Technical whitepaper

HP SureStart, whitelisting and intrusion detection security features

Table of contents

Feature operation

The HP SureStart, Whitelisting and Runtime Intrusion Detection features are firmware based and do not require any external dependencies. There are **no configuration options** and the features are **always on by default**. This is by design to prevent disabling of the features by an attacker as part of an advanced multi-stage attack or exploit.

HP SureStart

The printer's BIOS is a set of boot instructions to initiate hardware components and load the HP FutureSmart firmware. HP SureStart validates the integrity of the BIOS image using a SHA-256 hash signed with HP's digital signature. If validation of the primary BIOS image fails, a protected "Golden Copy" is used to boot the device providing a self-healing capability.

HP SureStart is dependent on a hardware component and is only available on devices introducing Spring 2015 and later. Please see "Appendix B: Device Support".

Whitelisting

Whitelisting validates the integrity of firmware system files during the load process using a SHA-256 hash signed with HP's digital signature. If validation fails the device reboots and holds at the preboot menu to prevent a potential malware exploit from executing.

Digital signatures for HP and 3rd party developed solutions residing on the printing device are validated using a SHA-256 hashing algorithm for HP firmware and a SHA1/256 hash for 3rd party firmware. If validation fails during the load of HP firmware, the device will reboot. If validation fails during the load of 3rd Party solution firmware, the firmware will not be loaded to prevent a malware exploit.

Runtime intrusion detection

Intrusion Detection detects potential malware intrusions in system memory. Firmware runs in the background to validate the memory space and reboots the device if a possible intrusion is detected. If the Auto-recover feature is disabled, or a possible intrusion occurs twice within 30 minutes, the device reboots and holds at the preboot menu to prevent a potential malware exploit from executing. The device will attempt to wait until in process print jobs have been cancelled to reboot.

Feature availability

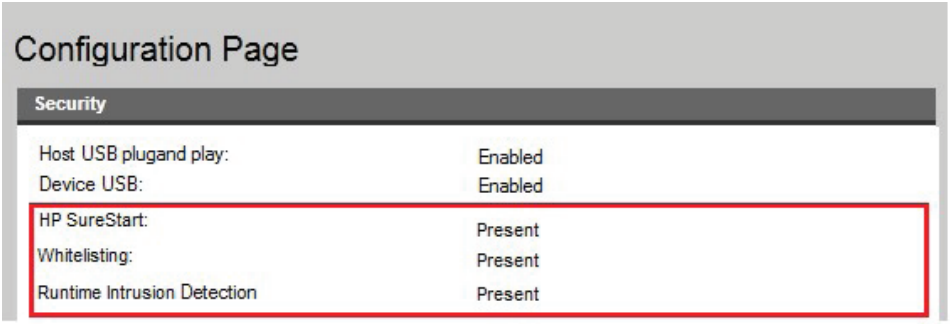
These features are available with the FutureSmart Bundle Version 3.7 and later. If present, the features are listed in the device configuration page in the Security Section. For specific firmware versions see "Appendix B: Device Support".

Note: HP SureStart is not supported on pre-2015 devices. See "Appendix B: Device Support".

Upgrade/Downgrade

HP SureStart capable devices

To downgrade HP SureStart capable devices from firmware supporting HP SureStart to firmware without HP SureStart support, the firmware downgrade requires physical presence and must be performed from the preboot menus.



Note: See "Appendix B: Device Support" for a listing of HP SureStart capable devices.

Attempting to downgrade an HP SureStart capable device to non-HP SureStart firmware in a fully running state either from the device EWS or through Web Jetadmin, will result in a **99.00.32** error. When receiving this error, the firmware **will no**t download to the device, and the firmware will need to be downloaded again through the preboot menus.

Non- HP SureStart capable devices

Firmware downgrades for devices that do not support HP SureStart can be downloaded using any method supported from the Ready screen. Downgrading through the preboot menus is not required.

Firmware downgrade instructions using the preboot menus

Follow these instructions to update the device firmware by downloading through the preboot menus:

1. Copy the device firmware onto a USB thumb-drive. The drive must be formatted using FAT32.
2. Insert the USB thumb drive containing the firmware bundle into an available USB port of the printer.
3. Turn the printer Off and then On, and when the HP logo displays on the control panel and all three Ready, Data, and Attention LEDs illuminate solid, press ⊗.
   OR
4. Turn the printer Off and then On, and when 1/8 displays below the HP logo on the control panel, touch the logo.
5. Scroll to select the Administrator > Download > USB Thumb-drive menu.
6. Select the firmware .bdl file from the list. Be sure to select the correct firmware for the device being updated.
7. Wait for the firmware to be transferred to the device.
8. When "Complete" is displayed, select Back twice to navigate to the top menu, and select Continue.
9. The device will reboot.
10. Verify the firmware successfully upgraded by reviewing the device Configuration Page.

Event log entries and Control panel messages

33.05.0X SureStart errors

The 33.05.0X HP SureStart error codes display on the printer's control panel and the Event Log Page when the downloaded firmware fails to validate the BIOS code. The following tables describe the HP SureStart error codes and solutions to resolve the issue.

33.05.0X Event log entries

Event log error code and message	Cause	Recommended action
33.05.00 Boot code corrupt **33.05.01 Boot code corrupt** **33.05.02 Boot code corrupt** **33.05.03 Boot code corrupt**	The printer detected and recovered from a corrupted version of the BIOS.	No action is required. The printer automatically restarts and arrives at a "Ready" state.
33.05.04 Upgrade corrupt **33.05.05 Boot code corrupt** **33.05.06 Upgrade corrupt** **33.05.07 Upgrade corrupt**	A previously downloaded firmware (FutureSmart firmware bundle version 3.7 or newer) failed to cryptographically validate the BIOS code.	No action is required.
33.05.08 Invalid boot attempt **33.05.09 Downgrade attempted**	An error occurred when a printer in a "Ready" state with FutureSmart firmware bundle version 3.7 is downgraded to an older firmware version. **NOTE:** The printer will not have downgraded when this error is displayed in the Event Log Page.	Downgrade the firmware from the Preboot menu using a USB flash drive. See "Firmware downgrade instructions using the preboot menus" in the Upgrade/Downgrade section.

33.05.0X Control panel error codes

Control panel error code and message	Cause	Recommended action
33.05.01 Security Alert **33.05.02 Security Alert** **33.05.03 Security Alert** **33.05.04 Security Alert** **33.05.05 Security Alert** **33.05.06 Security Alert** **33.05.07 Security Alert**	The newly downloaded firmware failed to cryptographically validate the BIOS code.	Update the firmware from the Preboot menu using a USB flash drive. See "Firmware downgrade instructions using the preboot menus" in the Upgrade/Downgrade section.

33.05.1X Whitelisting errors

The 33.05.1X Whitelisting error codes display on the printer's control panel and the Event Log Page when a failure occurs when validating the firmware files digital signature or the firmware file certificate. The following tables describe the Whitelisting error codes and solutions to resolve the issue.

33.05.1X Event log entries

Event Log error code and message	Cause	Recommended action
33.05.10 Firmware verification Error 33.05.11 Firmware verification Error 33.05.12 Firmware verification Error	A previous system boot cycle failed to cryptographically validate a firmware file's digital signature.	No action is required.

33.05.1X Control panel error codes

Control panel error code and message	Cause	Recommended action
33.05.10 Security alert 33.05.11 Security alert 33.05.12 Security alert	An error occurred with the firmware file's digital signature, or an error occurred with the certificate used to validate the firmware file digital signature.	Follow these steps to resolve the issue: From the device preboot menu, Perform a Partial clean. If the device does not reboot to the Ready screen, Download a firmware bundle from the Preboot menu using the USB flash drive See "Firmware downgrade instructions using the preboot menus"s in the Upgrade/ Downgrade section. **NOTE:** Performing a Partial Clean is required before downloading a firmware bundle in Step 2.

33.05.2X Intrusion detection error

The 33.05.2X Intrusion Detection error codes display on the printer's control panel and the Event Log Page when a potential malware intrusion is detected in the system memory. The following tables describe the Intrusion Detection error codes and solutions to resolve the issue.

33.05. X Event log entries

Event Log error code and message	Cause	Recommended action
33.05.21 Potential Intrusion	A possible intrusion detection occurred.	No action is required. **NOTE:** If this error displays frequently in the Event Log Page, a network intrusion might be present. Contact the network security administrator.
33.05.22 Cannot scan for potential intrusions	The intrusion detection memory process was not detected.	No action is required. **NOTE:** If this error displays frequently in the Event Log Page, a network intrusion might be present. Contact the network security administrator.
33.05.23 Intrusion detection not initialized 33.05.24 Intrusion detection initialization error	The intrusion detection memory process did not initialize.	No action is required. **NOTE:** If this error displays frequently in the Event Log Page, a network intrusion might be present. Contact the network security administrator.

33.05.2X Control panel error codes

Control panel error code and message	Cause	Recommended action
33.05.21 Potential Intrusion 33.05.21 Security Alert	A possible intrusion detection occurred. **NOTE:** When the printer encounters a security threat, a **33.05.21 Potential Intrusion** error message displays on the printer's control panel while canceling any print jobs, and then displays a **33.05.21 Security Alert** message in the Preboot menu.	Turn the printer Off, and then On to clear the error. The printer should return to a "**Ready**" state. **NOTE:** Selecting "Continue" from the Preboot menu will not resolve the error.
33.05.22 Security Alert	The intrusion detection memory process was not detected.	Turn the printer Off, and then On to clear the error. The printer should return to a "**Ready**" state. **NOTE:** Selecting "Continue" from the Preboot menu will not resolve the error.
33.05.23 Security Alert 33.05.24 Security Alert	The intrusion detection memory process did not initialize.	Turn the printer Off, and then On to clear the error. The printer should return to a "**Ready**" state. **NOTE:** Selecting "Continue" from the Preboot menu will not resolve the error.

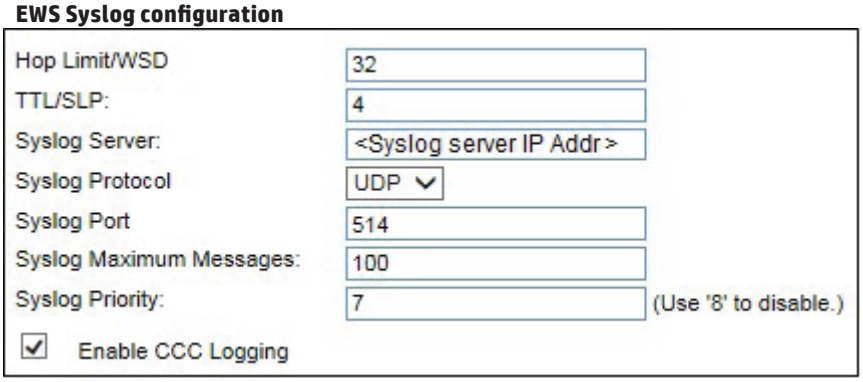
Device Syslog configuration for logging security events

The syslog protocol provides a transport allowing devices to send event notification messages across IP networks to syslog servers. HP printing devices support sending syslog event messages to a syslog server or compatible Security Information Event Management (SIEM) software including HP ArcSight and Splunk®.

Syslog Server settings

The following settings provide the ability for HP printing devices to send Syslog event notifications.

EWS Syslog configuration



Name	Description	Default Value	Recommended Value
Hop Limit/WSD	Set the WS-Discovery hop limit for the site local IPv6 multicast packet.	32	32
TTL/SLP	Specifies the IP multicast "Time To Live" (TTL) setting for Service Location Protocol (SLP) packets. The default value is 4 hops (the number of routers from the local network). The range is 1-15. When set to a -1, multicast capability is disabled.	4	4
Syslog Server	Syslog server network Address	None	Address of Syslog server of HP ArcSight
Syslog Protocol	UDP or TCP	UDP	UDP
Syslog Port	Port number of Syslog server	512	(Server port number if different from default)
Syslog Max Messages	Maximum per minute. Increase if Syslog messages being dropped.	10	100
Syslog Priority	Determines highest allowable priority message (4 allows priority 0 – 4)	7 (all messages)	**4**
Enable CCC Logging	Enables sending security related messages. Required for SureStart, Whitelisting and Intrusion Detection	Disabled	Enabled

Appendix A: Syslog message content

This section describes syslog message format and content. The format uses the following value construction:

<**Priority**> **Tag: Message: Time (UTC offset): Source IP**

Where

Priority = Number representing the combination Facility & Severity

Tag = "Printer"

Message = Error description

Time and (UTC offset) = time of security event

Source IP = printer IP address

Priority code:

<49>: Facility = 6 line printer sub-system

Priority = 1 Alert: action must be taken immediately

33.05.0X HP SureStart

33.05.01, 33.05.02, 33.05.03, 33.05.05

<49> printer: Boot code corrupt: time="2015-Sep-30 12:21:42 (UTC-07:00)" source _ IP="printer _ addr"

33.05.04, 33.05.06, 33.05.07

<49> printer: Upgrade corrupt: time="2015-Sep-30 12:21:42 (UTC-07:00)" source _ IP="printer _ addr"

33.05.08

<49> printer: Invalid boot attempt: time="2015-Sep-30 12:21:42 (UTC-07:00)" source _ IP="printer _ addr"

33.05.09

<49> printer: Downgrade attempted: time="2015-Sep-30 12:21:42 (UTC-07:00)" source _ IP="printer _ addr"

33.05.1X Whitelisting

33.05.10

<49> printer: Code Sign error: time="2015-Sep-30 12:21:42 (UTC-07:00)" source _ IP="printer _ addr"

33.05.11

<49> printer: Code sign error: time="2015-Sep-30 12:21:42 (UTC-07:00)" source _ IP="printer _ addr"

33.05.12

<49> printer: Code sign error: time="2015-Sep-30 12:21:42 (UTC-07:00)" source _ IP="printer _ addr"

33.05.2X Intrusion detection

33.05.21

<49> printer: Potential intrusion. Memory corruption detected: time="2015-Sep-30 12:21:42 (UTC-07:00)" source _ IP="printer _ addr"

33.05.22

<49> printer: Intrusion detection disabled. Unable to scan for memory corruption: time="2015-Sep-30 12:21:42 (UTC-07:00)" source _ IP="printer _ addr"

33.05.23

<49> printer: Failed to initialize intrusion detection: time="2015-Sep-30 12:21:42 (UTC-07:00)" source _ IP="printer _ addr"

Appendix B: Device Support

This table lists the features for supported devices when running FutureSmart Bundle Version 3.7.

Printing Device Model	HP SureStart	Whitelisting	Intrusion Detection
HP LaserJet Enterprise MFP M527	●	●	●
HP Color LaserJet Enterprise MFP M577	●	●	●
HP LaserJet Enterprise M506	●	●	●
HP Color LaserJet Enterprise M552, M553	●	●	●
HP LaserJet Enterprise M604, M605, M606	●	●	●
HP LaserJet Enterprise 700 color MFP M775	N/A	●	●
HP LaserJet Enterprise 500 color MFP M575	N/A	●	●
HP LaserJet Enterprise 500 MFP M525	N/A	●	●
HP LaserJet Enterprise MFP M725	N/A	●	●
HP LaserJet Enterprise flow MFP M830z	N/A	●	●
HP LaserJet Enterprise M806	N/A	●	●
HP Color LaserJet Enterprise M855	N/A	●	●
HP Color LaserJet Ent. flow MFP M880	N/A	●	●
HP Officejet Enterprise Color MFP X585	N/A	●	●
HP Officejet Enterprise Color X555	N/A	●	●
HP Color LaserJet Enterprise M651	N/A	●	●
HP Color LaserJet Enterprise MFP M680	N/A	●	●
HP LaserJet Enterprise MFP M630	N/A	●	●
HP LaserJet Enterprise 700 M712	N/A	●	●
HP Color LaserJet Enterprise M750	N/A	●	●
HP LaserJet Ent 600 M601, M602, M603	N/A	●	●
HP LaserJet Enterprise 500 color M551	N/A	●	●
HP LaserJet Enterprise M4555 MFP	N/A	N/A	N/A
HP Color LaserJet CM4540 MFP	N/A	N/A	N/A
HP Color LaserJet CP5525	N/A	N/A	N/A
ScanJet Enterprise 8500	N/A	N/A	N/A

● – Feature supported

N/A – Feature not supported

4AA6-4194EEW, February 2016