder settings present on each device.

Default Messages Settings

Use this option to specify the From address, subject, and body information that initially appears in all email messages sent from the digital send device. The digital send device uses the email message settings as the initial content text for each email message it generates. You can also restrict the address fields and message body from edits. The initial information provided can serve as a template for the email or provide instructions to the user. For example, you can specify the subject of the email as shown here: "Please type in a subject for your message here". For security reasons, you may not want to allow the user to change the From address provided on the digital send device. You can specify a setting in this section that prevents the user from changing the default From address.

Use the following steps to configure this option:

1. Specify the address field restriction by selecting one of the three options: **Allow users at the device to edit all of the address fields (From, To, CC, BCC)**, **Restrict users from editing the 'From:' address**, or **Restrict users from editing all address fields (From, To, CC, BCC)**.
2. To specify the default sender, type the email address in **Default Email Address**.
3. Type the name you want to appear in the From field of the email in **Default Display Name**.

NOTE: If the display name is not provided, the value entered in **Email Address** text box displays in the From field of the email.

4. Type a subject in **Default Subject**. The subject appears in **Subject** when the user composes an email message on the digital send device.
5. Type a default message in **Default Message**.
6. To prevent users from changing the message text of the email, select **Restrict users at the device from editing the 'Message:' field**.

Default Notification Settings for Email

This option lets you set the device to send a notification whenever an email is sent. You can also specify how and when these notifications should be sent.

Use the following steps to configure this option:

1. Select a value from **Condition on which to notify**:
   - **Never**: never send notices when an email is sent.
   - **Always**: always send notices when an email is sent.
   - **All Errors**: send notices only when there is an error.
2. Select a delivery method from **Method used to deliver notification**:
   - **Email**: send the notifications to the administrator's email address.
   - **Print**: print the notifications.

Default Scan Settings for Email

Use this option to specify the default settings for email attachments that best suits the business needs of your organization.

Use the following steps to configure this option:

1. Type the default file name in **Default File Name**.
2. Select the default file type from **Default File Type**.
3. Select the default color preference from **Default Color Preference**.

4. Select the default resolution from **Default Resolution**.
5. Select the default output quality from **Default Output Quality**.
6. Select the default quality optimization setting from **Optimize Text/Picture**.
7. Select the default original size from **Original Size**.
8. Select the default background cleanup setting from **Background Cleanup**.
9. Select the default original number of sides from **Original Sides**.
10. Select the darkness setting from **Darkness**.
11. Select the default orientation from **Content Orientation**.
12. Select the default sharpness setting from **Sharpness**.
13. Select the default 2-sided format setting from **2-Sided Format**.

    NOTE: This option is only enabled if **2-Sided** is selected from **Original Sides**.

14. Select the default contrast setting from **Contrast**.

Device Contacts Import

Use this option to import a predefined list of email addresses (500 maximum) from a comma separated value (CSV) file directly into the internal address book of the digital send device. The address book can store up to 2,000 addresses. Once an address file is imported to the digital send device, the addresses can be searched by alias. The alias can be a name or an email address. To ensure that searches are consistent in the digital send device address book, use the same format for all aliases. For example, type the first name and then the last name.

To send scanned documents from the digital send device through email, the user must provide an email address. The process of entering email addresses can be simplified by providing an address lookup list and by using an auto-complete feature. Importing addresses into the internal address book of the digital send device allows it to use the lookup list and the auto-complete feature.

Use the following steps to configure this option:

1. To import an address file:
   - To locate the CSV file using a dialog window, click **File**, or
   - Type the path and filename of the CSV file in the text box.
2. To clear the address book on the digital send device, select **Delete All Device Contacts**.

Digital Sending - Accessing the LDAP Server

This option lets you specify how the digital send device accesses the Lightweight Directory Access Protocol (LDAP) server to look up email addresses. To send scanned documents from the digital send device through email, the user must provide an email address. The process of entering email addresses can be simplified by providing an address lookup list and by using an auto-complete feature. Access to the LDAP server email address database provides a way for the digital send device to use the lookup list and the auto-complete feature.

Use the following steps to configure this option:

1. Select one of the following server bind methods from **LDAP server bind method**:

   NOTE: All options might not be available for all devices.

   - **Anonymous**: The selected LDAP Server does not require user credentials to access the LDAP database.
   - **Simple**: The selected LDAP Server requires user credentials. Note that the Password, if any, will be sent across the network unencrypted.

     NOTE: If you select **Simple**, the credentials are sent from the digital send device without encryption. Contact the LDAP server's administrator to determine the most appropriate server bind method settings.

   - **Simple over SSL**: The selected LDAP Server requires user credentials. Using SSL (Secure Sockets Layer) the password, if any, will be sent across the network encrypted and will be unreadable to a third party.
   - **Kerberos**: The selected LDAP (Active Directory) Server requires user credentials. A Kerberos ticket will be obtained from the Kerberos (Active Directory) Server and used to authenticate to the LDAP Server. The Password will be sent across the network encrypted and will be unreadable to a third party. In order to use Kerberos as a bind method, you must first configure Kerberos settings. If using "user's credentials", make sure that Kerberos Authentication is required for email.
   - **Kerberos over SSL**: The selected LDAP (Active Directory) Server requires user credentials. Using SSL (Secure Sockets Layer) the password, if any, will be sent across the network encrypted and will be unreadable to a third party.

2. Set the options for **LDAP credentials**: The credentials that are used to bind to a specific path (or subtree) in the LDAP Server. In most cases, this is a user's domain account name and a password. With the **Simple** or **Simple over SSL** methods, the user DN form should be used. In some Windows environments, the form DOMAIN\username may be used. If the user DN form is used, HP recommends that the bind path specified in the username match the **Search root** field. This ensures that the relative bind distinguished name has sufficient privileges to search from the specified **Search root**. You can choose one of the following:

   - **Use device user's credentials**
   - **Use public credentials**: Type the user name and password, and then select the Kerberos default realm or domain.

3. **Bind prefix**: This is the LDAP attribute used to construct the user's Distinguished Name (DN) for authentication. This prefix is combined with the username typed at the control panel to form the Relative Distinguished Name (RDN). Commonly used prefixes are "CN" (for common name) or "UID" (for user identity).

4. **Bind and search root**: This is used to validate the user's credentials with the LDAP server. This value is combined with the RDN to construct the full Distinguished Name (DN) of the user. The string consists of "attribute=value" pairs, separated by commas. For example:

   ```
   ou=engineering, o=HP, c=USou=marketing, o=HP,
   c=USo=hp.comou=engineering, cn=users, dc=hp, dc=com
   ```

   NOTE: The **Bind prefix** and **Bind and search root** settings are only used if the **LDAP server bind method** is set to **Simple** or **Simple over SSL**, **Use device user credentials** is selected, and the user authenticates to the device via Kerberos authentication.

5. Type the IP address or hostname for the LDAP server whose database contains the centralized address book in **LDAP server**.

NOTE: Some MFP devices only recognize IP addresses. In such cases, host names will be converted to the equivalent IP address.

6. Type the number of the TCP/IP port on the server that receives LDAP requests in **Port** (usually 389).

7. Set the options for **Searching the database**:

   - **Search root**: The Distinguished Name (DN) of the entry in the LDAP directory structure where address searching is to begin. A DN is made up of `attribute=value` pairs, separated by commas. For example:

     ```
     ou=engineering, o=HP, c=USou=marketing, o=HP,
     c=USo=hp.comou=engineering, cn=users, dc=hp, dc=com
     ```

     NOTE: On some LDAP Servers, the **Search root** can be left blank (in which case its root node will be assumed).

   - **User information retrieval method**: Depending on the type of LDAP server you are running, you might be able to use default settings for the email address look-up attributes.

     Exchange 5.5 Defaults: Select this setting if you are connecting to a Microsoft Exchange 5.5 server that is running LDAP. The LDAP attribute values are automatically set.

     Active Directory Defaults: Select this setting if you are connecting to a Microsoft Exchange Server 2000 server that is running LDAP. The LDAP attribute values are automatically set.

     Custom: Select this setting if you need to manually configure the LDAP attribute values for MFP user's information look-up.

   - **Match the name entered with the LDAP attribute of**: The attribute in the LDAP database that identifies a person in the address book. The value of this attribute will be compared to the person entered by the MFP user in order to retrieve that person's email address. Following are a few examples of possible LDAP attributes:

     – **uid**: User Identifier

     – **cn**: Common Name

     – **sn**: Surname

   - **Obtain email address from**: The LDAP attribute that contains the person's email address. The following are some, but not all, possible LDAP attributes:

     rfc822Mailboxmail

   - **Obtain fax number from**: The LDAP attribute that contains the person's fax number.

Digital Sending - Auto Reset Settings

This option lets you specify how long the digital send device waits after a digital sending operation is complete before it reverts back to the specified default settings. You may need to specify settings other than the default settings for a digital sending operation. If you need to send multiple jobs, it can be time consuming to specify the settings for each additional job. Setting a timeout allows you to send another document before the settings revert to default.

Use the following steps to configure this option:

1. To have the digital device reset to the default settings immediately after each digital send job, select **Immediately reset to default settings**.

   To allow a delay before the digital send device resets to the default settings after each digital send job, select **Delay before resetting the default settings**.

2. If you selected **Delay before resetting the default settings**, type a timeout value in **Number of seconds (10–300) to delay**.

Digital Sending – Default 'From:' Address

This option lets you specify the From address and subject information that initially appears in all email messages sent from the digital send device. The digital send device uses these settings as the initial From address and subject line for each email message it generates. You can also specify whether the digital send device user has permission to change the default From address at the device. For example, you can specify the subject of the email: `Please type in a subject for your message here`. For security reasons, you may not want to allow the user to change the From address provided on the digital send device. You can specify a setting in this section that prevents the user from changing the default From address.

Use the following steps to configure this option:

1. If desired, select **Prevent user from changing the default 'from:' address**.
2. If desired, select **Use Address Book Entries only** to specify the from address can only be from the device's address book.
3. To specify the default sender, type the email address in the **Email address**.
4. Optional: Type the name you want to appear in the From field of the email in the **Display name**.
5. Type the default subject for emails in **Default subject**. For example, type `Please type in a subject for your message here`.
6. Type the default file name for emails in **Default file name**.

Digital Sending – Default Scanner Settings

The default scanner settings determine the initial settings used when a user scans a document. These settings apply to both copying and digital sending operations. Set the default scanner settings to the preferences used most often for scanning on the digital send device. This increases user efficiency because the user does not need to spend time manually configuring the scanner settings as often.

NOTE: The digital send device user can override each of the default scanner settings from the device control panel.

Use the following steps to configure this option:

1. Select the default paper size the device scanner uses when scanning the document from **Document size**.
2. Select the default document type the scanner's image processor uses when scanning the document from the **Document type**:

- **Text**: For documents consisting mostly of textual information.
- **Graphics**: For documents consisting mostly of graphical images.
- **Mixed**: For documents consisting of both text information and graphical images.

3. If the device scanner supports two-sided scanning, select **2 Sided document** to have the scanner device scan both sides of the document.

Digital Sending - Email Attachment Settings

This option lets you specify the default email attachment settings for each email sent from the digital send device. The digital send device uses the email attachment settings as the initial settings for each email message the device generates. Set the default attachment settings to the preferences used most often for email attachments on the digital send device. This increases user efficiency because the user does not need to spend additional time manually configuring the attachment settings as often.

NOTE: The default values can be changed as necessary when sending emails from the device.

Use the following steps to configure this option:

1. Select the file format used for email attachments from **Default file format**.
2. Select black and white or color from **Default color preference**.

   NOTE: Color attachments are larger in size and take more time to send.

3. Select the resolution for email attachments from **Default resolution**.
4. Select the attachment file size from **Default file size**.
5. Select the Tiff version from **Tiff version**.

Email Address Validation

This option lets you configure HP Web Jetadmin to check email syntax when you type an email address. Valid email addresses require the “at” sign (@) and a period (.).

To enable or disable address validation, select **On** or **Off**.

Email Address/Message Settings

Use this option to configure the email address and message settings that the device uses as the initial content for outgoing email messages when users send scanned documents to email. The email address and message settings that are available vary depending on the device.

You can use these settings as a template for the outgoing email message or to provide instructions for the user. For example, you can specify `Enter a subject for the email message` as the initial subject of the outgoing email message.

To configure the email address and message settings for outgoing email messages, perform the following steps:

NOTE: Some devices do not support all of the email address and message settings that are described in the following steps. For these devices, the unsupported settings are not available.

1. Some devices support the **User editable** checkbox for some of the email address and message settings.

   To allow users to change a setting from the device control panel, select the **User editable** checkbox next to that setting.

   -or-

   To prevent users from changing a setting from the device control panel, clear the **User editable** checkbox next to that setting.

2. To allow users to enter email addresses on the device control panel, select the **User can type address** option from the **Address field restrictions** list.

   -or-

   To require users to select email addresses from the address book on the device, select the **User must select from address book** option from the **Address field restrictions** list.

3. To include the email address specified in the **Default from** box in the From list, select the **Default From** option from the **From** list.

   -or-

   To include the email address of the user who is signed in on the device in the From list, select the **User's address (sign-in required)** option from the **From** list.

4. If the **Default From** option is selected from the **From** list, perform the following steps:

   This text box can use static data or custom variables supported in the following formats:

   - Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

     %%<custom variable>%% (where "<custom variable>" is the name of the user defined field)

     Example: `%%var_DefaultFrom%%`

   - Variable data along with a combination of static content before or after the variable

     <static value>%%<custom variable>%%<static value>

     Example: `Info.%%var_DefaultFrom%%`

     Example: `Info.%%var_DefaultFrom%%@MyCompany`

   TIP: By starting the variable data name with var_, it's easier to find and identify user defined fields in HP Web Jetadmin.

   TIP: In HP Web Jetadmin, text boxes that support variable data are highlighted blue. For more information on variable data, see Create and Use Variable Data on page 183.

   a. In the **Default from** box, enter the default email address for the From list. The default email address is required.

   b. In the **Default display name** box, enter a name for the default email address that the device displays in the outgoing email message. The display name is optional.

      This text box can use static data or custom variables supported in the following formats:

      - Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

        %%<custom variable>%% (where "<custom variable>" is the name of the user defined field)

Example: `%%var_DefaultDisplayName%%`

- Variable data along with a combination of static content before or after the variable

  <static value>%%<custom variable>%%<static value>

  Example: `Info.%%var_DefaultDisplayName%%`

  Example: `Info.%%var_DefaultDisplayName%%@MyCompany`

💡 TIP: By starting the variable data name with var_, it's easier to find and identify user defined fields in HP Web Jetadmin.

TIP: In HP Web Jetadmin, text boxes that support variable data are highlighted blue. For more information on variable data, see Create and Use Variable Data on page 183.

5. To allow users to enter the email addresses of the recipients, select the **Blank** option from the **To** list.

   -or-

   To send the outgoing email message to the user who is signed in on the device, select the **User's address (sign-in required)** option from the **To** list.

6. To allow users to enter the email addresses of the recipients who receive a copy of the outgoing email message, select the **Blank** option from the **Cc** list.

   -or-

   To send a copy of the outgoing email message to the user who is signed in on the device, select the **User's address (sign-in required)** option from the **Cc** list.

7. To allow users to enter the email addresses of the recipients who receive a blind copy of the outgoing email message, select the **Blank** option from the **Bcc** list.

   -or-

   To send a blind copy of the outgoing email message to the user who is signed in on the device, select the **User's address (sign-in required)** option from the **Bcc** list.

8. In the **Subject** box, enter the subject for the outgoing email message.

   This text box can use static data or custom variables supported in the following formats:

   - Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

     %%<custom variable>%% (where "<custom variable>" is the name of the user defined field)

     Example: `%%var_Subject%%`

   - Variable data along with a combination of static content before or after the variable

     <static value>%%<custom variable>%%<static value>

     Example: `INFO:%%var_Subject%%`

     Example: `INFO:%%var_Subject%%FROM MFP`

   💡 TIP: By starting the variable data name with var_, it's easier to find and identify user defined fields in HP Web Jetadmin.

   TIP: In HP Web Jetadmin, text boxes that support variable data are highlighted blue. For more information on variable data, see Create and Use Variable Data on page 183.

9. In the **Message** box, enter a custom message for the outgoing email message.

   This text box can use static data or custom variables supported in the following formats:

   - Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

     %%<custom variable>%% (where "<custom variable>" is the name of the user defined field)

     Example: `%%var_Message%%`

   - Variable data along with a combination of static content before or after the variable

     <static value>%%<custom variable>%%<static value>

     Example: `Important%%var_Message%%`

     Example: `Important%%var_Message%%Dev Team`

TIP: By starting the variable data name with var_, it's easier to find and identify user defined fields in HP Web Jetadmin.

TIP: In HP Web Jetadmin, text boxes that support variable data are highlighted blue. For more information on variable data, see Create and Use Variable Data on page 183.

10. To specify that the device digitally signs outgoing email messages, select the **Digitally sign email messages (requires Smart Card Sign In)** checkbox.

    -or-

    To specify that the device does not digitally sign outgoing email messages, clear the **Digitally sign email messages (requires Smart Card Sign In)** checkbox.

NOTE: The **Digitally sign email messages (requires Smart Card Sign In)** checkbox is available only if a Smart Card reader is installed on the device and the Smart Card sign-in method is enabled.

11. To allow users to change the digital signing setting from the device control panel, select the **Digitally sign email messages user editable** checkbox.

    -or-

    To prevent users from changing the digital signing settings from the device control panel, clear the **Digitally sign email messages user editable** checkbox.

12. To specify that the device digitally encrypts outgoing email messages, select the **Encrypt email messages** checkbox.

    -or-

    To specify that the device does not digitally encrypt outgoing email messages, clear the **Encrypt email messages** checkbox.

13. To allow users to edit the digital encryption settings from the device control panel, select the **Encrypt email messages user editable** checkbox.

    -or-

    To prevent users from editing the digital encryption settings from the device control panel, clear the **Encrypt email messages user editable** checkbox.

14. To retrieve the recipient's public key from an LDAP server when the device signs the outgoing email message, enter the LDAP search attribute in the **Attribute for recipient public key** box.

Email File Settings

Use this option to specify the default settings that the digital send device uses when sending scanned documents as email attachments. You can specify the settings that are used most often as the defaults. These default settings increase efficiency because users do not need to manually configure the settings each time they send an email attachment.

Use the following steps to configure this option:

NOTE: Some devices do not support all of the following configuration options. The settings that are available for the configuration options vary depending on the device.

1. In the **File Name Prefix** list or box, specify the prefix that is added to the attachment file name.
2. In the **Default file name** box, enter the file name.
3. To allow users to edit the file name from the device control panel, select the **User Editable** checkbox.

   -or-

   To prevent users from editing the file name from the device control panel, clear the **User Editable** checkbox.
4. From the **File Name Suffix** list, select the suffix that is added to the attachment file name. The suffix can be the date, time, or name of the user who is logged in on the device.
5. From the **Default color preference** list, select the color that the device uses to save the document.
6. From the **Default output quality** list, select the level of quality that the device uses to save the document.

   NOTE: If the **High (larger file)** option is selected, the files are larger and it takes the device more time to send the files.
7. From the **Default file type** list, select the file format that the device uses to save the document.
8. From the **Default resolution** list, select the resolution that the device uses to save the document.

   NOTE: Files that have a higher resolution have more dots per inch (dpi) and show more detail. Files that have a lower resolution have fewer dpi and show less detail, but the files are smaller.
9. From the **Compression** list, select the type of compression that the device uses when saving the document as a PDF or XPS file.

   NOTE: If the **High** option is selected, the files are smaller, but the scanning process takes longer.
10. From the **Black TIFF compression method** list, select the type of black TIFF compression that the device uses to save the document.
11. From the **Color/grayscale TIFF compression method** list, select the type of color/grayscale compression that the device uses to save the document.
12. To encrypt PDF files, select the **PDF encryption** checkbox. A password is specified as part of the encryption process. This password must be used to open the PDF file.

    If a password was not set prior to starting a scan, users are prompted to enter a password.

    -or-

    To save PDF files without encryption, clear the **PDF encryption** checkbox.
13. To delete blank pages in the scanned document, select the **Blank page suppression** checkbox.

    -or-

    To retain blank pages in the scanned document, clear the **Blank page suppression** checkbox.

Email Message Text

This option lets you specify the information that initially appears in the body of all email messages sent from the digital send device. The digital send device uses the email message settings as the initial content text for each email message it generates. The initial information provided can serve as a template for the email or provide instructions to the user. For example, you can type the following message in the body text of the email: `Type the body of the email here`.

Use the following steps to configure this option:

1. To use the default message for the email, select **Message language** and then select a language from the drop-down list. The device generates an email message containing the default message in the selected language.
2. To compose a custom message, select **Use a custom message** and then type a custom message into the text box.
3. To allow the users to change the message text of the email, select **Editable by user**.

Email Notification Settings

Use this option to specify the method and under what conditions notifications are sent when users send scanned documents by email. If a recipient email address is not specified, the user must enter an email address at the device.

Use the following steps to configure this option:

1. Select a value from **Condition on which to notify**:
   - **Do not notify**: Never send a notification when a user sends a scanned document by email.
   - **Notify when job completes**: Always send a notification when a user sends a scanned document by email.
   - **Notify only if job fails**: Send a notification only when an error occurs.
2. Select a delivery method from **Method used to deliver notification**:
   - **Email**: Send the notifications by email.
   - **Print**: Print the notifications. This option is not available for scanners.
3. If **Email** is selected from the **Method used to deliver notification** drop-down list, enter the email address to which the notifications are sent in the **Email address** text box.

Email Scan Settings

The default scanner settings determine the initial settings used when a user scans a document for sending to email. Set the default scanner settings to the preferences used most often for sending email from the digital send device. This increases user efficiency because the user does not need to spend time manually configuring the scanner settings as often.

Use the following steps to configure this option:

NOTE: Some devices do not support all of the following configuration options. The settings that are available for the configuration options vary depending on the device.

1. Select the page size of the original document in **Original size**.
2. If the original size is **Custom**:
   - Set the unit of measurement for the document in **Custom dimension units**.
   - Set the width for the document in **Custom X dimension**.
   - Set the height for the document in **Custom Y dimension**.
3. Specify whether the original document is single-sided or double-sided in **Original sides**.
4. Optimize the output for text or printed pictures, or manually adjust the setting in **Optimize text/picture**.
5. If **Optimize text/picture** is set to **Manually adjust**, then specify the value in **Optimize for**.
6. Specify the way the content of the original document is placed on the page in **Content orientation**.
7. Determine if the back side of the page is upside down or right side up in **2–Sided format**.
8. Specify whether faint images or a light background color should be removed in **Background cleanup**.
9. Adjust the darkness of the file in **Darkness**.
10. Adjust the sharpness of the file in **Sharpness**.
11. Adjust the contrast of the file in **Contrast**.
12. Remove a specific color from the output of a scanned document in **Color dropout**. For example, if an original document has black text and has comments written on it with a red pen, select the **Remove red** option. The scanned file will not contain any of the red marks. Removing a color can improve legibility, improve Optical Character Recognition (OCR) accuracy, and reduce the file size.
13. To scan a document and then display a preview before completing the job, enable **Image preview**.
14. Enable **Job build** to combine several sets of original documents into one email attachment. Also use this feature to scan an original document that has more pages than the document feeder can accommodate at one time.
15. Select **Misfeed detection** for the product to stop scanning when it senses that multiple pages are being fed at one time. To prevent a jam from being reported when a user scans an original document with multiple pages, such as a folded booklet, make sure **Misfeed detection** is not selected; multiple pages fed at one time are not reported as a misfeed.

Enable Device Fax Archive Settings

Use this option to enable or disable the ability to archive faxes on the device.

NOTE: To archive faxes on the device, you might need to configure additional settings, such as the archive destination, fax archive email address for copies of incoming and outgoing faxes, and type of fax job to archive. For more information about these settings, see the **Fax Archive**, **Fax Archive Setting**, and **Fax Archiving** configuration options.

To configure this option, select the **Enabled** or **Disabled** option.

Enable Save to Network Folder

Use this option to enable or disable the Save to Network Folder feature on the device. This feature provides the ability to save scanned documents in a shared folder on a network computer or server. If you enable this feature, the device might require additional configuration settings, such as DNS and WINS server settings.

To configure this option, select the **Enabled** or **Disabled** option.

Enable Save to SharePoint

Use this option to enable or disable the Save the SharePoint® feature on the device. This feature provides the ability to save scanned documents directly on a Microsoft SharePoint site. If you enable this feature, the user does not need to scan a document to a network folder, USB flash drive, or email message, and then manually upload the file to the SharePoint site.

To configure this option, select the **Enabled** or **Disabled** option.

Enable Save to USB

Use this option to enable or disable the Save to USB feature on the device. This feature provides the ability to save scanned documents on a USB flash drive that is inserted into the easy-access USB port on the device.

To configure this option, select the **Enabled** or **Disabled** option.

Enable Send to Email

This option lets you configure the device to send scanned documents as an email. The device may require additional configuration settings in order to send email, such as an outgoing SMTP server or other default email settings. This feature eliminates the need to scan the media remotely, save it to file, and then send it in an email from a computer.

To set this option, select **Enabled** or **Disabled**.

Folder Access Settings

Use this option to set the device to first check access to the shared network folder before saving a file. When this option is disabled, users can save jobs more quickly, but jobs may fail if the folder is unavailable.

To set this option, check the corresponding checkbox.

Import/Export Address Book

Use this option to import a predefined list of email addresses (500 maximum) from a comma separated value (CSV) file directly into the internal address book of the digital send device. You must use this option to configure Fax Speed Dials or add Device User Accounts with PINs.

Also use this option to import a list of fax numbers, speed dials, or device user accounts with PIN numbers.

NOTE: The CSV file must have a header, which is always the first line of that file. If the CSV file does not have a header, the first line of an address is considered a header and that address is lost.

NOTE: For more information about the fields that are valid in the CSV file for a specific device, see the device documentation.

Use the following steps to configure this option:

NOTE: A digital send device can store up to 2,000 entries, but only up to 500 entries can be loaded at a time.

NOTE: The CSV file must have at least one pair of entries for each new address, where the first entry is the name of the person and the second entry is a valid email address. The CSV file can have the following headers; the first two are required:

```
name, emailaddress, dlname, faxnumber, speeddial, code, pin,
permissionset, networkname
```

Following is a sample of a CSV file:

```
name, emailaddress, dlname, faxnumber, speeddial, code, pin,
permissionset, networkname

KellyJacobsonUser, kelly.jacobson@hp.com,,,,,57127, Device User,
KellyJacobsonTest

KellyTest2, kelly@hp.com,,,,,12345, Device User, KellyTest2

KellyTest3, jacobson@hp.com,,,,,54321, Device User, KellyTest3

KellyJacobsonUser, kelly.jacobson@hp.com,,,,,,,

KellyTest2, kelly@hp.com,,,,,,,

KellyTest3, jacobson@hp.com,,,,,,,

,,,12345678, SpeedDial1,1,,,

,,,5432100, SpeedDial2,2,,,

,,,8765432, SpeedDial2,2,,,
```

1. To import an address file, select the **Import address book** option. Click **File**, and then browse to the CSV file.
2. To clear the entire address book on the digital send device, select **Clear device address book**.

   To clear parts of the address book (if supported), select the appropriate checkboxes after you select the **Clear device address book** option.

   Address Book contains both Default and Custom Address Book. In order to clear the Custom Address Book, select the **Clear device address book** option, and then select the **Custom Address Book** check box or only the default address book clears.
3. To export an address book from the digital send device, select the **Export device address book** option, and then click **Export Address book**. Save the file when prompted.

   NOTE: **Export** is only available if you have a single device selected in the device list.

Import/Export Address Book (Pro)

Use this option to manage the address book that is stored on the HP Pro MFP device. You can import a comma-separated values (CSV) file into the address book, clear the address book, and export the address book to a CSV file.

Each line in an imported CSV file is one record. Each record must have entries separated by a comma and must end with a line break (CRLF). At a minimum, each record must contain a person's name, PIN, and permission set.

For more information about other entries that are valid for a specific device, see the documentation for that device.

The first line in the CSV file must be a header record that contains the names of the entries. If the first line is not a header record, the first record is considered the header. The information from that first record is lost when the CSV file is imported.

The following is an example of a CSV file:

```
name, emailaddress, pin, permissionset, networkname
KellyJacobson, kelly.jacobson@company.com,57127, deviceUser, KJacobson
JohnHarris, john.harris@company.com,66212, deviceUser, JHarris
SallySmith,,34432, deviceUser,
```

Import a CSV file

The digital send device can store up to 50 entries in the address book. A maximum of 50 entries can be imported at one time.

1. Select the **Import address book** option.
2. Click the **File** button.
3. On the **Open** window, navigate to and select the CSV file, and then click the **Open** button.

Clear the entries in the address book

▲ Select the **Clear device address book** option.

Export the entries in the address book

The address book can be exported only if a single device is selected in a device list.

1. Select the **Export device address book** option.
2. Click the **Export Address book** button.
3. On the **Save As** window, navigate to the folder to save the file, enter a file name in the **File name** box, and then click the **Save** button.

LDAP Search Method

Use this option to specify the search method for looking up information in the LDAP address book. You can specify the most efficient search method for your organization:

- **Quick Search**: Returns results faster by only searching for entries that begin with the search string.
- **Detailed Search**: Returns more thorough results by searching for entries that contain the search string.

To specify the search method, select **Quick Search** or **Detailed Search**.

LDAP Settings

To send scanned documents through email, users must enter email addresses on the device. The device can provide an address lookup list and auto-complete feature by accessing the database on a Lightweight Directory Access Protocol (LDAP) server.

Use this option to enable the device to connect to an LDAP server and search the database.

Enable the device to search an LDAP server database

1. Select the **Enable network contacts (use LDAP server)** checkbox.
2. In the **LDAP server address** box, enter the IP address or hostname of the LDAP server. The LDAP server address cannot contain the following characters:

   & < > ;

   -or-

   To search for the LDAP server address, click the **Find servers** button.
3. To use Secure Sockets Layer (SSL) to connect to the LDAP server, select the **Use a secure connection (SSL)** option. The default is port 636.

   -or-

   To use a custom port to connect to the LDAP server, select the **Use Custom Port** option, and then enter the port number in the box next to the button. The default is port 389.
4. In the **LDAP server authentication** section, select one of the following options:
   - **Anonymous**: The device does not use credentials to access the LDAP server.
   - **Simple**: The device uses the user's device credentials to access the LDAP server.

     NOTE: The device does not encrypt the user's device credentials when sending them to the LDAP server. Contact the LDAP server administrator to determine the appropriate settings for the server bind method.
   - **Windows Negotiated (SPNEGO)**: The device uses the user's Windows credentials to access the LDAP server.
5. To use the credentials of the user who is signed in on the device to access the LDAP server, select the **Use MFP user credentials to connect after sign in at the control panel** checkbox.

   NOTE: If this checkbox is selected, the device does not use the user name and password specified in the **Default credentials for LDAP server connection** section.
6. To specify the default credentials that the device uses to connect to the LDAP server, perform the following steps:

   a. If the **Windows Negotiated (SPNEGO)** option is selected, enter the fully qualified domain name that the device uses for the authentication in the **Windows domain** box.

   The Windows domain name must comply with the Domain Name System (DNS) standards. An example of a fully qualified domain name is abc.mid.company.com.

   b. In the **Username** box, enter the name of a user who has access permission on the LDAP server.

   c. In the **Password** and **Confirm password** boxes, enter the specified user's password.
7. In the **Path to start search (BaseDN, Search Root)** box, enter the Distinguished Name (DN) of the entry in the LDAP directory structure where the device begins the search. A DN contains one or more attribute=value pairs separated by commas.

   -or-

   On some LDAP servers, the search root can be blank. In these cases, the device starts the search on the root node.

   -or-

To search for the DN in the LDAP directory structure, click the **Find** button.

8. From the **Source for Attribute Names** list, select the source for the attribute names.

9. In the **Match the Recipient's Name with this attribute** box, enter the LDAP attribute for recipient names. The attribute name cannot contain the following characters:

   & < > ;

10. In the **Attribute Name for Recipient’s Email Address** box, enter the LDAP attribute for email addresses. The attribute name cannot contain the following characters:

    & < > ;

11. In the **Attribute Name for Recipient's Fax Number** box, enter the LDAP attribute for fax numbers. The attribute name cannot contain the following characters:

    & < > ;

    NOTE: Some devices do not support this attribute. If you are configuring a single device, these devices ignore the attribute that you enter.

12. To test the retrieval of address book entries from the LDAP server database, enter at least 3 characters in the **Test for LDAP Retrieval** box, and then click the **Test** button.

Disable the device from searching an LDAP server database

▲ Clear the **Enable network contacts (use LDAP server)** checkbox.

Network Folder File Settings

Use this option to specify the default settings for scanned documents that are saved to a network folder.

Use the following steps to configure this option:

1. From the **File name prefix** list, select the prefix that is added to the filename.

   NOTE: You can select more than one option from the **File name prefix** list. The selected options appear in the field below the list.

2. In the **Default file name** box, enter the filename. The filename can be a maximum of 1,024 characters and cannot contain the following characters:

   / \ : * ? " | < >

3. To allow users to edit the default filename from the device control panel, select the **User editable** checkbox.

4. From the **File name suffix** list, select the suffix that is added to the filename.

   NOTE: You can select more than one option from the **File name suffix** list. The selected options appear in the field below the list.

5. From the **Default color preference** list, select the color in which the document is scanned.

6. From the **Metadata file format** list, select the file format that is used for the metadata that is added to the saved file.

7. From the **Default output quality** list, select the level of quality that is used to scan the document.

   NOTE: If you select the **High (large file)** option, the file is larger and it takes more time to scan the document.

8. From the **Default file type** list, select the file format that is used for the scanned document.

9. From the **Default resolution** list, select the resolution that is used to scan the document.

   NOTE: Documents that are scanned at a lower resolution have fewer dots per inch (dpi) and show less detail. Documents that are scanned at a higher resolution have more dpi and show more detail, but the file size is larger.

10. From the **Compression** list, select the compression method that is used to scan the document.

    NOTE: If you select the **High** option, the file is smaller, but it takes more time to scan the document.

11. From the **Black TIFF compression method** list, select the compression method that is used for black TIFF files.

12. From the **Color/grayscale TIFF compression method** list, select the compression method that is used for color or grayscale TIFF files.

13. To encrypt PDF files, select the **PDF encryption** checkbox. A password must be specified as part of the encryption. The same password must be used to open the file.

    NOTE: The user is prompted to enter a password prior to scanning the document if a password was not set prior to touching the Start button.

14. To remove blank pages from the scanned document, select the **Blank page suppression** checkbox.

Network Folder Notification Settings

Use this option to specify the method and under what conditions notifications are sent when users save scanned documents to network folders. If a recipient email address is not specified, the user must enter an email address at the device.

Use the following steps to configure this option:

1. Select a value from **Condition on which to notify**.
   - **Do not notify**: Never send a notification when a user saves a scanned document to a network folder.
   - **Notify only if job fails**: Send a notification only when an error occurs.
   - **Notify when job completes**: Always send a notification when a user saves a scanned document to a network folder.
2. Select a delivery method from **Method used to deliver notification**.
   - **Email**: Send the notifications by email.
   - **Print**: Print the notifications. This option is not available for scanners.
3. If **Email** is selected from the **Method used to deliver notification** drop-down list, enter the email address to which the notifications are sent in the **Email address** text box.

Network Folder Scan Settings

The default scanner settings determine the initial settings used when a user scans a document for saving to a network folder. Set the default scanner settings to the preferences used most often for saving to network folders from the digital send device. This increases user efficiency because the user does not need to spend time manually configuring the scanner settings as often.

Use the following steps to configure this option:

1. Select the page size of the original document in **Original size**.
2. If the original size is **Custom**:
   - Select the unit of measurement for the document in **Custom dimension units**.
   - Set the width for the document in **Custom X dimension**.
   - Set the height for the document in **Custom Y dimension**.
3. Specify whether the original document is single-sided or double-sided in **Original sides**.
4. Optimize the output for text or printed pictures, or manually adjust the setting. in **Optimize text/picture**.
5. If **Optimize text/picture** is set to **Manually adjust**, then specify the value in **Optimize for**.
6. Specify the way the content of the original document is placed on the page in **Content orientation**.
7. Determine if the back side of the page is upside down or right side up in **2–Sided format**.
8. Specify whether faint images or a light background color should be removed in **Background cleanup**.
9. Adjust the darkness of the file in **Darkness**.
10. Adjust the sharpness of the file in **Sharpness**.
11. Adjust the contrast of the file in **Contrast**.
12. To scan a document and then display a preview before completing the job, enable **Image preview**.
13. Remove a specific color from the output of a scanned document in **Color dropout**. For example, if an original document has black text and has comments written on it with a red pen, select the **Remove red** option. The scanned file will not contain any of the red marks. Removing a color can improve legibility, improve Optical Character Recognition (OCR) accuracy, and reduce the file size.
14. Enable **Job build** to combine several sets of original documents into one email attachment. Also use this feature to scan an original document that has more pages than the document feeder can accommodate at one time.
15. Select **Misfeed detection** for the product to stop scanning when it senses that multiple pages are being fed at one time. To prevent a jam from being reported when a user scans an original document with multiple pages, such as a folded booklet, make sure **Misfeed detection** is not selected; multiple pages fed at one time are not reported as a misfeed.

Network Folder Setup

Once **Enable Send to Folder** is enabled, you can use this option to save device settings to a file or load other device settings from a file. You can also use this feature to easily view and manage all of your quick access folders in one interface.

Use the following steps to configure this option:

1. Enable the send to folder settings feature by selecting **Enable Send to Folder**.
2. Click **Add Folder**.
3. Select the preferred folder type: **Standard** or **Personal**.
4. Type the alias name for the folder in **Alias Name**.
5. Type the UNC path name for the folder in **UNC Path Name**.

6. Select the operating system on the computer hosting the quick access folder from **Located On**.
7. If the server connection requires authorization and you want to authorize using the device user's credentials, then select **Use MFP user's credentials**.
8. If the server connection requires authorization and you want to authorize using common credentials, then select **Use Common Credentials**.
9. If the server is Windows-based, type the name of the Windows domain in **Windows Domain**.
10. If the server connection requires authorization and you want to provide default authorization credentials, type the user name in **Username** and type the password in **Password**.
11. Type the NDS Tree value in **NDS Tree** and type the NDS Context value in **NDS Context**.
12. Select a value from **Condition on Which to Notify**.
    - **Never**; never send notices when a file is sent to a folder.
    - **Always**; always send notices when a file is sent to a folder.
    - **All Errors**; send notices only when there is an error.
13. Select a delivery method from **Method Used to Deliver Notification**.
    - **Default File Name**;
    - **Print**; print the notifications.
14. Specify the default settings for files sent to a network folder.

> NOTE: The option **2-Sided Format** is only enabled if the 2-sided option is selected from **Original Sides**.

15. Verify that all the information is correct and then click **OK**.

Follow these steps to edit a quick access folder entry:

1. Select the entry and click **Edit Folder**.
2. Make the changes and click **OK**.

Follow these steps to delete a quick access folder entry:

1. Select the entry and click **Remove Folder**.
2. Click **OK**.

Follow these steps to verify a quick access folder access:

1. Select the entry and click **Verify Access**.
2. On the **Verify Folder Access** dialog box, check if the credentials entered are able to access the folder and click **OK**.

OXPd 1.4 Configuration

Use this option to:

- Specify workflow service servers' URLs.
- Specify the URL polling interval.

- Upload an SDC configuration file to the device.
- Remove the current configuration file.

If a configuration file has already been uploaded to the device, its name and file version will be shown. Refer to the documentation provided with the server software for information about the Server URL, Polling Interval and server software setup.

Use the following steps to configure this option:

1. To upload a configuration file, select a file and click **Load document capture file**. You can browse to the file if desired.
2. To remove a configuration file, click on **Remove Current File**. A new window will open with the operation's results.
3. Type the polling interval in **Polling interval**.
4. To connect to a workflow service installed on a network server, enter one or more URLs into the **URL**. At the specified polling interval, this device will connect to the specified servers and retrieve workflow configuration data.
5. To force URL polling, click **Force update now**. A new window will open with the operation's results.

Personal Contacts Setup

Use this option to sign-in on the device and access personal contacts from the Microsoft Exchange server.

To configure this option, select **Enable Personal Contacts (when users sign in to Windows at the device)**.

Replicate MFP

This option lets you copy the local digital send settings from one device to another. Using this feature enables the settings for **General**, **Email**, **Fax**, and **LDAP** to be replicated.

NOTE: Any configured **Send to folders** cannot be copied or replicated.

To configure this option, specify the IP address of the source device you wish to replicate.

NOTE: Setting this option successfully does not imply that the device settings were successfully replicated. Communication errors between this device and the source device are not reported as an error. To verify that settings were copied, you must examine the device settings after applying this option.

NOTE: This setting may affect the configuration items in the **Digital Sending**, **Fax** and **Security** categories. it is not recommended to set the this feature with other configuration items under those categories.

Reset Copy Send Timeout

This option lets you specify the default amount of time that HP Web Jetadmin waits after any control panel activity completes before it resets the send settings to their defaults. You should set the value to provide users with enough time to set up and complete their digital sending tasks before the product resets their send settings.

To configure this option, type the number of seconds in the text box.

Scan To Folder Predefined Jobs

Use this option to specify the network folder settings, scan settings, and file settings that the device uses to send scanned documents to a network folder.

Add network folder entries

1. If you are configuring multiple devices or creating device configuration templates, select one of the following options from the **Overwrite options** section:

   - **Replace/overwrite existing lists**—Replaces any existing folders on the devices with this list of folders.
   - **Append to existing lists**—Adds this list of folders to the existing list of folders on the devices.

     To update folders on devices that have the same name as the folders in this list, select the **Overwrite any existing items with the same name** checkbox.

2. Click the **Add** button. The **Add Predefined Folder** wizard starts.

3. On the **Specify Network Folder Settings** page, specify the following options, and then click the **Next** button:

   - **Display Name**: Enter a name for the network folder settings. The name can be a maximum of 30 characters and can contain any Unicode characters.
   - **Network path**: Enter the path for the network folder using the Universal Naming Convention (UNC) format. This setting is optional.

     The format for a UNC path is `\\server\share\directory_path`. The UNC path can be a maximum of 512 characters and is not case-sensitive.
   - **User name**: Enter the user name that is required to access the network folder. The user name can be a maximum of 512 characters.
   - **Password**: Enter the password that is required for server authentication. The password can be a maximum of 512 characters and is case-sensitive.
   - **Confirm password**: Enter the password again.
   - **PIN (Optional)**: Enter the Personal Identification Number (PIN) that is required.
   - **Confirm PIN**: Enter the PIN again.

4. On the **Specify Scan Settings** page, specify the following settings, and then click the **Next** button:

   - **Original Size**: Select the default size of the original scanned documents.
   - **Original Sides**: Select the default number of sides of the original scanned documents.
   - **Contrast**: Select the default amount of contrast that is applied when the original documents are scanned.

5. On the **Specify Attachment Settings** page, specify the following settings, and then click the **Finish** button:

   - **File name prefix**: Enter the prefix that is added to the filenames of the scanned documents. The filename prefix can be a maximum of 30 characters. This setting is optional.
   - **Default file type**: Select the file type that is used to save the scanned documents.
   - **Default resolution**: Select the level of resolution that is used to scan the documents.
   - **Default color preference**: Select the color that is used to scan the documents.
   - **Compression**: Select the compression method that is used to scan the documents.

Edit network folder entries

1. Select the folder entry from the list, and then click the **Edit** button. The **Edit Predefined Folder** wizard starts.
2. Change the appropriate settings on the wizard pages. The pages in the **Edit Predefined Folder** wizard are the same as the pages in the **Add Predefined Folder** wizard described previously.
3. Click the **Finish** button.

Delete network folder entries

1. To delete a network folder entry, select the folder entry from the list, and then click the **Remove** button.

   -or-

   To delete all of the network folder entries, click the **Remove All** button.
2. On the **Confirm Remove** window, click the **OK** button.

Send to Network Folder

This option lets you send documents to a network folder. There is a list of predefined folders. You can set the default document setting to apply to documents sent to a network folder.

Use the following steps to configure this option:

1. To enable this option select **Enable send to folder**.
2. To add folders to the list of predefined folders, click **Add** and enter the shared folder or FTP site.
3. To edit an existing folder click **Edit**.
4. To remove all of the predefined folders in the list click **Remove All**.
5. To determine whether you have access to a folder click **Test Folder Access** and enter a domain, username, and password for the credentials to use to access public folders.

   NOTE: **Test Folder Access** is only enabled if you are configuring a single device, because it tests access to the network folder from that specific device.
6. Select settings from the drop-down lists: **Color preference**, **Resolution**, **Default file size**, **File format**, **TIFF version**, and **NTLM authentication setting**.

Send to Network Folder - MSeries or later

Use this option to enable or disable the ability to send scanned documents to predefined folders on the network or an FTP site. The default settings that the device applies to scanned documents can be configured for each predefined folder.

Enable and configure predefined folders

1. Select the **Enable send to folder** checkbox.
2. Use the following steps to add a predefined folder:

   a. Click the **Add** button. The **Add Predefined Folder** wizard starts.

   b. On the **Choose the destination type** page, select the **Shared folder** or **FTP site** option, and then click the **Next** button.

   c. On the **Specify the shared folder settings** or **Specify the FTP site settings** page, specify the appropriate settings, and then click the **Finish** button.

3. Use the following steps to edit a predefined folder:

   a. Select the folder from the **Predefined folders** list, and then click the **Edit** button. The **Edit Predefined Folder** wizard starts.

   b. On the **Specify the shared folder settings** or **Specify the FTP site settings** page, change the settings, and then click the **Finish** button.

4. Use the following steps to delete predefined folders:

   a. To delete a predefined folder, select the folder from the **Predefined folders** list, and then click the **Remove** button.

   -or-

   To delete all of the predefined folders, click the **Remove All** button.

   b. On the **Remove folders** window, click the **OK** button.

5. To verify that the device can access the predefined folder, select the folder from the **Predefined folders** list, and then click the **Test Folder Access** button. Enter the domain, user name, and password that are required to access the folder.

NOTE: The **Test Folder Access** button is enabled only if you are configuring a single device because it tests access to the network folder from that specific device.

6. In the **WINS server** box, enter the IP address for the WINS server.

7. From the **NTLM authentication setting** list, select the authentication protocol that the device uses to access the folder.

8. From the **TIFF version** list, select the version of TIFF that the device uses to scan the document.

9. To verify that the device can access the predefined folder before scanning begins, select the **Verify access before scanning** checkbox. If the device cannot access the predefined folder, the user must enter new credentials. The job does not start until the device can access the predefined folder.

   -or-

   To start scanning immediately after the Start button is pressed without verifying that the device can access the predefined folder, clear the **Verify access before scanning** checkbox. If the device cannot access the predefined folder, the job fails.

Disable predefined folders

▲ Clear the **Enable send to folder** checkbox.

SMTP Gateway Settings

This option lets you specify the SMTP gateway settings for the digital send device. The device uses the SMTP gateway settings to connect to an email server to send scanned documents directly from the digital send device to an email address.

NOTE: The SMTP gateway settings of the digital send device must be specified before scanned documents can be sent through email.

Use the following steps to configure this option:

1. **Send emails**: You can specify the SMTP gateway IP by providing a valid IP hostname or a valid IP address for the gateway server in **IP hostname** or **IP address**.

   NOTE: If you are unsure about the correct SMTP gateway IP address or hostname, click **Find Gateway** to search the network for a suitable SMTP gateway server (if one is available).

2. Specify the TCP/IP port number on which the server is processing SMTP requests by typing it in **Port** (usually this port is 25)

3. Select the maximum size the SMTP gateway server allows for email attachments from the **Maximum attachment size** drop-down list.

4. To specify the use of authentication for using the SMTP server, check **Enable SMTP Authentication**.

   - To use the device's credentials, select **Use Device User's Credentials**.

   - To use public credentials, select **Use Public Credentials** and specify the username and password to use in the authentication.

5. To test the connection to the gateway server, click **Test**. The digital send device attempts to connect to the SMTP gateway server using the specified IP hostname or IP address. The results of the test display in a separate window.

SMTP Multiple Gateway Settings

Use this option to specify the connection and authentication information for one or more SMTP servers. You can add, edit, or delete each of the entries.

NOTE: When adding or editing an SMTP gateway entry, the settings specified in **Default Notification Settings for Email** and **Default Scan Settings for Email** are applied to the specified gateway entry.

To add an SMTP Gateway entry:

1. In the first row, type the name or address of the server in **Server Name or Address**.

2. In the first row, type the port number of the server in **Port Number**.

3. In the first row, select the maximum attachment size from **Maximum Attachment Size**.

4. In the first row, if the server connection requires authorization select **Requires Authorization**.

5. In the first row, if the server connection requires authorization and you want to authorize using the device user's credentials, then select **Use MFP User's Credentials**.

6. In the first row, if the server connection requires authorization and you want to provide default authorization credentials, type the user name in **Username** and type the password in **Password**.

7. Verify the information is correct by clicking **Test Server**. If it is correct, click **Add Server**.

To edit an SMTP Gateway entry, select the entry by clicking the radio button in the second column and then edit the values in the row and click **Edit Server**

To delete an SMTP Gateway entry, select the entry by clicking the radio button in the second column and then click **Remove Server**.

USB File Settings

This option lets you specify the default file settings for each file saved to an attached USB media from the digital send device. The digital send device uses the USB file settings as the initial settings for each file the device saves to USB media. Set the default file settings to the preferences used most often for USB on the digital send device. This increases user efficiency because the user does not need to spend additional time manually configuring the USB file settings as often.

Use the following steps to configure this option:

1. Select the filename prefix in **File Name Prefix**.
2. Specify the filename for the file to be saved in **Default file name**.
3. To allow users to edit the default USB filename at the device control panel, select the **User Editable** checkbox.
4. Select the filename suffix in **File Name Suffix**.
5. Specify whether this file should be saved in black and white or color in **Default color preference**.
6. Select the quality for the file in **Default output quality**.

   NOTE: Higher-quality images require a larger file size than lower-quality images, and they take more time to send.

7. Select the file format for the saved file in **Default file type**.
8. Set the resolution for the file in **Default resolution**.

   NOTE: Higher resolution images have more dots per inch (dpi), so they show more detail. Lower resolution images have fewer dots per inch and show less detail, but the file size is smaller.

9. Specify if the file uses **Normal** or **High** compression when saving a scanned document as a PDF or XPS file in **Compression**.

   NOTE: If compression is set to **High**, the scanned file is smaller, but the scanning process might take longer than **Normal** compression.

10. Select the black TIFF compression method from the **Black TIFF compression method** drop-down list.
11. Select the color/grayscale compression method from the **Color/Grayscale TIFF compression method** drop-down list.
12. For PDF files, enable **PDF Encryption** if you want to encrypt the output PDF file. A password must be specified as part of the encryption. The same password must be used to open the file. The user will be prompted to enter a password prior to scanning their job if one has not been set prior to pressing **Start**.
13. If the **Blank page suppression** checkbox is selected, blank pages are ignored.

USB Notification Settings

Use this option to specify the method and under what conditions notifications are sent when users save scanned documents to USB storage devices. If a recipient email address is not specified, the user must enter an email address at the device.

Use the following steps to configure this option:

1. Select a value from **Condition on Which to Notify**:

- **Do not notify**: Never send a notification when a user saves a scanned document to a USB storage device.
- **Notify only if job fails**: Send a notification only when an error occurs.
- **Notify when job completes**: Always send a notification when a user saves a scanned document to a USB storage device.

2. Select a delivery method from **Method Used to Deliver Notification**:
   - **Email**: Send the notifications by email.
   - **Print**: Print the notifications. This option is not available for scanners.
3. If **Email** is selected from the **Method Used to Deliver Notification** drop-down list, enter the email address to which the notifications are sent in the **Email address** text box.

USB Scan Settings

The default scanner settings determine the initial settings used when a user scans a document for saving to an attached USB media. Set the default scanner settings to the preferences used most often for saving to an attached USB media from the digital send device. This increases user efficiency because the user does not need to spend time manually configuring the scanner settings as often.

Use the following steps to configure this option:

1. Select the page size of the original document in **Original size**.
2. If the original size is **Custom**:
   - Set the unit of measurement for the document in **Custom dimension units**.
   - Set the width for the document in **Custom X dimension**.
   - Set the height for the document in **Custom Y dimension**.
3. Specify whether the original document is single-sided or double-sided in **Original sides**.
4. Optimize the output for text or printed pictures, or manually adjust the setting. in **Optimize text/picture**.
5. If **Optimize text/picture** is set to **Manually adjust**, then specify the value in **Optimize for**.
6. Specify the way the content of the original document is placed on the page in **Content orientation**.
7. Determine if the back side of the page is upside down or right side up in **2–Sided format**.
8. Specify whether faint images or a light background color should be removed in **Background cleanup**.
9. Adjust the darkness of the file in **Darkness**.
10. Adjust the sharpness of the file in **Sharpness**.
11. Adjust the contrast of the file in **Contrast**.
12. Remove a specific color from the output of a scanned document in **Color dropout**. For example, if an original document has black text and has comments written on it with a red pen, select the **Remove red** option. The scanned file will not contain any of the red marks. Removing a color can improve legibility, improve Optical Character Recognition (OCR) accuracy, and reduce the file size.
13. To scan a document and then display a preview before completing the job, enable **Image preview**.

14. Enable **Job build** to combine several sets of original documents into one email attachment. Also use this feature to scan an original document that has more pages than the document feeder can accommodate at one time.

15. Select **Misfeed detection** for the product to stop scanning when it senses that multiple pages are being fed at one time. To prevent a jam from being reported when a user scans an original document with multiple pages, such as a folded booklet, make sure **Misfeed detection** is not selected; multiple pages fed at one time are not reported as a misfeed.

Device Configuration Options for Embedded Web Server

Configuration options for Embedded Web Server define functions for the device's Embedded Web Server.

Embedded Web Server Configuration Options

This option lets you select various features for the embedded Web server. If you have a set of standard configuration options for embedded Web servers, you can direct all of your embedded Web servers to the URL of the printer that has the correct configuration options. This eliminates the need to manually specify the configuration options for each embedded Web server, reducing errors.

To turn a feature on, select the feature check box. To turn a feature off, clear the feature check box.

Embedded Web Server Language Settings

Use this option to specify what language the embedded Web server uses to display Web pages.

Use the following steps to configure this option:

NOTE: If you want to receive HP Web Jetadmin alerts, you must use English or the browser language. To do this, set the **Select a language** to **English** and then specify the language in your browser to the language you need to use. Then select the **View pages in browser language** option.

1. To display the Web pages in a specific language, select **Select a language** and select a language from the drop-down list.

2. To display the Web pages in the language assigned in the user's browser, select **View pages in browser language**.

3. To display the Web pages in the language assigned in the printer, select **View pages in printer language**.

Embedded Web Server Mail Settings

Use this option to configure email settings for an individual printer or printers in a device group. You can specify email settings for sending and receiving email messages from the printer.

Use the following steps to configure this option:

1. Select **SMTP server** and then type the SMTP server IP address in the text box.

2. Select **Domain name** and then type the SMTP server domain name in the text box.

3. To specify the incoming email options:

- Select **POP3 server** and then type the POP3 server IP address in the text box.
- Select **Username** and then type the printer name in the text box.
- If required, select **Password** and then type a password in the text box. Confirm the password by typing it again in the **Confirm password** text box.

Embedded Web Server Other Links

Use this option to create links to other Web sites. This is a convenient way to quickly browse to a Web site. These links appear on the printer’s embedded Web server page. You can create up to five links.

NOTE: **My Printer**, **Order Supplies**, and **Solve a Problem** links are defaults and cannot be deleted or changed.

Use the following steps to configure this option:

NOTE: The following characters are not allowed in a link name or link address: |, ", /, *, +, =, !, @, #, $, %, ¨, &, *, (,) , {, [, },], `, ´, ~, ^, ?, \, ;, :, >, , <

1. Type a name for the link in **Link name**.
2. Type the URL in **Link URL** and click **Add Link**.

   If you typed a link that you do not want, highlight it in the **User-defined links** box and click **Remove**.

   To remove all the links displayed in the list, click **Clear List**. Sending an empty list to the printer will remove any links that may have been previously created.

Embedded Web Server URL

Specify a URL where the embedded Web server can retrieve configuration information. If you have a set of standard configuration options for embedded Web servers, you can set up a URL with those configuration options and direct all of your embedded Web servers to that URL. This eliminates the need to manually specify the configuration options for each embedded Web server, reducing errors.

To assign or change the URL, type it in the text box.

Time Services

Use this option to access another machine on the network to obtain the correct time for an individual printer or printers in a device group. HP printers do not have an internal clock to keep track of the time; therefore, they need to connect to another machine on the network to obtain the current time.

Use the following steps to configure this option:

1. To specify the default values, select **Use default values**.
2. **Enable clock drift correction**: the device will check with the server periodically and update its time. This is beneficial because your device is always set to the correct time but it does cause some network traffic.
3. To specify the network time server address select **Network time server address** and type the IP address.

   NOTE: The printer receives the time from this machine on the network. For the default value, HP Web Jetadmin looks for another machine on the network. If another machine on the network is not found, the value appears as 0.

4. **Local port to receive time from server**: specify the port to use for the device to get data from the time server.

5. To specify an hour for the printer to synchronize with a machine on the network, select **Synchronize time with server every** and type an integer value between 1 and 168 (default is 24 hours).

> NOTE: The time synchronizes with another machine on the network at the designated hourly interval and not immediately after saving. For example, if you specify 2 hours, the printer waits 2 hours after you save this configuration.

Device Configuration Options for Fax

Configuration options for Faxes define functions for fax devices including setup and default fax settings.

Blocked Fax List

This option lets you maintain the list of fax numbers that are blocked by the fax device. Your organization can prevent unwanted fax solicitation by adding the fax number of the solicitor to the blocked fax list.

Following are steps to configure this option:

1. To add a fax number to block, type the number in **Fax number** and click **Add Number**.
2. To remove a fax number from the list, highlight it in **Blocked fax numbers** and click **Remove**.

Enable Fax Receive

Use this option to specify if the device accepts incoming faxes. This setting does not affect the ability of the device to send faxes.

To allow the device to accept all incoming faxes, select the **Enable Fax Receive** checkbox.

-or-

To prevent the device from accepting any incoming faxes, clear the **Enable Fax Receive** checkbox.

Fax Activity Log

Use this option to specify whether the fax activity log is printed, cleared, or both. The fax activity log contains a record of all incoming and outgoing fax calls that have occurred since the last time the fax activity log was cleared. You should periodically print the fax activity log for record-keeping purposes, and then clear the fax activity log to prevent it from becoming too large.

To configure this option, select **Clear**, **Print**, or **Print and Clear** from the drop-down list. The log is printed and cleared when you apply the settings for the digital send device.

Fax Answer Mode

This option lets you select the answer mode for this device. **Manual** mode requires user input and **Automatic** does not.

Fax Answer Mode Settings

This option lets you select the answer mode for this device. Options are:

- **Manual**: requires user input.
- **Automatic**: requires no user input.
- **Telephone Answering Machine (TAM)**: a telephone answering machine is attached to the Auxiliary (Aux) phone port of the product. The product only listens for fax tones after the answering machine has picked up the call; it will not pick up any incoming calls.
- **Fax/Tel**: The product must automatically pick up the call and determine if the call is a voice or fax call. If the call is a fax call, the product handles the call as usual. If the call is a voice call, an audible synthesized ring is generated to alert the user of an incoming voice call.

Following are steps to configure this option:

1. Select the setting.
2. If you select **Fax/Tel**, specify the number of rings and the answer ring pattern.

Fax Archive

Use this option to specify a particular fax number for archiving the fax job in addition to the ones specified by the user. This is useful if you want to track the fax jobs sent to the printer.

To configure this option, select **Enable fax archive** and then type the fax number.

Fax Archive Setting

Use this option to configure the type of fax archive.

Use the following steps to configure this option:

1. Select the **Fax archive setting**:
   - **Disabled**: No archiving of faxes will occur.
   - **Fax**: All faxes are sent to this fax number. Enter the fax number in the **Fax archive number** text box.
   - **Email**: All faxes are archived to the email address specified. Enter the email address in the **Fax archive email address** text box. To specify multiple email addresses, separate the email addresses by a semicolon. This option can be enabled for **Send and receive**, **Send**, or **Receive**.

   NOTE: To enable the **Fax archive to email**, an SMTP gateway must be configured on the **Email Settings** and an administrator email address must also be configured on the **General Settings** page.
2. Select when to archive faxes: **Send and receive**, **Send**, or **Receive**.
3. To disable the printing of incoming faxes when the faxes are successfully archived, select the **Disable print on incoming faxes** checkbox.

NOTE: This option is available only when **Email** is selected in the **Fax archive setting** list and the **Send and receive** or **Receive** option is selected in the **When to archive faxes** section.

Fax Archiving

Use this option to enable fax archiving and specify the type of faxes that are archived. You can specify if faxes are archived or printed or both, and specify how faxes are archived.

Use the following steps to configure this option:

1. To specify how faxes are handled, select one of the following options from the **Fax Archiving** list:
   - **Archive and print**: Faxes are archived and printed.
   - **Archive only**: Faxes are archived, but are not printed.
   - **Do not archive (print only)**: Faxes are printed, but are not archived.
2. To specify how faxes are archived, select one of the following options from the **Archive Destination** list:
   - **Email**: A copy of the fax is sent to the address specified in the **Fax archiving email address** field.
   - **FTP**: A copy of the fax is saved on the FTP server specified in the **FTP settings** section.
   - **Network Folder**: A copy of the fax is saved in the shared network folder specified in the **Folder settings** section.
3. To specify the type of faxes that are archived, select one of the following options from the **Type of fax job to archive** list:
   - **Receive Only**: Only incoming faxes are archived.
   - **Send and Receive**: Outgoing and incoming faxes are archived.
   - **Send Only**: Only outgoing faxes are archived.
4. If you selected **Email** from the **Archive Destination** list, enter the email address where copies of the faxes are sent in the **Fax archiving email address** field.
5. If you selected **Network Folder** from the **Archive Destination** list, specify the following options in the **Folder settings** section:
   - **UNC folder path**: The UNC path of the network folder where the archived faxes are saved. The path must be specified in the format `\\servername\sharename`.

     This text box can use static data or custom variables supported in the following formats:

     – Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

     %%<custom variable>%% (where “<custom variable>” is the name of the user defined field)

     Example: `%%var_folderpath%%`

     – Variable data along with a combination of static content before or after the variable

     <static value>%%<custom variable>%%<static value>

     Example: `\\servername\%%var_sharename%%`

     Example: `\\servername\%%var_sharename%%faxarchive`

     TIP: By starting the variable data name with var_, it’s easier to find and identify user defined fields in HP Web Jetadmin.

TIP: In HP Web Jetadmin, text boxes that support variable data are highlighted blue. For more information on variable data, see Create and Use Variable Data on page 183.

- **Windows domain**: The Windows domain where the network folder is located. The domain name must be less than 128 characters.
- **File Name Prefix**: The prefix added to the filename of the archived faxes.

  This text box can use static data or custom variables supported in the following formats:

  – Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

    %%<custom variable>%% (where "<custom variable>" is the name of the user defined field)

    Example: `%%var_filenameprefix%%`

  – Variable data along with a combination of static content before or after the variable

    <static value>%%<custom variable>%%<static value>

    Example: `fax%%var_faxfilename%%`

    Example: `fax%%var_faxfilename%%archive`

TIP: By starting the variable data name with var_, it's easier to find and identify user defined fields in HP Web Jetadmin.

TIP: In HP Web Jetadmin, text boxes that support variable data are highlighted blue. For more information on variable data, see Create and Use Variable Data on page 183.

- **User name**: The user name required to access the network folder.
- **Password**: The password required to access the network folder.
- **Verify Folder Access**: Click this button to verify that the specified location and credentials for the network folder are valid.

6. If you selected **FTP** from the **Archive Destination** list, specify the following options in the **FTP settings** section:

   - **FTP server**: The FTP server where the archived faxes are saved. The server name is required and must be less than 256 characters.
   - **Port**: The FTP port where the archived faxes are saved. The port number must be from 1 through 65535.
   - **FTP folder path**: The path of the folder on the FTP server where the archived faxes are saved.
   - **File Name Prefix**: The prefix added to the filename of the archived faxes.
   - **User name**: The user name required to access the FTP server.
   - **Password**: The password required to access the FTP server.
   - **Verify Access**: Click this button to verify that the specified location and credentials for the FTP server are valid.

Fax Billing Code

This option lets you specify the billing code information for the digital send device. Billing codes provide a way to track faxes from different locations. When supported by the fax method, billing codes can be used to track the fax source to a specific machine or sender.

Use the following steps to configure this option:

1. To allow the user to enter a billing code other than the default, select **Yes** from **Editable by the user**.
2. Type the default billing code value in **Default billing code**.
3. Select the minimum number of characters that a user is allowed to enter as a valid billing code from **Minimum length**. (The maximum number of characters allowed for a billing code is 16.)

Fax Forwarding

Use this option to send a copy of all incoming and outgoing faxes to another fax number.

Use the following steps to configure this option:

1. To configure this option, select **Enable Fax Forwarding**.
2. Select the type of fax job to forward.
3. Type the fax phone number for all copies of incoming and outgoing faxes to be forwarded to.

Fax General

This option lets you specify advanced fax settings for the digital send device. You can specify the modem and ringer volumes, whether the header information is overlaid on top of the fax image, and whether the fax device should use JBIG compression or Error Correction Mode (ECM). Printing the header over the top of the fax image instead of above it reduces the chance that each faxed page is larger than the selected paper size and prints as two pages on the receiving fax device.

JBIG compression is a protocol that allows for faster fax sending between two JBIG compliant fax devices. It is possible that older fax machines may fail to connect when JBIG is enabled. Error Correction Mode (ECM) should normally be enabled, except in extreme circumstances where line conditions are too poor to support ECM faxes.

Use the following steps to configure this option:

1. Select the fax modem volume from **Modem volume**.
2. Select the fax ringer volume from the **Ringer volume**.
3. The phone number, time, and date are stamped at the top of all outgoing faxes. To print this information over a small portion of the top of the fax image, select the **Overlay header**.
4. To disable JBIG compression, select the **Disable JBIG compression**.
5. To disable Error Correction Mode, select the **Disable error correction**.

Fax Header

You can specify the company name and fax number to be included at the top of your faxes.

Use the following steps to configure this option:

1. Type the company name in **Company name**.
2. Type the fax number in **Fax number**.

Fax Header Settings

Use this option to specify information about the origin of sent faxes. You can include Company Name, Phone Number, and Country/Region of origin.

Use the following steps to configure this option:

1. Type the phone number from which the device is dialing in **Phone number**.

   This text box can use static data or custom variables supported in the following formats:

   - Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

     %%<custom variable>%% (where "<custom variable>" is the name of the user defined field)

     Example: `%%var_phone_number%%`

   - Variable data along with a combination of static content before or after the variable

     <static value>%%<custom variable>%%<static value>

     Example: `971%%var_phone_number%%`

     Example: `1%%var_number%%9000`

2. Type the name of the company of origin in the **Company name**.

   This text box can use static data or custom variables supported in the following formats:

   - Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

     %%<custom variable>%% (where "<custom variable>" is the name of the user defined field)

     Example: `%%var_company_name%%`

   - Variable data along with a combination of static content before or after the variable

     <static value>%%<custom variable>%%<static value>

     Example: `ABC Company%%var_company_state%%`

     Example: `ABC Company%%var_company_state%%@YourService`

3. Select the country/region of origin from the **Location** drop-down list.

TIP: By starting the variable data name with var_, it's easier to find and identify user defined fields in HP Web Jetadmin.

TIP: In HP Web Jetadmin, text boxes that support variable data are highlighted blue. For more information on variable data, see Create and Use Variable Data on page 183.

Fax Maximum Baud Rate

Use this option to specify the maximum baud rate for the fax transmission. If the fax is having communication issues use this setting to select a slower baud rate to determine if the error is being caused by the phone line.

To configure this option, select the baud rate from the drop-down list.

Fax Maximum Baud Rate - Receive

Use this option to specify the maximum baud rate (Kilobits per second) for receiving faxes. The baud rate is normally set to the highest value available. The fax modem negotiates the appropriate speed up to this setting while receiving faxes.

If the fax modem is having communication issues, set this option to a slower baud rate to determine if the phone line is causing the error.

To configure this option, select the baud rate from the drop-down list.

Fax Maximum Baud Rate - Send

Use this option to specify the maximum baud rate (Kilobits per second) for sending faxes. The baud rate is normally set to the highest value available. The fax modem negotiates the appropriate speed up to this setting while sending faxes.

If the fax modem is having communication issues, set this option to a slower baud rate to determine if the phone line is causing the error.

To configure this option, select the baud rate from the drop-down list.

Fax Modem Settings

Similar to a fax machine, the digital send device sends scanned documents to a fax phone number. Specify the fax settings to ensure that the fax line associated with the digital send device is properly configured.

Use the following steps to configure this option:

1. Select the country/region of origin from **Country/region**.
2. Optional: Type the name of the company of origin in **Company name**.
3. Type the phone number from which the device is dialing in **Phone number**.
4. If a prefix number is required by the local phone system, select **Enable dialing prefix** and then type it in **Dialing prefix**.

Fax Notification

The digital send device can generate notification reports to provide further details about the result of a fax send or receive operation. Use this option to specify when the digital send device generates notification reports and how those reports are delivered to the user. Depending on your needs, you can configure the device to deliver notification reports regularly or only when specific types of errors occur.

Use the following steps to configure this option:

1. Select the condition when fax notifications should be sent from **Condition upon which to notify**.
2. Select the notification delivery method from the **Method used to deliver notification**:

   NOTE: The device must be correctly configured to use either option.

   - **Print**: print the fax notification report directly at the digital send device.
   - **Email Sender**: send the fax notification report to the user's email address.
3. To include a thumbnail image of each fax with the fax notification report, select **Yes** from **Include thumbnail**.

Fax Number Confirmation

When this option is enabled, prior to sending a fax the device displays a confirmation screen asking for the fax number again to ensure the number is correct. This is useful in companies and offices that often need to send restricted and confidential information via fax.

To enable this option, select **Enabled**.

Fax Printing

This option lets you specify the fax printing settings for the fax capable device. You can specify a PIN to secure incoming fax documents and prevent unauthorized users from printing them. You can also specify whether incoming faxes are printed or stored. For printed faxes, you can schedule when they are printed. If incoming faxes contain sensitive information, securing the fax modem with a PIN prevents unauthorized users from printing those faxes. If the fax device is not attended regularly, storing all received faxes or specifying a printing schedule prevents the faxes from being printed when the device is unattended.

Use the following steps to configure this option:

1. Type a numeric PIN in **PIN number**.

   Confirm the numeric PIN by typing it again in **Confirm PIN number**.
2. To specify the printing mode settings for the fax, select one of the following options:
   - **Print All Received Faxes**: Print all faxes when they are received.
   - **Store All Received Faxes**: Store all received faxes on the device. The faxes can only be printed by entering the correct PIN on the device.
   - **Use Fax Printing Schedule**: Specify the times when incoming faxes can be printed. You can specify the days and times when the device is unlocked.

     Specify the days that the digital send device is unlocked by selecting the appropriate checkboxes in the **Week day** column.

     Select a start time from **Start printing faxes** and a stop time from **Stop printing faxes**.

     NOTE: If you do not specify a schedule then the device stores all received faxes.

Fax Printing Schedule

This option lets you specify how faxes are stored and printed. You can choose to always print faxes, always store faxes, or print faxes according to a specific daily schedule. Depending on the security needs of your organization, you may choose to always store faxes or only print them during a time when an administrator is present to collect them. Choose the fax printing schedule that best suits the needs of your organization.

Use the following steps to configure this option:

1. Select one of the three options:
   - **Always store faxes**: store all received faxes in memory.
   - **Always print faxes**: print each fax as it is received.
   - **Use fax printing schedule**: print received faxes according to a specified schedule.
2. If you select the **Use fax printing schedule** option, specify the fax printing schedule. For each day of the week, select the checkbox in the second column, and then enter the time you want faxes to start printing in the **Start printing faxes** field. Select the checkbox in the fourth column, and then enter the time you want faxes to stop printing in the **Stop printing faxes** field.

   You can also enable or disable the **Use Holiday Sleep Schedule** option. If you enable this option, incoming faxes are stored during the holidays, and then printed after the holiday.

NOTE: Some device models do not support the **Use Holiday Sleep Schedule** option.

Fax Receive

Use this option to specify the most efficient fax receive settings for the digital send device. You can specify which bins on the digital send device the faxes are printed from and delivered to, how the faxes are formatted for printing, the number of rings the fax device waits before answering an incoming call, and whether the device should forward the fax document to another fax capable machine. These settings will ensure that the majority of the incoming faxes are received successfully and delivered to the user in the most effective manner.

Use the following steps to configure this option:

1. Select the number of the input tray from which the digital send device prints faxes from **Fax paper tray**.
2. Select the number of the output bin to which the digital send device prints faxes from **Fax destination bin**.
3. Select the number of rings that the fax machine waits before answering an incoming call from the **Number of rings before answering**.
4. To stamp received faxes with available information from the sender, select **Stamp received faxes**.
5. To scale the incoming fax image to the size of the paper contained in the input tray, select **Fit image to page size**.
6. To forward incoming faxes on the digital send device to another fax capable machine, type the phone number of the target fax in **Forwarding number**.

NOTE: Even if the digital send device forwards a fax, it will still handle the fax normally by printing it, emailing it, or storing it in memory.

Fax Receive – Disposition

This option lets you define what a device should do when receiving a fax. Either print the fax or forward it to a different fax number.

Fax Receive – Other Options

This option lets you select additional options the device can do when receiving a fax. You can allow users to get faxes even when attached to an extension phone, let the device detect if there is silence after the incoming phone is answered, or even force each incoming fax to be time-stamped.

Fax Receive – Setup

Use this option to specify the fax receive settings. You can specify which bins the faxes are delivered to, how the faxes are formatted for printing, the number of rings each fax device waits before answering an incoming call, and whether each device should forward the fax document to another fax capable machine. These settings will ensure that the majority of the incoming faxes are received successfully and delivered in the most effective manner possible.

Use the following steps to configure this option:

1. To forward incoming faxes to another fax capable machine, select **Enabled** from the **Fax forwarding** drop-down list.
2. To stamp incoming faxes with available information from the sender, select **Enabled** from the **Stamp received faxes** drop-down list.
3. Select the number of retry attempts when the receiving line is busy from the **Rings to answer** drop-down list.
4. Type the ring interval (in milliseconds) in the **Ring interval** text box.
5. Select the ringer volume for incoming faxes from the **Ringer volume** drop-down list.
6. To scale the incoming fax image to the size of the paper contained in the input tray, select **Enabled** from the **Fit to page** drop-down list.
7. Select the bin that incoming faxes are printed out of from the **Paper selection** drop-down list.
8. Select which output tray the device prints faxes from the **Output bin** drop-down list.

Fax Receive Settings

Use this option to specify the fax receive settings. You can specify which bins the faxes are delivered to, how the faxes are formatted for printing, the number of rings each fax device waits before answering an incoming call, and whether each device should forward the fax document to another fax capable machine. These settings ensure that the majority of the incoming faxes are received successfully and delivered in the most effective manner possible.

Use the following steps to configure this option:

1. Select the ringer volume for incoming faxes from the **Ringer volume** drop-down list.
2. Select the number of retry attempts when the receiving line is busy from the **Rings to answer** drop-down list.

3. Select the speed for the fax from the **Fax receive speed** drop-down list.
4. Type the ring interval (in milliseconds) in the **Ring interval** text box.
5. Type the ring frequency in the **Ring frequency** text box.
6. Enter the time in milliseconds between rings that must elapse before the modem can detect an incoming ring in the **Ring burst off time (220-600) ms** text box.
7. Select the duplex setting to use when printing incoming faxes from the **Duplexing** drop-down list.
8. Select which paper to use for faxes in the **Paper selection** drop-down list.
9. Select which output tray the device prints faxes from the **Output bin** drop-down list.
10. To scale the incoming fax image to the size of the paper contained in the input tray, select the **Fit to page** option.
11. To stamp incoming faxes with available information from the sender, select the **Stamp received faxes** option.
12. Select which circumstances to deliver a notification in **Condition on which to notify** drop-down list.
13. Select the method to deliver the notification from the **Method used to deliver notification** drop-down list.
14. Type the email address for notifications to be sent to in the **Notification email** text box.
15. If you are sending faxes using the internal modem, and you include the thumbnail of the first page, select **Include thumbnail**.

Fax Reporting and Error Corrections

This option lets you set up options with errors and tracking reports. Enabling error correction lets the device automatically attempt error correction with faxes. You can also select how often the fax log is printed by selecting the frequency in the drop-down list. You can also choose to include the first page or not.

Fax Reports and Logs

This option lets you specify whether to print or clear the fax activity logs. The fax activity log contains a record of all the incoming and outgoing fax calls that have occurred since the last time the fax log was cleared. Periodically, the log should be printed for record-keeping purposes and then cleared. This prevents the log from becoming too large.

Use the following steps to configure this option:

1. To print the fax activity log, select **Print activity log**. The log is printed when the settings for the digital send device are applied.
2. To clear the fax activity log, select **Clear activity log**. The log is cleared when the settings for the digital send device are applied.

Fax Resolution Quality

This option lets you specify the resolution quality of outbound faxes. Use the resolution setting to manage the efficiency of the fax sending operation. Lower resolution typically results in faster fax send times, but the quality of the fax document is reduced.

NOTE: The resolution setting cannot be changed by the user.

To configure this option, select the quality of outbound faxes from the **Resolution** drop-down list.

Fax Ring Burst Off Time

Use this option to specify a the amount of time between rings that must elapse before the modem can detect an incoming ring (or, Ring Burst Off Time). You may want to specify a custom value for Ring Burst Off Time if you use the fax line for multiple purposes and only want the fax answering for a specific ring duration.

To configure this option, select **Enable Custom Ring Burst Off Time** and then type the value in milliseconds in **Ring Burst Off Time**.

Fax Ring Frequency

Use this option to specify a particular frequency for the fax ring. You may need to specify a custom value in order to fix oscillations generated by a custom PBX policy. This option might be required by technical support to adjust the fax ring communication.

NOTE: Change this setting only when directed by an HP technical support agent.

To configure this option, select **Enable custom ring frequency** and then type a numeric value.

Fax Send

This option lets you specify the most efficient settings for sending faxes from the digital send device. These settings affect how the device dials outbound faxes and how it behaves when the receiving line fails to answer the fax. These settings will ensure that the majority of the outbound faxes are received successfully while minimizing time spent attempting to send faxes to unreachable recipients.

Use the following steps to configure this option:

1. Select the dialing mode from the **Dialing mode** drop-down list.
2. To have the fax wait for a dial tone before dialing for an outbound fax document, select **Yes** from the **Detect dial tone** drop-down list.
3. Select the number of retry attempts when the receiving line is busy from the **Redial on busy** drop-down list.
4. Select the number of retry attempts when the receiving line fails to answer from the **Redial on no answer** drop-down list.
5. Select the number of minutes to wait between retry attempts from the **Redial interval** drop-down list.

Fax Send - Dialing Mode

This option lets you sets the default dialing mode for dialing a number on a fax send (**Tone** or **Pulse**). This lets you select the dialing mode that suits the characteristics of the available communication line.

To configure this option, select the radio button for the dialing mode.

Fax Send - Other Options or Other Settings

This option lets you define what the device should do if the number dialed is busy or there is no answer.

Fax Send - Resolution

This option lets you sets the default resolution that will be used when sending faxes. The available selections are **Standard**, **Fine**, **Superfine**, and **Photo**. This lets you control the quality of the sent faxes when the default setting is used.

To configure this option, select the desired resolution.

Fax Send - Setup

Use this option to specify the send settings for faxes. You can specify the modem and ringer volumes, the dial and redial settings, and whether the fax device should use JBIG compression or Error Correction Mode (ECM).

Use the following steps to configure this option:

1. Select the fax dial volume from the **Fax dial volume** drop-down list.
2. To enable Error Correction Mode (ECM), select **Enabled** from the **Error correction mode** drop-down list. ECM should normally be enabled, except in extreme circumstances where line conditions are too poor to support ECM faxes.
3. To enable JBIG compression, select **Enabled** from the **JBIG compression** drop-down list. JBIG compression is a protocol that allows for faster fax sending between two JBIG compliant fax devices. It is possible that older fax machines may fail to connect when JBIG is enabled. For such a scenario, use the JBIG disable option.
4. Select **Tone** or **Pulse** from the **Dialing mode** drop-down list.
5. Select the number of retry attempts when the receiving line is busy, from the **Redial on busy** drop-down list.
6. Select the number of retry attempts when the receiving line fails to answer from the **Redial on no answer** drop-down list.
7. To have the fax wait for a dial tone before dialing for an outbound fax document, select **Enabled** from the **Detect dial tone** drop-down list.
8. To specify a dialing prefix, type the value in the **Dialing prefix** text box.
9. To print the billing code report, select the **Print billing code list** checkbox.

Fax Send Settings

Use this option to specify the settings for sending faxes. You can specify the fax send method, scan settings, notification settings, internal modem settings, LAN fax settings, and Internet fax settings.

Use the following steps to configure this option:

1. To enable sending faxes, select the **Enable fax send** checkbox.
2. Select the method the device uses to send faxes from the **Fax send method** drop-down list.

3. In the **Common Job Settings—Scan settings** section, specify the following settings for the original documents and scanned output:

   - **Default resolution**: Select the default resolution used when the original documents are scanned.
   - **Original size**: Select the default size of the original documents.
   - **Custom dimension units**: If you select **Custom** from the **Original size** drop-down list, select the default unit of measurement used for the original documents.
   - **Custom X dimension**: If you select **Custom** from the **Original size** drop-down list, enter the default width of the original documents.

     If the **Custom dimension units** option is set to **inches**, the default width must be between 54.86 mm (2.16 in) and 215.9 mm (8.5 in).

     If the **Custom dimension units** option is set to **mm**, the default width must be between 52 mm (2.047 in) and 215.9 mm (8.5 in).
   - **Custom Y dimension**: If you select **Custom** from the **Original size** drop-down list, enter the default height of the original documents.

     If the **Custom dimension units** option is set to **inches**, the default width must be between 73.66 mm (2.9 in) and 863.6 mm (34 in).

     If the **Custom dimension units** option is set to **mm**, the default width must be between 73.7 mm (2.902 in) and 863.6 mm (34 in).
   - **Original sides**: Select the default number of sides of the original documents.
   - **Optimize text/picture**: Select the default type of content optimized when the original documents are scanned.
   - **Optimize for**: If you select **Manually adjust** from the **Optimize text/picture** drop-down list, select the value that specifies whether the original documents are optimized more for text or more for pictures by default.
   - **Content orientation**: Select the default orientation of the original documents.
   - **2-sided format**: Select the default duplex format of the original documents.

     If you select **Book style**, the pages are turned like a book (long edge).

     If you select **Flip style**, the pages are turned like a flip book (short edge).
   - **Background cleanup**: Select the default amount of background removed when the original documents are scanned.
   - **Darkness**: Select the default amount of exposure applied when the original documents are scanned.
   - **Contrast**: Select the default amount of contrast applied when the original documents are scanned.
   - **Sharpness**: Select the default amount of sharpness applied when the original documents are scanned. A higher value produces sharper output.
   - **Image preview**: Specify whether the device displays a preview of the scanned output before sending the fax.

     If you select the **Make optional** option, users can choose whether a preview is displayed before they send a fax.
   - **Misfeed detection**: Select this checkbox to stop scanning when the device senses that multiple pages are being fed at one time.

NOTE: To prevent the device from reporting a jam when a user scans an original document that has multiple pages, such as a folded booklet, make sure that the **Misfeed detection** checkbox is not selected. The device does not report a misfeed when multiple pages are fed at one time.

- **Job build**: Select this checkbox to allow users to combine multiple scanned pages into a single outgoing fax. If this checkbox is not selected, multiple scanned pages result in multiple outgoing faxes.
- **Enable Blank Page Suppression**: Select this checkbox to remove blank pages from the outgoing faxes.

4. In the **Common Job Settings—Notification settings** section, specify the following settings for fax notification reports:

   - **Condition on which to notify**: Select when the device generates notification reports for sent faxes.
   - **Include thumbnail**: Select this checkbox to include a thumbnail image of each fax with the fax notification report.
   - **Method used to deliver notification**: Select how the device delivers fax notification reports.
   - **Email address**: Enter the email address to which the notification reports are sent.

5. In the **Common Job Settings—General Fax Send Settings** section, select the **Fax number confirmation** checkbox to display a confirmation screen asking the user to enter the fax number again. This option is useful for companies that send restricted and confidential information via fax.

6. In the **Internal modem—General fax settings** section, specify the following settings for the internal modem on the device:

   - **Enable PC fax send**: Select this checkbox to allow users to send faxes from their computers.
   - **Enable error correction mode**: Select this checkbox to enable Error Correction Mode (ECM). If ECM is enabled, the receiving fax device checks the fax information for errors. If the receiving fax device detects an error, it requests the sending fax device to resend all or part of the fax.

   NOTE: ECM is normally enabled. However, if the line conditions are too poor to support ECM faxes, do not select the **Enable error correction mode** checkbox.

   - **Enable JBIG compression**: Select this checkbox to enable JBIG compression. JBIG compression is a protocol that allows for faster fax transmissions between two JBIG-compliant fax devices.

   NOTE: Older fax machines might fail to connect if JBIG compression is enabled.

   - **Enable overlay header**: Select this checkbox to overlay or prepend the fax header to the fax pages.
   - **Enable speed dialing matching**: Select this checkbox to enable speed dial matching. When speed dial matching is enabled, walk-up users can enter speed dial numbers instead of full fax phone numbers when sending a fax.

7. In the **Internal modem—Fax dialing settings** section, specify the following settings for the internal modem on the device:

   - **Fax dial volume**: Select the volume of the internal modem dialer.
   - **Dialing mode**: Select the dialing mode used.
   - **Dialing prefix**: Enter the dialing prefix added to all phone numbers when dialed. For example, enter 9 if it is required to access an outside line.
   - **Fax send speed**: Select the speed used to process outgoing faxes.
   - **Redial interval**: Enter the number of minutes that the internal modem waits between redialing attempts.

- **Redial on no answer**: Enter the number of times that the internal modem redials when there is no answer.

- **Redial on busy**: Enter the number of times that the internal modem redials when there is a busy signal.

- **Redial on error**: Select this checkbox to enable the internal modem to automatically redial if a communication error occurs while sending the fax. Select the number of times that the internal modem redials from the list.

- **Detect dial tone**: Select this checkbox to have the internal modem wait for a dial tone before dialing.

8. In the **Internal modem—Billing code settings** section, specify the following settings for the internal modem on the device:

   - **Enable billing codes**: Select this checkbox to prompt users to enter a billing code when faxes are sent. If this option is selected, the billing code that the user enters is included in the billing code report.

   - **Default billing code**: Enter the default billing code used.

   - **Minimum length**: Enter the minimum number of characters users can enter as a valid billing code.

   NOTE: The maximum number of characters allowed for a billing code is 16.

   - **Allow users to edit billing code**: Select this checkbox to allow users to edit the billing code when sending a fax. If this checkbox is not selected, the default billing code is always used.

9. In the **LAN fax setup—LAN fax service settings** section, specify the following settings for a third-party fax device used over a LAN connection:

   - **Third party LAN fax product**: Select the third-party LAN fax device used.

   - **File format**: Specify the file format used for outgoing faxes.

10. In the **LAN fax setup—Folder settings** section, specify the following settings for accessing the server where the LAN fax device stores fax jobs:

    - **UNC folder path**: Enter the path to the folder where fax jobs are stored using the Universal Naming Convention (UNC) format. The format for a UNC path is "`\\server\share\directory path`", and it is not case-sensitive.

    - **Windows domain**: If the network is a Windows-based domain, enter the domain name.

    - **User name**: If the network requires authentication to access the fax folders, enter a valid user name.

    - **Password**: If the network requires authentication to access the fax folders, enter the password for the user name.

11. In the **LAN fax setup—Dialing settings** section, specify the following settings for the LAN fax device:

    - **Maximum retry attempts**: Enter the maximum number of times that the LAN fax device tries to send the fax again if the first attempt fails.

    - **Retry interval (minutes)**: Enter the number of minutes that the LAN fax device waits before trying to send the fax again.

12. In the **LAN fax setup—Input settings** section, specify the following settings for the LAN fax device:

- **Enable notification**: Select this checkbox to send a notification when an error occurs sending the fax to the network folder.
- **Notification timeout (minutes)**: Enter the number of minutes that the LAN fax device waits before sending a notification when an error occurs.
- **Enable error correction**: Select this checkbox to enable Error Correction Mode (ECM). When ECM is enabled, the LAN fax device resends any portions of the fax that were not successfully sent.

13. In the **LAN fax setup—Output settings** section, specify the following settings for the LAN fax device:
    - **LAN fax transmission speed**: Select the transmission speed used for outgoing faxes.
    - **Enable cover page**: Select this checkbox to include a cover page with outgoing faxes.
14. In the **Internet fax setup** section, specify the following settings for an Internet fax service:
    - **Internet fax provider domains**: Enter the domain for the Internet fax service provider, and then click the **Add** button.
    - To delete a domain, select the domain from the list, and then click the **Remove** button.

      -or-

      To delete all of the domains, click the **Remove All** button.
    - **Default internet fax provider domain**: Select the default domain that is used for the Internet fax provider.
    - **Default account email address**: Enter the default email 'from' address used to send faxes. The email address must comply with RFC 5322, 5321, and 3696.
    - **T37 prefix**: Enter the T37 prefix used to send faxes. The prefix can contain characters 0 through 9 and a comma (,).
    - **File format**: Select the file format used to send faxes.
    - **If available, use the signed in user's email address as the fax account address**: Select this checkbox to use the signed-in user's email address as the fax account address when faxes are sent.
    - **Auto complete to North American Numbering Plan (NANP) format using area code**: Select this checkbox to automatically add the area code to the fax number when faxes are sent. Enter the area code in the text box.

Fax Send Setup

Use the following steps to configure this option:

1. **Enable fax send**: enable sending faxes and specify the fax send method.
    - Select **Enable fax send**.
    - Select a send method from **Fax send method**.
2. **Common settings – Billing code settings**: enable and configure billing codes. Billing codes provide a way to track faxes from different locations. When supported by the fax method, billing codes can be used to track the fax source to a specific machine or sender.
    - To enable billing codes, select **Enable billing code**.
    - To specify the default billing code value, type the billing code value in **Default billing code**.

- To allow the user to enter a billing code other than the default, select **Editable by user**.
- To specify the minimum number of characters a user is allowed to enter as a valid billing code, type the value in **Minimum length**.

3. **Common settings – Default original settings**: specify the default settings for scanning fax originals.
   - Select the default resolution from the **Default resolution** drop-down list.
   - Select the default two-sided format from the **2-sided format** drop-down list.
   - Select the default original size from the **Original size** drop-down list.
   - Select the default background cleanup setting from the **Background cleanup** drop-down list.
   - Select the default original number of sides from the **Original sides** drop-down list.
   - Select the darkness setting from the **Darkness** drop-down list.
   - Select the default quality optimization setting from the **Optimize text/picture** drop-down list.
   - Select the default sharpness setting from the **Sharpness** drop-down list.
   - Select the default orientation from the **Content orientation** drop-down list.
   - Select the default contrast setting from the **Contrast** drop-down list.
4. **Common settings – Default notification settings**: set the device to send a notification whenever a fax is sent.
   - Select a value from the **Condition on which to notify** drop-down list:
     - **Always**: always send notices when a fax is sent.
     - **Never**: never send notices when a fax is sent.
     - **All errors**: send notices only when there is an error.
   - Select a delivery method from the **Method used to deliver notification** drop-down list:
     - **Email**: send the notifications to the administrator's email address.
     - **Print**: print the notifications.
5. **LAN fax setup – LAN fax service settings**: specify the third-party fax product to use over a LAN connection. You can also specify the file format for the faxes.
   - Select the fax product from the **Third party LAN fax product** drop-down list.
   - Select the fax file format from the **File format** drop-down list
6. **LAN fax setup – Common job settings**: specify common information about the network that is used to store fax jobs. If you have configured your fax device to store faxes on a network server, the common job settings specify the network information needed to access the server. Save device resources by storing faxes on a server instead of the device.
   - Select the type of network the folder is located on from the **Folder is located on** drop-down list. The type of network determines the folder format.
   - Type the folder path in **Common folder path (UNC)**.
   - If the network is a Windows-based domain, type the domain name in **Windows domain**.
   - If the network requires authentication to access the fax folders, type a valid user name in **User name** and type a valid password in **Password**.
   - Type the NDS Tree value in **NDS tree** and type the NDS Context value in **NDS context**.

7. **LAN fax setup – Dialing settings**: specify the dialing settings for sending faxes. These settings affect how the devices dial outbound faxes and how they behave when the receiving line fails to answer a fax. Use this section to specify the most efficient fax dialing settings for your organization. These settings will ensure that the majority of the outbound faxes are received successfully while minimizing time spent attempting to send faxes to unreachable recipients.

   - Enter the maximum number of retry attempts the fax should make in **Maximum retry attempts**.
   - Type the retry interval in minutes in the **Retry interval (minutes)** text box

8. **LAN fax setup – Input settings**: specify the settings for incoming faxes on the receiving device. Choose the settings that best suit the needs of your organization. If you need notifications for each received fax, you can turn on fax notifications. If there are problems with the quality of the incoming line, you can turn on **Error correction mode** to compensate.

   - To enable notifications, select **Enabled** from the **Notification** drop-down list.

     To disable notifications, select **Disabled** from the **Notification** drop-down list.

   - To turn on **Error correction mode**, select **On** from the **Error correction mode** drop-down list.

     To turn off ECM, select **Off** from the **Error correction mode** drop-down list.

   - Type the number of minutes for notification timeout in **Notification timeout (minutes)**.

9. **LAN fax setup – Output settings**: specify the settings for outgoing faxes on the sending device. Choose the fax transmission speed that best suits the speed capabilities of your organization's outgoing fax lines. If your organization requires a cover page, you can turn it on.

   - Select the fax transmission speed setting from the **LAN fax transmission speed** drop-down list.
   - To turn on the cover page for outgoing faxes, select **On** from the **Cover page** drop-down list.

     To turn off the cover page, select **Off** from the **Cover page** drop-down list.

10. **Internet fax setup**: if your organization uses a separate fax service over an internet connection, use this option to enable sending faxes from your device through the internet fax service.

    NOTE: The device must be configured to send emails before the internet fax feature can be set up.

    - Type the domain name for the internet provider in **Internet fax provider domain**.
    - Type the email address for the account that processes the faxes in **Default account email address**.
    - If the internet fax provider requires a T37 Prefix for fax emails, type the prefix in **T37 prefix**.
    - Select the email file format from the **File format** drop-down list.
    - If you want to use the user's email address as the fax account address, select **If available, use the signed in user's email address as the fax account address**.
    - If you want the area code for the fax number to auto-complete, select the **Auto complete to North American Numbering Plan (NANP) format using area code** and type the area code in the corresponding text box.

Fax Service

Use this option to enable the V.34 fax standard, print fax reports, and set the speaker mode.

Use the following steps to configure this option:

1. To print a T.30 report, select the **Print T.30 report** check box and then select when the report should print from the **When to print report** drop-down list.
2. To enable or disable the V.34 fax standard, select **Enabled** or **Disabled** from the **Fax V.34** drop-down list.
3. To adjust the speaker mode, select a value from the **Speaker mode** drop-down list.

Fax Time Format

This option lets you select the time format this device should use (12 hour or 24 hours).

Fax Transmit Signal Loss

Use this option to specify the decibel range for transmit signal loss. This compensates for phone line signal loss. You can increase the amount of decibels used by the fax to compensate for weaknesses in the phone line signal.

To configure this option, type a decibel value in the **Decibels** field.

Import Speed Dials

Use this option to import a predefined list of fax speed dials from a comma separated value (CSV) file directly into the internal memory of the device. To send a fax, you must provide a fax number. The process of entering multiple fax numbers can be simplified by providing an speed dial list. Importing fax numbers into the internal memory of the device provides a list of fax numbers for users to choose from.

The CSV file should be in the following format:

```
Fax number, user name, distribution list name, code
```

where:

- **fax number** is the fax destination number.
- **user name** is the sign in name. This value is always 'MFP Public'.
- **distribution list name** is the name of a distribution list of fax numbers. The code is a unique number assigned to the distribution list name.

Use the following steps to configure this option:

1. To import a speed dial list, click **File** to locate the CSV file using a dialog window, or type the path and filename of the CSV file in the text box.
2. To clear the speed dial list on the device, select **Delete all device contacts**.

LAN Fax Service Settings

Use this option to specify the settings that the device uses to send faxes through a LAN fax service.

⚠ CAUTION: When you enable or make any changes to this configuration option, the fax send method is automatically set to LAN Fax Service.

Use the following steps to configure this option:

1. In the **LAN fax service settings** section, specify the following options:
   - **Third-party LAN fax product**: Select the LAN fax vendor that the device uses to send faxes.
   - **File format**: Select the file format that the LAN fax vendor uses for faxes.
2. In the **Folder settings** section, specify the following options:
   - **Folder is located on**: Select the platform on which the fax folder is located.
   - **UNC folder path**: Enter the path to the folder where outgoing faxes are stored using the Universal Naming Convention (UNC) format. The format for a UNC path is `\\server\share\directory_path`. The UNC path is not case-sensitive.
   - **Windows domain**: Enter the Windows domain name where the fax folder is located. The format of the domain name must comply with DNS standards. The domain name can be a maximum of 128 characters.
   - **User name**: If the network requires authentication to access the fax folder, enter a valid user name. The user name can be a maximum of 255 characters.
   - **Password**: If the network requires authentication to access the fax folder, enter the password for the specified user name. The password can be a maximum of 255 characters.
   - **Test Folder Access**: Click this button to verify that the specified location and credentials for the fax folder are valid.
3. In the **Dialing settings** section, specify the following options:
   - **Maximum retry attempts**: Enter the maximum number of times that the device tries to send a fax again if the first attempt fails. Valid values are from 0 to 99.
   - **Retry interval (minutes)**: Enter the number of minutes that the device waits before trying to send a fax again. Valid values are from 0 to 999.
4. In the **Input settings** section, specify the following options:
   - **Condition on which to notify**: Select one of the following options to specify when the device sends a notification for outgoing faxes:
     - **Do not notify**: The device does not send a notification under any conditions. This option is equivalent to the **Never** option in the HP Embedded Web Server (EWS).
     - **Notify only if job fails**: The device sends a notification only when a fax job fails. This option is equivalent to the **For errors on any faxes** option in the EWS.
     - **Notify when job completes**: The device sends a notification when a fax job completes. This option is equivalent to the **Always** option in the EWS.
   - **Error Correction Mode**: Select the option to enable or disable Error Correction Mode (ECM). If you select the **On** option, the device resends any portion of a fax that was not successfully sent.
   - **Method used to deliver notification**: Select one of the following options to specify how the device delivers notification reports when the notification condition occurs:
     - **Email Sender**: The device sends the notification report to the email address that is specified by using the **Administrator Information** configuration option.
     - **Print**: The device prints the notification report.
   - **Email Notification Attachment**: Select this checkbox to send the scanned pages to the specified email address as an attachment.
5. In the **Output settings** section, specify the following options:

- **LAN fax transmission speed**: Select the transmission speed that is used for outgoing faxes. If you select the **Default** option, the transmission speed that is defined for the device is used.
- **Cover page**: Select the option that specifies if a cover page is included with outgoing faxes.

6. In the **Quality** section, select the default resolution that is used for outgoing faxes from the **Resolution** list.

PC Fax Send

Use this option to specify whether users can send faxes from their computer.

To allow users to send faxes from their computer, select the **Enabled** option.

To prevent users from sending faxes from their computer, select the **Disabled** option.

TCF Settings

Use this option to optimize fax performance by fine tuning the fax ring frequency and TCF signals to best suit the needs of your organization. If your fax device is having trouble sending outbound faxes, increasing the TCF delay and extending the TCF signal may improve communication with difficult fax receivers. TCF is a series of zeros sent to the receiver to confirm that the connection is working and to establish the optimal connection speed. The sending fax generates a series of TCF signals at different speeds until it receives a Confirmation To Receive (CFR) signal from the receiving fax. **TCF T.30 delay** specifies how long to wait before sending each TCF signal. **TCF extend** specifies how long to extend the TCF signal beyond the default time length (1500 milliseconds).

Use the following steps to configure this option:

NOTE: By default, **TCF T.30 delay** and **TCF extend** values are set to the manufacturer's default.

1. To specify a custom TCF delay value, check the box next to **Enable custom TCF T.30 delay** and then type the length for the delay in **TCF T.30 delay**. The value can be from 60 milliseconds to 255 milliseconds.
2. To specify a custom TCF extend value, check the box next to **Enable custom TCF extend** and then type the length for the extend in **TCF extend**. The value can be from 0 milliseconds to 2550 milliseconds.

Device Configuration Options for File System

Configuration settings for File System are used to delete files on the device’s memory.

File System External Access

This option allows you to manage the access to file systems by various printer communication languages on a device hard drive, which helps protect a device’s file system from unauthorized reading or writing of data. If you disable a printer communication language, that printer communication language cannot read or write any data to the file system on a device’s hard drive.

NOTE: All printer communication languages are enabled by default.

To configure this option, select the printer communication language or languages to enable.

File System Password

This option prevents unauthorized users from changing any file system configuration options and from performing a secure storage erase operation. The file system password must be set to perform a secure storage erase operation and to configure the secure file erase modes and the file system external access.

NOTE: For easier password management, it is recommended to set the same file system password for all devices.

NOTE: The file system password needs to be set for a device before the new file erase mode can be configured. The file system password should be set via a separate device configuration. Once set, the new file erase mode value can be set.

To set the initial file system password for a device, type the password in **File system password**. Type the password again in **Confirm password**.

Secure File Erase Mode

This option determines the behavior of a secure storage erase operation and the erase operation that a printer automatically performs to make space available on a hard disk drive for incoming print jobs. The erase operations are designed to add available space to a device's hard disk drive and to prevent unauthorized users from accessing confidential information from a device's hard disk drive or other erasable storage device. The following are the supported secure file erase modes:

- **Non-secure Fast Erase**: Erases the file system references to operations, such as completed print jobs. By erasing the references, space on the hard disk drive is made available. This is the fastest erase mode and the default mode.
- **Secure Fast Erase**: Erases the file system references to operations and provides one layer of masking to hide data stored on the hard disk drive or other erasable storage devices. This mode is slower than the **Non-secure Fast Erase** but more secure.
- **Secure Sanitizing Erase**: Erases the file system references to operations and provides multiple layers of masking to hide data stored on the hard disk drive or other erasable storage devices. This mode may introduce a significant performance impact to the device while the process is executing.

NOTE: The file system password needs to be set for a device before the new file erase mode can be configured. The file system password should be set via a separate device configuration. Once set, the new file erase mode value can be set.

To configure this option, select a file erase mode from the drop-down list.

Device Configuration Options for Network

Configuration options for Network define network communication functions for the device including TCP/IP setup, and protocols.

Bonjour Service Name (mDNS Service Name)

Use this option to configure a user-friendly service name for a device that is running in a Bonjour (mDNS) environment. The service name is configured on the HP Jetdirect card. You can use this service name to easily find the device in the device lists.

To configure the Bonjour service name (mDNS Service Name), enter the name in the box.

Configuration Precedence

Use this option to configure the precedence that the device uses when setting several configuration parameters (for example, hostname) by using different configuration methods. The order in which the configuration methods are listed determines which configuration method has precedence over another method for duplicate configuration parameter values. For example, a DHCP hostname overwrites a TFTP hostname if DHCP/BOOTP has precedence over TFTP.

To specify the configuration precedence, select a method in the list, and then click **Move Up** or **Move Down**.

To restore the default configuration preference, click **Reset**.

NOTE: To specify the configuration precedence in a template or for multiple devices, you must click **Reset**.

Desired USB Mode

This option lets you specify the protocol that the USB uses to interface with this device. HP Jetdirect normally uses the best protocol that the device supports. If a more complex interface does not work with the HP Jetdirect print server, change this option to a simpler interface. If you select **Automatic**, the HP Jetdirect print server uses the best protocol available. If you select **Unidirectional**, the HP Jetdirect print server uses the forward-data only protocol (USB class 7.1.1). If you select **Bidirectional**, the HP Jetdirect print server uses the simple forward and reverse data protocol (USB class 7.1.2). If you select **Multiple Logical Channels (MLC)**, the HP Jetdirect print server uses the HP-MLC protocol (USB class 7.1.2+).

To change the protocol, select the option for the protocol that you want this HP Jetdirect print server to use.

DHCP User Class Option (Tag 77)

Use this option to determine the manufacturer, type, model, and serial number of the device.

To configure this option, select the checkbox.

DHCPv4 FQDN compliance with RFC 4702

The Dynamic Host Configuration Protocol for IPv4 (DHCPv4) provides a mechanism for host configuration that includes dynamically assigning IP addresses and fully qualified domain names (FQDNs). Use this option to enable or disable DHCPv4 FQDN compliance with RFC 4702.

To enable DHCPv4 FQDN compliance with RFC 4702, select the checkbox.

To disable DHCPv4 FQDN compliance with RFC 4702, clear the checkbox.

HP Connection Inspector

Use this option to enable or disable HP Connection Inspector.

To enable the HP Connection Inspector information, select the **Enable** option.

To disable the HP Connection Inspector information, select the **Disable** option.

DNS Server

If your network uses Domain Name System (DNS) services, use this option to specify the IP address of a primary DNS server for specified devices. If a secondary DNS server is available on your network and can be configured on the device, you may also specify the IP address of the secondary DNS server. A secondary DNS server is used when the primary DNS server is not available. Use **Domain name** to specify a Domain Name for this device. A domain is a set of one or more IP addresses, and the Domain Name identifies the domain in which the device resides (for example, support.hp.com). A Domain Name typically consists of a series of labels separated by the dot (.) character, ending with a predefined suffix to identify its top-level domain. For example, top-level domain .com is used for commercial businesses, .edu for educational institutions, and .org for nonprofit organizations.

Devices on an IP network actually use IP addresses for communications. However, device IP addresses may dynamically change or be difficult to remember, use or manage. Domain Name System (DNS) services are used to automatically translate user-friendly Domain Names to corresponding device IP addresses. A server on the network that provides this service is a DNS server.

Use the following steps to configure this option:

1. Enter the IP address of the primary DNS server in **Primary DNS server IP**.
2. Enter the IP address of the secondary DNS server in the **Secondary DNS server IP**.

   NOTE: Some devices may not support configuration of a secondary DNS server.

3. To specify a Domain Name for a device, enter the Domain Name assigned to this device in **Domain name**. (The entry is limited to 254 alphanumeric ASCII characters, including the dash (-) character and dot (.) label separator.)

   NOTE: When specifying the Domain Name, do not include the device host name. The entry in **Domain name** is not the fully-qualified host name (for example, printer1.support.hp.com is a fully-qualified host name for a device with host name “printer1” in the domain “support.hp.com”).

Error Handling

This option specifies how the HP Jetdirect EX print server handles error conditions. The print log provides information that you can use to troubleshoot printer problems and recover from errors.

To configure this option, select one of the settings:

- **Dump then Reboot**: Device does a memory dump and then reboots.
- **Reboot without Dump**: Device reboots without doing a memory dump.
- **Dump then Halt**: Device does a memory dump but doesn’t do a reboot; operations are halted.

Google Cloud Print

Google Cloud Print allows customers to print web pages, emails, photos, and content from applications that have integrated Google Cloud Print. Customers simply add the unique email address of their HP ePrint-enabled product to their Google account, which provides the ability to print easily and securely from any Google Cloud Print-enabled app, product, or service on any computer or smartphone to the selected HP ePrinter.

Use this option to enable or disable the Google Cloud Print feature on the printer or remove the Google Cloud Print feature from the printer.

To configure the Google Cloud Print feature, select one of the following options from the list:

- Enable—Enables the Google Cloud Print feature on the printer. The printer must then be registered with Google Cloud Print by using the printer HP Embedded Web Server (EWS).
- Disable—Disables the Google Cloud Print feature on the printer.

  After the Google Cloud Print feature is disabled on the printer, you can use the printer EWS or HP Web Jetadmin to enable the feature again.
- Remove—Removes the Google Cloud Print feature from the printer control panel and printer EWS.

  After the Google Cloud Print feature is removed from the printer control panel and printer EWS, you must use HP Web Jetadmin to enable the feature again.

HTTP Idle Timeout

Use this option to configure the amount of time (in seconds) that an HTTP connection to the device remains open when there is no traffic, such as when a print job stops sending data to the device.

To specify an HTTP idle timeout period, enter a value from `5` to `60`. The default is `15`.

To disable the HTTP idle timeout period, enter `0`.

IPP Printer Install Wizard

This option lets you specify the URL for the Internet Printing Protocol (IPP) Printer Install Wizard link for this printer. When you access this link, an Install Wizard runs that lets you create a print path between your computer and this printer.

⚠ CAUTION: If you change this URL, the availability of the Install Wizard may change. Make sure that the Install Wizard has been properly set up before changing this.

To configure this option, type the URL for the IPP Printer Install Wizard in the text box.

IPv4 Information

Network devices use an IP address to communicate with another network device and the subnet mask to determine the network and host portions of the IP address. The default gateway is the address of a gateway system or a router, which are the nodes that let a network device communicate on other networks or subnets. These options define the IP address, subnet mask, and default gateway address that the HP Jetdirect print server uses. The IP address, subnet mask, and gateway address are required to communicate with a device that uses the TCP/IP protocol.

⚠ CAUTION: These options are fundamental to TCP/IP-based networks. Before you change these options, make sure that you clearly understand how the network is designed.

NOTE: The IP address specified here overrides BOOTP, DHCP, or any previously configured IP address on the HP Jetdirect print server. This is similar to configuring static addresses through Telnet or the device control panel in the case of an internal HP Jetdirect print server. Use the static configuration method if you do not have any automatic or server methods, such as BOOTP or DHCP.

NOTE: You can only apply this configuration option to a single device. You cannot use this configuration option to configure multiple devices at one time or include this configuration option in a template.

To change the IP address, type the new IP address in **IP Address**. To change the subnet mask, type the new subnet IP address in **Subnet Mask**. To change the gateway address, type the new gateway IP address in **Gateway**.

IPv6 Information

You can enable or disable an IPv6-capable device to use the IPv6 protocol. IPv6 must be enabled to access other IPv6-capable devices through an IPv6 network.

You can specify how the Dynamic Host Configuration Protocol version 6 (DHCPv6) functions on the network. DHCPv6 is a protocol for assigning dynamic IP addresses to devices on a network. If you use dynamic addressing, a different IP address is assigned to the device when it connects to the network. A device's IP address can even change while it is still connected. DHCP also supports static IP addresses. Dynamic addressing monitors IP addresses on the network rather than requiring an administrator to manage the task. This means that a new device can be added to a network without manually assigning a unique IP address to the device.

If you are configuring a single device, you can specify a manual IPv6 address and prefix for the device. This option is not available with multiple devices or templates.

You can set the priority of how a device obtains IP addresses on the network, based on the best method for the network. The priority is determined by the order listed in the configuration precedence list. For example, if DHCP/BOOTP has precedence over DHCPv6, an IP address provided through DHCPv4 will have precedence over an IP address provided by DHCPv6.

You can set IPv6 DNS options, including the Domain, Primary DNS, and Secondary DNS.

Use the following steps to configure this option:

1. To enable support for IPv6-capable devices, select **Enable IPv6**. To disable support, deselect this option.
2. Select one of the DHCPv6 policy options:
   - **Always perform DHCPv6 at startup**
   - **Perform DHCPv6 when stateless configuration is unsuccessful**
   - **Perform DHCPv6 only when requested by the router**
3. If you are configuring a single device and wish to enter a manual IPv6 address, select **Manual** and enter the appropriate information.
4. To specify the configuration precedence, highlight the method and then click **Move Up** or **Move Down**. To restore the default configuration scheme, click **Reset**. You must click **Reset** in order to set the precedence in a template, or with multiple devices selected.
5. You can specify a domain name for this device to be used in IPv6. The domain name does not include the device host name, and multiple devices may share the same domain name.
6. You can specify the Primary and Secondary DNS servers for the device to be used in IPv6. If the network uses Domain Name System (DNS) services, use this option to specify the IP address of a primary DNS server for this device. If a secondary DNS server is available on the network and can be configured on the device, specify the IP address of the secondary DNS server. A secondary DNS server is used when the primary DNS server is not available.

IPX - Ethernet Frame Type

This option lets you specify the Ethernet frame types that the HP Jetdirect print server uses on the network. If you select **Auto**, the HP Jetdirect print server tries all of the frame types until it finds the one that works. If you know that you are only going to use one frame type, selecting that frame type reduces network traffic.

To configure this feature, select one of the Ethernet frame type options:

- Auto
- Ethernet 802.3
- Ethernet II
- Ethernet 802.2
- Ethernet SNAP

IPX - Frame Type Token Ring

IPX protocol is supported by Novell NetWare network OS. This option lets you specify which encapsulation type for IPX to use for a token ring LAN or it can be set to let the device automatically decide which is best to use.

IPX - Queue Server Job Polling Interval

IPX protocol is supported by Novell's NetWare network operating system. This option lets you specify the number of seconds for the queue server job polling interval.

IPX - RCFG Support Enabled

RCFG (remote configuration protocol) was developed by HP for remote configuration and management of devices on an IPX/SPX network, typically a Novell NetWare network. By factory default, RCFG is enabled. RCFG does not support encrypted communications or authentication, and is not secure. If RCFG is not required for device configuration and management, it should be disabled. Disabling RCFG does not affect the use of IPX/SPX Direct-Mode (peer-to-peer) printing. Use this feature to enable or disable RCFG. If enabled, RCFG (sometimes called RCONFIG) allows the device to be remotely configured on an IPX/SPX network. HP Web Jetadmin may use RCFG to configure Novell NetWare queue-server linkages on older HP Jetdirect print servers.

To enable RCFG, select **Enable RCFG support**. To disable RCFG, deselect this field.

IPX - SAP Broadcast Interval

By default, the HP Jetdirect print server sends out a Service Advertising Protocol (SAP) broadcast every 60 seconds to advertise itself on the network and make Novell print servers aware of its presence. SAP broadcasts are necessary for the print server services to be located in some Novell NetWare environments. This option lets you specify how often the HP Jetdirect print server sends out a SAP broadcast. If you have many HP Jetdirect print servers on your network, SAP broadcasts can cause network traffic. To reduce the impact that SAP broadcasts have on network traffic, increase the IPX SAP broadcast interval. You might want to disable HP Jetdirect SAP broadcasts on Novell networks that use Novell Distributed Print Services (NDPS) or on other networks that do not require them.

To assign or change the IPX SAP broadcast interval , type the broadcast interval in minutes in the text box. To disable the IPX SAP broadcast interval, type 0 (zero) in the text box.

IPX - Source Routing

IPX protocol is supported by Novell's NetWare network OS. This option lets you set how source routing is handled by the device or allow it to automatically choose.

IPX Name

Use this option to change the name of a printer that is running in an IPX/SPX environment. The printer name is changed on the HP Jetdirect card.

⚠ WARNING! If you are in an IPX/SPX environment, changing the printer name could disable the print paths for types such as NetWare Bindery. If you are not using IPX/SPX, this option becomes another description field. You can assign a user-friendly printer name that helps you easily find the printer in device lists.

To change the IPX/SPX name, type the name in the text box.

Jetdirect External Print Server

The HP Jetdirect External Print Server setting allows you to restart the print server remotely. The external print server may not be close or be conveniently positioned for access.

To restart the external print server, select **Restart**.

Job Timeout

This value represents (in seconds) the maximum time of inactivity which must elapse before the print server card switches from the current network protocol to another when a normal end of job is not detected. For external HP Jetdirect print servers, allowable values are zero, and also within the range 30 to 3600 seconds. For internal HP Jetdirect print servers, allowable values are zero, and also within the range 30 to 127 seconds.

NOTE: If the timeout value is set at zero, the print server will never time out (it will always stay in the current network protocol being used).

To specify a new job timeout, enter the timeout in seconds in the text field.

Locally Administered Address

Locally administered addresses are only supported in Token Ring HP Jetdirect print servers. The network device manufacturer originally sets the media access control (MAC) address in the device read-only memory. You can change the MAC address for most Token Ring network devices. This option lets you specify the MAC address on the Token Ring HP Jetdirect print server. Some Token Ring environments use the Locally Administered Address feature. While it is not a requirement that you change the MAC address, the Locally Administered Address feature might be implemented in some Token Ring environments. Some administrators find it easier to manage devices if the MAC address for all of the devices of the same type start with specific characters. For example, starting all HP devices with 003.

⚠ CAUTION: To prevent potential problems, make sure that the address you assign is not already in use.

NOTE: While the Novell protocol environment on the HP Jetdirect print server can restart and begin printing again after you assign locally administered addresses, you must reconfigure the other protocol environments to acknowledge the new address. This includes the Linux and Microsoft host software.

NOTE: You can only apply this configuration option to a single device. You cannot use this configuration option to configure multiple devices at one time or include this configuration option in a template.

To assign or change the locally administered address, type the address in the text box.

Link Setting

Use this option to specify the link speed (10 or 100 Mbps) and the communication mode (full- or half-duplex) that the device should use when connecting to your 10/100Base-TX network each time it is powered on. To communicate on your network, the device link speed and communication mode must match the operation of your network. If the device setting is AUTO, the device will attempt to autonegotiate its link settings with the network each time it is powered on. If the device successfully links to the network, you can then use this feature to explicitly configure the required link setting on the device. When the device is powered on again, the configured setting will be used directly. However, if the device fails to link using AUTO, then the link settings on the device will default to 100 Mbps and half-duplex mode. Communications with the device over the network may, or may not, be possible. The link setting options:

- AUTO: Link settings are automatically negotiated.
- 10TXFULL: The link is set to 10 Mbps, full-duplex operation.
- 10TXHALF: The link is set to 10 Mbps, half-duplex operation.
- 100TXFULL: The link is set to 100 Mbps, full-duplex operation.
- 100TXHALF: The link is set to 100 Mbps, half-duplex operation.
- 1000TFULL: The link is set to 1000 Mbps full-duplex operation.

NOTE: Setting the link to a setting incompatible with the network causes the printer to lose access to the network and might require a cold reset of the printer.

To configure this option, select one of the Link Setting options from the drop-down box.

Mgmt Protocol

Use this option to enable and disable the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols that the device uses to provide communication security and encryption over the Internet.

Federal Information Processing Standard (FIPS) supports only the TLS 1.0, TLS 1.1, and TLS 1.2 protocols. To configure the security protocol when FIPS mode is enabled on the device, you must specify the TLS 1.0, TLS 1.1, and TLS 1.2 protocols. If you specify the SSL 3.0 protocol, the configuration fails.

If you configure only the SSL 3.0 protocol for a device, a discovery finds the device and adds the device to the device lists, but the device is in a Device Communication Error state.

To enable a protocol, select the corresponding checkbox.

To disable a protocol, clear the corresponding checkbox.

Network Enable Features

Use this option to enable or disable various network configuration tools, printing methods, and other features that the device supports. Because each device supports different features, the configurable items available for a specific device vary. The following are examples of configurable items:

- Network configuration tools, such as Telnet and HP Embedded Web Server (EWS). Telnet and EWS provide additional access to print server configuration and management Web pages.
- Printing services, such as the following:
  - File Transfer Protocol (FTP)
  - Line Printer Daemon (LPD), which provides line printer spooling services for TCP/IP systems
  - Internet Printing Protocol (IPP)
  - IPP protocol over the HTTPS transport binding (IPPS)
  - Port 9100 (direct-mode printing)
- The AirPrint feature on the device, which allows instant wireless printing from iPad, iPhone, and iPod touch devices. Before you enable the **AirPrint** option, you must enable the **Bonjour (mDNS Config)** option and enable either the **IPP Printing** or the **IPPS Printing** option.
- Other features that some client applications use to discover and identify devices, such as the Service Location Protocol (SLP).
- The mDNS, IPv4 Multicast, and Link Local Multicast Name Resolution (LLMNR) protocols. mDNS is used for IP address and name resolution through UDP port 5353. mDNS is typically used on small networks where a conventional DNS server is not used. IPv4 Multicast allows the print server to send and receive IPv4 multicast packets. LLMNR allows both IPv6 and IPv4 hosts to perform name resolution for neighboring computers without requiring a DNS server or DNS client configuration.
- HP Web Services, which accesses XML-based data on HP Jetdirect print servers.
- The Web Services (WS) protocol, which is used to discover network-connected and PC-connected devices on both local and remote subnets.
- The Windows Internet Name Service (WINS) port and registration support.
- The Trivial File Transfer Protocol (TFTP) configuration file, which controls the behavior of the TFTP server.

To enable a feature, select the checkbox.

-or-

To disable a feature, clear the checkbox.

Network Enable Features – More Settings

The AirPrint-FaxOut feature is used to send faxes from an iPad, iPhone, iPod touch, or Macintosh computer to an AirPrint-enabled printer. The AirPrint Scan (eSCL/WebScan) feature is used to send scanned documents from an AirPrint-enabled printer to an iPad, iPhone, iPod touch, or Macintosh computer. The AirPrint Secure Scan (Secure eSCL/WebScan) feature is used to send scanned documents securely from an AirPrint-enabled printer to an iPad, iPhone, iPod touch, or Macintosh computer.

Use this option to enable or disable the AirPrint-FaxOut, AirPrint Scan (eSCL/WebScan), and AirPrint Secure Scan (Secure eSCL/WebScan) features on the device. Before these features can be enabled, first enable the **Air Print** option on the **Network Enable Features** configuration option.

Enable the AirPrint features

1. Select the **AirPrint Fax** check box.
2. Select the **AirPrint Scan (eSCL/WebScan)** check box.
3. Select the **AirPrint Secure Scan (Secure eSCL/WebScan)** check box.

Disable the AirPrint features

1. Clear the **AirPrint Fax** check box.
2. Clear the **AirPrint Scan (eSCL/WebScan)** check box.
3. Clear the **AirPrint Secure Scan (Secure eSCL/WebScan)** check box.

Parallel Handshake

This option lets you specify the parallel mode that the HP Jetdirect EX print server uses. If the specified mode does not work, the HP Jetdirect print server tries other modes until it finds one that does work. The default option tells the HP Jetdirect print server to select whichever mode is the fastest. If you know which parallel mode is the fastest, select it; otherwise, leave this option set to the default.

NOTE: You can only access this option through utilities such as HP Web Jetadmin.

To configure this option, select one of the parallel mode options.

- **nACK and Busy**: Device checks both the nACK and Busy lines. This is the most reliable because no data is lost in transfer, but it is the slowest for network communication.
- **nACK only**: Faster than nACK and Busy but not quite as reliable.
- **Busy only**: Fastest for network communication but also the least reliable.

Parallel Mode

This option specifies the parallel mode that the HP Jetdirect EX print server uses. If the specified mode does not work, the HP Jetdirect print server tries other modes until it finds one that does work. The default option tells the HP Jetdirect print server to select whichever mode is the fastest. If you know which parallel mode is the fastest, select it; otherwise, leave this option set to the default.

NOTE: You can only access this option through utilities such as HP Web Jetadmin.

To set the parallel mode, select one of the options:

- **Bi-Directional (Jetdirect EX)**: A parallel connection that supports bidirectional communications.
- **Centronics (Jetdirect EX)**: A standard parallel connection that transfers data in one direction only (to the printer).
- **Automatic**: Select the fastest mode (default).
- **Multiple Logical Channels (MLC)**: A bidirectional parallel connection (IEEE-1284) that supports an enhanced capabilities port.

Phone Home Privacy Setting

This feature allows you to control whether HP may collect statistical data on product use. By allowing HP to collect this information, improved product features and services can be provided in the future. HP will not collect network-specific or personal data. For information on HP privacy policies, read the HP Online Privacy Statement available by clicking privacy statement at www.hp.com in your language. For HP to collect any information, Internet access must be available. If you enable this feature, information collected by HP will be limited to the following items:

- HP Jetdirect product number.
- Firmware version and manufacturing date.
- Model number of the attached printer or device.
- Web browser and operating system detected.
- Local language selections used for viewing.
- Web pages Network communications protocols enabled.
- Network management interfaces enabled.
- Device discovery protocols enabled.
- Printing protocols enabled.
- TCP/IP configuration methods enabled.
- SNMP control methods enabled.
- Wireless configuration methods enabled.

To allow HP to collect data on the use of this product, select the check box. To disable this feature, clear the check box.

Protocol Stacks

This option lets you enable or disable the various protocol stacks on the HP Jetdirect print server. Many networks only use a few protocols. For example, the AppleTalk and DLC protocols are enabled by default on HP Jetdirect print servers, but many networks do not use them. Although leaving unused protocols active will not harm the network, you might gain the following benefits if you disable them:

- A slight improvement in network performance.
- An additional measure of security and control because each user must access the HP Jetdirect print services centrally instead of establishing a direct connection. For example, a Macintosh user cannot set up a direct AppleTalk connection with the printer, but the user can access centralized print services through TCP/IP or IPX/SPX.

To enable a protocol stack, select the check box next to the protocol stack. To disable a protocol stack, clear the check box next to the protocol stack.

Scan Idle Timeout

This option lets you specify how long the printer waits before closing an idle connection and going to the next print job. If your network is busy, there may be a delay in the packet transmissions. In this case, you might want to specify a longer timeout value.

To assign or change the scan idle timeout, type the timeout value in seconds in the text field.

SNMP Trap Destination Table

HP Web Jetadmin runs a background trap-server utility that is used to receive HP Jetdirect traps and alerts, and can route alert notifications to email addresses. However, some networks may require that specific network servers and management applications receive SNMP traps. This feature allows you to specify different trap-management servers along with the use of special trap community names and supported SNMP agents. Specified trap servers are stored in a Trap Destination Table on the print server. The number of trap servers that can be configured (typically 3, 5, 10, or 12) depends on the print server model. A trap server is specified by its IP address and/or its Fully Qualified Domain Name (FQDN), and a TCP/IP port number used by a management application on the server (a trap server port number). If a port number is not specified, the default port 162 is used. The print server can be configured to use a standard SNMPv1 or SNMPv2c agent, or an optional SNMPv2c Inform agent that requires an acknowledgement from the trap server. The agent selected remains configured when the print server is powered off/on. The default agent is SNMPv1. A trap community name can be specified for the SNMP agent to use when sending traps. By default, the trap community name is “public”. If the Trap Destination Table is empty, traps are not sent unless enabled through HP Web Jetadmin running its background trap-server utility. Because trap objects (or pre-defined events) are encoded in each device, the available traps depend on the particular HP Jetdirect print server model and its current firmware version.

Some newer HP devices do not use SNMP to generate alerts through HP Web Jetadmin. For these devices, changing the **SNMP Trap Destination Table** configuration option does not affect alerts. You must manage alerts for these devices by using the Alerts feature in HP Web Jetadmin.

Use the following steps to configure this option:

1. Select one of the following actions:
   - **Clear All**: Clears all trap table entries.
   - **Clear Slot #**: Clears the specified trap table entry number, if it exists.
   - **Clear Any**: Clears any trap table entry matching the specified parameters:
     - If only IP or Fully Qualified Domain Name (FQDN) is specified, all entries with the matching value are cleared.
     - If a port is specified, only the entry matching that IP and FQDN and port is cleared.
   - **Replace Slot #**: Replaces the existing trap table entry for that slot, if it exists.
     - If a device does not support that slot, no action will be taken.
     - If only an IP or FQDN is specified, the default port 162 is used.
   - **Add Any**: Adds the specified entry to the next available slot.
     - If only an IP or FQDN is specified, the default port 162 is used.
     - If the trap table is full, an error will be displayed.

   ⚠ CAUTION: Clearing or replacing trap table entries may cause other applications using those entries to function incorrectly.

2. Enter the IP address of the desired trap server (to save or clear) in **IP Address**, or enter the FQDN in **FQDN**.

   NOTE: **FQDN** is shown only when FQDN is supported by the print server.

3. If required by the trap server:

- Specify a TCP/IP port number for the management application in **Port number**.
- Select an SNMP agent version from the **Version** drop-down list.
- Specify a trap community name in **Community** (up to 255 alphanumeric and special characters).

Support Contact

Use this option to specify the name of the person that users can contact for device support.

Support Phone Number

Use this option to specify the phone number of the person defined for the **Support Contact** configuration option.

System Contact

The system contact is the name of the person who owns or is responsible for the device. HP Web Jetadmin displays the system contact on the device **Status** page and on several of the device lists. The system contact is useful when you need to dispatch repair personnel, have questions about device settings or usage, or need to report a problem with a device. You can also search for and display a list of all of the devices that a particular person is responsible for.

To assign or change the system contact, type the name of the person to contact in **System Contact**.

System Location

This option identifies the system based on its location.

Type or change the device location in **System Location**.

System Log Server

This option lets you specify the IP address of the server where you want the HP Jetdirect print server to send system log messages. System log messages identify, for example, when the HP Jetdirect print server was turned on or when a printer problem occurred.

To assign the system log server, type the IP address of the system log server in the text box.

System Log Server Info – More Settings

Use this option to configure the settings that the HP Jetdirect print server uses to send system log messages to a Syslog server. System log message identify events that occur on the printer, such as when the HP Jetdirect print server is turned on or when a problem occurs.

If the printer has received Common Criteria Certification (CCC), advanced security logging events are available. If CCC logging is enabled, the HP Jetdirect print server also sends the CCC log messages to the Syslog server.

Use the following steps to configure the settings:

1. To use TCP to send system log messages to the Syslog server, select the **TCP** option.

   IMPORTANT: If the **Enable CCC Logging** checkbox is selected, select the **TCP** option to ensure that audit events are reliably delivered to the Syslog server.

   -or-

   To use UDP to send system log messages to the Syslog server, select the **UDP** option.

2. In the **SysLog Port** box, enter the port that the HP Jetdirect print server uses to send the system log messages. The default is port 514 for both the TCP and UDP protocols.

3. In the **Syslog Maximum Messages** box, enter the maximum number of system log messages that can be sent per minute. Valid values are from 0 to 1000. The default value is 10.

4. In the **Syslog Priority** box, enter one of the following values to define the severity of the system log messages that are sent:

   - 0—Emergency. The system is unusable.
   - 1—Alert. Action must be taken immediately.
   - 2—Critical. A critical condition occurred.
   - 3—Error. An error condition occurred.
   - 4—Warning. A warning condition occurred.
   - 5—Notice. A normal but significant condition occurred.
   - 6—Informational. Informational messages.
   - 7—Debug. Debug-level messages.
   - 8—Disable. System log messages are queued internally for logging at a later time.

5. To enable CCC logging, select the **Enable CCC Logging** checkbox.

   IMPORTANT: Before CCC logging can be enabled, the IP address for the Syslog server must be configured by using the **System Log Server Info** configuration option.

   -or-

   To disable CCC logging, clear the **Enable CCC Logging** checkbox.

System Name

This option lets you specify the system name, sometimes called the host name, for the HP Jetdirect print server. You might want to specify the system name for the HP Jetdirect print server for a variety of reasons, such as the following example:

- The system name is a static name that is saved on the HP Jetdirect print server. Use the system name to identify and track devices on the network. You can also include the system name as a column in device list views. Under some conditions, the system name is visible on the network or the IP name can be resolved through network name services. This typically occurs in a DHCP environment.

NOTE: This option does not change the DNS server entries. If you want to view the system name on the network, you must update network name services, such as DNS, with name and address data.

NOTE: You can only apply this configuration option to a single device. You cannot use this configuration option to configure multiple devices at one time or include this configuration option in a template.

To configure this option, type the host name in **System Name**.

TCP Idle Timeout

This option lets you specify how long TCP/IP stays open when there is no traffic. If the network is busy, there may be a delay in the packet transmissions. In this case, you might want to specify a longer timeout value.

To assign or change the TCP idle timeout, type the timeout value in seconds in the text box.

TCP/IP Configuration Method

This option lets you specify how the HP Jetdirect print server obtains its TCP/IP configuration. This is a quick method for resetting the IP stack on the HP Jetdirect print server, forcing it to try and obtain an IP configuration through BOOTP or DHCP.

NOTE: The current HP Jetdirect print server TCP/IP configuration is erased.

- **BOOTP Server**: Forces the HP Jetdirect print server to obtain its TCP/IP configuration on the network through a BOOTP server, if one exists and if the print server configuration parameters have been defined. When you save the configuration, the HP Jetdirect print server immediately resets its IP address to 0.0.0.0. If a BOOTP configuration does not occur within a short period of time, the IP address defaults to 192.0.0.192.
- **DHCP Server**: Forces the HP Jetdirect print server to obtain its TCP/IP configuration on the network through a DHCP server, if one exists and if the print server configuration parameters have been defined. When you save the configuration, the print server immediately resets its IP address to 0.0.0.0. If a DHCP configuration does not occur within a short period of time, the IP address defaults to 192.0.0.192.
- **Auto IP**: Automatically configure the IP address.

To reconfigure the HP Jetdirect print server, select the configuration method option.

TCP/IP Domain Suffix

Use this option to add domain suffixes to the **DNS suffixes** list, which is a list of domain names for the printer. The **DNS suffixes** list may contain up to 31 entries. Each suffix can have up to 255 letters, numbers, or dots. If you remove all entries from the **DNS suffixes** list, all suffixes are removed from the device as well.

Use the following steps to configure this option:

1. To add a new suffix, type the new suffix in **Suffix name** and click **Add Suffix**.
2. To remove a suffix from the **DNS suffixes** list, select the suffix and click **Remove**. To remove all suffixes from this list, click **Remove All**. You do not have to select any suffixes if you are removing all entries in the list.

Upload CA Certificate

Use this option to upload a certificate authority (CA) certificate to the network interface card (NIC) on the device. You can upload root CA certificates and intermediate CA certificates. You cannot upload user certificates.

An intermediate CA is a subordinate of a root CA. An intermediate CA is capable of signing and issuing identity certificates. The result is a certificate chain that begins at the root CA and ends with identity certificates. Intermediate CAs provide an added level of security that reduces the risk of the root CA being compromised.

Federal Information Processing Standard (FIPS) supports only CA certificates that are signed by using the SHA-1 authentication protocol or later. To upload CA certificates when FIPS mode is enabled on the device, the CA certificates must be signed by using SHA-1 or later. If you upload a CA certificate that is signed by using the MD5 authentication protocol or earlier (MD2 or MD4) or is in the PFX format with the RC4 Message Authentication Code (MAC) verification, the configuration fails.

Use the following steps to configure this option:

1. Click the **Browse** button, navigate to and select the CA certificate, and then click the **Open** button.
2. For a root CA certificate, clear the **Allow Intermediate CA certificate** checkbox.

   -or-

   For an intermediate CA certificate, select the **Allow Intermediate CA certificate** checkbox.

⚠ CAUTION: If an intermediate CA certificate is installed, the scope of authentication is limited.

Upload Jetdirect Certificate

Use this option to upload a valid HP Jetdirect certificate to the authentication server and copy the certificate to the device. Some organizations require secure authentication for their devices. You can upload the HP Jetdirect certificate remotely to meet the security needs of your organization.

Federal Information Processing Standard (FIPS) supports only HP Jetdirect certificates that are signed by using the SHA-1 authentication protocol or later. To upload HP Jetdirect certificates when FIPS mode is enabled on the device, the HP Jetdirect certificates must be signed by using SHA-1 or later. If you upload an HP Jetdirect certificate that is signed by using the MD5 authentication protocol or earlier (MD2 or MD4) or is in the PFX format with the RC4 Message Authentication Code (MAC) verification, the configuration fails.

Use the following steps to configure this option:

1. Click the **Browse** button.
2. On the **Open** window, navigate to and select the certificate file, and then click the **Open** button.
3. In the **Password** box, enter the password for the HP Jetdirect certificate.

Web Services Print

Use this option to enable or disable the Microsoft Web Services for Devices (WSD) Print services supported on the HP Jetdirect print server.

Enable or disable this option and then click **Apply**.

WINS Server

Use this feature to specify the IP address of a primary Windows Internet Naming Service (WINS) server for this device. A secondary WINS server may also be specified, if supported by the device, for use when the primary WINS server is not available. Devices on IP networks actually use IP addresses for communications. A WINS server provides name resolution services, that is, it translates between user-friendly host names and IP addresses for each network computer or device. A WINS server employs a distributed database of host names and associated IP addresses. The database is automatically updated dynamically so that host name and IP address resolution is always current.

Use the following steps to configure this option:

1. Enter the IP address of the primary WINS server in **Primary WINS server IP**.
2. Enter the IP address of the secondary WINS server in **Secondary WINS server IP**.

NOTE: Some devices may not support configuration for a secondary WINS server.

Device Configuration Options for Projector

Configuration options for Projector define functions specific to projectors.

Auto-search

When **Auto Search enabled** is checked, the projector will automatically search for a device connected to it.

Auto-sync VGA

When this option is selected, the device will automatically sync up its resolution with the incoming device.

Power

This option lets you remotely change the power level of the device. **Standby** uses less power while **Lamp On** will set the projector so it can be used.

Requested Source

This option lets you specify what video standard source the projector will use for its source. You can also specify the projector to scan for any attached source, and select the source from the drop-down list.

Device Configuration Options for Security

Configuration options for Security define functions for the device including authentication methods and access.

802.1X Authentication

Use this option to specify the 802.1X authentication settings on the HP Jetdirect print server required for client authentication on the network. You can also use this option to reset the 802.1X authentication settings to the factory-default values.

⚠ CAUTION: Use caution when changing the 802.1X authentication settings. You might lose the connection. If communication with the device is lost, you might need to reset the device server to a factory-default state, and then reinstall the device.

For most 802.1X networks, the infrastructure components, such as LAN switches, must use 802.1X protocols to control a port's access to the network. If these ports do not allow partial or guest access, you might need to configure the print server with the 802.1X parameters prior to connecting to the network. To configure the initial 802.1X settings before connecting to the network, you can use an isolated LAN or a direct computer connection using a crossover cable. The supported 802.1X authentication protocols and associated configuration depend on the print server model and firmware version.

Use the following steps to configure this option:

1. Select the supported protocols that are used for 802.1X authentication on the network.

   - **PEAP (configure certificate first)**: Protected Extensible Authentication Protocol (PEAP) uses digital certificates for network server authentication and passwords for client authentication. PEAP requires an EAP user name, EAP password, and Certificate Authority (CA) certificate. Dynamic encryption keys are also used.

   - **EAP-TLS (configure certificate first)**: Extensible Authentication Protocol using Transport Layer Security (EAP-TLS) is a mutual authentication protocol based on digital certificates for authentication of the client and network server. EAP-TLS requires an EAP user name, HP Jetdirect certificate, and CA certificate. Dynamic encryption keys are also used.

2. In the **User name** text box, enter the EAP/802.1X user name for the device (maximum of 128 characters). The default user name is the default hostname of the print server, NPIxxxxxx, where xxxxxx is the last six digits of the LAN hardware (MAC) address.

3. In the **Password** text box, enter the EAP/802.1X password for the device (maximum of 128 characters).

4. In the **Confirm password** text box, enter the password again.

5. In the **Server ID** text box, enter the server ID that identifies and validates the authentication server. The server ID is specified on the digital certificate that a trusted CA issued for the authentication server.

   NOTE: If the **Require Exact Match** checkbox is not selected, you can specify any string for the server ID.

6. To validate the server ID that is specified in the **Server ID** box against the server ID that is specified in the digital certificate issued by the CA for the authentication server, select the **Require Exact Match** checkbox.

7. In the **On Authentication Failure** section, select one of the following options:

   - **Connect Anyway (802.1x Fail-over)**: If this option is selected and the 802.1X authentication settings are applied to an unsecured port, the device does not lose connectivity if you do not change from an unsecured port to a secured port on the device. The device connectivity functions without 802.1X authentication.

   - **Block Network (Secure failure)**: If this option is selected and the 802.1X authentication settings are applied to an unsecured port, the device enters a communication error status if you do not change from an unsecured port to a secured port on the device. To return the device to a ready state, change to a secured port on the device.

8. From the **Encryption strength** list, select the level of encryption for the selected protocols.

   Federal Information Processing Standard (FIPS) supports only the **High** encryption strength. To configure the encryption strength when FIPS mode is enabled on the device, you must specify the **High** encryption strength. If you specify the **Low** or **Medium** encryption strength, the configuration fails.

9. To initialize the port, select the **Re-authenticate on apply** checkbox. The device re-authenticates the 802.1X settings after they are applied.

Access Control for Device Functions

Use this option to specify the sign-in method that is required to access applications from the device control panel and enable or disable access to the applications by using the built-in permission sets. The sign-in methods and applications that are available vary depending on the device.

You can create custom permission sets. You can then use these custom permission sets to restrict access to the applications.

Signed-in users cannot be more restricted than guest users. If signed-in users are restricted from accessing applications, guest users are also restricted from accessing those applications.

You can specify the default sign-in method that is required to access all of the applications. You can then specify a different sign-in method for individual applications. You must enable and configure the sign-in methods on the device. For example, to select Windows as the sign-in method, you must enable and configure the **Windows Sign In Setup** configuration option on the device.

The following are examples of the sign-in methods that might be available for a device:

- Local Device

  The Local Device sign-in method is always available, regardless of whether or not the method is enabled. When a user accesses the device, the device prompts the user to enter a device PIN only if the Local Device sign-in method is enabled and configured.

- Windows
- LDAP
- Smart Card

  If an HP Smart Card Reader is installed, users must sign-in. You should disable all of the other sign-in methods. You might need to install certificates separately to support this configuration.

If the **Restrict Color** configuration option has been used to enable or disable color printing and copying for all of the HP Web Jetadmin users, the device ignores any color printing and copying settings that are enabled for the permission sets here.

Based on what’s selected in the Applications Group drop-down list, it displays the supported applications for Control Panel or EWS.

Manage permission sets

The default permission sets that are available vary depending on the device.

1. Use the following steps to create a permission set:

   a. Click the **Create** button.

   b. On the **Create Permission Set** window, enter a name for the permission set, and then click the **OK** button.

      The new permission set is added as a column to the table in the **Access control for device applications** section.

2. Use the following steps to edit a permission set:

   NOTE: You cannot edit the **Device Administrator**, **Device Guest**, and **Device User** permission sets.

   a. Select the permission set from the list, and then click the **Edit** button.

   b. On the **Edit Permission Set** window, enter a new name for the permission set, and then click the **OK** button.

3. Use the following steps to delete a permission set:

   NOTE: You cannot delete the **Device Administrator**, **Device Guest**, and **Device User** permission sets.

   a. Select the permission sets from the list, and then click the **Delete** button.

   b. On the **Delete Permission Set** window, verify that the information is correct, and then click the **OK** button.

4. Use the following steps to copy a permission set:

   a. Select the permission set from the list, and then click the **Copy** button.

   b. On the **Copy Permission Set** window, enter a name for the new permission set, and then click the **OK** button.

5. If you are configuring multiple devices or creating device configuration templates, select one of the following options from the **Overwrite options** section:

   - **Replace/overwrite existing lists**: Replaces any existing permission sets on the devices with this list of permission sets.

   - **Append to existing lists**: Adds this list of permission sets to the existing permission sets on the devices.

     To update permission sets on devices that have the same name as the permission sets on this list, select the **Overwrite any existing items with the same name** checkbox.

Configure the access for device applications

1. From the **Default sign in method** list, select the sign-in method for all of the applications.

2. To assign a sign-in method to an application that is different from the default, select the sign-in method from the list next to the application.

3. Use the following steps to configure the access for an application:

   a. Scroll to the application in the list.

   b. To enable access to the application, select the checkbox for the permission set.

      -or-

      To disable access to the application, clear the checkbox for the permission set.

4. To allow users to select an alternate sign-in method from the control panel, select the **Allow users to choose alternate sign-in methods** checkbox.

   -or-

   To require users to use the sign-in method that is specified for each application, clear the **Allow users to choose alternate sign-in methods** checkbox.

5. To automatically sign out users when a job starts, select the **Automatically sign users out after starting each job** checkbox. The user must sign in again to start another job.

   -or-

   To leave users signed in when a job starts, clear the **Automatically sign users out after starting each job** checkbox. Users remain signed in until they sign out or their session times out.

Create device configuration templates for devices that have new or custom sign-in methods

Some devices have new or custom sign-in methods installed that are not available on the **Access Control for Device Functions** configuration option. To create device configuration templates and configure this option for these devices, perform the following steps:

1. From the device list, select a single device that has a custom sign-in method installed.
2. Click the **Config** tab, expand the **Security** category, and then select the **Access Control for Device Functions** configuration option.
3. Verify that the custom sign-in method appears in the **Default sign in method** list.
4. Specify the appropriate settings for the device.
5. Click the **Apply** button.
6. On the **Confirm** window, verify that the information is correct, and then click the **Configure Devices** button.
7. On the **Results** page, click the **Done** button.

Access Control Level for Device Functions

Use this configuration option to set the access control levels for the device. A different authentication method and security level can be assigned to each device function. You can reduce costs and increase security by only allowing users access to the minimum set of device functions necessary for your organization's operational needs.

Use the following steps to configure this option:

1. Set the access control level for device functions:
   - **Maximum**: Require sign-in before any device features can be accessed.
   - **Minimum**: Allow unauthenticated access to all device features except **Service Mode**.

     NOTE: If you selected **Minimum**, you do not need to define permission sets.
   - **Custom**: Require sign-in for selected device features.
2. If you choose **Maximum** or **Custom** access control level, you need to define one or more permission sets. The permission sets control which device features a member of the defined group has access to. To create a permission set, click **Add** and type the new permission set name in **Permission set name** and then define which functions should require signing.
3. After a permission set has been created, you can edit it; select the permission set in **Permission sets** and then click **Edit**.
4. To delete a permission set, select the permission set in the **Permission sets** box and then click **Delete**.

Access Control List

An access control list (ACL) is used to specify the IP addresses on your network that are allowed access to the device. The list supports up to 10 entries. If the list is empty, then any system is allowed access. By default, host systems with HTTP connections (such as Web browser or Internet Printing Protocol connections) are allowed access regardless of access control list entries. This allows hosts to access the device when Proxy Servers or Network Address Translators are used. However, unfiltered access by HTTP hosts may be disabled by clearing the **Check ACL for HTTP** check box.

⚠ CAUTION: You may lose your ability to communicate with the device if your system is not properly specified in the list, or access through HTTP is disabled. If communication with the device is lost, restoring network settings to factory-default values may be required.

The access control list (ACL) is normally used for security purposes. Network administrators can configure the device to limit which systems or management stations have access to the device. The device will block communications from systems that are not configured for access.

Host systems to be allowed access are specified by their IP host or network address. If the network contains subnets, an address mask may be used to specify whether the IP Address entry is for an individual host system or a group of host systems. For an individual host system, the mask 255.255.255.255 is assumed and is not required.

To add an entry into the **Access Control List**:

1. Enter an IP address in **IP Address**.
2. To identify whether the IP address entry is an individual host or a group of hosts, enter a subnet mask in **Mask**.

NOTE: The first item in the ACL must be the IP address of the HP Web Jetadmin server or an IP address with a wide subnet mask that includes the IP address of the HP Web Jetadmin server.

To delete entries from the **Access Control List** for batch and template configuration, click **Clear all ACL Table entries**.

Authenticate LDAP and Kerberos Without Email

Use this option to enable or disable the Kerberos and LDAP Authentication functions that allow users to sign in to the servers even if they do not have an email address.

To enable authentication without an email address, select the appropriate checkboxes. Users who do not have a published email address on the LDAP or Kerberos server can sign in by using their username and password, and then authenticate successfully.

To disable authentication without an email address, clear the appropriate checkboxes. Users who do not have a published email address on the LDAP or Kerberos server cannot sign in and authenticate successfully.

Authentication Manager

Use this option to set the authentication method used to access the device and various functions on the device. The authentication methods are **HP Digital Send Service**, **Group 1 PIN**, **Group 2 PIN**, **User PIN**, **LDAP**, and **Kerberos**. The device functions include **Copy**, **Send email**, **Send fax**, **Send to folder**, **HP Digital Send Service workflow**, and so on. If another device function becomes available through a third-party installation, that function appears in the function list and you can enable an authentication method for it.

Automatic Update

Use this option to enable or disable Automatic Update in the device control panel. This is a one-time setting, and it can be configured after a cold reset.

1. Select the check box.
2. To enable Automatic Update, select the **Enabled** option.

   -or-

   To disable Automatic Update, select the **Disabled** option.
3. Click the **Apply** button.

Bootloader Password

This option lets you configure a password on the bootloader screens for a device. This keeps the user from making any changes when the device first boots up. The **Bootloader PIN** keeps users from changing the Bootloader Password. You can enter a new 4 digit PIN (or enter the existing 4 digit PIN if it had been set previously) and then enter the Bootloader Password itself.

NOTE: If you forget the **Bootloader PIN**, the Bootloader password can not be changed and could only be cleared (along with the Bootloader PIN) via a service call.

Color Access Control

Use this option to manage the usage of color printing supplies within your organization. If you select **Color permissions**, you can also specify which users (up to 50) have permission to print in color on a device or you can import a permission configuration file to set the permissions. This feature also lets you specify which applications have permission to print in color on a device (up to 10) or you can import a permission configuration file to set the permissions.

Use the following steps to configure this option:

1. Select one of the available permissions:
   - **Enable Color**: All color jobs will print in color.
   - **Disable Color**: All color jobs will print in black.
   - **Color permissions**: Requires the device to check the permissions defined for the user (up to 50) and the application to determine if the job can be printed in color. If either the user or the application has "black-only" permission, then the job is printed without color.

   NOTE: If you select this option, be sure to set the user and application permissions to control access to color printing features.
2. If you selected **Color permissions**, you can now restrict color user permissions.
   - To specify the default user permission, select an option from **Color permission**.
   - To look up a user, click **Locate Name**. You can search for users by object or location.
   - To add a user to the permissions list, type the name of the user in **System User Name** and then select a permission from **Permission**.

     NOTE: This list can contain up to 50 users.
   - To edit the permissions for a user on the list, click on the user name in the list and then select a permission from **Permission**.

- To delete a user from **Permissions**, select a user name entry on the list by clicking on it and then click **Delete**.
- To import a permissions configuration file, click **Browse** and search for a configuration file to import.

  NOTE: The file is imported when the changes to the device(s) are saved.

3. You can also specify the default application permission.
   - To add an application to the permissions list, type the name of the application in **Technical Application Name** and then select a permission from **Permission**.

     NOTE: This list can contain up to ten applications.

   - To edit the permissions for an application on the list, click on the application name entry and select a permission from **Permission**.
   - To delete an application from the permissions list, click on an application name entry on the list.
   - To import a permissions configuration file, click **Browse** and search for a configuration file to import.

     NOTE: The file is imported when the changes to the device(s) are saved.

Color Access Control Level

Use this option to specify whether to allow jobs to print in color. The **On** setting allows all color jobs to print in color. The **Custom access control** setting requires the device to check the permissions defined for the user and the application to determine whether each job will be printed in color or not. If either the user or the application has “black-only” permission, then the job will be printed without color. The **Off** setting will result in all color jobs printing in black.

The driver used for printing must be an HP print driver because the printer relies on the print driver to tell it who is printing and from which application. The print drivers that ship with Microsoft Windows do not support this functionality.

The EWS page for the device has a job log that lists who has printed and from what application. This log can be accessed in order to find out the application and user name that needs to be entered into this configuration option in order to restrict the user or application.

To configure this option, select one of the available settings.

Control Panel Access

This option allows you to lock the device control panel, preventing unauthorized users from accessing it and changing the device settings. Users can still read the settings on the device’s control panel. The unlock options that are available depend on the device. For some devices, you can only lock and unlock the control panel. For other devices, you can specify the level of access: minimum, moderate, or maximum. The definitions for the different levels of access also depend on the device. If you install a printer in a public area, you might require additional security. Locking the device control panel prevents unauthorized users from accessing the device settings either at the device or though a software utility that provides control panel access.

To prevent users from changing device settings, select the appropriate lock option. To let users change device settings, select **Unlock**.

Control Panel Shortcuts

Use this option to specify the shortcuts that appear in the Shortcuts folder on the device control panel and specify the order in which the shortcuts appear in the Shortcuts folder.

1. To show a shortcut in the Shortcuts folder, select the checkbox next to the feature name.

   -or-

   To remove a shortcut from the Shortcuts folder, clear the checkbox next to the feature name.

2. To move a shortcut up in the list, select the feature name, and then click the **Move up** or **Move to top** button. On the device control panel, the shortcut moves to the left in the list.

3. To move a shortcut down in the list, select the feature name, and then click the **Move down** or **Move to bottom** button. On the device control panel, the shortcut moves to the right in the list.

Default Sign In Method

This option lets you specify the sign in method for accessing the device. You should select the method that best suits the needs of your organization. You can choose a local sign in or alternative sign in methods such as a user's Windows login.

NOTE: The sign in options may vary depending on installed plug-in solutions and other accessories, such as Smart Card readers.

To configure this setting, select an option from the drop-down list.

Device Announcement Agent

The device announcement agent provides automatic configuration out of the box with no administrator intervention. When the device is turned on, the device sends an announcement to the configuration server, and then the configuration server pushes the configuration settings to the device. This feature is enabled by default and requires a configuration server, such as HP Imaging and Printing Security Center.

Use this option to specify the settings for the device announcement agent that the device uses to announce its presence to the configuration server. By default, the device announcement agent uses the DNS hostname hp-print-mgmt to locate the configuration server. Authentication between the device and configuration server is not required.

Use the following steps to configure this option:

1. Select the **Enable Device Announcement Agent** checkbox.

2. To override the default DNS hostname or if a DNS server is not available, enter the IP address of the configuration server that the device announcement agent uses in the **Configuration Server IP Address (v4/v6)** text box.

3. To enable authentication of the device announcement agent, select the **Require Mutual Authentication via Certificates** checkbox. This is the most secure configuration method because certificates must be installed and trusted on the device and on the configuration server.

   -or-

   To disable authentication of the device announcement agent, clear the **Require Mutual Authentication via Certificates** checkbox.

Device User Accounts

A permission set establishes the access level for various device functions, such as the ability to print in color, cancel jobs, and edit fax speed dial numbers. Devices support the predefined Device Administrator and Device User permission sets. To create custom permission sets, use the **Access Control Level for Device Functions** configuration option.

Use this option to specify the default permission set that is applied to new device user accounts on the device.

To configure this option, select the permission set from the list.

To create device user accounts by using the HP Embedded Web Server (EWS) on the device, perform the following steps:

1. Click the **Security** tab.
2. In the left pane, click the **Access Control** link.
3. Scroll down to the **Device User Accounts** section, and then click the **New** button.
4. On the **New Device User Account** page, specify the information, and then click the **OK** button.

Device user accounts can act as address book entries depending on which fields are populated. For a fleet configuration of device user accounts, use the import/export features that are available in the EWS on the device and in HP Web Jetadmin. If you are not familiar with the CSV format that is used to import files, HP recommends that you use the EWS on the device to configure the device user accounts, and export the device user accounts to a CSV file. Then use the **Import/Export Address Book** configuration option in HP Web Jetadmin to import the CSV file, and set the device user accounts on multiple devices simultaneously. The **Import/Export Address Book** configuration option is available in the **Config** tab > **Digital Setting** category.

Digital Sending Service

The Digital Sending Service is an independent HP product that allows you to configure digital sending. If you select the **Allow use of digital send service** checkbox, the Digital Sending Service manages the device. If you select the **Allow transfer to new digital send service** checkbox, any Digital Sending Service can manage the device, even if another Digital Sending Service is currently managing the device.

Disable Direct Ports

Checking the disable direct ports makes the device more secure but it only allows printing through the network connection. If this option is selected, the device must be rebooted afterwards.

Display Color Usage Job Log Page On Information Tab

Use this option to display the **Display Color Usage Job Log Page On Information Tab** of the device Embedded Web Server.

Enable or disable this option and then click **Apply**.

Display Options on Information Tab

Use this option to enable or disable the options that appear on the **Information** tab in the HP Embedded Web Server (EWS) on the device.

To configure this option, perform the following steps:

1. To enable the **Print** option, select the **Display Print Page on Information Tab** checkbox.

   -or-

   To disable the **Print** option, clear the **Display Print Page on Information Tab** checkbox.

2. To enable the **Job Log** option, select the **Display Job Log on Information Tab** checkbox.

   -or-

   To disable the **Job Log** option, clear the **Display Job Log on Information Tab** checkbox.

Embedded Web Server Password

If you are concerned about security, specify a password for the Embedded Web Server configuration.

NOTE: When setting a password on the device, you must enter the current password, if any, regardless of credentials stored in the application. If you don't, the setting will fail as "Invalid Data".

To assign the password, type it in **Password**. Type the same password in **Confirm password**. To change the password, type it in **Current EWS password**. Type the same password in **Confirm password**.

Enable Host USB plug and play

Use this option to enable or disable the USB Plug and Play feature on the device. The USB Plug and Play feature is used to perform tasks such as scanning to a USB flash drive.

NOTE: If this option is disabled, control-panel applications that require the USB Plug and Play feature, such as the **Save To USB** application, are automatically disabled.

To enable the USB Plug and Play feature, select the **Enabled** option.

-or-

To disable the USB Plug and Play feature, select the **Disabled** option.

Enable PJL Device Access Commands

HP Printer Job Language (PJL) is a command language that can be used to request information from printers (for example, printer model, configuration settings, and status) and change the configuration settings on printers.

Use this option to enable or disable PJL commands on the printer.

To allow users to send PJL commands to the printer, select the **Enabled** option.

NOTE: If the **Enabled** option is selected for non-HP FutureSmart devices, be aware of the following issues:

- Disk jobs can no longer be deleted by using the **Erase Customer Data** button on the **Storage** tab.
- If the **Printer Wakeup** configuration option is enabled, this feature might not work.

-or-

To prevent users from sending PJL commands to the printer, select the **Disabled** option.

Encrypt all web communication

This option lets you to enable or disable the HP Jetdirect card to encrypt any information coming from the device.

Select **Enabled** to encrypt information or **Disabled** to not encrypt information.

Encryption Strength

Use this option to specify the SSL encryption strength. If encryption is enabled, ciphers display the weakest cipher allowed for the encryption strength specified.

Federal Information Processing Standard (FIPS) supports only the **High** encryption strength. To configure the encryption strength when FIPS mode is enabled on the device, you must specify the **High** encryption strength. If you specify the **Low** or **Medium** encryption strength, the configuration fails.

To configure this option, select the encryption strength from the list.

EWS Information Protection

Use this option to enable or disable protection for the **Information** tab on the device Embedded Web Server (EWS) page.

If the **Enabled** option is selected and an EWS password is configured on the device, users cannot access the **Information** tab on the EWS without logging in with the EWS device password.

If the **Disabled** option is selected and an EWS password is configured on the device, users can access the **Information** tab without logging in with the EWS device password. To access all the other tabs on the EWS page, users must log in with the EWS password.

FIPS-140 Mode

Use this option to enable or disable the Federal Information Processing Standard (FIPS) mode on the device. FIPS mode enforces the use of cryptographic suites and protocols that comply with the FIPS-140 standards for computer security. FIPS supports the following protocols for the configuration options on the device:

- **SNMP Version Access Control** configuration option: SHA-1 authentication protocol and AES-128 privacy protocol
- **Kerberos** setting on the **IPsec/Firewall Policy** configuration option: AES128-SHA1 and AES256-SHA1 protocols
- **Upload Jetdirect Certificate** configuration option: Certificates that are signed by using SHA-1 or later
- **Upload CA Certificate** configuration option: Certificates that are signed by using SHA-1 or later
- **Mgmt Protocol** configuration option: TLS 1.2, TLS 1.1, or TLS 1.0

Enable FIPS mode

▲ Select the **Enabled** option.

⚠ CAUTION: The enable configuration fails if the following non-FIPS protocols are configured on the device:

- **SNMP Version Access Control** configuration option: MD5 authentication protocol and DES privacy protocol
- **Kerberos** setting on the **IPsec/Firewall Policy** configuration option: DES-CBC-MD5 algorithm
- **Upload Jetdirect Certificate** configuration option: Certificates that are signed by using MD5 or earlier (MD2 or MD4)
- **Upload CA Certificate** configuration option: Certificate that are signed by using MD5 or earlier (MD2 or MD4)
- **Mgmt Protocol** configuration option: SSL 3.0 or earlier

Disable FIPS mode

▲ Select the **Disabled** option.

Get Community Name

The Get Community Name password can be set to prevent unauthorized people from using SNMP utilities to access a device and get the device settings.

Use the following steps to configure this option:

1. Type the password and then repeat it for confirmation.
2. To disable the `public` Get Community Name, select **Disable SNMPv1/v2 default Get Community Name of 'public'**. If a device does not support this option, it will ignore it in batch configurations or when applying templates.

Group 1 PIN

This option enables you to force users to use a pin to access a device. You can then use the Authentication Manager function to specify what features (such as walk-up, copy, send, fax) are restricted by this. You can have two different groups, each with a unique pin.

To set this option, type the PIN and then type it again for confirmation.

Group 2 PIN

This option enables you to force users to use a pin to access a device. You can then use the Authentication Manager function to specify what features (such as walk-up, copy, send, fax) are restricted by this. You can have two different groups, each with a unique pin.

To set this option, type the PIN and then type it again for confirmation.

IPsec/Firewall Policy

(Full-featured HP Jetdirect print servers only) The Firewall and Internet Protocol security (IPsec) features provide network-layer security on both IPv4 and IPv6 networks. The Firewall provides simple control of which IP addresses are allowed access. IPsec (RFC 2401) provides the additional security benefits of authentication and encryption.

IPsec configuration is relatively complex. However, because IPsec provides security at the network layer and can be relatively independent of the application layers, the opportunity for secure host-to-host communications over a widespread network, such as the Internet, is greatly enhanced.

- If IPsec is supported, you can control IP traffic by using both Firewall and IPsec protection.
- If IPsec is not supported, you can control IP traffic by using only Firewall protection.

NOTE: In addition to Firewall and IPsec protection at the network layer, the HP Jetdirect print server also supports the following:

- An SNMPv3 agent at the application layer for management application security
- Open Secure Sockets Layer (SSL) standards at the transport layer for secure client-server applications, such as client/server authentication or HTTPS Web browsing

For IPsec/Firewall operation on the HP Jetdirect print server, use this option to configure an IPsec/Firewall policy that is applied to specified IP traffic. For more information about configuring IPsec/Firewall policies and the specific settings, see the *HP Jetdirect Print Servers Administrator's Guide*.

NOTE: To ensure communications with an HP Jetdirect print server that is configured with an IPsec policy, computer systems that communicate with the print server must be properly configured. IPsec policies that are configured on the print server and computer systems must be compatible. Otherwise, connections fail.

Use the following steps to modify a rule:

1. Select the rule, and then click the **Add / Modify Rules** button. The **IPsec/Firewall Policy** wizard starts.
2. On the **Specify Address Template** page, select the address template.
3. Use the following steps to modify the address template:
   a. Click the **Modify** button.
   b. On the **Create Address Template** window, make the appropriate changes, and then click the **OK** button.
4. On the **Specify Address Template** page, click the **Next** button.
5. On the **Specify Service Template** page, select the service template.
6. Use the following steps to modify the service template:
   a. Click the **Modify** button.
   b. On the **Create Service Template** window, click the **Manage Services** button.
   c. On the **Manage Services** window, make the appropriate changes, and then click the **OK** button.
   d. On the **Create Service Template** window, click the **OK** button.
7. On the **Specify Service Template** page, click the **Next** button.
8. On the **Specify Action** page, select the appropriate option, and then click the **Next** button.
9. If the **Require traffic to be protected with an IPsec/Firewall policy** option is selected, the **Specify IPsec/ Firewall Template** page appears. Use the following steps to modify the IPsec template:

   a. Select the IPsec template, and then click the **Modify** button. The **IPsec Template** wizard starts.
   b. On the **IPsec Protocols** page, make the appropriate changes, and then click the **Next** button.
   c. On the **Identity Authentication** page, make the appropriate changes, and then click the **Next** button. The **IPsec Template** wizard closes.

10. On the **Specify IPsec/Firewall Template** page, click the **Next** button.
11. On the **Rule Summary** page, click the **Finish** button.

Use the following steps to delete a rule:

1. Select the rule, and then click the **Delete Rule** button.
2. On the **Confirm** window, click the **Yes** button.

Federal Information Processing Standard (FIPS) supports only the AES-128 and AES-256 ciphers. To configure the **Kerberos** setting when FIPS mode is enabled on the device, you must specify the AES-128 and AES-256 protocols. If you specify the DES-CBC-MD5 cipher for the **Kerberos** setting, the configuration fails.

HP Jetdirect IPsec supports the Kerberos authentication method. The Kerberos authentication method supports the AES128-SHA1 and AES256-SHA1 encryption protocols. These encryption protocols incorporate an iteration count that increases the complexity of the encryption keys. The default iteration count in HP Jetdirect is 4,096, which complies with current standards. The iteration count in HP Jetdirect and the iteration count on the Kerberos domain controller must match. To change the iteration count on the Kerberos domain controller, create the following Registry entry and provide the appropriate value. This Registry entry affects all of the Kerberos clients of the domain controller.

```
HKLM\SYSTEM\CurrentControlSet\Services\Kdc\IterationCount (DWORD)
```

The HP Web Jetadmin administrator can create an IPsec rule with Kerberos pre-authentication by using one of the following methods:

- Use HP Web Jetadmin to configure the settings for the IPsec rule, which includes the Kerberos server admin credentials and organization unit (OU) path. HP Web Jetadmin uses these settings to create an account on the Key Distribution Center (KDC) server.
- Log in to the KDC server and manually create an account. Then access the HP Embedded Web Server (EWS) on the device, and configure the settings for the IPsec rule.

The HP Web Jetadmin administrator must not configure the settings for an IPsec rule by using HP Web Jetadmin and then later update those settings by using the device EWS, or vice versa. The following are examples of the conflicts that can occur:

- The HP Web Jetadmin administrator uses HP Web Jetadmin to create an IPsec rule that has an encryption type of DES. Then the HP Web Jetadmin administrator uses the device EWS to change the encryption type to AES-128. If the HP Web Jetadmin administrator then uses HP Web Jetadmin to perform a refresh and reapply the rule to the device, the IPsec policy fails because the encryption type for the Kerberos server account is still DES. To ensure that the encryption type is updated on the Kerberos server, the HP Web Jetadmin administrator must use HP Web Jetadmin to change the encryption type.
- The HP Web Jetadmin administrator uses HP Web Jetadmin to create an IPsec rule. Then the HP Web Jetadmin administrator uses the device EWS to change the settings for the rule. When the HP Web Jetadmin administrator views the rule in HP Web Jetadmin, the changes that were made by using the EWS are not displayed. In this case, HP Web Jetadmin does not display an error message and the IPsec policy might not be applied correctly.

Kerberos Authentication

Use this feature to configure the device (multi-function peripheral, or digital sender) to authenticate users to a Kerberos Realm. When Kerberos authentication is selected as the **Log In Method** for one or more **Device Functions** on the **Authentication Manager** feature, the user at the device must enter valid credentials to gain access to those functions (username, password, and realm).

Authentication consists of two interdependent parts:

- The device verifies the user's credentials with the Key Distribution Center (KDC).
- After the device user has supplied valid credentials and has been authenticated, the device searches for the user's email address and name.

If either step fails, the user is denied access to the functions that have been configured to require Kerberos authentication.

Accessing the Kerberos Authentication Server

The **Kerberos realm (domain)** is the fully qualified domain name of the Kerberos realm (domain).

Use the **Advanced** button to the right of the **Kerberos realm (domain)** field to access the **Alternate Domain Configuration**. Alternate domains are mapped to the default realm.

The **Kerberos server hostname** can be the same as the **Kerberos realm (domain)** if a DNS (Domain Name Service) service is available and correctly configured. The device will use DNS to look up the first available KDC (Kerberos Domain Controller) on the network. If DNS is not available, the IP address of the Kerberos Server may be used.

The **Kerberos server port** is the default IP port used by the Kerberos authentication method. The default is port 88, but this can be different in different network environments. Please contact your IT administrator to determine the appropriate port if the default port does not work.

Accessing the LDAP Server

The **LDAP server bind method** determines how the device will access the LDAP server.

The **Credentials** configuration section is used to determine which credentials will be used to bind (authenticate) to the LDAP server.

- When **Use device user credentials** is selected, the device users credentials (entered at the control panel of the device) will be used to access the LDAP server. This method has the advantage of not having to store a username and password, which may expire, in the device.
- When **Use public credentials** is selected and user credentials are not available, the Username and Password entered will be used to access the LDAP server. This method should be used if for some reason device users do not have read access to the LDAP data.

The **Bind prefix** setting is the LDAP attribute used to construct the user's Distinguished Name (DN) for authentication. This prefix is combined with the username typed at the control panel to form the Relative Distinguished Name (RDN). Commonly used prefixes are "CN" (for common name) or "UID" (for user identity).

The **Bind and search root** value is used to validate the user's credentials with the LDAP server. This value is combined with the RDN to construct the full Distinguished Name (DN) of the user.

The string consists of "attribute=value" pairs, separated by commas. For example:

```
ou=engineering, o=HP, c=US
```

```
ou=marketing, o=HP, c=US

o=hp.com

ou=engineering, cn=users, dc=hp, dc=com
```

The **LDAP server** is typically the same as the **Kerberos server** in the Windows Active Directory Environment.

The **Port** is the IP port used by the LDAP protocol to communicate with the LDAP server. This is typically port 389 or port 3268.

Searching the LDAP Database

The **Search root** is the Distinguished Name (DN) of the entry in the LDAP directory structure where address searching is to begin. A DN is made up of ' attribute=value ' pairs, separated by commas. For example:

```
dc=HP, dc=com

ou=engineering, dc=northamerica, dc=HP, dc=com

ou=marketing, o=HP, c=US

o=hp.com

ou=engineering, cn=users, dc=hp, dc=com
```

NOTE: On some LDAP servers, the **Search root** can be left blank (in which case its root node will be assumed). The search root is not case sensitive.

Retrieve the Device User's Email Address Using Attribute Of

After the device user has been located in the LDAP database, the user's email address is retrieved from the database by using the LDAP attribute specified in **Retrieve device user's email address using attribute of** field. In the Windows Active Directory environment, this attribute is typically mail.

Retrieve the Device User's Name Using Attribute Of

The user's display name is obtained from the LDAP attribute that is specified in the **Retrieve device user's name using the attribute of** field. In the Windows Active Directory environment, this attribute is typically **displayName**.

LDAP - Accessing the Server

This option lets you specify how the digital send device accesses the Lightweight Directory Access Protocol (LDAP) server to look up email addresses. To send scanned documents from the digital send device through email, the user must provide an email address. The process of entering email addresses can be simplified by providing an address lookup list and by using an auto-complete feature. Access to the LDAP server email address database provides a way for the digital send device to use the lookup list and the auto-complete feature.

Use the following steps to configure this option:

1. Select one of the following server bind methods from **LDAP server bind method**:
   - **Simple**: The digital send device will use credentials to access the LDAP server.

NOTE: If you select **Simple**, the credentials are sent from the digital send device without encryption. Contact the LDAP server's administrator to determine the most appropriate server bind method settings.

- **Simple over SSL**: the digital send device will use credentials to access the LDAP server and to enable the Secure Sockets Layer (SSL) protocol for communication between LDAP server and the device. The SSL protocol encrypts the authentication credentials before sending the credentials to the device.

2. Type the IP address or hostname for the LDAP server in **LDAP server**.
3. Type the number of the TCP/IP port on the server that receives LDAP requests in **Port** (usually 389).
4. If you select **Simple over SSL**, type the complete specified name of a user who has access to the LDAP server in **LDAP administrator's DN** and the password for the user name in **Password**.

LDAP - Searching the Database

Use this option to specify the root and attributes used to search the LDAP database for the user's email.

LDAP Sign In Setup

Use this option to enable or disable the LDAP sign-in method and configure the settings that the device uses to establish a connection with the LDAP server, authenticate users, and search the LDAP server database.

Enable and configure the LDAP sign-in method

NOTE: Some devices do not support all of the following configuration options.

1. Select the **Enable LDAP Sign In** checkbox.
2. In the **LDAP server address** box, enter the IP address or hostname of the LDAP server. The LDAP server address cannot contain the following characters:

   & < > ;

3. In the **Port number** box, enter the port that the LDAP server monitors for queries. The default is port 389.
4. To enable SSL, select the **Use SSL** checkbox.

   -or-

   To disable SSL, clear the **Use SSL** checkbox.

5. In the **Server Authentication** section, select one of the following options:

   - **Use MFP User Credentials**: The device uses the credentials of the user who is signed in on the device to authenticate to the LDAP server.

     In the **Bind prefix** text box, enter the bind prefix. The bind prefix cannot contain the following characters:

     & < > ;

   - **Use LDAP Admin Credentials**: The device uses the LDAP Admin credentials to authenticate to the LDAP server.

     In the **LDAP Admin Distinguished DomainName(DN)** box, enter the LDAP distinguished name. The LDAP distinguished name is required.

In the **Password** box, enter the LDAP Admin password.

6. To configure the LDAP database search settings, perform the following steps in the **LDAP Database Search Settings** section:

   a. To add the location in the LDAP directory structure where the device begins the search, enter the root name in the **Bind and Search Root** box, and then click the **Add** button. To enter multiple locations, separate the root names with the vertical bar (|) symbol. The root name cannot contain the following characters:

   & < > ;

   This text box can use static data or custom variables supported in the following formats:

   - Variable data (a variable always starts and ends with `%%` with the name of the variable in between the starting and ending `%%` signs)

     %%<custom variable>%% (where "<custom variable>" is the name of the user defined field)

     Example: `%%var_DatabaseSearchSettings%%`

   - Variable data along with a combination of static content before or after the variable

     <static value>%%<custom variable>%%<static value>

   TIP: By starting the variable data name with var_, it's easier to find and identify user defined fields in HP Web Jetadmin.

   TIP: In HP Web Jetadmin, text boxes that support variable data are highlighted blue. For more information on variable data, see Create and Use Variable Data on page 183.

   b. To delete a search root, select the root name from the **BindSearchRoot** grid, and then click the **Remove** button.

   c. To delete all of the search roots, click the **Remove All** button.

7. In the **Match the name entered with this attribute** box, enter the attribute name that the device uses to authenticate the user login name. The attribute name cannot contain the following characters:

   & < > ;

8. In the **Retrieve the device user's email address using this attribute** box, enter the LDAP attribute name for user email addresses. The attribute name cannot contain the following characters:

   & < > ;

9. In the **Retrieve the device user's name using this attribute** box, enter the LDAP attribute name for user names. The attribute name cannot contain the following characters:

   & < > ;

10. In the **Retrieve the device user's group using this attribute** box, enter the LDAP attribute name for user groups. The attribute name cannot contain the following characters:

    & < > ;

11. If the specified group attribute must match the LDAP attribute exactly, select the **Exact match on group attribute** checkbox.

    -or-

    If the specified group attribute does not need to match the LDAP attribute exactly, clear the **Exact match on group attribute** checkbox.

Disable the LDAP sign-in method

▲ Clear the **Enable LDAP Sign In** checkbox.

LDAP Users and Groups

Use this option to set LDAP permissions for individual users or groups. These permissions control who has access to what features on the device. Choose the permission levels that best suit the security needs of your organization and the convenience needs of your users.

Use the following steps to configure this option:

1. Select a value from **Default permission set for LDAP users**.
2. To add a user permission setting, type the user name in **Name**.
3. Select the permission setting from **Permission**.
4. Select the type from **Type** and click **Add**.
5. To edit a permission set, select it from the list and then edit the **Permission set**.
6. To remove a user permission setting, select the permission setting and click **Remove**.

Local Administrator Password

Local Administrator Password is used to configure Account Lockout Policy for the device to avoid device lockout if login fails. It also prompts the user to enter the proper password for the device.

Use the following steps to configure the Local Administrator Password:

1. If **Enable Account Lockout** is enabled, then Maximum Attempts, Lockout Interval, and Reset Lockout Interval is enabled. Enable or disable account lockout using this option.

   a. **Maximum Attempts** - Maximum number of password attempts (3-30)

   b. **Lockout Interval**- Interval the account is locked out (5-1800 Secs)

   c. **Reset Lockout Interval**- Reset the interval of lockout (0-1800 Secs)

2. **Enable Password Complexity**- When enabled, the password must contain three of the following: uppercase letters, lowercase letters, numbers, and special characters.
3. **Minimum Password Length**- Password length should be 0-16 (when complexity disabled) 3-16 (when complexity enabled). (0) indicates that the minimum password length is disabled; no password is required.

NOTE: See the actual device for supported range of values.

Near Field Communication

Near field communication (NFC) capabilities enable an easy one-to-one HP wireless direct print connection by using a simple device-to-device touch. Users can quickly connect to the printer and print documents and images from a mobile device, such as a smartphone or tablet, by touching the mobile device to the NFC antenna on the printer. Use this option to enable and disable the NFC feature on the printer.

To enable the NFC feature, select the **Enable Near Field Communication** checkbox.

To disable the NFC feature, clear the **Enable Near Field Communication** checkbox.

Novell Sign In Setup

Use this option to set up Novell authentication on a device. Specify the Novell trees that a user can authenticate against. You can extend the structure and security of a Novell network to the device by enabling the Novell NDS sign in on the device. This provides for enhanced security and ease of use for users who are already members of a Novell tree.

Use the following steps to configure this option:

1. Select **Enable Novell NDS Sign In**.
2. To add a Novell tree, type the name of the Novell tree in the text field under **Add Tree** and then click **Add Tree**.

   To remove a Novell tree, highlight the tree and then click **Remove Tree**.
3. Type the address of the Novell server in **Novell Server Address**.
4. Type the context value in **Context**.
5. Type the bind prefix in **Bind Prefix**.
6. Type the root name for binding and searching in **Bind and Search Root**.
7. Type the name of the tree in **Default Tree**.

PJL Password

Printer Job Language (PJL) is a command language that enables some features of a device. Setting the PJL password restricts access to those PJL features. The PJL password is a numeric PIN. The PJL password is cleared by entering a zero (0) as the new password.

NOTE: The PJL password only provides security for configuring device settings from a Netware server.

Print Job Color Control

Use this option to enable or disable color printing for all print jobs or limit the color printing based on a list of approved software programs.

Use the following steps to configure this option:

1. Select a value from **Default for print jobs generated from unspecified computer applications**.
2. To add an application color control setting, type the name of the application in **Application name**.
3. Select the color control setting from **Color control** and click **Add**.
4. To edit and application color control setting, select the application from the list and edit the value of **Color control**.
5. To remove an application color control setting from the list, select the application color control and then click **Remove**.

Printer Firmware SHA1 Code Signing

Use this option to allow the device to install only firmware bundles that are signed by using Secure Hash Algorithm 2 (SHA-2) or allow the device to install firmware bundles that are signed by using SHA-1 or SHA-2.

Use the following steps to configure this option:

▲ To allow the device to install *only* firmware bundles that have an SHA-2 signature, select the **Disabled** option. The device uses SHA-256 to validate the bundle signature. The device does not install firmware bundles that have only an SHA-1 signature.

-or-

To allow the device to install firmware bundles that have an SHA-1 *or* SHA-2 signature, select the **Enabled** option. The device always validates the firmware bundles by using the more secure SHA-2 signature.

Printer Firmware Update

Use this option to enable or disable the ability of a device to have its firmware updated remotely. If disabled, the device will not accept RFU firmware update files.

Remote Configuration Password

Remote Configuration Password is used to configure CCC (Common Criteria Certification) Protection Profile. It locks the remote account after a fixed number of login fails and prompts the user to enter the proper password for the device.

1. If **Enable Account Lockout** is enabled, then Maximum Attempts, Lockout Interval, and Reset Lockout Interval is enabled. Enable or disable account lockout for remote configuration using this option.

   a. **Maximum Attempts** - Maximum number of password attempts (3-30)

   b. **Lockout Interval**- Interval the account is locked out (5-1800 Secs)

   c. **Reset Lockout Interval**- Reset the interval of lockout (0-1800 Secs)

2. **Enable Password Complexity**- When enabled, the password must contain three of the following: uppercase letters, lowercase letters, numbers, and special characters.

3. **Minimum Password Length**- Password length should be 0-16 (when complexity disabled) 3-16 (when complexity enabled). (0) indicates that the minimum password length is disabled; no password is required.

NOTE: See the actual device for supported range of values.

Restrict Color

Use this option to manage the use of color printing supplies within your organization. You can specify that all color print jobs are printed in color, all color print jobs are printed in their grayscale equivalent, or color printing is restricted based on the user's permission level or based on the application.

Use the following steps to configure this option:

1. Select one of the following options:

- **Enable color**: All color print jobs are printed in color.
- **Disable color**: All color print jobs are printed in their grayscale equivalent.
- **Set custom color access**: Color printing is restricted based on the custom settings that you define.

2. If the **Set custom color access** option is selected, perform the following steps:

   a. Select one or more of the following:

   - **Restrict by user permissions**: Select this checkbox to restrict color printing based on user permission sets. Use the **Access Control for Device Functions** configuration option to define the user permission sets.
   - **Restrict by application**: Select this checkbox to restrict color printing based on applications.

   If both the **Restrict by user permissions** and **Restrict by application** checkboxes are selected, the lowest level of permission is applied when restricting color print jobs.

   b. If the **Restrict by application** checkbox is selected, define the application permissions as follows:

   - Specify the default permission level for all applications: Select the type of color usage from the **Default permission for applications** drop-down list.
   - Identify and manage applications that require specific permission levels: These applications have the specific permission level applied to them instead of the default permission level. These applications are identified in the **Non default applications** list.

     To add an application to the list, enter the name of the application in the **Name** text box, select the type of color usage from the **Permission** drop-down list, and then click **Add**.

     To delete one or more applications from the **Non default applications** list, select the applications, and then click **Remove**.

     To delete all of the applications from the **Non default applications** list, click **Remove All**.

Secure Communication

Use this option to enable the ciphers.

The device communicates based on these secure communications and enabled ciphers. The enabled check boxes indicate currently active ciphers, and disabled check boxes indicate inactive ciphers. Securely manage the network device using a Web browser and the HTTPS protocol. To authenticate the HP Jetdirect Web Server when HTTPS is used, configure a certificate or use the pre-installed, self-signed X.509 Certificate. The encryption strength specifies what ciphers the Web server will use for secure communications.

AES256-GCM-SHA384 and AES128-GCM-SHA256 ciphers are only supported with TLS 1.2. If the active ciphers are limited to AES256-GCM-SHA384 and/or AES128-GCM-SHA256, then the supported TLS protocol must be set to only TLS 1.2 on the client and the server; otherwise, a communication error occurs. When browsing to the printer, or when configuring the printer via HP Web Jetadmin, the printer is the server and HP Web Jetadmin is the client.

Secure Disk Encryption Mode

Use this option to determine whether encryption is automatically enabled when an **HP Secure Hard Disk** is installed. This is the default and recommended mode. If you have a specific need to manually specify a drive password or want to start encrypting at a later time, the **Manual** setting allows this. If **Manual** is selected, you must use the EWS page to individually enable encryption of each device.

Use the following steps to configure this option:

1. To automatically enable encryption when an **HP Secure Hard Disk** is installed, select **Automatic**. This is the default and recommended mode.
2. If you need to manually specify a drive password or want to start encrypting at a later time, select **Manual** and then use the EWS page to individually enable encryption of each device.

Secure Disk Password

Use this option to configure a password for all of the secure disks installed on the device. This password provides access to the encrypted data on the secure disks. This password locks all of the secure disks, but does not encrypt the data on the disks. The device automatically generates a separate encryption key for each disk to encrypt the data.

If you change the password, no data on the secure disks is lost. If you remove the secure disk from the device, access to the encryption key is lost and the data on the secure disk cannot be decrypted.

NOTE: The password can be cleared only through the BIOS on the device. Clearing the password renders the data on the device unusable and makes the secure disk appear as a new disk.

Automatically generate a random password

1. Select the **Generate a new random password (Recommended)** option.
2. For HP FutureSmart devices, turn off the device, and then turn on the device. Other devices automatically turn off, and then turn on.

Manually assign a password

1. Select the **Manually set a new drive password** option.
2. In the **Password** and **Confirm Password** boxes, enter the password. The password must be between 8 and 32 characters long.
3. For HP FutureSmart devices, turn off the device, and then turn on the device. Other devices automatically turn off, and then turn on.

Service Access Code

A unique service personal identification number (PIN) is assigned to each HP product model. During the manufacturing process, the same service PIN is written to every device for a specific product model. The factory-default service PIN cannot be changed.

The factory-default service PIN is required to gain access to the Service menu at the device control panel. The factory-default service PIN for the various HP product models is public information. Anyone who can find the factory-default service PIN for the product model can sign in at the device control panel and access all of the troubleshooting tools and configuration settings that are available from the Service menu.

Use this option to configure a service access code on the device. This service access code provides additional security for the Service menu. The factory-default service PIN can no longer be used to gain access to the Service menu. However, the factory-default service PIN can be restored at any time.

Configure a service access code

1. In the **Service Access Code** box, enter the service access code. The service access code must be exactly 8 digits in the range of 00000000 to 99999999. All 8 digits must be entered.
2. In the **Verify Access Code** box, enter the 8-digit service access code again.

Restore the factory-default service PIN

1. In the **Service Access Code** box, select the current value, and then press the Delete key.
2. In the **Verify Access Code** box, select the current value, and then press the Delete key.

Service Loading

Use this option to enable or disable the ability to install third-party services and applications that run directly on the device.

To enable this feature, select the **Enabled** option.

-or-

To disable this feature, select the **Disabled** option.

Set Community Name

The Set Community Name, which is different than the device password, prevents unauthorized users from using SNMP utilities to access and change device setting. Once you assign a Set Community Name, only users who know the Set Community Name can change the device settings from an SNMP utility.

NOTE: When setting a password on the device, you must enter the current password, if any, regardless of credentials stored in the application. If you don’t, the setting will fail as “Invalid Data”.

To configure this option, type the Set Community Name in **Set community name** and then confirm it by retyping it in **Repeat set community name**. To change the Set Community Name password, type the current one in **Current set community name** and then type the new one in **Set community name**. Confirm it by retyping it in **Repeat set community name**.

Smart Card Sign In Setup

The structure and security of a domain network can be extended to the device by enabling the Smart Card sign-in method on the device. This feature provides enhanced security and ease-of-use for users who are members of that domain.

Use this option to enable or disable Smart Card authentication on the device and configure the trusted domains that the device uses to authenticate users.

NOTE: The Smart Card sign-in method is available only if an optional Smart Card reader accessory is installed on the device.

If the Smart Card sign-in method is required, disable all of the other sign-in methods. You might need to install certificates on the device. For more information about installing certificates, see Manage the Certificate Repository on page 69.

Enable and configure the Smart Card sign-in method

1. Select the **Enable Smart Card Sign In Setup** checkbox.
2. To add a trusted domain, enter the domain name in the box, and then click the **Add Domain** button.
3. To delete a trusted domain, select the domain from the list, and then click the **Remove Domain** button.

   -or-

   To delete all of the trusted domains, click the **Remove All** button.
4. From the **Default Windows domain** list, select the default domain.
5. To use Secure Sockets Layer (SSL) to sign in, select the **Use SSL** checkbox. The default is port 636.

   -or-

   To use a custom port to sign in, clear the **Use SSL** checkbox, and then enter the port number in the **Port** box. The default is port 389.
6. In the **Retrieve the device user's email address using this attribute** box, enter the attribute name for the email address.

Disable the Smart Card sign-in method

▲ Clear the **Enable Smart Card Sign In Setup** checkbox.

Smart UX

Use this option to configure Smart UX. Smart UX apps use Android technology.

To enable Smart UX, select the check box next to **Allow Smart UX apps on this product**.

To disable Smart UX, clear the check box next to **Allow Smart UX apps on this product**.

SNMP Version Access Control

SNMPv3 protects the network management information that is sent between HP Web Jetadmin and a device through user authentication and data encryption. SNMPv3 supports the MD5 and SHA-1 authentication protocols and the DES and AES-128 privacy protocols. SNMPv3 does not support the No Authentication Protocol and No Privacy Protocol modes.

You can use SNMPv3 to prevent unauthorized users from viewing or changing device settings. You can require SNMPv3 to view or change information on a device. You can allow SNMPv1 read-only access to the device and also require SNMPv3 to change information on a device. SNMPv1 does not use data encryption when sending information between HP Web Jetadmin and a device.

Use this option to enable and disable SNMPv3 on the device and specify the authentication protocol, privacy protocol, and passphrases that are required.

Federal Information Processing Standard (FIPS) supports only the SHA-1 authentication protocol and AES-128 privacy protocol. To create or update the SNMPv3 credentials when FIPS mode is enabled on the device, you must specify the SHA-1 and AES-128 protocols. If you specify the MD5 authentication protocol and DES privacy protocol, the configuration fails.

Enable SNMPv3

1. Select the **Enable SNMPv3** option.
2. In the **Set community name (optional)** box, enter the name that is currently configured for SNMPv1.
3. In the **User name** box, enter the user name.
4. From the **Authentication Protocol** list, select the protocol.
5. In the **Authentication passphrase** and **Confirm authentication passphrase** boxes, enter the passphrase for the specified authentication protocol.
6. From the **Privacy Protocol** list, select the protocol.
7. In the **Privacy passphrase** and **Confirm privacy passphrase** boxes, enter the passphrase for the specified privacy protocol.
8. To enable SNMPv1 read-only access on the device, select the **SNMPv1 read-only** option.

   -or-

   To disable SNMPv1, select the **SNMPv1 disabled** option.

Change the SNMPv3 credentials

1. Select the **Modify SNMPv3** option.
2. In the **Current SNMPv3 Credential** section, enter the user name, authentication protocol, authentication passphrase, privacy protocol, and privacy passphrase that are currently configured for SNMPv3. The current SNMPv3 credentials are required.
3. In the **New SNMPv3 Credential** section, enter the new values for the authentication protocol, authentication passphrase, privacy protocol, and privacy passphrase that are to be changed.

   NOTE: The user name that is currently configured for SNMPv3 cannot be changed.

   CAUTION: To change the authentication and privacy passphrases, the current passphrases must be specified even if global SNMPv3 credentials are stored in HP Web Jetadmin. If the current passphrases are not specified, the configuration fails.

4. To enable SNMPv1 read-only access on the device, select the **SNMPv1 read-only** option.

   -or-

   To disable SNMPv1, select the **SNMPv1 disabled** option.

Disable SNMPv3

1. Select the **Disable SNMPv3** option.
2. In the **Current SNMPv3 Credential** section, enter the user name, authentication protocol, authentication passphrase, privacy protocol, and privacy passphrase that are currently configured for SNMPv3. The current SNMPv3 credentials are required.

Temporary Limit Overrides

Use this option to override page limits for specific users in a permission set. If one or more users in a permission set has a specific need to print more pages than the page limit for the group allows, you can set an override for that user to allow for more page prints.

Use the following steps to configure this option:

1. Type the user name in **User Account**.
2. Select a value from **Total Override**: Drop-down list.
   - **Page Limit**: Specify a page limit for the total number of pages printed. Then type that number in the adjacent text box.
   - **No Page Limit**: Do not specify a page limit for the total number of pages printed.
3. Select a value from **Color Override**:
   - **Page Limit**: Specify a page limit for the number of color pages printed. Then type that number in the adjacent text box.

     NOTE: The page limit for color pages cannot exceed the total page limit.
   - **No Page Limit**: Do not specify a page limit for the number of color pages printed.
4. To add the overrides to the list below, click **Add**.
5. To edit the settings, select the overrides on the list and then edit **Total Override** and **Color Override**.
6. To remove a temporary limit override setting, select the override setting and click **Remove**.

Usage Limit and Reset Period

Use this option to enable usage limits. If usage limits are enabled, each user in a Permission Set is assigned a limited number of pages during a recurring time period. The number of pages is the same for each person in the device Permission Set. Limits and overrides will automatically reset at the start of each reset period. Usage limits can help reduce the operating costs of your organization. Use the usage reports to identify usage trends among your users.

Use the following steps to configure this option:

1. Select the **Enable usage limits on this device** check box.
2. Select one of the Usage Limit Exceeded Report options.
3. Select the reset option desired.
4. To reset usage tracking immediately, select **Reset usage tracking**.

Usage Limits for Permission Sets

Use this option to define the general page limits and the color page limits for predefined permission sets.

NOTE: You can apply this configuration option only to a single HP CM8060/CM8050 Color MFP with Edgeline Technology device. You cannot use this configuration option to configure multiple devices at one time or include this configuration option in a device configuration template.

Use the following steps to configure this option:

1. To assign page limits to a permission set, locate the permission set name in the **Permission Set** column.
2. Select a value from the corresponding **Total Page Limit** drop-down list.
3. If you selected a page limit, specify the number of pages in the corresponding **Color Page Limit** drop-down list.

NOTE: The page limit for color pages cannot exceed the total page limit. If a higher value is entered for the color page limit, then the total page limit is used.

User PIN Authentication

Use this option to add user PIN records into the device one at a time, and to edit or delete user PIN records that have already been saved in the device.

Use the following steps to configure this option:

1. To add or edit a user:
   a. Click **Add**, or select a user and click **Edit**.
   b. Type the person's name in **Name**.
   c. Type the person's email address in **Email address**. If email address validation is enabled on the device, the email address must include an at symbol (@).
   d. Type the user PIN in **User access PIN**. The PIN must be between 4 and 8 characters.
   e. Click **OK**.
2. To remove a user, select the user and click **Remove**.
3. To delete all users, click **Remove All**.
4. **Remove all existing entries**: In a template or with multiple devices selected, check this box to delete all existing user PINs from the device. If this box is not checked, user PINs will be added to any existing PINs in the device.
5. **Overwrite any existing entries**: In a template or with multiple devices selected, check this box to overwrite any existing user PINs with the same name. If this box is not checked, user PINs will be added to any existing PINs in the device, and existing PINs with the same name will not be changed.

Windows Sign In Setup

The structure and security of the Windows domain networks can be extended to the device by enabling the Windows sign-in method on the device. This feature provides enhanced security and ease-of-use for users who are members of a Windows domain.

Use this option to enable or disable the Windows sign-in method and configure the Windows trusted domain and attribute keys that the device uses to authenticate users.

Enable and configure the Windows sign-in method

1. Select the **Enable Windows Negotiated Sign In** checkbox.
2. Use the following steps to configure the trusted Windows domains that the device uses to authenticate users:
   a. To add a trusted domain, enter the domain name in the box that is next to the **Add Domain** button, and then click the **Add Domain** button.

NOTE: Some devices support only one trusted domain. For these devices, the **Add Domain** button becomes unavailable after a trusted domain is added.

b. To delete a trusted domain, select the domain name from the list, and then click the **Remove Domain** button.

c. To delete all of the trusted domains, click the **Remove All** button.

NOTE: For some devices, this feature is available only if you are configuring multiple devices or creating device configuration templates.

3. To specify the default trusted domain, select the domain name from the **Default Windows domain** list.

NOTE: For devices that support only one trusted domain, the specified trusted domain is automatically set as the default.

4. To enable SSL, select the **Use SSL** checkbox.

   -or-

   To disable SSL, clear the **Use SSL** checkbox.

NOTE: For some devices, this feature is available only if you are configuring multiple devices or creating device configuration templates.

5. In the **Match the name entered with this attribute** box, enter the Windows domain attribute for user login names. The attribute name cannot contain the following characters:

   & < > ;

6. In the **Retrieve the device user's email address using this attribute** box, enter the Windows domain attribute for user email addresses. The attribute name cannot contain the following characters:

   & < > ;

7. In the **Retrieve the device user's home folder using this attribute** box, enter the Windows domain attribute for user home network folders. The attribute name cannot contain the following characters:

   & < > ;

NOTE: For some devices, this feature is available only if you are configuring multiple devices or creating device configuration templates.

8. In the **Retrieve the device user’s name using this attribute** box, enter the Windows domain attribute for device user names. The attribute name cannot contain special characters.

NOTE: For some devices, this feature is available only if you are configuring multiple devices or creating device configuration templates.

Disable the Windows sign-in method

▲ Clear the **Enable Windows Negotiated Sign In** checkbox.

Windows Users and Groups

Use this option to set Windows permissions for individual users or groups. These permissions control who has access to what features on the device. Choose the permission levels that best suit the security needs of your organization and the convenience needs of your users.

Use the following steps to configure this option:

1. Select a permission set from **Default permission set for Windows users**.
2. To add a user permission setting, type the user name in **Name**.
3. Select the permission setting from **Permission**.
4. Select the type from **Type** and click **Add**.
5. To edit a permission set, select it from the list and then edit the **Permission set**.
6. To remove a user permission setting, select the permission setting and click **Remove**.

Device Configuration Options for Supplies

Configuration options for **Supplies** manage settings related to consumable supplies, such as cartridges.

Cartridge Low Action - Black

Use this option to specify the action that the device takes when the supply reaches a low condition. If a print supply becomes low during a print job, the print quality of the job might be unacceptable.

To specify the action that the device takes when the supply reaches a low condition, select one of the following options:

- **Stop**—The device stops printing the current print job and displays an error message on the device control panel that prompts the user to replace the supply.

  NOTE: If this option is selected, the **Cartridge Very Low Action - Black** configuration option is locked and cannot be configured.

- **Continue**—The device finishes printing the current print job and displays a warning message on the device control panel that reports the supply is low.

  NOTE: If this option is selected, the **Cartridge Very Low Action - Black** configuration option can be successfully configured.

Cartridge Policy

Use this option to specify that only genuine HP cartridges can be installed and used in this device.

To allow only genuine HP cartridges to be used in this device, select the **Authorized HP** option.

To allow any properly functioning cartridges to be used in this device, select the **Off** option.

Cartridge Protection

Use this option to configure the cartridge protection mode. When the cartridge protection mode is configured, all of the cartridges that are currently installed in the device or fleet of devices become permanently protected. After the cartridge protection mode is configured on a cartridge, the cartridge protection mode on that cartridge cannot be removed or changed.

Cartridges that are configured with single device cartridge protection mode cannot be used in any other devices. Cartridges that are configured with fleet ID cartridge protection mode cannot be used in any devices that are configured with a different fleet ID.

Allow the installed cartridges to be used in any device

When this mode is configured, cartridges are not protected and can be used in other devices.

If cartridge protection is turned off on the device, previously protected cartridges that are currently installed in the device remain permanently protected. These cartridges remain locked to the device or to a fleet ID, depending on the setting before cartridge protection is turned off.

When cartridge protection is turned off on a device that has a fleet ID configured, the fleet ID on the device is cleared, cartridge protection mode is set to device only, and protection is switched off. When new cartridges are installed in the device, the new cartridges are not protected and can be used in other devices.

▲ Select the **Off** option.

Allow the installed cartridges to be used only in this device

When single device cartridge protection mode is configured, the cartridges that are currently installed in the device become permanently protected and can be used only in this device. When new cartridges are installed in the device, the new cartridges become permanently protected and can be used only in this device. If a protected cartridge is removed from this device and installed in another device, the cartridge is unusable in that device.

⚠ CAUTION: After the cartridge protection mode is configured on a cartridge, the cartridge protection mode on that cartridge cannot be removed or changed.

To configure single device cartridge protection mode, perform the following steps:

1. Select the **Protect Cartridges by allowing the installed cartridges to be used only in this device** option.
2. In the **Cartridge Protection Warning** window, click the **OK** button.

NOTE: If you click the **Cancel** button, the **Protect Cartridges by allowing the installed cartridges to be used only in this device** option is disabled and the **Off** option is enabled.

Allow the installed cartridges to be used in all of the devices that have the same fleet ID

When fleet ID cartridge protection mode is configured, HP Web Jetadmin stores the fleet ID on the selected devices. The cartridges that are currently installed in the selected fleet of devices become permanently protected and can be used only in devices that are configured with the same fleet ID. When new cartridges are installed in a device in the fleet, the new cartridges also become protected. If a protected cartridge is removed from one of these devices and installed in a device that is not configured with the same fleet ID, the cartridge is unusable in that device.

⚠ CAUTION: After the cartridge protection mode is configured on a cartridge, the cartridge protection mode on that cartridge cannot be removed or changed.

IMPORTANT: Make sure that you keep a careful record of the fleet ID. After the fleet ID is configured on the devices, there is no method for retrieving the fleet ID if it is forgotten.

The HP Web Jetadmin administrator can assign a new fleet ID to a device. In this case, the cartridges that are currently installed in that device continue to function and can be used in devices that are configured with the old fleet ID. Any new cartridges that are installed in the device become protected with the new fleet ID and can be used only in devices that are configured with the new fleet ID.

TIP: If different fleet IDs are assigned to different device groups, it is easier to keep track of which fleet ID is assigned to each device group by creating a device configuration template for each fleet ID.

To configure fleet ID cartridge protection mode, perform the following steps:

1. Select the **Protect Cartridges by allowing the installed cartridges to be used in all devices with the same fleet ID** option.

2. In the **Cartridge Protection Warning** window, click the **OK** button.

   NOTE: If you click the **Cancel** button, the **Protect Cartridges by allowing the installed cartridges to be used in all devices with the same fleet ID** option is disabled and the **Off** option is enabled.

3. In the **Fleet ID password** box, enter the fleet ID. The fleet ID must be a value from 1 to 65535.

   NOTE: If the **Allow these cartridges in all device with same Fleet ID checkbox** is selected, a fleet ID must be specified.

4. In the **Confirm Fleet ID password** box, enter the fleet ID.

Delay Very Low Message

Use this option to specify a threshold for the number of pages that the device prints after a supply reaches a very low status before the device displays a notification message. The threshold can be configured based on the usage history for each supply. The following are examples:

- If one color cartridge is used more than the other color cartridges, specify a lower page count threshold for that color cartridge to ensure that there is enough time to order a new cartridge or locate a replacement cartridge.

- If one color cartridge is rarely used or a replacement cartridge is readily available, specify a higher page count threshold for that color cartridge to avoid having the device display the supply very low message any longer than necessary.

Configure the threshold for the very low supply message

1. Select the **Enable** option.

2. Select the checkbox next to the supply, and then enter the page count threshold for that supply in the box.

   NOTE: A higher page count threshold provides less warning before the supply runs out. Setting a page count threshold that is too high might result in the supply running out before the supply very low message appears.

Disable the very low supply message

▲ Select the **Disable** option.

Estimated Supplies Levels

By default, HP Web Jetadmin displays the estimated supplies levels in 10% increments. For some devices, you can choose to display the estimated supplies levels in 1% increments instead of 10% increments. However, displaying the estimated supplies levels in 1% increments does not imply a 1% level of accuracy. The accuracy of the actual supplies levels and the remaining pages varies depending on the types of documents printed and other factors. HP uses the first 20% of cartridge use to estimate the remaining pages. In addition, other HP tools might display supplies levels in different percentage increments.

Use this option to enable the device to display the estimated supplies levels in 1% increments instead of the default of 10% increments. Before you enable this option, carefully review and accept the Estimated Supplies Levels agreement.

Display the estimated supplies levels in 1% increments

1. Click the **"Opt In" to enable** button.
2. Carefully review the Estimated Supplies Levels agreement.
3. If you accept the terms of the agreement, select the **I accept** option.

   -or-

   If you do not accept the terms of the agreement, select the **I do not accept** option. You will not be able to enable this option.
4. Click the **Close** button.
5. Select the **Enable 1% Estimated Supplies Level** checkbox.

After this option is applied to a device, you might need to click the **Refresh Supplies** button on the **Supplies** tab to view the estimated supplies levels in 1% increments.

Return the estimated supplies levels to 10% increments

▲ Clear the **Enable 1% Estimated Supplies Level** checkbox.

Level Gauge

Use this option to specify if the supply level gauge is displayed on the control panel for single-function devices.

To display the supply level gauge on the device control panel, select the **On** option.

-or-

To hide the supply level gauge on the device control panel, select the **Off** option.

Supply Low Alerts

Use this option to enable or disable the supply low alerts. If this option is enabled, the device triggers an alert when the supply is very low.

To enable supply low alerts, select the **Enabled** option.

To disable supply low alerts, select the **Disabled** option.

Supply Threshold

Use the following configuration options to specify the supply level threshold that must be reached before the device displays the supply low message:

- Cartridge Threshold - Black
- Cartridge Threshold - Cyan
- Cartridge Threshold - Magenta

- Cartridge Threshold - Yellow
- Drum Threshold - Black
- Drum Threshold - Cyan
- Drum Threshold - Magenta
- Drum Threshold - Yellow
- Fuser Kit Threshold
- Maintenance Kit Threshold
- Transfer Kit Threshold

The threshold can be configured based on the expected usage rate for the supply. The following are examples:

- If one color cartridge is used more than the other color cartridges, specify a higher threshold for that color cartridge to ensure that there is enough time to order a new cartridge or locate a replacement cartridge.
- If one color cartridge is rarely used or a replacement cartridge is readily available, specify a lower threshold for that color cartridge to avoid having the device display the supply low message any longer than necessary.

To configure the supply threshold, enter the threshold as a percentage. A lower threshold provides less warning before the supply runs out.

Supply Very Low Action

Use the following configuration options to specify the action that the device takes when the supply reaches a very low condition:

- Cartridge Very Low Action - Black
- Cartridge Very Low Action - Color
- Document Feeder Kit Very Low Action
- Fuser Kit Very Low Action
- Maintenance Kit Very Low Action
- Toner Collection Unit Very Full Action
- Transfer Kit Very Low Action

If a print supply becomes very low or runs out during a print job, the print quality of the job might be unacceptable. If a maintenance supply reaches a very low condition, the print quality might be unacceptable or the device operation might be adversely affected.

To specify the action that the device takes when the supply reaches a very low condition, select one of the following options:

- Stop—The device stops printing the current print job.
- Prompt to Continue—The device displays a prompt. The user can choose to finish printing or stop the current print job.
- Continue—The device finishes printing the current print job.

Device Configuration Options for Web Services

The configuration options in the Web Services category define the settings that affect HP Web Services.

ePrint Settings

Use this option to enable or disable access to HP Web Services and specify which services are enabled for the device. HP Web Services includes HP ePrint and HP Print Apps. You can enable HP Web Services on all devices, but the supported services vary depending on the device model.

Use the following steps to configure this option:

1. Review the Terms of Use provided at welcome.hp.com/country/us/en/termsofuse.html?jumpid=in_R11549eprintercenter.
2. To accept the Terms of Use and enable HP Web Services, select the **Enable HP Web Services** check box.
3. To enable printing by sending an email with an attached document to the device, select the **Enable HP ePrint** check box. HP ePrint supports the following email attachments:
   - Microsoft Word, PowerPoint, Outlook, and Excel files
   - Text files
   - PDFs
   - Image files (BMP, JPG, PNG, and TIFF)
4. To enable access to printable web content from the device control panel, select the **Enable Print Apps** check box.
5. Click **Apply**.

ePrint Settings - More Settings

Use this option to specify whether or not the printer can be enrolled in the HP Instant Ink replacement service. For more information about enrolling eligible printers in HP Instant Ink, visit hpinstantink.com.

Allow the printer to be enrolled in the HP Instant Ink service

1. Verify that the **Allow device to connect to HP Web Services** checkbox on the **ePrint Settings** configuration option is selected.
2. Select the **HP Instant Ink** checkbox.

Prevent the printer from being enrolled in the HP Instant Ink service

▲ Clear the **HP Instant Ink** checkbox.

HP JetAdvantage (More Apps)

HP JetAdvantage is a cloud-based service that provides access to applications that extend the capabilities of devices. Use this option to enable or disable the HP JetAdvantage feature on the device and specify whether or not users can create accounts for HP JetAdvantage from the device control panel.

Configure the HP JetAdvantage feature

When the HP JetAdvantage feature is enabled, the More Apps button is available from the Home screen on the device control panel. HP Web Jetadmin adds the *.hpbizapps.com URL to the HP-hosted Trusted Sites list on the device and enables Cross-Origin Resource Sharing (CORS) for this website.

▲ To enable the More Apps button on the device control panel, select the **Enable HP JetAdvantage (More Apps)** checkbox.

-or-

To disable the More Apps button on the device control panel, clear the **Enable HP JetAdvantage (More Apps)** checkbox.

Configure the ability to create HP JetAdvantage accounts

▲ To allow users to create accounts from the device control panel, select the **Allow users to create an account** checkbox.

⚠ CAUTION: There is no mechanism in HP Web Jetadmin to restrict the ability to create HP JetAdvantage accounts to only specific users. If this checkbox is selected, any user can create an account from the device control panel.

To prevent users from creating accounts from the device control panel, clear the **Allow users to create an account** checkbox.

Proxy Server

Use this option to configure or view the web browser proxy settings on the device (for example, to enable OXPd 1.6 functionality that requires accessing web sites from a device). You can determine whether or not the web proxy is enabled. If enabled, the proxy address and port must be set. Proxy credentials may be provided. A proxy exception list is also supported. The device web browser does not use the proxy for addresses in the **Proxy server exception list**.

Use the following steps to configure this option:

1. To enable this option, select **Manual**.
2. Type the URL for the proxy server in **Proxy Server**.
3. Type the port number for the proxy server in **Proxy Port**.
4. Type the user ID and password in **User** and **Password**.
5. Type all proxy server exceptions in **Proxy server exception list**. Use a semicolon to separate multiple addresses.

Device Configuration Options for Wireless

Configuration options for Wireless define wireless communication for the device including setup and encryption.

Enable Wireless Direct

Use this option to enable or disable the HP wireless direct printing feature on the device. This feature provides the ability to print from a wireless mobile device directly to an HP wireless direct-enabled printer without requiring a connection to a network or the Internet.

To enable the HP wireless direct printing feature, select the **Enable Wireless Direct** checkbox.

To disable the HP wireless direct printing feature, clear the **Enable Wireless Direct** checkbox.

Enable Wireless Station (802.11)

Use this option to enable or disable the wireless station settings.

To enable the wireless station settings, select the **Enable Wireless Station (802.11)** check box.

-or-

To disable the wireless station settings, clear the **Enable Wireless Station (802.11)** check box.

Radio State

Use this option to enable or disable the Wireless Radio feature. If the device is in wired mode, you can configure the Wireless Radio state. If the device is in wireless station mode or access point mode, you cannot configure the Wireless Radio state.

To configure this option, select the **Disable Radio** or **Enable Radio** option from the list.

Wi-Fi Direct

HP Wi-Fi Direct printing provides the ability to print from a mobile device, such as a smartphone or notebook computer, directly to a printer without connecting to a Wi-Fi network. The mobile device must be within range of the printer.

Use this option to configure the settings that are used to connect the mobile device to the printer.

Enable HP Wi-Fi Direct printing

1. Select the **Enable Wi-Fi Direct** checkbox.
2. In the **HP Wi-Fi Direct Name** box, enter the printer model.

   The HP Wi-Fi Direct printing name consists of a predefined prefix and a suffix in the format of *printer_model*.
3. To specify the security method that is used to establish the Wi-Fi connection between the printer and the mobile device, select one of the following options from the **Connection Method** list:
   - **Auto**—The printer accepts all Wi-Fi connections. The user is not required to enter a passphrase on the printer control panel. However, if the mobile device requires a passphrase, the user must enter the

default passphrase on the mobile device before the Wi-Fi connection is established. The default passphrase is 12345678.

- **Manual**—The user must enter a passphrase on the printer control panel before the Wi-Fi connection is established.
- **Advanced**—The printer uses the specified advanced settings to establish a Wi-Fi connection.

4. To enable HP Wi-Fi Direct printing with security, enter the passphrase in the **Passcode** box. The passphrase must be 8 to 63 characters or 64 hexadecimal digits. The mobile device encrypts the passphrase and sends it to the printer.

   If the **Auto** option is selected from the **Connection Method** list, the default passphrase is 12345678. This default passphrase cannot be changed.

5. From the **Channel** list, select the channel that the printer uses to establish the Wi-Fi connection.

6. If the **Advanced** option is selected from the **Connection Method** list, use the following steps to configure the advanced settings:

   a. To prevent the printer from broadcasting the HP Wi-Fi Direct name on the Wi-Fi network, select the **Do not broadcast the Wi-Fi Direct name** checkbox.

      -or-

      To allow the printer to broadcast the HP Wi-Fi Direct name on the Wi-Fi network, clear the **Do not broadcast the Wi-Fi Direct name** checkbox.

   b. To prevent the HP Wi-Fi Direct name from being displayed on the configuration reports, select the **Do not show the Wi-Fi Direct name on reports** checkbox.

      -or-

      To display the HP Wi-Fi Direct name on the configuration reports, clear the **Do not show the Wi-Fi Direct name on reports** checkbox.

   c. To prevent the passphrase from being displayed on the configuration reports and printer control panel, select the **Do not show Wi-Fi Direct password on reports or printers control panel** checkbox.

      -or-

      To display the passphrase on the configuration reports and printer control panel, clear the **Do not show Wi-Fi Direct password on reports or printers control panel** checkbox.

Disable HP Wi-Fi Direct printing

▲ Clear the **Enable Wi-Fi Direct** checkbox.

Wireless Direct

HP wireless direct printing provides the ability to print from a mobile device, such as a smartphone or notebook computer, directly to a printer without connecting to a wireless network. The mobile device must be within range of the printer.

Use this option to configure the settings that are used to connect the mobile device to the printer.

Configure the settings for HP Officejet Pro devices

1. Select the **Enable Security** checkbox.
2. In the **HP Wireless Direct Name** box, enter the printer model.

   The HP wireless direct printing name is the service set identifier (SSID). The SSID consists of a prefix in the format of HP-Print-*XY*-, where *XY* is the last 2 characters of the HP Jetdirect 2800w NFC & Wireless Direct Accessory hardware or media access control (MAC) address, and a suffix in the format of *printer_model*.
3. To enable HP wireless direct printing with security, enter the passphrase in the **Passcode** box. The passphrase must be 8 to 63 characters or 64 hexadecimal digits. The mobile device encrypts the passphrase and sends it to the printer.
4. To allow the printer to broadcast the SSID on the wireless network, select the **Broadcast the SSID** checkbox.

   -or-

   To prevent the printer from broadcasting the SSID on the wireless network, clear the **Broadcast the SSID** checkbox.

Configure the settings for HP FutureSmart devices

1. In the **HP Wireless Direct Name** box, enter the printer model.

   The HP wireless direct printing name is the service set identifier (SSID). The SSID consists of a predefined prefix and a suffix in the format of *printer_model*.

   If the **Auto** or **Manual** option is selected from the **Connection Method** list, the prefix is DIRECT-*XY*-HP where *XY* is the last two hexadecimal characters of the wireless MAC address.

   If the **Advanced** option is selected from the **Connection Method** list, the prefix is HP-Print-*XY*-, where *XY* is the last 2 characters of the HP Jetdirect 2800w NFC & Wireless Direct Accessory hardware or media access control (MAC) address.
2. To specify the security method that is used to establish the wireless connection between the printer and mobile device, select one of the following options from the **Connection Method** list:

   - **Auto**—The printer accepts all wireless connections. The user is not required to enter a passphrase on the printer control panel. However, if the mobile device requires a passphrase, the user must enter the default passphrase on the mobile device before the wireless connection is established. The default passphrase is 12345678.
   - **Manual**—The user must enter a passphrase on the printer control panel before the wireless connection is established.
   - **Advanced**—The printer uses the specified advanced settings to establish a wireless connection.
3. To enable HP wireless direct printing with security, enter the passphrase in the **Passcode** box. The passphrase must be 8 to 63 characters or 64 hexadecimal digits. The mobile device encrypts the passphrase and sends it to the printer.

   If the **Auto** option is selected from the **Connection Method** list, the default passphrase is 12345678. This default passphrase cannot be changed.
4. From the **Channel** list, select the channel that the printer uses to establish the wireless connection. The default channel is 6.

   If the **Enable Wireless Station** configuration option is enabled, the printer ignores the **Channel** setting and uses the wireless station settings that are configured by using the **802.11 b/g/n** configuration option.
5. If the **Advanced** option is selected from the **Connection Method** list, use the following steps to configure the advanced settings:

a. To allow the printer to broadcast the SSID on the wireless network, select the **Broadcast the SSID** checkbox.

   -or-

   To prevent the printer from broadcasting the SSID on the wireless network, clear the **Broadcast the SSID** checkbox.

b. To display the SSID on the configuration reports and printer control panel, select the **Show the Wireless Direct name on reports and the printer's control panel** checkbox.

   -or-

   To prevent the SSID from being displayed on the configuration reports and printer control panel, clear the **Show the Wireless Direct name on reports and the printer's control panel** checkbox.

c. To display the passphrase on the configuration reports, printer control panel, and Near Field Communication (NFC) record, select the **Show the Wireless Direct password on reports and the printer's control panel** checkbox.

   -or-

   To prevent the passphrase from being displayed on the configuration reports, printer control panel, and NFC record, clear the **Show the Wireless Direct password on reports and the printer's control panel** checkbox.

Wireless Station (802.11)

Use this option to configure the wireless network configuration parameters for an IEEE 802.11 wireless Ethernet connection.

In the **Wireless Mode** section, specify the following options:

1. **Wireless Mode**: Select the 802.11 wireless mode.
2. **Guard Interval**: Select the guard interval, which is the space between the symbols (or characters) that are transmitted. This space eliminates the intersymbol interference (ISI) that occurs when echoes or reflections from one symbol interfere with another symbol. Adding time between symbol transmissions allows these echoes and reflections to dissipate before the next symbol is transmitted and prevents propagation delays. Select one of the following options:
   - **Auto**: Select this option to use the default guard interval.
   - **Short**: Select this option to set the guard interval to 400 nsec.
   - **Long**: Select this option to set the guard interval to 800 nsec. A longer guard interval reduces the channel efficiency.
3. **Enable AMSDU Aggregation**: Select this option to enable Aggregated Mac Service Data Unit (A-MSDU), which increases the maximum size of the frame transmission from 2,304 bytes to 7,935 bytes. This option applies only to the 802.11n wireless mode.

NOTE: You can use the **Enable AMSDU Aggregation** and **Enable AMPDU Aggregation** options separately or together.

4. **Enable AMPDU Aggregation**: Select this option to enable Aggregated Mac Protocol Data Unit (A-MPDU), which allows a maximum size of the frame transmission of 64 KB. This option applies only to the 802.11n wireless mode.

5. **Enable Block ACKs**: Select this option to enable block acknowledgements (ACKs), which allow each of the aggregated data frames to be individually acknowledged or retransmitted if an error occurs. This option applies only to the 802.11n wireless mode.

In the **Communications** section, specify the following options:

1. **Network name (SSID)**: Enter the Service Set Identifier (SSID) to which the HP Jetdirect print server connects. The SSID identifies the extended service set (ESS) that is normally associated with larger networks in Infrastructure mode. The SSID is case sensitive.

   The print server lists the detected SSIDs. An empty (or blank) **Network name (SSID)** field is acceptable for networks that rely on the signal strength, encryption, and authentication methods to control network access.

   The factory default SSID configured on the HP Jetdirect print server is hpsetup. To initially communicate with the print server, the SSID for the wireless device must also be hpsetup.

2. **Infrastructure (access point)**: Select this option to allow wireless devices on the network to communicate by using an access point. To connect to the network, the settings on the wireless device must match the wireless connection settings for the access point. Select this option if the wireless devices must be in Infrastructure mode.

3. **Ad-hoc (peer-to-peer)**: Select this option to allow wireless devices on the network to communicate directly with each other. Other terms used for Ad hoc mode include Independent Basic Service Set (IBSS) and Computer-to-Computer mode. Ad hoc mode is the factory default configured on the HP Jetdirect print server.

   Channel: Select the radio frequency the print server uses to broadcast its availability if it fails to associate with the specified ad hoc network on any channel. The factory default is channel 11 (2462 MHz). Channel 10 (2457 MHz) is also available. To initially communicate with the print server, the wireless device must be configured for Ad hoc mode.

In the **Authentication and Encryption** section, specify the following options:

1. **No authentication or encryption**: Select this option if device authentication or security is not required to access the wireless network.

> NOTE: The network might continue to use WEP encryption keys for data privacy.

2. **WEP** (Wired Equivalent Privacy):

   - **Authentication**: Indicates the authentication mode for the specified WEP settings.

   - **WEP-Personal**: Select this option if the devices on the wireless network use a shared encryption key (or a shared password value) for network access and communication. Each device on the network must use the same key. The HP Jetdirect print server supports IEEE 802.11 WEP keys for encrypted network communications. If you select this option, specify the following settings to configure the WEP key:

  - **Input key in**: Select the format for the WEP key.

  - **WEP Key**: The WEP key format is programmatically determined and validated by using either alphanumeric ASCII (8-bit) characters or hexadecimal (4-bit) digits.

  - **Index**: Select the WEP key index position (1, 2, 3, or 4) the print server uses for encrypted communications from the list.

- **WEP-Enterprise**: Select this option if the network uses WEP with EAP/802.1x authentication. This type of security uses a central authentication server, such as Remote Authentication Dial-In User Service (RADIUS), to authenticate users on the network. If you select this option, specify the following settings to configure the authentication:

  - **Enabled protocols**: Select one or more of the following server-based authentication protocols:

    LEAP: Lightweight Extensible Authentication Protocol. A proprietary protocol from Cisco Systems that uses passwords for mutual authentication. During mutual authentication, the client and server authenticate each other.

    PEAP (configure certificate using EWS first): Protected Extensible Authentication Protocol. A mutual authentication protocol that uses digital certificates for server authentication and uses passwords for client authentication.

    EAP-TLS (configure certificate using EWS first): EAP using Transport Level Security. A mutual authentication protocol that uses digital certificates for server authentication and uses passwords for client authentication. For additional security, the authentication exchanges are encapsulated in TLS.

  - **Encryption strength**: Select the minimum encryption strength to use during communications with the authentication server. For each encryption strength, ciphers are specified to identify the weakest cipher allowed.

3. **WiFi Protected Access (WPA)**:

   - **WPA Version**: Select the WPA version.

   - **Encryption**: Select the encryption method.

   - **WPA-Personal**: Enter the security key that is used to generate the preshared key for authentication on the network. The security key must be entered in one of the following formats:

     - A passphrase that is 8 to 63 characters and consists of 0 through 9, a through z, A through Z, and numerous special characters that include the following:

       ! @ # $ % ^ & () _ + = – { } [ ] \ / “ < > ? “ ‘ ~

     - A security key that is 64 hexadecimal characters (0 through 9, and A through F).

   - **WPA-Enterprise**: Select this option if the network uses WPA with EAP/802.1x authentication. This type of security uses a central authentication server, such as RADIUS, to authenticate users on the network. Specify the following settings:

     - **Enabled protocols**: Select one or more of the following server-based authentication protocols:

       LEAP: Lightweight Extensible Authentication Protocol. A proprietary protocol from Cisco Systems that uses passwords for mutual authentication. During mutual authentication, the client and server authenticate each other.

       PEAP (configure certificate using EWS first): Protected Extensible Authentication Protocol. A mutual authentication protocol that uses digital certificates for server authentication and uses passwords for client authentication.

EAP-TLS (configure certificate using EWS first): EAP using Transport Level Security. A mutual authentication protocol that uses digital certificates for server authentication and uses passwords for client authentication. For additional security, the authentication exchanges are encapsulated in TLS.

- **Encryption strength**: Select the minimum encryption strength to use during communications with the authentication server. For each encryption strength, ciphers are specified to identify the weakest cipher allowed.

7 End-User License Agreement

When you download, register, and install HP Web Jetadmin, you must read the End-User License Agreement (EULA) and acknowledge that you agree to the terms.

After HP Web Jetadmin is installed, the EULA is available from the online Help. To view the EULA, go to **Help** > **About**, and then click the **View the End-User License Agreement** link.

Index