



HP Solutions – Working with Secure by Default Settings

April 2018

Table of contents

Overview	2
Secure by Default Settings	2
1. “Enable Cross-site Request Forgery (CSRF) prevention”	3
2. “Enable PJJ Device Access Commands”	3
3. “Enable PJJ Drive Access”	3
Managing the Settings	3
1. Embedded Web Server (EWS)	3
2. HP Web JetAdmin (WJA)	3
3. HP Security Manager (HP SM)	4

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.

The screenshot displays the Embedded Webserver Security interface for an HP Color LaserJet Flow E87660. The page is titled "General Security" and includes a navigation menu with tabs for Information, General, Copy/Print, Scan/Digital Send, Fax, Supplies, Troubleshooting, Security (selected), HP Web Services, and Networking. A search bar and "Welcome Sign In" button are visible in the top right. The left sidebar lists various security settings under "General Security".

The main content area shows the following settings:

- Embedded Web Server Options:**
 - Enable Cross-site Request Forgery (CSRF) prevention** 1
 - EWS Session Timeout:** 30 (3-60) minutes
- WebScan Auto Capture Jobs:**
 - Enable Remote User Auto Capture**
When enabled, a remote user could receive scanned pages from the product without permission.
- PJI Security:**
 - Setting a numeric PJI password prevents PJI command processing unless the correct password is specified. The following commands are protected: PJI File System commands, PJI Device Attendance commands, SNMP Passthrough commands, and Environment commands that affect the default environment.
 - Old Password:** Password is not set.
 - New Password:** (1-2147483647)
 - Verify Password:**
- Enable PJI Device Access Commands** 2
Use this feature to enable PJI device attendance commands, SNMP passthrough commands, and environment commands that affect persistent settings on the product.
- Firmware Upgrade Security:**
 - Allow firmware upgrades sent as print jobs (port 9100)**
 - Allow installation of legacy packages signed with SHA-1 Hashing algorithm**
- File System Access Settings:**
 - These settings must be enabled for some accessory solutions to work properly.
 - Enable PJI Drive Access** 3
 - Enable PS Drive Access**

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 PJI 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 (PJI).

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

3. “Enable PJI Drive Access”

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

Important: Installation of solutions to the printer’s storage (HDD, SSD, USB drive, CF drive, etc.) may be blocked if PJI 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

© Copyright 2018 HP Inc. 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.

Edition 1, Created April 2018

