Technical Whitepaper

HP Sure Start

Automatic Firmware Intrusion Detection and Repair System

May 2016
902696-002

Contents

List of figures

List of tables

1 Introduction

HP Sure Start is the industry leader in a chipset and processor independent, firmware intrusion detection and automatic repair system. HP Sure Start provides a robust level of cyber-resiliency unique to HP platforms, while conforming to NIST 800-147 and 800-155 guidelines.

HP Sure Start provides the following capabilities:

- HP Core Platform Firmware authenticity enforcement and tamper protection

  HP Sure Start Hardware enforcement of the system booting only authentic and un-modified HP firmware and HP BIOS

- Firmware Health Monitoring & Compliance

  Logging of firmware health related events via isolated HP Sure Start hardware auditing exposes platform firmware state along with any anomalies that could be indicative of thwarted attacks.

- Self-healing

  Automatic repair of HP BIOS and HP firmware corruption using a hardware isolated backup copy of HP BIOS and HP firmware

Together, the above capabilities provide the following benefits to platform owners and administrators:

- Uninterrupted productivity

  HP Sure Start maintains business continuity in the event of an attack or accidental corruption in that there is no downtime waiting for IT/Service event

- Lower cost

  HP Sure Start's ability to recovery automatically reduces calls to IT Help Desk and enhances productivity which ultimately helps lower the maintenance cost for the platform

Regardless of the source of corruption, HP Sure Start automatically repairs the firmware / BIOS.

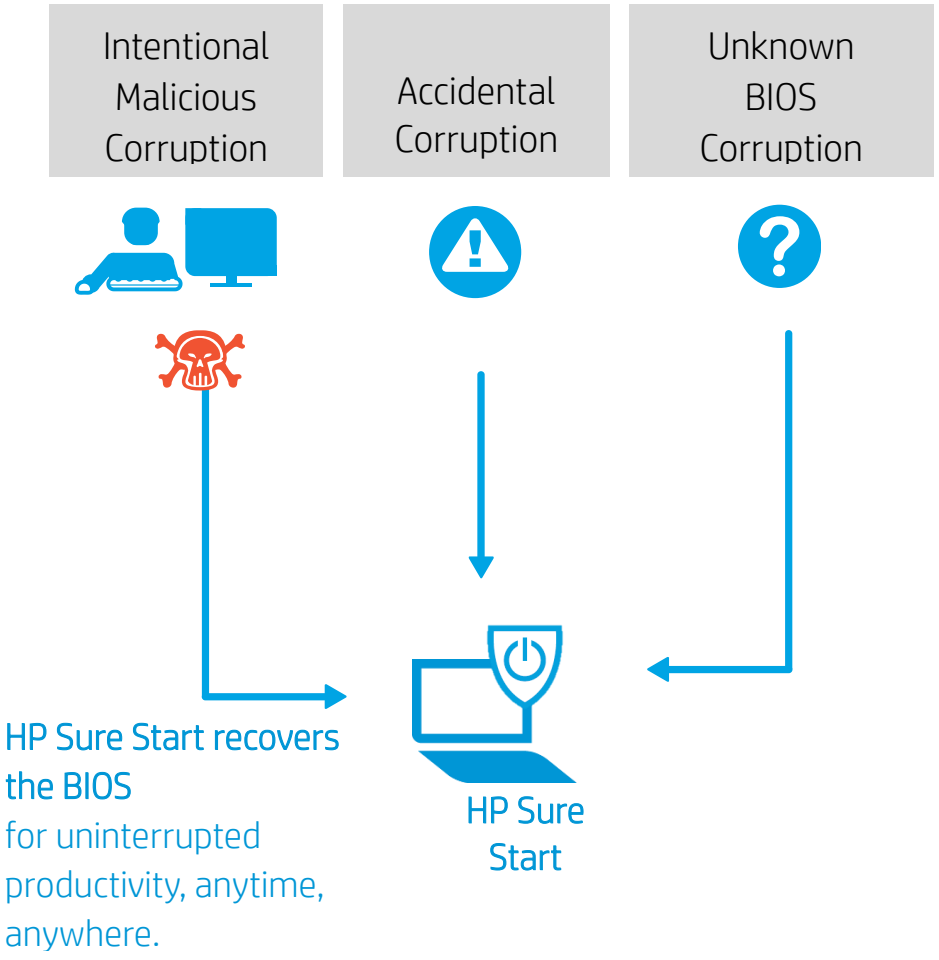

Figure 1 Possible sources of firmware corruption

1.1 Enhancements for 2015

HP introduced Sure Start in 2013. Since that time, HP has enhanced Sure Start and expanded the number of products that use Sure Start. HP is pleased to provide the 2nd Generation of Sure Start across the entire 2015 Elite product lineup, including Tablets, Notebooks, Desktops, and All in Ones (AIO's).

Significant enhancements include the following:

- **Windows Event Viewer Support.** The Windows Event Viewer now includes HP Sure Start events to provide enhanced visibility to the local user as well as remote management tools.
- **Dynamic Protection.**[1] Independent of the host CPU and main memory dedicated to the user Operating System, Sure Start hardware periodically checks the integrity of the HP firmware and HP BIOS boot images stored in the non-volatile (flash) memory even while the OS is running. Dynamic Protection provides an early warning of an attack to the boot image.

[1] HP Sure Start with Dynamic Protection supported on select Intel® based 800 G3 series commercial notebooks and 800 G2 series commercial desktops, retail systems, and on 2015 HP Elite products with Intel(R) 6th generation processors and higher

2 Sure Start-supported models

2.1 Notebook platforms supported

Table 1 Notebooks supporting HP Sure Start

Model	2013	2014	2015
HP EliteBook Folio 9480m		x	
HP EliteBook Folio 1040		G2	G3
HP EliteBook Folio 1020		G1	
HP ZBook 17	G1	G2	G3
HP ZBook 15	G1	G2	G3
HP ZBook 14	G1	G2	
HP ZBook 15u		G2	G3
HP EliteBook 850	G1	G2	G3
HP EliteBook 840	G1	G2	G3
HP EliteBook 820	G1	G2	G3
HP EliteBook 755		G2	G3
HP EliteBook 745		G2	G3
HP EliteBook 725		G2	G3
HP EliteFolio 940	G1		
HP EliteBook Folio			G1
HP EliteBook Revolve 810			G3
HP Elite x2		1011	1012
HP Pro x2 612			G1

2.2 Desktop platforms supported

Table 2 Desktop platforms supporting HP Sure Start

Platform	Model(s)	2015
HP EliteDesk	800 TWR	G2
HP EliteDesk	880 TWR	G2
HP EliteDesk	800 SFF	G2
HP EliteDesk	800 DM (35W)	G2
HP EliteDesk	800 DM (65W)	G2
HP EliteOne	800 AiO 23 T & NT (GPU down)	G2
HP EliteOne	800 AiO 23 T	G2
HP EliteOne	800 AiO 23 NT	G2
HP EliteDesk	705 MT	G2
HP EliteDesk	705 SFF	G2
HP EliteDesk	705 DM	G2
HP EliteOne	705 AiO 23 T (23 NT dropped)	G2
HP Collaboration PC		G2
Retail System	HP RP9	G1
Retail System	HP MP9	G2

3 Architectural Overview & Capabilities

HP Sure Start consists of two major architectural components:

- **HP Sure Start Embedded Controller** consisting of HP unique hardware and firmware
- **HP Sure Start BIOS** working in conjunction with the HP Sure Start Embedded Controller

3.1 HP Sure Start Embedded Controller

The Sure Start Embedded Controller is the first device in the system to execute firmware when the system powers up, active well before the system boots. The Sure Start Embedded Controller's activities include, but are not limited to, monitoring the system power button and power sequencing the start of the host CPU execution when the user presses the power button.

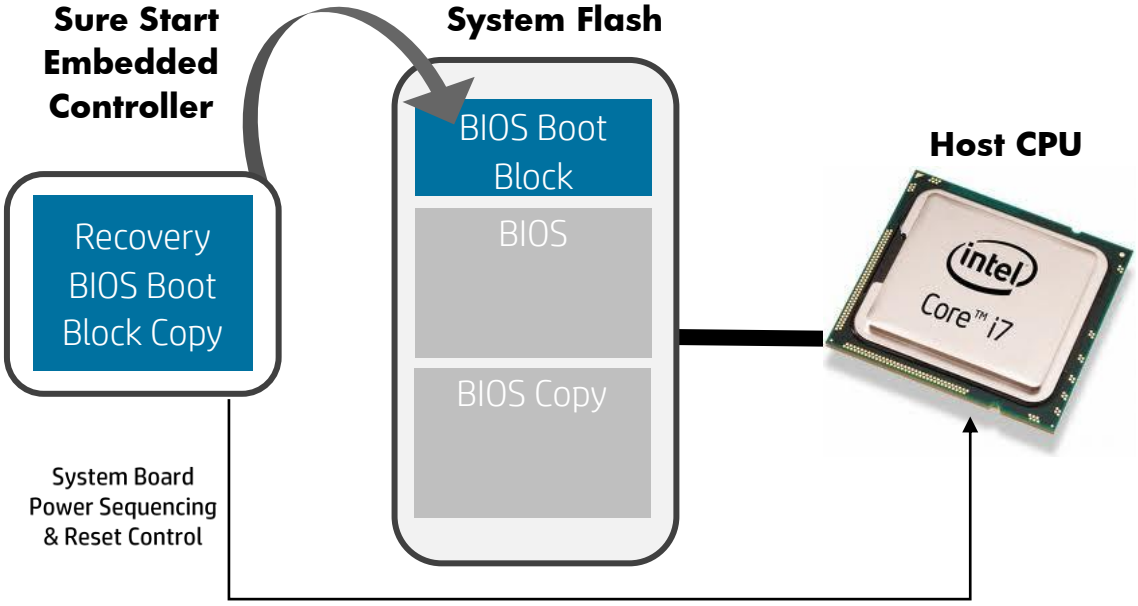

Figure 2 Firmware Integrity Verification Process

When power is first applied to the platform (before the system is turned on), the HP Sure Start Embedded Controller validates that its own firmware is authentic HP code before loading and executing the code. The Sure Start Embedded Controller hardware uses industry standard, strong cryptographic methods to perform the integrity verification. The method employs a 2048 bit HP RSA Public key contained within internal permanent read only memory. Therefore, the Sure Start Embedded Controller is the built-in hardware based Root of Trust (RoT) for the platform, used to validate its firmware and the HP BIOS before they are executed. This hardware Root of Trust protects against firmware replacement attacks regardless of their deployment method and serves as the foundation upon which all platform security is built.

Figure 2 illustrates the firmware integrity verification process. Once the HP Sure Start Embedded Controller authenticates and starts executing the HP Sure Start firmware, that firmware uses the same strong cryptographic operations to verify the integrity of the System Flash BIOS Boot Block. If a single bit is invalid, the HP Sure Start Embedded Controller replaces the System Flash contents with its own copy of the HP BIOS Boot Block that is stored within an isolated Non-Volatile Memory (NVM) dedicated to the Sure Start Embedded Controller.

The HP Sure Start design ensures that all the firmware and BIOS code running on both the HP Sure Start Embedded Controller and the Host CPU is the code HP intended to be on the device.

NOTE:
The System Flash Boot Block integrity checking and any needed recovery performed by the Embedded Controller takes place while the Host CPU is off. Therefore, from a user point of view, the entire operation takes place when the system is still off, in sleep mode, or hibernate mode.

The System Flash BIOS Boot Block is the foundation of the HP BIOS. HP Sure Start hardware guarantees that the BIOS Boot Block is the first code that the CPU executes after a reset. Once the Sure Start Embedded Controller determines that the BIOS Boot Block contains authentic HP code, it allows the system to boot as it normally would.

3.2 HP BIOS

An enhanced adaptation of HP BIOS Protection is one of the ingredients of HP Sure Start contained within the HP BIOS Boot Block. This enhancement provides NIST 800-147 conformant HP Boot Block code with the ability to use industry standard strong cryptographic methods to verify integrity of the remainder of the BIOS before passing execution control to it. In addition, the code has the ability to securely recover all pieces of the BIOS required for proper operation from a variety of sources. These sources include backups within the System Flash, Hard Drive, or USB key. Figure 3 illustrates the simplified system architecture and depicts the HP Sure Start capabilities built in the HP Boot Block code that executes on the Host CPU.

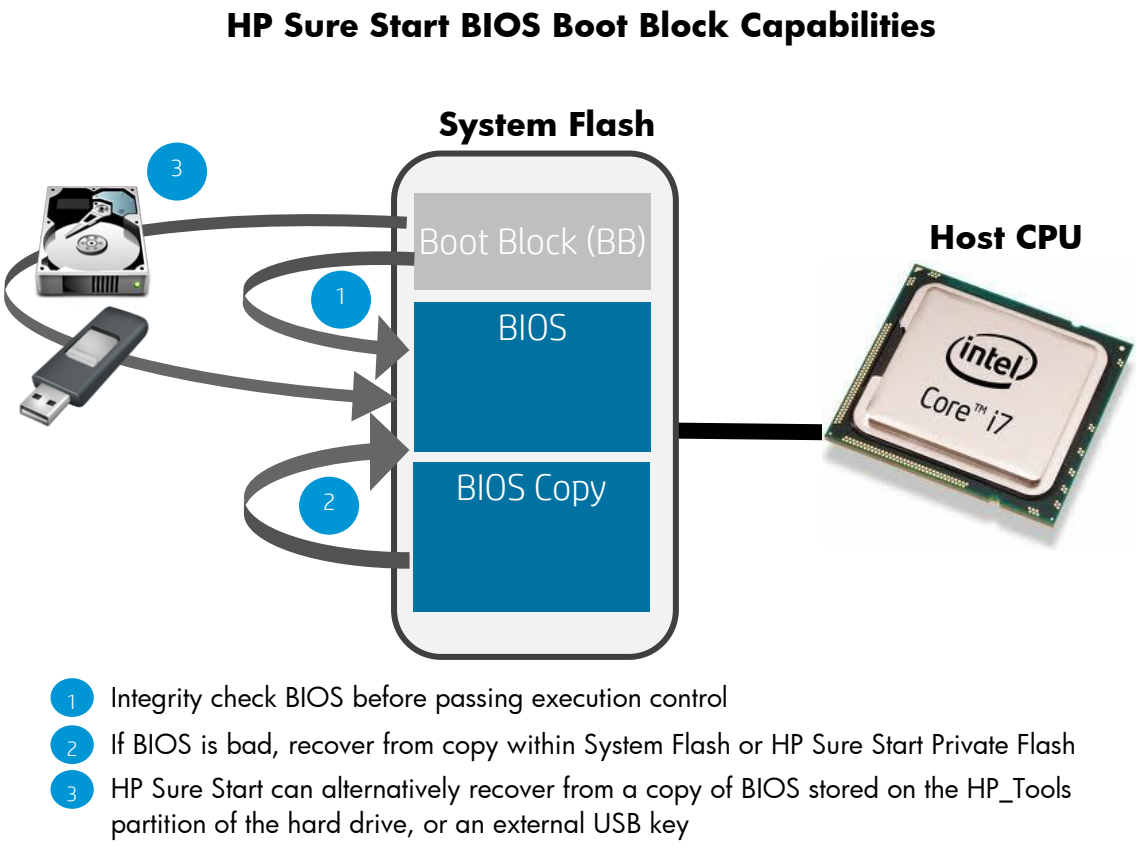

Figure 3 HP Sure Start BIOS Boot Block Capabilities

NOTE:
For added redundancy, the HP BIOS Boot Block code is able to recover from a recovery image available on the HP_TOOLS partition (included as part of the default shipping configuration) or a recovery image on a USB thumb drive. While not strictly required for HP Sure Start, the same HP BIOS Block code is leveraged for non – HP Sure Start platforms where this capability is crucial.

The HP Sure Start Embedded Controller will also check the integrity of the System Flash Boot Block code each time the system is turned off, put into a Hibernate, or Sleep mode. Since the CPU is powered off in each of these states and the CPU is therefore required to re-execute BIOS Boot Block code to resume, it is crucial to re-verify the integrity of the BIOS Boot Block each time to check for tampering. Additionally, starting in Intel 6th generation processor platforms, Sure Start with Dynamic Protection will periodically (every 15 minutes) check the integrity of the System Flash BIOS Boot Block while the system is running.

3.3 Machine Unique Data Integrity

The HP Sure Start Embedded Controller and BIOS work together to provide advanced protection of factory configured critical variables unique to each machine that are intended to be constant over the life of any specific platform. A backup copy of this variable data is saved in the HP Sure Start Embedded Controller Non-Volatile Memory store while in the factory environment that is then made available to the HP Sure Start BIOS component on a read only basis to perform integrity checking of the data on every boot. If any setting in the Shared Flash has changed versus the factory settings, the HP Sure Start BIOS components will automatically restore the data in the System Flash from the backup copy provided by the Sure Start Embedded Controller.

3.4 Descriptor Region

For HP Intel models, HP Sure Start protects the Descriptor Region of the System Flash. Unique to Intel architecture, the descriptor region contains critical configuration parameters that are sampled by the Intel core logic at reset and used thereafter to configure the core logic. The descriptor region also includes partitioning information for the system flash that is used by the Intel core logic to determine where the BIOS region resides within the flash and therefore where there CPU will start fetching code for execution from reset. HP Sure Start will monitor the integrity of this region and recover it to the intended configuration in the event of tampering or corruption.

3.5 Network controller Protection

In addition, for HP Intel models, HP Sure Start protects the network controller (NIC) settings contained with the System Flash. Some HP customers have use cases that require legitimate changes to factory configured NIC settings. Therefore, HP Sure Start does not prevent changes to NIC settings by default. Instead, HP Sure Start provides a feature that, when enabled, warns the user that NIC settings changed. In addition, HP Sure Start provides a method to restore the NIC settings to factory values. Some of the protected settings are the following: the MAC address, the Pre-boot Execution Environment (PXE) settings, and the remote Initial program load (RPL). This restoration is possible via a read-only backup copy provided by the Sure Start Embedded Controller.

3.6 HP Sure Start Event Logging

The HP Sure Start Embedded Controller records critical events related to HP Sure Start monitored firmware/BIOS code and data. These events are stored within the Sure Start Non-Volatile Memory Store. These events will be copied from the Sure Start Embedded Controller to the Windows Event Viewer when HP Notifications Software in installed in order to facilitate access to these events by the local user as well as the customers' preferred manageability agent.

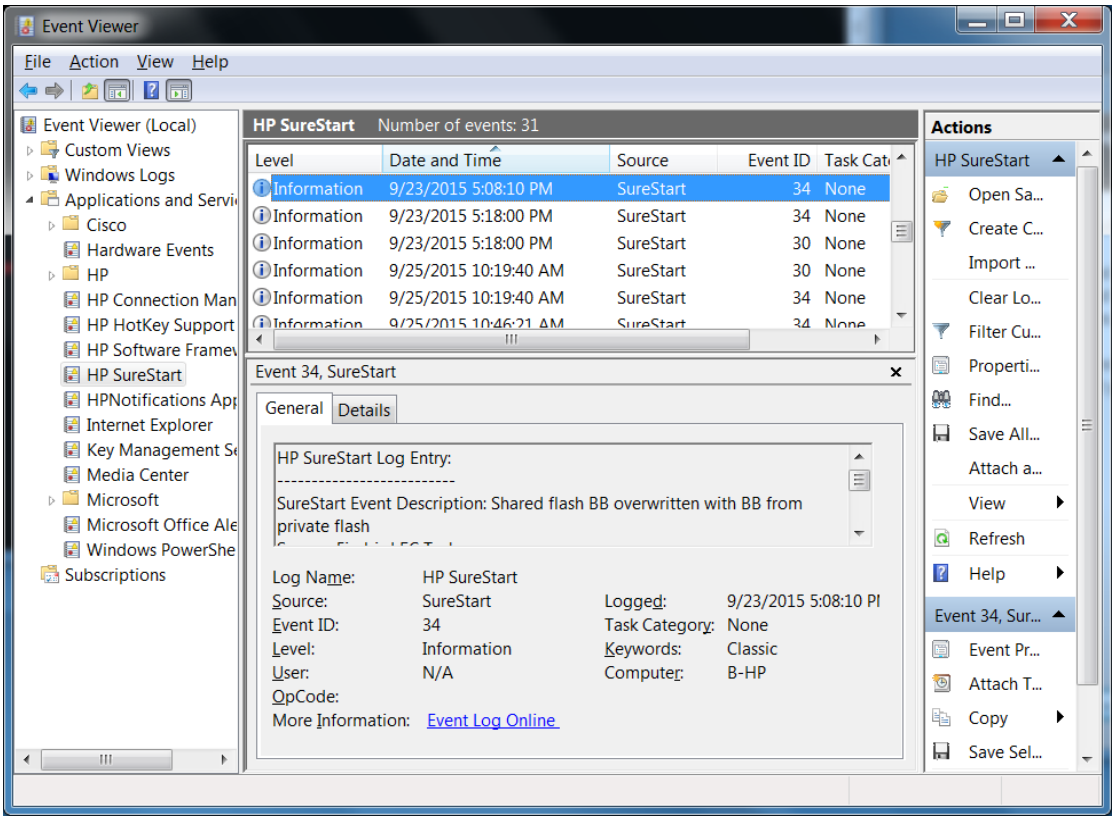

Figure 4 Windows Event Viewer showing Sure Start events

The following events will trigger the HP Notifications Software to gather all event from the Sure Start subsystem and ensure that the Windows Event Viewer is updated with any events that are not already recorded there:

- Windows Boot
- Windows Resume from Sleep / Hibernate
- Sure Start with Dynamic protection runtime event notifications

HP Notifications Software will populate the HP Sure Start events into a unique “HP Sure Start” application event log versus the general Windows Event Viewer. Only HP Sure Start events will be included in this log. The Windows Event Viewer path to the HP Sure Start events is the following: System Tools/ Event Viewer/ Applications and Services Logs / HP Sure Start

The Windows Event Viewer level categories related to HP Sure Start event are defined in Table 3.

The events will be populated into Windows Event Viewer in the order that they were generated by HP Sure Start. The oldest event in the HP Sure Start subsystem will be added to the Windows Event Viewer first and the more recent event shall be added last.

The timestamp for each Windows Event Viewer entry will be the time it was added to that log, NOT the time the event actually occurred. Each Sure Start Windows Event Viewer entry will include detailed data within the event details, which includes the timestamp of the actual occurrence.

NOTE:
Events are persistent in the HP Sure Start system even after being copied to the Windows Event Viewer. In the event that the Windows Event Viewer is cleared, the HP Notifications Software application will replace all HP Sure Start entries on the next event that triggers it to check for HP Sure Start event logs.

Types of HP Sure Start Windows Event Viewer events include:

Table 3 Windows Event Viewer level categories

Event Level	Definition
Info	Events that are expected to occur during the normal course of operation (e.g., updating the BIOS).
Warning	Unexpected events that have occurred but were fully recovered from by Sure Start and there is no user/admin action required for the platform to be fully operational. These events are anomalous operation that the user/admin may want to investigate further, especially if there is a trend of these events across multiple machines.
Error	Events that requires the admin/HP service to take action on the platforms to fully recover

Specific examples of HP Sure Start events include:

Table 4 Windows event ID's, levels, and messages

EVENT ID	Windows Event Level	Message
30	Warning	Sure Start found the primary BIOS in shared flash memory is either corrupted or missing. Possible causes include but not limited to interrupted BIOS update or recent BIOS attack.
31	Warning	Sure Start found the backup BIOS is either corrupted or missing. Possible causes include but not limited to interrupted BIOS update.
32	Warning	Sure Start found shared flash memory layout is different from original factory settings.
34	Information	Sure Start has recovered the primary BIOS in shared flash memory
35	Information	Sure Start has updated the backup copy of BIOS
36	Warning	Sure Start found shared flash memory layout is different from original factory settings and has repaired the shared flash layout.
38	Warning	Sure Start found that the primary BIOS in shared flash memory on resume from Sleep is different than what system originally booted with
40	Error	Sure Start found that the "BIOS Update Policy" setting was set to Locked but was unable to honor policy as backup copy of BIOS may be corrupted or missing.
43	Error	Sure Start integrity checking on backup copy of critical factory configured parameters failed and is no longer being used
44	Error	Sure Start integrity checking on backup copy of critical network parameters data failed and is no longer being used.
45	Error	Sure Start integrity checking on backup copy of shared memory layout descriptor failed and is no longer being used.
46	Warning	Sure Start has found that there was an issue with logging, some logging data may have been lost.
47	Error	Sure Start policy settings have been corrupted and reverted to factory defaults.
48	Warning	System was placed in manufacturing programming mode.
49	Informational	System was taken out of manufacturing programming mode.
50	Informational	Sure Start found that backup and primary copy of BIOS do not match.

3.7 HP Sure Start Policy Controls

Out of the box, the HP system BIOS enables and optimizes HP Sure Start policies for the typical user. Since HP Sure Start is enabled by default, there is no need for the typical user to modify the settings to be protected by HP Sure Start. For advanced users, the system BIOS provides some control of Sure Start behavior, using policy settings in the (F10) BIOS Setup. Unless otherwise noted, these settings and functions are located under "Security->BIOS Sure Start"

NOTE:
Policies are stored within the HP Sure Start Embedded Controller Non-Volatile Memory that is not directly accessible by the Host CPU; therefore, a reboot is required before any Sure Start settings take effect.

The following Sure Start settings & functions are available:

- Verify Boot Block on Every Boot
- BIOS Data Recovery Policy
- Prompt on Network Controller Configuration Change
- Restore Network Controller Configuration to the factory defaults
- Lock BIOS Version

Verify Boot Block On Every Boot
HP Sure Start always verifies the integrity of the System Flash BIOS Boot Block before resuming from Sleep, Hibernate or Power-off. When set to **enable**, this setting has HP Sure Start also verify the integrity of the boot block on each warm boot (Windows restart.) The trade-off to consider is faster restart time versus more security. The default setting of this feature is **disable**.

BIOS Data Recovery Policy
When set to **Automatic**, HP Sure Start automatically repair the BIOS or the Machine Unique Data when necessary. When set to **Manual**, HP Sure Start requires a special key sequence to proceed with the repair. In the case of an issue with the Boot block code, the system will refuse to boot and a unique blink sequence will flash on system LED. In the case of an issue with the Machine Unique Data, the system will display a message on the screen. The key sequence required and the blink sequence displayed vary depending on the system being a notebook, a desktop or a tablet. See the table below for details. Manual mode is useful to users that have the ability to perform forensics on the system flash contents before repair. Typical users are not encouraged to use manual mode. The default setting of this feature is **Automatic**.

Prompt on Network Controller Configuration Change
This setting is available on Intel systems only. HP provides a factory defined network controller configuration which includes the MAC address. When this setting is set to **enable**, the system will monitor the state of the network controller configuration and prompt the user in the event of a change from the factory configured state. The default setting of this feature is **disable**.

Restore Network Controller Configuration to the factory defaults
This restores network controller configuration stored in System Flash to factory defaults. Unlike other machine unique data, HP Sure Start does not validate and protect network controller configuration on each boot, nor does it automatically repair this parameter region, because there are valid reasons for changing network controller configuration such as the MAC address. This feature is useful for recovering the network controller from an unknown state that may be unreliable.

Lock BIOS Version
In the (F10) BIOS setup, this feature is located in Main->Update System BIOS.

When set to **disable**, update the BIOS using any supported process. When the Sure Start Embedded Controller detects a valid Boot Block update in the System Flash, it will update the backup copy of the Boot Block.

When set to **enable**, all HP BIOS update tools refuse to update the BIOS. In addition, HP Sure Start protects the BIOS from attempts to change the BIOS version by removing the system flash via an un-authorized method. The Sure Start Embedded Controller records the locked down version of BIOS. When the Sure Start Embedded Controller detects that the BIOS in the system flash changed, the Embedded Controller will overwrite the BIOS Boot Block with the Embedded Controller copy of

the Boot Block. The Embedded Controller copy of the Boot Block executes and recovers the remainder of the correct version of the BIOS. The default setting of this feature is **disable**.

3.8 Remote Management of HP Sure Start Policy Controls

Out of the box, HP Sure Start policies are optimized for the typical user. Since HP Sure Start is enabled by default, there is no need for the remote administrator take any action to enable (or "deploy") HP Sure Start. In the event a remote administrator has a desire to modify HP Sure Start policy settings, the same Windows Management Instrumentation (WMI) API's or HP BIOS Configuration Utility scripts that are used to Manage other platform BIOS policies can be used to manage HP Sure Start Policies.

Remote visibility of HP Sure Start events is via the Windows Event Viewer. This approach provides the flexibility for the customer to use their existing and preferred management agent/console to access the events using existing mechanisms across all versions of Windows.

4 HP Sure Start user experience

Customers see no noticeable experience degradation when HP Sure Start operates. Recovery operations are automatic using the default settings, with no end-user interaction or IT involvement for the recovery to occur in the case of HP Sure Start identifying a problem. Additionally, HP Sure Start is enabled “Out of the Box”, so there is no need for a customer to set up or configure the platform to take advantage of the feature!

4.1 Specific to the HP Sure Start Embedded Controller

HP Sure Start hardware is active from the moment power is applied to the system. Since the system is in the Off state at this point and it is not possible to display messages to the user, the HP Sure Start Embedded Controller uses one of the mechanisms defined in Table 6 to indicate HP Sure Start activity.

In a normal scenario where HP Sure Start examines the System Flash code and data that it monitors and finds no issues, the HP Sure Start activity indicator will only be active for a few seconds. In a scenario where HP Sure Start finds an integrity issue with any of the code or data monitored by Sure Start (and the recovery policy is set to the default; Automatic), the activity indicator will be active for approximately 10-20 seconds indicating HP Sure Start is making repairs.

As soon as HP Sure Start activity is complete, the system is ready to be powered up by the user. Attempts to power up the system while Sure Start is active will be ignored.

As previously mentioned, the HP Sure Start Embedded Controller will also check the integrity of the code and data monitored by Sure Start each time the system is turned Off, put into a Hibernate, or Sleep mode. If the Sure Start activity indicator is watched closely, the user will notice the HP Sure Start activity indication for a few seconds upon entry into those states which indicates that the code and data monitored by Sure Start was successfully verified.

The Sure Start Embedded Controller will update the recovery BIOS Boot Block image in the Sure Start Embedded Controller Non-Volatile Memory store to match the copy in the System Flash in the cases a valid update is detected. In this scenario, the user will perform a normal BIOS update which includes progress status displayed on the system display. To complete the final steps of the update, the system will reboot and the HP Sure Start activity indicator will be displayed for approximately 10-20 seconds as the HP Sure Start Embedded Controller first validates the update and then replaces the BIOS Boot Block recovery copy in the Sure Start Embedded Controller Non-Volatile Memory store.

NOTE:
BIOS Boot Block code will not always be updated as part of a BIOS update. In practice, the BIOS Boot Block code is rarely changed in production platforms and therefore the majority of BIOS updates do not update the BIOS Boot Block code.

In the event HP Sure Start Embedded Controller finds a problem with the contents of BIOS Boot Block in the System Flash, the user experience would be much the same as the “Update” scenario described above. In this case, the HP Sure Start Embedded Controller is replacing the BIOS Boot Block in System Flash with the backup copy in the Sure Start Embedded Controller Non-Volatile Memory Store.

This will happen automatically with the default setting, but there is a policy option to modify HP Sure Start Embedded Controller Firmware behavior such that it waits for end user input before repairing the Boot Block portion of the System Flash (Manual Recovery). With this policy option set, the HP Sure Start Embedded Controller firmware will halt the system and wait for the recovery sequence action from the local user. In a scenario where the recovery policy has been changed to Manual and the System Flash Boot Block is compromised, the system will refuse to power up and the user will see the “BIOS Manual Recovery Required” indication as shown in table 6 until the local user takes the “BIOS Manual Recovery Sequence” action shown in Table 7.

NOTE:
Manual Recovery Mode is only intended for scenarios where the machine owner would prefer to perform forensics on the system flash contents before it is repaired and is not recommended for the typical user. In the case of the HP Sure Start Embedded Controller finding an issue with the Boot Block code, the system will refuse to boot and flash a special LED sequence until the special key sequence is input by the local user.

Table 5 HP Sure Start Indicators

Description	Notebook	Tablet w/o keyboard attached (Elite x2)	Desktop
HP Sure Start Active	Pulsating White/Amber Battery charging LED	Pulsating White/Amber Battery charging LED	Major/Minor Power LED blink code = 2/4 (Only during recovery operations)
BIOS Manual Recovery Required Indication	CapsLock + Numlock LED blinks 8 times	Battery charge indicator LED blinks 8 times	Major/Minor Power LED blink code = 2/3
Machine Unique Data Manual Recovery Required	POST on screen warning Message.	POST on screen warning Message.	POST on screen warning Message.

Table 6 HP Sure Start Manual Recovery key sequences

Description	Traditional Notebook	Tablet w/o keyboard attached (Elite x2)	Desktop
BIOS Manual Recovery Sequence	Up Arrow+Down Arrow+ Esc	Volume Down button	Press Power Button twice within 2 seconds
Machine Unique Data Manual Recovery Sequence	Up Arrow+ Down Arrow+Esc	Volume Down button + Rotate button	Up Arrow+ Down Arrow+Esc

The following process is used to interpret the Major/Minor blink codes for desktop computers:

- Power Button red LED turns on for 0.6 seconds / off for 0.6 seconds the number of times corresponding to Major number
- 1 second pause
- Power Button white LED turns on for 0.2 seconds / off for 0.2 seconds the number of times corresponding to Minor number
- 2 second pause, then repeat from the beginning

4.2 Boot Messages

HP Sure Start will display a warning message to the user on the next boot after any significant event is detected or action is taken. However, with default settings under normal operating conditions, HP Sure Start is invisible to the user, even though it is performing the integrity checks on every power state change and while the OS is running (in the case of Dynamic Protection) .

4.3 Dynamic Protection Runtime Messages

HP Sure Start will display notifications to the end user in the event of a BIOS integrity problem detected while the operating system was running. Normally, HP Sure Strat will repair this issue automatically in the background. If the event that HP Sure Start is unable to repair the problem while the system is running, a notification will be displayed prompting the user to shut down to enable HP Sure Start to repair the issue. Under normal operating conditions, the user will never see these messages.

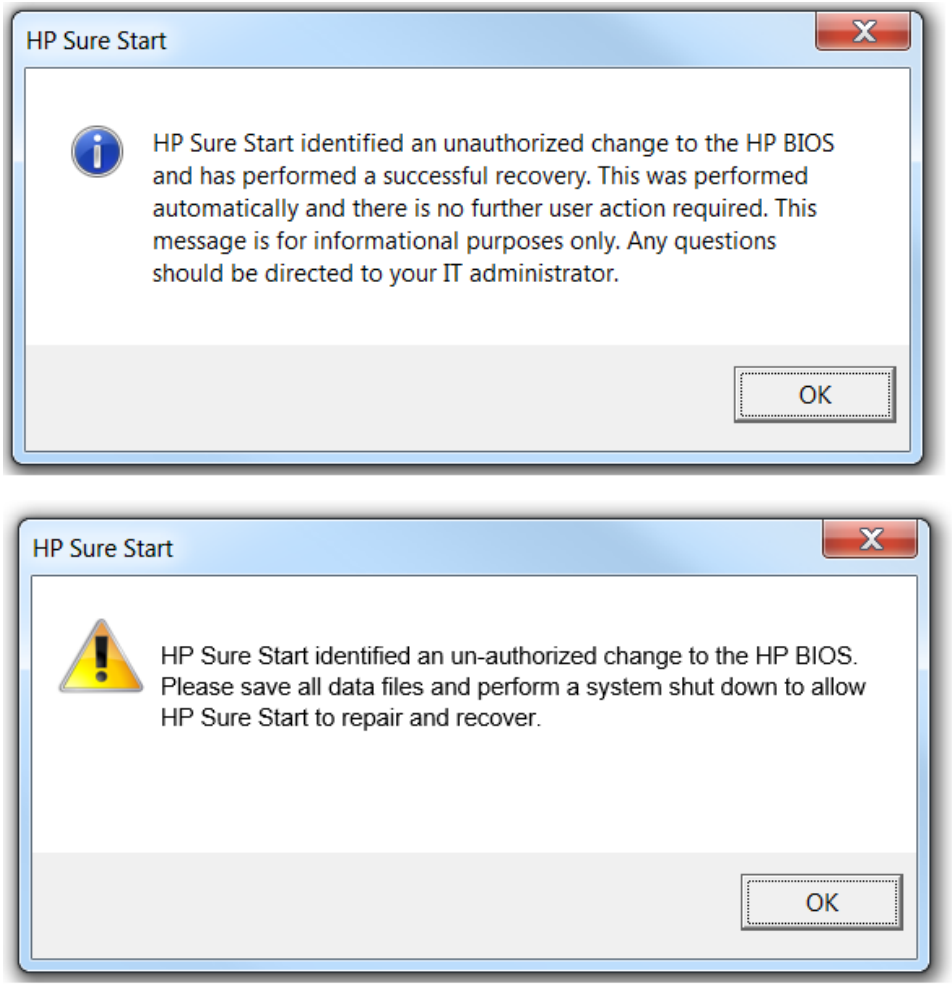

Figure 5 Dynamic Protection runtime messages