APPLICATION AND DEVICE SECURITY FOR HP WEB JETADMIN

CONTENTS

OVERVIEW

Protecting IT environments against loss or harm is crucial in today's data and system-driven world. HP Web Jetadmin provides tools and features that work in tandem with your device fleet to bring you superior security management. HP Web Jetadmin has a robust set of features that provide the following:

- Protection against the unauthorized use of HP Web Jetadmin
- Role-based administration using Microsoft® account management
- Feature enablement tied to an account login
- Control over device-based security features for both individual devices and batches of devices

This document discusses security details for HP Web Jetadmin in two sections—application security and device security. Note that this document does *not* cover all the aspects of device and application security that should be considered when managing devices or implementing software applications.

To meet the needs for higher levels of imaging and printing security, HP implemented a Storage Erase feature that meets the U.S. Department of Defense 5220-22.M requirements for clearing storage media when the administrator selects certain options and uses supported devices.

APPLICATION SECURITY

HP Web Jetadmin has the following features that make it easy to secure the application and its features:

- **Single sign-on**—Users do not have to provide password and user details to access the application.
- **.NET Remoting**—The client displays through a local application that uses Microsoft .NET Remoting as a secure means of communicating with the server.
- **Active Directory (AD) integration**—Domain accounts are used to identify who has access to the application and its features.[1]
- **Low-privilege service**—HP Web Jetadmin does not run as a system and has no direct access to key OS components. The client application runs under user credentials.[2]
- **Secure online downloads**—The HP Web Jetadmin installer and update files obtained from hp.com are digitally signed. This helps to ensure the integrity and authenticity of the files and underlying components as they are installed.
- **Optional SSL/TLS**—The ClickOnce client deployment can apply added security with certificates.

Roles and users

HP Web Jetadmin is a single sign-on application. A username and password are not always required if the user's Windows® user account has been granted access to an HP Web Jetadmin role.[3] The administrator can create roles that define the feature access to the client and enable and disable features for various user levels.

[1] For HP Web Jetadmin to validate AD user accounts, the HP Web Jetadmin host system must be joined to the AD domain.

[2] The HP Web Jetadmin service runs under NT AUTHORITY\Network Service, a local, built-in account on the server that hosts the application. By using this account, the HP Web Jetadmin service runs as a low-privilege service. HP does not support and strongly discourages changing the account that the HP Web Jetadmin service uses. Be aware that NT AUTHORITY\Network Service should have default access rights to its ServiceProfiles\Network directory (typically C:\Windows\ServiceProfiles\NetworkService\AppData\Local\HP Inc\HPWebJetadmin). During installation, HP Web Jetadmin also sets Read, Execute, and List permissions on the HP Web Jetadmin directory (usually in C:\Program Files\HP Inc) for the user NT AUTHORITY\Network Service. Finally, the Microsoft SQL Server instance that either the HP Web Jetadmin installer or the end user creates should log on as NT AUTHORITY\Network Service.

[3] For more information, including scenarios in which single sign-on is not the active log-in mechanism, see "User/role assignment" on page 3.

When the HP Web Jetadmin client application launches, the user is authenticated to the server using Windows Integrated Authentication. Features that have been disabled as a result of assigned role permissions cannot be viewed or accessed from the user's account. To log in to the HP Web Jetadmin server using a different Windows account user name, users must launch Microsoft Internet Explorer by going to **Internet Explorer** > **Start**, right-clicking **Programs**., and then selecting **Run As**.

HP Web Jetadmin administrator role

After installing HP Web Jetadmin, all accounts with membership to the local administrator group also have HP Web Jetadmin administrative account access to all the features and settings on the HP Web Jetadmin server. Within the client, this account role privilege is referred to as HP Web Jetadmin Administrator (Read Only). The administrator role is read-only and cannot be deleted. Any local user, domain user, or group that is part of the Microsoft local administrator group on the HP Web Jetadmin server host has full administrator rights to the HP Web Jetadmin server. Additional roles beyond administrator can be created to define access or privileges for different users based on their job functions.

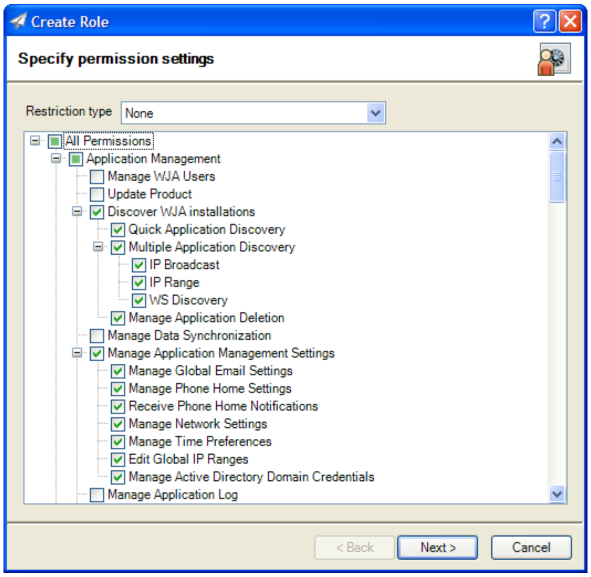
Create roles

Roles are created by launching the **Create Role** wizard (Figure 1). To launch the wizard, go to **Application Management** > **User Security** > **Roles**, and then click **New**.

Select **None** from the **Restriction type** list to display the global permission choices that apply to all parts of the application.

The **Groups** restriction type provides permission choices that are specific to device groups. The **Groups** permissions are discussed in "Device group restriction type" on page 6.

After the restriction type is selected, the permission settings can be defined (Figure 1). Use the checkboxes to enable or disable access to the application features. For example, you can allow access to device features for a group working in the helpdesk operations. These permissions can allow viewing device status and information, but not allow device configuration.



Restriction type: None

- ■ All Permissions
  - ■ Application Management
    - ☐ Manage WJA Users
    - ☐ Update Product
    - ☑ Discover WJA installations
      - ☑ Quick Application Discovery
      - ☑ Multiple Application Discovery
        - ☑ IP Broadcast
        - ☑ IP Range
        - ☑ WS Discovery
      - ☑ Manage Application Deletion
    - ☐ Manage Data Synchronization
    - ☑ Manage Application Management Settings
      - ☑ Manage Global Email Settings
      - ☑ Manage Phone Home Settings
      - ☑ Receive Phone Home Notifications
      - ☑ Manage Network Settings
      - ☑ Manage Time Preferences
      - ☑ Edit Global IP Ranges
      - ☑ Manage Active Directory Domain Credentials
    - ☐ Manage Application Log

Figure 1—Role permissions

After specific permission settings are configured, click **Next** to assign the **Role name**. After the role settings are complete, a **Confirm** page displays the selected settings. Next, the **Results** page shows the settings for the role and has an **Assign to users now** checkbox that is selected by default.

The name and permissions for an existing role can be changed. The restriction type cannot be changed. Roles can also be deleted. The deletion of a role is immediately applied to all the connected clients. To access existing roles, go to **Application Management** > **User Security** > **Roles**.

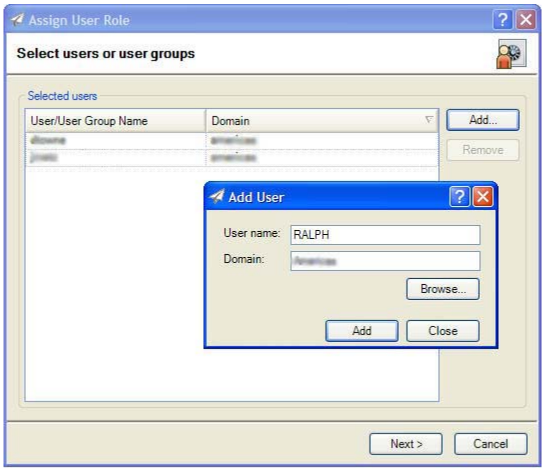
User/role assignment

Custom roles and the HP Web Jetadmin Administrator role can have one or more user assignments. Assign users and roles with Windows users or user groups. These users or user groups can be based in either the local system or the Windows domain.

HP Web Jetadmin servers that are joined to a Windows domain exist in the list of domain member computers. Users who log in to the computers are members of the domain. These users, as well as the user groups to which they belong, can be assigned to HP Web Jetadmin roles. After these assignments are made, users have access to the features defined by the role permissions settings.

To view and manage the user/role assignments, go to **Application Management** > **User Security** > **Roles** > **Users**.

- **Assign Role**—Launches the **Assign User Role** wizard that initially provides controls to select one or more users or groups (Figure 2).
- **User name**—Specifies the local or domain user account or group name.
- **Domain**—Specifies the Windows domain or the HP Web Jetadmin host name in the case of local users or groups.
- **Browse**—Finds users or groups on either the HP Web Jetadmin host or the Windows domain.



User/User Group Name	Domain
[redacted]	[redacted]
[redacted]	[redacted]

User name: RALPH

Domain: [redacted]

Figure 2—Assign user role

After clicking **Next**, one role can be selected for assignment. Group selection is possible when the role has a **Group**, which is discussed in "Device group restriction type" on page 6. After confirming the settings, the **Results** page shows the new user/role assignments. After these assignments are complete, users can access HP Web Jetadmin by browsing to the server without being prompted for a username or password.

Users and user groups can be selected when making user/role assignments. The following table shows how both user and user groups can be referenced when making user/role assignments.

Type	Domain	User/user group
Domain user	Domain name	User name
Domain group	Domain name	Domain group name
Local user	Computer name	Local user name
Local group	Computer name	Local group name

In most cases, the domain user, domain user group, or local user group is used in user/role assignment. The following are examples:

- Helpdesk employees are members of a domain group that the IT team manages. New helpdesk employees are automatically granted permissions to the HelpDesk role in HP Web Jetadmin by virtue of the domain group membership. The domain group membership is managed at the Windows domain.
- The HP Web Jetadmin administrator has many partners who also use HP Web Jetadmin. These users can be tracked locally by using a group on the HP Web Jetadmin installation host.

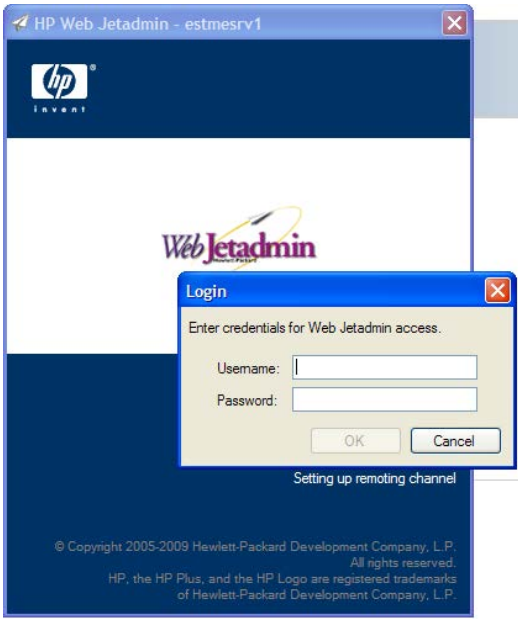
For more information about local or domain user accounts and domain or local groups, see the Microsoft security documents.

Existing user/role assignments can be edited to change or delete the user/user group or the HP Web Jetadmin role. To view the existing assignments, go to **Application Management** > **User Security** > **Users**.

NOTE At this time, HP Web Jetadmin does not support groups within groups. For example, assume that User A is a member of Group A and Group A is a member of Group B. If Group B is assigned to a role, User A does not have access to that role.

Alternate log-in prompt

In some cases, the client host and the server that hosts HP Web Jetadmin do not reside on the same or on any Windows security domain. An alternate log-in prompt (Figure 3) is provided so that users can enter log-in credentials other than the credentials that the current Windows session uses. Single sign-on is normally used to pass the identity of a user who is logged in to the local desktop Windows session to HP Web Jetadmin. If HP Web Jetadmin fails to authenticate this identity for any reason, it displays the alternate log-in prompt.



Enter credentials for Web Jetadmin access.

Username:

Password:

Setting up remoting channel

© Copyright 2005-2009 Hewlett-Packard Development Company, L.P.
All rights reserved.
HP, the HP Plus, and the HP Logo are registered trademarks
of Hewlett-Packard Development Company, L.P.

Figure 3—Alternate log-in prompt

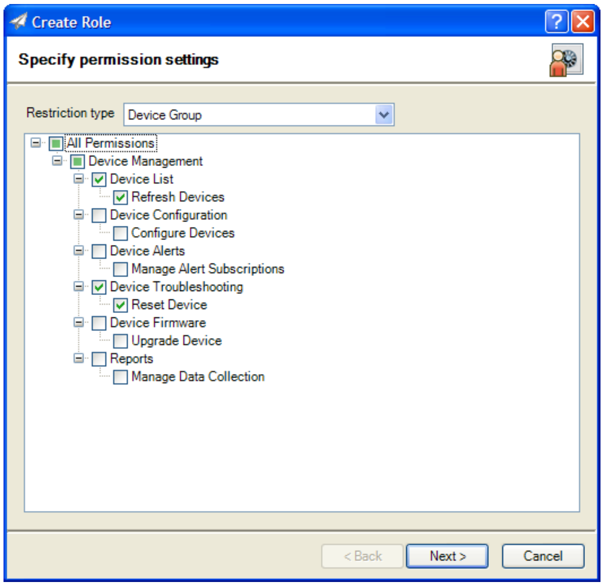
An alternate log-in prompt is useful in the following situations:

- An HP Web Jetadmin-authorized user accesses the software from an unauthorized person's desktop.
- The HP Web Jetadmin server is on a secured domain while the end-user desktops are not. However, the end users have log-in identities in this domain that have been given access rights in HP Web Jetadmin user/roles.
- Windows users are managed locally at the HP Web Jetadmin server and have been given access in HP Web Jetadmin to user/roles.

NOTE HP Web Jetadmin running on Windows XP Professional and other operating systems might continue to display **not authorized** messages even though the user has been authorized for user/roles features. If these messages continue to display, check the **Local Security Settings** on the Windows host running HP Web Jetadmin. Under **Local Policies** > **Security Options**, find the policy labeled **Network Security: Sharing and security model** for local accounts. Be sure this policy is set to **Classic, local users authenticate as themselves**. Always review the Microsoft documentation when adjusting security policies on Windows hosts.

Device group restriction type

A role can be created that has a **Restriction type** of **Group**. These roles provide access to features based on both user account and device group details. When the **Restriction type** is set to **Group**, the feature permissions that are available in the **Create Role** wizard are limited to device management items (Figure 4). After the role is named and settings are confirmed, this role is assigned to both users and device groups.



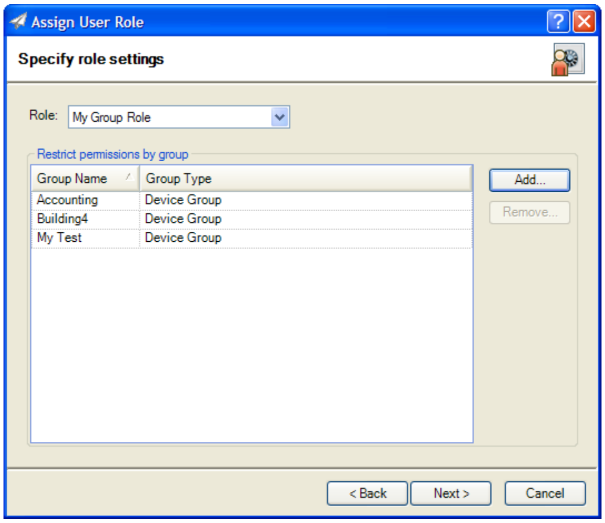
Specify permission settings

Restriction type: Device Group

- ■ All Permissions
  - ■ Device Management
    - ☑ Device List
      - ☑ Refresh Devices
    - □ Device Configuration
      - □ Configure Devices
    - □ Device Alerts
      - □ Manage Alert Subscriptions
    - ☑ Device Troubleshooting
      - ☑ Reset Device
    - □ Device Firmware
      - □ Upgrade Device
    - □ Reports
      - □ Manage Data Collection

Figure 4—Group restrictions

From the **Assign User Role** wizard (Figure 5), device groups *and* users are specified when the role selected has a group restriction type. When a role is selected that does not have this restriction type, the **Groups** area is unavailable and groups cannot be selected.



Specify role settings

Role: My Group Role

Restrict permissions by group

Group Name	Group Type
Accounting	Device Group
Building4	Device Group
My Test	Device Group

Figure 5—User/group role assignment

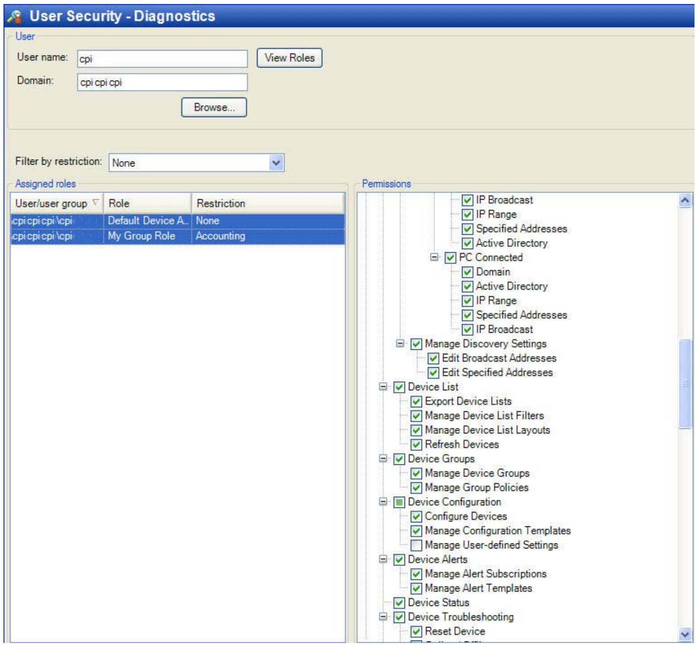
Using roles in restricted groups can be valuable, as in the case of regionalized helpdesk operations. Consider the following:

- The helpdesk in the north region is staffed by five people. All of these people are given permissions to the appropriate application features and are given HP Web Jetadmin feature access to the devices in their region.
- The helpdesk in the south region is staffed by eight people who have HP Web Jetadmin feature access to the devices in their region.

In both cases, the helpdesk has a role assignment on the same role, but for the appropriate group containing the devices in its region. The features needed to perform helpdesk tasks are specified by the role. The device groups are selected during the role assignment.

User/role diagnostics

Users can be assigned to multiple roles. A common scenario might be that a small helpdesk is staffed with 15 people. All of them are assigned to the HelpDesk role that gives them the ability to troubleshoot devices using the Status, Detailed Info, Troubleshooting, and Capabilities features. To keep device information up-to-date, two of the senior helpdesk staff are given additional access to the Configuration, Firmware,



User

User name: cpi

Domain: cpi cpi cpi

Filter by restriction: None

Assigned roles

User/user group	Role	Restriction
cpi cpi cpi \cpi	Default Device A...	None
cpi cpi cpi \cpi	My Group Role	Accounting

Permissions

- ☑ IP Broadcast
- ☑ IP Range
- ☑ Specified Addresses
- ☑ Active Directory
- ☑ PC Connected
  - ☑ Domain
  - ☑ Active Directory
  - ☑ IP Range
  - ☑ Specified Addresses
  - ☑ IP Broadcast
- ☑ Manage Discovery Settings
  - ☑ Edit Broadcast Addresses
  - ☑ Edit Specified Addresses
- ☑ Device List
  - ☑ Export Device Lists
  - ☑ Manage Device List Filters
  - ☑ Manage Device List Layouts
  - ☑ Refresh Devices
- ☑ Device Groups
  - ☑ Manage Device Groups
  - ☑ Manage Group Policies
- ■ Device Configuration
  - ☑ Configure Devices
  - ☑ Manage Configuration Templates
  - □ Manage User-defined Settings
- ☑ Device Alerts
  - ☑ Manage Alert Subscriptions
  - ☑ Manage Alert Templates
- ☑ Device Status
- ☑ Device Troubleshooting
  - ☑ Reset Device

Figure 6—User/role diagnostics

and Discovery features. In addition to the HelpDesk role, they have been given an assignment to another role named ExtendedHelp. These two users now have access to additional features beyond those needed by the normal helpdesk staff. HP Web Jetadmin uses the least restrictive permissions in its user/roles feature. A user can access any feature that is enabled in a role that has been assigned to that user.

Diagnostics can be used to observe the privileges granted to any user that has a user/role assignment (Figure 6). To access the diagnostics feature, go to **Application Management** > **User Security** > **Diagnostics**. To display the diagnostic information for a user, specify the **User name** and **Domain**, and then click **View Roles**.

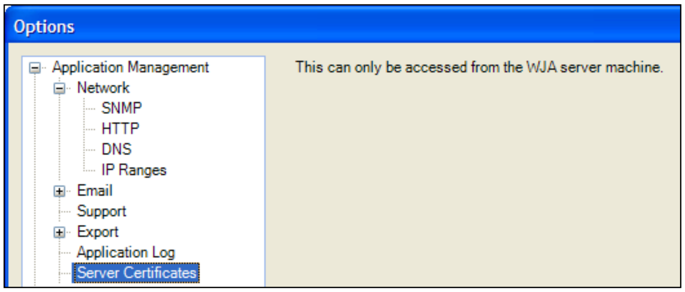
Manage the role permissions and user assignments

As already noted, user/role assignments, role permissions, and even local/domain user groups can be edited and changed. When managing these items, keep the following rules in mind:

- As users have role permission changes applied to them, the display interface does not change to reflect (hide) the feature access changes until the next time the user logs in to the application.
- As users have role permission changes applied to them, access to restricted features are blocked and the users receives an **access denied** message from the application in areas where feature restrictions have been implemented.
- Scheduled tasks implemented by users with role permission changes or authorization removals remain intact and are not affected by user/role or permission changes.

HTTPS and Secure Sockets Layer (SSL)

HP Web Jetadmin administrators can enable the Secure Sockets Layer (SSL) protocol on HP Web Jetadmin. This forces browser communication to the more secure HTTPS protocol. The administrator enables SSL from the console or host running the application. A notice occurs when users try to enable this feature from a remote client (Figure 7).



This can only be accessed from the WJA server machine.

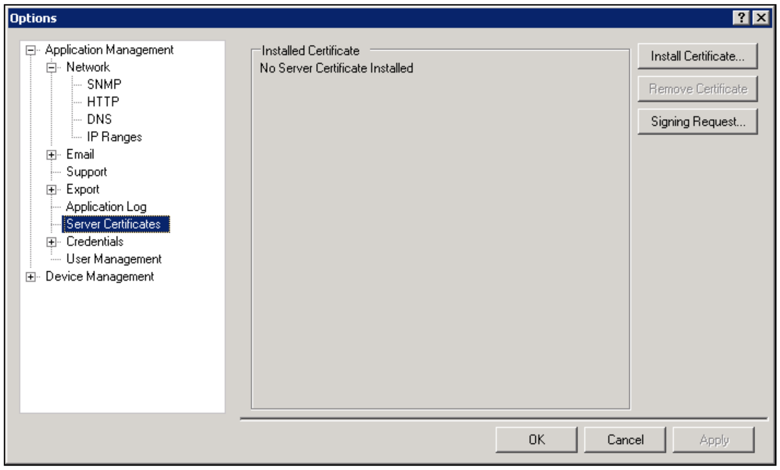
Figure 7—Certificates notice

Prior to HP Web Jetadmin 10, SSL was enabled by default and the primary client interface went through a web browser. SSL is not enabled by default on HP Web Jetadmin 10.x for the following reasons:

- HP Web Jetadmin 10.x does not use a web browser as a primary application interface.
- The HTTP service in HP Web Jetadmin 10.x provides minimal or limited functionality and is not core to the client/server communication. Microsoft .NET Remoting provides data encryption and user authentication.
- Self-signed certificates cannot be used unless all the clients have the appropriate Certificate Authority (CA) installed.

In some environments, SSL is required every time an HTTP interface or service is used for communication. The administrator can enable and enforce t SSL. When SSL is enforced, it provides an industry-accepted protocol for both authentication and encryption of HTTP communication. A host that requests access to the HP Web Jetadmin ClickOnce client download is assured that the system hosting HP Web Jetadmin is authentic and that communication between the two systems is encrypted.

SSL uses certificates to accommodate both authentication and encryption. HP Web Jetadmin can generate a signing request that a CA can use to generate a certificate. From the application console only, the user can generate a signing request through **Tools** > **Options** > **Application Management** > **Server Certificates** (Figure 8).



Installed Certificate
No Server Certificate Installed

Figure 8—Server certificates

After the CA fulfills the request, the certificate is ready to be installed on the HP Web Jetadmin application. The Install Certificate feature is used to browse to and upload the certificate file. After the certificate is installed, the HTTP service enforces SSL. Any web browser contact with HP Web Jetadmin should indicate HTTPS in the URL when SSL is enforced. The Remove Certificate feature uninstalls the certificate and SSL is no longer enforced.

Important points to remember when implementing SSL

SSL-enforced client communication requires one or more of the following considerations:

- When SSL is implemented on HP Web Jetadmin with an internal 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 ClickOnce page fails to load.
- Proxy servers tend to use the standard SSL port, which is port 443. If the HP Web Jetadmin ClickOnce page is called through a proxy server, a redirect error might occur because the URL is redirected to port 443 rather than port 8443, which is the port that SSL in HP Web Jetadmin uses. The workaround for this problem is to place the fully qualified domain name (FQDN) for HP Web Jetadmin in the browser's exceptions list under **Tools** > **Internet Options** > **Connections** > **LAN Settings** > **Advanced**. The browser pulls HTTP and HTTPS content directly from the HP Web Jetadmin server.

  NOTE The HTTP and HTTPS port numbers in HP Web Jetadmin HTTP and HTTPS can be changed to something other than ports 8000 and 8443. A procedure for implementing custom ports is outlined in the online Help for HP Web Jetadmin.
- When a user implements SSL in HP Web Jetadmin, a redirect occurs when the browser URL uses port 8000. For example:
  - Known URL prior to SSL implementation: http://servername.domain.domain.xxx:8000
  - After SSL implementation, HP Web Jetadmin redirects to the new URL: HTTPS://servername.domain.domain.xxx:8443
- The URLs shown here use FQDN. In most cases the certificate issued and installed in the SSL implementation for HP Web Jetadmin contain an FQDN for the host on which HP Web Jetadmin is installed. If a non-FQDN is used in the browser, a certificate failure occurs. As a general rule, create the HP Web Jetadmin URL with FQDN when HP Web Jetadmin is implemented with SSL.
- The server host FQDN used in the certificate must be DNS resolvable. If it is not, the client application might fail to launch.

Certificates and backup/restore procedures

HP Web Jetadmin provides backup and restore scripts and instructions for qualifying and using them. These scripts are designed to help the administrator save time when a catastrophic hardware, operating system (OS), or application failure occurs. The backup and restore scripts act on the HP Web Jetadmin database and the HP Web Jetadmin settings files. Most software settings and device data can be restored.

The certificate used to enforce HTTPS/SSL communications is not retained or restored during the backup and restore processes. The certificate is installed in the local Windows certificate store. The following outcomes are possible when using the HP Web Jetadmin restore scripts on a server that has HTTPS/SSL enabled:

- If HP Web Jetadmin is restored to a host where the certificate is already installed and if the application settings have SSL enabled, HP Web Jetadmin enforces SSL using that certificate.
- If HP Web Jetadmin is restored to a host where the certificate is not installed and if SSL is enabled through application settings, HP Web Jetadmin runs without SSL enforced. A certificate must be installed on the server using **Tools** > **Options** > **Application Management** > **Certificates** as described previously. Always test to make sure that SSL is enabled and being enforced when performing an HP Web Jetadmin restore.

Digital signatures

HP Web Jetadmin uses digital signatures for all of its packages and plug-in descriptor files to ensure file integrity and authenticity. All files downloaded from hp.com for product updates are digitally signed. HP Web Jetadmin verifies the digital signatures by using a Verisign-managed root certification authority. During the application installation, this root CA is installed in the Trusted Root Certification Authorities location in the Local Machine certificate store. Files and packages are signed by a certificate derived from this CA chain. If authentication of a package or file fails, HP Web Jetadmin refuses to load it. This industry-standard infrastructure also uses Certificate Revocation Lists (CRLs) to track any certificates that might have been revoked. If necessary, the most up-to-date CRL can be manually obtained at:

http://onsitecrl.verisign.com/HewlettPackardCompanyEIPPrintingDeviceCSID/LatestCRL.crl

Network ports

HP Web Jetadmin uses the following ports.

Port number	Type	Inbound/Outbound (I/O)	Details
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 (EWS) on the device.
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.

Port number	Type	Inbound/Outbound (I/O)	Details
443	TCP	O	Web Services (HTTPS): HP Web Jetadmin uses this port to manage some newer HP devices. HP Web Jetadmin sends device configuration as well as queries to this port.
445	UDP	O	WMI Communication: Windows Management Instrumentation (WMI) is a protocol on Microsoft Windows hosts. HP Web Jetadmin uses WMI to detect the presence of a printer on the Windows host. This is one of the ports on the Windows host that WMI uses to allow communication from outside servers, including servers running HP Web Jetadmin.
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.
1434	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	UDP	O	WS Discovery: HP Web Jetadmin uses this port to perform a Web Services discovery on newer HP devices.
3910	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.
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	TCP	O	Web Services (HTTPS): HP Web Jetadmin uses this port to manage communications on some newer HP devices. The HPWSProAdapter Service, which is an additional service that HP Web Jetadmin launches, opens this port.
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, online Help content, and device file transfer operations.
8050	TCP	I	Device Eventing Callback (HTTPS): Newer HP devices use a WS eventing protocol for management communications.
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.

Port number	Type	Inbound/Outbound (I/O)	Details
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.
37893	UDP	I	WS Hello Listener: HP Web Jetadmin monitors this port for incoming WS Hello packets from the HP WS Pro Proxy Agent software installed on hosts in the enterprise. When HP Web Jetadmin detects a packet, it follows up to determine if there are any discoverable printers on the sending host. For more information, see the *HP Web Jetadmin Proxy Agents Readme*. This document is available by going to the HP Web Jetadmin support page.
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.

NOTE 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.

NOTE 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 the internal HPWSProAdapter service.

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

HPWJA Service

HPWJA Service is core to the HP Web Jetadmin application and runs under the low-privilege Microsoft user account called NT Authority\Network Service. Many environments require that applications such as HP Web Jetadmin do not have administrative access to the operating system.

SQL Server (HPWJA)—database access and authentication

For HP Web Jetadmin 10.3 SR8 and later, a SQL Server 2012 Express database instance is created during the installation. For HP Web Jetadmin 10.3 SR7 and earlier, SQL Server Express 2005 is installed.

NOTE When upgrading HP Web Jetadmin, the existing version of SQL Server does not change. For instructions how to upgrade a SQL Express version for HP Web Jetadmin, see the *Upgrade Microsoft® SQL Server Express for HP Web Jetadmin* white paper. This white paper is available from the HP Web Jetadmin support page.

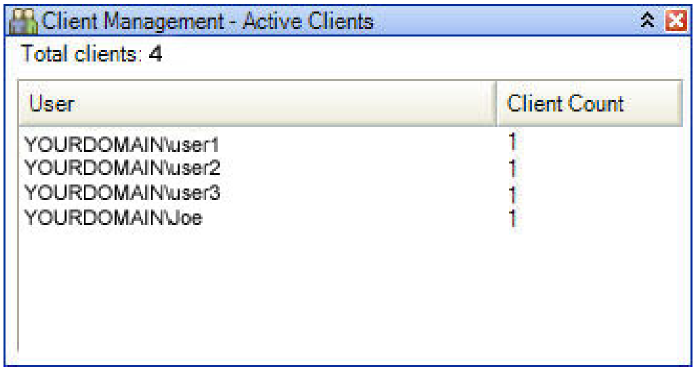
HP Web Jetadmin uses Windows credentials to access this database instance. The service for this database instance runs under the NT Authority\Network Service user and is named SQL Server (HPWJA). HP Web Jetadmin uses the Network Service account in the local Windows system to access SQL Server. Sensitive information, such as device credentials and other data identity settings, are encrypted and stored securely in the SQL Server data tables.

NOTE As of November 2009, HP Web Jetadmin 10.2 SR1 (10.2.62227) can be configured to use a remote instance of SQL Server and authenticate using a SQL user account. Windows authentication to the SQL Server instance and secure, certificates-based authentication are not currently possible. This might be considered a security vulnerability in some environments.

During SQL authentication, the SQL username and password are hidden to prevent casual observation. However, using HP Web Jetadmin on untrusted networks might be a concern to some administrators.

Active Clients task module

The Active Clients task module can be activated and viewed from the **Task Module Docking** area or from **Application Management** > **Overview**. This task module shows the clients who are logged in to HP Web Jetadmin and the number of active client applications that each client is running. This feature helps the administrator determine which clients are logged in to the system prior to running product updates or performing tasks that might burden the system and cause slow performance. A short custom message can be sent to clients using **Tools** > **Broadcast Message**, which is available from **Application Management** (Figure 9).



Total clients: 4

User	Client Count
YOURDOMAIN\user1	1
YOURDOMAIN\user2	1
YOURDOMAIN\user3	1
YOURDOMAIN\Joe	1

Figure 9—Active Clients task module

DEVICE SECURITY

In many environments, password policies require the device administrator to periodically reconfigure the security credentials. HP Web Jetadmin is a powerful device management tool because it can configure many devices at once. This saves administrators from having to contact each device separately to assign configuration items such as passwords and other credentials.

Device passwords, community names, ports, and other credentials are used to prevent unauthorized access. Even though an HP Web Jetadmin installation is secure, other HP Web Jetadmin installations and other utilities can access devices. These can include the following:

- HP Web Jetadmin
- Telnet
- HP Embedded Web Server (EWS)
- Other SNMP utilities

The protocols that these and other utilities use include the following:

- SNMP over UDP—changes to PML objects
- SNMP over UDP—changes to PML objects
- RFU file through port 9100 over TCP—printer firmware upgrades
- PJL file through port 9100 over TCP—changes to PML objects
- PCL file through port 9100 over TCP—changes to PML objects
- NFS over TCP—changes to storage, such as a hard disk

In addition to providing additional security methods to prevent unwanted device configuration, HP Web Jetadmin provides security against unwanted printing. For example, printing can occur to printers using the following techniques:

- HP Standard Port Monitor
- HP Jetdirect port

- Microsoft Standard Port Monitor
- LPD
- FTP
- IPP

Passwords and credentials

To prevent unauthorized access to device configuration interfaces, several password and credential options are available. Setting these items through HP Web Jetadmin is possible in both the batch and single device configuration modes. In addition to configuring passwords and credentials from HP Web Jetadmin, the administrator can protect these items through the Credential Store.

Security settings are consolidated in the **Security** category on the **Config** tab so they are easy to find and manage. Security settings can also be stored in device configuration templates so they can be applied through schedules and group configuration policies. Security settings can also be customized in the **My Settings** category so that an individual user can easily find and configure all the settings that are considered critical to security.

Credentials Store

The Credentials Store prevents HP Web Jetadmin users from having to provide device credentials every time one or more devices require credentials. The Credentials Store also facilitates batch and background device operations.

The Credentials Store uses a portion of the HP Web Jetadmin SQL Server database that securely encrypts and stores device credentials whenever a correct credential value is authenticated. These values are stored on a per-credential and per-device basis. HP Web Jetadmin uses the following HP device credentials:

- **EWS Password**—Blocks unauthorized access to the device-embedded HTTP interface. This password is synchronized with the HP Jetdirect Telnet password.
- **PJL Password**—Blocks unauthorized PJL command strings.
- **File System Password**—Protects the printer disk and other storage facilities from unauthorized access.
- **SNMPv3 Credentials**—Consists of the user name, passphrase1 and passphrase2 that are used when SNMPv3 is enabled. This version of SNMP secures and authenticates communication between management applications, such as HP Web Jetadmin, and the device. This protocol is used when strong security is required.
- **SNMP Set Community Name**—Provides the grouping mechanism for SNMPv1/SNMPv2 that many users have adopted as a security mechanism. Device configuration is not possible without knowledge of the Set name value. However, the Set name value traverses the network in clear text and can be *sniffed*, or viewed, by eavesdroppers.
- **SNMP Get Community Name**—Provides a mechanism that is used sometimes to prevent device discovery from other HP Web Jetadmin installations. Devices do not respond to Get packets that do not contain the correct value. However, the Get name value traverses the network in clear text and can be sniffed by eavesdroppers.

The following actions cause the value of any credential to be stored:

- **Configuration**—The credential value is stored after it is configured on the device.
- **Use**—The credential value is stored when it is used during a configuration and the software has not previously stored the credential.

The application reuses the stored credentials whenever a requirement for them is encountered. A user who configures a device that has had a credential stored is not required to re-enter the credential in the application. The application uses the credential as a background operation in the HP Web Jetadmin server's steps to configure the device.

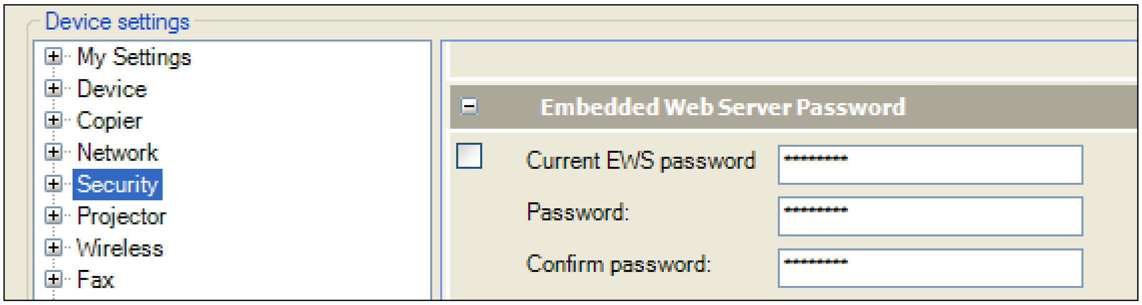
After a backup and restore, the content of the Credential Store is retained if the restore occurs on the same machine with the same OS. If the restore occurs on a different machine or the OS is rebuilt between the backup and the restore, all the credentials are lost.

NOTE Instructions and sample script files for the backup and restore procedures are in the following HP Web Jetadmin installation directory:

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

Configure a device credential

Figure 10 shows the configuration item that is used to set the EWS password.



□ Current EWS password: *********

Password: *********

Confirm password: *********

Figure 10—EWS password configuration item

Before HP Web Jetadmin sets the device credential, the software authenticates the user's knowledge of the credential. This is true in both the batch and single device configuration modes for password or credential configuration. After a password or credential is successfully configured or changed, it is added to the Credentials Store as an encrypted value.

Credentials delegation

With credentials stored, HP Web Jetadmin can apply them transparently any time the need arises. HP Web Jetadmin uses these passwords or credentials during a live configuration or during automated background tasks, such as scheduled firmware upgrades or configurations. When configuring devices, users do not have to know the credential to perform the configuration. The user just needs access to HP Web Jetadmin and the device configuration features. This is called *credentials delegation*.

Credentials delegation is used to allow device configuration without having to share confidential credential information across a large distribution. The IT staff can control and configure devices while IT administrators control and configure passwords. Any user with access to devices and configuration features has delegated access to the Credential Store.

Credentials settings and global credentials

Controls for adding global multiple try-values for each of the following credential types can be found under **Tools** > **Options** > **Application Management** > **Credentials**:

- EWS Password
- File System Password
- SNMPv3 Credentials
- SNMP Set Community Name

- SNMP Get Community Name

The user sets the global credentials. HP Web Jetadmin then uses the global credentials when a credential is needed, but the credential is not available in the Credentials Store. Multiple values can be set for global credentials. HP Web Jetadmin tries each credential value in the stack until it encounters success. If the application uses a global credentials value and it results in a success, that value is stored for that device in the Credentials Store. If success is not achieved, the device is placed in a credentials needed state.

In **Tools** > **Options** > **Credentials**, the following options are available to clear the stored credentials:

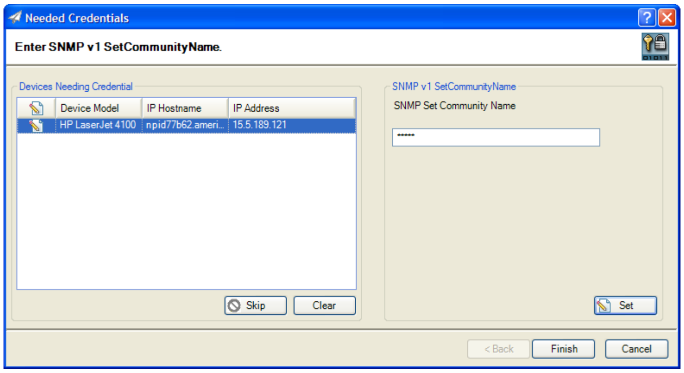
- **Clear All Credentials**—Removes all the device credentials from the Credentials Store in the HP Web Jetadmin database.
- **Clear Global Credentials**—Clears all the global values stored in each of the credential types.

Credentials needed

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

1. Checks the store for the credential.
    - If the credential exists, attempts the configuration using the credential value.
    - If the credential does not exist, goes to the global credentials.
    - If the credential succeeds, stops.
    - If the credential fails, goes to the global credentials.
2. Checks for a global credential.
    - If a global credential exists, attempts the configuration using the global credential value.
    - Else, logs a credential-needed, and prompts the user if it is a live configuration session.
    - If the credential succeeds, stops, and adds the credential to the device store.
    - Else, logs a credential-needed, and prompt the user if it is a live configuration session.

During a live user-attended configuration session, HP Web Jetadmin prompts for credentials (Figure 11).



Needed Credentials

Enter SNMP v1 SetCommunityName.

Devices Needing Credential

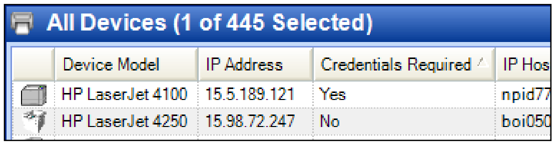
	Device Model	IP Hostname	IP Address
	HP LaserJet 4100	npid77b62.ameri...	15.5.189.121

SNMP v1 SetCommunityName

SNMP Set Community Name: ******

Figure 11—Needed Credentials dialog

If the user did not supply the credential or the session was not live, the device is flagged as requiring credentials. This state can be observed in the **Credentials Required** column that can be enabled in any device list (Figure 12). To resolve this state, users can right-click the device, and add the needed credential to the system.



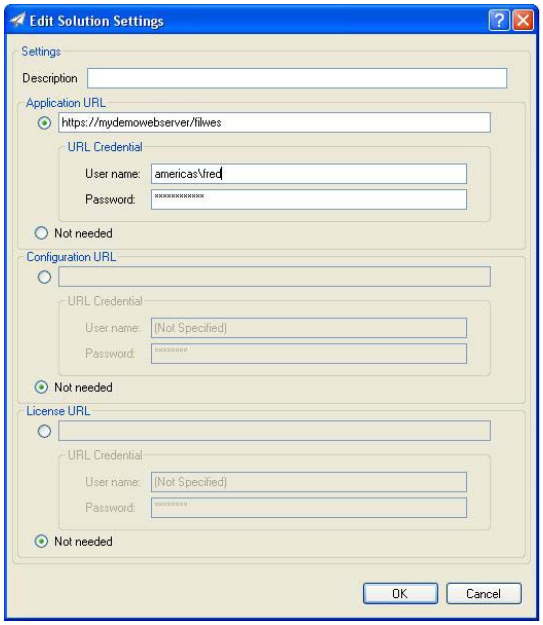
All Devices (1 of 445 Selected)

	Device Model	IP Address	Credentials Required	IP Hos
	HP LaserJet 4100	15.5.189.121	Yes	npid77
	HP LaserJet 4250	15.98.72.247	No	boi050

Figure 12—Credentials Required column

Sensitive device information

In some cases, HP Web Jetadmin sends sensitive information to the device. This information can include user and password details (Figure 13). In this case, HP Web Jetadmin uses SSL/TLS to send the information. 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 SSL/TLS, HP Web Jetadmin uses the certificates stored on the printer's HP Jetdirect network interface. These certificates can be self-signed or they can be signed by a verifiable CA. At this time, HP Web Jetadmin does not check the authenticity of certificates stored on the device. HP Web Jetadmin simply uses the certificate when communicating with the device through SSL/TLS. This security limitation might be exploited to allow unauthorized individuals to access sensitive information. Administrators should keep this in mind when using HP Web Jetadmin to manage sensitive device information.



Edit Solution Settings

Settings

Description:

Application URL

● https://mydemowebserver/filwes

URL Credential

User name: americas\fred

Password: ************

○ Not needed

Configuration URL

○

URL Credential

User name: (Not Specified)

Password: ********

● Not needed

License URL

○

URL Credential

User name: (Not Specified)

Password: ********

● Not needed

Figure 13—Solutions settings include user/password

Notes about backups and restores

HP Web Jetadmin stores many items securely in the SQL Server data tables that it uses for all information storage and retrieval. Much of this information is considered sensitive and is encrypted in these data tables. HP Web Jetadmin uses security techniques that include tying this data encryption to the Windows certificate that is unique to each instance of Windows. For this reason, many securely stored items do not traverse a restore when this operation is being performed on a new or different instance of Windows. These items include the following:

- All stored device credentials
- Sensitive device configuration items stored in templates, such as account details and passwords
- Any other device-based credentials that are either stored for retrieval and use by HP Web Jetadmin or used for device configuration

IMPORTANT Backup data, including the HP Web Jetadmin Settings directory backup and HP Web Jetadmin/SQL Server backup .dat files, should be secured. These files might contain sensitive information and should not be stored unsecured.

Get Images feature

HP Web Jetadmin users can retrieve files directly from the Internet by using the Get Images feature in the Firmware Repository. These files can be automatically stored on the HP Web Jetadmin server.

The HP Web Jetadmin client application runs on the end-user host computer. The client application can contact hp.com and acquire an index file that shows all the available HP Jetdirect, printer, and MFP firmware images. The user can select the firmware images to download to the client. The downloaded files are passed to the HP Web Jetadmin server host. The files are then available in the Firmware Repository and can be installed on HP devices by using the Firmware Upgrade feature.

The HP Web Jetadmin server and client applications do not check the authenticity of either the downloaded files or the systems hosting them. The software simply uses the HTTP protocol to contact an hp.com URL and uses the same HTTP protocol to download the files. Administrators should be aware that this might constitute a security weakness in their particular environment.

To address this weakness, administrators and users can download HP printer and MFP firmware in self-extracting, signed files as follows:

1. Use Internet Explorer to visit the HP Support and Drivers Web pages at hp.com for a particular product model.
3. On the **Download Drivers and Software** page, select the file to download, and then click **Download**.
4. On the **Do you want to run or save this file?** dialog box, click **Run**. The file is downloaded, and the **Do you want to run this software?** dialog box appears.
5. Verify that the publisher displayed is HP.
6. Optionally, click **HP** to examine the digital signature information.
7. If the publisher information is correct, click **Run** to extract the driver from the self-extracting file.
8. To upload the extracted firmware image to HP Web Jetadmin, go to **Device Management** > **Firmware** > **Repository**, and then click **Import**.

NOTE At this time, HP does not sign firmware image downloads (DLD files) for HP Jetdirect print servers.

Device disk security

Managing device credentials and passwords primarily prevents unauthorized management and configuration. The following are other ways to protect devices. HP Secure Erase technology is applied in two different ways to remove data from storage devices.

- **Secure File Erase**—Erases files on a continuous basis as soon as they are no longer needed to perform the requested function. This feature controls the way a device deletes its files on an ongoing basis and is set in the **File System** category (Figure 14). The mode in which a device erases its files can be set to Non-secure Fast Erase, Secure Fast Erase, or Secure Sanitizing Erase.

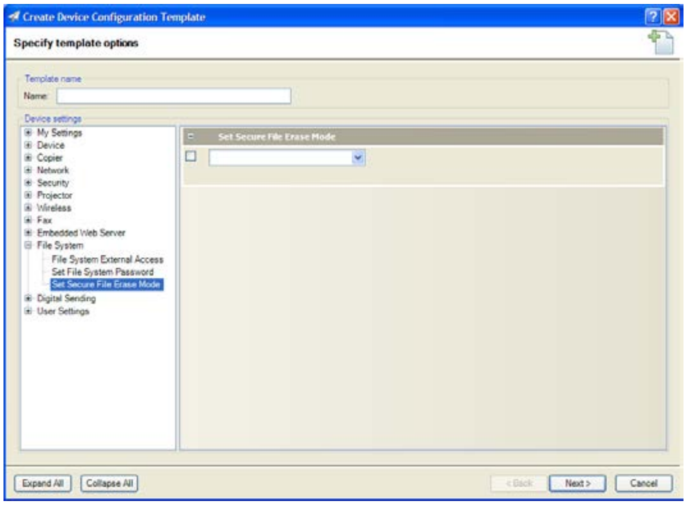


Figure 14—Secure File Erase option in configuration

- **Secure Storage Erase**—Removes all non-essential data from storage devices in a manner consistent with preparation for decommissioning or redeployment. This operation can be initiated on demand or scheduled for a later time. Secure Storage Erase is a device feature that can be invoked from the **Storage** tab on any device list for one or more devices. When this feature is invoked, it clears all the user files from the disk in one of the three erase modes.

HP Secure Erase technology provides a choice of three modes of erase security. An administrator can configure each erase security mode and can protect them from unauthorized changes with a password. The following are the erase security modes:

- **Secure Sanitizing Erase**—This mode conforms to the U.S. Department of Defense 5220-22.M specification for deleting magnetically stored data. This mode uses multiple data overwrites to eliminate trace magnetic data and also prevents subsequent analysis of the hard disk drive's physical platters for data retrieval.
- **Secure Fast Erase**—This mode completes the erasure faster than Secure Sanitizing Erase mode. This mode overwrites the existing data once and prevents software-based undelete operations on the data.
- **Non-secure Fast Erase**—The mode is the quickest of the three erasing modes. This mode marks the print job data as deleted and allows the MFP's operating system to reclaim and subsequently overwrite the data when needed.

Other access controls

Managing device credentials and passwords primarily prevents unauthorized management and configuration. The following areas describe other ways of protecting devices.

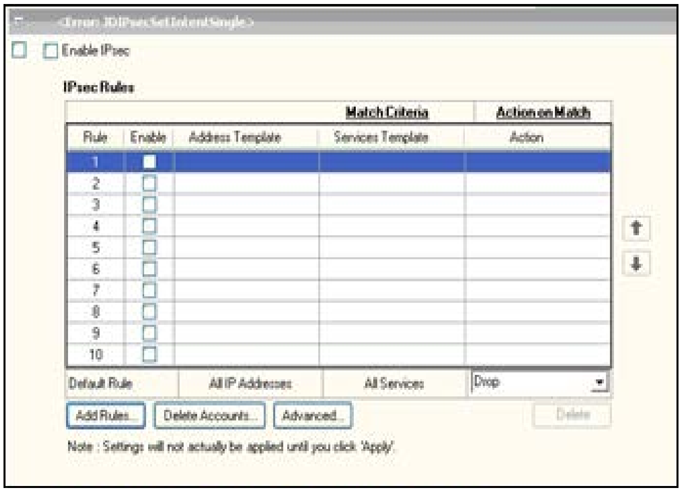
NOTE This document does not cover all of the device security features.

HP Jetdirect IPsec plug-in

HP Web Jetadmin offers plug-in packages that add functionality through the Application Update feature. The IPsec plug-in is used to manage security policies on HP Jetdirect print servers. This plug-in can be obtained directly through the **Application Management** > **Application Update** feature if the application is capable of communicating with hp.com. Alternatively, users can download the application update package file from www.hp.com/go/wja.

After the plug-in is installed, extra device configuration items are available in the **Network** configuration category (Figure 15). These configuration items can be used to apply and manage IPsec policies on the HP Jetdirect devices. Through an IPsec policy, IP traffic can be processed or discarded and processed traffic can be protected by IPsec authentication and encryption protocols. For more information about the IPsec configuration, see the online Help after the plug-in is installed.

For more information about IPsec and other device security, see www.hp.com/go/secureprinting.



<Error: JDIPsecSetIntentSingle>

□ □ Enable IPsec

IPsec Rules

			Match Criteria	Action on Match
Rule	Enable	Address Template	Services Template	Action
1	□			
2	□			
3	□			
4	□			
5	□			
6	□			
7	□			
8	□			
9	□			
10	□			
Default Rule		All IP Addresses	All Services	Drop

Note : Settings will not actually be applied until you click 'Apply'.

Figure 15—IPsec configuration in HP Web Jetadmin

Disable unused protocols and services

Many paths exist for providing both configuration and print access to devices. The **Enable Features** option can be used to disable unused items on single or multiple devices.

Control panel lock

Many HP devices have a security feature that locks the control panel to varying degrees. Control panel lock settings vary by device model. See the device documentation to determine the best settings for a given environment.

Other device security features

Security features can depend on the device feature set. However, the following items can be configured from HP Web Jetadmin. See the device documentation when working with any of these items.

- **Color access control**—Color functionality on devices can be restricted on a by-user, group, or application basis.
- **MFP access**—There are a large number of feature and authentication settings to ensure authorization for features such as scan-to-email and scan-to-fax.
- **Jetdirect access control list**—A feature used to lock out IP address connections.
- **Encryption**—Some network communication with devices can be encrypted by using SNMPv3, device-based SSL, or both methods.
- **Disable direct ports**—A feature used to lock the physical hardware ports on a device.
- **Disable RFU firmware upgrade**—A feature used to prevent unauthorized firmware images from being implemented on devices.

c01840730EN, Rev. 8, April 2016