Technical white paper

Firmware updates sent as Print Jobs Disabled by default in FutureSmart bundle 4.10

Table of contents

Created : January 2020 , Version 1

Introduction

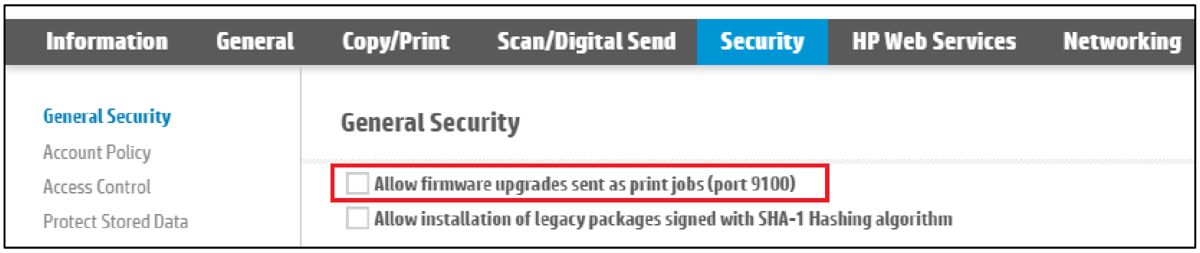
This whitepaper describes the change to the default value of the "**Allow firmware updates sent as print jobs (Port 9100)**" setting being introduced in FutureSmart firmware bundle version 4.10. It details it's effects on firmware installation methods and printing software solutions. This change is part of the Secure by Default initiative to provide a more secure printing device "out of box".

Detailed Description

HP printing devices have the ability to accept firmware upgrades, solutions software and custom color table "bundles sent as a print job. The "**Allow firmware updates sent as print jobs (Port 9100)**" setting controls the ability for the printing device to accept firmware over the standard printing port, and also applies to firmware sent over all print-path methods including FTP, LDP, IPP(s), EWS Print page or Copy command.

The setting is available from the device EWS, HP Web Jetadmin and HP Security Manager.

- EWS – "Allow firmware updates sent as print jobs (Port 9100)
- HP Web Jetadmin – "Printer Firmware Update"
- HP Security Manager – "Remote Firmware Update (RFU)"

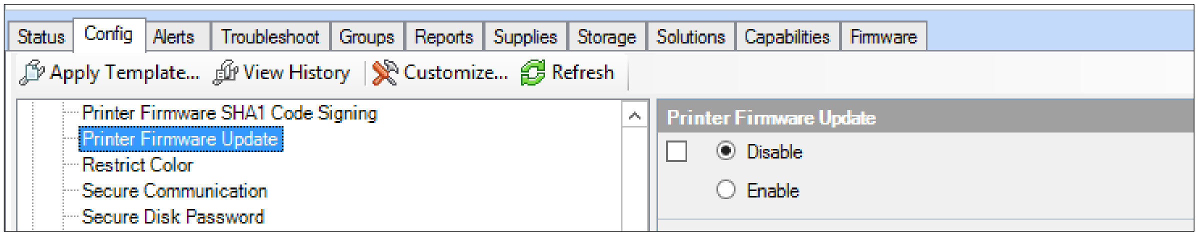


General Security

□ Allow firmware upgrades sent as print jobs (port 9100)

□ Allow installation of legacy packages signed with SHA-1 Hashing algorithm

"Allow firmware upgrades sent as print jobs" setting in the Embedded Web Server (EWS)

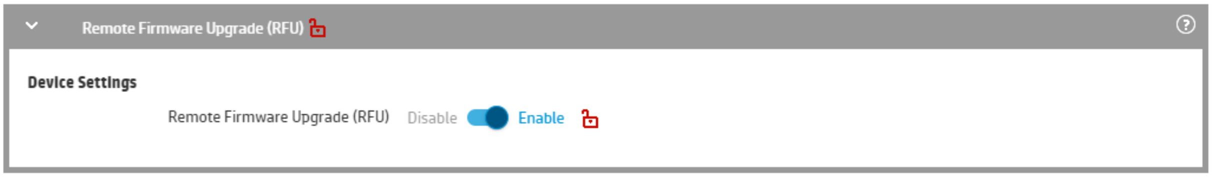


Printer Firmware Update

□ ● Disable

○ Enable

"Printer Firmware Update" setting in Web Jetadmin



Device Settings

Remote Firmware Upgrade (RFU) Disable [✓ Enable]

"Remote Firmware Update (RFU)"policy setting in HP Security Manager

Firmware bundle formats

Standard firmware and software bundles have the extension "BDL" and are processed by the device's Firmware Integration Manager (FIM) service. Content processed by the FIM service is sent over the standard web services transport/protocol.

Firmware and software formatted with specialized commands PJL use the file extension "RFU". Disabling the **"Allow firmware updates sent as print jobs (Port 9100)"** setting will cause the device to ignore PJL wrapped firmware and software.

Firmware upgrade behavior

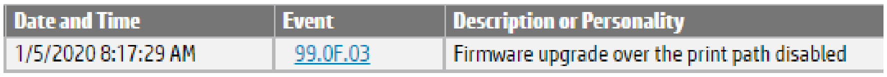
The updated “Allow firmware upgrades sent as print jobs (port 9100)” setting defaults are applied in the following circumstances:

- Devices purchased with FutureSmart bundle 4.10 and later use the new setting defaults (setting is disabled)
- Devices updated to FutureSmart bundle 4.10 or later from FutureSmart 3 bundles or FutureSmart 4 bundles before version 4.10 are not updated to the new setting default and maintain their current setting.
- Performing the following device resets on devices with FutureSmart 4.10 or later update the setting to the new default, overwriting any previously configured setting.
  - Format Disk
  - Partial Clean
  - Cold Reset

Printer firmware update behavior with setting disabled

The print device will act in the following ways when the “Allow firmware upgrades sent as print jobs (port 9100)“ setting is disabled

1. The printing device will accept and download a firmware bundle and reboot similar to a normal firmware update. However, the device will not load the firmware bundle, and delete the firmware code from the firmware repository.
2. The Configuration Page shows the FutureSmart firmware bundle has remained at the previous firmware version.
3. This printer behavior applies to attempted firmware upgrades and downgrades.
4. The printer Event Log will show a 99.0F.03 “Firmware upgrade over print path disabled” message



Date and Time	Event	Description or Personality
1/5/2020 8:17:29 AM	99.0F.03	Firmware upgrade over the print path disabled

Impact to Solutions software

HP and 3rd party solution software may have a dependency requiring print path updates to be enabled / re-enabled for installation, configuration or to function properly after installation. The following software may be impacted:

- Solutions that install on device agents to the EWS Solutions installer page
- Solutions that install licenses on the device
- Custom Color Tables sent as RFU formatted files

For more information

To read more about this settings default change and other Secure by Default initiative changes see the “**Secure by Default Initiative**” whitepaper, available here: http://h10032.www1.hp.com/ctg/Manual/c05818654

c06530233ENW, Created January 2020