HP Sure Recover

A comprehensive, flexible recovery solution for HP Elite computers

Minimize downtime via an automated operating system recovery solution integrated into HP computer hardware and firmware. HP Sure Recover enables you to quickly recover the operating system whenever needed, throughout the lifecycle of the computer. HP Sure Recover succeeds even if the primary drive has been completely erased.

HP SURE RECOVER REQUIREMENTS

HP Sure Recover is available on HP Elite computers with 8th generation Intel® or AMD processors and requires an open, wired network connection.

HP Sure Recover with Embedded Reimaging is available on select HP Elite computers with 8th generation Intel processors.

You must back up important files, data, photos, videos, etc. before using either version of HP Sure Recover to avoid loss of data.

Not available on computers with multiple internal storage drives or Intel Optane™.

The need for cyber-resilient computers

Cyberattacks continue to grow at an incredible pace. Reports of cybersecurity breaches have become commonplace, even impacting companies that deploy state-of-the-art defenses. Defenses against these types of attacks are an absolute necessity, but given the increasing sophistication of the attackers and the growing number of breaches, additional strategies are needed.

Cyber-resilience is an emerging strategy that is rapidly gaining acceptance in business and the public sector. Cyber-resilience is defined as the ability to prepare for and adapt to changing conditions in order to recover rapidly from disruptions to IT systems or critical infrastructure. One of the core principles of cyber-resilience is to recognize up front that hackers may launch a successful attack against you. Cyber-resilient systems are designed to include mechanisms to enable rapid recovery to a working and secure state after such an attack.

A cyber-resilient computer is designed to quickly and automatically recover itself to a working state, even from unforeseen attacks that bypass existing protections and inject malicious software and/or firmware into the target platform.

This kind of attack may also attempt to render the computer inoperable by removing or corrupting software and/or firmware on the device. To thwart such attempts by malware, the ideal solution must be designed to function independently of the operating system and of any software stored on the mass storage device.

Beyond attack responses, cyber-resilient computers can also optimize standard processes that can be pain points for IT administrators and individual users. The operating system may need to be restored for reasons other than malware or corruption—such as initial system installations, or to reset the system drive before a device is re-provisioned for another user. In a public environment—for example, a hotel or grocery store—the administrator may want to schedule regular reimaging of all devices to help keep the OS image in a clean state.

In all these examples, manually restoring the OS can be a time-intensive process. An automatic, easy-to-use recovery process can save time for administrators of large fleets of computers. And for the end user, a straightforward, quick and reliable mechanism to recover or reset the operating system can be the difference between a momentary outage or days of downtime.

4AA7-4556ENW, October 2018

HP Sure Recover

HP Sure Recover helps make computers cyber-resilient

HP Sure Recover is a PC OS recovery solution built into the hardware and firmware that can fully recover the HP OS image without requiring that recovery software be present on the machine. HP Sure Recover supports recovery using a network connection. Some devices have additional embedded storage on the motherboard to support recovery in an offline state (not connected to a network). This configuration is called HP Sure Recover with Embedded Reimaging. The embedded storage is unique from other technologies in that it is hardware-isolated from the host operating system to disallow unauthorized change.

HP Sure Recover is enabled by default and can be started manually by pressing the F11 key at boot, or it can be configured to trigger automatically. HP Sure Recover is configured by default to restore from Windows® 10 image and device driver repositories that are hosted by HP and accessible via the public Internet. During the recovery process, HP Sure Recover utilizes strong public key cryptography to verify both the identity of the recovery image's provider and the integrity of the images themselves.

HP Sure Recover with Embedded Reimaging benefits the local user with a shorter recovery time, since there is a local copy of the Windows 10 image and device driver already on the computer. This shortens the recovery process by removing the need to first download the image from the network. Additionally, local users benefits by having recovery capability when they are in a location without a wired connection to the public Internet. HP recommends not distributing secrets within custom images, as HP currently does not offer the capability to securely erase the contents of the local embedded storage device.

HP Sure Recover with Embedded Reimaging also utilizes strong public key cryptography to verify the integrity of the image on the local embedded storage device. HP Sure Recover with Embedded Reimaging can be configured to determine if there is a newer version of the image online and refresh the local image.

Alternatively, HP Sure Recover can be configured to use custom images hosted on an internal private network or the public Internet. Additionally, the HP Sure Recover configuration can be managed either locally or remotely, with the HP Sure Recover configuration for each computer protected in the isolated, non-volatile memory of the HP Endpoint Security Controller hardware.

HP Sure Recover can be used by an administrator or the user to easily restore the system to the desired state, quickly installing the latest version of the operating system, platform-specific device drivers, and (in the case of a custom image) software applications.

All HP computers that support HP Sure Recover also support HP Sure Start, HP's industry-leading firmware security-and-resiliency solution that meets or exceeds the National Institute of Standards Technology (NIST) Platform Firmware Resiliency guidelines (Special Publication 800-193). Building on the resilient firmware foundation provided by HP Sure Start, HP computers with HP Sure Recover for the OS are extremely cyber-resilient.

Regardless of whether you want to perform custom operating system installations, recover from destructive malware, reset the system drive to the desired state prior to computer redeployment, or automatically re-image on a regular schedule, HP's cyber-resilient computers with HP Sure Recover are the right solution.

4AA7-4556ENW, October 2018

HP Sure Recover

When an image recovery is triggered, the HP Sure Recover policies stored in the HP Endpoint Security Controller are deployed through the BIOS to download the recovery image from the proper repository and install it on the system hard drive.

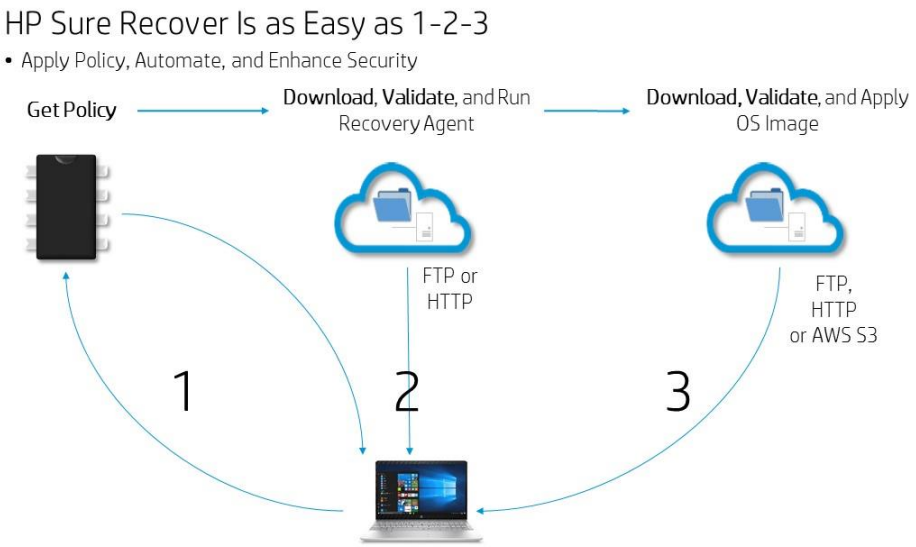

Figure 1: Image recovery process (with download)

Alternatively, when an image recovery is triggered with Embedded Reimaging in use, the HP Sure Recover policies stored in the HP Endpoint Security Controller are deployed through the BIOS to install it the recovery image on the system hard drive from its onboard repository.

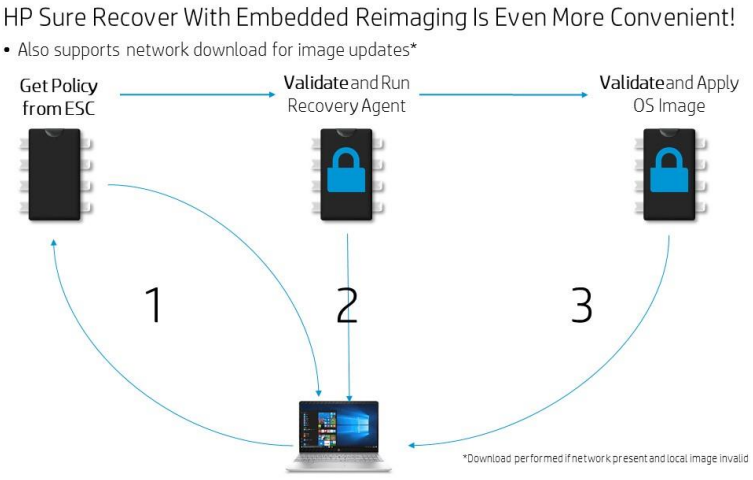

Figure 2: Image recovery process (with embedded reimaging)

Flexible and customizable management

HP Sure Recover can be started manually by an end user, or it can be configured to trigger automatically:

- When no OS is found on the hard drive
- When Sure Run determines that the platform is out of compliance
- On a schedule

HP Sure Recover

HP Sure Recover is enabled by default but can be disabled by the local user via F10 setup or the HP Client Security Manager Software that is pre-installed in the HP image. HP Client Security Manager can also be used to manage policies locally. Alternatively, HP Sure Recover can be securely enabled and configured remotely using the HP Manageability Integration Kit (MIK) for Microsoft® System Center Configuration Manager (SCCM).

Images can be installed from HP repositories or from custom image repositories managed by the system administrator in either the public or private cloud. Custom images can be created with standard tools such as the Windows Assessment and Deployment Kit (Windows ADK).

The process for creating custom images is simple: use the Windows ADK to create an image in a Windows IMaging (WIM) format file, create a manifest containing a version header, the sha256sum hash of the image, its filename, and its file size in bytes, then sign the manifest with your private key. Place the image, manifest, and signature file in a public or private cloud repository, and then provision the system with the location of the image repository and corresponding public key.

HP Sure Recover can be configured remotely via the HP MIK plugin.

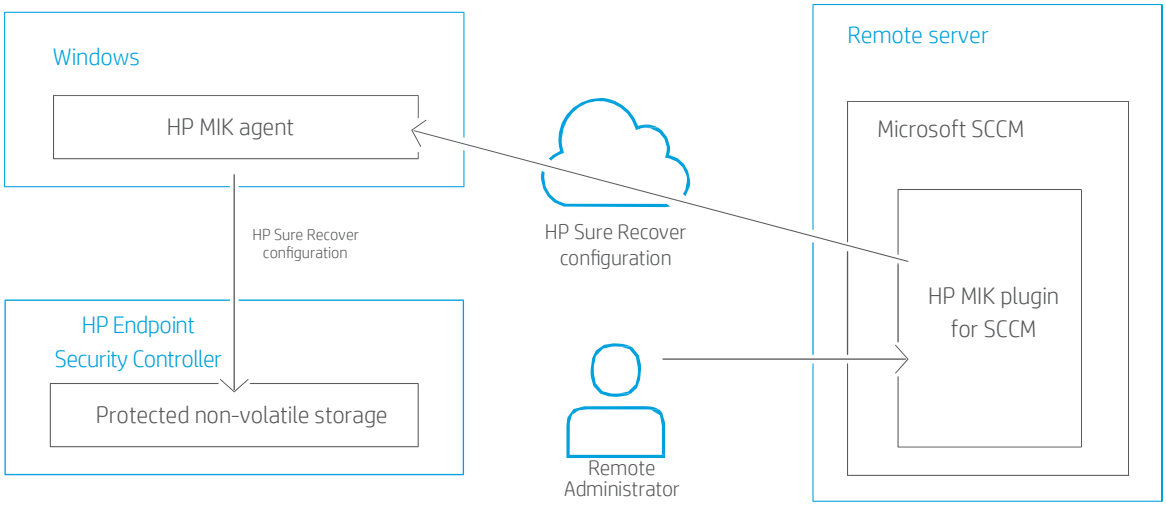

Figure 3: Remote configuration

Local users can configure HP Sure Recover using the HP Client Security Manager.

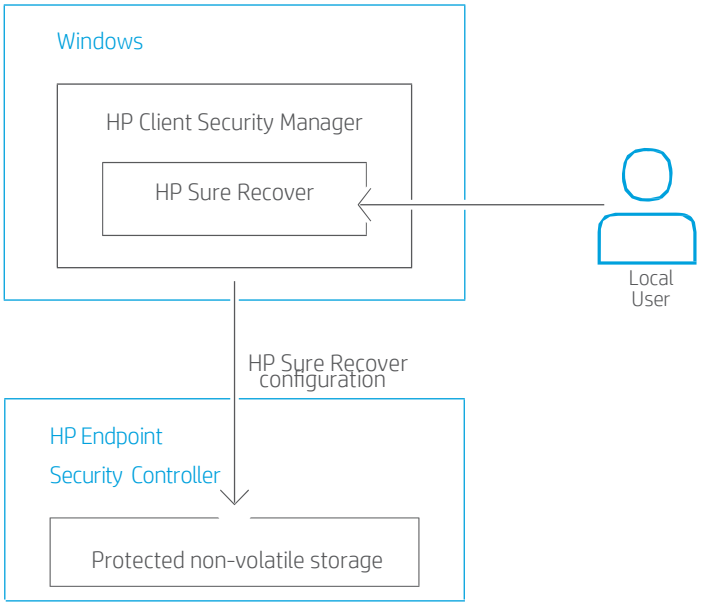

Figure 4: Remote configuration

HP Sure Recover

Conclusion

No matter the reason you need to restore the operating system, HP Sure Recover makes the process simple. Count on hardware-based platform resiliency throughout the lifecycle of the computer, from initial provisioning through end-of-life deprovisioning.

Learn more:
hp.com/go/computersecurity

Technical content:
support.hp.com/us-en/topic/goIT.

4AA7-4556ENW, October 2018