whitepaper

Security
and HP Web Jetadmin 10.1

Table of Contents:

Overview 2

Part 1 – Application Security 2
- Application Security - HP Web Jetadmin Roles and Users 2
  - The HP Web Jetadmin Administrator Role 3
  - Creating Roles 3
  - User/Role Assignment 3
  - User/Role Assingment in Workgroups 5
  - Roles, Device Group Restriction Type 5
  - User/Role Diagnostics 6
  - Managing Role Permissions and User Assignments 6
  - HTTPS & SSL (Secure Sockets Layer) 7
  - Important Points to Remember when Implementing SSL 8
  - HP Web Jetadmin Certificates and Backup/Restore Procedure 8
- Application Security – Other Application Security Items 9
  - Digital Signatures 9
  - Network ports 9
  - HPWJA Service 9
  - SQL Server (HPWJA) – Database Access and Authentication 10
  - HP WJA Update Service 10
  - Active Client Task Module 10

Part 2 – Device Security 10
- Device Security – Passwords and Credentials 11
  - The Credentials Store 11
  - Configuration of a Device Credential 12
  - Credentials Delegation 12
  - Credentials Settings and Global Credentials 13
  - Credentials Needed 13
  - Jetdirect Device Password Discontinuance 14
- Device Disk Security 14
- Device Security – Other Access Controls 15
  - HP Jetdirect IPsec Plug-in for HP Web Jetadmin 10.1 15
  - Disable Unused Protocols & Services 16
  - Control panel lock 16
  - Other Device Security Features 16

Overview

Protecting IT environments against loss or harm is crucial in today's data-and system-driven world. HP Web Jetadmin 10.1 has tools and features that work in tandem with your device fleet to bring you superior security management. HP Web Jetadmin 10.1 has a robust set of features that allow:

- protection against unauthorized use of the application.
- roles-based administration using Microsoft account management, and
- feature enablement tied to account login.
- single and batch control over device-based security features

This document discusses security details for HP Web Jetadmin 10.1 in two parts: Application Security and Device Security. Please note that this document does *not* cover all device or application security aspects that should be considered when managing devices or implementing software applications.

To meet the needs for higher levels of print and imaging security, HP has implemented a storage erase feature which 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.

Part 1 – Application Security

HP Web Jetadmin 10.1 has several features that make it easy to secure the application and its features:

- **Single sign-on** –users don't have to provide password and user details in order to access the application.
- **.NET Remoting** – the client displays through a local application that uses .NET Remoting as a secure means of communicating with the server.
- **Active Directory Integration** – domain accounts are used to identify who has access to application and features.
- **Low privilege service** – HP Web Jetadmin 10.1 does not run as system and has no direct access to key OS components (Client application runs under user credentials).
- **Secure on-line downloads** – product update packages are signed ensuring integrity and authenticity of files and components downloaded from the Web.
- **Optional SSL/TLS** – ClickOnce client deployment can have added security applied via certificates.

Application Security - HP Web Jetadmin Roles and Users

HP Web Jetadmin 10.1 is a single sign-on application, which means user/password detail is not required to gain access to the application if the user's Windows user account has been granted access to an HP Web Jetadmin Role. Through the HP Web Jetadmin 10.1 client, HP Web Jetadmin administrator-created Roles define feature access. These Roles enable and disable features for the various users logged into HP Web Jetadmin10.1.

When the HP Web Jetadmin 10.1 client application is launched, the user is authenticated to the server using Windows Integrated Authentication. Features that have been disabled as a result of assigned role permissions are not viewable or accessible from that account after logging in with the HP Web Jetadmin 10.1 client. To log in to the HP Web Jetadmin 10.1 server using a different

windows account user name, users must launch Microsoft Internet Explorer using the *Run As…* feature (which is accessed through *Internet Explorer* > *Start* and then right-clicking on *Programs*).

The HP Web Jetadmin Administrator Role

Following the installation of HP Web Jetadmin 10.1, all accounts that are members of the local Administrators group will have also have Web Jetadmin Administrative account access to all features and settings of the HP Web Jetadmin 10.1 server. Within the HP Web Jetadmin 10.1 client, this account role privilege is referenced as *HP Web Jetadmin Administrator (Read Only)*. The HP Web Jetadmin 10.1 Administrator role is a read-only role and cannot be deleted. Any local user, domain user/group that is part of the Microsoft local Administrator group of the HP Web Jetadmin 10.1 server host will have full administrator rights to the HP Web Jetadmin 10.1 server. Roles beyond the HP Web Jetadmin administrator can be created to define access or privileges to different.

Creating Roles

Role creation is performed by launching the *Create Role* tool from within *Application Management* > *User Security* > *Roles* and selecting *New* (Figure 1).

- First, select the restriction type of *None* for global permission choices that apply to all parts of the application.
- The *Groups* restriction type provides permission choices that are specific to Device Groups. Groups permissions are discussed later.

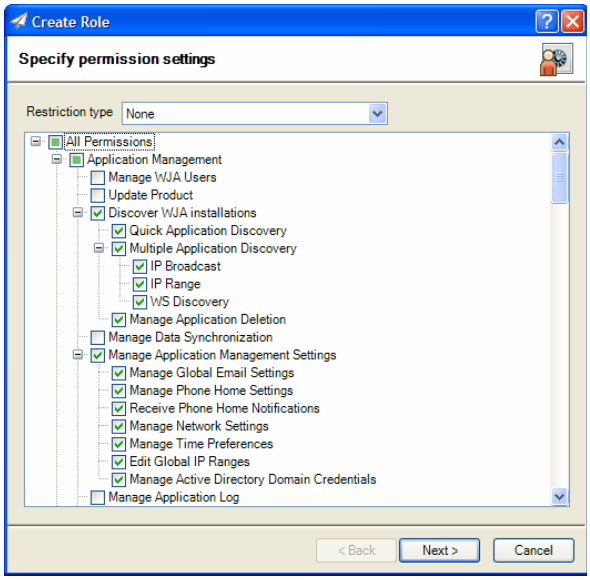

Figure 1 – Role Permissions

After the restriction type is selected, the permission settings can be defined (Figure 1). Use the checkboxes to enable or disable access to application features. An example is allowing use of device features may apply to a group working within Helpdesk operations. These permissions could allow viewing device status and information but not configuring devices.

Once specific permission settings have been configured and the *Next* button is selected, the *Role Name* is assigned. Once Role settings are complete, a *Confirm* screen is displayed showing the selected settings. The *Results* screen shows the role as it was just created and has a checkbox that enables *Assign to users now* (the default is checked). Any role can be edited to have its name and/or permissions changed. Changes to *Restriction type* are not allowed after the role has been created.

Existing Roles can be edited to have their permissions changed. Roles can also be removed and the deletion of a role is immediate to all connected clients. To access existing Roles, go to *Application Management* > *User Security* > *Roles* from the navigation tree.

User/Role Assignment

Custom Roles as well as the *HP Web Jetadmin Administrator Role* can have one or more user assignments. User/Role assignment is done with Windows users or user-groups. These users or user-groups can be based in either the local system or on the Windows domain.

HP Web Jetadmin 10.1 servers joined to a Windows domain will exist in the list of domain member computers. Users logging onto the computers will be members of the domain. These users, as well as

user-groups to which they may belong, can be assigned to HP Web Jetadmin Roles. Once these assignments are made, users have access to the features defined within Role permissions settings.

User/Role assignment can be viewed and managed in *Application Management* > *User Security* > *Roles, Users* (Figure 2). A number of controls exist in the *Users* display allowing management of user/role assignment.

- **Assign Role** launches the assign user role tool that initially provides controls to select one or more users or groups.
- **User name** specifies the local or domain user account or group name.
- **Domain** specifies the windows domain or the HP Web Jetadmin 10.1 host name in the case of local users or groups.
- **Browse** is used to find users or groups on either the HP Web Jetadmin 10.1 host or on the windows domain.

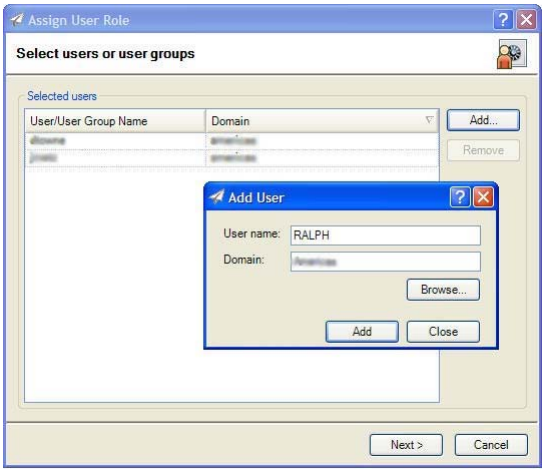

Figure 2 – Assign User to Role

After *Next* is chosen, one role can be selected for assignment. Group selection is possible when the role has a Groups restriction type. *Restriction type: Group* will be discussed in further in the document in a section named "Rolls, Device Group Restriction Type". After confirming settings, the Results screen is displayed showing the new User/Role assignment(s). Once these assignments are complete, users can access HP Web Jetadmin 10.1 by browsing to the server without being prompted for 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 (before using local user accounts, see the section "User/Role Assignment in Workgroups" below)
Local Group	Computer name	Local group name

In most cases the domain user, domain user group, or local user group will be used in User/Role assignment. A common scenario would be to have help-desk employees as members of a domain group managed by the IT team. As new help-desk employees are staffed onto the Helpdesk team, they are automatically granted permissions to the *HelpDesk* Role in HP Web Jetadmin 10.1 by virtue of domain group membership. Remember, this domain group membership is managed at the Windows domain. Another case is where the HP Web Jetadmin 10.1 administrator has many partners who also use the HP Web Jetadmin10.1 installation. These users can be tracked locally on a group within the HP Web Jetadmin 10.1 install host. (For more details about local or domain user accounts and domain or local groups, see Microsoft security documents.)

Existing User/Roll assignments can be edited to change or delete the user/user group or the HP Web Jetadmin Roll. Existing assignments are found in *Application Management* > *User Security* > *Users*.

Note: At this time, HP Web Jetadmin 10.1 does not support groups within groups. For example, assume 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 will not have access to that role.

User/Role Assingment in Workgroups

Microsoft defines a "Workgroup" where either computers, users, or both are not members of a Microsoft domain. In these cases, HP Web Jetadmin 10.1 client access is possible. Remote client access can be established if the following is true:

Administrative access

	Web Jetadmin host	Client host
Local user account	"Joe"	"Joe"
Password	"XYZ"	"XYZ"
Local Administrator Membership	Yes	

Application access via Roles

	Web Jetadmin host	Client host
Local user account	"Joe"	"Joe"
Password	"XYZ"	"XYZ"
HP Web Jetadmin 10.1 Role assignment	Specified Role(s)	

In the case above, the local user account "Joe" exists on both hosts and the password for "Joe" is the same. In the first case, "Joe" is a member of the local administrators group which gives "Joe" rights to all HP Web Jetadmin 10.1 features and settings. In the second case, Joe has been granted access through Roles. In both cases, the user account name "Joe" as well as Joe's password are both managed within the local user accounts on each host.

In some cases, the workgroups systems hosting both HP Web Jetadmin and client will require some special security settings. Local Security Policies may have to be adjusted on both the HP Web Jetadmin and client hosts. (See Microsoft documentation about local security policies.)

Roles, Device Group Restriction Type

A Role can be created that has a *Restriction Type* of *Group*. These roles provide feature access based on both user account and device group details. The *Create Role* wizard has feature permissions limited to device management items when the *Restriction Type* is set to *Group* (Figure 3). Once the Role is named and settings are confirmed, this Role is assigned to both users and device groups.

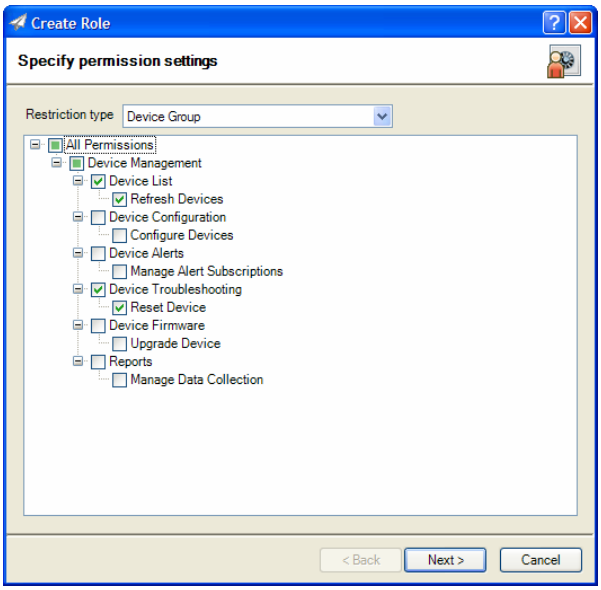

Figure 3 – Restriction Type: Group

During the *Assign User Role* wizard (Figure 4), device groups *and* users, are specified when the Role selected has a *Restriction Type* of *Group*. When a Role is selected that does not have this restriction type, the *Groups* area remains gray and no groups can be selected.

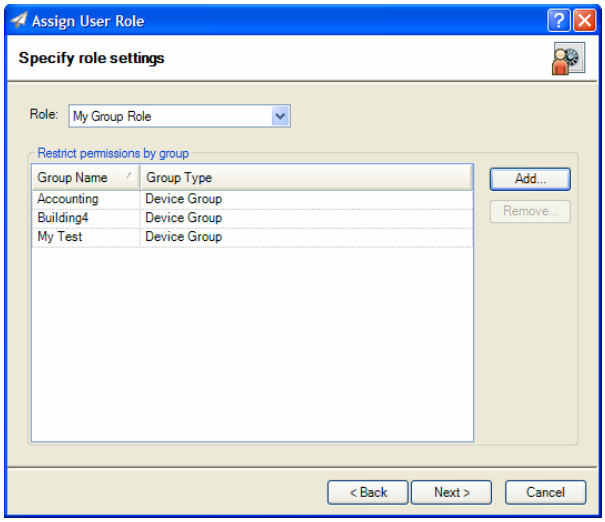

Figure 4 – User/Group Role Assignment

A scenario where Roles with *Restriction Type: Group* are valuable could be in the case of regionalized help-desk operations. Consider this: The north regional help-desk is staffed with five people. All of these people are given permissions to the appropriate application features and are given HP Web Jetadmin 10.1 feature access to the devices within their region. Similarly, the help-desk staff in the south region is staffed with eight people who have HP Web Jetadmin 10.1 feature access on devices within their region. In both cases these users can have Role assignment on the same role but for the appropriate group containing the devices within their region. The features needed to perform help-desk tasks are specified by the Role and the device groups are specified during the Role assignment.

User/Role Diagnostics

Users can be assigned to multiple Roles. A common scenario might be:A small help-desk operation is staffed with 15 people. All of them are assigned to the *HelpDesk* Role which gives them the ability to troubleshoot devices by using the *Status*, *Detailed Info*, *Troubleshooting*, and *Capabilities* features. In order to keep device information up-to-date, two of the senior help-desk staff are given access to the *Configuration*, *Firmware*, and *Discovery* features. In addition to the *HelpDesk* Role, they have been given an assignment into another Role named *ExtendedHelp*. These two users now have a super-set of features that enable functionality beyond those needed by normal help-desk staff. The HP Web Jetadmin 10.1 administrator has the ability to manage Roles for both help desk and senior help desk staff. HP Web Jetadmin 10.1 uses least restrictive permissions in its User/Roles feature; HP Web Jetadmin 10.1 will grant access to any feature that is enabled in a Role for which a user has an assignment.

Diagnostics can be used to observe the privileges that are granted to any user that has a User/Roll assignment (Figure 5). Diagnostics is invoked in *Application Management* > *User Security* > *Diagnostics* from within the navigation tree. To invoke the Diagnostics feature simply add the *User name* and *Domain* detail and then choose the *View Roles* button.

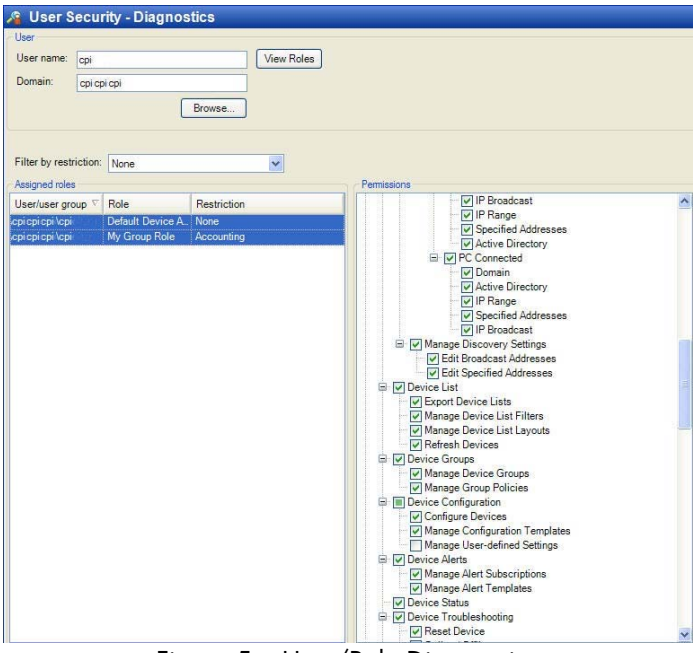

Figure 5 – User/Role Diagnostics

Managing 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 a few rules should be kept in mind:

- As users have Role permission changes applied to them, the display interface will not change to reflect (hide) feature access changes until the next time the user logs into the application.
- As users have Role permission changes applied to them, access to restricted features will be blocked and the users will experience an "access denied" message from the application in areas where feature restrictions have been implemented.
- Scheduled tasks implemented by users with Role permissions changes or authorization removal will remain intact and will not be blocked by User/Role or permissions changes.

HTTPS & SSL (Secure Sockets Layer)

HP Web Jetadmin 10.1 administrators can enable the SSL (secure sockets layer) on HP Web Jetadmin after software installation. This forces browser communication to the more secure HTTPS protocol. SSL is enabled by the administrator from the console or host running the application. A notice will occur when users try to enable this feature from a remote client (Figure 6).

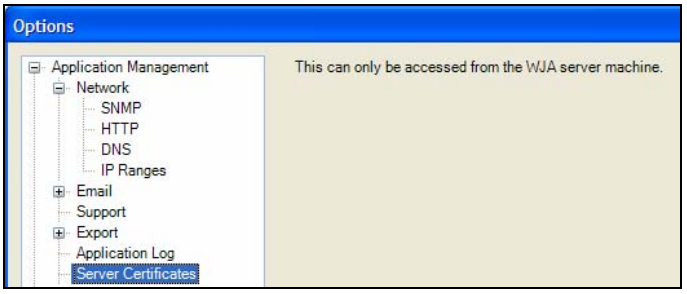

Figure 6 – Certificates Notice

SSL was enabled by default on HP Web Jetadmin versions prior to HP Web Jetadmin 10.1 where the primary client interface went through a Web browser. SSL is not enabled by default on HP Web Jetadmin 10.1 for several reasons:

- HP Web Jetadmin 10.1 does not use a browser as a primary application interface.
- HP Web Jetadmin 10's HTTP service provides only minimal or limited functionality and is not core to client/server communication.
- .NET Remoting provides data encryption and user authentication.
- Self-signed certificates cannot be used unless all clients have the appropriate CA installed.

In some environments, SSL is required anytime an HTTP interface or service is being used for communication and can be enabled and enforced by the administrator. When SSL is enforced, it provides an industry acceptable protocol for both authentication and encryption of HTTP communication. A host requesting access to the HP Web Jetadmin ClickOnce client download is assured that the system hosting HP Web Jetadmin is authentic and the communication between the two systems is encrypted.

Certificates are used by the SSL protocol to accommodate both authentication and encryption. HP Web Jetadmin is capable of generating a signing request that can be used by a CA (certificate authority) for the purpose of generating a certificate. The user can generate a *Signing Request* through *Tools* > *Options* > *Application Management* > *Certificates* (Figure 7).

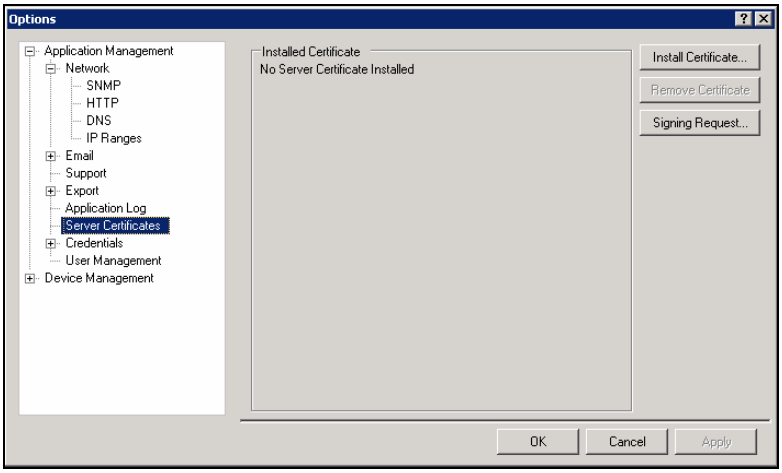

Figure 7 – Server Certificates

Once the request has been fulfilled by the CA, the certificate is ready to be installed on the HP Web Jetadmin application. Remember, it is not possible to use *Tools* > *Options* > *Application Management* > *Certificates* without being at the application console. *Install Certificate* is used to

browse, upload the certificate file (Figure 7). Once the certificate is installed, the HTTP service enforces SSL. Any browser contact with HP Web Jetadmin 10.1 should indicate HTTPS on the URL line when SSL is enforced. Using the *Remove* control uninstalls the certificate and SSL will no longer be enforced.

Important Points to Remember when Implementing SSL

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

1) When SSL has been implemented on HP Web Jetadmin 10.1 with an internal CA (certificate authority), the CA's authorizing certificate is required to be installed in the client browser. If this certificate is not installed in the client browser the HP Web Jetadmin ClickOnce page will fail to load.
2) Proxy servers tend to use the standard SSL port which is 443. If HP Web Jetadmin's ClickOnce 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 HP Web Jetadmin's SSL. The workaround for this problem is to place the HP Web Jetadmin FQDN into the browsers exceptions list under *Tools* > *Internet Options* > *Connections* > *LAN Settings* > *Advanced*. This will cause the browser to pull http and https content from the HP Web Jetadmin server directly.

   Note: HP Web Jetadmin http and https port numbers can be customized to something other than 8000 and 8443. A procedure for implementing custom ports is outlined in the onlne help for HP Web Jetadmin 10.1.

3) When a user has implemented SSL on HP Web Jetadmin 10, a redirect will occur when the browser URL uses port 8000. Here is an example:

   Known URL prior to SSL implementation: http://servername.domain.domain.xxx:8000

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

   The URLs shown here use FQDN (fully qualified domain name). 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.
4) The server host FQDN used in the certificate must be DNS resolvable. If it is not, the client application launch might fail.

HP Web Jetadmin Certificates and Backup/Restore Procedure

HP Web Jetadmin 10.1 software contains backup/restore scripts and instructions for qualifying and using them. These scripts are designed to help the administrator save time in the case when a catastrophic hardware, OS or application failure occurs. Backup and restore act on the HP Web Jetadmin database as well as the HP Web Jetadmin settings files. Most of the software settings as well as device data can be restored to an HP Web Jetadmin installation.

The certificate used to enforce HTTPS/SSL communications is not retained or restored during the backup/restore processes. The certificate is installed in the local Windows certificate store. Two outcomes are possible when utilizing HP Web Jetadmin 10.1 restore scripts on a server that had HTTPS/SSL enabled:

1) If HP Web Jetadmin is being restored to a host where the certificate is installed already, and if application settings had SSL enabled, HP Web Jetadmin will start enforcing SSL using that certificate.
2) If HP Web Jetadmin is being restored onto a host where the certificate is not installed, and if SSL was enabled through application settings, HP Web Jetadmin will run without SSL enforced. A certificate will have to be installed onto the server using Tools, Options, Application Management, Certificates as described above. Always test to be sure SSL is enabled and being enforced when performing an HP Web Jetadmin restore.

Application Security – Other Application Security Items

Digital Signatures

HP Web Jetadmin 10.1 uses digital signatures for all of its packages and plug-in descriptor files to ensure the integrity and authenticity of these files. All files downloaded from hp.com for the purpose of Product Updating are digitally signed. HP Web Jetadmin 10.1 verifies the digital signatures by using our Verisign-managed root certification authority. During 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 10.1 will refuse to load it. This industry standard infrastructure also uses Certificate Revocation Lists to track any certificates that may 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

A list of network ports used by HP Web Jetadmin (0 denotes random port number).

Application Server Ports

Port #	Type	I/O	Details
0	UDP	I/O	TFTP send/receive request handling
0	UDP	O	SNMP
0	TCP	O	WMI Communication
0	TCP	O	Firmware upgrade
69	UDP	I	TFTP incoming port
427	UDP	I	SLP Listen
3702	UDP	I	WS Discovery Listen*
4088	TCP	I/O	Client Remoting
8000	UDP	I	Web Jetadmin Discovery Listen*
8000	TCP	I	WebServer (http)
8443	TCP	I	WebServer (https)
27892	UDP	I	Traps Listener

*for the discovery of other HP Web Jetadmin servers

Client/Device Ports

Port number	Type	I/O	Details
161	UDP	I	SNMP
445	TCP	I	WMI communication
9100	TCP	I	Firmware upgrade

HPWJA Service

HPWJA Service is core to the HP Web Jetadmin 10.1 application and runs under the low privilege Microsoft user account "NT Authority\Network Service". Many environments require that applications like HP Web Jetadmin not have administrative access to the operating system.

SQL Server (HPWJA) -- Database Access and Authentication

The SQL Server 2005 Express database instance that was created at install time is accessed by the application, HP Web Jetadmin 10.1, using Windows credentials. The service for this instance runs under user NT Authority\Network Service and is named SQL Server (HPWJA).

HP WJA Update Service

HP WJA Update Service exists as a process-agent outside of the HP Web Jetamin core service, HP WJA Service for the purpose of controlling updates. This service, when activated by HP Web Jetadmin *Product Updates*, requires the administrator to provide user credentials that have Microsoft administrative privileges on the HP Web Jetadmin 10.1 install host.

Active Client Task Module

The **Active Clients** task module can be activated and viewed within the *Task Module Docking* area or from the *Application Management* > *Overview* area. This task module shows clients that are logged into HP Web Jetadmin 10.1 as well as the number of active client applications that are being run by each client. This feature helps the Administrator determine which clients are logged into the system prior to running *Product Updates* or performing tasks that may burden the system and cause slow performance. A short custom message can be sent to clients by using *Tools* > *Broadcast Message* which is available while in *Application Management* (Figure 8).

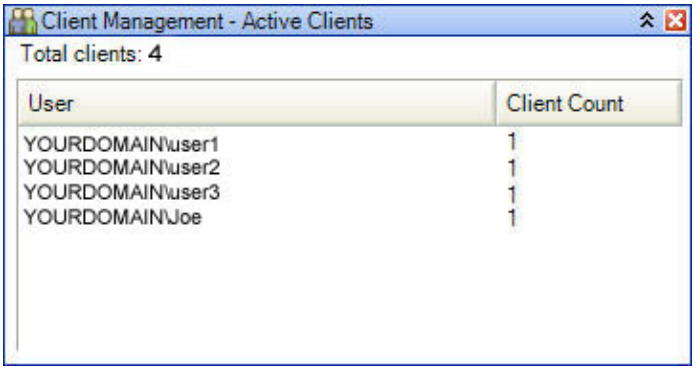

Figure 8 – Active Clients Task Module

Part 2 – Device Security

In many environments, password policies exist that require the device administrator to periodically reconfigure security credentials. HP Web Jetadmin 10.1 is a powerful device management tool because it can configure many devices at once. This saves device administrators from having to contact every device separately for the purpose of assigning configuration items like passwords and other credentials.

Device passwords, community names, ports, and other credentials are used to prevent unauthorized access. Even though the HP Web Jetadmin 10.1 installation has been made secure, other installations and even other utilities can access devices. Access to devices is available through a variety of utilities and configuration paths including:

- HP Web Jetadmin
- Telnet
- Embedded Web Server
- Other SNMP Utilities

Protocols used by these and other utilities include:

- SNMP over UDP – changes of PML objects
- SNMP over UDP – changes of PML objects

- RFU file through Port 9100 over TCP – printer firmware upgrades
- PJL file through Port 9100 over TCP – changes of PML objects
- PCL file through Port 9100 over TCP – changes of PML objects
- NFS over TCP – changes to storage (such as hard disk)

In addition to providing additional security methods to prevent against unwanted device configuration, HP Web Jetadmin 10.1 also provides security against unwanted printing access. For example, printing can occur to printers using the following techniques, among others:

- HP Standard Port Monitor
- HP Jetdirect Port
- Microsoft Standard Port Monitor
- LPD
- FTP
- IPP

Device Security – 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 10.1 is possible in both batch and single configuration. In addition to configuring passwords and credentials from within HP Web Jetadmin 10.1, the administrator can protect these items through the *Credential Store*.

Security settings are consolidated beneath the *Security* configuration category making them easy to find and manage. Security settings can also be stored in *Configuration Templates* so that they can be applied through *Schedules* and/or group configuration policies. Security settings can also be customized under *My Settings* so that all things considered critical to security can be easily found and configured by the individual user.

The Credentials Store

The concept of a *credential store* is not new to HP Web Jetadmin. Older versions of HP Web Jetadmin stored device credentials required to make configuration changes on devices. This feature keeps HP Web Jetadmin 10.1 users from having to provide device credentials every time one or more devices require credentials; it also facilitates batch and background device operations.

The *Credentials Store* uses a portion of the HP Web Jetadmin 10.1 SQL database that securely encrypts and stores device credentials when ever a correct credential value is authenticated. 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 10.1:

- **EWS Password** – blocks unauthorized access to the device embedded http interface and 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 user name, passphrase1 and passphrase2 which are used when SNMPv3 is enabled. This version of the Simple Network Management Protocol secures and authenticates communication between management applications like HP Web Jetadmin 10.1 and the device. This protocol is used when strong security is a requirement.
- **SNMP Set Community Name** –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 "sniffed" be eavesdroppers.

- **SNMP Get Community Name** –sometimes used to prevent device discovery from other HP Web Jetadmin 10.1 installations. Devices will not respond to Get packets that don't contain the correct value. The Get name value traverses the network in clear text and can be "sniffed" by eavesdroppers.

Two actions will 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 becomes stored when used during a configuration and when the credential was not previously stored by the software.

Stored credentials are reused by the application any time the requirement for them is encountered. A user configuring a device that has had a credential stored is not required to re-enter the credential into the application. The application uses the credential as a background operation in the HP Web Jetadmin 10.1 server's steps to configure the device.

Note: HP Web Jetadmin 10.1 supports backup and restore procedures. Instructions and sample script files can be found in the HP Web Jetadmin 10.1 *install* directory which is typically at: `Drive:\Program Files\Hewlett-Packard\Web Jetadmin 10\WJABackupRestore`.

After a backup and restore, the contents of the *Credential Store* are 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 credentials will be lost.

Configuration of a Device Credential

Figure 9 shows the configuration item used to set the Embedded Web Server password.

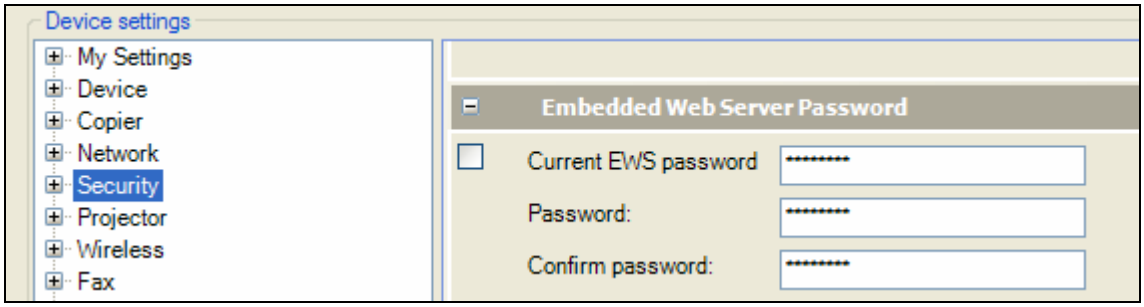

Figure 9 – EWS Password Configuration Item

Prior to HP Web Jetadmin 10.1 actually setting the device credential, the software authenticates the user's knowledge of the credential. This is true in both batch and single device modes of password or credential configuration. Once 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 10.1 can apply them transparently any time the need arises. HP Web Jetadmin 10.1 uses these passwords or credentials during live configuration or during automated background tasks such as scheduled firmware upgrades or configuration. When configuring devices, users do not have to know the credential to perform the configuration. The user just needs access to HP Web Jetadmin 10.1 and device configuration features. This is called "credentials delegation".

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 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* provides controls:

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

Global credentials are values that are set by the user and then used by HP Web Jetadmin 10.1 when a credential is needed but is not available in the Credentials Store. Multiple values can be set in *Global Credentials*. HP Web Jetadmin 10.1 will try each credential value in the stack until it encounters success. If the *Global Credential* value is used by the application and results in success, that value is stored for that device within the *Credentials Store*. When success is not achieved, the device is placed in a "credentials needed" state.

In *Tools* > *Options* > *Credentials* there are options to clear all credentials stored within the application and to clear *Global Credentials*.

- *Credentials Options* > *Clear all Credentials*: removes all device credentials from the Credentials Store in the HP Web Jetadmin 10.1 database.
- *Credentials Options* > *Clear all Global Credentials*: clears all global values stored in each of the credential types.

Credentials Needed

If HP Web Jetadmin 10.1 is performing an action such as device configuration, and it encounters a device with a credential such as SNMP Set Community Name, it follows a specific sequence. Here is a simplified example of how HP Web Jetadmin 10.1 attempts to resolve a credential:

- **Check store for credential**
  - If exists, attempt config using credential value.
  - Else, go to Global.
  - If success, stop.
  - If fail, go to Global.

- **Check Global for credential**
  - If exists, attempt config using credential value.
  - Else, log credential-needed, prompt user if live session.
  - If success, stop, add credential to device store.
  - Else, log credential-needed, prompt user if live session.

During a live user-attended, configuration session, HP Web Jetadmin 10.1 prompts for credentials (Figure 10).

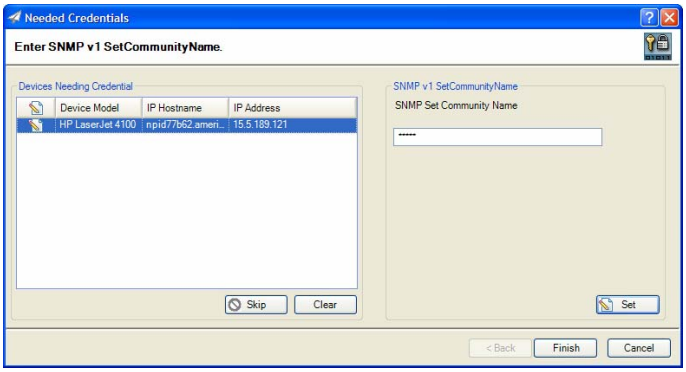

Figure 10– Needed Credentials

If the user did not supply the credential or the session was not live, the device will be flagged as *Credentials Required* (Figure 11). This state can be observed in the *Credentials Required* column that can be enabled in any list's column layout. Users can right-click the device and add the needed credential to the system in order to resolve this state.

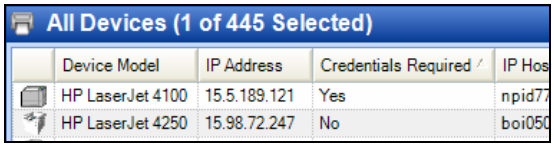

Figure 11 – Credentials Required

Jetdirect Device Password Discontinuance

HP Web Jetadmin 10.1 is designed to enable device security by providing management over appropriate, device based security settings. The HP Jetdirect password that was used by HP Web Jetadmin 10.1 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 Jeatdmin developers have opted out of using the Jetdirect device password as a protective mechanism for device authentication. There are two recommendations for providing device security in place of the Jetdirect device password:

- **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 won't accept or acknowledge the packet. Set community names traverse the network in clear text and can therefore be "sniffed" or viewed by eavesdroppers. In most environments, security provided by Set community names may provide adequate security.

- **SNMPv3**: recommended in security sensitive environments. First, SNMPv3 configures a user account and two pass-phrases onto the device which requires the user (or application) to authenticate. This blocks unauthorized management of devices. The account/pass-phrase details do not traverse the network in clear text; this makes it difficult for eavesdroppers to learn "secrets". Second, communication between the management application and the device is encrypted using the SNMP credentials so information about the device is protected.

Device Disk Security

Managing device credentials and passwords primarily prevents unauthorized management and configuration. The following areas describe other ways of protecting 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 in which a device deletes its files on an ongoing basis and is set within the File System category under Configuration (Figure 12). The mode in which a device can erase its files can be set to non-secure fast erase, secure fast erase or secure sanitize.
- **Secure Storage Erase** removes all non-essential data from storage devices in a manor consistent with preparation for decommissioning or redeployment. This operation can be initiated on demand or scheduled for a later date and time. Secure Storage Erase is a device feature which can be invoked from the Storage tab on any device list for one or many devices. This device feature, once invoked, clears all user files from the disk in one of three erase modes. (See below.)

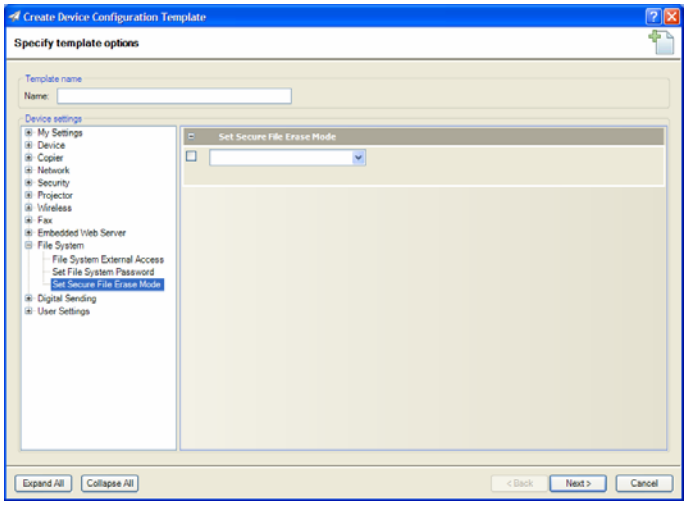

Figure 12 – Secure File Erase option in Configuration

HP Secure Erase technology provides a choice of three different modes of erase security, each of which can be configured by an administrator and may be protected from unauthorized changes with a password. The three erase security modes are:

- **Secure Sanitizing Erase** 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 the retrieval of data. For an explanation of the erase algorithm implemented, see Section 4, Specifications.
- **Secure Fast Erase** mode: This mode completes the erasure faster than Secure Sanitize mode. Secure Fast Erase mode overwrites the existing data once, and prevents software-based undelete" operations on the data.
- **Non-secure Fast Erase** mode: 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.

Device Security – Other Access Controls

Managing device credentials and passwords primarily prevents unauthorized management and configuration. The following areas describe other ways of protecting devices. NOTE: Not all device security features are covered in this document.

HP Jetdirect IPsec Plug-in for HP Web Jetadmin 10.1

HP Web Jetadmin 10.1 offers plug-in packages through *Application Update* that add functionality to the base application. One of these is the IPsec plug-in which is used to manage security policies on HP Jetdirect print servers. This can be obtained directly through the *Application Update* feature in HP Web Jetadmin 10.1 *Application Management* view when the application is capable of

communication with hp.com. When no communication with hp.com is possible, users can download the application update package file from the Software and Driver downloads pages on hp.com.

Once the plug-in is installed, extra device configuration items appear within the *Network* configuration category (Figure 13). These configuration items can apply and manage IPsec policies to the Jetdirect device. 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 details, see the help documentation for IPsec configuration after the plug-in is installed.

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

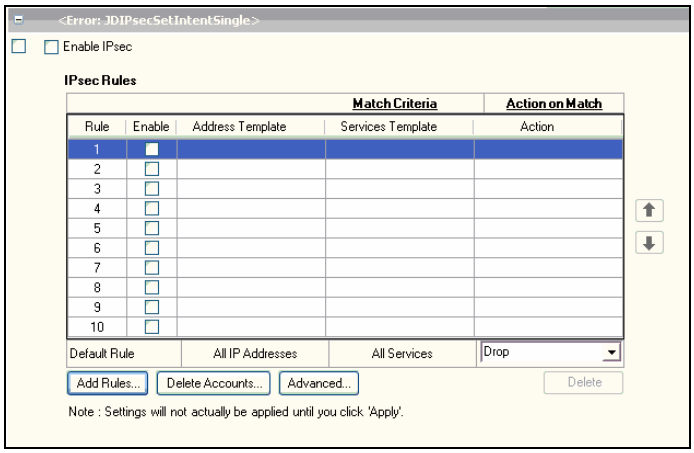

Figure 13 – IPSEC Configuration in HP Web Jetadmin

Disable Unused Protocols & Services

Many paths exist providing both configuration and print access to devices. Unused items can be disabled on single or multiple devices by using the Enable Features configuration item.

Control panel lock

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

Other Device Security Features

Some or all of these features may not be available on all models of HP printers. All of these items are configurable from within HP Web Jetadmin 10.1. Consult 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 by-application basis.
- **MFP Access** – a large number of feature and authentication settings exist to ensure authorization to features such as scan to mail, scan to fax, etc.
- **Jetdirect Access Control list** – provides a way to lock out IP Address connections.
- **Encryption** – some network communication with devices can be encrypted by using one or both of SNMPv3 or device based SSL (secure sockets layer).
- **Disable Direct Ports** – provides a way to lock the physical, hardware ports on a device.
- **Disable RFU Firmware Upgrade** – prevents unauthorized firmware images from being implemented on devices.