



HP SURESTART, WHITELISTING & INTRUSION DETECTION SECURITY FEATURES

Troubleshooting Guide

Table of contents

Feature Operation	3
HP SureStart	3
Whitelisting.....	3
Runtime Intrusion Detection.....	3
Feature Availability	3
Upgrade/Downgrade	4
HP SureStart Capable devices	4
Non- HP SureStart Capable devices	4
Firmware downgrade instructions using the preboot menus.....	4
Control panel messages, Event log entries and Control Panel messages	5
33.05.0X SureStart Errors	5
33.05.1X Whitelisting errors.....	6
33.05.2X Intrusion detection errors	6
33.05.5X Intrusion detection errors	7
Device Syslog configuration for logging security events	9
Appendix A: Syslog message content	10
33.05.1X HP SureStart	10
33.05.2X Whitelisting	11
33.05.2X Intrusion detection.....	11
33.05.5X Intrusion detection.....	11
Appendix B: Device Support	12

Feature Operation

These security 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/exploit.

HP SureStart

HP SureStart validates the integrity of the BIOS image using a SHA-256 hash signed with HP’s digital signature. If validation fails a reserve “Golden Copy” is used to boot providing a self-healing capability.

HP SureStart is dependent on a hardware-based microcontroller and is only available on devices introducing in Spring 2015 and later. Please see [Appendix B: Device Support](#).

Whitelisting

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

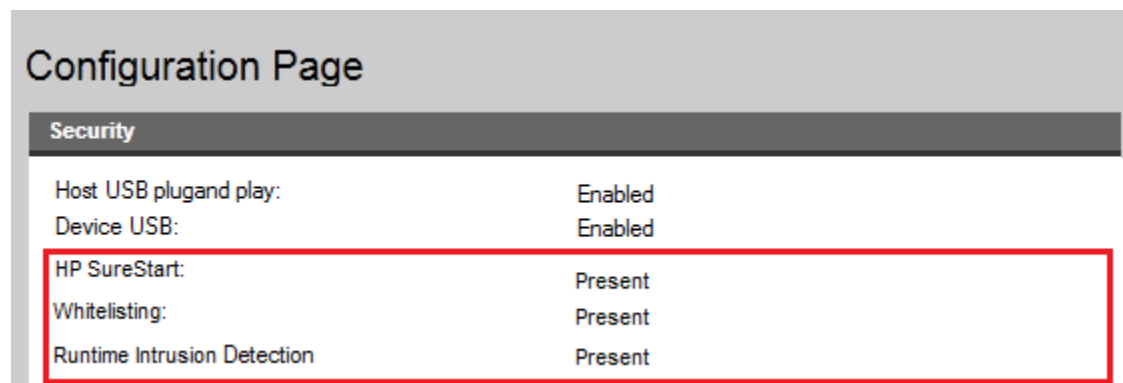
Level 1 embedded solutions digital signatures are validated using either a SHA-1 or SHA-256 hashing algorithm. If validation fails the device will either reboot or the solution may not be loaded to prevent a malware exploit.

Runtime Intrusion Detection

Intrusion Detection detects possible 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. The device will attempt to wait to reboot until pending print jobs have been cancelled.

Feature Availability

These features are available with the 23.7 firmware release and later. If present, the features are list in the device configuration page in the Security Section. For specific firmware versions see [Appendix B: Device Support](#).



The image shows a screenshot of a 'Configuration Page' with a 'Security' section. A red box highlights the status of three features: HP SureStart, Whitelisting, and Runtime Intrusion Detection, all of which are listed as 'Present'.

Security	
Host USB plugand play:	Enabled
Device USB:	Enabled
HP SureStart:	Present
Whitelisting:	Present
Runtime Intrusion Detection	Present

NOTE: HP SureStart is not supported on pre-fall 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 the [Appendix B: Device Support](#) section for a listing of HP SureStart capable devices.


Attempting to downgrade an HP SureStart capable device to non-HP SureStart firmware in 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 not have been downloaded 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

Turn the printer Off and then On, and when 1/8 displays below the HP logo on the control panel, touch the logo.

4. Scroll to select the Administrator > Download > USB Thumb-drive menu.
5. Select the firmware .bdl file from the list. Be sure to select the correct firmware for the device being updated.
6. Wait for the firmware to be transferred to the device.
7. When “Complete” is displayed, select Back twice to navigate to the top menu, and select Continue.
8. The device will reboot.
9. Verify the firmware successfully upgraded by reviewing the device Configuration Page.

Control panel messages, Event log entries and Control Panel messages

33.05.0X SureStart Errors

Description

33.05.00 Boot code corrupt (Event Log)

33.05.01 Boot code corrupt (Event Log)

33.05.02 Boot code corrupt (Event Log)

33.05.03 Boot code corrupt (Event Log)

These messages indicate that the product detected and recovered from a corrupted/tampered version of BIOS.

Recommended action

No action necessary

Description

33.05.01 Security Alert (Control Panel Message)

33.05.02 Security Alert (Control Panel Message)

33.05.03 Security Alert (Control Panel Message)

33.05.04 Upgrade corrupt (Event Log Only)

33.05.04 Security alert (Control Panel Message)

33.05.05 Boot code corrupt (Event Log Only)

33.05.05 Security alert (Control Panel Message)

33.05.06 Upgrade corrupt (Event Log Only)

33.05.06 Security alert (Control Panel Message)

33.05.07 Upgrade corrupt (Event Log Only)

33.05.07 Security alert (Control Panel Message)

These messages show the newly downloaded firmware failed to cryptographically validate the BIOS code.

Recommended action

Download a firmware bundle to the device from the preboot menu.

Description

33.05.08 Invalid boot attempt (Event Log Only)

33.05.09 Downgrade attempted (Event Log Only)

These messages show a downgrade was attempted to firmware that does not include the SureStart feature from the Ready screen.

NOTE: The device will not have downgraded when this error is seen in the event log.

Recommended action

Download a firmware bundle to the device from the preboot menu.

33.05.1X Whitelisting errors

Description

33.05.10 Firmware verification Error: XX (Event Log Only)

33.05.10 Security alert (Control Panel Message)

33.05.11 Firmware verification Error: XX (Event Log Only)

33.05.11 Security alert (Control Panel Message)

33.05.12 Firmware verification Error: XX (Event Log Only)

33.05.12 Security alert (Control Panel Message)

These messages show an error occurred with a firmware file digital signature indicating the file has been tampered with in some way or an error with the certificate used to validate the firmware signature.

Recommended action

1. Perform a Partial Clean
2. If the device does not reboot to the Ready screen, Download a firmware bundle to the device from the preboot menu

NOTE: Performing a Partial Clean is required before downloading a firmware bundle in step 2.

33.05.2X Intrusion detection errors

Descriptions

33.05.21 Potential Intrusion (Event Log Only)

33.05.21 Security alert (Control Panel Message)

This message shows the intrusion detection memory process determined an unauthorized change in system memory and may be indicative of a malware injection attack.

33.05.22 Cannot scan for potential intrusions (Control Panel Message)

33.05.22 Security alert (Control Panel Message)

This message shows the intrusion detection memory process heartbeat was not detected.

33.05.23 Intrusion detection not initialized (Control Panel Message)

33.05.23 Security alert (Control Panel Message)

33.05.24 Intrusion detection initialization error (Control Panel Message)

These messages show the intrusion detection memory process did not initialize.

Recommended action

Power cycle the device.

Note: Selecting “Continue” from the preboot menu will not resolve the error. The device must be power cycled to clear the error allowing the device to reboot to the ready screen.

Note: In firmware version 3.7 the error “A disk or boot error has occurred. Clear Error. Press Any Key” is displayed when selecting “Continue” from the preboot menu after encountering a 33.05.2X error. The message is a defect and should be ignored.

33.05.5X Intrusion detection errors

Descriptions

33.05.51 Potential Intrusion (Event Log Only)

33.05.51 Security alert (Control Panel Message)

This message shows the intrusion detection memory process determined an unauthorized change in system memory and may be indicative of a malware injection attack.

33.05.52 Cannot scan for potential intrusions (Control Panel Message)

33.05.52 Security alert (Control Panel Message)

This message shows the intrusion detection memory process heartbeat was not detected.

33.05.53 Intrusion detection not initialized (Control Panel Message)

33.05.53 Security alert (Control Panel Message)

33.05.54 Intrusion detection initialization error (Control Panel Message)

These messages show the intrusion detection memory process did not initialize.

Recommended action

Power cycle the device.

Note: Selecting “Continue” from the preboot menu will not resolve the error. The device must be power cycled to clear the error allowing the device to reboot to the ready screen.

Note: In firmware version 3.7 the error “A disk or boot error has occurred. Clear Error. Press Any Key” is displayed when selecting “Continue” from the preboot menu after encountering a 33.05.2X error. The message is a defect and should be ignored.

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.

Syslog Server Settings

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

Hop Limit/WSD	<input type="text" value="32"/>
TTL/SLP:	<input type="text" value="4"/>
Syslog Server:	<input type="text" value="<Syslog server IP Addr >"/>
Syslog Protocol	<input type="text" value="UDP"/> ▼
Syslog Port	<input type="text" value="514"/>
Syslog Maximum Messages:	<input type="text" value="100"/>
Syslog Priority:	<input type="text" value="7"/> (Use '8' to disable.)
<input checked="" type="checkbox"/> Enable CCC Logging	

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	UPD 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

Name	Description	Default Value	Recommended Value
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

33.05.1X 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"

33.05.2X Whitelisting

33.05.10

<49> printer: Code Sign error: time="2015-Sep-30 12:21:42 (UTC-07:00)" source_IP="printer_addr"s

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"

33.05.5X Intrusion detection

33.05.51

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

33.05.52

<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"

33.05.53

<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

Supported devices	HP FutureSmart firmware update	HP SureStart	Whitelisting	Run-time Intrusion Detection
HP Color LaserJet Enterprise MFP M577	TBD at release	✓	✓	✓
HP LaserJet Enterprise M506	TBD at release	✓	✓	✓
HP Color LaserJet Enterprise M552, M553	TBD at release	✓	✓	✓
HP LaserJet Enterprise M604, M605, M606	TBD at release	✓	✓	✓
HP LaserJet Enterprise 700 color MFP M775	TBD at release	∅	✓	✓
HP LaserJet Enterprise 500 color MFP M575	TBD at release	∅	✓	✓
HP LaserJet Enterprise 500 MFP M525	TBD at release	∅	✓	✓
HP LaserJet Enterprise MFP M725	TBD at release	∅	✓	✓
HP LaserJet Enterprise flow MFP M830z	TBD at release	∅	✓	✓
HP LaserJet Enterprise M806	TBD at release	∅	✓	✓
HP Color LaserJet Enterprise M855	TBD at release	∅	✓	✓
HP Color LaserJet Enterprise flow MFP M880	TBD at release	∅	✓	✓
HP Officejet Enterprise Color MFP X585	TBD at release	∅	✓	✓
HP Officejet Enterprise Color X555	TBD at release	∅	✓	✓
HP Color LaserJet Enterprise M651	TBD at release	∅	✓	✓
HP Color LaserJet Enterprise MFP M680	TBD at release	∅	✓	✓
HP LaserJet Enterprise MFP M630	TBD at release	∅	✓	✓
HP LaserJet Enterprise 700 M712	TBD at release	∅	✓	✓
HP Color LaserJet Enterprise M750	TBD at release	∅	✓	✓
HP LaserJet Ent 600 M601, M602, and M603	TBD at release	∅	✓	✓
HP LaserJet Enterprise 500 color M551	TBD at release	∅	✓	✓

hp.com/go/support

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

© Copyright 2021 HP Development Company, L.P. 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.

c04863614ENWW, Created on August 2015

