DISCOVERING AND CONFIGURING FUTURESMART DEVICES VERSION 4.5 AND LATER

with HP Web Jetadmin

CONTENTS

OVERVIEW

The FutureSmart 4.5 firmware introduces new default security (secure by default) values to increase the out-of-box security. These new default values are applied to new, and factory reset devices after upgrading to FutureSmart 4.5. HP Web Jetadmin 10.4 SR2 with Feature Pack 6 or higher manages these new security settings.

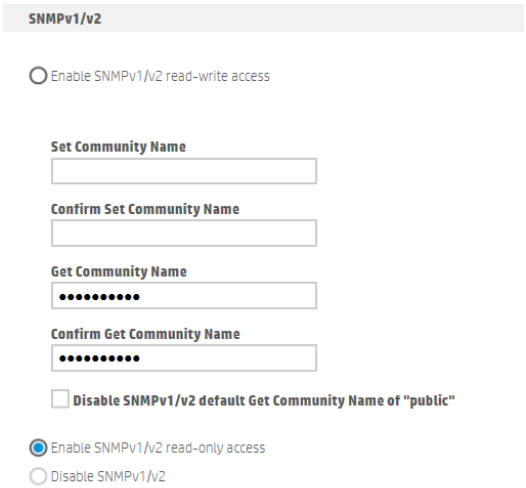
NOTE Devices upgraded to FutureSmart 4.5 will maintain the settings from before the upgrade. Only after a cold-reset, the upgraded devices will have the increased security settings active.

FUTURESMART 4.5 NEW DEFAULT SECURITY VALUES

The higher in the list, the more it impacts HP Web Jetadmin operations.

1. SNMP v1/v2 defaults to Read-Only

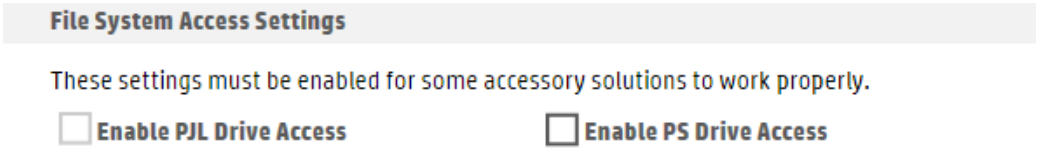
   EWS Setting Configuration Path:
   Networking Tab > Management Protocols menu > SNMP page



   SNMP settings in the Embedded Web Server (EWS)

2. PJL/PS File System Access Disabled by default

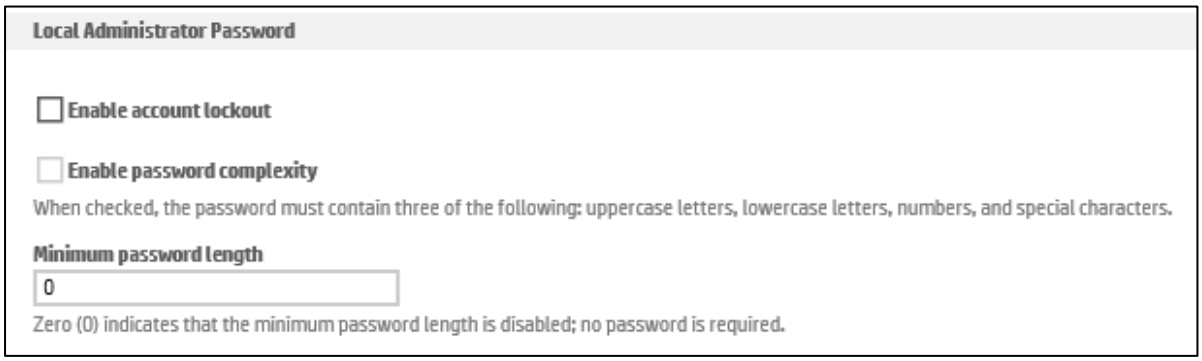
   EWS Setting Configuration Path:
   Security Tab > General Security Menu



   File System Access Settings in the EWS

3. Local Password Complexity (the password must contain three of the following: uppercase letters, lowercase letters, numbers, and special characters), Minimum Password Length (8 characters) and Local Account Lockout (after 5 wrong attempts within 10 seconds).

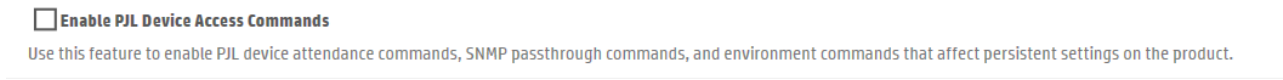
EWS Setting Configuration Path:
Security Tab > Account Policy



Account Policy settings in the EWS

4. Disabling PJL Device Access Commands setting

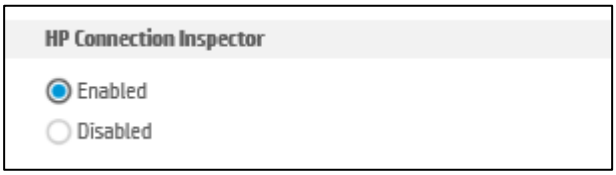
   EWS Setting Configuration Path:
   Security Tab > General Security Menu



PJL Device Access Commands in the EWS

5. HP Connection Inspector enabled by default

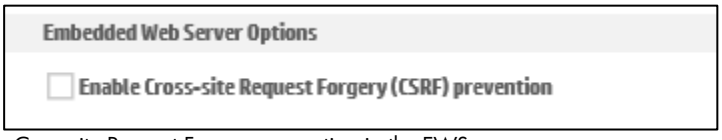
   EWS Setting Configuration Path:
   Security Tab > TCP/IP Menu > Network Identification Page



HP Connection Inspector in the EWS

6. Cross-site Request Forgery (CSRF) prevention enabled by default

   EWS Setting Configuration Path:
   Security Tab > General Security



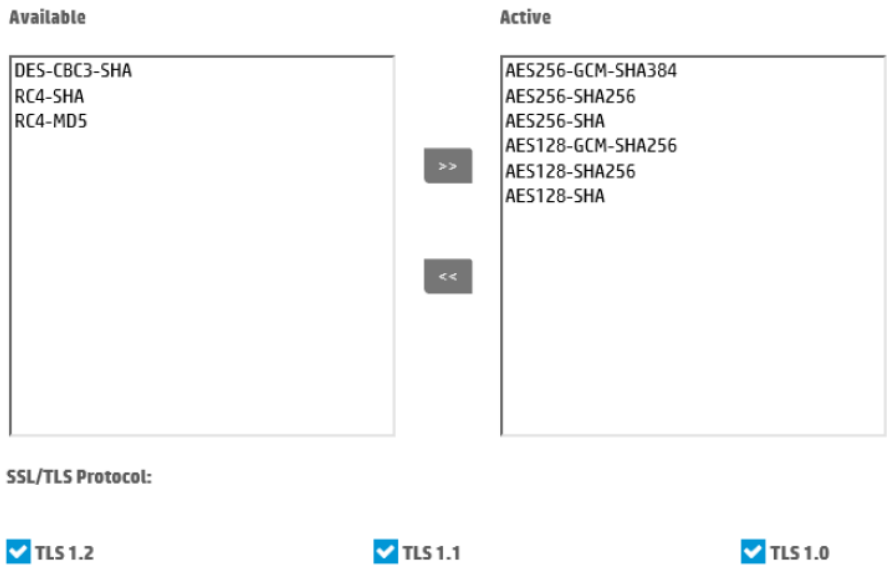
Cross-site Request Forgery prevention in the EWS

7. Default TLS Cipher Suites

   The following ciphers disabled by default:

- RC4-SHA
- RC4-MD5
- 3DES

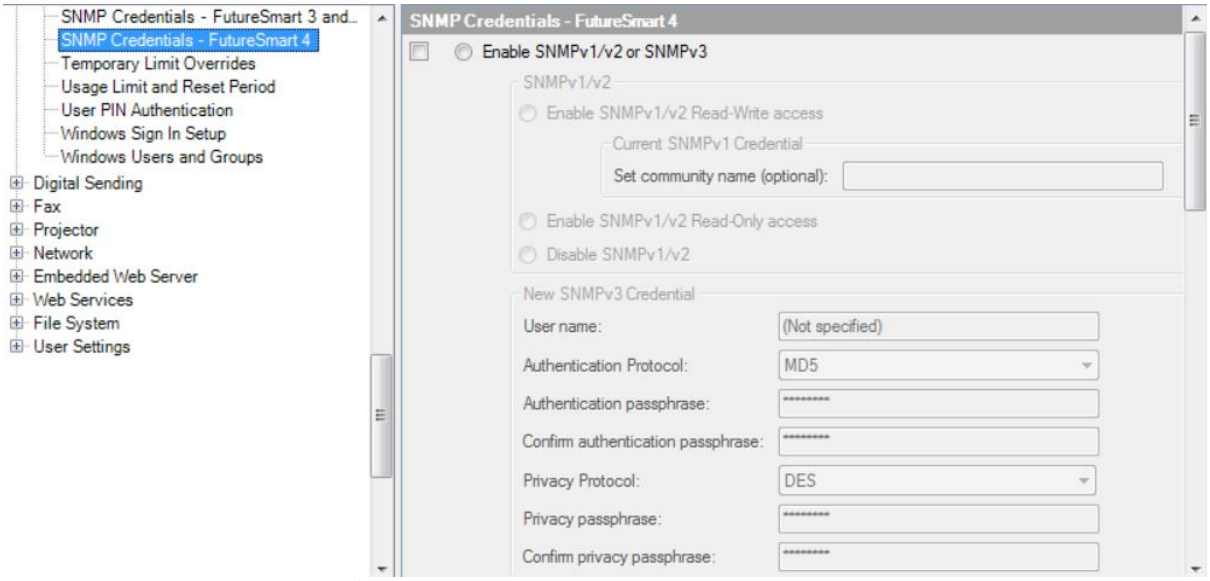
EWS Setting Configuration Path:
Security Tab > Secure Communication Menu



Default Cipher with FutureSmart 4.5 settings in the EWS

SNMPV1/V2 DEFAULTS TO READ-ONLY

With SNMPv1/v2 set to Read-Only, HP Web Jetadmin discovers and recognizes the devices, but SNMP needs to be configured first using a new configuration option in Feature Pack 6 called **SNMP Credentials – FutureSmart 4** under the Security category.

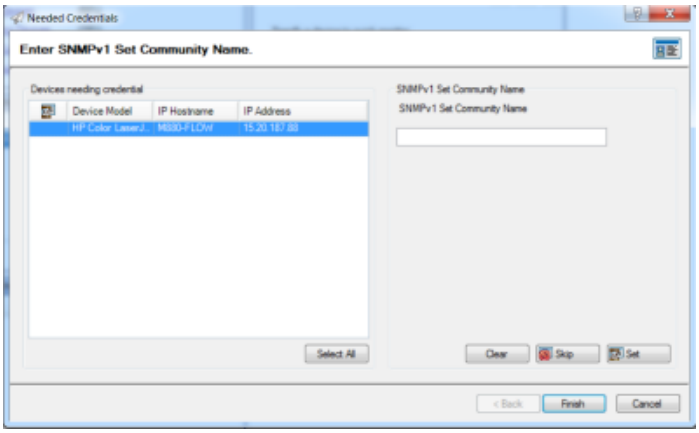


SNMP Credentials –FutureSmart 4 configuration option

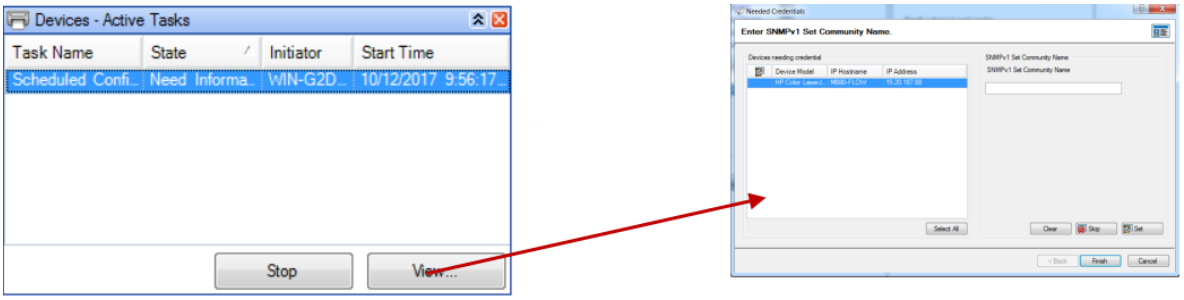
Even if SNMPv1/v2 is set to Read-Only and SNMPv3 is not enabled, with this configuration option, SNMP settings can be configured.

The other configuration option **SNMP Credentials – FutureSmart 3 and Non-FutureSmart devices** (previously known as Access Control for Device Functions) cannot configure the SNMP settings if SNMPv1/v2 is set to Read-Only (and SNMPv3 is not enabled).

Existing templates (including templates upgraded to 10.4 SR3) continue to use the configuration option **SNMP Credentials – FutureSmart 3 and Non-FutureSmart devices**. Configuring SNMP settings with this configuration option when SNMPv2 is set to Read-Only fails and results in a "Needed credentials" pop-up with a request for the SNMPv1/v2 credentials.



Needed Credentials pop-up after attempting to configure one FutureSmart 4.5 device



Needed Credentials screen after attempting to configure several FutureSmart 4.5 devices

Create a new configuration step/template and use the new configuration option **SNMP Credentials – FutureSmart 4** under the Security category.

In order to maintain a high security standard, HP recommends enabling and configuring SNMPv3 instead of providing SNMPv1/v2 read/write access. SNMPv3 passphrases require a minimum of 8 characters and password complexity must contain 3 of the following: upper case letters, lower case letters, numbers, and special characters.

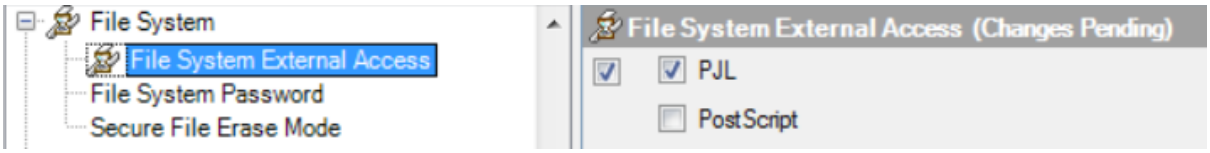
PJL/PS FILE SYSTEM ACCESS DISABLED BY DEFAULT

When PJL File system access is disabled, the following PJL commands are no longer getting executed:

PJL Command	Description
File system commands (FS*)	Controlled by PJL File Access command

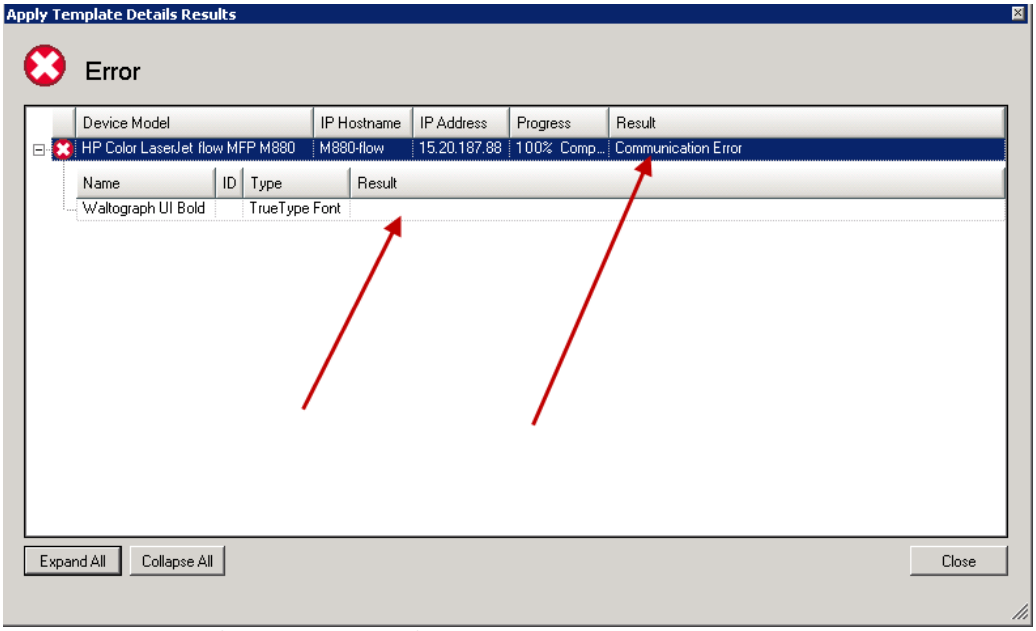
HP Web Jetadmin uses File System Access over PJL to configure Fonts and Macros on the device. Enable PJL Drive Access on the device before HP Web Jetadmin can manage the Fonts and Macros on the device. Enable with the option **PJL** of the File System External Access configuration settings under the File System Category.

NOTE In order to match the wording in the EWS, these names will change slightly in a later HP Web Jetadmin release.



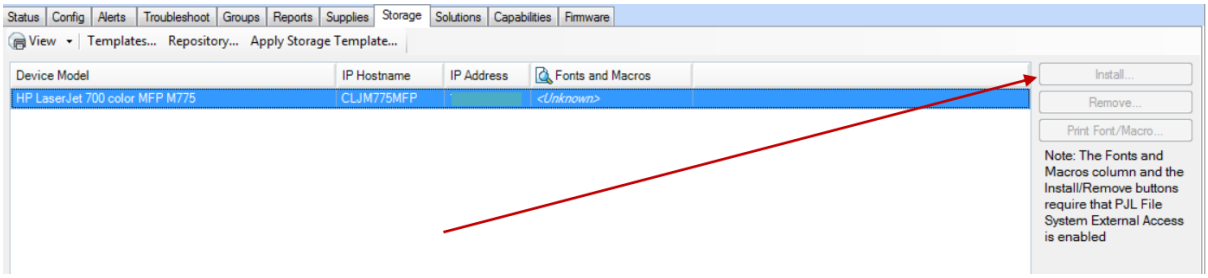
File System External Access configuration option in HP Web Jetadmin

When configuring Fonts or Macros on a device that has PJL File System External Access disabled with a template, HP Web Jetadmin displays a communication error in the Results screen after expanding the Results screen.



Communication error after trying to install a font with PJL device access disabled

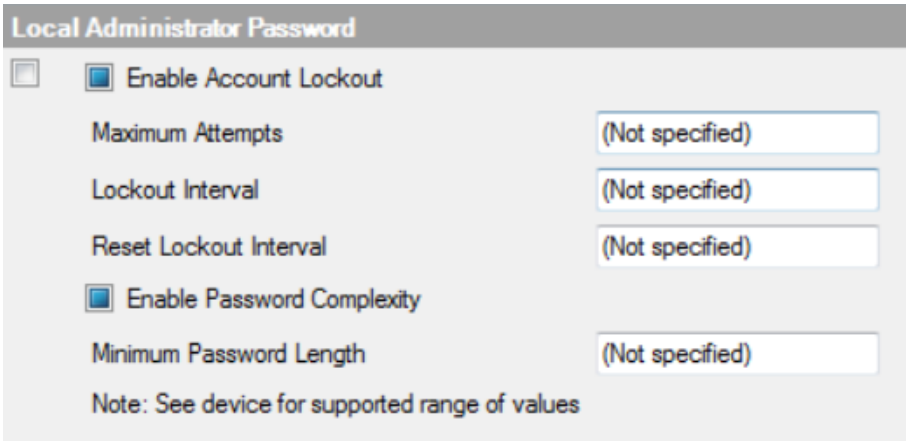
When selecting a single device, the Install button greys out under the Storage tab and a hint regarding the required setting displays.



Fonts and Macros view with Install button greyed out

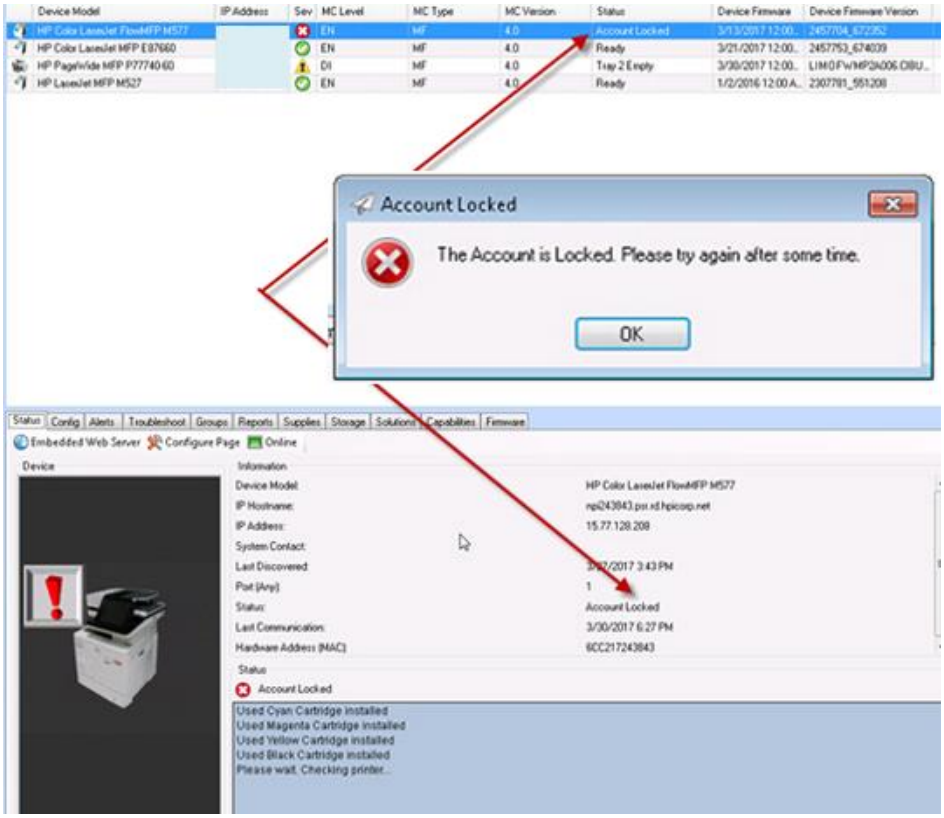
LOCAL PASSWORD COMPLEXITY AND LOCAL ACCOUNT LOCKOUT

HP Web Jetadmin can configure the local password complexity (EWS password) and local account lockout settings on the device with the **Local Administrator Password** configuration option under the Security category.

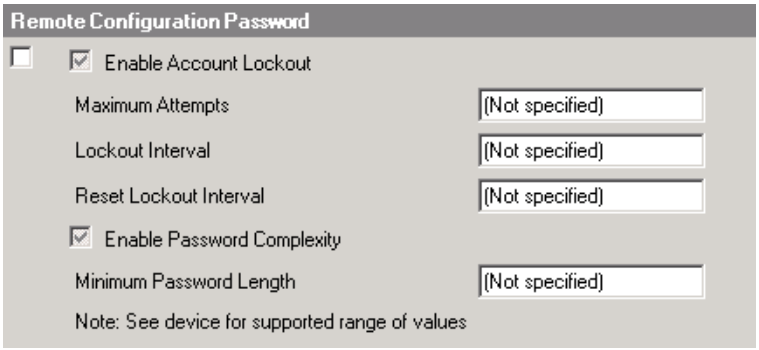


Local Administrator Password configuration option

HP Web Jetadmin 10.4 SR3 and later displays and handles the Account Lockout in the Status and Config tabs.



The Remote Password complexity and remote account lockout can also be configured with HP Web Jetadmin with the **Remote Configuration Password** configuration option under the Security category.



Remote Configuration Password configuration option

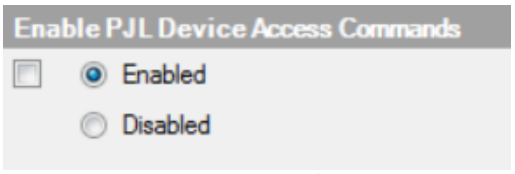
PJL DEVICE ACCESS COMMANDS SETTING

When PJL Device Access commands is disabled, the following PJL commands no longer execute:

PJL Command	Description
DEFAULT	Sets default values for environment variables.
OPMSG, RDYMSG, STMSG	Ready, Status and Operator messages

DMINFO, DMCMD	SNMP over PJL commands
INITIALIZE	Resets PJL values to factory default

HP Web Jetadmin offers the option to send PJL configuration files to the printer with the **PJL configuration** configuration option. This option requires PJL Device Access Commands enabled with the **Enable PJL Device Access Commands** configuration option under the Security category.

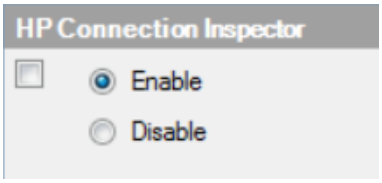


PJL Device Access Commands configuration option

Sending PJL files will be possible regardless of the above setting. HP Web Jetadmin always reports success after the file submits to the printer. In other words, HP Web Jetadmin validates that the file transferred successfully to the printer, but cannot verify if any settings were changed. When PJL Device access commands are disabled, the printer settings don't change (even when HP Web Jetadmin reports success).

HP Connection Inspector

HP Web Jetadmin enables/disables HP Connection Inspector with Feature Pack 6. Later Feature Packs will have more configuration options for HP Connection Inspector.



HP Connection Inspector configuration option

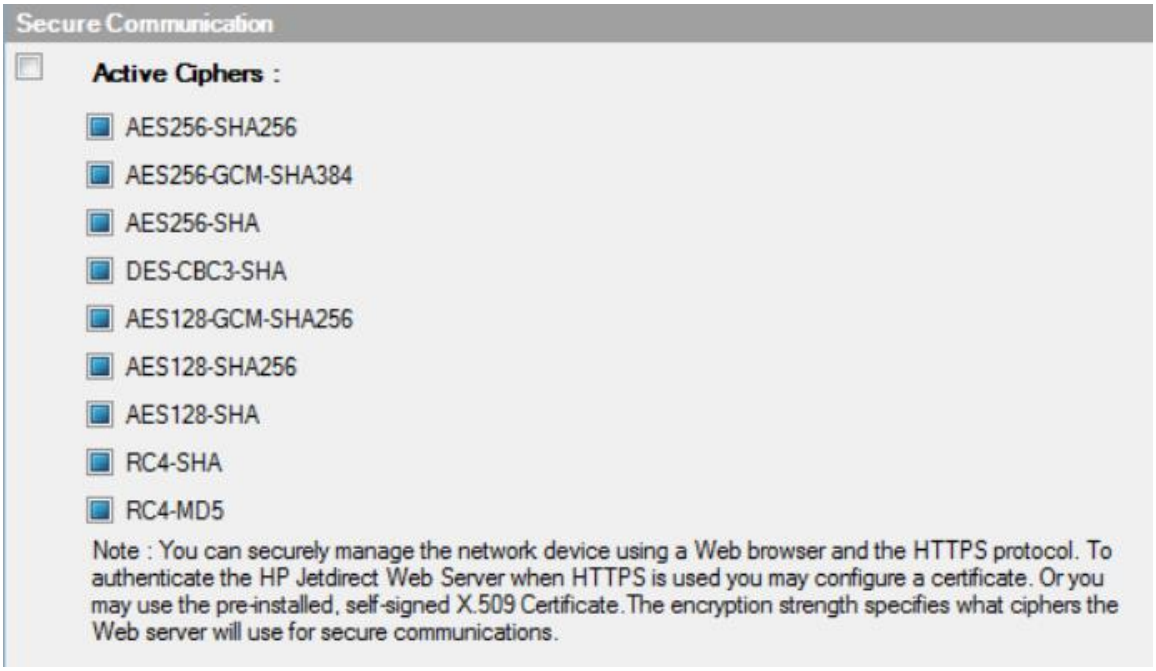
Cross-site Request Forgery (CSRF) prevention

The latest release of HP Web Jetadmin (10.3 with Feature Pack 6) does not have an in-build configuration option for this. This will be added to Feature Pack 7.

HP Web Jetadmin operations are not impacted by this configuration option.

Default TLS Cipher Suites

HP Web Jetadmin is not impacted by the change in active TLS ciphers. If needed, the active ciphers can be reconfigured using the option **Secure Communication** under the Security category.



Secure Communication configuration option

c05813511EN, Rev. 2, November 2017