



HP SURE ADMIN

INFOBLATT



HP WOLF SECURITY

HP Sure Admin⁵ bietet moderne Sicherheit für die Verwaltung der PC-Firmware-Konfiguration, da Remote-Administratoren BIOS-Einstellungen sicher verwalten und Kundendienstmitarbeiter einen sicheren persönlichen Zugriff auf das BIOS-Setup erhalten können. Die Verwendung digitaler Zertifikate und Kryptographien mit öffentlichen Schlüsseln eliminiert die Risiken, die mit älteren, kennwortbasierten Ansätzen verbunden sind.



BIOS-EINSTELLUNGEN SIND FÜR DIE PC-SICHERHEIT VON ENTSCHEIDENDER BEDEUTUNG

Die Verwaltung der PC-Firmware (BIOS)-Einstellungen und die Kontrolle des Zugriffs auf diese Einstellungen ist ein wichtiger Bestandteil des Sicherheitsmanagements jedes Unternehmens. Wenn sie ungeschützt bleiben, können BIOS-Sicherheitseinstellungen, die vor einem Angreifer mit physischem Zugriff auf ein Gerät schützen, durch einfaches Deaktivieren dieser Einstellungen umgangen werden. Wenn beispielsweise Secure Boot deaktiviert ist, kann ein Angreifer ein Root-Kit auf dem Gerät installieren, das vom Betriebssystem nicht erkannt werden kann. Ein Angreifer kann außerdem den DMA-Angriffsschutz (Direct Memory Access) deaktivieren, der das Lesen von Geheimnissen direkt aus dem Speicher des Betriebssystems über einen externen Port verhindert. Ein Angreifer kann sogar Firmware- oder hardwarebasierte Remote-Verwaltungstechnologien aktivieren, um Remote-Zugriff auf den PC zu erhalten. Daher ist es so wichtig, den Zugriff auf die BIOS-Einstellungen zu schützen und zu kontrollieren.

FALLSTRICKE BEI KENNWORTBASIERTEN LÖSUNGEN

Wie die übrige PC-Branche bietet auch HP seit vielen Jahren einen kennwortbasierten Autorisierungsgeheimnis-Mechanismus zum Schutz und zur Verwaltung der BIOS-Einstellungen und der privilegierten BIOS-Vorgänge an. Alle kennwortbasierten Lösungen (unabhängig von der Anwendung) weisen jedoch inhärente Bereitstellungsfallen auf, z. B. schwache Kennwörter, vergessene Kennwörter, die Verwendung desselben Kennworts über mehrere Systeme hinweg oder das Nichteinrichten eines Kennworts. Darüber hinaus muss selbst in einem Szenario, in dem von einem Unternehmen starke und eindeutige Kennwörter für jedes Gerät verwendet werden, dieses Kennwort offengelegt werden, um jede BIOS-Einstellungsänderung oder jeden privilegierten BIOS-Vorgang zu autorisieren. Die Anforderung, das Autorisierungsgeheimnis bei jeder Verwendung zu offenzulegen (für kennwortbasierte Ansätze) steigert das Risiko, dass ein Angreifer dieses Geheimnis erfährt. Das Problem wird durch den heute verwendeten branchenüblichen Ansatz noch verschärft. Dasselbe Kennwort wird für die Fernverwaltung von BIOS-Einstellungen und den lokalen Zugriff auf das BIOS-Setup-Menü durch Kundendienstmitarbeiter verwendet.

KEIN STRESS MEHR

MIT HP SURE ADMIN



HARDWAREBASIERTER SCHUTZ

HP Sure Admin speichert Konfigurationen und öffentliche Schlüssel im isolierten und geschützten Speicher des HP Endpoint Security Controllers im Ziel-PCs, was einen umfassenden Integritätsschutz vor Angriffen ermöglicht, die auf den Austausch autorisierter Schlüssel durch den öffentlichen Schlüssel des Angreifers abzielen.



ELIMINIEREN VON KENNWORTANGRIFFEN

HP Sure Admin setzt auf die RSA-Kryptographie mit öffentlichem Schlüssel, was bedeutet, dass niemals Autorisierungsgeheimnisse an den Ziel-PC übertragen werden oder sich darauf befinden.

EIN MODERNER ANSATZ FÜR DAS BIOS-MANAGEMENT

Um Kunden die Möglichkeit zu geben, von der kennwortbasierten BIOS-Verwaltung auf einen modernen Sicherheitsansatz umzusteigen, bietet HP Sure Admin jetzt einen optionalen BIOS-Verwaltungsmechanismus an, für den kein Kennwort erforderlich ist. Dieser neue Ansatz basiert auf der branchenüblichen Kryptographie mit öffentlichen Schlüsseln, die zur sicheren Verwaltung der BIOS-Einstellungen für HP Business-PCs verwendet werden kann, ohne dass ein Autorisierungsgeheimnis offengelegt werden muss.



VERTRAUTE TOOLS

Die Verwaltungstools für die BIOS-Einstellungen, die Teil der Client-Management-Lösungen von HP sind, unterstützen den HP Sure Admin Modus mit nur wenigen Unterschieden bei der Verwendung dieser Tools. Sobald die Ersteinrichtung mit kundenspezifischen Schlüsseln abgeschlossen ist, ist die Verwaltung der BIOS-Einstellungen im HP Sure Admin Modus für den Administrator transparent. Zu den Tools gehören das HP BIOS-Konfigurationsdienstprogramm und das HP Manageability Integration Kit.

NEUE FUNKTIONEN

HP Sure Admin bietet gegenüber dem herkömmlichen kennwortbasierten Ansatz eine Reihe von Vorteilen.

- Die Unterstützung getrennter Autorisierungsgeheimnisse für die Fernverwaltung und den lokalen Zugriff sowie die Abschaffung der Anforderung, das Autorisierungsgeheimnis für beide Szenarien offenzulegen sind bahnbrechende Neuerungen.
- Die Anti-Replay-Unterstützung verhindert, dass ein Angreifer die Einstellungen in einen früheren Zustand zurückversetzen kann.
- Device-Targeting ermöglicht es einem Remote-Administrator, Einstellungen auf einem bestimmten Rechner zu ändern, die auf anderen Rechnern in derselben Bereitstellung nicht verwendet werden können.
- Sperren Sie den lokalen Zugriff auf HP Computer Setup vollständig, ohne die Möglichkeit der Fernverwaltung der Einstellungen zu beeinträchtigen, oder verwenden Sie den optionalen Sure Admin Local Access Authenticator, um einen sicheren Zugriff zu ermöglichen.
- Die Verwendung von HP Custom System Setting Services für HP Sure Admin⁴ sichert die BIOS-Einstellungen ab dem Zeitpunkt, an dem der PC das HP Werk verlässt, und ermöglicht eine sichere Zero-Touch-Firmware-Verwaltung direkt nach dem Aufstellen.

HÄUFIG GESTELLTE FRAGEN

F: Wie hoch sind die Kosten für HP Sure Admin?

A: HP Sure Admin ist eine Funktion, die in ausgewählten HP PCs³ ohne zusätzliche Kosten enthalten ist. Die für die Konfiguration und Verwaltung von Sure Admin erforderlichen HP Client Management Tools¹ werden ebenfalls kostenlos zur Verfügung gestellt.

F: Welche Geräte unterstützen HP Sure Admin?

A: HP Sure Admin wird auf einer Vielzahl von HP Business-Produkten³ unterstützt, darunter Pro- und Elite-Desktops, Pro- und Elite-Notebooks, Z-Desktops und Z-Mobile-Workstations.

F: Erfordert HP Sure Admin eine Backend-Infrastruktur?

A: HP Sure Admin kann sowohl von Großunternehmen als auch von kleinen und mittleren Unternehmen eingesetzt werden. Die HP Client Management Tools ermöglichen HP Sure Admin Bereitstellungen mit oder ohne Backend-Infrastrukturanforderungen.

F: Ist zusätzliche Hardware für den Einsatz von HP Sure Admin erforderlich?

A: Bei Bereitstellungen, bei denen ein sicherer lokaler Zugriff auf das HP BIOS-Setup (F10-Setup) erforderlich ist, ist ein Android- oder iOS-Telefon mit einer Kamera und einer kostenlosen HP-Anwendung erforderlich, die über den Apple App Store oder Google Play erhältlich ist.

F: Wo erhalte ich weitere Informationen zu HP Sure Admin?

A: Weitere Informationen zur Funktionsweise und Verwendung von Sure Admin finden Sie im technischen Whitepaper² von HP Sure Admin und in der Dokumentation¹ der HP Client Management Tools.

F: Was ist der Unterschied zwischen dem HP Sure Admin Remote-Management und dem lokalem Zugriff/Management?

A: Das Remote-Management von BIOS-Einstellungen bezieht sich auf die programmatischen Schnittstellen, die das BIOS dem Betriebssystem zur Verwaltung von BIOS-Einstellungen zur Verfügung stellt, die in den meisten Fällen (aber nicht unbedingt erforderlich) von einem Remote-Administrator stammen. Der lokale Zugriff auf oder die lokale Verwaltung von BIOS-Einstellungen bezieht sich auf das Szenario eines Kundendienstmitarbeiters, der physisch auf dem Zielcomputer arbeiten kann und die BIOS-Einstellungen manuell über die F10 BIOS-Setup-GUI ändert.

F: Kann HP Sure Admin dafür sorgen, dass der Kunde HP keine Geheimnisse mehr für werkseitig konfigurierte Geräte mitteilen muss?

A: Bei einem BIOS-Administrator Kennwort muss der Kunde HP das Kennwort zur Verfügung stellen, um die Einstellung dieses

Kennworts im Werk von HP zu aktivieren. Bei HP Sure Admin muss HP nur der öffentliche Schlüssel des Kunden zur Verfügung gestellt werden, sodass der Kunde den privaten Schlüssel vollständig schützen kann.

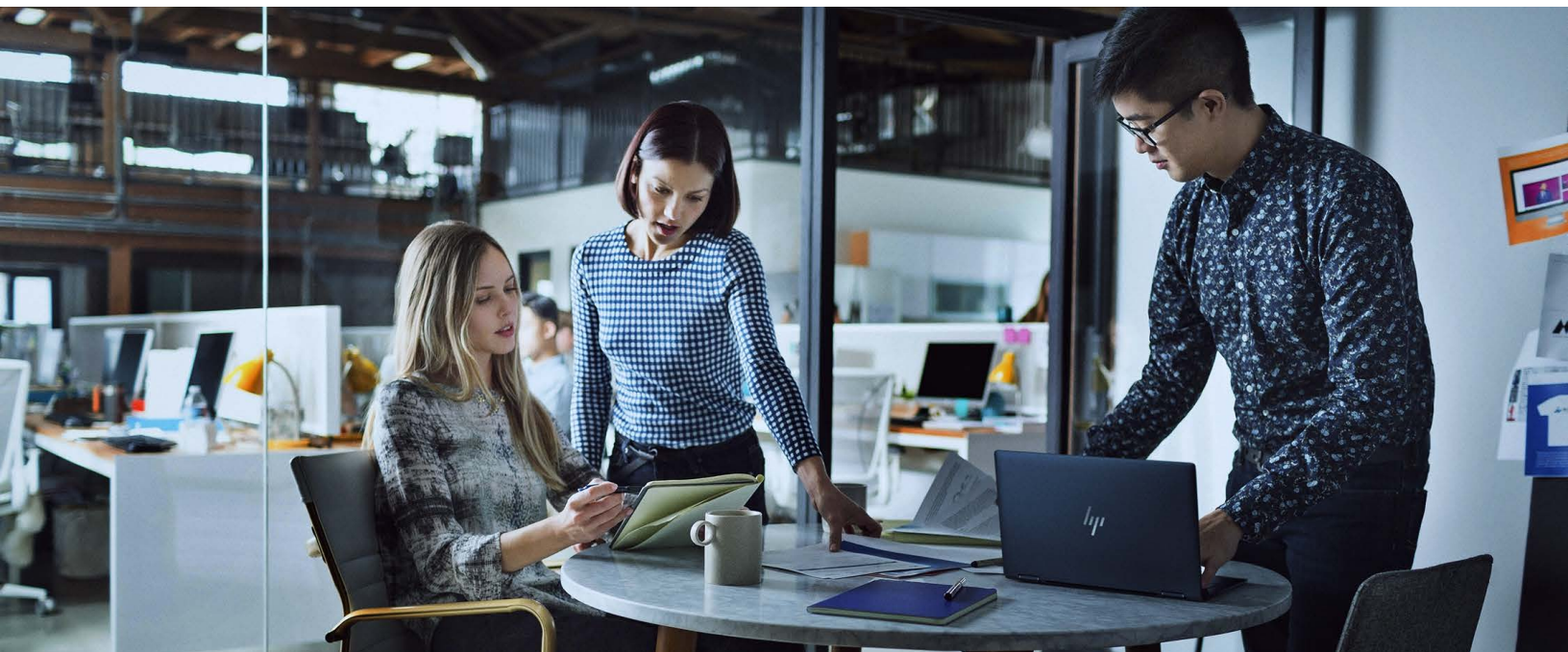
F: Welchen kryptografischen Algorithmus nutzt HP Sure Admin?

A: HP Sure Admin nutzt branchenübliche digitale RSA-Signaturen, um Befehle zur Änderung der BIOS-Einstellung zu autorisieren. HP Sure Admin nutzt außerdem die RSA-Verschlüsselung mit öffentlichem Schlüssel, um sicheren lokalen Zugriff auf HP Computer Setup zu implementieren und privilegierte lokale Vorgänge zu autorisieren.

F: Muss ich HP Sure Admin auf den Geräten nutzen, die es unterstützen?

A: HP Sure Admin ist optional. Standardmäßig funktionieren die üblichen kennwortbasierten BIOS-Mechanismen genauso wie bei früheren Produkten. Darüber hinaus sind die HP Client Management Tools für den Einsatz in einer heterogenen Umgebung konzipiert (einige Geräte verwenden übliche BIOS-Kennwörter, während andere HP Sure Admin verwenden), wenn die gesamte Flotte auf HP Sure Admin umgestellt wird.

Weitere Informationen finden Sie unter hp.com/wolfsecurityforbusiness.



HP SURE ADMIN

¹Die HP Client Management Tools sind unter <http://www.hp.com/go/clientmanagement> verfügbar.

²Das HP Sure Admin Technische Whitepaper ist unter <http://h20195.www2.hp.com/v2/GetDocument.aspx?docname=4AA7-7307ENW> erhältlich.

³Zu den unterstützten Plattformen gehören HP Business-Produkte, die 2019 oder später eingeführt wurden, darunter Pro- und Elite-Desktops, Pro- und Elite-Notebooks, Z-Desktops und Z-Mobile-Workstations. In einigen Fällen ist ein Upgrade auf die neueste BIOS-Version erforderlich, um den Sure Admin Support zu aktivieren.

⁴Custom System Setting Services ist optional und verursacht zusätzliche Kosten. Weitere Informationen erhalten Sie unter <https://www8.hp.com/us/en/business-services/pcandprintservices/configuration.html>.

⁵HP Sure Admin erfordert Windows 10, HP BIOS, HP Manageability Kit von <http://www.hp.com/go/clientmanagement> und die Smartphone-App HP Sure Admin Local Access Authenticator aus dem Android- oder Apple-Store.



HP WOLF SECURITY

© Copyright 2021 HP Development Company, L.P. Änderungen vorbehalten. Neben der gesetzlichen Gewährleistung gilt für HP Produkte und Dienstleistungen ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Dienstleistungen explizit genannt wird. Aus den Informationen in diesem Dokument ergeben sich keinerlei zusätzliche Gewährleistungsansprüche. HP haftet nicht für technische bzw. redaktionelle Fehler oder fehlende Informationen.

4AA7-7978DEE, Juni 2021