Technical White Paper

HP Solutions – Working with Secure by Default Settings

April 2018

Table of contents

Overview

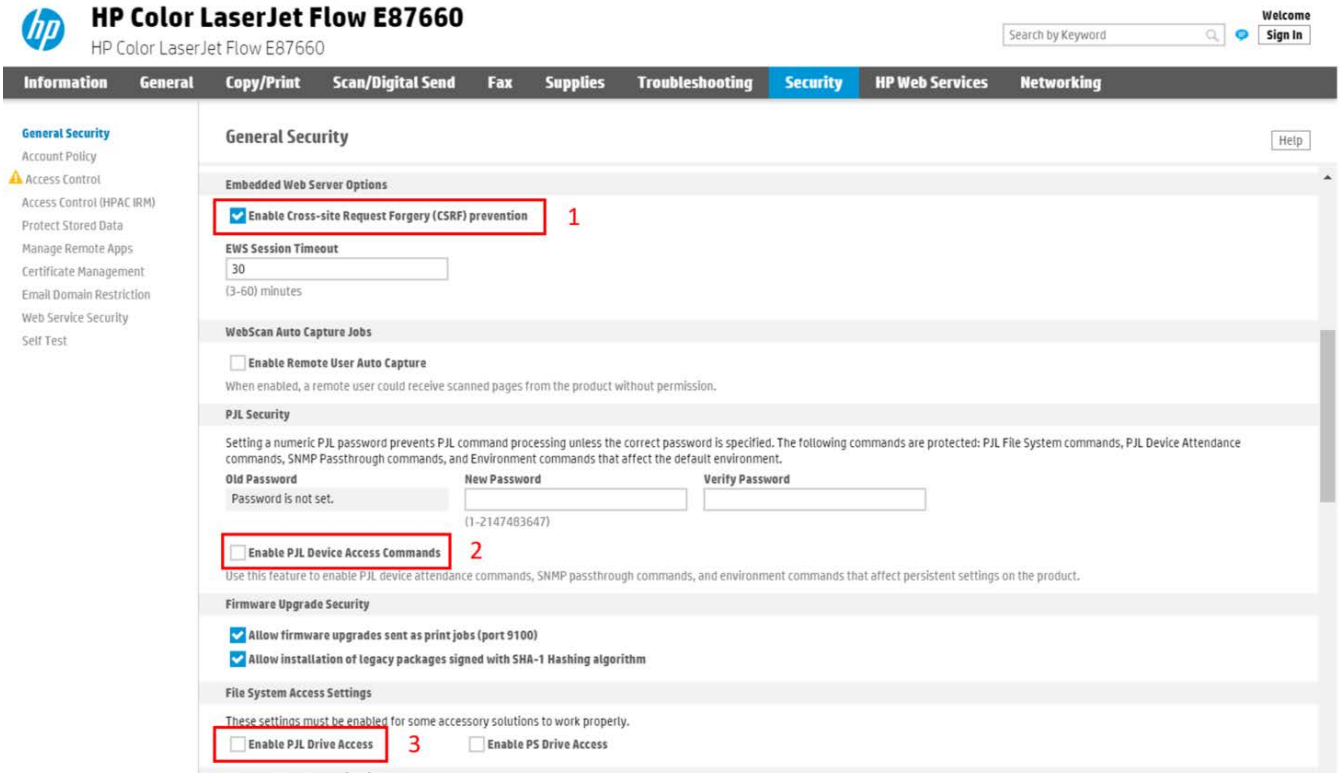
Secure by Default refers to updated default settings for a suite of security features implemented in HP FutureSmart firmware to make printers and MFPs more secure “out of box”. Some of these updated settings may block installation or configuration of certain solutions that require agents to be installed on the device.

For solutions that require agents to be installed on the device, administrators may need to temporarily disable Secure by Default settings prior to performing agent installation or configuration. Following that activity, Secure by Default settings should be re-enabled.

For more information about the Secure by Default Initiative including impact and workarounds on a per-solution basis, see the whitepaper here: http://h10032.www1.hp.com/ctg/Manual/c05818654.

Secure by Default Settings

In the following screenshot of the Embedded Webserver Security tab, several Secure by Default settings implemented in FutureSmart bundle 4.5 are highlighted.



1. “Enable Cross-site Request Forgery (CSRF) prevention”

This feature is enabled by default and is designed to prevent browser redirection to a malicious webserver. It can also prevent legitimate interactions with the device such as Solution configuration that are dependent on HTTP Post methods.

Important: In FutureSmart bundle 4.6, this feature protects against CSRF risks and may potentially impact Solutions.

2. “Enable PJL Device Access Commands”

This feature is disabled by default. When enabled, it allows printer configuration commands to be sent within print jobs using Printer Job Language (PJL).

Important: Some solutions may not install or function properly when this feature is disabled.

3. “Enable PJL Drive Access”

This feature is disabled by default. When enabled, it allows access to device storage using PJL commands.

Important: Installation of solutions to the printer’s storage (HDD, SSD, USB drive, CF drive, etc.) may be blocked if PJL drive access is not enabled.

Managing the Settings

This section describes strategies for managing Secure by Default settings.

1. Embedded Web Server (EWS)

The device EWS is a convenient way to manage settings on a small number of devices. Prior to installation of the Solution agent or configuration, disable these Secure by Default settings on each of the devices. Following installation or configuration of the solution, use the EWS to re-enable Secure by Default settings.

2. HP Web JetAdmin (WJA)

For larger device fleets, use WJA to manage the Secure by Default settings. A configuration template can be created to disable these settings prior to Solution installation or configuration. A second template can be used to re-enable the Secure by Default settings after the deployment is complete. The templates can be used again whenever Solution configuration changes are needed.

NOTE: WJA compatibility with Secure by Default settings was introduced in version 10.4 SR2 with FP6.

3. HP Security Manager (HP SM)

For customer fleets managed by HP SM, be aware that HP SM may try to re-implement Secure by Default settings during your solution maintenance.

NOTE: HP SM compatibility with Secure by Default settings was introduced in version 3.1. You may need to temporarily disable HP SM while you are configuring or installing solutions.

support.hp.com

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

Public

Edition 1, Created April 2018