



# Discovering and Configuring FutureSmart Devices Version 4.5 and Later with HP Web Jetadmin

## Table of contents

|   |    |
|---|----|
| Overview  | 2  |
| New default security values in FutureSmart 4.5      | 2  |
| SNMPV1/V2 defaults to read-only                     | 5  |
| PJL/PS File System access is disabled by default    | 6  |
| Local password complexity and local account lockout | 7  |
| PJL device access commands and settings             | 9  |
| HP Connection Inspector                             | 9  |
| Cross-site Request Forgery (CSRF) prevention        | 10 |
| Default TLS Cipher Suites                           | 10 |

## 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 later manages these new security settings.

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

## New default security values in FutureSmart 4.5

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

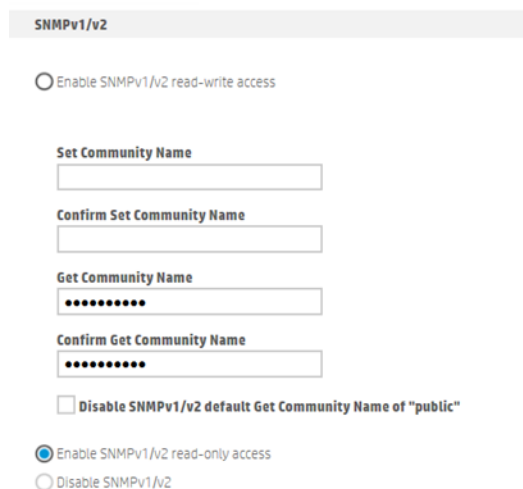


Figure 1: SNMP settings in the Embedded Web Server (EWS)

### 2. PJL/PS File System Access Settings is disabled by default

EWS setting configuration path:

**Security** tab > **General Security** menu



Figure 2: File System Access Settings in the EWS

- 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** menu

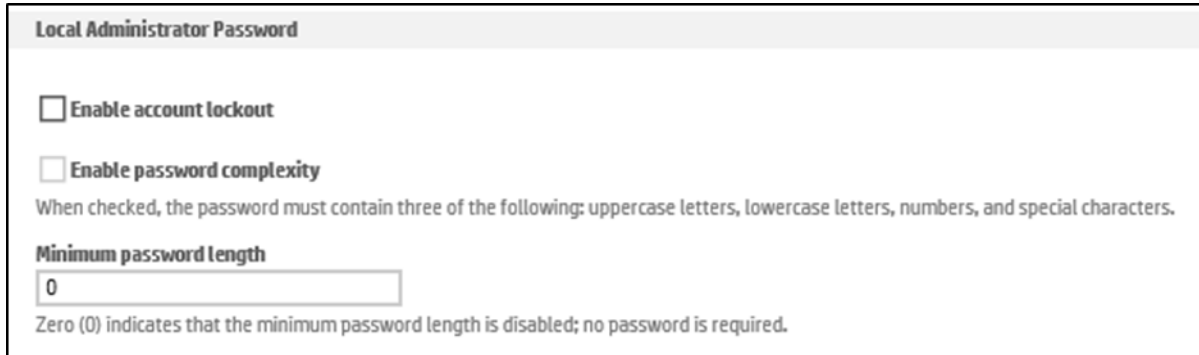


Figure 3: Account Policy settings in the EWS

- Disabling the PJJ Device Access Commands setting

EWS setting configuration path:  
**Security tab > General Security** menu



Figure 4: PJJ Device Access Commands setting in the EWS

- HP Connection Inspector is enabled by default

EWS setting configuration path:  
**Security tab > TCP/IP** menu > **Network Identification** page



Figure 5: HP Connection Inspector setting in the EWS

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

EWS setting configuration path:  
**Security Tab > General Security** menu



Figure 6: Cross-site Request Forgery prevention setting in the EWS

## 7. Default TLS Cipher Suites

The following ciphers are disabled by default:

- RC4-SHA
- RC4-MD5
- 3DES

EWS setting configuration path:

**Security** tab > **Secure Communication** menu

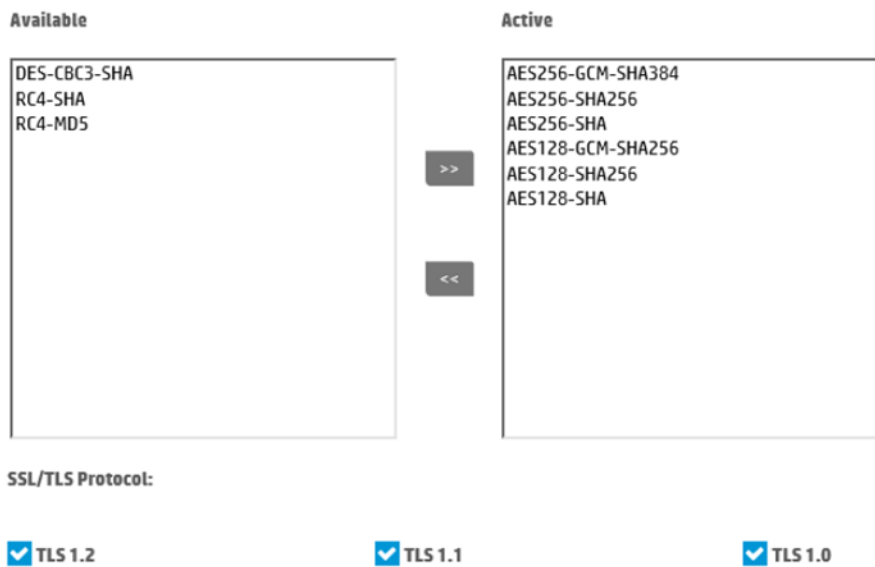


Figure 7: Default Cipher with FutureSmart 4.5 settings in the EWS

## SNMPV1/V2 defaults to read-only

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

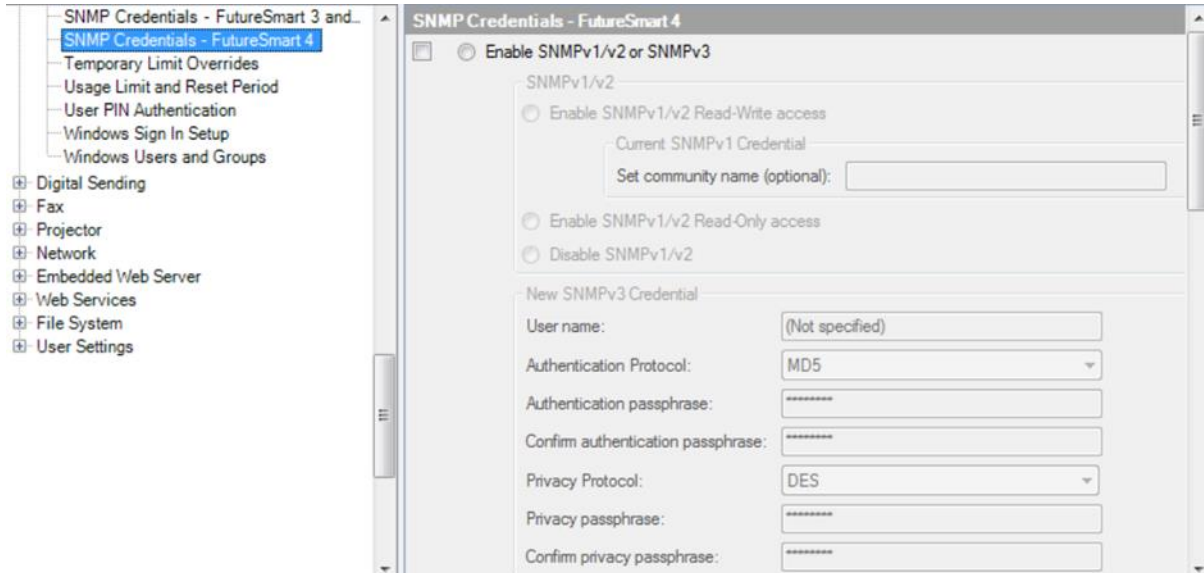


Figure 8: SNMP Credentials - FutureSmart 4 configuration option

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

The **SNMP Credentials - FutureSmart 3 and Non-FutureSmart devices** configuration option (previously called **Access Control for Device Functions**) cannot be used to 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 **SNMP Credentials - FutureSmart 3 and Non-FutureSmart devices** configuration option. Configuring SNMP settings with this configuration option when SNMPv2 is set to Read-Only fails and results in a **Needed Credentials** dialog box with a request for the SNMPv1/v2 credentials.

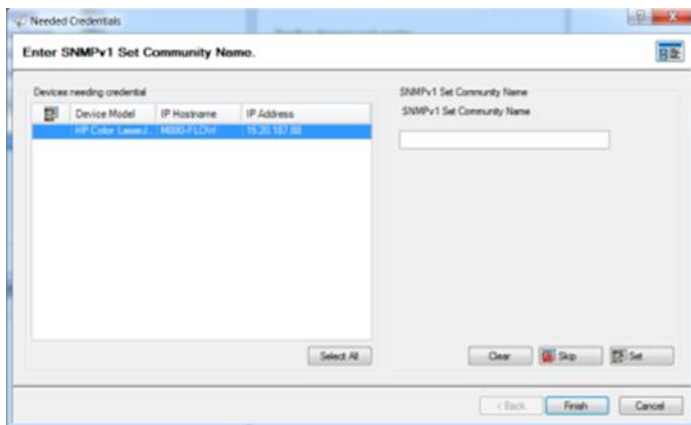


Figure 9: Needed Credentials dialog box after attempting to configure one FutureSmart 4.5 device

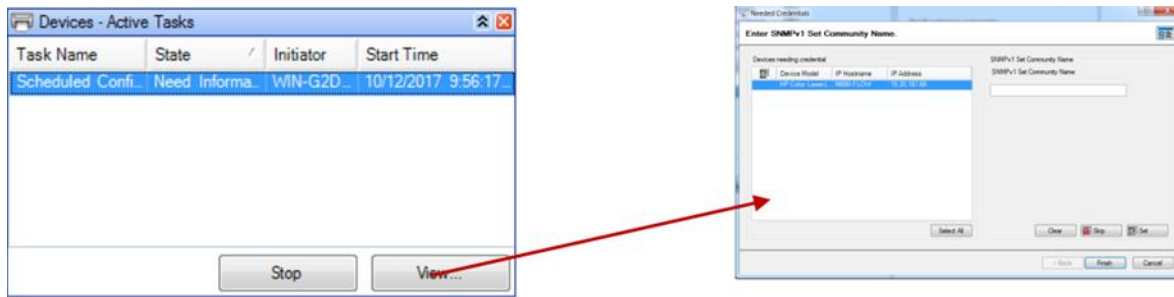


Figure 10: Needed Credentials dialog box after attempting to configure several FutureSmart 4.5 devices

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

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 three of the following: uppercase letters, lowercase letters, numbers, and special characters.

## PJL/PS File System access is disabled by default

When the PJL File System access is disabled, the following PJL command is no longer 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. PJL Drive Access must be enabled on the device before HP Web Jetadmin can manage the Fonts and Macros on the device. To enable this feature, select the **PJL** option of the **File System External Access** configuration option in 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.

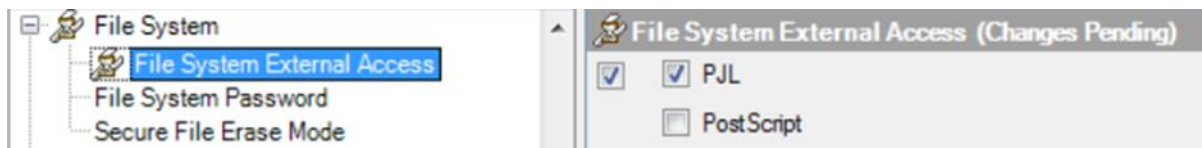


Figure 11: File System External Access configuration option in HP Web Jetadmin

When using a template to configure Fonts or Macros on a device that has PJL File System External Access disabled, HP Web Jetadmin displays a communication error in the **Results** column after expanding the **Results** window.

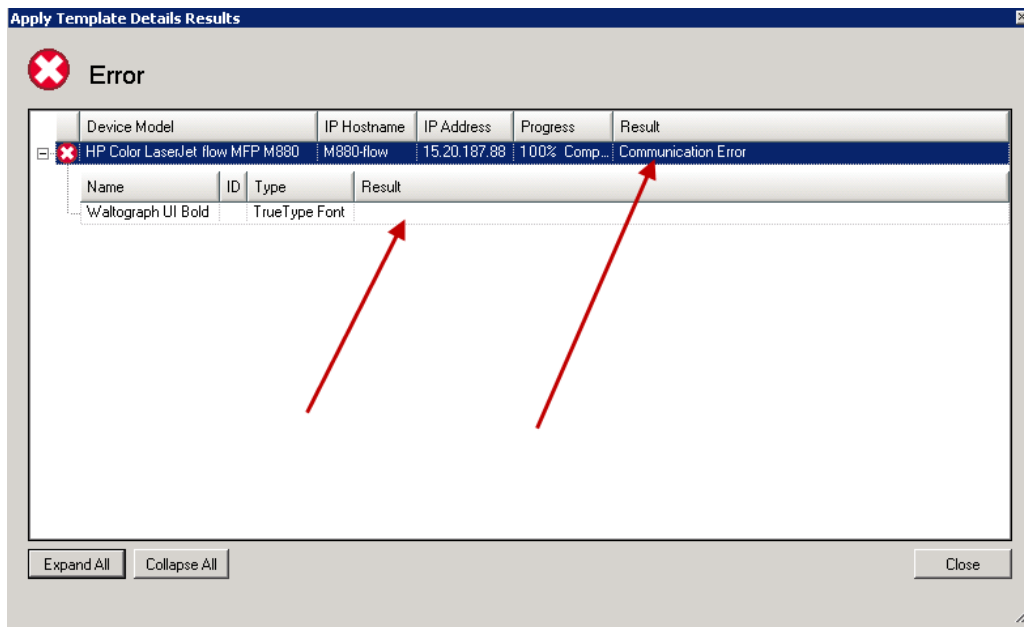


Figure 12: Communication error after trying to install a font with PjL device access disabled

When selecting a single device, the **Install** button is disabled on the **Storage** tab and a hint about the required setting displays.

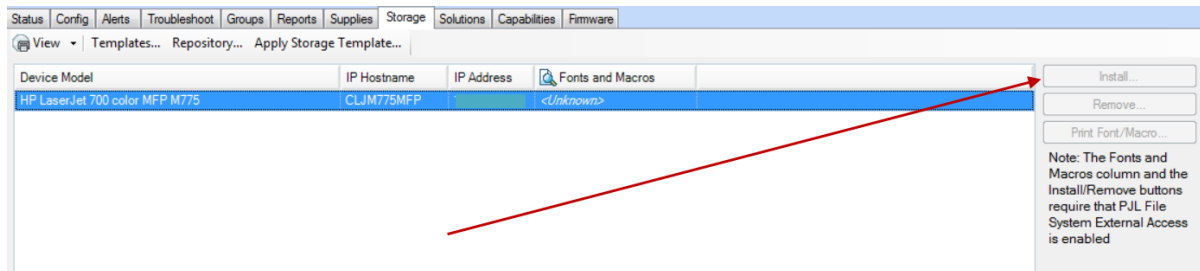


Figure 13: Fonts and Macros view with Install button disabled

## 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 in the **Security** category.

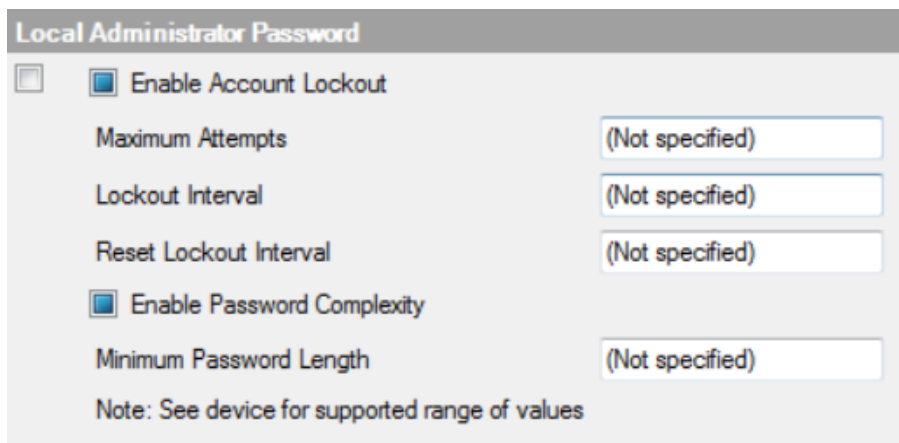


Figure 14: Local Administrator Password configuration option

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

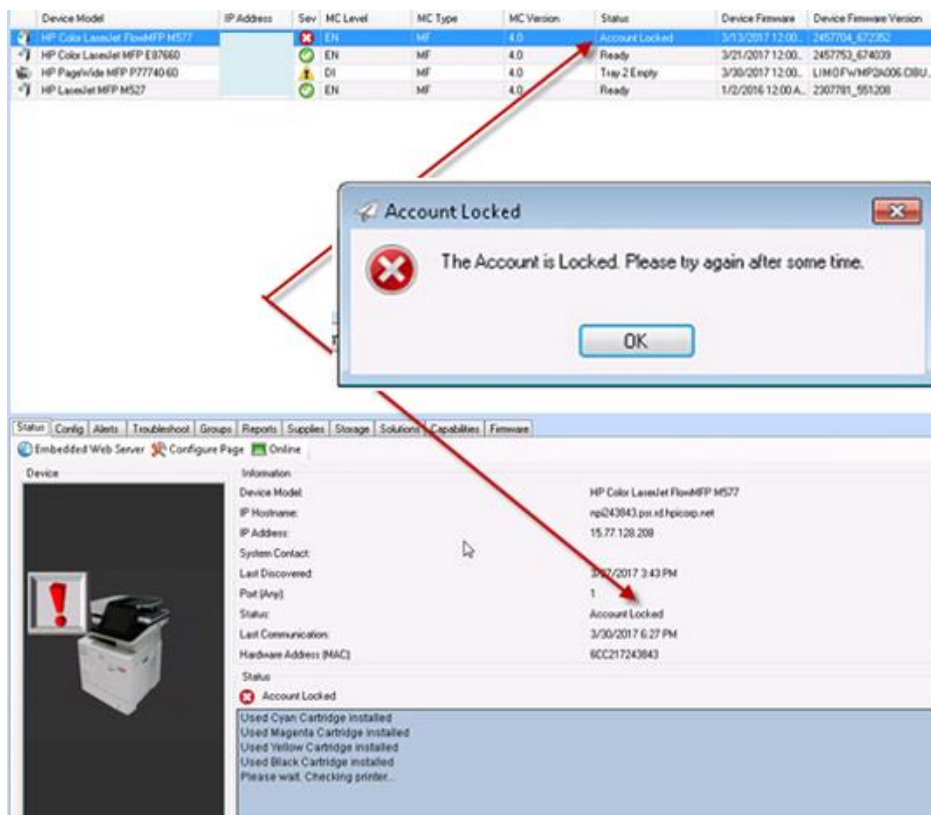


Figure 15: Account Lockout in HP Web Jetadmin 10.4 SR3 and later

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



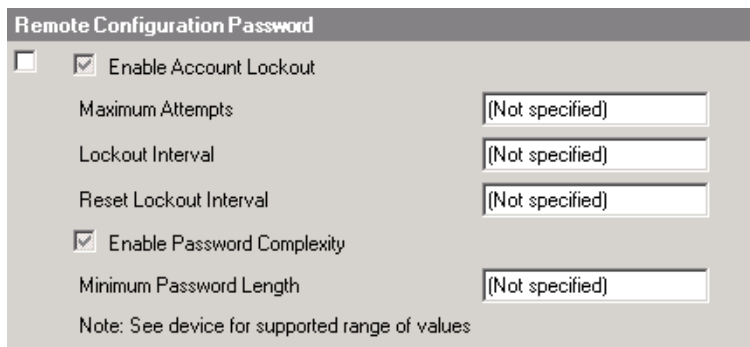


Figure 16: Remote Configuration Password configuration option

## PJL device access commands and settings

When PJJ Device Access commands is disabled, the following PJJ commands are no longer executed:

| PJJ Command          | Description                                   |
|----------------------|---|
| DEFAULT              | Sets default values for environment variables |
| OPMSG, RDYMSG, STMSG | Ready, Status, and Operator messages          |
| DMINFO, DMCMD        | SNMP over PJJ commands                        |
| INITIALIZE           | Resets PJJ values to factory default          |

HP Web Jetadmin offers the option to send PJJ configuration files to the printer with the **PJJ configuration** configuration option. The PJJ Device Access Commands must be enabled using the **Enable PJJ Device Access Commands** configuration option in the **Security** category.

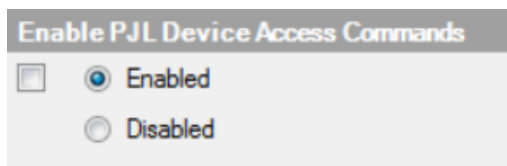


Figure 17: PJJ Device Access Commands configuration option

Sending PJJ files is 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 PJJ Device Access Commands are disabled, the printer settings do not change (even when HP Web Jetadmin reports success).

## HP Connection Inspector

HP Connection Inspector can be enabled/disabled in HP Web Jetadmin with Feature Pack 6. Later Feature Packs will have more configuration options for HP Connection Inspector.

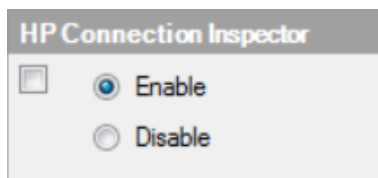


Figure 18: HP Connection Inspector configuration option

## Cross-site Request Forgery (CSRF) prevention

The latest release of HP Web Jetadmin (10.3 with Feature Pack 6) does not have a 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 **Secure Communication** configuration option in the **Security** category.

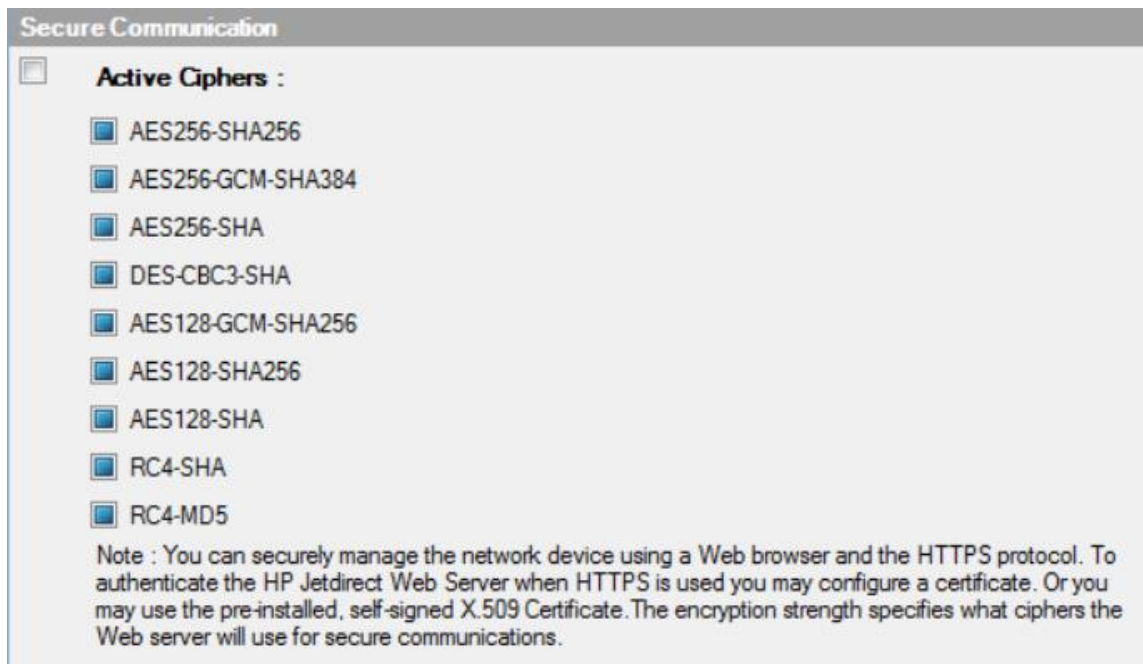


Figure 19: Secure Communication configuration option

---

[hp.com/go/getconnected](https://hp.com/go/getconnected)

Current HP driver, support, and security alerts  
delivered directly to your desktop

© Copyright 2020 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

