



Secure by Default Initiative

Device Settings and Features

Table of contents

Overview	2
Changes to Device Security Settings Defaults	2
SNMP v1/v2 write access disabled	2
Printer Job Language (PJL) / Postscript (PS) Drive Access	3
PJL Device Access Commands	3
TLS Ciphersuites	4
TLS Protocols	4
New FutureSmart 4 Security Features	5
HP Connection Inspector	5
Cross-Site Request Forgery Protection	5
Administrator Password Complexity and Minimum Length	6
Account Lockout	6
New Device Security Settings & Firmware Upgrade Behavior	7
Settings Defaults	8
Appendix A – Print Solution and Fleet Tool Impacts	9
Appendix B – Web Jetadmin SNMP Configuration for FutureSmart 4.5	11
Appendix C – PJL Device Access Commands	12
References	12

Overview

This document lists the security settings changes for the Secure by Default initiative beginning in Fall of 2017.

The following settings are affected by the initiative: (default settings changes)

- SNMP v1/v2 defaults
- File System Access through PDL and Postscript
- PDL Device Access Commands
- Ciphersuites containing RC4 and Triple DES (CBC3, 3DES)

The following new security features are enabled by default:

- Cross-Site Request Forgery (CSRF) prevention
- HP Connection Inspector (Network Behavioral Anomaly Detection)

Changes to Device Security Settings Defaults

SNMP v1/v2 write access disabled

Simple Network Management SNMP version 1 & 2 (v1/v2) is a legacy configuration protocol introduced in 1988. SNMP v1/v2 is not considered a secure configuration protocol for the following reasons:

- SNMP v1/v2 communications are sent in the clear through the network. Encryption is not available for v1/v2 connections. SNMPv3 provides encryption capabilities.
- SNMP v1/v2 is secured with a “community name” password string. The Set community name is also sent in the clear due to lack of encryption.
- SNMP supports configuration OIDs from the management Managed Information Database (MIB) structure. All configuration settings available in the management MIB can be set or changed using SNMP SET commands. Even when a SET community name is configured and required for write operations, it can be captured from the unencrypted SNMP data streams.

New Default:

The Secure by Default initiative disables the SNMPv1/v2 write capabilities and enables the device setting “**Enable SNMPv1/v2 read-only access**”. This disables SNMPv1/v2 Sets (writes) while allowing SNMPv1/v2 Gets (reads). The Get Community Name is used if configured.

EWS Setting Configuration Path:

Networking Tab -> Management Protocols menu -> SNMP page



Figure 1: SNMP v1/v2 settings in the Embedded Web Server (EWS)

Note: Printer drivers, Fleet management tools and printing device solutions that require SNMNP access to query the device for print capabilities are not affected by disabling the SNMPv1/v2 write access, requiring only read access.

Note: See [Appendix A – Print Solution and Fleet tool Impacts](#) for effects on device solutions and fleet management tools.

Printer Job Language (PJL) / Postscript (PS) Drive Access

The PJL and Postscript print languages support commands providing access to the device mass storage device; typically a HDD. This access is commonly used to install onboard printing solutions and specialized fonts.

New Default:

The Secure by Default initiative disables the “Enable PJL Drive Access” and “Enable PS Drive Access” settings.

EWS Setting Configuration Path:

Security Tab ->General Security Menu

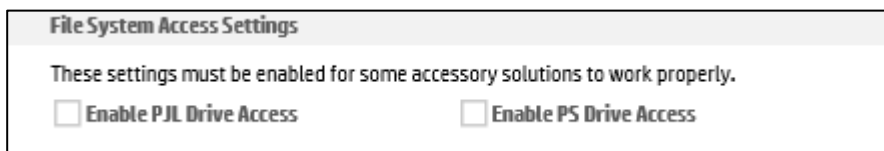


Figure 2: File System Access Settings in the Embedded Web Server (EWS)

Note: See the [Appendix A – Print Solution and Fleet tool Impacts](#) for effects on device solutions and fleet management tools.

PJL Device Access Commands

The “Enable PJL Device Access Commands” setting enables PJL management command structures over the PJL protocol. This includes changing the printing device control panel messages, changing printer default settings and sending SNMP commands over PJL.

Note: See Appendix B for additional information regarding PJJ management commands.

New Default:

The Secure by Default initiative disables the “Enable PJJ Device Access Commands” setting.

EWS Setting Configuration Path:

Security Tab -> General Security Menu

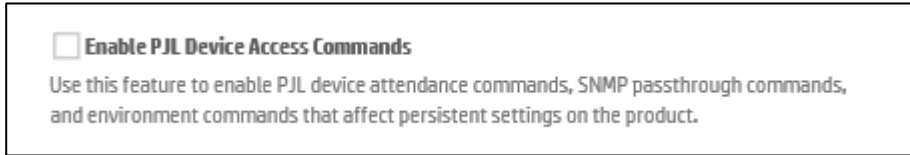


Figure 3: PJJ Device Access Command in the Embedded Web Server (EWS)

This setting may need to be temporary re-enabled to allow PJJ scripting for installation and management.

Note: See [Appendix A – Print Solution and Fleet tool Impacts](#) for effects on device solutions and fleet management tools.

TLS Ciphersuites

The RC4, DES and 3DES protocols have known vulnerabilities and are no longer recommended for HTTPS encryption. RC4 (Rivest Cipher 4) was designed in 1987 and 3DES was approved in 1995.

New Default:

The RC4 and 3DES (DES-CBC3-SHA) based cipher suites are disabled as in the Secure by Default security profile.

EWS Setting Configuration Path:

Security Tab -> Secure Communication menu

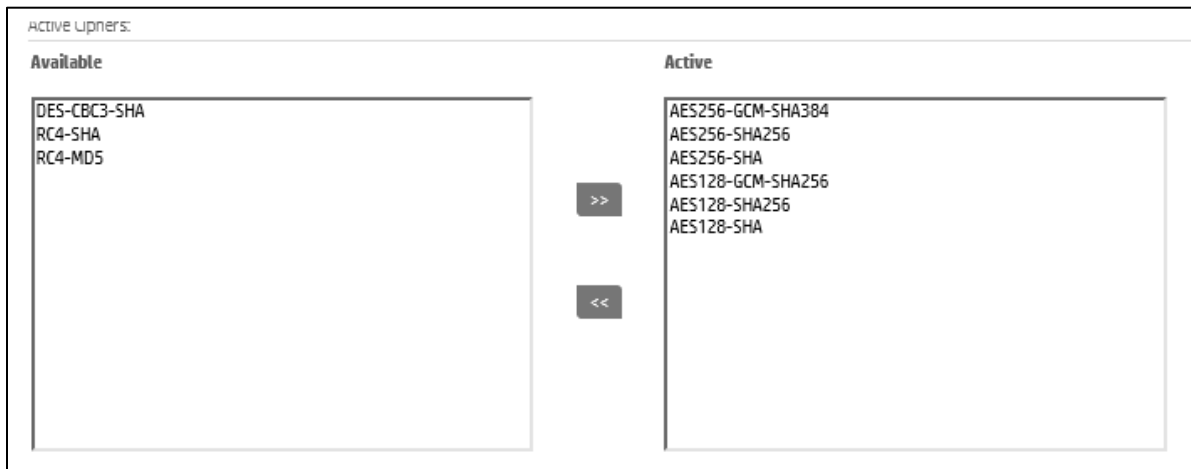


Figure 4: HTTPS Ciphersuite Selection in the Embedded Web Server (EWS)

Note: These ciphersuites may be needed for Windows XP, Windows Server 2003 and Internet Explorer 8 legacy installations.

TLS Protocols

The Transport Layer Security (TLS) protocol versions 1.0 & 1.1 will be disabled by default beginning with FutureSmart bundle 4.7.2 and later, including the 4.8 fleet release in June 2019.

TLS versions 1.0 & 1.1 have known vulnerabilities and are no longer recommended for cryptographic communications. TLS 1.0 and 1.1 were defined in 1999 and 2006 respectively.



Figure 5: TLS protocols in the Embedded Web Server (EWS)

Note: Some HP and 3rd party solution software may have TLS 1.0 dependencies requiring TLS 1.0 to be enabled / re-enabled for installation or to function properly after installation.

Note: HP and 3rd party solutions may inherit their TLS protocol properties from their host server. Some server operating system versions may not support TLS versions greater than TLS 1.0 or may require additional configuration to enable TLS 1.2 support.

See [Appendix A – Print Solution and Fleet tool Impacts](#) for effects on device solutions and fleet management tools.

New FutureSmart 4 Security Features

The FutureSmart 4.5 FutureSmart bundle includes several new security features. All new security features are enabled by default when introduced to ensure the most secure printing device state. These features may include a configuration setting to be disabled for specific networking environments.

HP Connection Inspector

HP Connection Inspector is a new intelligent embedded security feature. The technology is unique in that it can inspect outbound network connections typically abused by malware, determine what is normal and stop suspicious activity. If the printer is compromised, it will automatically trigger a reboot to initiate HP Sure Start self-healing procedures.

This feature is enabled by default. It can be disabled and has user configurable settings to tune the feature to specific networking environments and reduce false positives.

EWS Setting Configuration Path:

Networking Tab -> TCP/IP Menu -> Network Identification Page



Figure 6: HP Connection Inspector in the Embedded Web Server (EWS)

Please see the [HP Connection Inspector Technical Whitepaper](#) more information.

Note: See [Appendix A – Print Solution and Fleet tool Impacts](#) for effects on device solutions and fleet management tools.

Cross-Site Request Forgery Protection

Cross-Site Request Forgery (CSRF) is an exploit which hijacks the authenticated user session to send unauthorized requests to a server. When the device administrator authenticates to the EWS server, it generates a session authentication token. The CSRF feature provides for generating an additional cryptographic randomly generated CSRF token which protects against an attacker sending commands as the authenticated administrator.

When enabled the CSRF feature prevents sending commands to the device through the EWS configuration interface without first having initiated a EWS session, which establishes the CSRF Token. This method is referred to as “web scraping” as the commands are captured and replayed to configure device settings through scripting.

This feature is enabled by default. It can be disabled if required.

EWS Setting Configuration Path:

Security Tab -> General Security

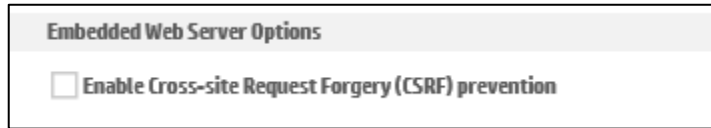


Figure 7: Cross-Site Request Forgery (CSRF) Protection in the Embedded Web Server (EWS)

Note: See [Appendix A – Print Solution and Fleet tool Impacts](#) for effects on device solutions and fleet management tools.

Please see [Preventing Cross Site Request Forgery \(CSRF\) Attack using CSRF-Tokens on HP Printing Devices](#) for more information.

Administrator Password Complexity and Minimum Length

The administrator password complexity feature requires complex passwords requiring 3 of the 4 following categories:

- Upper case characters
- Lower case characters
- Numbers
- Special characters

The minimum password length feature requires an administrative password between 1- 16 characters long. The default setting is 8 characters. A Zero (0) minimum password length disables the minimum password length feature.

This feature is enabled by default. It can be disabled if required.

Account Lockout

The Account lockout feature protects the device administrative accounts by providing safeguards to prevent brute force hacking attempts. After a set number of failed authentication attempts the system prevents further authentication attempts for a specific interval.

The account lock feature applies to the following passwords:

- EWS password
- Remote configuration password
- SNMPv3 authentication and privacy passphrases

This feature is enabled by default. It can be disabled if required.

EWS Setting Configuration Path:
Security Tab -> Account Policy

The screenshot shows the 'Local Administrator Password' configuration page. It features two unchecked checkboxes: 'Enable account lockout' and 'Enable password complexity'. Below the second checkbox is a note: 'When checked, the password must contain three of the following: uppercase letters, lowercase letters, numbers, and special characters.' Underneath is a section for 'Minimum password length' with a text input field containing the value '0'. A final note states: 'Zero (0) indicates that the minimum password length is disabled; no password is required.'

Figure 8: Account Lockout, Complexity & Minimum Length in the Embedded Web Server (EWS)

New Device Security Settings & Firmware Upgrade Behavior

All devices delivered with FutureSmart firmware bundle 4.5 will include the new security features and security settings defaults. Devices upgraded to FS 4.5 will switch to the new settings defaults only after a full device reset as listed below.

The following scenarios apply:

- Devices purchased with FutureSmart bundle 4.5 (after November 2017)
 - New security defaults apply
 - New security features present and enabled by default
- Devices updated to FutureSmart bundle 4.5 from FutureSmart 3 bundles or FutureSmart 4 bundles before version 4.5
 - Security settings are not update the security settings to the new defaults and maintain their current setting.
 - New security features are present and enabled by default
- Performing the following device resets update the security settings to the new defaults, overwriting any previously configured setting
 - Format Disk
 - Partial Clean
 - Cold Reset

Important: Device Resets found in the EWS Troubleshooting Tab **do not** fully reset security settings to the Secure by Default security profile. The following resets should not be used to enable Secure by Default settings:

- Reset Factory Defaults
- Firmware Reset

Settings Defaults

The following tables contain the Secure by Default settings current and updated defaults.

Security Setting	FutureSmart 3 and FutureSmart pre-4.5 Defaults	FutureSmart 4.5 Defaults
SNMPv1/v2	Enable SNMPv1/v2 Read-Write access	Enable SNMPv1/v2 Read-only access
PJL/PS File Access	Enabled	Disabled
PJL Device Access Commands	Enabled	Disabled
TLS Ciphersuites containing RC4 and 3DES	Active (enabled)	Available (not enabled)
TLS version 1.0 / 1.1	Enabled	Disabled (beginning with FutureSmart 4.7.2)

Security Feature	Default	Can be disabled	Affected Technologies
Cross-Site Request Forgery Prevention	Enabled	Yes	Print solutions from specific vendors may need to disable setting until compliant. MPS and customer scripting tools may need to temporarily disable CSRF to execute.
HP Connection Inspector	Enabled	Yes	None
Administrative Password Min Length and Complexity	Enabled	Yes	Defaults may need to be changed to accommodate existing passwords used for print solutions and fleet tools.
Account Lockout	Enabled	Yes	Defaults may need to be changed to accommodate WJA.

Appendix A – Print Solution and Fleet Tool Impacts

This section describes known impacts resulting from the new security features and updated security default settings.

Fleet Tool or Print Solution	Minimum Compatible Solution version if impacted	Impact to Customers New device deployment OR Upgraded devices after performing a Format Disk, Partial clean or Cold Reset	Available Workarounds
HP Web Jetadmin (WJA)	10.4-SR2 FP6 or 10.4-SR3 FP6	FP6 required for new configuration item “SNMP Credential” (FutureSmart Version 4.0 and higher) See Appendix B – Web Jetadmin SNMP Configuration Options for FutureSmart 4.5 for additional information.	For WJA versions before 10.4SR2 FP6 Use HP SM v3.1 or EWS to enable write access for SNMPv1/v2 or Configure SNMPv3
		WJA requires PjL Disk Access to manage fonts and macros.	Use WJA to enable PjL Disk Access
		WJA requires PjL Device Access Commands to be enabled for device configuration with PjL files sent from WJA.	Use WJA to enable PjL Device Access Commands
HP JetAdvantage Security Manager (HP SM)	HP SM 3.1	Version 3.1 required for SNMPv1/v2 compatibility	For HP SM versions before 3.1 Use WJA 10.4-SR2 w/FP6 or EWS to enable SNMPv1/v2 write access or Configure SNMPv3
		CSRF must be disabled for any policy modifying LLMNR and 802.1x, or other settings using HTTP POST configuration method	Include disabling CSRF in any HP SM policy modifying these settings
Fleet Deployment Tool (FDT)	FDT 1.7.4	Version 1.7.4 required for CSRF compatibility FDT may be impacted and requires TC to verify all Workflows against device. May need to enable features via EWS based on the task or recording.	For FDT versions before 1.7.4 Use WJA 10.4 w/XTP ticket, HP SM or EWS to disable CSRF
HP Access Control (HP AC)	All versions of HP AC impacted.	PjL disk access and PjL Device Access Commands are required for installation and configuration of HP AC. CSRF must be disabled for solution installation and configuration of HP AC.	Use WJA, HP SM or EWS to enable PjL disk access and PjL Device Access Commands and disable CSRF for installation and configuration of HP AC IRM agent. Following installation/configuration, PjL disk access and CSRF can be disabled again.
HP Capture and Route (HP CR)	All versions of HP CR impacted.	SNMP write access required for solution installation.	Use WJA 10.4-SR2 w/FP6, HP SM 3.1 or EWS to enable SNMPv1/v2 write access for installation and configuration of HP CR on the device. Following installation/configuration, SNMP write access can be disabled again.
HP Embedded Capture (HP EC)	All versions of HP EC impacted	CSRF must be disabled for solution installation and configuration.	Use WJA, HP SM or EWS to disable CSRF for installation and configuration of HP CR on the device. Following installation/configuration, CSRF enabled again.
		TLS version 1.0 required for solution compatibility.	Use WJA, HP SM or EWS to enable TLS version 1.0

Fleet Tool or Print Solution	Minimum Compatible Solution version if impacted	Impact to Customers New device deployment OR Upgraded devices after performing a Format Disk, Partial clean or Cold Reset	Available Workarounds
JetAdvantage Management /Smart Device Services JAM/SDS	20171009.8/JAMC 4.1.2986 or later	SDS features that require SNMP write access (ex: Remote Reboot or Supplies Message Suppression) must turn on SNMPv1/v2 writes or SNMPv3 credentials.	Use WJA 10.4-SR2 w/FP6, HP SM 3.1 or EWS to enable SNMPv1/v2 write access
LRS MFPsecure	All versions of MFPsecure are impacted.	PJL disk access and PJL Device Access Commands required for installation and configuration of MFPsecure.	Use WJA, HP SM or EWS to enable PJL disk access and PJL Device Access Commands for installation and configuration. Following installation/configuration, PJL disk access can be disabled again.
Safecom	Latest SafeCom Agent *31.25 or Newer	Basic testing shows no impact. Contact the Solution Partner for confirmation of Support before deploying.	
Equitrac	Equitrac 5.7 WITH Hotfix(v 294662) or newer only	Basic testing shows no impact. Contact the Solution Partner for confirmation of Support before deploying.	
Troy	Customer/Account team should contact Troy for compatibility information	TROY has stated that depending on the customer and configuration of their solution they should perform a POC and then work with TROY Group to further diagnose.	
Pharos and Celiveo	The changes have been communicated to Partners.	Contact the Solution Partner for confirmation of Support before deploying.	
Partner Solutions (Silver)	The changes have been communicated to Partners.	Contact the Solution Partner for confirmation of Support before deploying.	
DSS	Version 5.0 and earlier	Unable to configure DSS workflows with CSRF enabled on FS 3.9.2 or later	Use WJA, HP SM or EWS to disable CSRF for configuration of DSS workflows.
ePrint	No impact		
JetAdvantage Connect	No impact		
Windows operating system support for TLS 1.1 / 1.2	Windows Server 2008 R2 and higher Windows Vista and higher	TLS 1.0 required for print devices accessing solutions running on Windows OS not supporting TLS 1.1 / 1.2	Use WJA, HP SM or EWS to enable TLS 1.0 for print devices with FutureSmart bundle 4.7.1 or previous.

Appendix B – Web Jetadmin SNMP Configuration for FutureSmart 4.5

Web Jetadmin feature pack 6 adds an SNMP configuration option “**SNMP Credentials – FutureSmart 4**” for the configuration of FutureSmart 4.5 and higher. The setting allows configuring SNMP over the Common Data Model (CDM) protocol, which is new in FutureSmart 4.5. For older FutureSmart versions the WJA SNMP configuration setting is “**SNMP Credentials – FutureSmart 3 and Non-FutureSmart devices**” (before 10.4SR3 this option was called “**SNMP Version Access Control**”)

The option “**SNMP Credentials – FutureSmart 4**” must be used instead of the option **SNMP Credentials – FutureSmart 3 and Non-FutureSmart devices** “to configure SNMP through WJA when SNMP is set to read-only (or disabled) on the device.

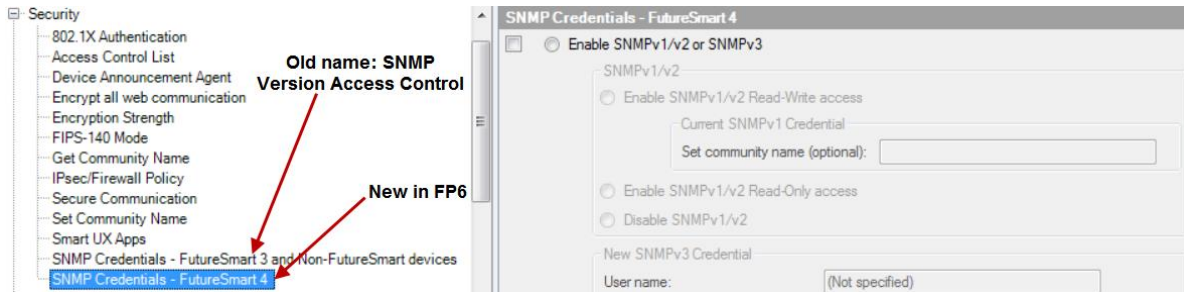


Figure 8: WJA SNMP configuration options in batch mode with Feature Pack 6

This table describes the WJA SNMP configuration option to use for specific FutureSmart versions and SNMP configurations.

Device family and SNMP state	Required WJA	Name of Configuration option to configure SNMP
FutureSmart 4.5 with SNMPv1/v2 set to read-only and SNMPv3 not configured	10.4-SR2 w/FP6 10.4-SR3 w/FP6 (or higher)	SNMP Credentials - FutureSmart Version 4.0
FutureSmart 4.4 and older devices and non FutureSmart devices	10.4-SR2 w/FP6 10.4-SR3 w/FP6 (or higher)	SNMP Version Access Control SNMP Credentials – FutureSmart 3 and Non-FutureSmart devices
FutureSmart 4.5 with SNMPv1/v2 set enabled and/or SNMPv3 configured	Legacy WJA	SNMP Version Access Control
FutureSmart 4.4 and older and non FutureSmart devices	Legacy WJA	SNMP Version Access Control

Appendix C – PJJ Device Access Commands

The PJJ Device Access Command setting controls access to PJJ management commands. The following table lists which PJJ commands are controlled with this command.

PJJ Command	Controlled by PJJ Device Access Command setting	Description
DEFAULT	Yes	Sets default values for environment variables.
OPMSG, RDYMSG, STMSG	Yes	Ready, Status and Operator messages
DMINFO, DMCMD	Yes	SNMP over PJJ commands
INITIALIZE	Yes	Resets PJJ values to factory default
SET	Yes	Sets environment variable to specified value for duration of a PJJ job.
File system commands (FS*)	No	Controlled by PJJ File Access command
UEL, COMMENT, ENTER, JOB, EOJ, RESET INQUIRE, DINQUIRE, ECHO, INFO USTATUS, USTATUSOFF	No	Job control and job status commands

References

- Preventing Cross Site Request Forgery (CSRF) Attack using CSRF-Tokens on HP Printing Devices
<http://h10032.www1.hp.com/ctg/Manual/c05428973.pdf>
- HP FutureSmart 4 Administrative Password Security Features
<http://h10032.www1.hp.com/ctg/Manual/c05429015>
- Discovering And Configuring FutureSmart Devices Version 4.5 And Later with HP Web Jetadmin
<http://h10032.www1.hp.com/ctg/Manual/c05813511>

Additional documents TBD

Get connected

hp.com/go/getconnected

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

