HP Wolf Pro Security Kurzanleitung

Version 1.0

Kurzanleitung – HP Wolf Pro Security

Inhalt

Einführung

HP Wolf Pro Security (WPS) besteht aus 3 wesentlichen Schutzfunktionen. Sie können alle 3 Technologien auf jedem unterstützten Computer aktivieren.

1. Bedrohungseindämmung – Hardware-gestützte Datei-Isolation und Eindämmung in sämtlichen virtuellen Maschinen des gesamten Stacks.
2. NGAV – Signatur- und verhaltensbasierter Schutz – Quarantäne schädlicher Inhalte mithilfe von KI- und Deep Learning-Tools.
3. Zugangsdatenschutz – Die Eingabe von Zugangsdaten auf bekannten schädlichen Seiten wird verhindert und auf unbekannten Seiten wird der Benutzer bzw. die Benutzerin gewarnt

Da die häufigsten Quellen für Angriffe gegen Endgeräte-PCs der Download von E-Mal-Anhängen, böswillige Websites und infizierte Links sind, öffnet die Bedrohungseindämmung nicht vertrauenswürdige Inhalte in isolierten VMs. So wird die Malware in einer Hardware-gestützten virtuellen Maschine ausgeführt. Dieser Ansatz verhindert, dass die Bedrohung das Endgerät infiziert oder sich über das Netzwerk ausbreitet. Außerdem kann der Inhalt auf verdächtiges Verhalten überwacht werden. Durch isoliertes Öffnen der Dateien werden Zero-Day-Bedrohungen eingedämmt. Der leistungsstarke Zugangsdatenschutz in einer AV-Lösung der nächsten Generation ergänzt die Lösung zu einem vollständigen Paket zum Schutz Ihres Windows-PCs vor den am weitesten entwickelten Bedrohungen.

Neben der branchenweit besten Sicherheitstechnologie sind Server und Agent-Upgrades sowie eine automatische Überwachung der Plattformintegrität enthalten. Das Onboarding erfolgt mithilfe eines einfachen Prozesses und Hilfe bei der Fehlersuche ist jederzeit telefonisch oder per E-Mail möglich. Die HP Sicherheitsexpert:innen helfen Ihnen während Ihrer Vertragslaufzeit gerne weiter.

Zielgruppe

Sie sollten entweder ein Anfrageformular für einen Testzeitraum (POC) übermittelt oder das WPS-Produkt gekauft haben. Nach der Genehmigung sollten Sie eine E-Mail mit Anweisungen zu den nächsten Schritten erhalten haben.

Hinweis: Es ist wichtig, dass Sie bei der Bestellung eine korrekte E-Mail-Adresse angeben, da der Versand der E-Mail zur Aktivierung an diese E-Mail-Adresse erfolgt.

Wenn Sie diese E-Mail nicht finden können oder die Person, die den Zugriff auf unseren Service angefragt hat, nicht erreichbar ist, besuchen Sie bitte https://support.hpwolf.com für weitere Kontaktmöglichkeiten. Nachdem Sie Ihre Genehmigungs-E-Mail erhalten haben, besuchen Sie bitte den Onboarding-Bereich.

Diese Anleitung sollte Antworten auf die meisten Ihrer anfänglichen Fragen bieten. Bitte wenden Sie sich bei Problemen an Ihren Partner-Support.

Der erste Teil dieses Dokuments ist für *IT- und Cybersicherheits-Administratoren vorgesehen*. Hier ist Folgendes enthalten:

- Technische Zusammenfassungen des Produkts

- Ein Überblick, wie die IT- und Cybersicherheits-Administratoren mit dem Wolf Pro Controller interagieren
- Welche Kommunikation für den Service erwartet werden kann.
- Überblick über das Support-Portal

Der zweite Teil dieses Dokuments beschäftigt sich mit der HP Wolf Pro *Endbenutzer-Erfahrung*:

- Desktop-Benutzeroberfläche
- Status
- System-Popups und Interaktionen mit dem Produkt.
- Einsenden einer Anfrage mit der Bitte um Unterstützung.

Quick Links

Zugriff auf Ihre Controller-Instanz

Melden Sie sich hier mit Ihrer HPID an:

https://portal.hpwolf.com

Systemanforderungen - Hardware und Software

Unsere Produkte müssen mit minimalem Hardware und Software installiert werden, um korrekt zu funktionieren. Weitere Informationen finden Sie hier:

https://support.hpwolf.com/s/article/System-Requirements-WPS

Technischer Support und FAQ

Sie haben Fragen? Möglicherweise finden Sie die Antwort hier:

https://support.hpwolf.com

Kontakt zum Support

Kontaktinformationen finden Sie hier: https://support.hpwolf.com/s/contact

Für IT- und Cybersicherheits-Administratoren

Produkt-Terminologie

Die HP Wolf Pro Security Lösung besteht aus 2 primären Komponenten:

- Der HP Wolf Security Controller ist Ihr in der HP-Cloud gehosteter „Controller“ für Administrator:innen zur Verwaltung der Endgeräte-„Agents“
- HP Wolf Security ist aus mehreren Softwarefunktionen bestehender „Agent“, die auf einzelnen Endbenutzer-Computern installiert sind.
    - HP Wolf Pro Security Schutzfunktionen
    - HP Wolf Security „Desktop Console“ zur Überprüfung des Agent-Status oder zum Aktivieren/Deaktivieren von Funktionen auf einem lokalen Gerät.
    - HP Sure Click Pro Secure Browser, ein Browser, der Funktionen zur Bedrohungseindämmung nutzt, um Seiten isoliert zu öffnen. Darüber hinaus werden zusätzliche Browser-Erweiterungen und ein Outlook-Plugin installiert

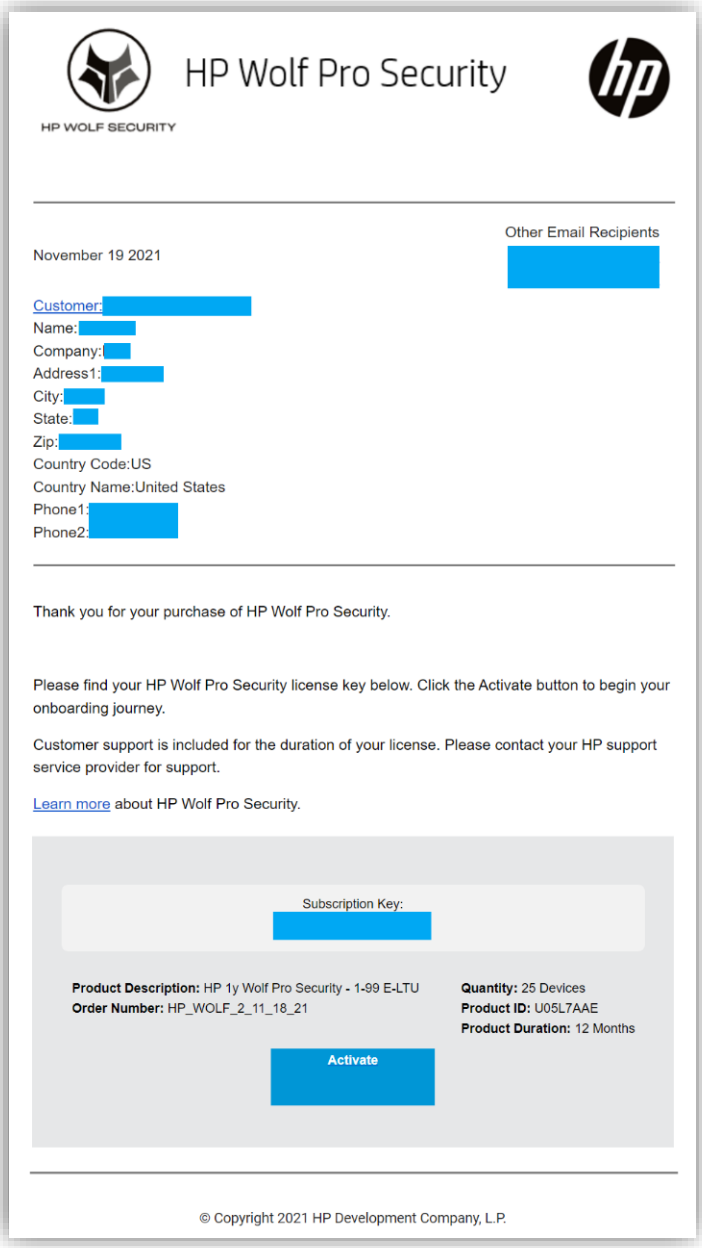
Self-Onboarding und Aktivierung

Die WPS-Installation und der Schutz Ihrer Endgeräte beginnt mit dem Aktivierungs- und Onboarding-Schritt.

In bestimmten Fällen kann Ihr Managed Service-Partner, je nachdem, wie Sie WPS erworben haben, diesen Schritt für Sie übernehmen. Bitte wenden Sie sich an Ihren MSP.

Aktivierungs-E-Mail

Ob eine POC-Anfrage genehmigt oder WPS käuflich erworben wurde, der Weg beginnt damit, dass der Kunde (oder MSP) eine E-Mail von HP erhält. Diese E-Mail enthält den Lizenzschlüssel, SKU-Informationen und einen Aktivierungslink.



HP Wolf Pro Security

HP WOLF SECURITY

Other Email Recipients

November 19 2021

Customer:
Name:
Company:
Address1:
City:
State:
Zip:
Country Code:US
Country Name:United States
Phone1:
Phone2:

Thank you for your purchase of HP Wolf Pro Security.

Please find your HP Wolf Pro Security license key below. Click the Activate button to begin your onboarding journey.

Customer support is included for the duration of your license. Please contact your HP support service provider for support.

Learn more about HP Wolf Pro Security.

Subscription Key:

Product Description: HP 1y Wolf Pro Security - 1-99 E-LTU
Order Number: HP_WOLF_2_11_18_21

Quantity: 25 Devices
Product ID: U05L7AAE
Product Duration: 12 Months

Activate

© Copyright 2021 HP Development Company, L.P.

Mit dem Anklicken des Aktivierungslinks beginnt der Onboarding-Prozess.

Onboarding-Einrichtungsprogramm

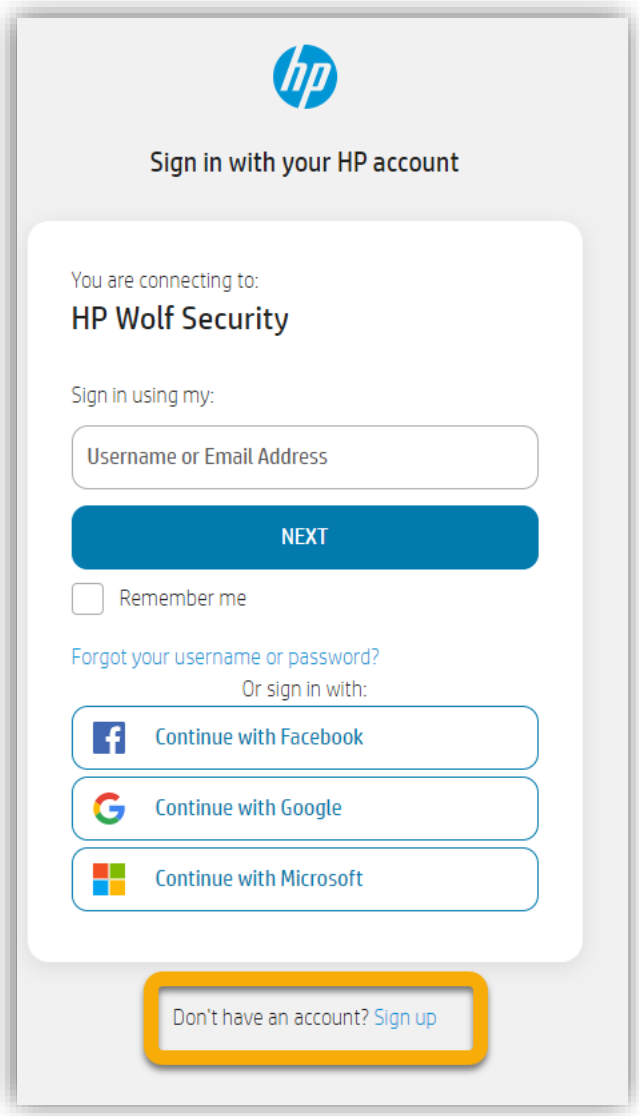
Zur Aktivierung von WPS sind nur wenige einfache Schritte erforderlich.

Schritt 1: Anmelden mit Ihrer HPID

Nach dem Klicken auf den Aktivierungslink werden Sie zunächst um Ihre HPID-Anmeldung gebeten.

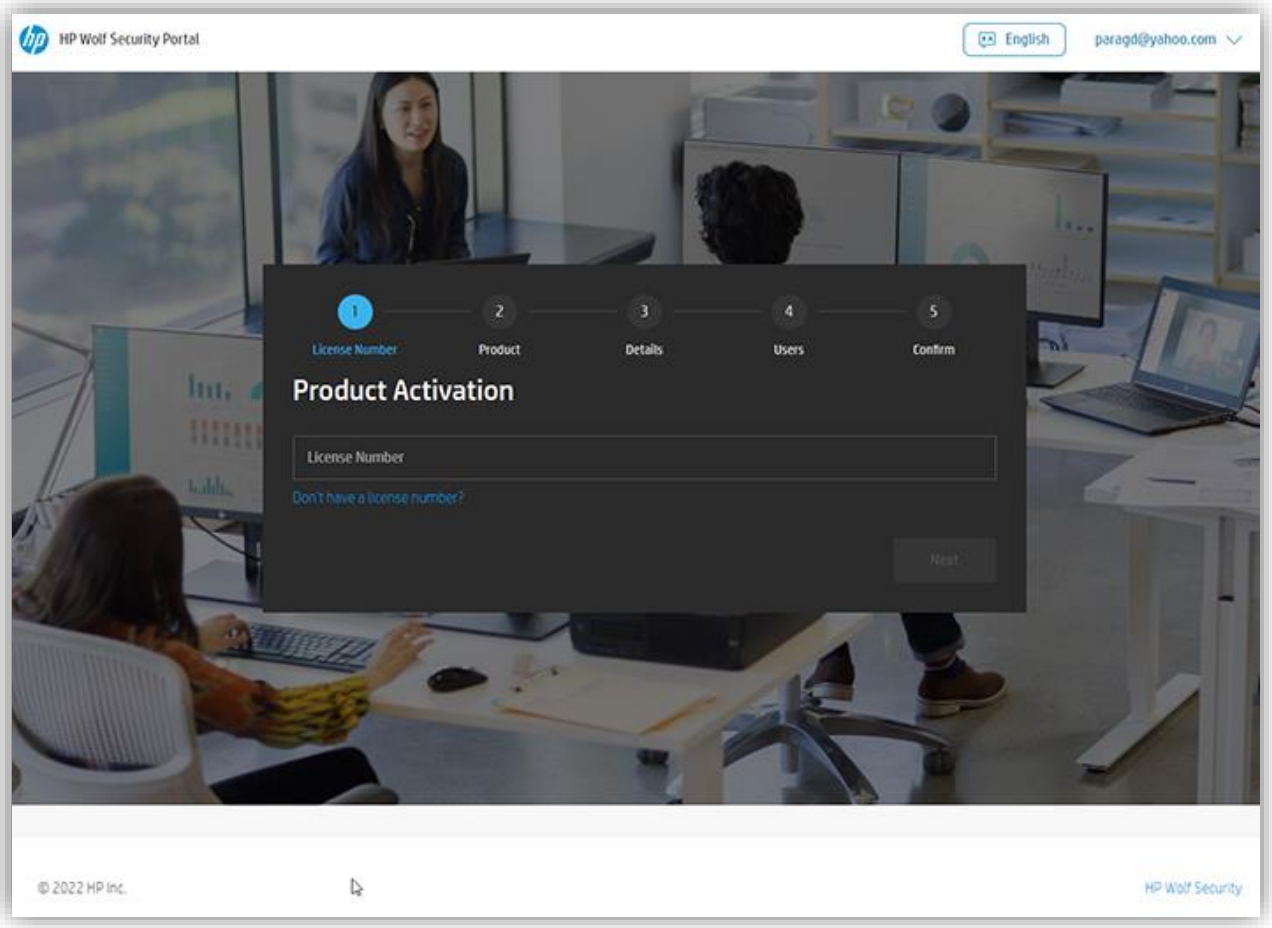
Kurzanleitung – HP Wolf Pro Security

1. Wenn Sie bereits über ein HPID Konto verfügen, geben Sie bitte Ihre Zugangsdaten ein.
2. Falls Sie noch kein HPID Konto besitzen, folgen Sie diesen Anweisungen.
3. Wählen Sie im unteren Seitenbereich „Anmelden“.



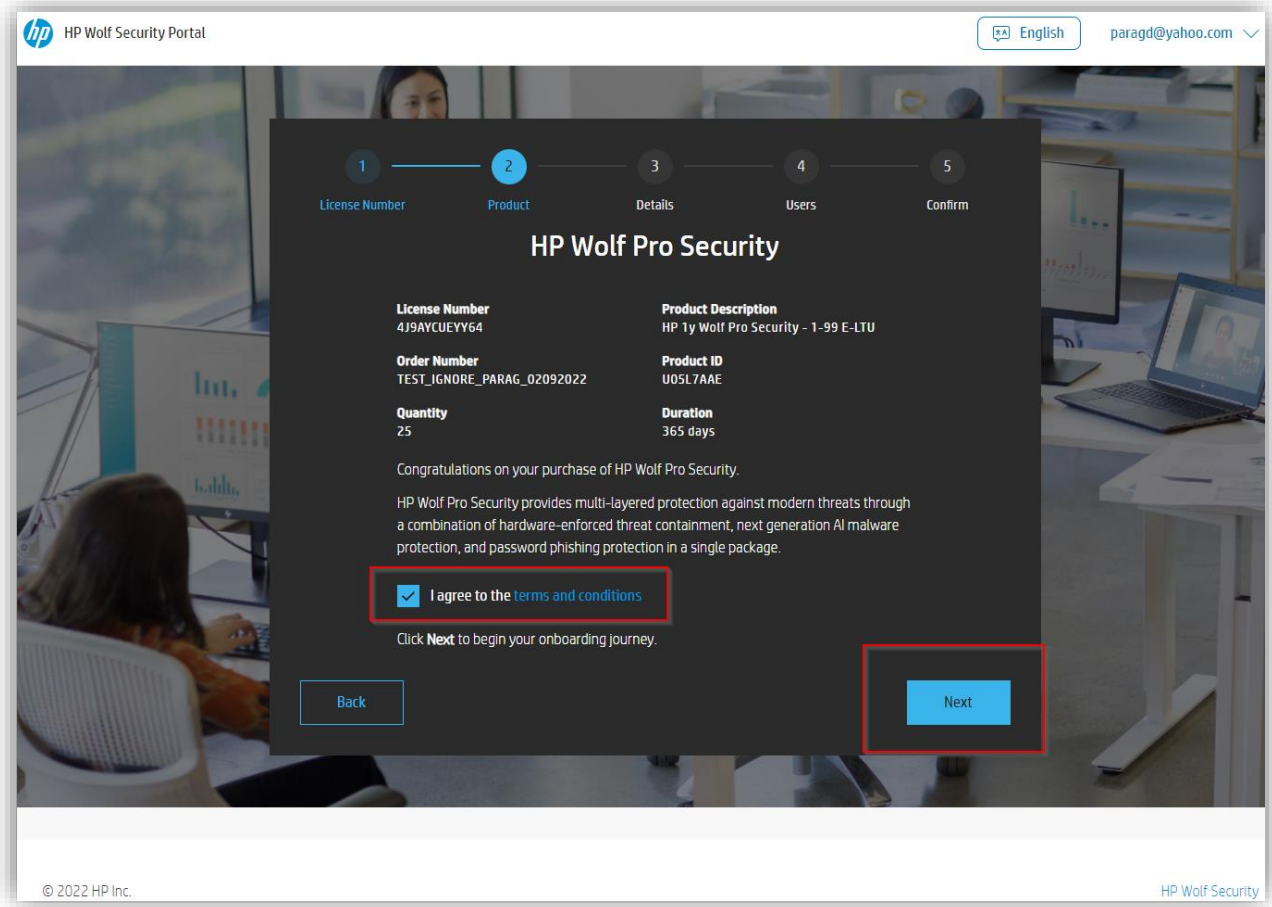
4. Geben Sie Ihre Kontodaten ein und klicken Sie auf „Konto erstellen“.
5. In einem 2FA-Schritt werden Sie aufgefordert, einen Code einzugeben, der an die eingegebene E-Mail-Adresse versandt wurde.
6. Nachdem das Konto erfolgreich erstellt wurde, werden Sie automatisch zu Ihrem Controller weitergeleitet und sollten die nachstehende Ansicht angezeigt bekommen:

Schritt 2: Lizenzvalidierung



In den meisten Fällen wird die Lizenznummer automatisch eingetragen. Falls nicht, kopieren Sie die Ihnen per E-Mail zugesandte Lizenznummer, fügen Sie diese ein und klicken Sie auf WEITER.

Nach erfolgreicher Validierung der Lizenz wird Ihnen der folgende Bildschirm angezeigt:



Bitte stellen Sie sicher, dass Sie die Geschäftsbedingungen lesen und akzeptieren, die ebenfalls einen Link zur Datenschutzrichtlinie sowie ein Daten-FAQ-Dokument enthalten.

So lange die Bedingungen nicht akzeptiert werden, ist die Schaltfläche WEITER nicht nutzbar.

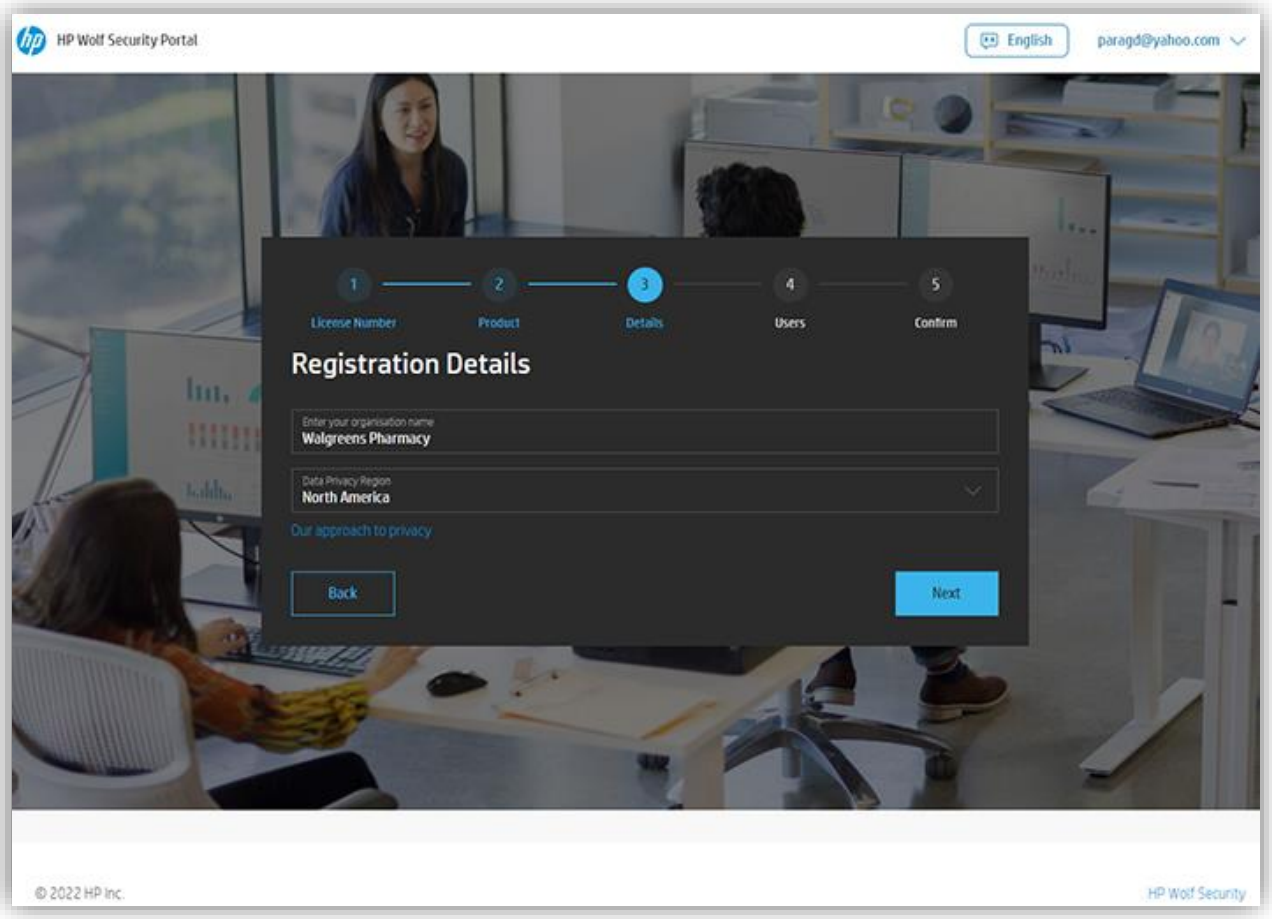
Wenn Sie die Bedingungen gelesen haben und akzeptieren, klicken Sie bitte auf die Schaltfläche „Weiter“.

Schritt 3: Mandanteninformationen

Im nächsten Schritt geben Sie den Namen Ihres Mandanten ein und wählen Sie die Datenregion. Hierdurch wird festgelegt, wo Ihr Mandant erstellt wird und Ihre Daten gespeichert werden. Zum Zeitpunkt der Erstellung dieses Dokuments bestehen nur zwei Optionen:

EU und Nordamerika.

Für Länder außerhalb der EU wählen Sie bitte Nordamerika. Weitere Datenregionen werden bei Bedarf erstellt, um regionale und andere Datenschutzrestriktionen zu erfüllen.



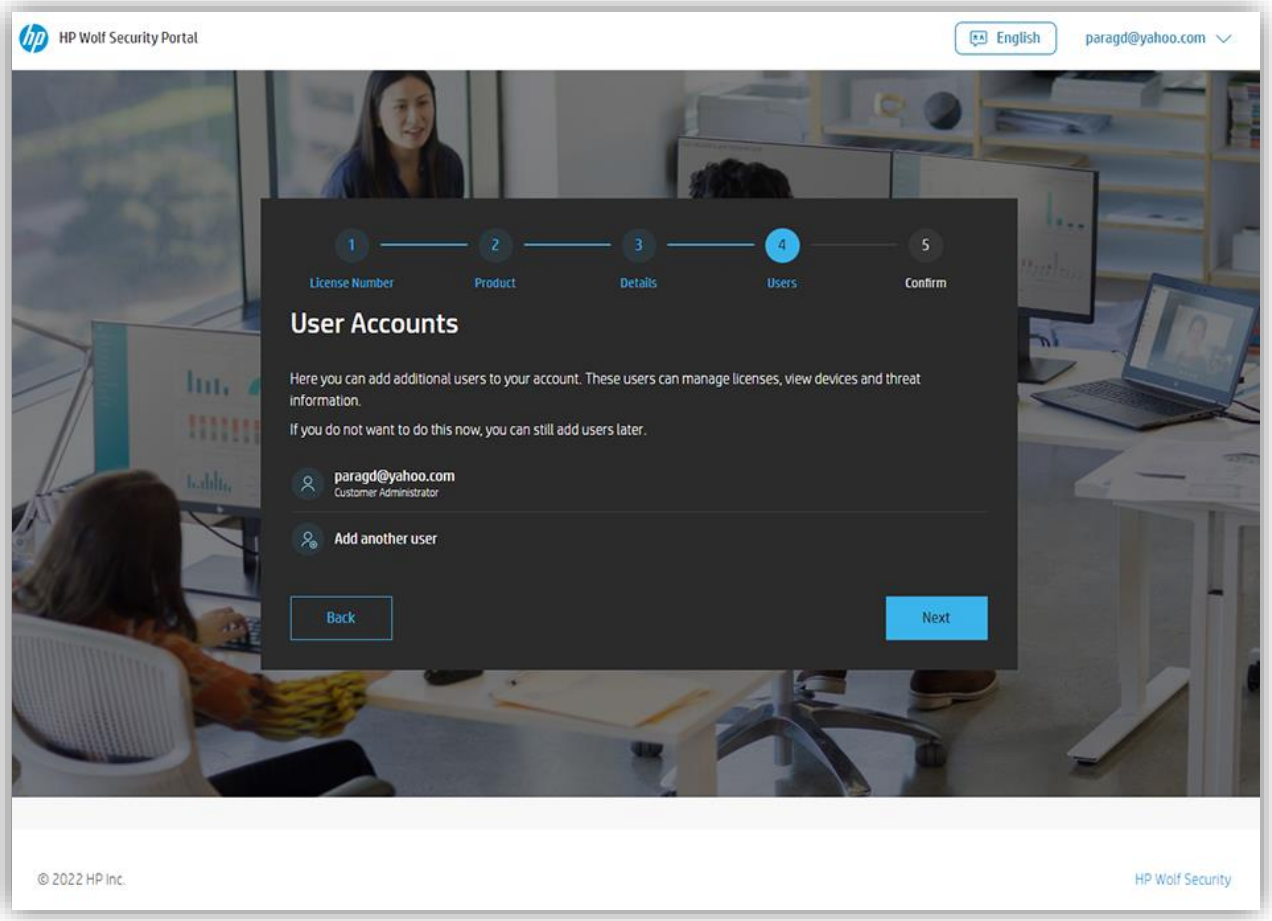
Schritt 3: Hinzufügen von Benutzer:innen

Die für das Onboarding verwendete HPID wird standardmäßig mit einer Kundenadministrator-Rolle erstellt. Fügen Sie hier bei Bedarf weitere Benutzer:innen hinzu, die Zugriff auf den Mandanten benötigen. An diesem Punkt stehen nur zwei Optionen zur Verfügung.

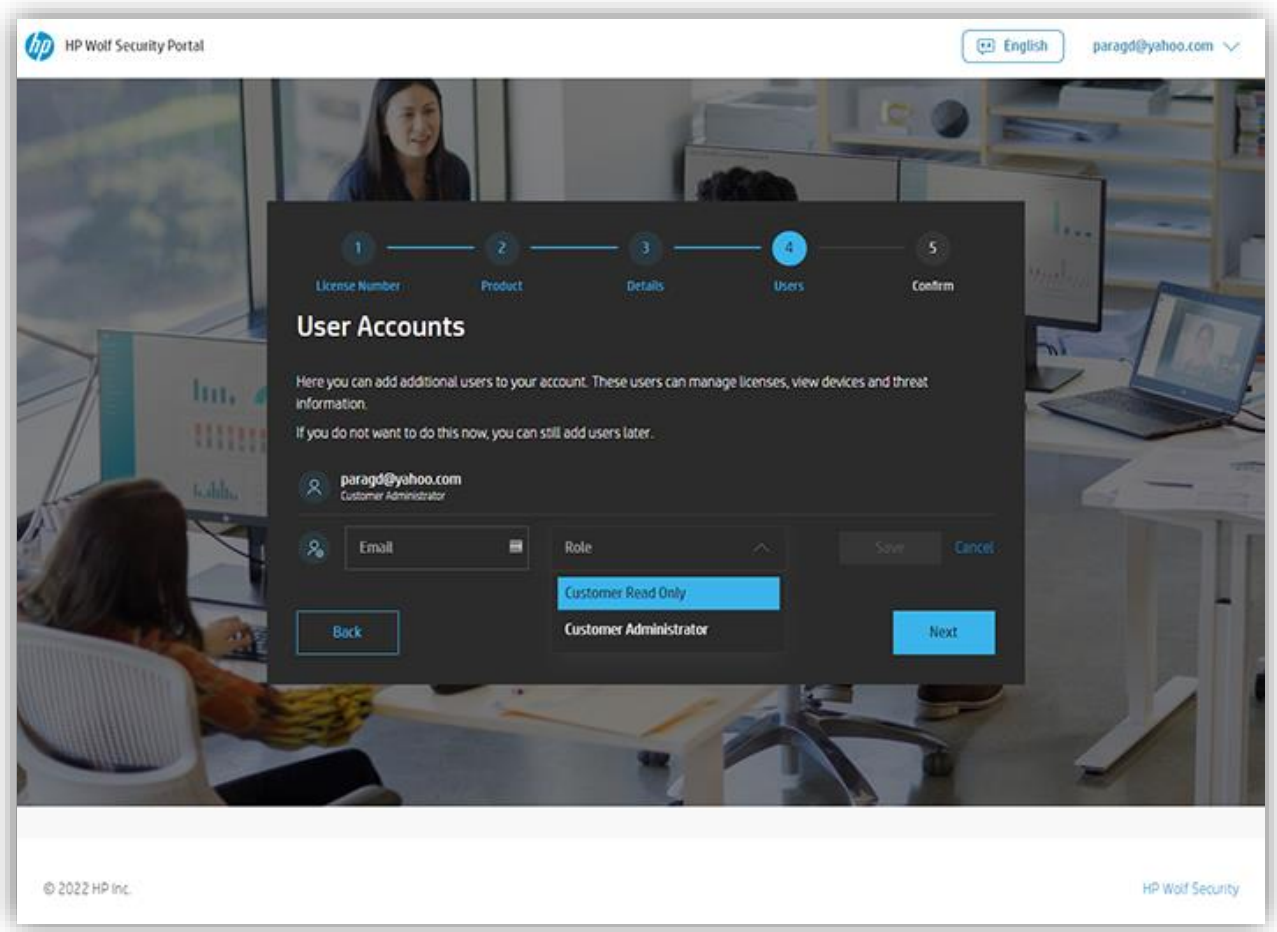
Kundenadministrator:in – Der Administrator bzw. die Administratorin kann Änderungen im Controller vornehmen.

Kunde bzw. Kundin mit reinem Lesezugriff – Kann die Controller-Einstellungen und Berichte nur anzeigen lassen.

Kurzanleitung – HP Wolf Pro Security



Kurzanleitung – HP Wolf Pro Security



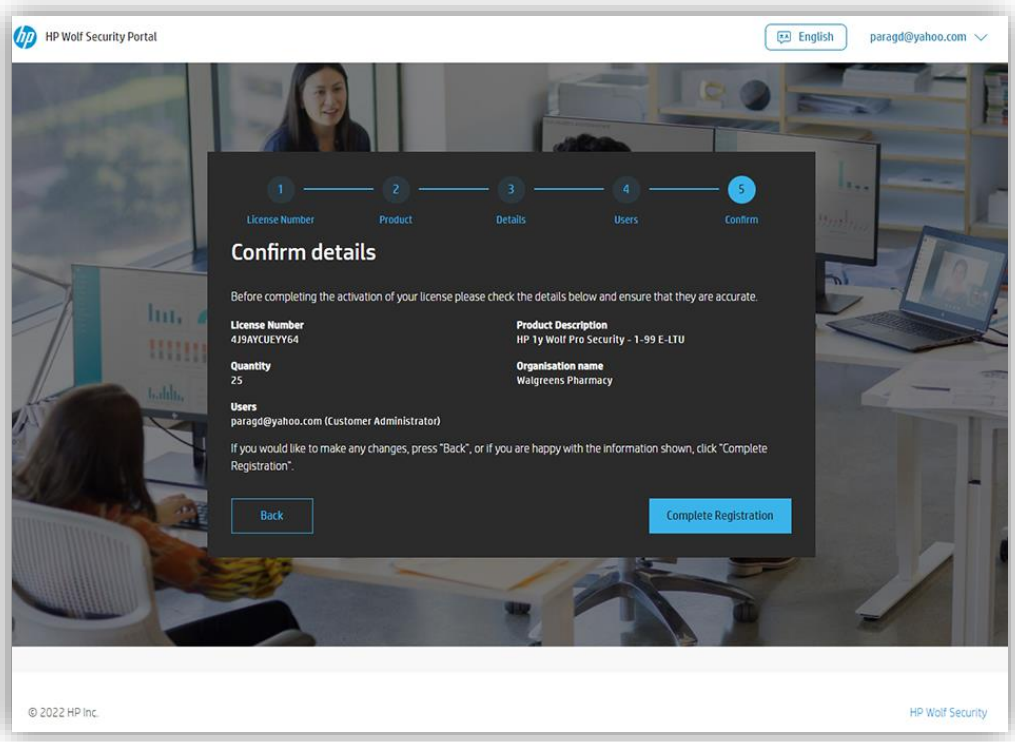
Falls Sie ein MSP sind und das Onboarding für Ihren Kunden bzw. Ihre Kundin durchführen oder die Software im Auftrag Ihres Kunden bzw. Ihrer Kundin aktivieren, können Sie hier die E-Mail-Adresse des Kunden-IT-Admin oder eines anderen entsprechend autorisierten Benutzers bzw. einer anderen entsprechend autorisierten Benutzerin angeben. In ähnlicher Weise, falls Sie Kunde bzw. Kundin sind, das Onboarding selbst durchführen und Ihrem Managed Service-Partner Zugriff gewähren möchten, können Sie hier die E-Mail-Adresse Ihres Partners eingeben.

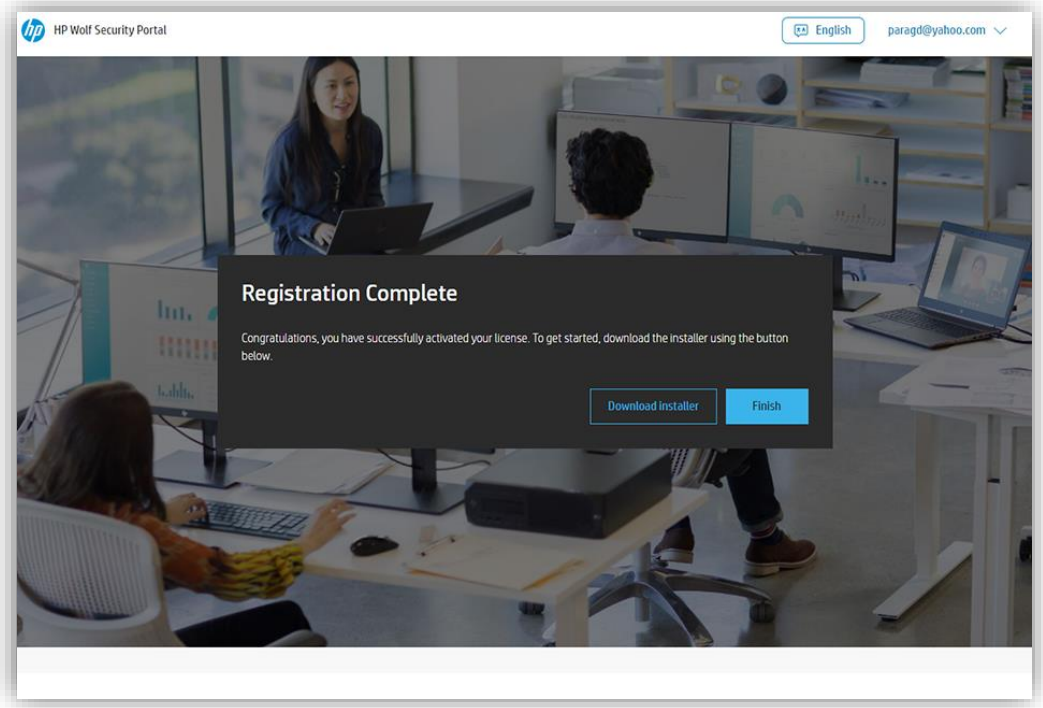
Das Hinzufügen ist zudem auch zu einem späteren Zeitpunkt möglich.

Nachdem Sie die benötigten Benutzer:innen hinzugefügt haben, fahren Sie mit dem nächsten Schritt fort.

Schritt 4: Registrierung abschließen

Anschließend wird eine Bestätigungs-seite angezeigt. Vergewissern Sie sich, dass alle Angaben korrekt sind. Navigieren Sie bei Bedarf zurück, um Änderungen vorzunehmen. Falls nicht, schließen Sie die Registrierung ab.



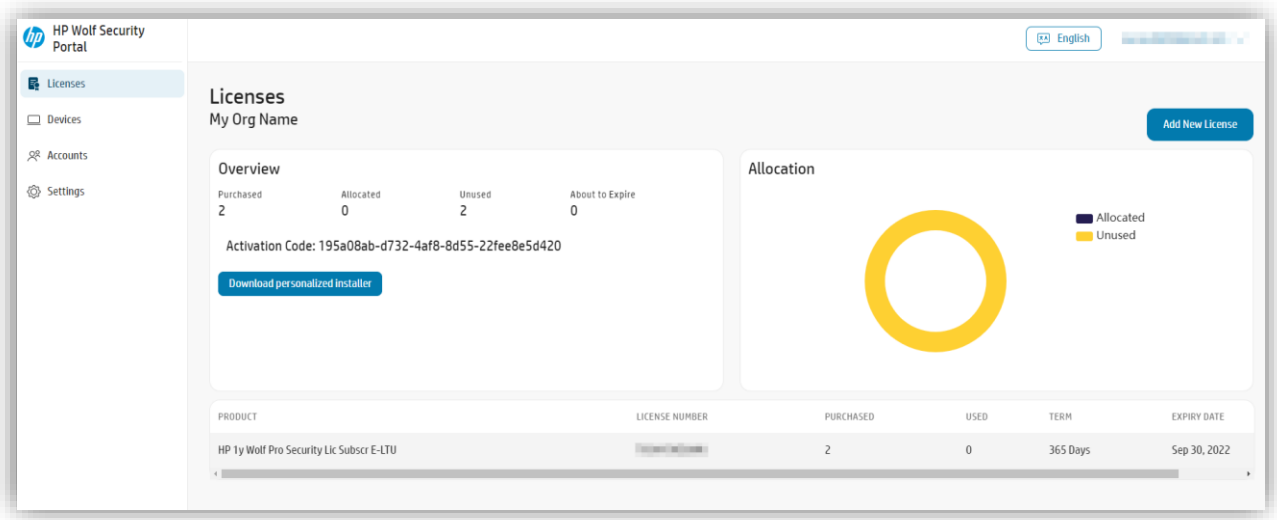


Schritt 5: Einrichten der Cloud-Funktionen

Alle Kunde:innn erhalten Zugang zu einer Cloud-Konsole. Es bestehen jedoch einige wesentliche Unterschiede

Weniger als 25 Arbeitsplatzlizenzen erworben

Wenn Sie eine Lizenz für weniger als 25 Arbeitsplätze erworben haben, wird Ihnen dieser Bildschirm direkt nach Abschluss der Registrierung im vorherigen Schritt angezeigt:

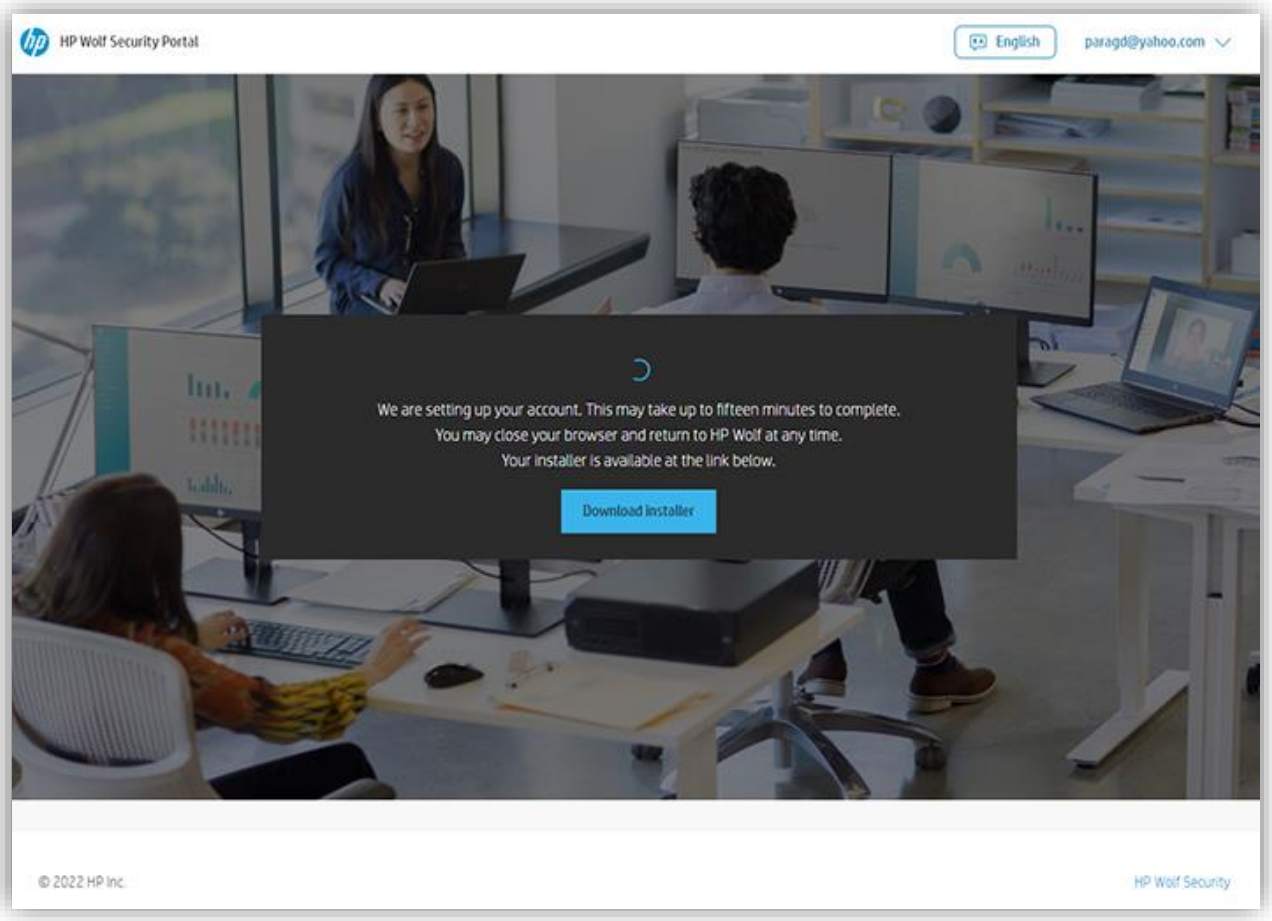


Diese Konsole bietet Ihnen die Möglichkeit, Lizenzen und Benutzerkonten anzuzeigen und zu verwalten sowie grundlegende Details zu den mit dem Mandanten verknüpften Geräten zu sehen. Zur vollständigen Freischaltung aller Verwaltungsfunktionen müssen dem Mandanten 25 oder mehr Arbeitsplätze zugeordnet sein.

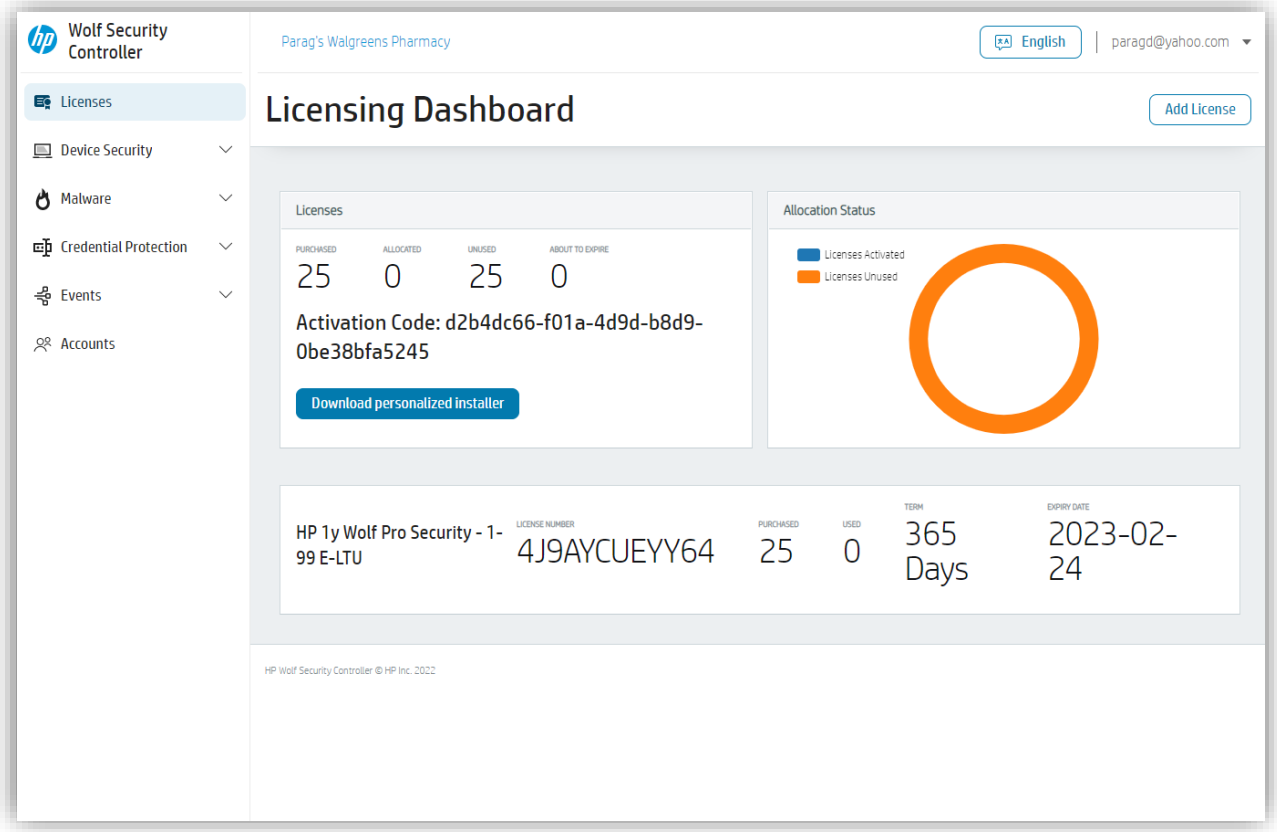
Falls weitere Arbeitsplätze erworben und diesem Mandanten zugeordnet werden (wodurch sich die Gesamtzahl auf mehr als 24 erhöht) oder eine Lizenz für einen neuen Mandanten mit mehr als 24 Arbeitsplätzen erworben wird, führt dies automatisch zur Aktivierung der vollständigen Verwaltungsfunktionen dieses Mandanten. Siehe unten.

25 oder mehr Arbeitsplätze erworben

Wenn mehr als 24 Arbeitsplätze erworben wurden oder die Aktivierung dieser Lizenz für einen bestehenden Mandanten zu einer Gesamtzahl von 25 oder mehr zugeordneten Arbeitsplätzen führt, werden durch diesen nächsten Schritt sämtliche Verwaltungsfunktionen freigeschaltet. Die Durchführung dieses Schrittes nimmt bis zu 15 Minuten in Anspruch, da WPS eine vollständige und umfassende Datentrennung zwischen Mandanten vornimmt. Nach Anklicken der Schaltfläche „Abschließen“ im obigen Registrierungsbildschirm wird Folgendes angezeigt:



Nachdem der Mandant erstellt wurde, werden Sie automatisch zu Ihrem Mandanten weitergeleitet und sollten eine Ansicht wie die Folgende angezeigt bekommen:



Installation des Endgeräte-Agents

Das Installationsprogramm für das Produkt ist zum Download verfügbar, sobald der Mandant eingerichtet wurde, vor dem Erstellen der Controller-Instanz.

HP empfiehlt, das Installationsprogramm erst auszuführen, nachdem der Controller vollständig erstellt wurde. Der Grund hierfür ist, dass das Installationsprogramm bestimmte Produktinformationen und Pakete vom Controller herunterladen muss.

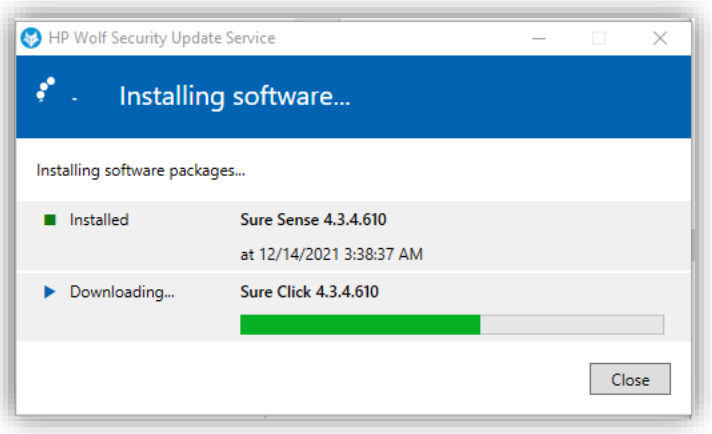
Das Installationsprogramm für unser Produkt finden Sie nach der Anmeldung im Controller und auf der Lizenzseite. Wenn Sie das Installationsprogramm bereits zuvor heruntergeladen haben (bevor die Controller-Instanz erstellt wurde), müssen Sie ihn nicht erneut herunterladen.

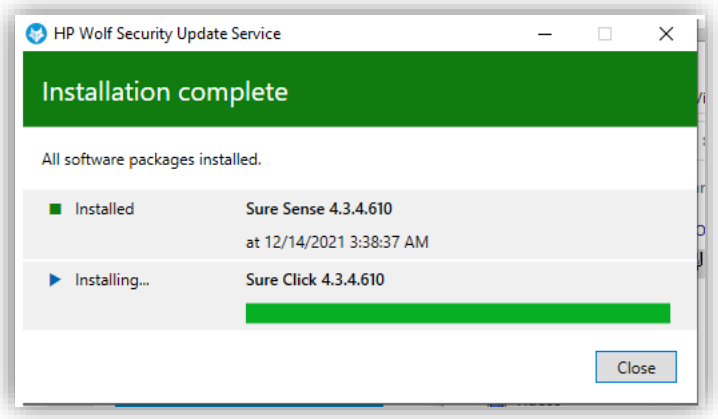
Das Installationsprogramm mit der Bezeichnung *HPSecurityUpdateService – [hier steht der Name Ihres Mandanten].msi* ist lediglich 2 MB groß und lässt sich schnell auf dem Computer installieren. Das Installationsprogramm führt eine Reihe von Prüfungen durch und beginnt kurz nach dem Start mit dem Download sowie der Installation des Agents auf Ihrem Computer.

Installation auf einem einzelnen Gerät

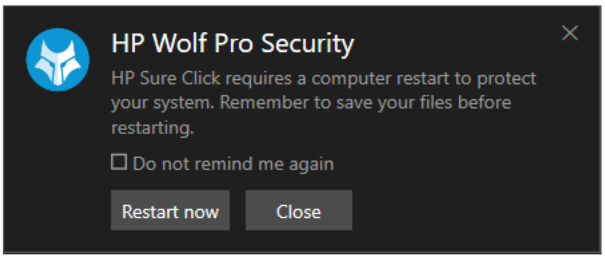
- Führen Sie einen Rechtsklick auf das Installationsprogramm durch und wählen Sie „Installieren“.

- Hinweis: Das Installationsprogramm stellt automatische eine Verbindung zum richtigen Cloud-Mandanten her. Sie müssen das Installationsprogramm nicht mit speziellen Befehlszeilen ausführen, falls Sie den Agent nicht im Hintergrund installieren möchten.
- Sie müssen Administrator-Zugangsdaten eingeben, wenn Sie den Computer mit Ihrem aktuellen Benutzer nur eingeschränkt nutzen können.
- Das Installationsprogramm ist interaktiv, wenn es auf diese Weise ausgeführt wird, und Sie können nacheinander den Download und die Installation der einzelnen Anwendungen beobachten. Je nach den auf Ihrem Computer verfügbaren Ressourcen, kann dieser Vorgang bis zu 10 Minuten in Anspruch nehmen, vermutlich jedoch weniger.

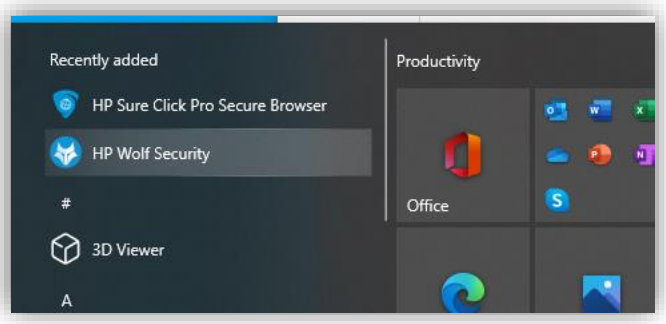




Ihnen wird im unteren rechten Bereich ein Popup-Fenster angezeigt, dass Sie zum Neustart des Computers auffordert, um die Installation abzuschließen. Sie können den Neustart über die Schaltfläche „Jetzt neu starten“ oder später durchführen. Für einen Neustart zu einem späteren Zeitpunkt klicken Sie auf das Windows-Symbol in der Ecke Ihrer Task-Leiste und wählen Sie „Ein/Aus | Neu starten“. (Wählen Sie nicht „Herunterfahren“.)

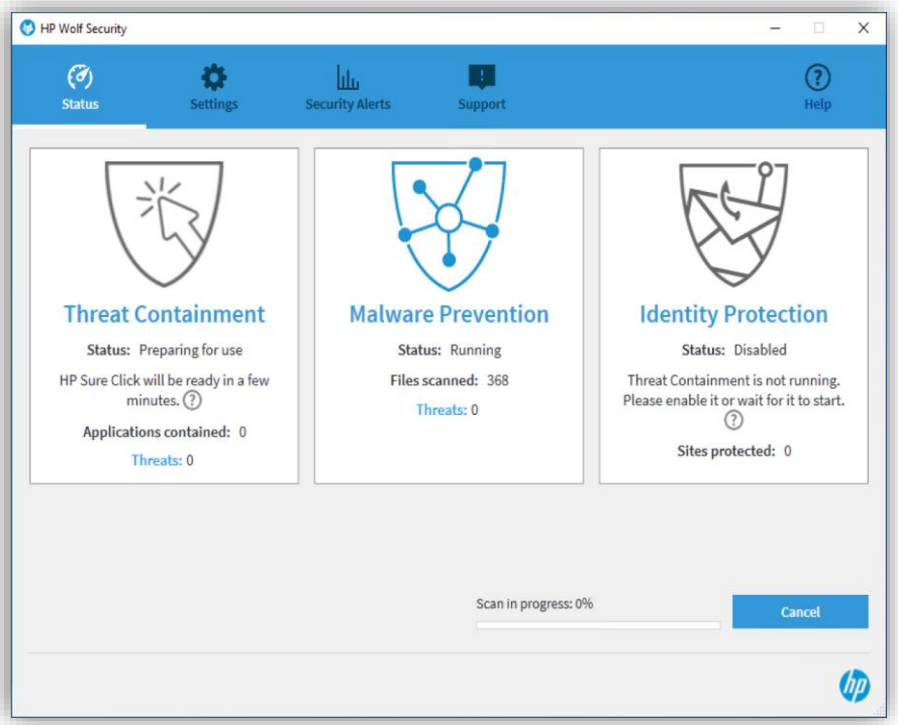


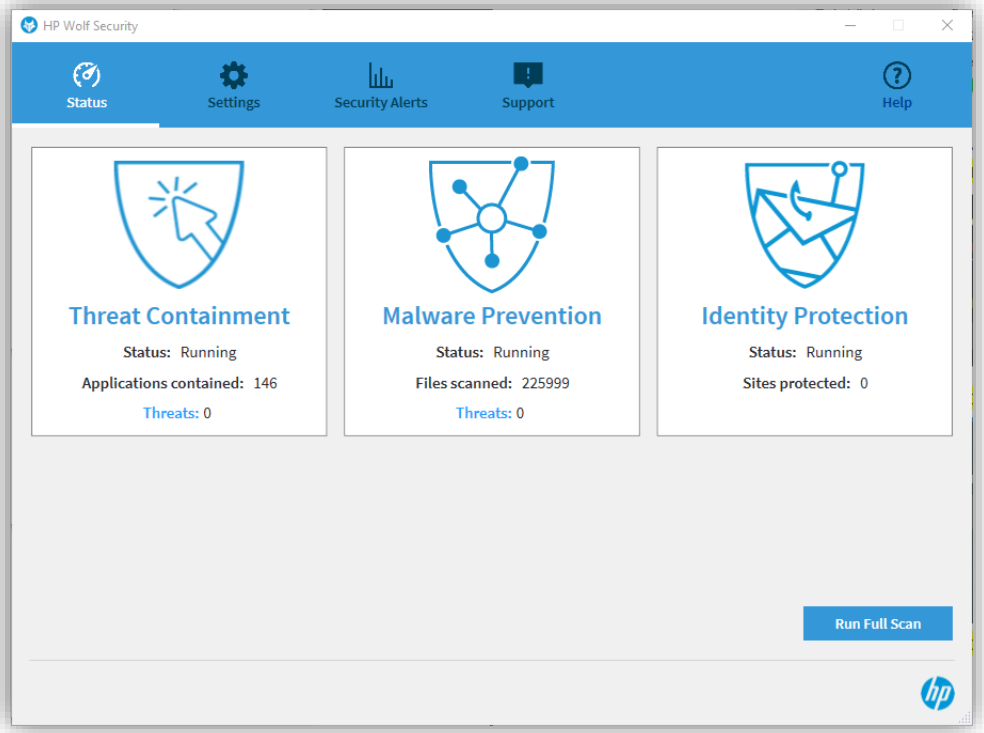
Nach dem Neustart des Computers finden Sie das HP Wolf Symbol in der Taskleiste  und alle neuen Anwendungen im Startmenü.



Der Agent führt einige Wartungsschritte durch. Diese beinhalten die Ersteinrichtung, das Herstellen einer Verbindung zum Cloud-Mandanten sowie das Ausführen eines vollständigen Scans, um den PC auf möglicherweise vorhandene schädliche Inhalte zu überprüfen. Während dieser Zeit erhalten Sie beim Öffnen der obigen „„HP Wolf Security“" Konsole eine der Folgenden ähnliche Anzeige:

Kurzanleitung – HP Wolf Pro Security





Bereitstellung für mehrere Geräte

Sie können das Installationsprogramm von jeder beliebigen zentralen Bereitstellungslösung wie SCCM oder BigFix bereitstellen. Dies ist ebenfalls über GPO und einen Filesharing-Dienst möglich.

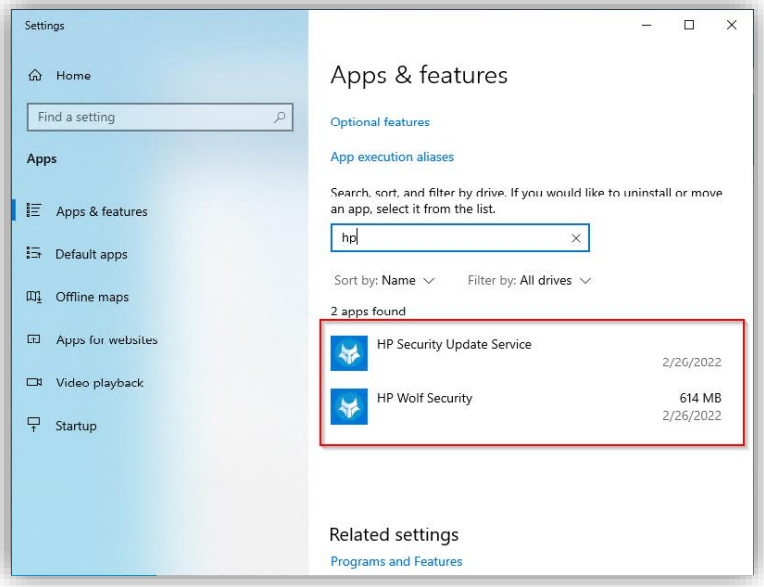
Da es sich um ein Paket vom Typ *msi* handelt, können Sie alle *Msiexec.exe* Standard-Flags wie Installation im Hintergrund oder Erstellen einer Protokolldatei verwenden.

Deinstallation des Agents

Durch die Deinstallation wird HP Wolf Pro Security von dem PC entfernt.

Hinweis: Alle nachstehend aufgeführten Komponenten müssen deinstalliert werden, um unerwartete Ergebnisse zu vermeiden. Zum Beispiel: Wenn der HP Security Update Service nicht deinstalliert wird, versucht er, den Agent erneut herunterzuladen und zu installieren. Bitte deinstallieren Sie alle nachstehenden Komponenten, um eine vollständige Deinstallation zu gewährleisten.

- Öffnen Sie in den Windows-Einstellungen den Bereich „Programme hinzufügen oder entfernen“.
- Deinstallieren Sie die Anwendungen **HP Wolf Security** und **HP Security Update Service**.



Kurzanleitung – HP Wolf Pro Security

HP Wolf Security Controller – Überblick

Hinweis: Der HP Wolf Security Controller ist nur bei Installationen mit 25 oder mehr Arbeitsplätzen verfügbar. Wenn Sie nicht zur Nutzung eines Controllers berechtigt sind, stehen Ihnen die meisten der beschriebenen Funktionen nicht zur Verfügung.

Der HP Wolf Security Controller ist Ihr Zugang zur Interaktion mit Ihrem Sicherheitsservice. Es handelt sich um einen dedizierten Controller, der nicht von anderen Kund:innen genutzt wird. Somit ist eine echte Datentrennung gewährleistet. Während manche Bedrohungsdaten anonymisiert und aggregiert werden, um die Überwachungs- und Alarmierungsprozesse zu verbessern, bleiben diese Daten innerhalb des Service und werden niemals an Händler:innen oder Drittparteien übermittelt. Das dedizierte HP Wolf Support-Team kann zu Supportzwecken auf Ihren Controller zugreifen. HP erfüllt oder übertrifft die ISO- und SOC-Compliance-Standards für Benutzer- und Administratorzugriff.

Mehr über die HP Datenschutzrichtlinie erfahren Sie hier. Klicken Sie außerdem hier, um die HP Wolf Pro Security Daten-FAQ anzuzeigen.

Diese Anleitung setzt voraus, dass Sie Ihren Controller bereits vorbereitet haben und darauf zugreifen können.

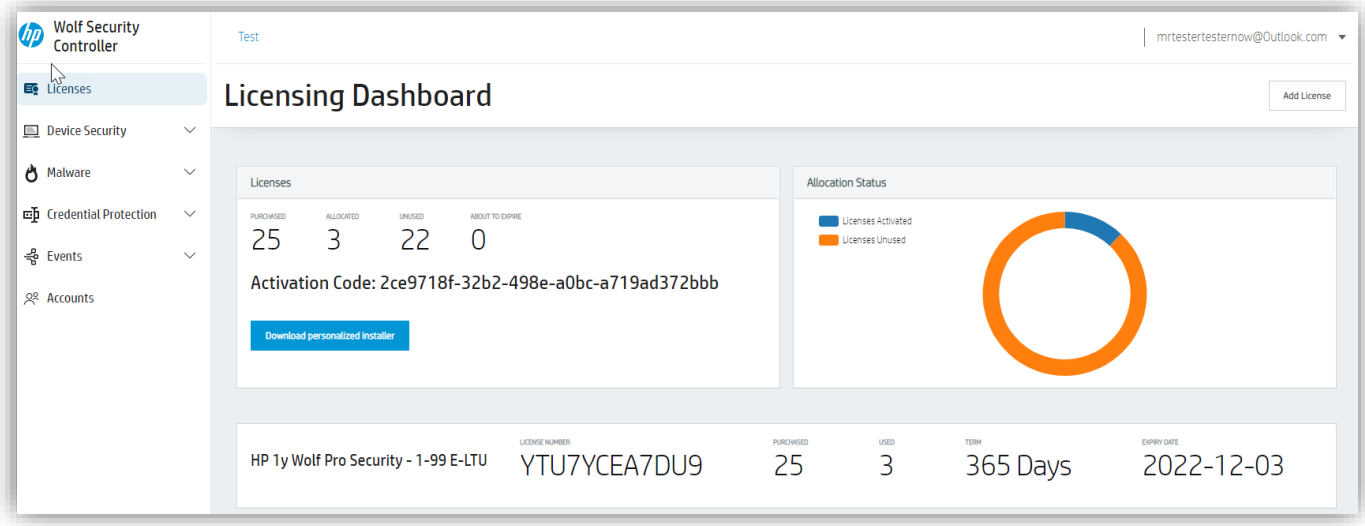
Login

Der Zugriff auf Ihren Controller erfolgt über:

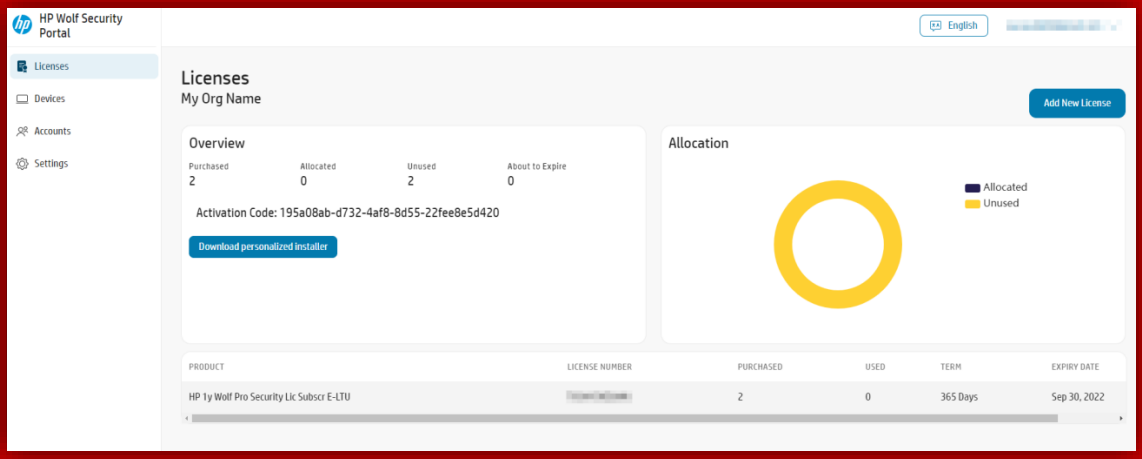
https://portal.hpwolf.com

Bei der ersten Anmeldung am Controller wird Ihnen die nachstehende Ansicht angezeigt. Die oberste Option des Menüs links ist die Seite **Lizenzen**.

Kurzanleitung – HP Wolf Pro Security



Hinweis: Wenn Sie dem Mandanten weniger als 25 Arbeitsplätze zugeordnet haben, sind für diesen nur die Bereiche „Lizenzen“ und „Konten“ anwendbar. Sie können die vollständigen Verwaltungsfunktionen durch den Kauf zusätzlicher Lizenzen aktivieren.



Lizenzen

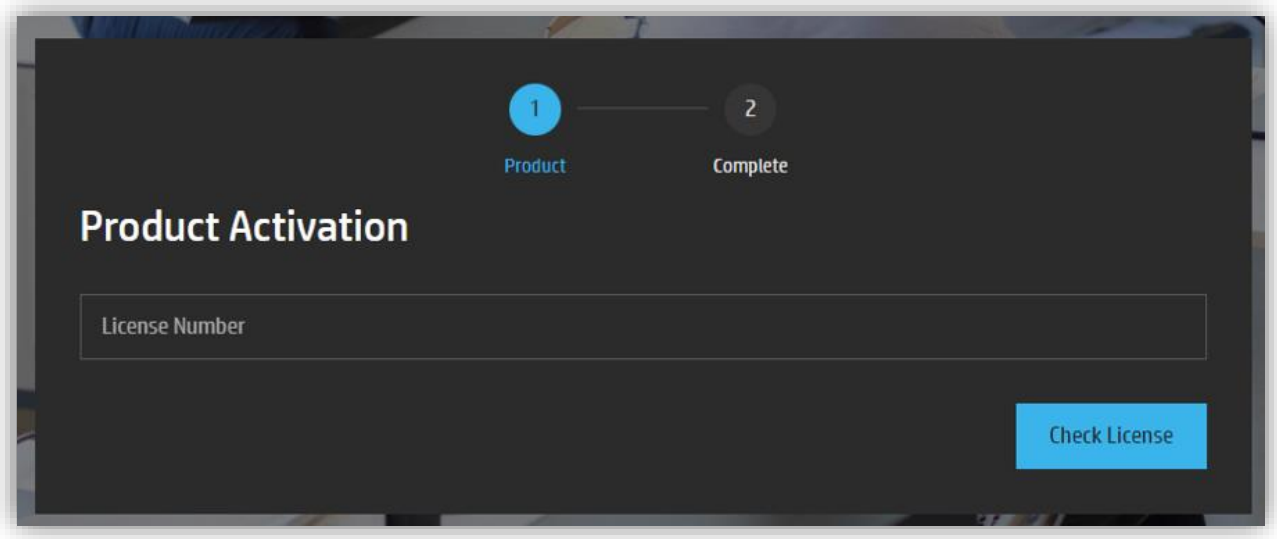
Die Seite **Lizenzen** enthält alle administrativen Daten, die Sie zur Überprüfung Ihres Kontos benötigen. Oben wird die Anzahl der erworbenen, zugeordneten, unbenutzten und ablaufenden Lizenzen angezeigt.

Hier können Sie ebenfalls das HP Wolf Pro Security Installationsprogramm (.msi) herunterladen, das speziell für Ihren Controller vorgesehen ist und mit keinerlei anderen Produkten oder Controller-Umgebungen genutzt werden kann. Im nachstehenden Abschnitt „Installation“ wird hierauf detailliert eingegangen.

Auf der Seite **Lizenzen** sehen Sie ebenfalls Ihre Lizenznummer, sowie die Restlaufzeit der Produktlizenz und können neue Lizenzschlüssel übernehmen.

Übernahme neuer Lizenzschlüssel für denselben Mandanten

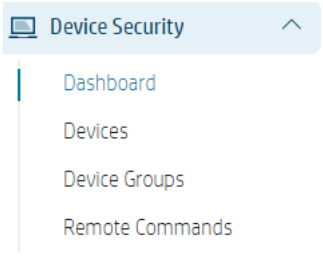
Klicken Sie in der oberen rechten Ecke der Seite auf die Option „Lizenz hinzufügen“. Geben Sie den von HP bereitgestellten Lizenzschlüssel ein und wählen Sie „Lizenz überprüfen“.



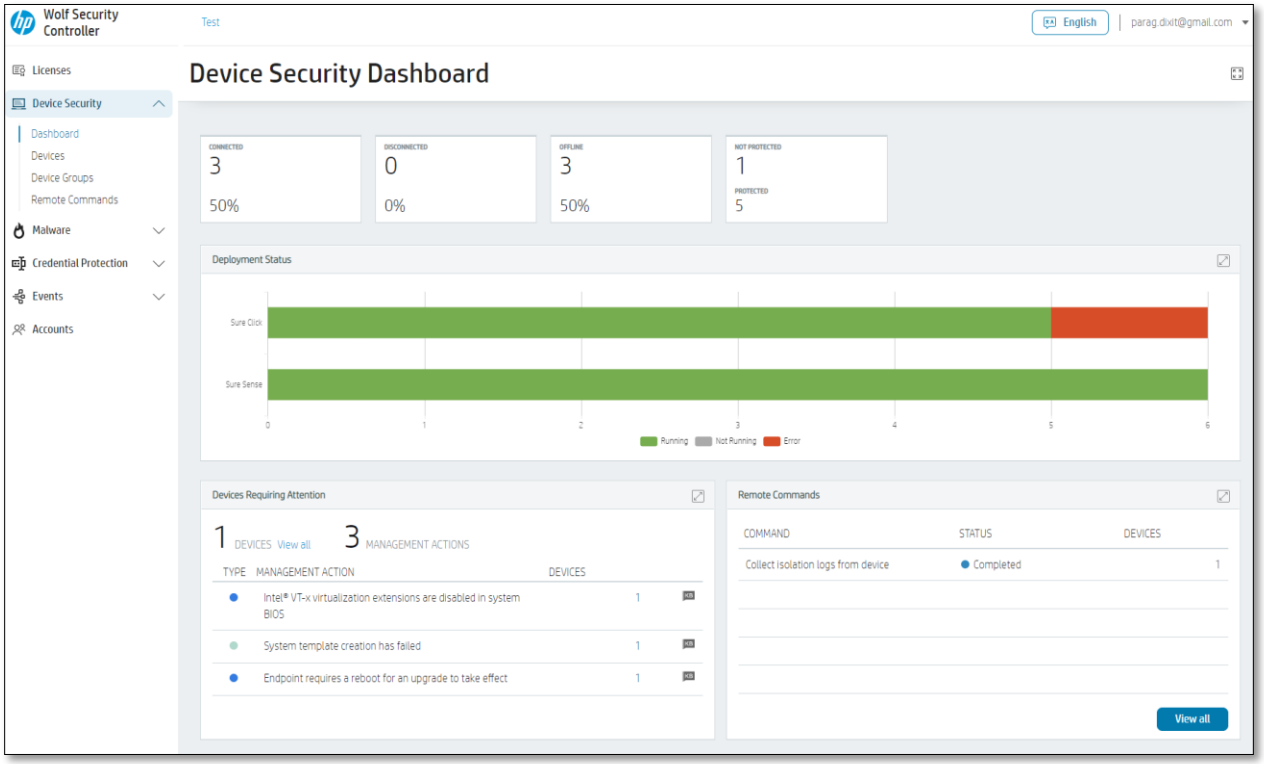
Wenn dieser Schritt abgeschlossen ist, werden auf der Seite für die Controller-Lizenzen automatisch die neue Lizenz, die Anzahl zusätzlicher Arbeitsplätze sowie die Restlaufzeit angezeigt.

Gerätesicherheit

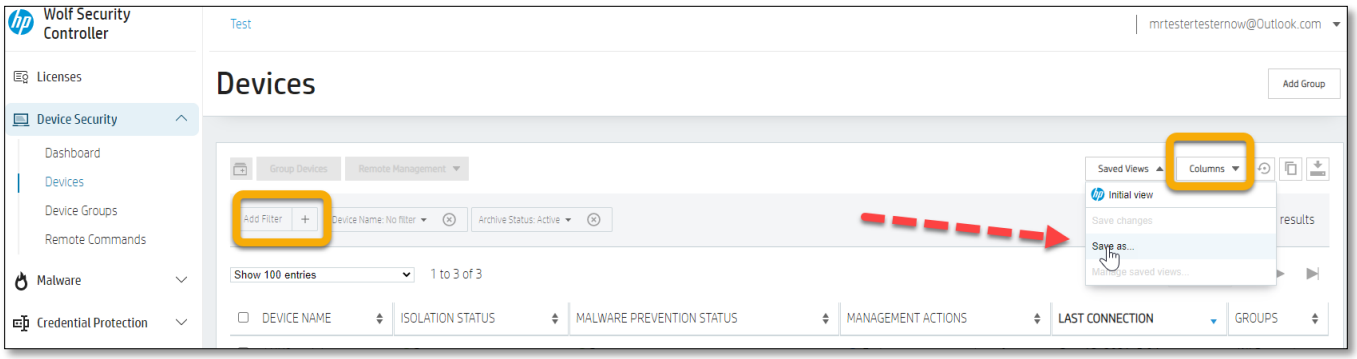
Dieser Bereich ist hilfreich für den Geräteadministrator bzw. die Geräteadministratorin oder den Sicherheitsexperten bzw. die Sicherheitsexpertin, der bzw. die für die Überwachung der Metriken in Verbindung mit dem Status der Agent-Flotte, der aktuellen Bereitstellung oder allgemeinen Fragen verantwortlich ist, wie z. B. „Wie viele Geräte sind vollständig geschützt?“ oder „Welche Geräte müssen überprüft werden?“



- Das **Dashboard** bietet Ihnen einen Überblick über die Geräte, auf denen das Produkt ausgeführt wird. Vom Dashboard aus können Sie die wichtigsten Statistiken zum Gerätestatus, den Bereitstellungsstatus insgesamt sowie die Ergebnisse von Fernbefehlen überwachen. Das Dashboard ist ausgesprochen interaktiv und Sie können auf Feld oder Objekt klicken, um weitere Details zu diesem anzeigen zu lassen.



- Unter **Geräte** sind alle diesem Mandanten zugeordneten Geräte aufgeführt. Dies ist eine sehr nützliche Seite, auf der Sie benutzerdefinierte Geräteansichten speichern können, so dass Sie nicht nach für Sie interessanten Geräten suchen müssen. Definieren Sie die Spalten und Filter nach Ihren Wünschen ein, um dieselbe Ansicht bei nachfolgenden Besuchen anzuzeigen, und wählen Sie *Speichern unter*. Vergeben Sie einen Namen für jede gespeicherte Ansicht, damit Sie diese stets zuordnen können.

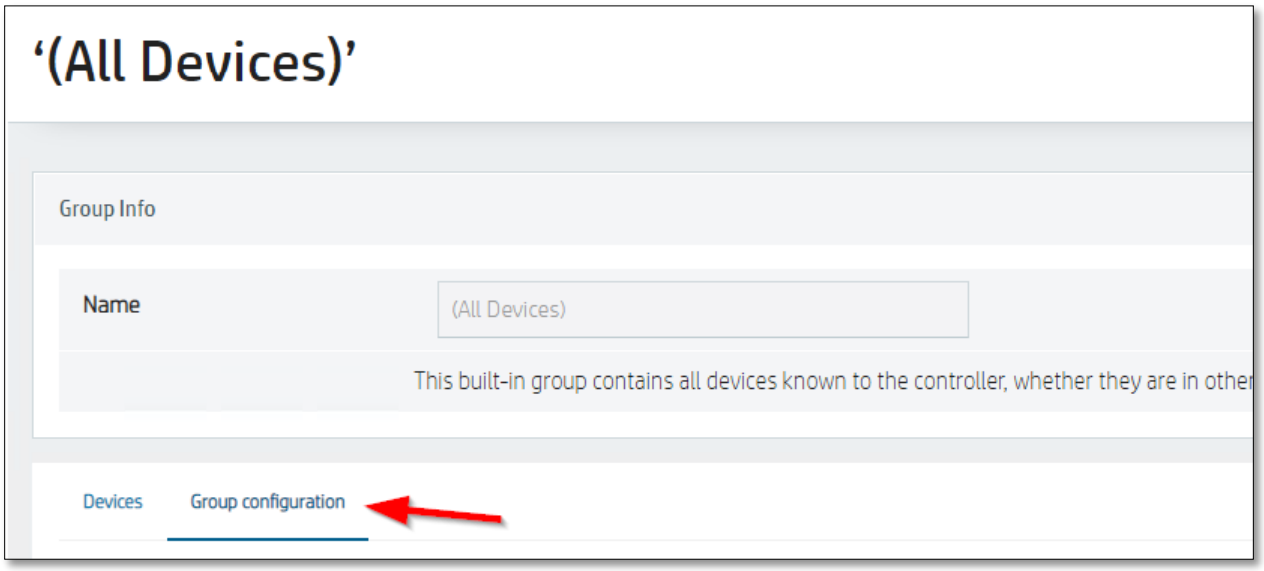


(Alle Geräte) Gruppe und Richtlinie

WPS ermöglicht die Definition bestimmter Richtlinienwerte zur Bestimmung des Produktverhaltens. Es wird dringend empfohlen, Ihre eigene ***unternehmensweite*** Richtlinie in der (Alle Geräte) Gruppe zu erstellen. Diese Richtlinie wird auf alle neuen Geräte, die für diesen Mandanten eingerichtet werden, angewendet.

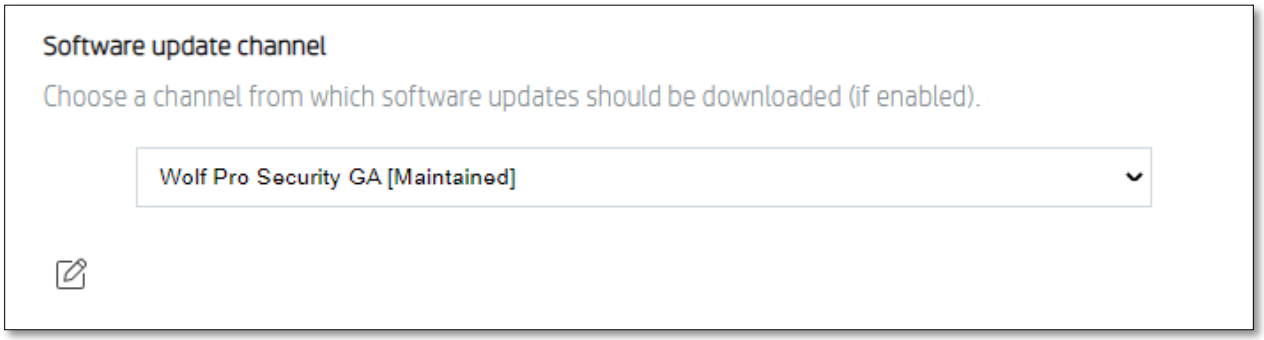
Betrachten wir die Richtlinieneinstellungen und wie sie sich auf das Verhalten des Endgeräte-Produkts auswirken:

Beginnen Sie mit einem Klick auf die ***(Alle Geräte)*** Gruppe auf der Seite **Gerätegruppen** und klicken Sie auf **Gruppenkonfiguration**



Sure Click Richtlinien-Einstellungen

Software-Update-Kanal



Wählen Sie den Software-Update-Kanal, der zur Aktualisierung der Endgeräte-Software genutzt wird. In den meisten Fällen kann hier die Standardauswahl zur Verwaltung der Software-Updates durch HP verwendet werden.

In Fällen, in denen ein neues Test oder POC-Build erforderlich ist, ist es stets besser, zunächst eine neue Gerätegruppe zu erstellen, dieser die erforderlichen Geräte hinzuzufügen und eine Richtlinie zuzuordnen,

die ihren Softwarekanal ändert. Weitere Informationen finden Sie im nächsten Abschnitt „Kundenspezifische Gerätegruppen und Richtlinien"

Vertrauenswürdige Websites

Fügen Sie hier Seiten hinzu, die vom sicheren Browser ohne Isolation geöffnet werden. Dies ist hilfreich bei internen oder bekannten vertrauenswürdigen Domains, die nicht in einer sicheren virtuellen Maschine geöffnet werden müssen.

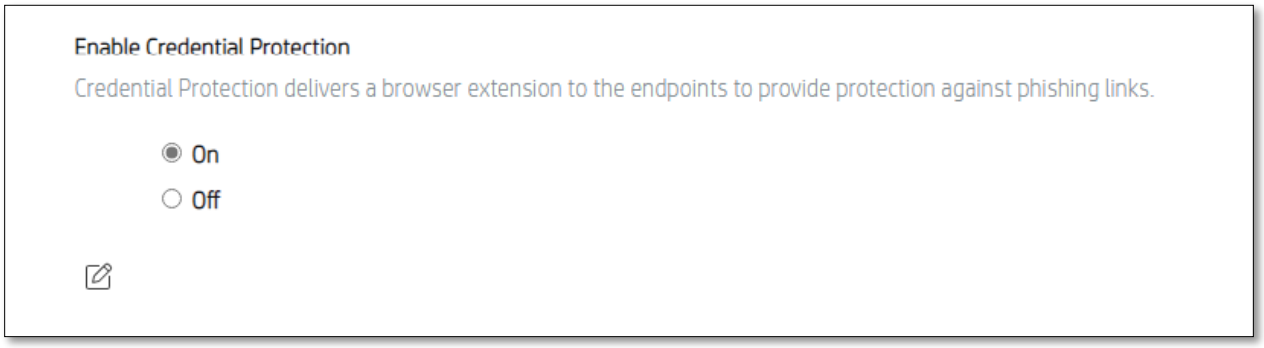
Bitte gehen Sie hier sehr sorgfältig vor, da ansonsten alle Subdomains einer TLD ebenfalls ohne Schutz geöffnet werden.

Zum Beispiel:

SICHER: https://my-company-name.sharepoint.com

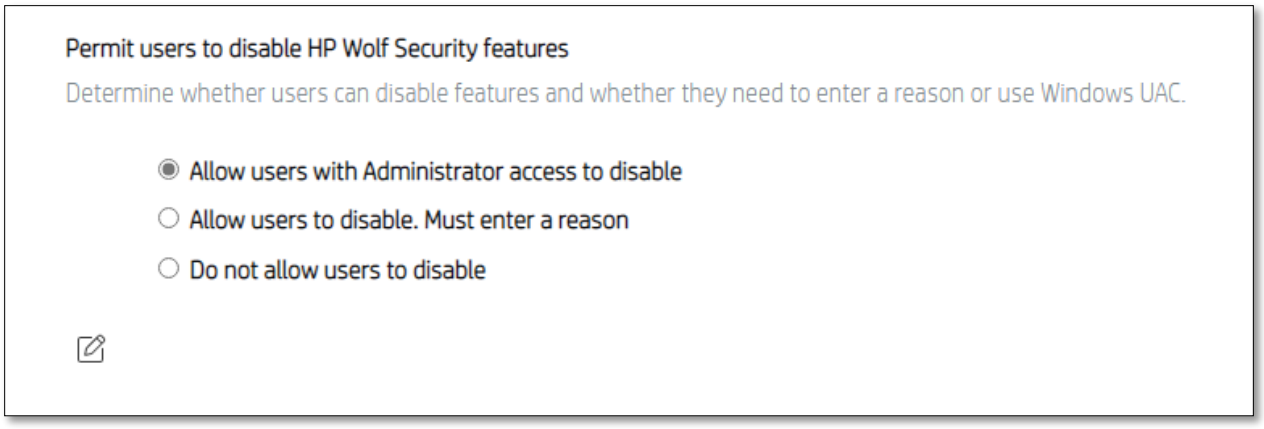
NICHT SICHER: https://sharepoint.com

Zugangsdatenschutz aktivieren



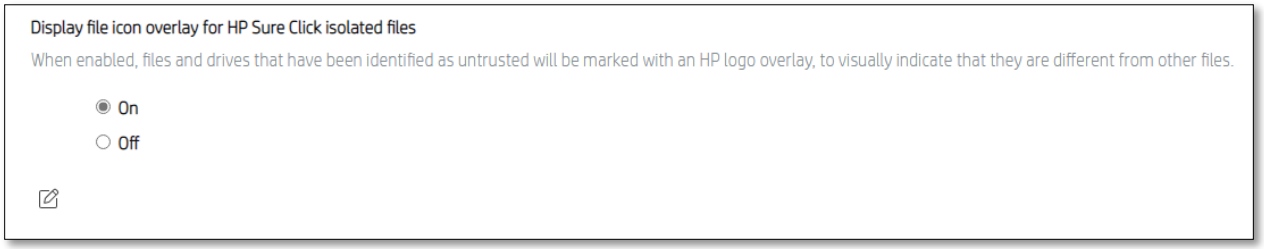
Dies schaltet die Funktion für den Zugangsdatenschutz ein oder aus Ist die Funktion AUSGESCHALTET, können die Benutzer sie am Endgerät nicht wieder EINSCHALTEN.

Benutzerkontrolle der WPS Endgerätefunktionen



Verwenden Sie diese Einstellung, wenn Sie strikte Vorgaben für das Endbenutzer-Verhalten festlegen möchten und nicht wünschen, dass Endbenutzer jegliche Schutzfunktionen deaktivieren oder nur Funktionen deaktivieren können sollen, wenn sie als lokaler Administrator angemeldet sind. Sie können ebenfalls Standard-Windows-Benutzern die Deaktivierung gestatten, hierzu müssen diese jedoch einen Grund angeben. Diese Gründe können im nachstehend beschriebenen Bereich „Ereignisse“ nachverfolgt werden.

Symbol-Overlay-Kontrolle

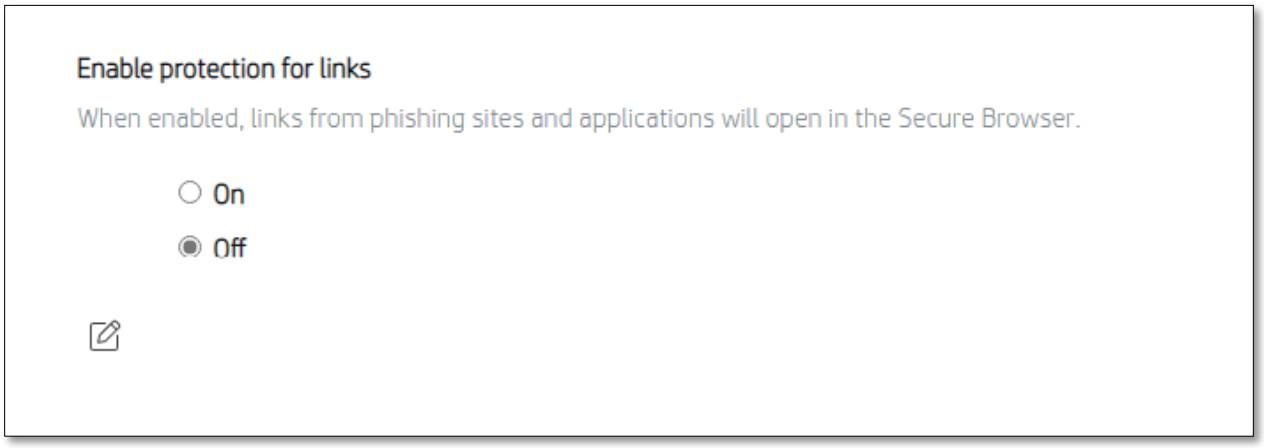


Wenn eine Datei von WPS als *nicht vertrauenswürdig* eingestuft wird, sie also aus dem Internet heruntergeladen wurde oder aus einem E-Mail-Anhang eines externen Absenders oder aus zahlreichen weiteren Eintrittspunktion stammt, wird für die Datei ein kleines Wolf Overlay-Symbol angezeigt. Dies signalisiert dem Endbenutzer bzw. der Endbenutzerin, dass die Datei durch WPS geschützt und stets isoliert geöffnet wird.

Diese Richtlinien-Einstellung entfernt dieses Overlay-Symbol.

Hinweis: Diese Einstellung ist hilfreich, wenn sich Ihre Beschäftigten angewöhnen, den Schutz von Dateien zu entfernen, bevor sie damit arbeiten. Das Entfernen des Schutzes von Dokumenten ist in nahezu allen Fällen unnötig, da WPS den Benutzer:innen ermöglicht, die Dokumente lokale zu bearbeiten und zu speichern, während sie in einem isolierten Container geöffnet sind.

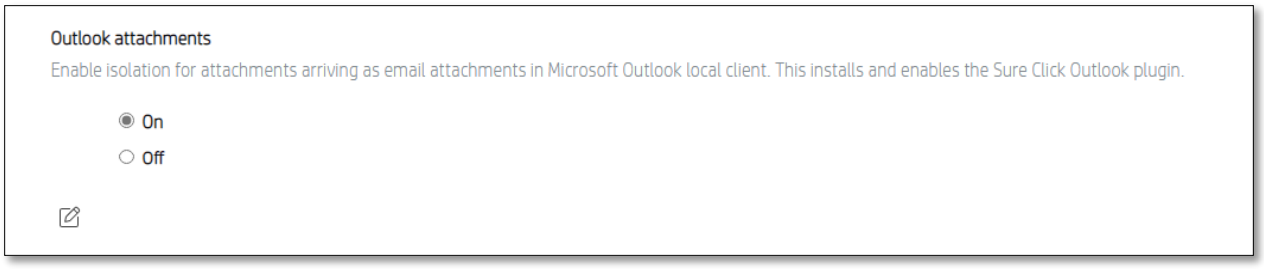
Linkschutz



Der Linkschutz arbeitet in Verbindung mit der Liste vertrauenswürdiger Seiten. Wenn diese Einstellung EINGESCHALTET ist, werden alle Links in E-Mails, Chats oder Link-Eintrittspunkten unabhängig vom festgelegten Standard-Browser in einem sicheren Browser geöffnet. Befindet sich der Link auf der Liste vertrauenswürdiger Seiten, wird er im Standard-Browser geöffnet.

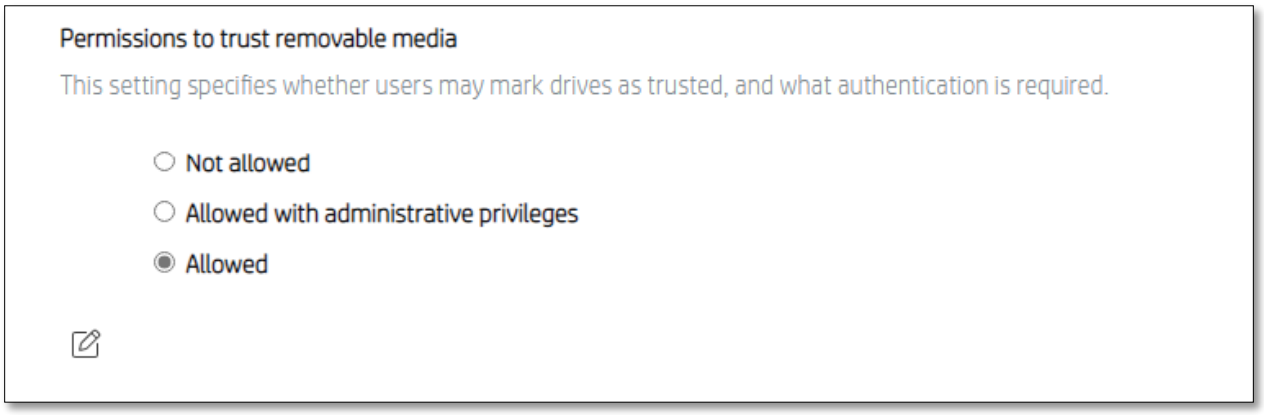
Hinweis: Nutzen Sie diese Einstellung mit Vorsicht. Sie ist üblicherweise nicht erforderlich, denn die meisten Eintrittspunkte für Malware sind heute Dokumente, die von schädlichen Websites heruntergeladen werden. Unabhängig von dieser Einstellung oder der Liste vertrauenswürdiger Seiten werden heruntergeladene Dateien stets als nicht vertrauenswürdig angesehen.

Outlook-Anhänge



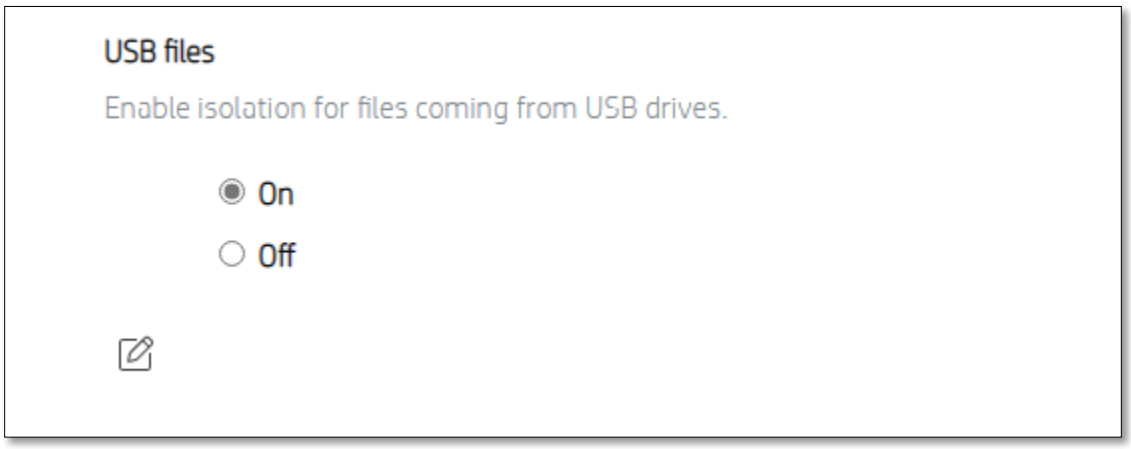
Diese Einstellung ist speziell für Microsoft Outlook vorgesehen. Verwenden Sie die Einstellung, wenn Sie die Isolation von Dateien ermöglichen möchten, die als Anhänge in Outlook-E-Mails empfangen werden. die Empfehlung ist, diese Einstellung EINGESCHALTET zu lassen.

Einstellungen für Wechseldatenträger



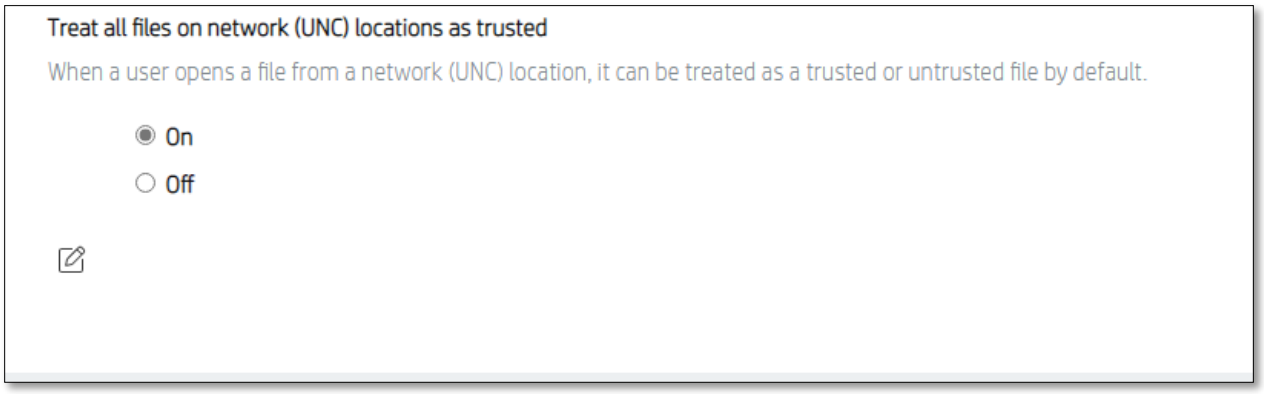
Bitte beachten Sie, dass diese Einstellung keinen Ersatz für die Gerätekontrolle darstellt. Sie bietet den Endbenutzer:innen schlicht die Möglichkeit, mit dem PC verbundene Wechseldatenträger als vertrauenswürdig einzustufen. Standardmäßig werden Dateien auf dem Datenträger als nicht vertrauenswürdig eingestuft und daher isoliert geöffnet. Wenn Sie ein engmaschigeres Sicherheitskonstrukt wünschen, setzen Sie diese Einstellung auf „Nicht erlaubt“ oder auf „„Nur mit lokalen Admin-Berechtigungen erlaubt“.

USB-Laufwerkskontrolle



Diese Einstellung bestimmt, ob USB-Geräte als vertrauenswürdig eingestuft werden. Ist sie EINGESCHALTET und werden Dateien auf einem USB-Laufwerk vom Endbenutzer-PC aus geöffnet oder auf diesen kopiert, werden diese als nicht vertrauenswürdig eingestuft und isoliert geöffnet.

Netzwerk (UNC) Laufwerkskontrolle



Wird eine Datei von einem Ort innerhalb des Netzwerks aus geöffnet, kann dies isoliert erfolgen, wenn die Einstellung EINGESCHALTET ist

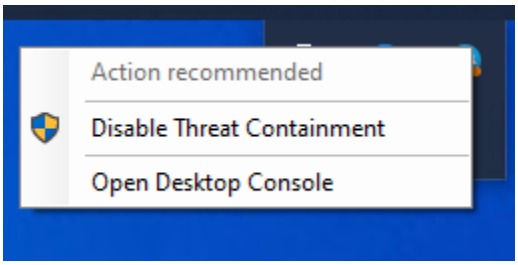
Sure Sense Richtlinieneinstellungen

Die folgenden Richtlinieneinstellungen sind für den NGAV-Bereich von WPS konfigurierbar

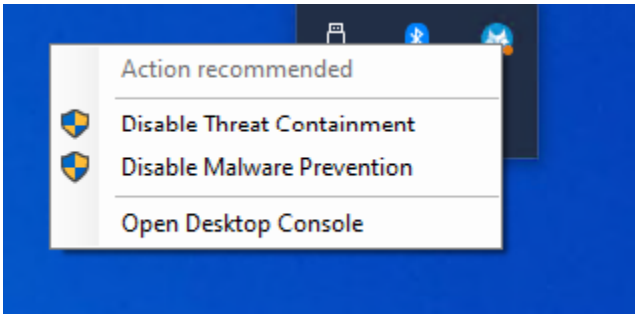
Sure Sense aktivieren/deaktivieren

Dies ermöglicht Ihnen die Konfiguration des NGAV-Status am Endgerät. Erfolgt eine **Aktivierung** oder **Deaktivierung** über diese Richtlinie, bleibt die NGAV-Lösung am Endgerät entweder aktiviert oder deaktiviert und der Benutzer kann diesen Zustand nicht ändern.

Erfolgt über diese Richtlinie eine **Aktivierung** oder **Deaktivierung** wird die Benutzeroption zur Aktivierung oder Deaktivierung des Malwareschutzes am Endgerät automatisch verborgen.



Wenn hier „Aktivierung/Deaktivierung durch lokalen Endgeräte-Admin erlauben“ ausgewählt ist, bleibt die letzte Endgeräte-Einstellung für den Malwareschutz erhalten und der Benutzer bwz. die Benutzerin kann diese wunschgemäß aktivieren oder deaktivieren.

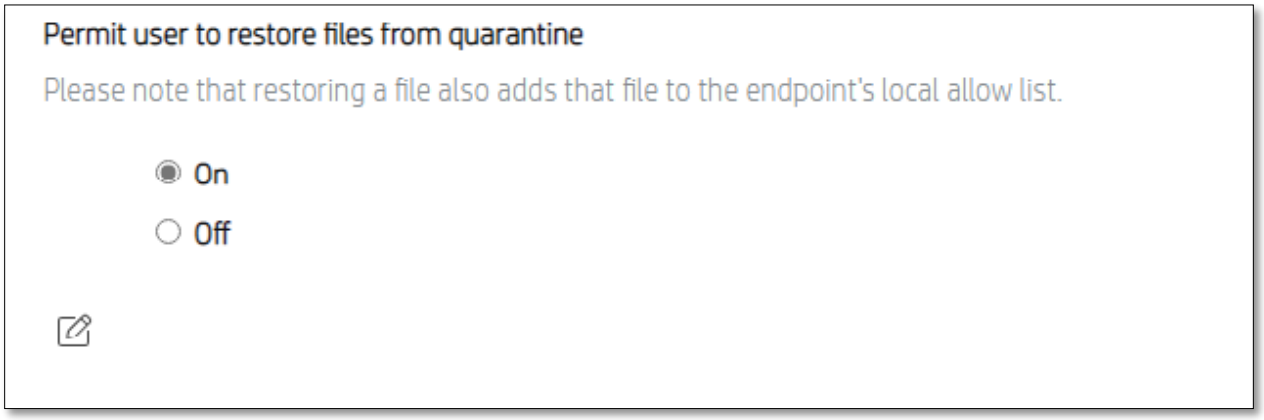


Kontrolle der lokalen Ausschlussliste

Diese Einstellung kontrolliert, ob der Benutzer die NGAV-Ausschlusslisten an seinem Endgerät bearbeiten darf. Verwenden Sie diese Option, wenn Sie vermuten, dass Benutzer :innenmöglicherweise unerwünschte Prozesse oder Dateien in die Ausschlussliste aufnehmen (wie c:\).

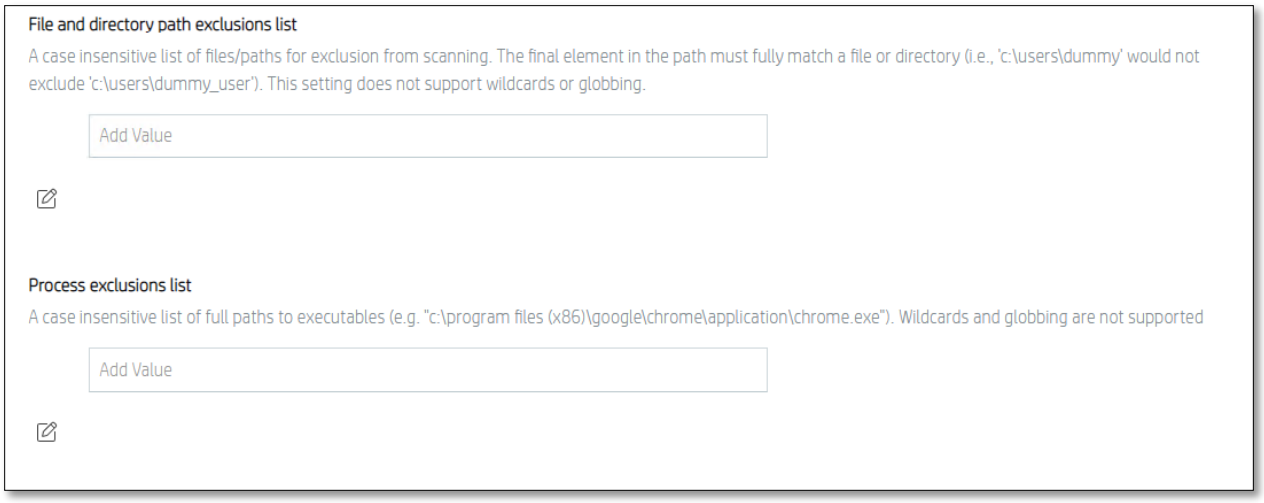
Ist diese Einstellung AUSGESCHALTET, wird die Registerkarte „Ausschlüsse“ auf der Seite „Einstellungen“ ausgeblendet und der Benutzer darf keine Ausschlüsse definieren.

Kontrolle der lokalen Quarantäneliste



Ist diese Einstellung ausgeschaltet, darf der Benutzer bzw.. die Benutzerin keine bereits in Quarantäne verschobenen Dateien auf dem Endgerät wiederherstellen. Die Dateien bleiben auf der Quarantäneliste.

Kontrolle der Ausschlussliste



Dies ermöglicht dem IT-Admin Datei-, Ordner- und Prozessausschlüsse über eine Richtlinie hinzuzufügen, so dass sie auf alle Geräte innerhalb der Gruppe angewendet werden, für die diese Richtlinie gilt. Die hier angegebenen Dateien, Ordner oder Prozesse werden von allen NGAV-Scans ausgeschlossen.

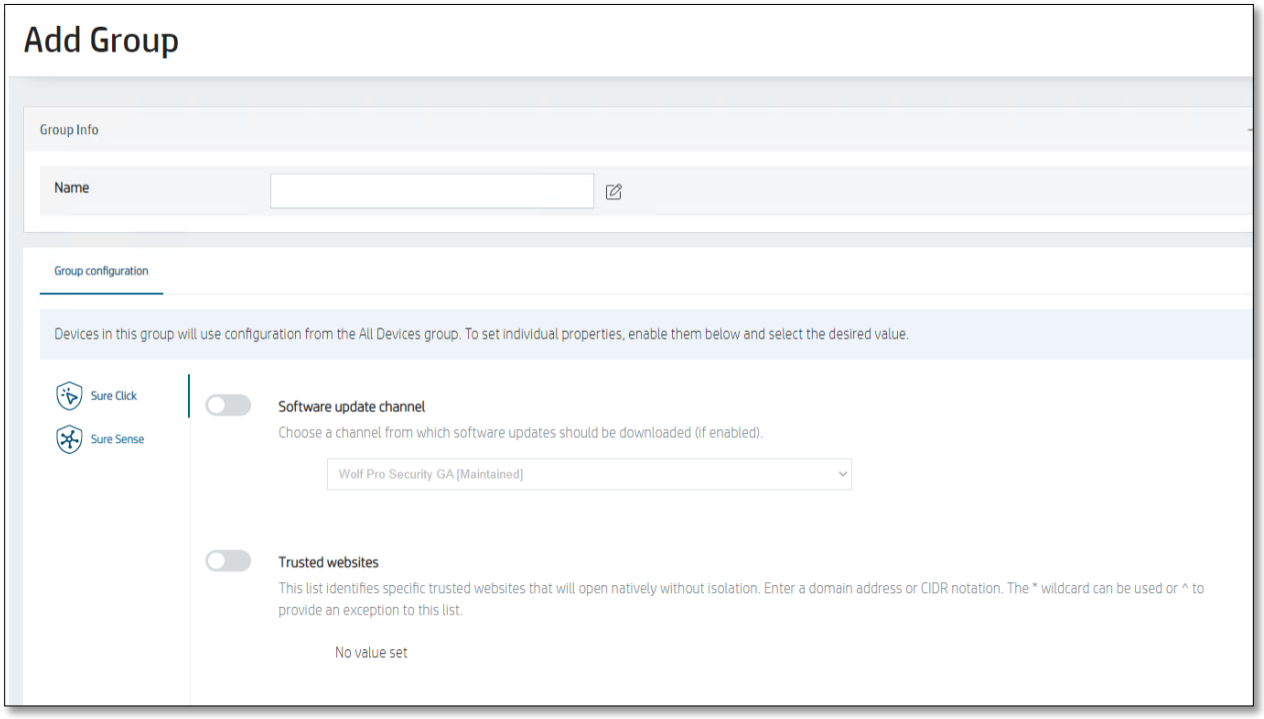
Untergruppen-Richtlinien-Einstellungen

Der obige Abschnitt beschäftigte sich damit, wie eine Richtlinie für alle Geräte konfiguriert wird. Dies sollte Ihre unternehmensweite Richtlinie sein.

In manchen Situationen jedoch benötigen Sie möglicherweise andere Richtlinieneinstellungen für bestimmte Geräte oder eine ausgewählte Gerätegruppe.

Der Bereich/die Seite **Geräte** bietet die Möglichkeit, **Gerätegruppen** zu erstellen, für die eine spezielle Richtlinie gilt. Wählen Sie hierzu zunächst „Gruppe hinzufügen“.

Auf der Seite **Gruppe hinzufügen** können Sie eine Gruppe mit einem neuen Namen und einer neuen Richtlinie erstellen.

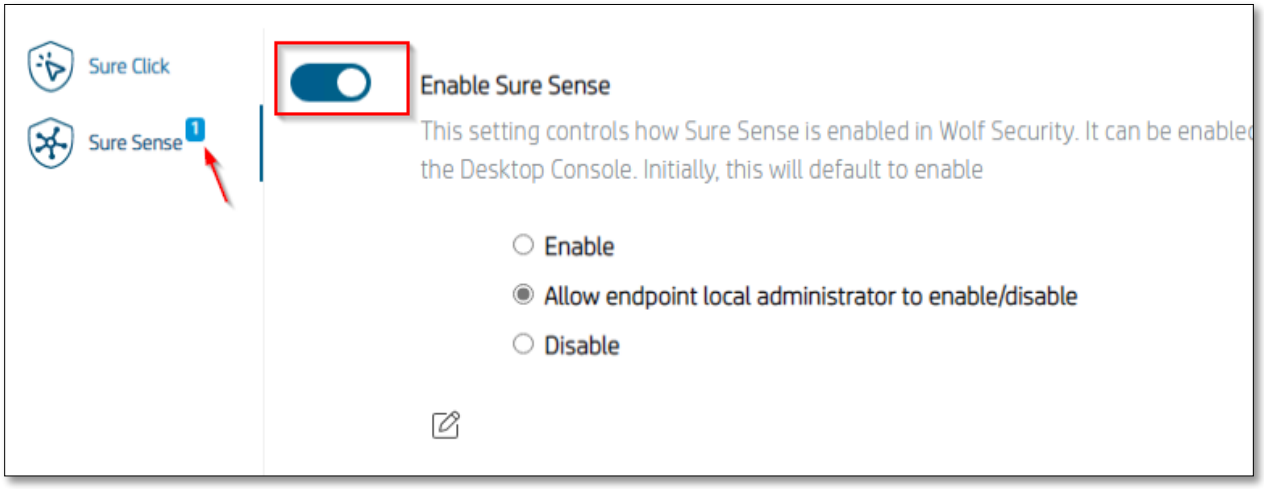


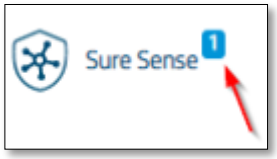
Wenn Sie einer Gruppe lediglich neue Geräte hinzufügen möchten, ohne jegliche Richtlinienwerte zu definieren (z. B. zur einfachen Überwachung des Status einer Untergruppe von Geräten) vergeben Sie einfach die Bezeichnung für die Gruppe auf der obigen Seite, speichern Sie die Gruppe und fügen Sie ihr dann Geräte hinzu.

Das Definieren einer Richtlinie für eine neue Gruppe ist optional.

Ist keine Richtlinie definiert, übernehmen die Geräte innerhalb der Gruppe automatisch die Richtlinien der (Alle Geräte) Gruppe.

Wenn Sie eine Richtlinie für die Gruppe definieren möchten, geben Sie an, welche Richtlinieneinstellungen der (Alle Geräte) Gruppe Sie außer Kraft setzen möchten, indem Sie den Schalter wie nachstehend dargestellt umstellen und den neuen Wert festlegen:

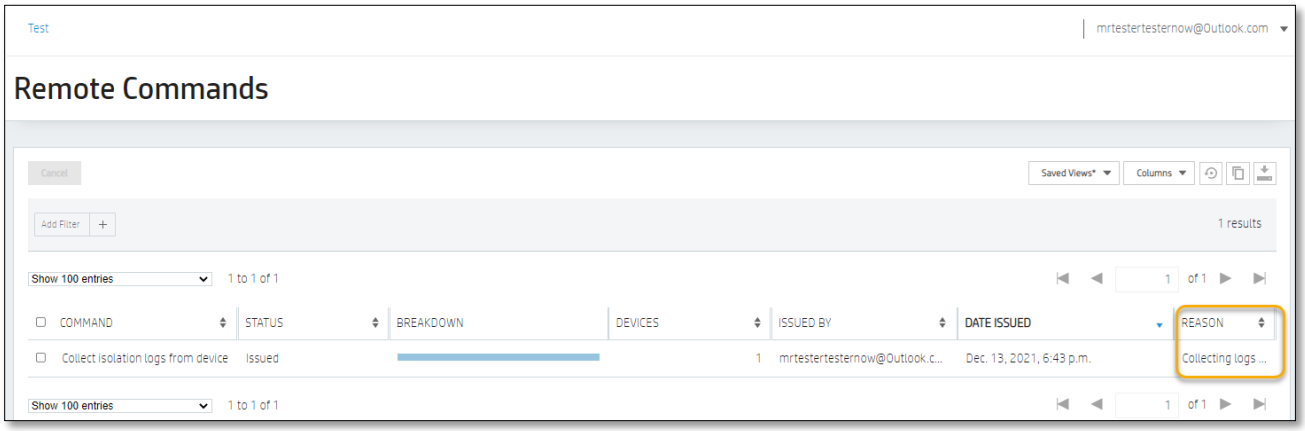




Alle anderen Richtlinieneinstellungen können unverändert bleiben. Die Meldung zeigt an, wie viele Richtlinien in der neuen Gruppe aktiviert wurden

Remote-Befehle

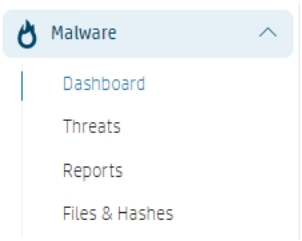
Unter „Remote-Befehle“ sehen Sie alle vorherigen und aktuell in der Warteschlange befindlichen *Befehle*, die von diesem Controller ausgegeben wurden. Zu Auditzwecken setzt HP stets eine Fallnummer sowie ein Datum in dieses Feld ein. Sie müssen die Spalten sowie den Grund auswählen, um diese in ihre Ansicht einzuschließen. Sie können diese Ansicht ebenfalls speichern, um sie nicht erneut hinzufügen zu müssen. Weitere Informationen zu Remote-Befehlen finden Sie nachstehend unter **Erklärung der Remote-Befehle**.

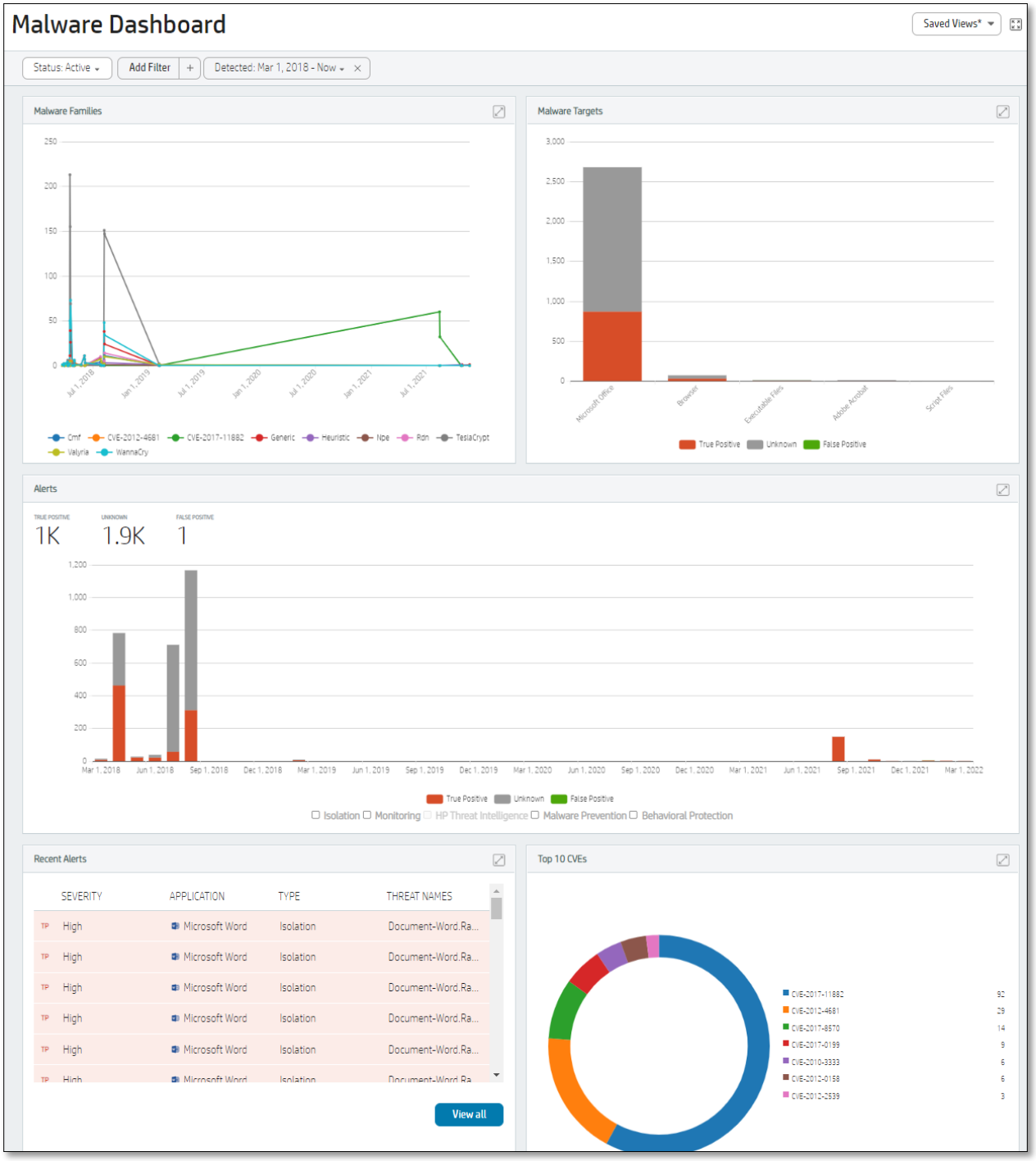


Malware

Der Bereich „Malware“ ist hilfreich für den für die Sicherheit verantwortlichen Analyst:innen oder IT-Administrator:innen innerhalb des Unternehmens. Alle unsere Technologien generieren bedrohungsbasierte Ereignisse, die Sie öffnen und analysieren können.

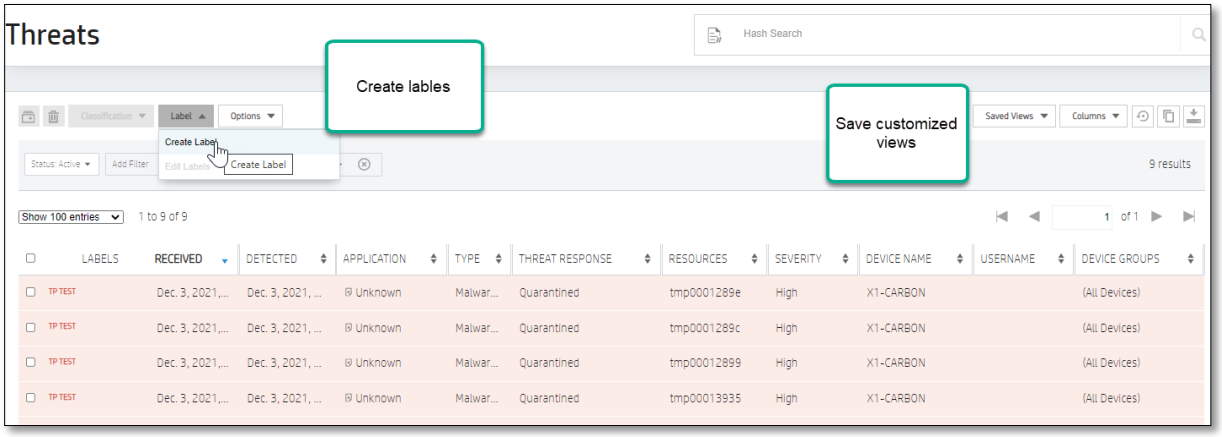
- Das **Dashboard** bietet Ihnen eine Ansicht der in der Umgebung erkannten Bedrohungen sowie der risikobehafteten Computer.



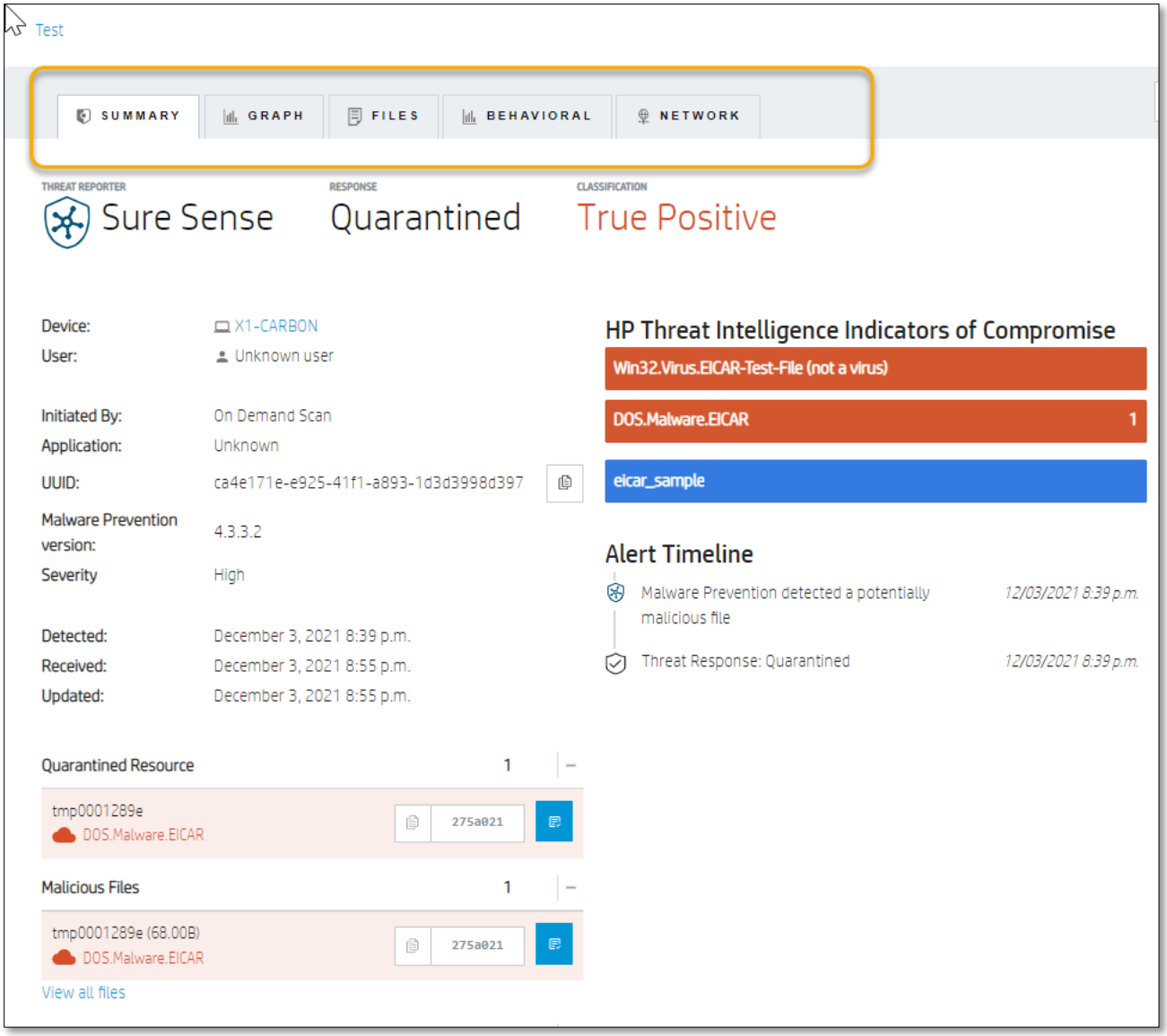


- **Bedrohungen** liefert eine Listenansicht mit der Möglichkeit, Ansichten zu sortieren und zu speichern. Hier verbringt der Analyst einen Großteil seiner Zeit mit der Untersuchung von Ereignissen. Sie können Kennzeichnungen wie „Muss untersucht werden“ für Bedrohungen

vergeben und so die internen Teams bei der Überwachung von Gefahren unterstützen, die bereits abgewendet wurden.



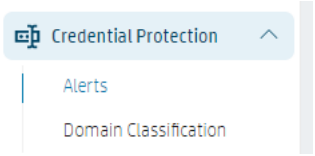
- Unter **Bedrohungen** haben Sie ebenfalls die Möglichkeit zum Anklicken und Untersuchen. Innerhalb eines Ereignisses können Sie die Informationen für weitere Untersuchungen der Bedrohung nutzen.



- Unter **Berichte** haben Sie gegenwärtig die Möglichkeit, einen Sicherheitsbericht zu erstellen und anzuzeigen, der Bedrohungen hervorhebt, die Sie in der Umgebung beobachtet haben
- **Dateien & Hashes** liefert eine Liste aller erlaubten Ausnahmen in Ihrem Controller. Hilfreich für eine Prüfliste.

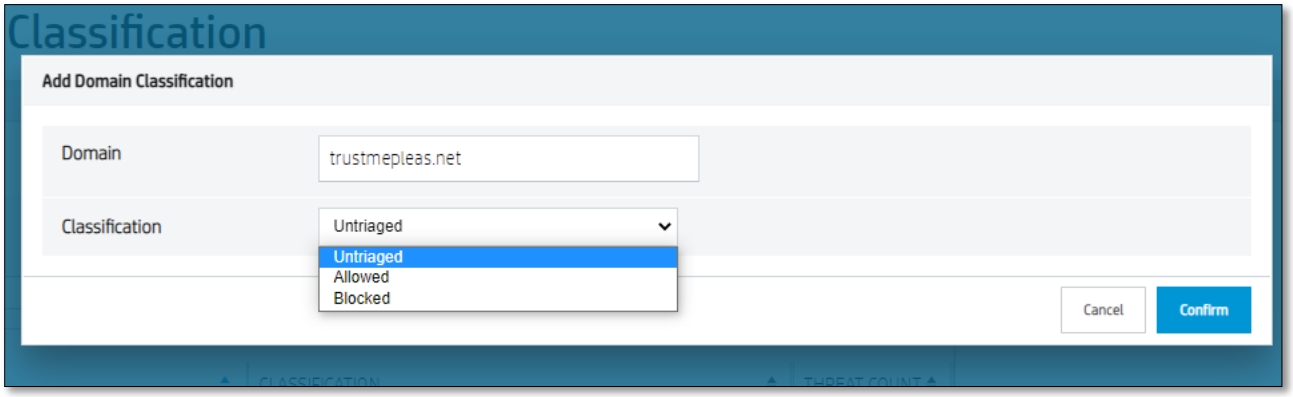
Zugangsdatenschutz

Der Zugangsdatenschutz ist hilfreich für alle Benutzer, die mit Drittparteien zusammenarbeiten und ein Ziel für Phishing-Attacken darstellen. Hier können Sie anzeigen lassen, was durch den Zugangsdatenschutz innerhalb Ihres Unternehmens gekennzeichnet oder blockiert wurde, um Phishing-Attacken abzuwehren



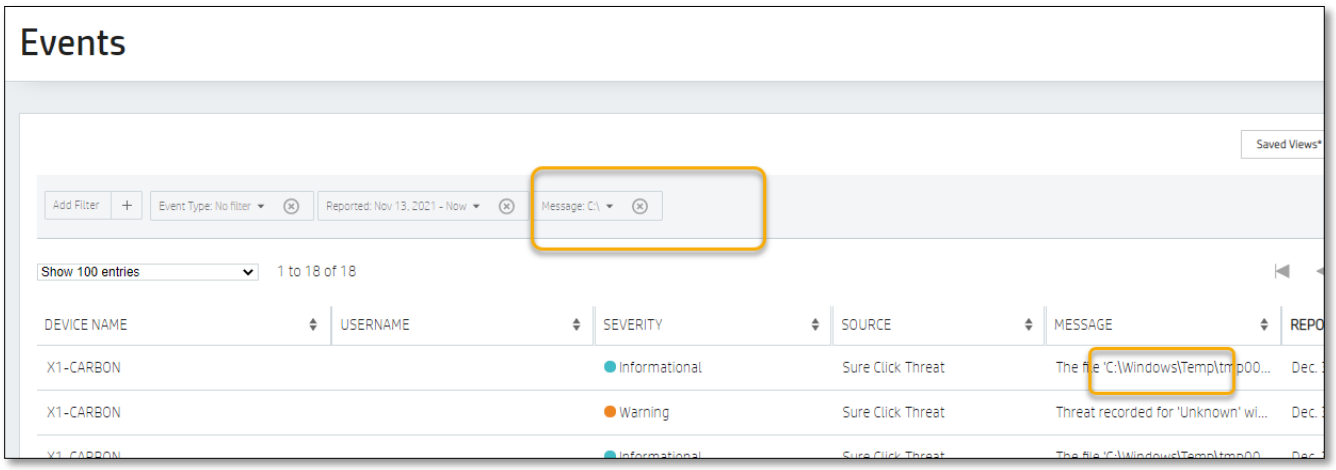
- Unter **Alarme** erhalten Sie eine Listenansicht aller Erkennungen oder Blockierungen innerhalb Ihres Unternehmens. Sie können ebenfalls gespeicherte Ansichten basierend auf den von Ihnen gewünschten Informationen erstellen.

- Die **Domain-Klassifizierung** bietet die Möglichkeit, Seiten außer Kraft zu setzen, die falsch eingestuft wurden oder die Sie zulassen möchten, wie eine interne Portalanmeldung. Sie können die Klassifizierung hier ändern.



Ereignisse

Dieser Bereich ist hilfreich für den Geräteadministrator oder den Sicherheitsspezialisten, der für die Überwachung der Metriken in Verbindung mit dem Status der Agent-Flotte, der aktuellen Bereitstellung oder speziellen Fragen verantwortlich ist, wie z. B. „Wann erfolgte die letzte Initialisierung eines Computers?“ oder „Wie viele Geräte haben eine Datei in C:\Windows\temp als vertrauenswürdig behandelt?“



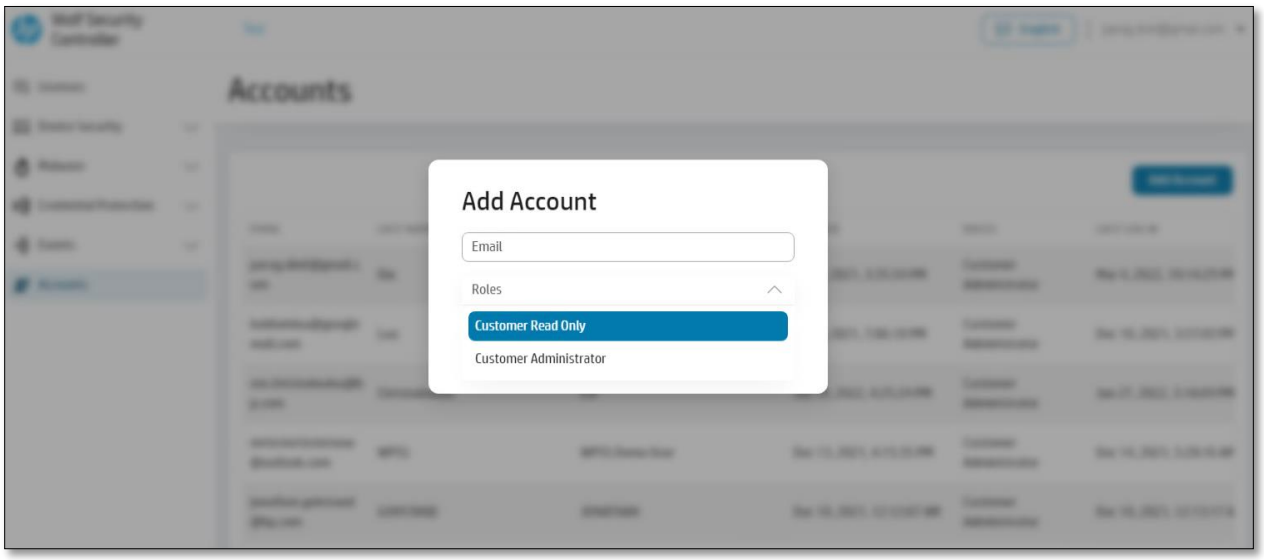
Konten

Bei der Ersteinrichtung Ihres Controllers (möglicherweise in Ihrem Auftrag durch HP oder einen Partner) hatten Sie die Möglichkeit, Benutzerk:innen hinzuzufügen. Sie können zu einem beliebigen späteren Zeitpunkt weiterhin Benutzer:innen hinzufügen, wenn Sie über „Kundenadministrator“-Rechte verfügen. Navigieren Sie einfach zur Seite **Konten** und wählen Sie „Konto hinzufügen“. Geben Sie eine E-Mail-Adresse für den neuen Benutzer bzw. die neue Benutzerin an sowie die Zugriffsstufe, die Sie diesem bzw. dieser zuordnen möchten.

Es stehen 2 Zugriffsstufen zur Auswahl.

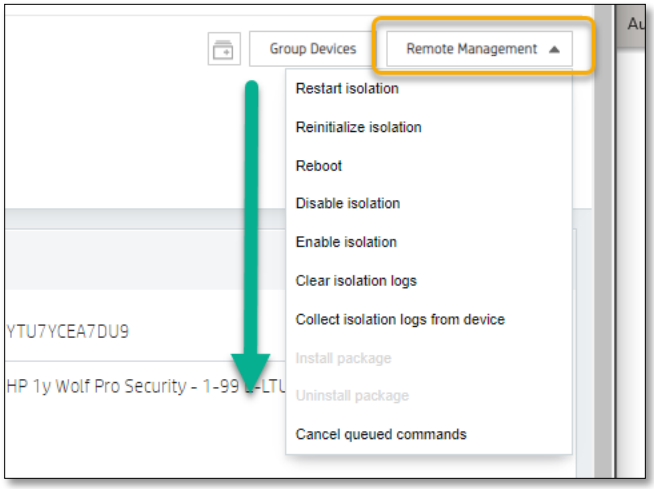
Kundenadministrator :in – Der Administrator bzw. die Administratorin kann Änderungen im Controller vornehmen.

Kunde bzw. Kundin mit reinem Lesezugriff – Kann die Controller-Einstellungen und Berichte nur anzeigen lassen.



Erklärung der Remote-Befehle

Remote-Befehle sind eine Möglichkeit, Ihre bereitgestellten Computer über den Controller zu verwalten. Nachstehend finden Sie eine Übersicht der Befehle zur Verwaltung Ihrer Computer. Remote-Management-Optionen finden Sie auf mehreren bereits behandelten Seiten. Rufen Sie einfach das Dropdown-Menü auf, um den gewünschten Befehl zu finden.



- Isolation neu starten – Dieser Befehl bezieht sich speziell auf die Bedrohungseindämmung und kann Probleme beheben, mit denen die Software auf dem Computer konfrontiert ist. Dieser Befehl wird nur selten benötigt.

- Isolation reinitialisieren – Dieser Befehl bezieht sich speziell auf die Bedrohungseindämmung und sollte als erster Schritt zur Fehlerbehebung auf jedem Gerät ausgeführt werden, auf dem Probleme auftreten.

- Neustart – ACHTUNG! Dieser Befehl erzwingt einen Windows-Neustart auf dem Computer des Endbenutzers ohne vorherige Warnung. Sämtliche nicht gespeicherten Arbeiten auf dem Gerät gehen verloren. Der Benutzer bzw. die Benutzerin kann den sofortigen Neustart nicht verhindern oder verzögern.

- Isolation deaktivieren – Dieser Remote-Befehl entspricht dem Befehl über die Computer-Desktop-Konsole. Er deaktiviert die Funktion zur Bedrohungseindämmung, üblicherweise zur Fehlerbehebung.

- Isolation aktivieren – Das Gegenteil von „Deaktivieren“. Kann ebenfalls über die Computer-Desktop-Konsole ausgeführt werden.

- Klare Isolationsprotokolle – Die Erstellung kann vom Support vor dem Beginn einer Fehlersuche bei bestimmten Problemen verlangt werden.

- Erfassen von Isolationsprotokollen des Geräts – Hierdurch werden die Agent-Protokolle auf den Controller geladen und können später vom Support abgerufen werden.

- Befehle in der Warteschlange abbrechen – Dies kann hilfreich sein, wenn Sie einen Remote-Befehl an eine große Geräteflotte gesendet haben und den ursprünglichen Befehl aufgrund von Timing-Problemen beenden möchten.

Tipps zur Fehlerbehebung

Nachstehend finden Sie eine Reihe von Schritten, mit denen Sie als IT-Administrator:in bei der Lösung eines Problems unterstützen können.

Ermitteln Sie zunächst, welche Funktion das Problem verursacht

Üblicherweise lässt sich schnell bestimmen, welches Produkt Probleme verursacht. Befolgen Sie die nachstehenden Abläufe, um das Produkt zu bestimmen und eine Supportanfrage vorzubereiten, falls erforderlich.

Wenn Sie Probleme mit Office-Dokumenten oder dem Öffnen von Dokumenten in VMs haben, besteht eine schnelle Lösungsmöglichkeit in der „Reinitialisierung“. Sie können zunächst eine Überprüfung durchführen, indem Sie die Bedrohungseindämmung deaktivieren.

Triage-Ablauf der Bedrohungseindämmung

Deaktivieren Sie die Bedrohungseindämmung.

Wird das Problem hierdurch gelöst?

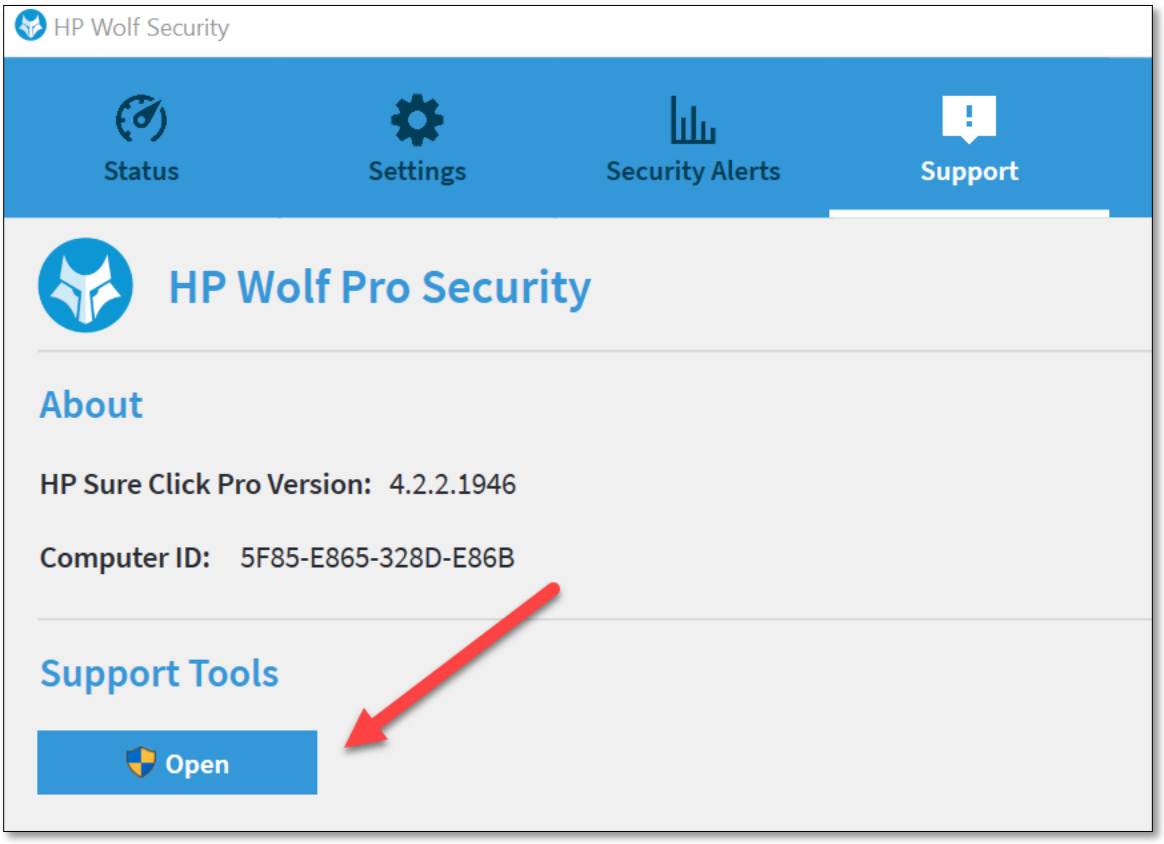
Ja: Versuchen wir, es zu beheben. Fahren Sie mit den nachfolgenden Schritten fort.

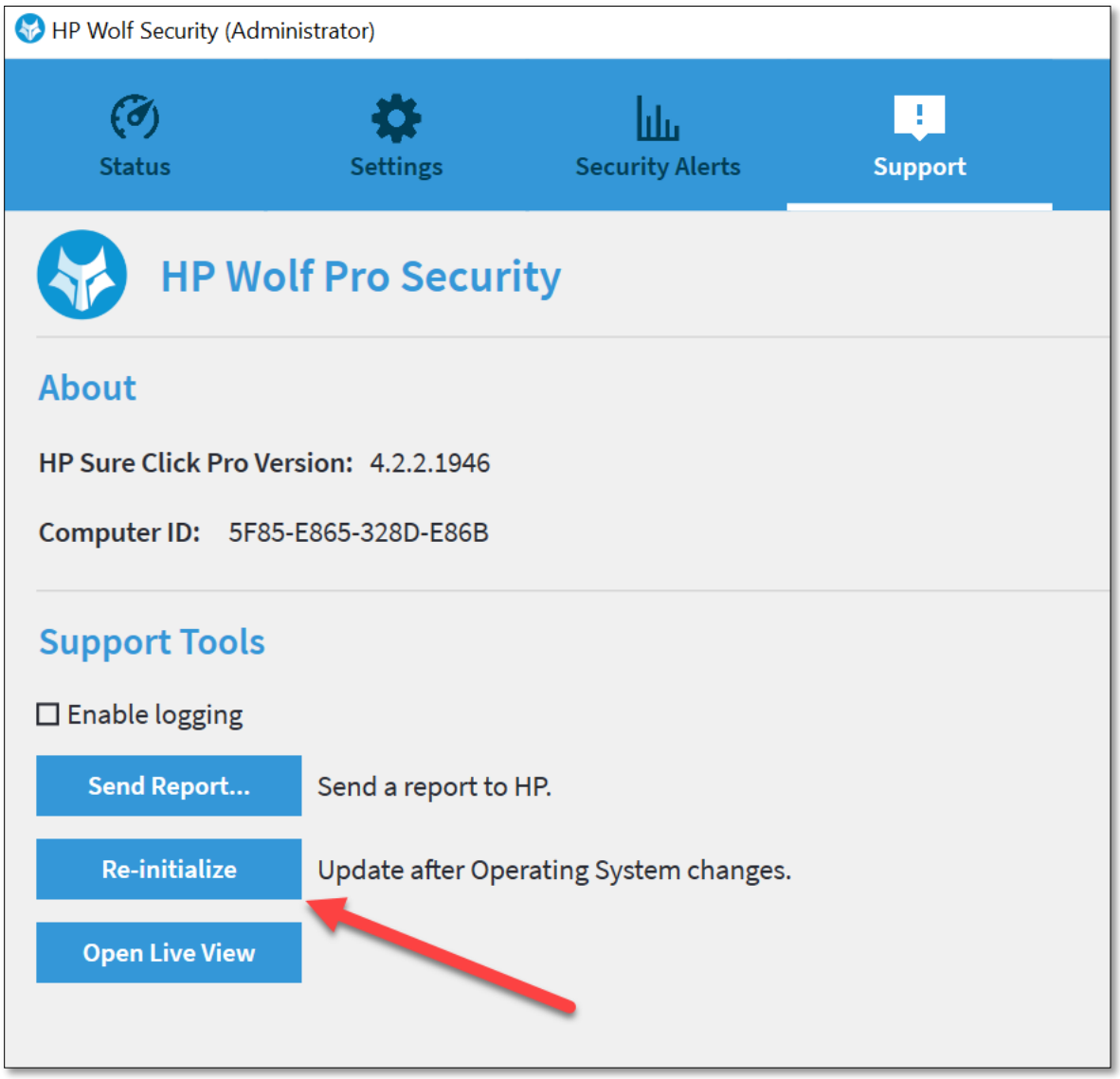
Nein: Fahren Sie fort mit dem Triage-Ablauf des Malwareschutzes

Aktivieren Sie die Bedrohungseindämmung

Starten Sie den Computer neu

Öffnen Sie nach dem Neustart die Wolf Desktop Console und reinitialisieren Sie





Triage-Ablauf des Malwareschutzes

Deaktivieren Sie den Malwareschutz

Wird das Problem hierdurch gelöst?

Ja: Versuchen wir, es zu beheben. Fahren Sie mit den nachfolgenden Schritten fort.

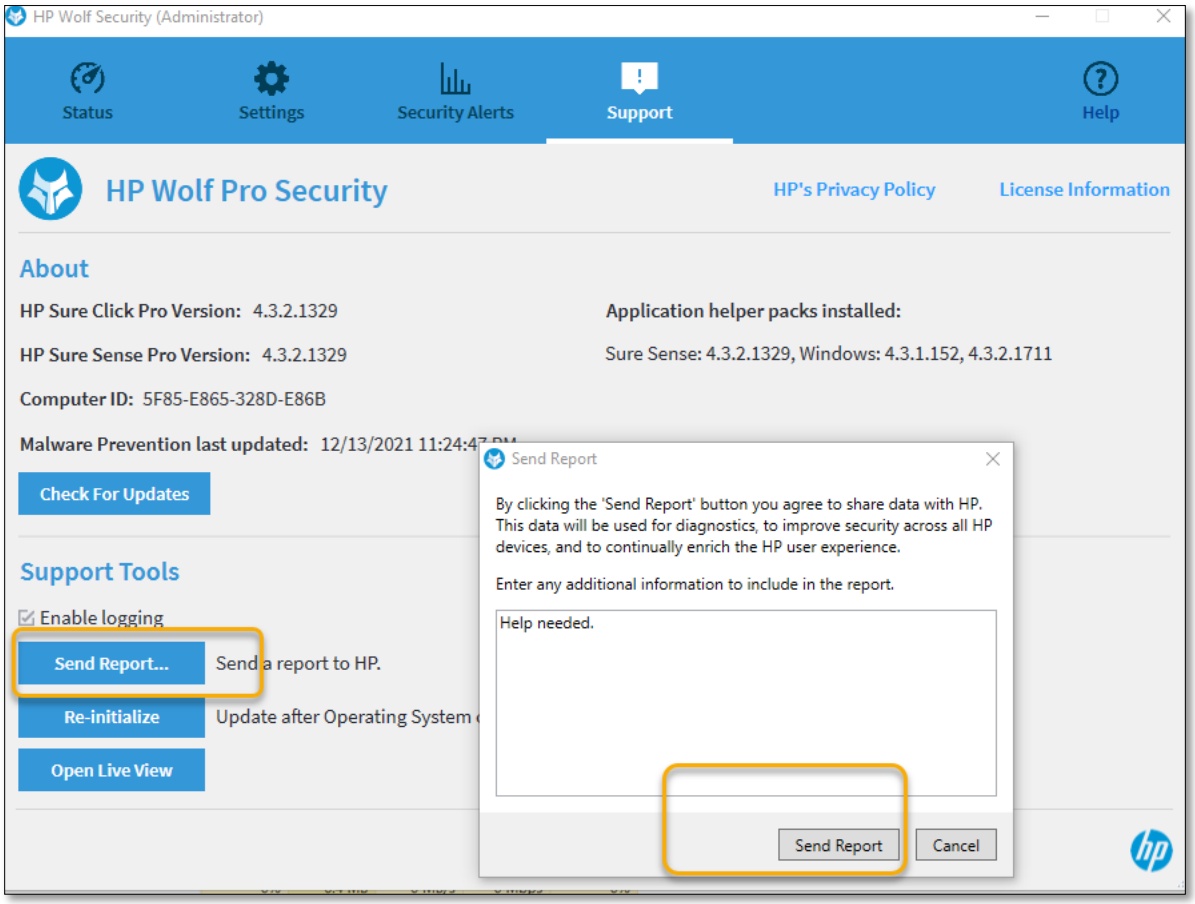
Nein: Entweder besteht kein Problem mit unserem Produkt oder zur Lösung des Problems ist das Erstellen eines Kunden-Supportvorgangs erforderlich.

Lassen Sie den Malwareschutz deaktiviert und überprüfen Sie die Ausschlüsse auf Produkte, die einen potenziellen Konflikt erzeugen, z. B. AV-Lösungen von Drittanbietern. Starten Sie den Computer neu, nachdem Sie alle erforderlichen Ausschlüsse übernommen haben.

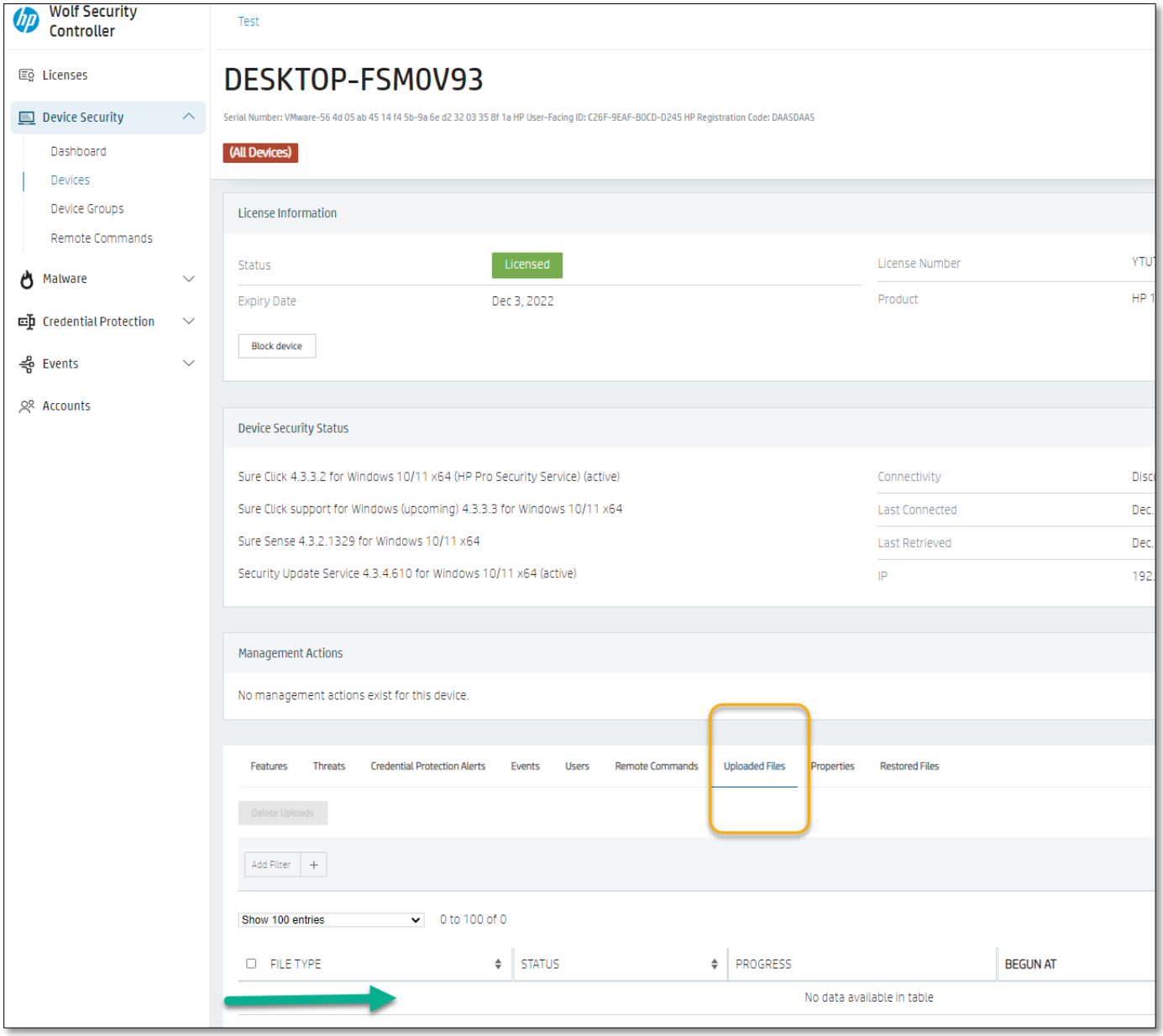
Erfassen von Protokollpaketen für den Support

Wenn Sie einen Supportfall eröffnen, ist es sehr hilfreich, über ein Protokollpaket des betroffenen Geräts zu verfügen. Sie können dieses ebenfalls mit Ihrer ersten E-Mail-Anfrage einsenden.

- Zur Erstellung eines Protokollpakets können Sie dieses entweder per Remote-Befehl über den Controller anfordern oder sich durch den Endbenutzer bzw. die Endbenutzerin zusenden lassen.

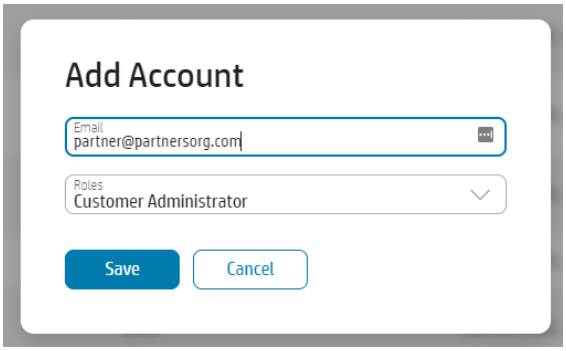
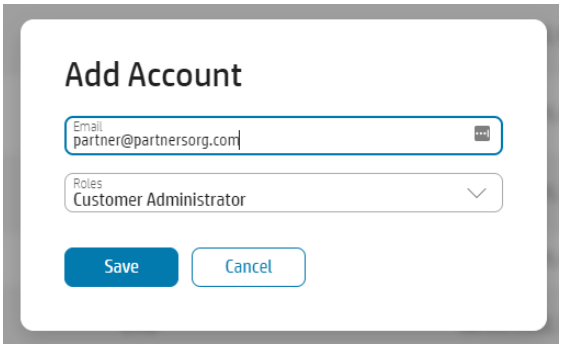


- Sie können das hochgeladene Protokollpaket in Ihrem Controller auf der Seite „Geräteinformationen“ anzeigen lassen.

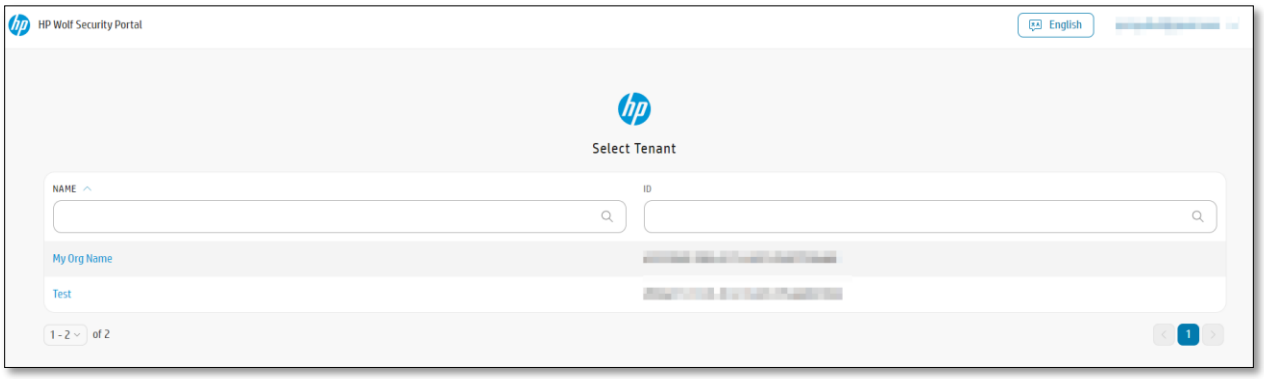


für Partner: Verwalten mehrerer Kund:innen

Partner haben die Möglichkeit, mehrere Kund:innen mithilfe einer Basis-Partnerkonsole zu verwalten. Damit diese Partneransicht möglich ist, muss der Partner sicherstellen, dass die E-Mail-Adresse seines Vertreters (oder die E-Mail-Adresse der für die Unterstützung des Kunden verantwortlichen Person) dem Mandanten des Kunden bzw. der Kundin als Admin-Benutzer:in hinzugefügt wird.

Kunde bzw. Kundin A	Kunde bzw. Kundin B
	

Wenn demselben HPID-Konto der Zugriff auf zwei separate Mandanten gewährt wurde, liefert die Anmeldung mit dieser HPID diese Ansicht:



Dies ermöglicht dem Partner ein **Single-Sign-on** für das Kundenkonto mithilfe dieser Seite und bietet grundlegende Funktionen wie die Kundensuche nach Namen und/oder ID, falls der Partner eine hohe Anzahl an Kund:innen betreut.

Kommunikation und Supportanfragen

Es gibt zwei einfache Möglichkeiten für das Einsenden einer Supportanfrage.

- Wenn Sie sich in der POC-Phase Ihrer Service-Bereitstellung befinden, senden Sie Ihrem zugeordneten HP Sicherheitsexperten eine E-Mail bezüglich Ihrer Frage oder Ihres Problems.
- Wenn Sie zahlender Kunde bzw. zahlende Kundin sind und sich nicht mehr in der POC-Phase Ihres Service befinden, finden Sie im Kundenportal entsprechende Kontaktmöglichkeiten: https://support.hpwolf.com/s/contact

Kommunikation

HP kontaktiert Sie unter folgenden Umständen:

- HP antwortet auf eine von Ihnen gesendete E-Mail mit einer Supportanfrage.
- HP sendet Ihnen Mitteilungen zu geplanten Upgrades.

Sammeln von Informationen/Einreichen eines Support-Tickets

Wenn Sie Hilfe bei einem Problem wünschen oder Fragen haben, kontaktieren Sie den HP Support unter https://support.hpwolf.com/s/contact und halten Sie die nachstehenden Informationen bereit. Wir benötigen ebenfalls die Kundeninformationen sowie den Grund für Ihre Anfrage.

Übermitteln von Kundeninformationen

Bevor Sie eine Service-Anfrage zur Ursachenanalyse übermitteln, ist es wichtig, Informationen in Bezug auf die Person und das Unternehmen zu erfassen.

Bitte stellen Sie sicher, dass Sie die folgenden zwingend notwendigen Informationen übermitteln:

- Name des Kunden bzw. der Kundin
- E-Mail-Adresse des Kunden bzw. der Kundin
- Telefonnummer des Kunden bzw. der Kundin
- Geografischer Standort und Zeitzone des Kunden bzw. der Kundin
- Primärer HP-interner Ansprechpartner und/oder Partnerinformationen

Erfassen allgemeiner Informationen

Einige Informationen sind erforderlich, um das gemeldete Problem oder die mögliche Lösung zu erläutern.

Bitte stellen Sie sicher, dass Sie die folgenden zwingend notwendigen Informationen übermitteln:

- Gerätename
- Zusammenfassung des Problems
- Zusammenfassung eines Lösungsvorschlags. Wissen Sie, wie wir Ihnen helfen können?

- Wie viele Personen sind betroffen?
- Ist das Problem konsistent reproduzierbar?

Erfassen zusätzlicher Informationen

Bitte versuchen Sie, die folgenden Fragen zu beantworten – optional, doch hilfreich:

- Wurde eine Datei isoliert?
  - Denken Sie, die Seite sollte automatisch als vertrauenswürdig eingestuft werden? Warum?
  - Haben Sie Fehlermeldungen erhalten, die bei der Lösung des Problems hilfreich sind?
  - Jegliche Screenshots der HP Wolf Pro Security Desktop Console
    - Statusseite
    - Supportseite
- Ist die Leistung schlecht?
  - Screenshot des Desktops bei Auftreten des Problems
  - Screenshot der Prozess-Registerkarte des Task-Managers
  - Screenshot der HP Wolf Pro Security Desktop Console
    - Statusseite
    - Supportseite
- Haben Sie einen möglichen Lösungsvorschlag?
- Wissen Sie, wie wir Ihnen helfen können?
  - Muss eine Datei entsperrt werden?
  - Muss eine Seite als vertrauenswürdig eingestuft werden?
  - Müssen Sie den Agent zur Behebung von Leistungsproblemen deaktivieren?
- Können Sie die Seriennummer des Geräts angeben?
- Können Sie den angemeldeten Benutzernamen angeben?
- Welche Tests/Maßnahmen zur Fehlerbehebung hat der Kunde bzw. die Kundin bisher durchgeführt?
- Welche Priorität hat dieses Problem? Kritisch, hoch, mittel, niedrig –
  Hinweis: Dies gibt in keiner Weise ein Service-Level-Ziel (SLO) zur Lösung vor, sondern dient bei der Betrachtung des Tickets lediglich einer schnellen Einstufung in Bezug auf die Art unserer Reaktion.

Kurzanleitung – HP Wolf Pro Security

HP Wolf Pro Security führt mindestens 2 Agent-Upgrades pro Kalenderjahr durch.

- Agent-Upgrades – Jährlich erfolgen mindestens 2 Agent-Upgrades. Diese richten sich üblicherweise in etwa nach dem Microsoft BS-Release-Kalender. Diese Upgrades werden remote über den Controller durchgeführt und Ihrerseits sind diesbezüglich keine Maßnahmen erforderlich. Wir informieren Sie in einer Mitteilung über den Zeitplan für QS- und Produktion-Releases. Bei Problemen senden Sie uns bitte eine Support-E-Mail mit den entsprechenden Informationen. Falls wir darüber hinaus Probleme feststellen, können wir einen Vorgang eröffnen, kontaktieren und um Hilfe bei der Lösung oder um Ihr Feedback zu unseren Beobachtungen bitten. Jegliche Probleme können zu einer Verzögerung des Upgrades führen.

Für Benutzer:innen

Dieser Abschnitt ist für Endbenutzer:innen von HP Wolf Pro Security vorgesehen. Es wird jedoch empfohlen, dass IT-Admins diesen Abschnitt ebenfalls durchgehen, um Probleme besser einordnen und Endbenutzer-Anliegen besser nachkommen zu können.

Funktion von HP Threat Containment

HP Threat Containment schützt Sie durch Isolation potenziell schädlicher Inhalte in Dateien, die von einer nicht vertrauenswürdigen Quelle außerhalb Ihrer Organisation heruntergeladen wurden.

Ihre IT-Abteilung hat bereits Seiten als *vertrauenswürdig* eingestuft, sodass Sie Dateien von diesen Seiten herunterladen können. Üblicherweise werden alle internen Seiten für den Dateiaustausch sowie Unternehmens-Web-Anwendungen als vertrauenswürdig für Downloads eingestuft. Von diesen vertrauenswürdigen Seiten heruntergeladene Dateien werden weiterhin so geöffnet, wie dies heute der Fall ist. Die Einstufung interner Seiten, Web-Anwendungen und E-Mail-Adressen als vertrauenswürdig wird als Whitelisting bezeichnet.

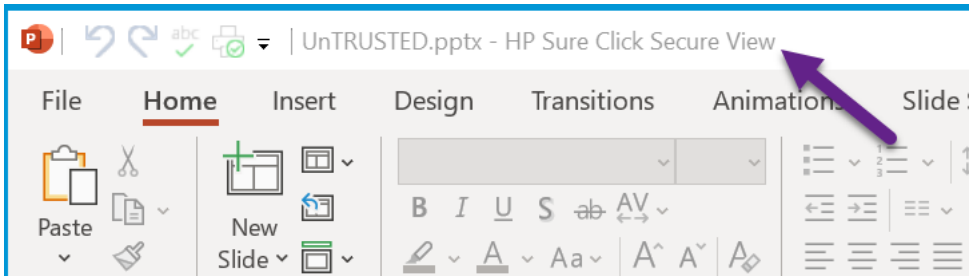
Ihre IT-Abteilung hat ebenfalls interne E-Mail-Adressen als vertrauenswürdige Quellen für Anhänge definiert. Dateien, die intern erstellt oder von vertrauenswürdigen Seiten heruntergeladen werden, können als E-Mail-Anhang an Kolleg:innen innerhalb Ihrer Organisation weitergeleitet werden. Diese Dateien werden als vertrauenswürdig eingestuft und normal geöffnet.

Heruntergeladene Dateien und E-Mail-Anhänge aus jeglichen anderen Quellen werden als nicht vertrauenswürdig eingestuft. Jegliche nicht vertrauenswürdigen Dateien, die per E-Mail empfangen und in Microsoft Word, Excel PowerPoint oder Adobe Acrobat Reader geöffnet werden, können weiterhin geöffnet, angezeigt, bearbeitet, ausgedruckt und gespeichert werden. HP Threat Containment isoliert automatisch jegliche schädlichen Aktivitäten durch nicht vertrauenswürdige Dateien.

Somit schützt HP Threat Containment Ihren Computer ebenfalls vor Dateien, die Sie herunterladen könnten:

- Aus dem Internet heruntergeladene oder aus E-Mails gespeicherte Dateien werden als nicht vertrauenswürdig gekennzeichnet.
- Nicht vertrauenswürdige Dateien werden innerhalb der Bedrohungseindämmung geöffnet.
- Isolierte Dateien sind weiterhin vollständig funktionsfähig und können gespeichert, kopiert, bearbeitet sowie ausgetauscht werden.

Wenn Sie eine nicht vertrauenswürdige Datei gespeichert haben, erhält diese den Status „nicht vertrauenswürdig“. Wenn Sie nicht vertrauenswürdige Dateien an Personen innerhalb Ihrer Organisation senden, die Wolf Pro Security nutzen, werden diese Dateien als nicht vertrauenswürdig gekennzeichnet. Wenn Sie überprüfen möchten, ob HP Threat Containment eine von Ihnen geöffnete Datei schützt, suchen Sie in der Titelleiste im oberen Bereich des Anwendungsfensters nach den Worten "HP Sure Click Secure View" (wie nachstehend dargestellt). Dies weist darauf hin, dass Sie auf die sicherste Weise mit dieser Datei arbeiten.



Wenn Sie denken, dass eine Website oder eine E-Mail-Adresse als vertrauenswürdig eingestuft werden sollte, wenden Sie sich bitte für eine Sicherheitsüberprüfung der Seite oder der E-Mail-Adresse an Ihre IT-Abteilung. Ihre IT-Abteilung wird die Seite oder E-Mail-Adresse hinzufügen lassen, wenn sie das Geschäftsszenario genehmigt.

Entfernen des HP Threat Containment Schutzes

Geräte werden häufig ausgenutzt, wenn schädliche Dateien aus dem Internet heruntergeladen werden. HP Threat Containment schützt vor solchen Schwachstellen, indem nicht vertrauenswürdige Seiten in einer virtuellen Umgebung geöffnet werden.

Nachfolgend sind einige Gründe für ein Whitelisting vertrauenswürdiger Seiten aufgeführt:

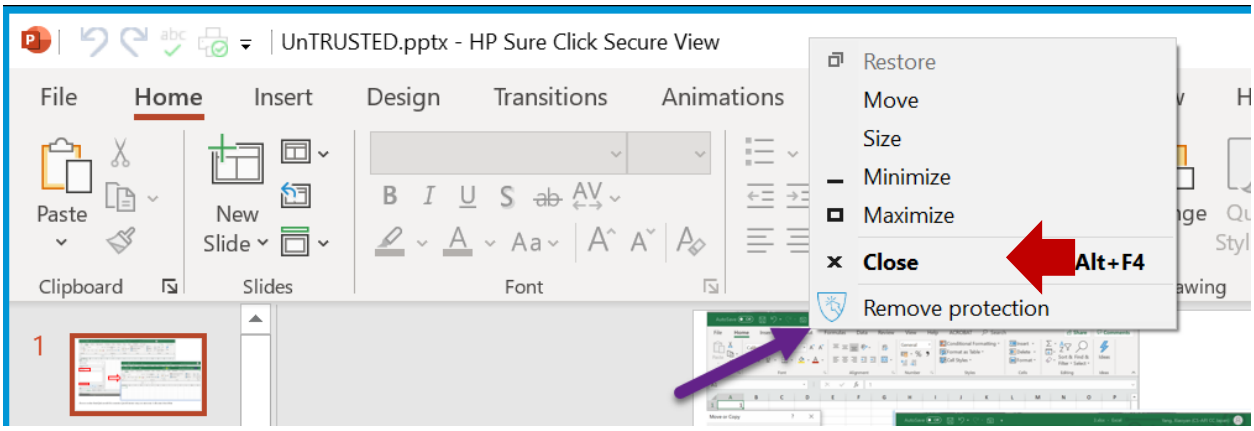
- Vereinfachen von Benutzerworkflows
- Unterstützung der Authentifizierung web-basierter Anwendungen
- Vermeiden wiederholter MVM-Isolationen sicherer Seiten

Darüber hinaus stehen manche Funktionen in MS Office oder im Adobe Acrobat Reader nicht vollständig zur Verfügung, wenn eine Datei durch HP Threat Containment geschützt ist. Beispielsweise können Excel Add-ins oder PowerPoint Presenter View deaktiviert werden. Wenn Sie über eine gültige geschäftliche Rechtfertigung verfügen und es sich nicht um eine schädliche Datei handelt, können Sie die Bedrohungseindämmung von der Datei entfernen. In den meisten Fällen sollten Sie sich an Ihre IT-Abteilung wenden, um den Schutz durch ein Whitelisting von Websites und E-Mail-Adressen zu entfernen. Jedoch kann die Bedrohungseindämmung bei Bedarf von einzelnen Dateien entfernt werden, sodass diese Dateien als vertrauenswürdig eingestuft werden.

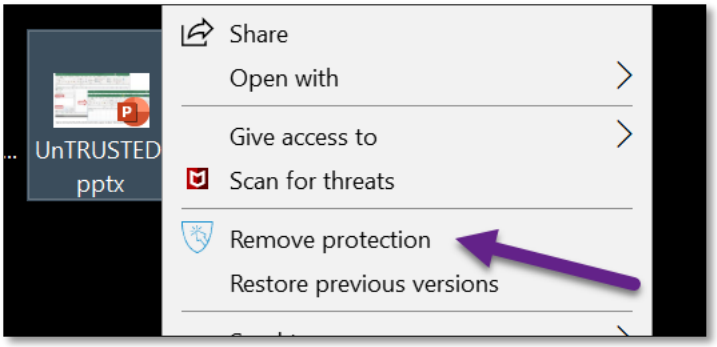
Hinweis: Das Entfernen der Bedrohungseindämmung einer Datei führt zum Versand einer Benachrichtigung an den Controller

Mit diesen zwei Möglichkeiten können Sie den Schutz entfernen:

- Wenn eine Datei innerhalb von Threat Containment geöffnet wird, führen Sie oben in der Anwendung einen Rechtsklick auf **HP Sure Click Pro Secure View** aus. Klicken Sie anschließend auf **Schutz entfernen**.



- Führen Sie im Windows Explorer einen Rechtsklick aus und wählen Sie **Schutz entfernen.** Ein neues Fenster wird geöffnet. Wählen Sie erneut **Schutz entfernen.**



Bitte beachten Sie, dass die Datei vor dem Entfernen des Schutzes von HP Threat Containment analysiert wird. Die Datei wird ab diesem Zeitpunkt ohne Schutz in MS Office oder Adobe Acrobat Reader geöffnet. Wenn Sie eine nicht vertrauenswürdige Datei speichern und erneut öffnen, bleibt die Datei vertrauenswürdig. Wird die Datei per E-Mail an eine nicht vertrauenswürdige Partei außerhalb Ihrer Organisation gesendet, wird sie automatisch auf einen nicht vertrauenswürdigen Status zurückgesetzt.

Falls HP Threat Containment verdächtige Inhalte in einer MS Office-, Adobe PDF-, oder einer ausführbaren EXE-Datei erkennt, wird die Datei als nicht vertrauenswürdig eingestuft. Sie sollten die Datei sicher schließen. Falls Sie weitere Hilfe benötigen, wenden Sie sich bitte an Ihre IT-Abteilung.

Funktion des Malwareschutzes

Der Malwareschutz der HP Wolf Pro Security Software arbeitet wie eine herkömmliche Antivirus-Software, die Sie in der Vergangenheit genutzt haben. Er wird stets ausgeführt, verschiebt erkannte Bedrohungen in Quarantäne und blockiert sie. Basierend auf der Richtlinie Ihres Unternehmens können Sie möglicherweise Objekte aus der Quarantäne freigeben, ohne dass hierzu zusätzlicher Support erforderlich ist. Wenn Sie in Quarantäne verschobene Objekte anzeigen möchten, können sie die Desktop-Konsole über die Taskleiste starten und die Seite „Sicherheitsalarme“ betrachten. Sofern durch die Richtlinie zulässig, können Sie

ebenfalls den Malwareschutz deaktivieren, falls dies für die Fehlersuche notwendig ist. Der Schutz bleibt bis zur erneuten Aktivierung deaktiviert.

Zugangsdatenschutz

Der Zugangsdatenschutz wird nachstehend ebenfalls als Identitätsschutz bezeichnet. Er verhindert, dass Benutzer Passwörter auf bekannten schädlichen Websites eingeben und warnt vor potenziell schädlichen Websites.

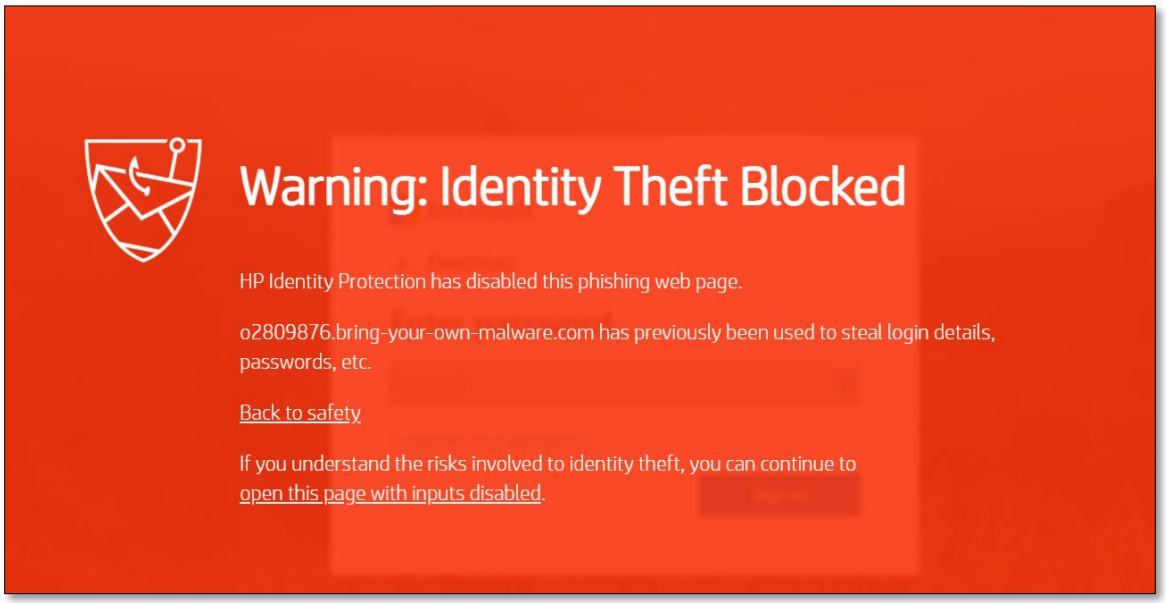
Unterstützte Browser

Die Identitätsschutz-Erweiterung wird gegenwärtig von den neuesten Versionen der Web-Browser Google Chrome, Mozilla Firefox und Microsoft Edge (Chromium-basiert) unterstützt. Sie ist ebenfalls für den HP Sure Click Pro Secure Browser erhältlich.

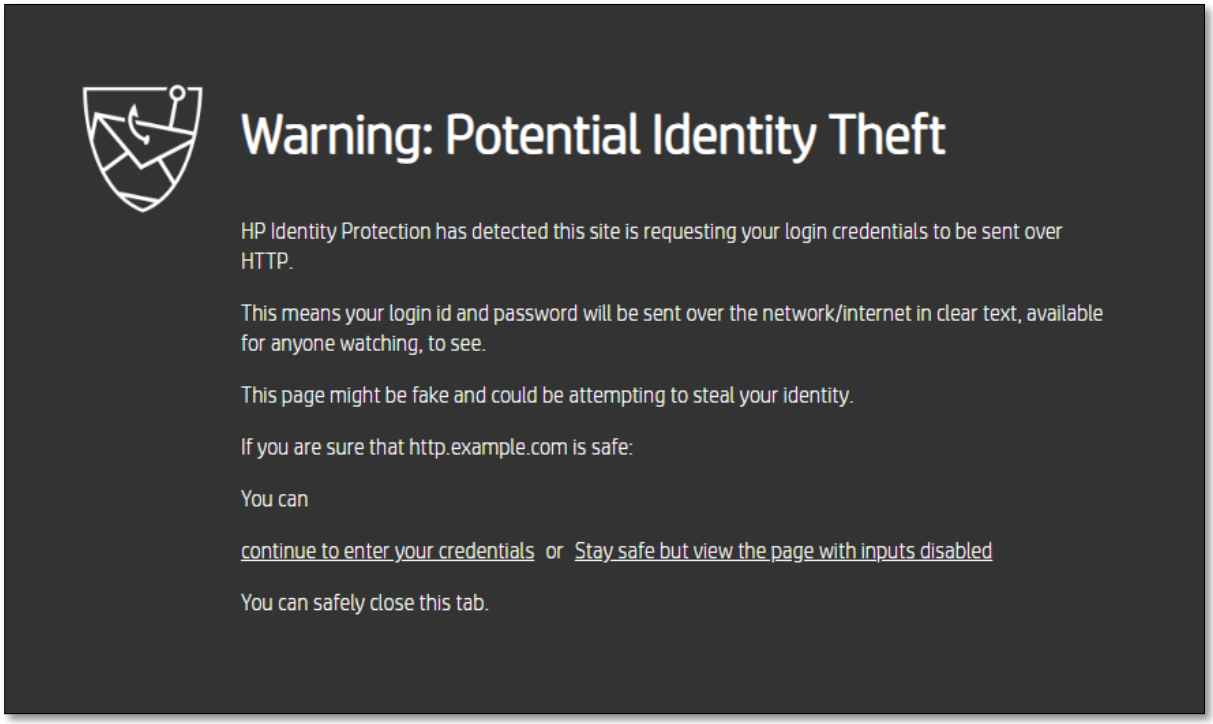
Schutzverhalten

Auf Geräten, auf denen die Funktion aktiviert ist, wird eine Warnmeldung angezeigt, wenn ein Benutzer versucht, über einen geschützten Browser ein Passwort auf einer verdächtigen oder bekannten schädlichen Website einzugeben.

Wird das Website-Risiko als hoch eingestuft, wird dem Benutzer bzw. der Benutzerin ein Warnbildschirm angezeigt, wie dargestellt. Der Benutzer bzw. die Benutzerin wird gewarnt und kann die Warnung nicht umgehen. Der Zugriff auf die Seite wird eingeschränkt, sodass die Steuerungen des Anmeldeformulars deaktiviert werden.



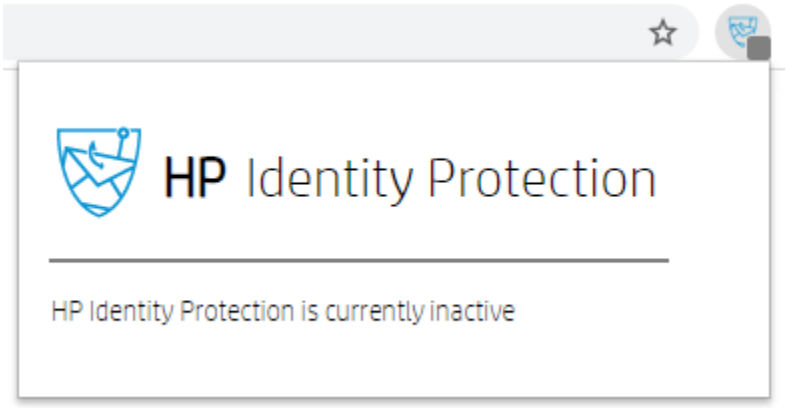
Wird das Risiko für eine Seite als mittel (verdächtig) eingestuft, wird dem Benutzer ein grauer Warnbildschirm angezeigt, wie nachstehend dargestellt:



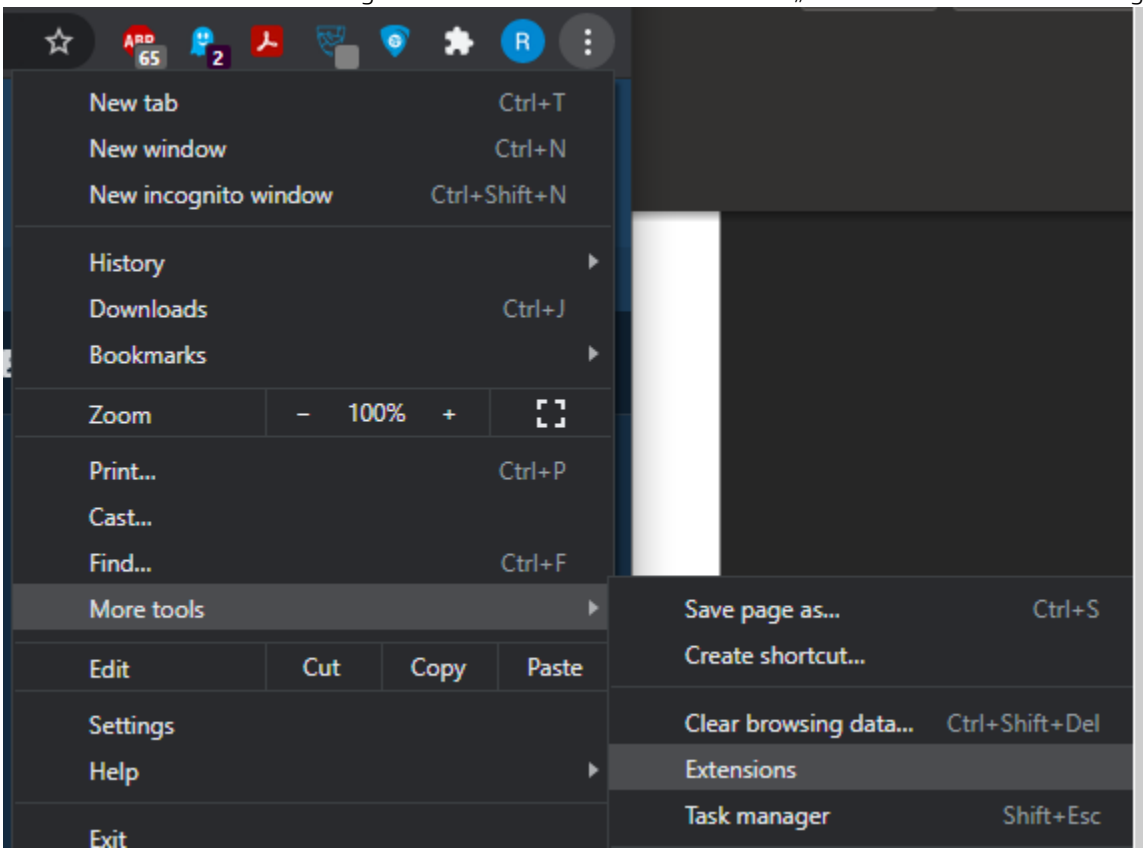
Da diese Seiten absichtlich nicht als schädlich bestätigt werden, erhält der Benutzer bzw. die Benutzerin die Möglichkeit, mit der Eingabe seiner Zugangsdaten fortzufahren oder die Website mit deaktivierten Anmeldungsfenstern zu nutzen, so dass eine versehentliche Passworteingabe verhindert wird. Weiterhin wird, falls sich der Benutzer bzw. die Benutzerin für die Eingabe der Zugangsdaten entscheidet, die Seite der Liste vertrauenswürdiger Seiten dieses Endbenutzers bzw. dieser Endbenutzerin hinzugefügt und es werden keine weiteren Warnungen angezeigt.

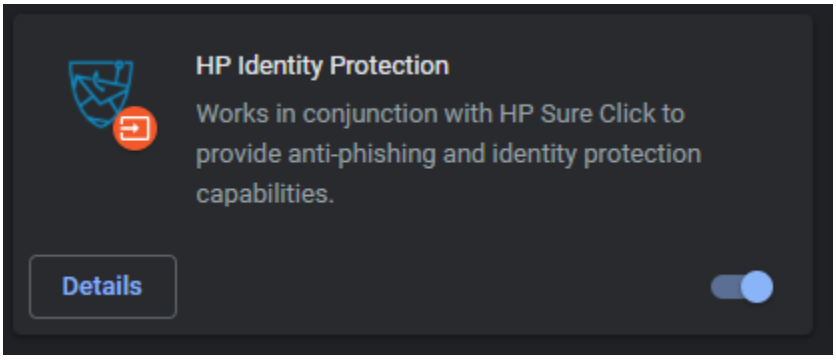
Aktivieren der Identitätsschutz-Erweiterung

Wenn sie überprüfen möchten, ob der Identitätsschutz aktiviert ist, klicken Sie in der Liste der Browser-Erweiterungen auf das Symbol für HP Identity Protection. Ist die Erweiterung im Browser-Profil des Benutzers bzw. der Benutzerin nicht aktiviert, wird das folgende Popup-Fenster angezeigt.



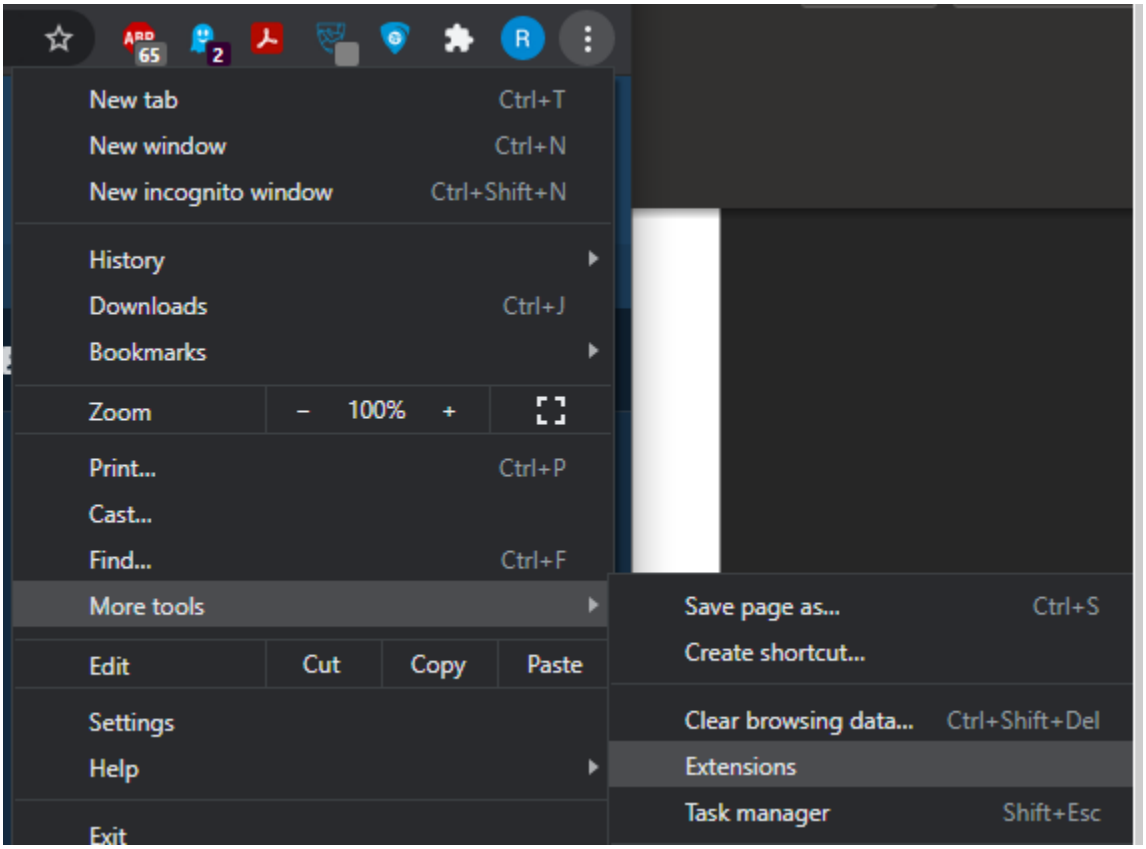
Zum Aktivieren der Erweiterung wählen Sie im Web-Browser-Menü „Weitere Tools→ Erweiterungen".



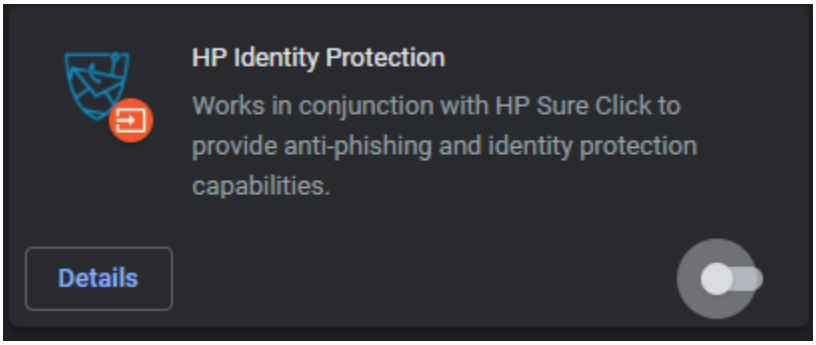


Deaktivieren der Identitätsschutz-Erweiterung

Zum Deaktivieren der Identitätsschutz-Erweiterung navigieren Sie zum Erweiterungsmenü für Ihren Browser und schalten Sie die Erweiterung aus. Bei Google Chrome und Microsoft Edge (Chromium) erfolgt dies im Browser-Menü unter „Weitere Einstellungen→ Erweiterungen“.

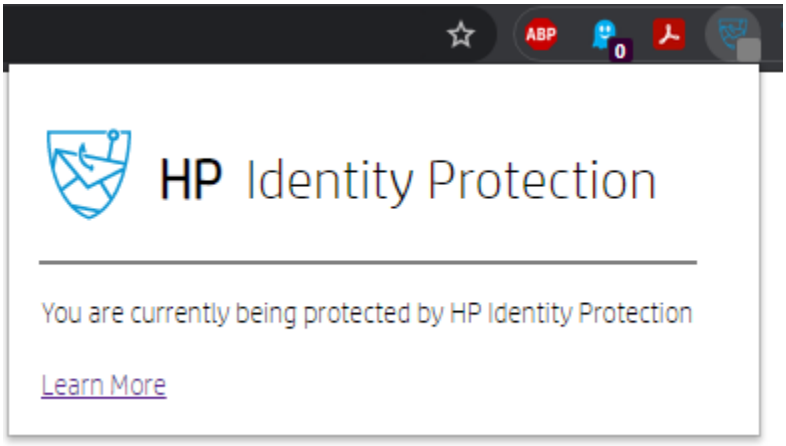


Suchen Sie in der Liste der Erweiterungen die Kachel für die Erweiterung HP Identity Protection und schalten Sie die Funktion aus.



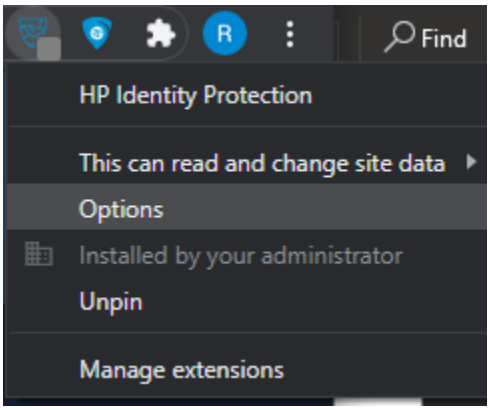
Bestätigen, ob die HP Identity Protection Browser-Erweiterung aktiviert ist

Nach der Aktivierung können Sie überprüfen, ob die Erweiterung aktiv ist, indem Sie in der Browser-Menüleiste auf das Symbol der HP Identity Protection Erweiterung klicken.

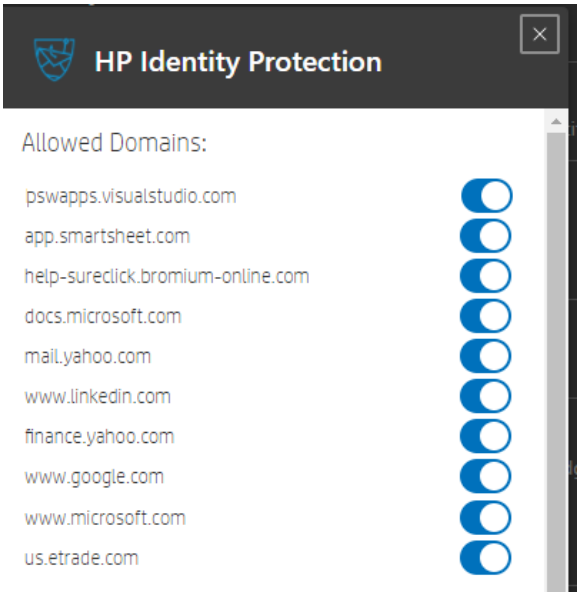


Umgang mit benutzerdefinierten Anmeldeseiten-Ausschlüssen

Zur Verwaltung der Liste zulässiger oder blockierter Anmeldeseiten führen Sie in der Menüleiste des Browsers einen Rechtsklick auf die HP Identity Protection Browser-Erweiterung aus und wählen Sie „Optionen“.



In diesem Menü kann der Benutzer die Einstellungen zur Vertrauenswürdigkeit zulässiger Websites ändern. Bitte beachten Sie, dass diese Funktion durch Ihr Unternehmen eingeschränkt sein kann.

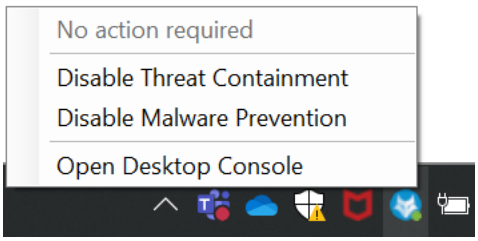


Lokale Verwaltung (Desktop-Konsole)

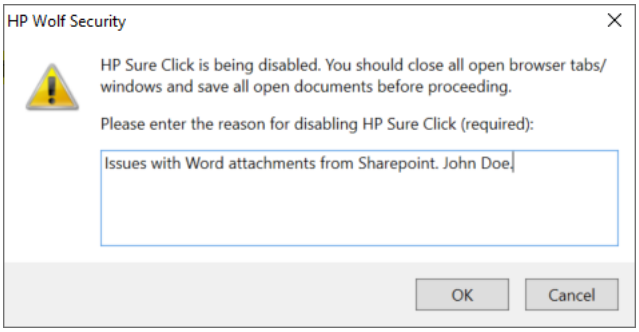
Dieser Abschnitt beschreibt, wie der Endbenutzer bzw. die Endbenutzerin mit HP Wolf Pro Security Agents und Service interagiert.

Suchen der Desktopkonsole

Die Desktopkonsole (Benutzeroberfläche) wird angezeigt, wenn Sie das HP Wolf Pro Security Symbol neben der Uhr in der Taskleiste anklicken, wie nachstehend dargestellt.

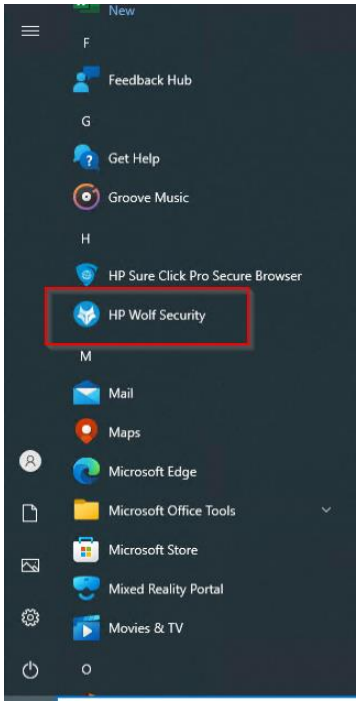


- Der Gesamtstatus informiert Sie über ggf. erforderliche Maßnahmen.
- Die Deaktivierung oder Aktivierung der Bedrohungseindämmung kann durch Anklicken dieser Option erfolgen. Dies deaktiviert die Bedrohungseindämmungstechnologie.
- Die Deaktivierung oder Aktivierung der des Malwareschutzes kann durch Anklicken dieser Option erfolgen. Dies deaktiviert die Sure Sense Technologie.
    - Bei jeder Deaktivierung einer Funktion sollten Sie einen Grund sowie Ihren Namen angeben. Dies könnte jedes Problem schneller lösen, das sich möglicherweise auf andere Benutzer:innen auswirkt.



- „Desktop-Konsole öffnen“ öffnet die Benutzeroberfläche.

Die Desktop-Konsole kann ebenfalls durch Anklicken von „HP Wolf Security“ im Startmenü geöffnet werden.



Kurzanleitung – HP Wolf Pro S

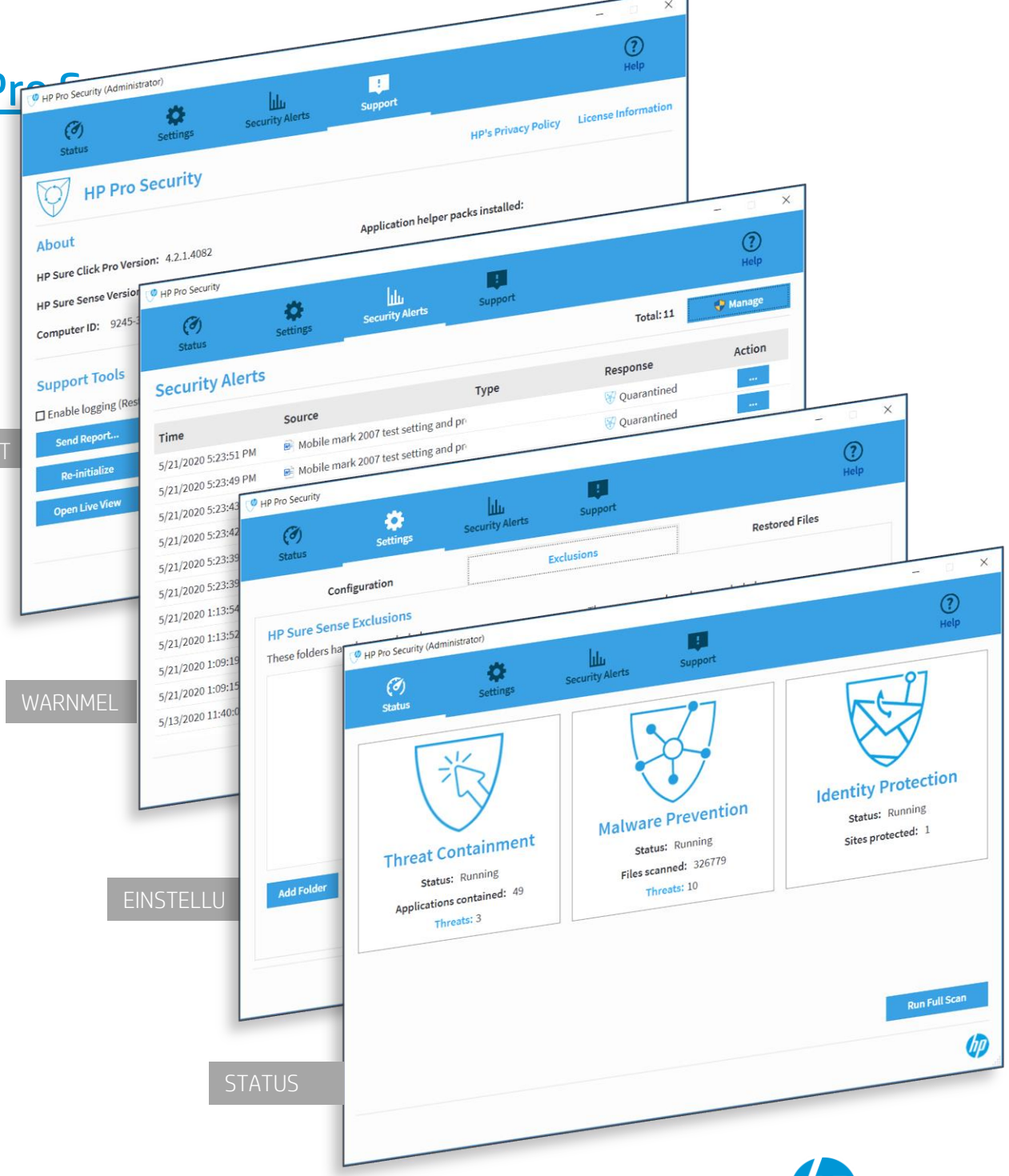
Details zur Desktop-Konsole

- Status
  - Aktiver Status, Fehlermeldungen, Anzahl erkannter und geminderter Bedrohungen, Anzahl gescannter Dateien.

- Einstellungen
  - Status – Endgeräteverbindung zum Controller
  - Definieren Sie lokale Datei- und Ordnerausschlüsse, ergreifen Sie Maßnahmen für aus der Quarantäne wiederhergestellte Dateien

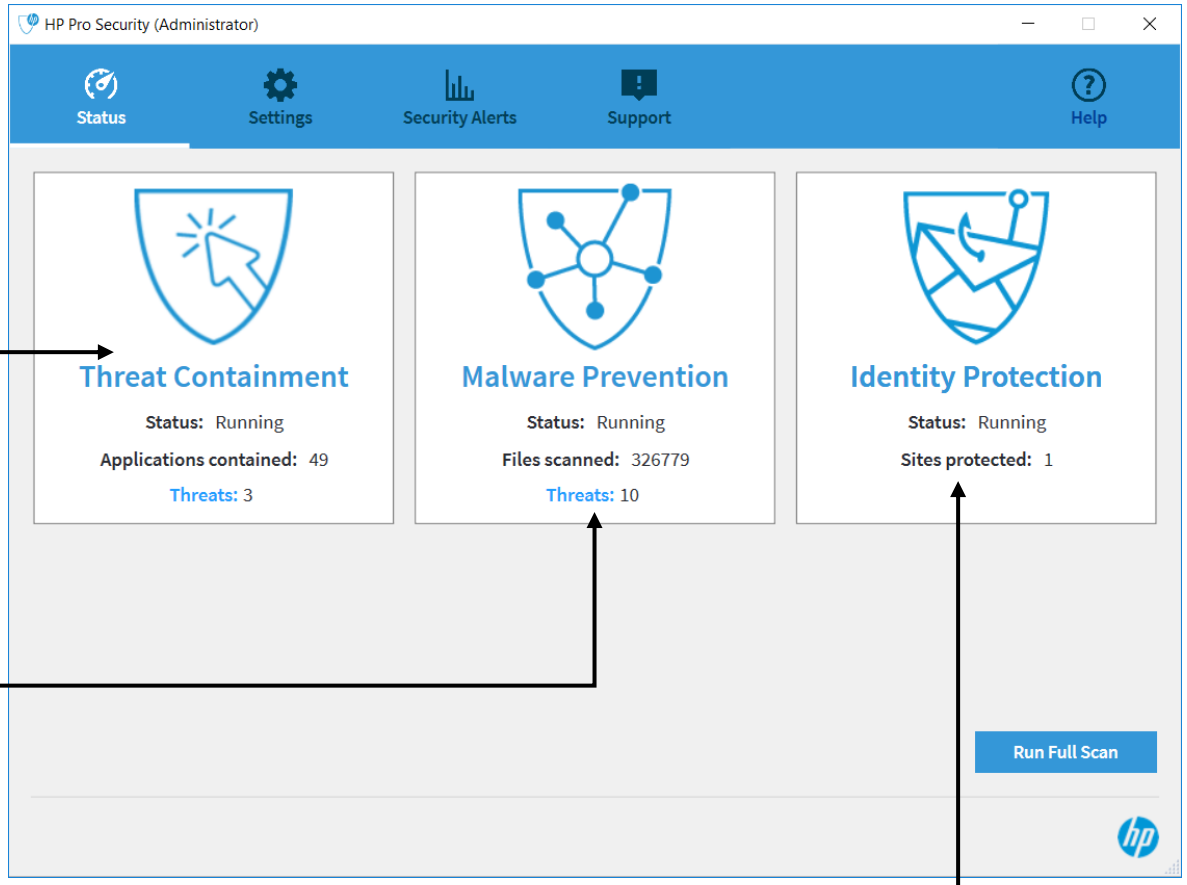
- Warnmeldungen
  - Ereignisliste erkannter schädlicher Dateien, Websites und Phishing-Attacken zum Diebstahl von Zugangsdaten
  - Korrigieren und behandeln Sie in Quarantäne verschobene Dateien mithilfe der Isolationstechnologie, um ein sicheres Öffnen der Dateien zu ermöglichen

- Support
  - Software-Info – Versionsnummer, PC #
  - Erweiterte Tools
    - Protokollierung, VM-Reinitialisierung, Live-Ansicht



Nach dem Aufrufen des **HP Pro Security** Dashboards über das Windows Startmenü öffnet das Dashboard die Seite ***Status***. Nachstehend finden Sie Beschreibungen für jeden der 3 in HP Pro Security enthaltenen Schutzmechanismen. Durch Anklicken der Symbole im oberen Bereich (Status, Einstellungen, Sicherheitsalarme und Support) werden Einstellungen und Informationen für jedes der Software-Attribute angezeigt.

Kurzanleitung – HP Wolf Pro Security



Status – Zeigt an, dass der Schutz aktiv ist und der Benutzer bzw. die Benutzerinvvor schädlichen Websites und verdächtigen E-Mail-Anhängen geschützt ist. Wird das Symbol gelb oder rot angezeigt,

Eingedämmte Anwendungen – Dokumente/Websites, die in einer sicheren Ansicht geöffnet werden.

Bedrohungen – Blockierte und in Quarantäne verschobene Websites (siehe Seite „Sicherheitsalarme“ für weitere Informationen zu Namen und Typen der Bedrohungen).

Malwareschutz – Deep Learning-KI – Malwareschutz.

Status - Zeigt an, ob der KI-Schutz-Agent aktiv ist, den PC vor eingehenden schädlichen Dateien schützt und diese isoliert.

Gescannte Dateien – Vom Agent gescannte Dokumente/Websites Hinweis: Wenn der Agent aktiv ist, werden alle Dateitypen gescannt, die auf dem PC eingehen.

Bedrohungen – Blockierte Dateien/Objekte (siehe Seite „Sicherheitsalarme“ für weitere Informationen zu Namen und Typen der Bedrohungen).

Identitätsschutz – Die Anti-Phishing-Engine mit der Möglichkeit, Benutzer zu warnen oder deren Eingabe von Passwörtern auf verdächtigen Websites zu verhindern

Status – zeigt an, ob der Anti-Phishing-Schutz von HP aktiv oder inaktiv ist.

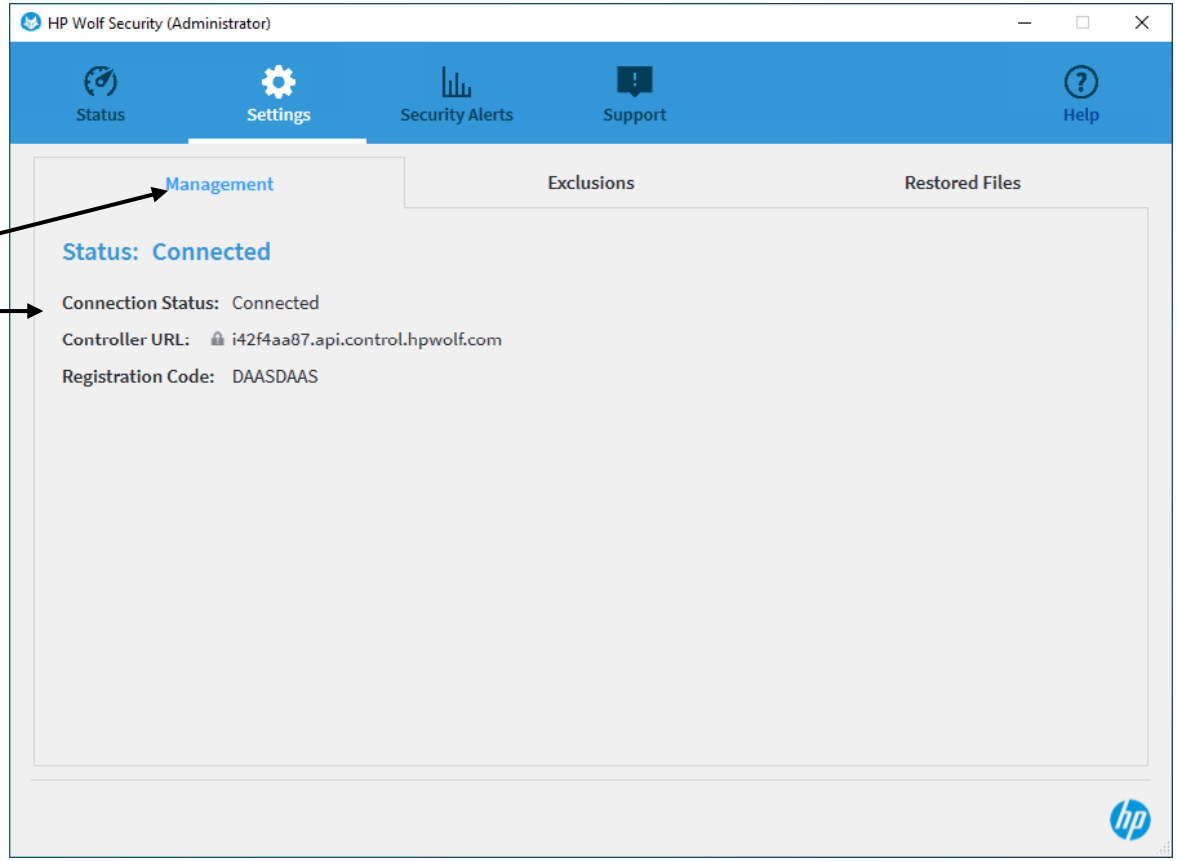
Geschützte Seiten – Zeigt die Anzahl der Websites an, auf denen versucht wurde, Zugangsdaten zu stehlen (Benutzer-Login, Passwort)

Nach dem Aufrufen des **HP Pro Security** Dashboards über das Windows Startmenü wird das Dashboard geöffnet. Bei der Auswahl des ***Einstellungs***-Symbols werden 3 Registerkarten-Seiten mit Funktionen geöffnet, die über die Software gesteuert werden können: Einstellungen, Ausschlüsse und wiederhergestellte Dateien.

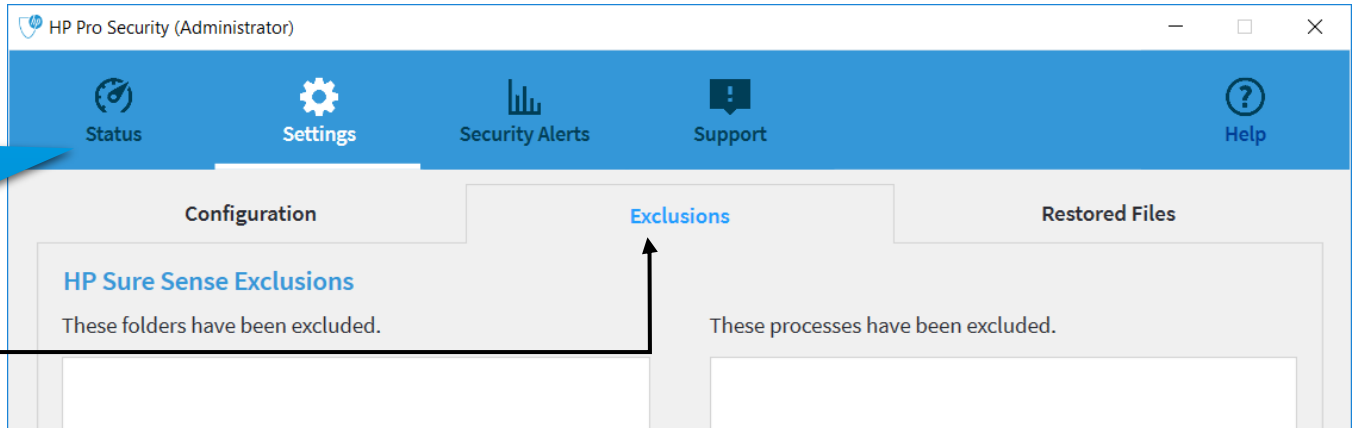
Kurzanleitung – HP Wolf Pro Security

Verwaltung: Tab 1 von 3 auf dieser (Einstellungs-) Seite

Verwaltung: "Status" – Zeigt den Status der Endgeräte-Verbindung zum Controller.



Nach dem Aufrufen des **HP Pro Security** Dashboards über das Windows Startmenü wird das Dashboard geöffnet. Bei der Auswahl des ***Einstellungssymbols werden*** 3 Registerkarten-Seiten mit Funktionen geöffnet, die über die Software gesteuert werden können: Konfiguration, Ausschlüsse und wiederhergestellte Dateien.



Kurzanleitung – HP Wolf Pro Security

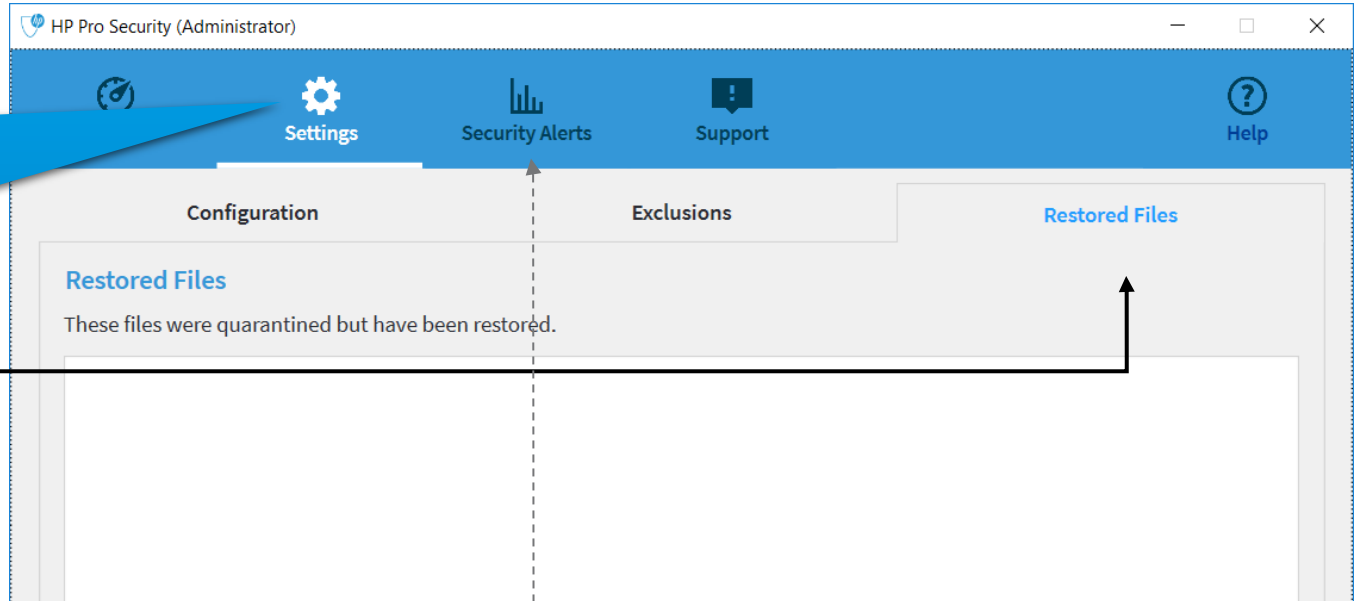
Ausschlüsse: Tab 2 von 3 auf dieser (Einstellungs-)Seite

Ausschluss: Listen von Ordnern und/oder Prozessen, bei denen es sich um bekannt sichere Ordner, Dateien oder Prozesse handelt. Durch das Hinzufügen eines Ordners (mit einer Datei) oder Prozesses zu einer dieser Listen auf dieser Seite bewirkt, dass er bei der *Durchführung eines Sicherheits-Überprüfungen* durch HP Pro Security übergangen (als sicher angesehen) wird.

Durch das Hinzufügen einer solchen benutzerspezifischen Anwendung zur Ausschlussliste wird die Datei

Nach dem Aufrufen des **HP Pro Security** Dashboards über das Windows Startmenü wird das Dashboard geöffnet. Bei der Auswahl des ***Einstellungs-*** Symbols ***werden*** 3 Registerkarten-Seiten mit Funktionen geöffnet, die über die Software gesteuert werden können: Konfiguration, Ausschlüsse und wiederhergestellte Dateien.

Wiederhergestellte Dateien: Tab 3 von 3 auf dieser (Einstellungs-) Seite

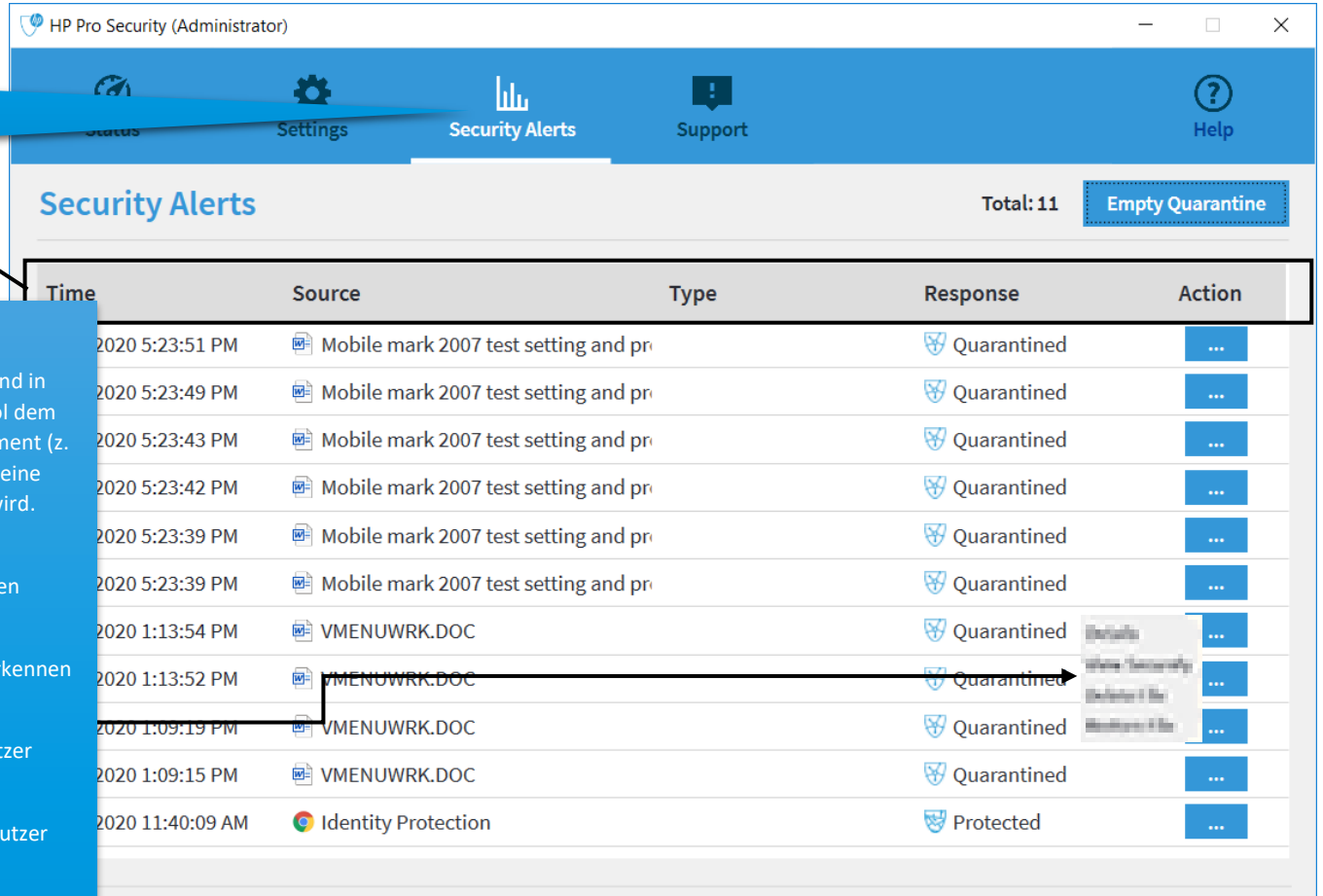


Kurzanleitung – HP Wolf Pro Security

Wiederhergestellte Dateien: Diese Seite enthält eine aktive Liste von Dateien, die HP Wolf Pro Security anfänglich als schädlich, vom Benutzer jedoch als sicher gekennzeichnet wurden. Üblicherweise stammt eine sichere Datei *aus einer vertrauenswürdigen Quelle und der Benutzer hat diese als sicher gekennzeichnet.*

HINWEIS: Als unsicher

Nach dem Aufrufen des **HP Pro Security** Dashboards über das Windows Startmenü wird das Dashboard geöffnet. Durch Auswahl des Symbols für die ***Sicherheitsalarme*** wird eine Liste der Dateinamen und/oder Websites angezeigt, die *in Quarantäne verschoben* oder als schädlich gekennzeichnet wurden.



Die Angriffsdaten enthalten *Uhrzeit, Quelle und Art (des Angriffs), Reaktionen*und *Maßnahmen.*

Zeit: Monat, Tag, Jahr und Uhrzeit der Bedrohungserkennung.

Quelle: Zeigt den Typ der als potenziell schädlich eingestuften und in Quarantäne verschobenen Datei. Üblicherweise zeigt das Symbol dem Benutzer an, ob es sich bei der verdächtigen Datei um ein Dokument (z. B. Word, Excel) oder ein Webbrowser-Ereignis handelt, bei dem eine Website als versuchter Diebstahl von Zugangsdaten eingestuft wird.

Typ: Manche Malware-Typen können kategorisiert werden (z. B. Ransomware). Wenn möglich, zeigt HP Pro Security Informationen hierzu in dieser Spalte an.

Reaktion: Die von HP Pro Security ergriffene Maßnahme beim Erkennen einer verdächtigen Datei oder Website.

Maßnahme: Die Schaltfläche „Maßnahme“ ... bietet dem Benutzer mehrere Optionen.

1. Für eine in Quarantäne verschobene Datei stehen dem Benutzer bzw. der Benutzerin 4 Optionen zur Verfügung.
   i. Details zu Datei, Ort, Zeit und Hash-Wert

Kurzanleitung – HP Wolf Pro Security

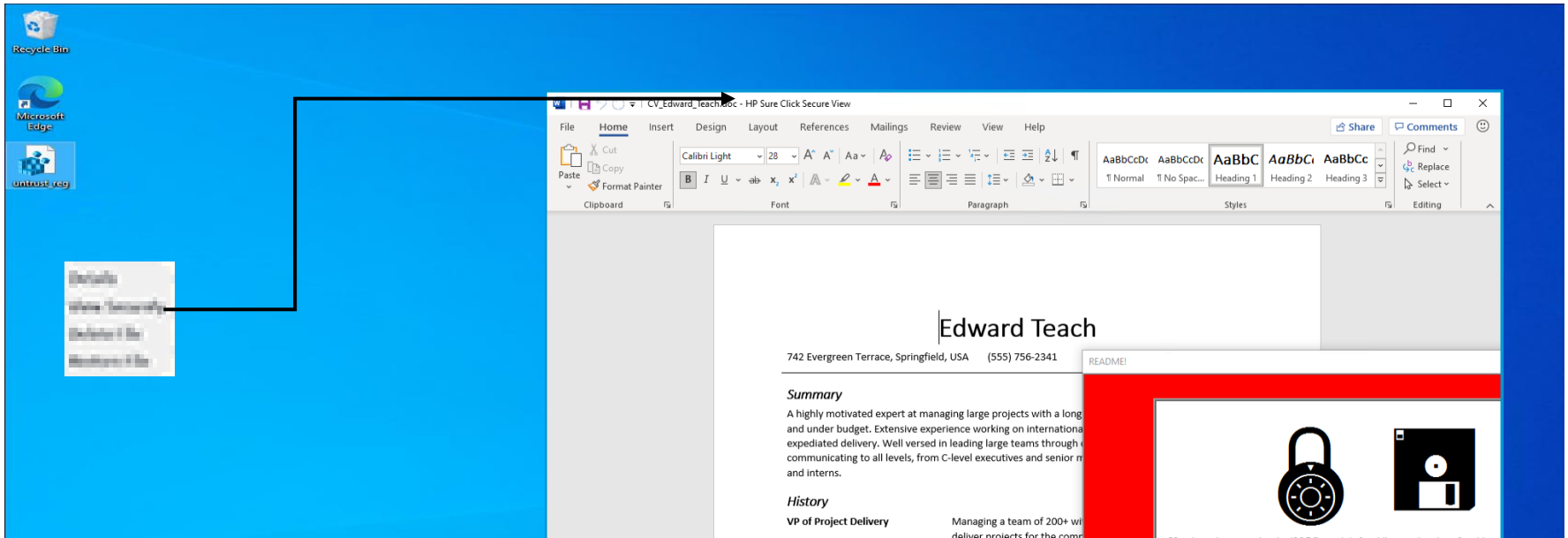
Dies ist ein branchenweit einzigartiger Quarantäne-Workflow, der nachstehend näher beschrieben wird.

Einzigartiger Workflow für in Quarantäne v

Die Kombination aus hardware-gestützter Isolation und NGAV ermöglicht WPS den Einsatz branchenweit einzigartiger Quarantäne-Workflows. Bei den meisten NGAVs besteht die Standardreaktion auf eine potenziell schädliche, in Quarantäne verschobene Datei daraus, sie zu löschen oder sicher für eine Analyse hochzuladen, wenn der Benutzer bzw. die Benutzerin davon überzeugt ist, dass es sich um eine falsch-positive Erkennung handelt. Dies führt zu Workflow-Unterbrechungen, insbesondere im Fall falsch-positiver Ergebnisse, da selbst die Anzeige der Datei unzulässig ist. Abhängig von der in Quarantäne verschobenen (und somit für den Benutzer bzw. die Benutzerin nicht mehr zugänglichen) Datei können die Unterbrechungen schwerwiegend sein.

WPS umgeht dieses Problem vollständig, indem das Öffnen in Quarantäne verschobener Dateien in einer sicheren isolierten Umgebung ermöglicht wird, sofern die Isolationsfunktion diesen Dateityp unterstützt. Der Benutzer bzw. die Benutzerin muss sich keine Gedanken darüber machen, ob die Datei schädlich ist oder nicht, und kann sie sicher betrachten. Falls es sich um eine schädliche Datei handelt, wird sie erkannt und zerstört, sobald das Dokument geschlossen wird. Das Gerät des Endbenutzers bzw. der Endbenutzerin wird in keiner Weise beeinträchtigt.

Nachstehend finden Sie ein Beispiel für die Wiederherstellung einer schädlichen, Ransomware enthaltenden Datei, die bereits in Quarantäne verschoben wurde, bei der sich der Benutzer bzw. die Benutzerin jedoch nicht sicher ist, ob es sich um eine schädliche Datei handelt oder nicht. Der Benutzer kann sie weiterhin sicher anzeigen lassen und sie wird in einer vollständig isolierten VM geöffnet. Selbst wenn sich herausstellt, das es sich tatsächlich um eine schädliche Datei handelt, wie nachstehend dargestellt, erfolgt eine vollständige Eindämmung der Malware innerhalb der VM sowie die Zerstörung der Datei beim Schließen des Word-Dokuments.



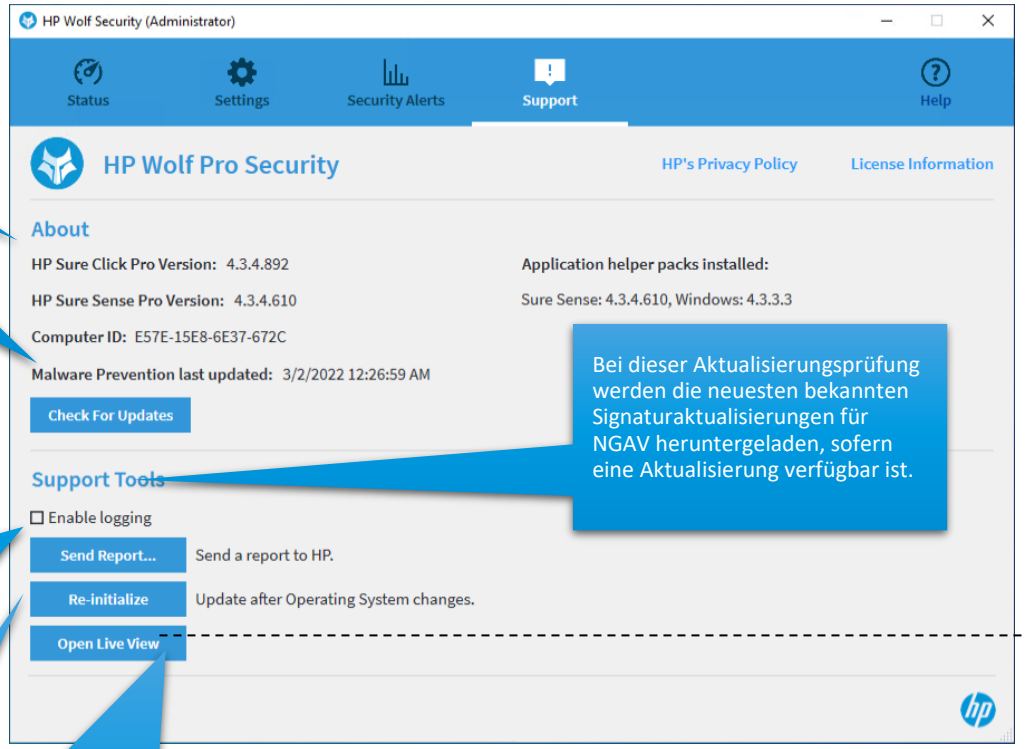
Kurzanleitung – HP Wolf Pro Security

HP Sure Click Pro und HP Sure Sense Pro stellen gemeinsam die Funktionen bereit, die Bestandteil von WPS sind. Für jede Anwendung können separate Aktualisierungen über die HP Cloud bereitgestellt werden. Die **Versionsnummern** sind nicht identisch.

Die **Computer-ID** ist eine eindeutige, diesem Endgerät zugewiesene ID. Sie wird verwendet, um dieses Endgerät am Controller zu identifizieren, und ist ebenfalls für Supportzwecke hilfreich.

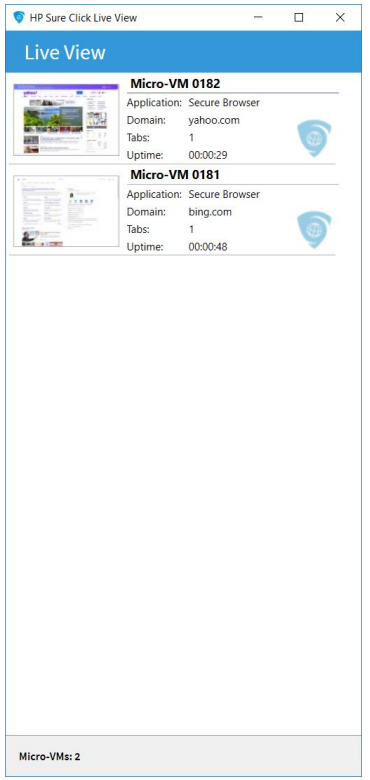
Durch Aktivieren der Protokollierung wird eine Protokolldatei im ZIP-Format erzeugt, die in einem benutzerdefinierten Verzeichnis auf dem PC gespeichert wird (z. B. „Desktop“), um dem Support-Team Informationen zu liefern. Durch Betätigen der Schaltfläche „Bericht senden“ wird die Protokolldatei zur weiteren Analyse an den Controller übertragen

Die „Reinitialisierung“ ist in bestimmten Situationen hilfreich, wenn bei der Bedrohungseindämmung unerwartete Fehler auftreten. Durch Betätigen dieser Schaltfläche werden die Templates der virtuellen Maschine wiederhergestellt, die zur Isolation schädlicher Inhalte verwendet werden.



Bei dieser Aktualisierungsprüfung werden die neuesten bekannten Signaturaktualisierungen für NGAV heruntergeladen, sofern eine Aktualisierung verfügbar ist.

Die offene Live-Ansicht ist eine erweiterte Funktion, die bei Supportvorgängen hilfreich ist. Durch Betätigen der Schaltfläche „Offene Live-Ansicht“ wird ein Dialogfenster (Beispiel, weit rechts) erstellt, in dem die gegenwärtig auf dem PC ausgeführten virtuellen Maschinen angezeigt werden.



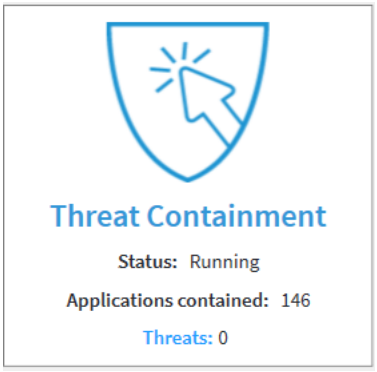
Kurzanleitung – HP Wolf Pro Security

Statusarten der Desktopkonsole

Bedrohungseindämmung

Es gibt drei Statusarten für Isolation und Überwachung:

- **Wird ausgeführt** – Normaler Betrieb ohne Probleme.
- **Maßnahme empfohlen** – Die Anwendung verursacht Probleme, die untersucht werden sollten.
- **Deaktiviert** – Dies bedeutet, dass der Agent deaktiviert wurde und den Computer nicht schützt.
- Sie können sehen, wie viele Objekte analysiert wurden
- Sie können sehen, wie viele Bedrohungen abgewehrt wurden



Die folgenden **Status-Meldungen** könnten in dieser Kachel angezeigt werden:

Status	Beschreibung
Warten auf HP Sure Click	Wenn HP Sure Click in diesem Zustand bleibt, versuchen Sie, den Computer neu zu starten.
HP Sure Click wird ausgeführt	HP Sure Click schützt Sie vor Websites und Dokumenten, die Malware enthalten.
HP Sure Click aktivieren, um Ihr System zu schützen	HP Sure Click ist deaktiviert. Wählen Sie zur Aktivierung „Bedrohungseindämmung aktivieren“ im Menü des Taskleisten-Symbols.
HP Sure Click wird nicht ausgeführt	HP Sure Click wird nicht ausgeführt. Versuchen Sie, Ihren Computer neu zu starten.
HP Sure Click muss initialisiert werden	HP Sure Click wurde nicht initialisiert. Betätigen Sie auf der Seite „Support“ die Schaltfläche „Initialisieren“.
HP Sure Click Anforderungen werden überprüft...	Diese Meldung kann kurz angezeigt werden, wenn HP Sure Click gestartet wird.
HP Sure Click Status wird überprüft...	Diese Meldung kann kurz angezeigt werden, wenn HP Sure Click gestartet wird.
HP Sure Click Aktualisierungen werden überprüft...	HP Sure Click muss möglicherweise Aktualisierungen herunterladen, bevor es ausgeführt werden kann. Bitte warten Sie, bis dieser Vorgang abgeschlossen ist.
Warten auf Empfang der Konfiguration	HP Sure Click muss vor der Ausführung die Konfiguration vom Controller herunterladen. Bitte warten Sie, bis dieser Vorgang abgeschlossen ist.
Konfiguration konnte nicht abgerufen werden. Bitte überprüfen Sie Ihre Netzwerkverbindung.	HP Sure Click muss vor der Ausführung die Konfiguration vom Controller herunterladen. Bitte

	überprüfen sie, ob Ihr Computer mit dem Internet verbunden ist.
Bitte überprüfen sie, ob Ihr Computer mit dem Internet verbunden ist	Bitte überprüfen sie, ob Ihr Computer mit dem Internet verbunden ist
HP Sure Click ist in wenigen Minuten betriebsbereit	HP Sure Click wird für den Betrieb vorbereitet. Bitte warten Sie, bis dieser Vorgang abgeschlossen ist.
Initialisierung wird durchgeführt	HP Sure Click erfasst den aktuellen Systemstatus des Computers. Bitte warten Sie, bis dieser Vorgang abgeschlossen ist.
Initialisierung erforderlich/Initialisierung angehalten	HP Sure Click muss den aktuellen Systemstatus des Computers erfassen. Dieser Vorgang sollte durchgeführt werden, wenn sich das System im Leerlauf befindet. Alternativ können Sie die Schaltfläche „Initialisieren“ auf der Seite „Support“ betätigen, um den Vorgang zu starten.
Reinitialisierung wird durchgeführt	HP Sure Click erfasst den aktuellen Systemstatus des Computers. HP Sure Click wird weiterhin ausgeführt, so dass Sie während dieses Vorgangs geschützt bleiben.
Reinitialisierung erforderlich/Reinitialisierung angehalten	HP Sure Click muss den aktuellen Systemstatus des Computers erfassen. Dieser Vorgang sollte durchgeführt werden, wenn sich das System im Leerlauf befindet. Alternativ können Sie die Schaltfläche „Reinitialisieren“ auf der Seite „Support“ betätigen, um den Vorgang zu starten. HP Sure Click wird weiterhin ausgeführt, so dass Sie während dieses Vorgangs geschützt bleiben.
HP Sure Click erfordert einen Neustart des Computers, damit das Upgrade wirksam wird	Aktualisierungen für HP Sure Click wurden installiert. Starten Sie den Computer neu, um die aktualisierte Version zu nutzen.

Die folgenden Fehler-Meldungen könnten in dieser Kachel angezeigt werden

Fehlermeldungen	Beschreibung
HP Sure Click unterstützt diese CPU nicht	HP Sure Click unterstützt diese CPU nicht und kann daher nicht ausgeführt werden.
HP Sure Click erfordert ein VT-x-fähiges System	Die CPU unterstützt keine VT-x Virtualisierungserweiterungen (oder vergleichbare), daher kann HP Sure Click nicht ausgeführt werden.
Die Aktivierung von HP Sure Click erfordert VT-x	VT-x Virtualisierungserweiterungen (oder vergleichbare) sind im System-BIOS deaktiviert. Sie müssen VT-x im System-BIOS aktivieren, damit HP Sure Click ausgeführt werden kann. Siehe Aktivieren der Virtualisierungs-Technologie im BIOS.
Die Aktivierung von HP Sure Click erfordert Extended Page Tables (EPT)	Extended Page Table Virtualisierungserweiterungen sind im System-BIOS deaktiviert. Sie müssen EPT im System-BIOS aktivieren, damit HP Sure Click ausgeführt werden kann.
Nicht unterstützte AMD CPU-Familie	Der Computer verfügt über einen AMD-Prozessor, der von HP Sure Click nicht unterstützt wird.
HP Sure Click Arbeitsspeicher-Anforderungen wurden nicht erfüllt	HP Sure Click hat erkannt, dass der verfügbare Arbeitsspeicher nicht ausreicht. Bitte schließen Sie einige Programme, um mehr Arbeitsspeicher freizugeben.
Nicht genügend freier Arbeitsspeicher. Bitte schließen Sie einige Programme, um weiteren Arbeitsspeicher freizugeben.	HP Sure Click hat erkannt, dass der verfügbare Arbeitsspeicher nicht ausreicht. Bitte schließen Sie einige Programme, um mehr Arbeitsspeicher freizugeben.
Stellen Sie mehr freien Laufwerksspeicher bereit und starten Sie den Computer neu	Für die Initialisierung von HP Sure Click sind mindestens 1,5 GB freier Speicherplatz auf dem Systemlaufwerk erforderlich. Bitte stellen Sie sicher, dass mindestens 1,5 GB Laufwerksspeicher verfügbar sind und starten Sie den Computer neu.
HP Sure Click ist nicht mit Systemen kompatibel, die Gladinet nutzen	HP Sure Click ist nicht mit der Gladinet Software kompatibel.
HP Sure Click ist in einer anderen Benutzersitzung aktiv	HP Sure Click ist nicht für die Unterstützung mehrere Benutzer konfiguriert, die gleichzeitig auf demselben Computer angemeldet sind.
HP Sure Click erfordert einen Neustart des Computers, um Ihr System zu schützen	Der Computer muss neu gestartet werden, bevor HP Sure Click ausgeführt wird.
HP Sure Click benötigt Aktualisierungen, um die installierte Version von Windows zu unterstützen. Starten Sie Ihren Computer neu, um die Installation dieser Updates zu gestatten.	HP Sure Click benötigt eine Zusatzkomponente, um diese Version von Windows zu unterstützen. Das System muss neu gestartet werden, um die Installation dieser Komponente zu gestatten.
HP Sure Click kann die zur Unterstützung der installierten Version von Windows erforderlichen Aktualisierungen nicht herunterladen. Bitte überprüfen Sie Ihre Internetverbindung.	HP Sure Click benötigt eine Zusatzkomponente, um diese Version von Windows zu unterstützen. Das System konnte die erforderlichen Komponenten nicht herunterladen. Bitte stellen Sie sicher, dass Ihr System mit dem Internet verbunden ist und warten Sie anschließend, bis der Download abgeschlossen ist.

HP Sure Click benötigt Aktualisierungen, um die installierte Version von Windows zu unterstützen. Bitte warten Sie, bis die Aktualisierungen installiert wurden.	HP Sure Click benötigt eine Zusatzkomponente, um diese Version von Windows zu unterstützen. Bitte warten Sie, bis das System die Installation dieser Komponente abgeschlossen hat.
HP Sure Click benötigt Aktualisierungen, um die installierte Version von Windows zu unterstützen	HP Sure Click benötigt eine Zusatzkomponente, um diese Version von Windows zu unterstützen.
Ein nicht unterstütztes Windows Sprachpaket ist installiert	HP Sure Click erfordert die Installation eines Windows Sprachpakets.
Die Windows Anzeigesprache des Benutzers wird nicht unterstützt	Die Windows Anzeigesprache des Benutzers wird nicht unterstützt
Starten Sie den Computer neu, um ausstehende Windows Aktualisierungen zu installieren	HP Sure Click kann nicht initialisiert werden, da der Computer neu gestartet werden muss, um die Windows Aktualisierungen zu übernehmen. Bitte starten Sie den Computer neu, warten Sie, bis die Aktualisierungen übernommen wurden und betätigen Sie anschließend die Schaltfläche „Initialisieren“, um den Initialisierungsprozess zu starten.
Windows-Aktualisierung wird durchgeführt	HP Sure Click kann nicht initialisiert werden, da eine Windows Aktualisierung durchgeführt wird. Bitte warten Sie, bis der Vorgang abgeschlossen ist, oder starten Sie den Computer neu. Betätigen Sie anschließend die Schaltfläche „Initialisieren“, um den Initialisierungsprozess zu starten.
HP Sure Click erfordert, dass die VBA-Komponente gemeinsam mit Microsoft Office installiert wird	HP Sure Click erfordert, dass Visual Basic for Applications gemeinsam mit Microsoft Office installiert wird. Bitte installieren Sie die VBA-Komponente und betätigen Sie anschließend die Schaltfläche „Initialisieren“, um den Initialisierungsprozess zu starten.
Office ist nicht aktiviert	HP Sure Click erfordert die Aktivierung von Microsoft Office. Bitte aktivieren Sie Microsoft Office und betätigen Sie anschließend die Schaltfläche „Initialisieren“, um den Initialisierungsprozess zu starten.
Ein nicht unterstütztes UI-Sprachpaket ist installiert	HP Sure Click erfordert die Installation eines der folgenden UI-Sprachpakete für Microsoft Office
HP Sure Click kann Hyper-V auf diesem Computer nicht unterstützen	Damit HP Sure Click ausgeführt werden kann, deaktivieren Sie entweder Hyper-V oder aktivieren Sie die Windows Hypervisor Platform (siehe Windows Hyper-V Support).
HP Sure Click erfordert einen Systemstart im UEFI-Modus, um Hyper-V zu unterstützen	Es wurde kein Systemstart im UEFI-Modus erkannt. Damit HP Sure Click ausgeführt werden kann, deaktivieren Sie entweder Hyper-V oder aktivieren Sie die Windows Hypervisor Platform (siehe Windows Hyper-V Support).
HP Sure Click erfordert Windows 10 oder neuer, um Hyper-V zu unterstützen	Eine nicht unterstützte Betriebssystem-Version wurde erkannt. Deaktivieren Sie Hyper-V, damit HP Sure Click ausgeführt werden kann.

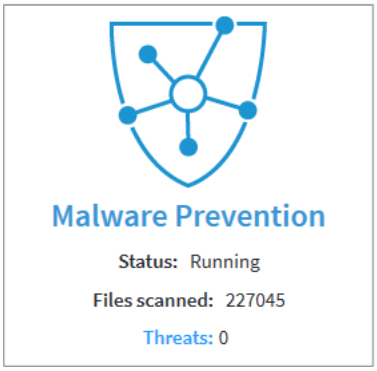
HP Sure Click unterstützt diese CPU nicht, wenn Hyper-V aktiviert ist	Eine nicht unterstützte CPU wurde erkannt. Damit HP Sure Click ausgeführt werden kann, deaktivieren Sie entweder Hyper-V oder aktivieren Sie die Windows Hypervisor Platform (siehe Windows Hyper-V Support).
HP Sure Click erfordert einen Secure Boot Drittanbieterschlüssel, um Hyper-V zu unterstützen	Öffnen Sie im System-BIOS das Secure Boot Konfigurationsmenü Wählen Sie „MS UEFI CA Schlüssel aktivieren“, damit HP Sure Click ausgeführt werden kann.
HP Sure Click erfordert eine VMCS Shadowing-fähige CPU, um Hyper-V zu unterstützen	Die CPU unterstützt kein VMCS Shadowing. Damit HP Sure Click ausgeführt werden kann, deaktivieren Sie entweder Hyper-V oder aktivieren Sie die Windows Hypervisor Platform (siehe Windows Hyper-V Support).
HP Sure Click konnte die Unterstützung für Hyper-V nicht aktivieren	Bitte wenden Sie sich an den HP Support, um das Problem zu beheben.
Mikro-Virtualisierung blockiert, während die Unterstützung für Hyper-V aktiviert ist	Bitte wenden Sie sich an den HP Support, um das Problem zu beheben.
BitLocker muss deaktiviert werden, bevor der Computer heruntergefahren/neu gestartet wird	Sie müssen BitLocker deaktivieren, bevor der Computer neu gestartet wird. Wählen Sie in der Windows Systemsteuerung „BitLocker-Laufwerk verschlüsseln“ und anschließend „Schutz deaktivieren“/
HP Sure Click kann die UEFI-Bootreihenfolge nicht konfigurieren, wenn die Unterstützung für Hyper-V aktiviert ist	Bitte wenden Sie sich an den HP Support, um das Problem zu beheben.
HP Sure Click kann das Boot-Laufwerk nicht konfigurieren, wenn die Unterstützung für Hyper-V aktiviert ist	Bitte wenden Sie sich an den HP Support, um das Problem zu beheben.
Letzte Initialisierung abgebrochen	Der Initialisierungsprozess von HP Sure Click wurde abgebrochen und nicht abgeschlossen.
Letzte Initialisierung blockiert	HP Sure Click konnte den Initialisierungsprozess nicht abschließen. Versuchen Sie, die Schaltfläche „Initialisieren“ auf der Seite „Support“ zu betätigen, um den Intitialisierungsprozess erneut zu starten. Ist diese Maßnahme nicht erfolgreich, wenden Sie sich bitte an den HP Support.
Letzter Initialisierungsversuch fehlgeschlagen	HP Sure Click konnte den Initialisierungsprozess nicht abschließen. Versuchen Sie, die Schaltfläche „Initialisieren“ auf der Seite „Support“ zu betätigen, um den Intitialisierungsprozess erneut zu starten. Ist diese Maßnahme nicht erfolgreich, wenden Sie sich bitte an den HP Support.
Letzter Initialisierungsversuch nicht erfolgreich	HP Sure Click konnte den Initialisierungsprozess nicht abschließen. HP Sure Click wurde zuvor bereits initialisiert und kann Ihren Computer daher weiterhin schützen. Versuchen Sie, die Schaltfläche „Reinitialisieren“ auf der Seite „Support“ zu betätigen, um den Intitialisierungsprozess erneut zu starten.

Nicht unterstützte Konfiguration. Wenden Sie sich an den Support.	Bitte wenden Sie sich an den HP Support, um das Problem zu beheben.
Interner Fehler, bitte starten Sie den Computer neu	Starten Sie den Computer neu, um dieses Problem zu beheben. Falls das Problem weiterhin besteht, wenden Sie sich bitte an den HP Support.
Mikro-VM konnte nicht geladen werden. Starten Sie den Computer neu. Falls das Problem weiterhin besteht, wenden Sie sich bitte an den HP Support.	Ein Problem ist aufgetreten, das ein korrektes Laden der Mikro-VMs durch HP Sure Click verhindert. Versuchen Sie, den Computer neu zu starten. Falls das Problem weiterhin besteht, wenden Sie sich bitte an den HP Support.
Die Installation von HP Sure Click wurde beschädigt und muss repariert werden	Einige Dateien fehlen in der HP Sure Click Installation. Dies kann das Ergebnis einer Windows Systemwiederherstellung sein. Laden Sie die neueste Version des Produkts herunter und installieren Sie diese, um die beschädigte Installation zu reparieren - siehe Neueste Version herunterladen.

Malwareschutz

Es gibt drei Statusarten für diese Funktion:

- **Wird ausgeführt** – Normaler Betrieb ohne Probleme.
- **Maßnahme empfohlen** – Die Anwendung verursacht Probleme, die untersucht werden sollten.
- **Deaktiviert** – Dies bedeutet, dass der Agent deaktiviert wurde und den Computer nicht schützt.
- Sie können sehen, wie viele Objekte überprüft wurden
- Sie können sehen, wie viele Bedrohungen abgewehrt wurden



Die folgenden **Statusmeldungen** könnten in dieser Kachel angezeigt werden:

Statusmeldung	Beschreibung
HP Sure Sense wird ausgeführt	HP Sure Sense schützt Sie vor schädlichen Dateien.

HP Sure Sense aktivieren, um Ihr System zu schützen	HP Sure Sense ist deaktiviert. Wählen Sie zur Aktivierung „Malwareschutz aktivieren“ im Menü des Taskleisten-Symbols.
HP Sure Sense ist in wenigen Minuten betriebsbereit	HP Sure Sense wird für den Betrieb vorbereitet. Bitte warten Sie, bis dieser Vorgang abgeschlossen ist.
HP Sure Sense erfordert einen Neustart des Computers, damit das Upgrade wirksam wird	Aktualisierungen für HP Sure Sense wurden installiert. Starten Sie den Computer neu, um die aktualisierte Version zu nutzen.
HP Sure Sense wird nicht ausgeführt	HP Sure Sense ist offenbar installiert, doch HP Wolf Pro Security kann nicht darauf zugreifen. Bitte versuchen Sie, Ihren Computer neu zu starten.
Aktualisierungen konnten nicht heruntergeladen werden	HP Sure Sense muss Aktualisierungen herunterladen, bevor es ausgeführt werden kann. Bitte überprüfen sie, ob Ihr Computer mit dem Internet verbunden ist.
Der Verhaltensschutz ist aufgrund einer Produkt-Inkompatibilität deaktiviert	Zur Aktivierung des Verhaltensschutzes entfernen Sie bitte sämtliche Produkte, von deinen eine Inkompatibilität mit diesem Produkt bekannt ist.
Warten auf Empfang der Konfiguration	HP Sure Sense muss vor der Ausführung die Konfiguration vom Controller herunterladen. Bitte warten Sie, bis dieser Vorgang abgeschlossen ist.
Konfiguration konnte nicht abgerufen werden. Bitte überprüfen Sie Ihre Netzwerkverbindung.	HP Sure Sense muss vor der Ausführung die Konfiguration vom Controller herunterladen. Bitte überprüfen sie, ob Ihr Computer mit dem Internet verbunden ist.
Unbekannter Fehler	Bitte wenden Sie sich an den HP Support, um das Problem zu beheben.

Identitätsschutz

Es gibt drei Statusarten für den Identitätsschutz:

- **Keine Maßnahme erforderlich** – Normaler Betrieb ohne Probleme.
- **Maßnahme empfohlen** – Die Anwendung verursacht Probleme, die untersucht werden sollten.
- **Deaktiviert** – Dies zeigt an, dass das Add-in im Browser oder der Schutz insgesamt deaktiviert ist.
- Sie können sehen, vor wie vielen Seiten Sie geschützt wurden

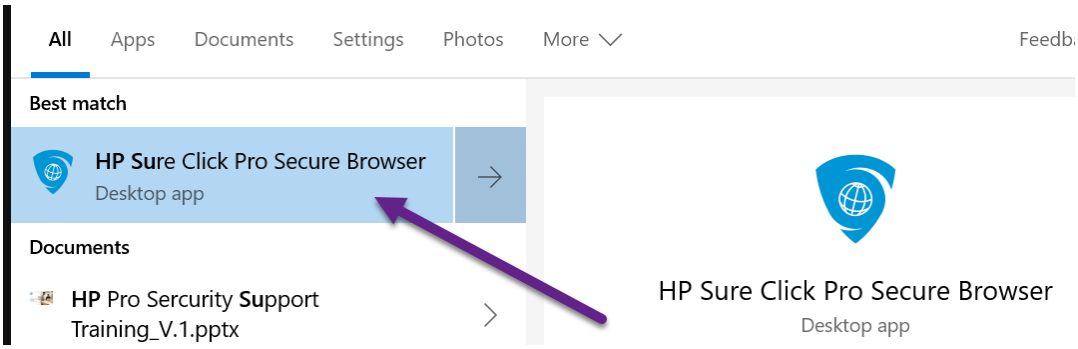
Die folgenden **Statusmeldungen** könnten in dieser Kachel angezeigt werden:

Status	Beschreibung
Identitätsschutz wird ausgeführt	HP Identity Protection schützt Sie vor Identitätsdiebstahl.
Die HP Sure Click Secure Browsing Erweiterung ist offenbar in Ihrem Standard-Browser deaktiviert. Bitte aktivieren Sie sie.	Wenn Sie Ihren Standard-Browser öffnen, werden Sie möglicherweise aufgefordert, die HP Sure Click Secure Browsing Erweiterung zu aktivieren. In Ihrem Standard-Browser können Sie außerdem die Seite „Erweiterungen“ über das Erweiterungsmenü öffnen. Suchen Sie anschließend nach der HP Sure Click Secure Browsing Erweiterung und aktivieren Sie diese.
Bedrohungseindämmung wird nicht ausgeführt. Bitte aktivieren oder warten, bis sie gestartet wird.	Die HP Sure Click Secure Browsing Erweiterung erfordert HP Sure Click Pro, um ausgeführt werden zu können. Falls dies deaktiviert ist, aktivieren Sie es bitte. Falls momentan die Vorbereitung für den Betrieb erfolgt, warten Sie bitte, bis dieser Vorgang abgeschlossen ist.
Die HP Sure Click Secure Browsing Erweiterung wird von Ihrem Standard-Browser nicht unterstützt	Die HP Sure Click Secure Browsing Erweiterung ist im HP Sure Click Secure Browser, in Google Chrome, Mozilla Firefox und dem neuen Microsoft Edge verfügbar. Sie können Ihren Standard-Browser auf einen dieser Browser ändern, indem Sie im Windows Startmenü nach „Standard-Web-Browser“ suchen.
Identitätsschutz kann nicht ausgeführt werden	HP Identity Protection kann nicht ausgeführt werden. Bitte versuchen Sie, Ihren Computer neu zu starten.

Sichere Browsernutzung

Sie können den HP Secure Browser direkt öffnen, wenn Sie wissen, dass Sie Seiten besuchen, die ein hohes Risiko darstellen.

Befolgen Sie diese Schritte, um zu beginnen:



Der Secure Browser wird geöffnet. Nutzen Sie das Internet wie mit jedem anderen Browser auch. Dieser Browser ist Chromium-basiert und jeder Tab wird in einem isolierten Container geöffnet. Nutzen Sie den Browser, um verdächtige Websites direkt aufzurufen, wenn Ihr Arbeitsablauf dies erfordert. Wenn der Linkschutz per Richtlinie aktiviert ist, öffnet WPS nicht vertrauenswürdige Links automatisch in diesem Browser.

Support erhalten

Erfassen von Informationen

Es werden einige Informationen benötigt, um das gemeldete Problem oder die mögliche Lösung zu erläutern. Bitte unterstützen Sie eine schnelle Problemlösung, indem Sie die folgenden Informationen an Ihren IT-Administrator oder Ihr Sicherheitsteam weiterleiten, so dass diese eine Anfrage in Ihrem Auftrag einreichen können.

Bitte stellen Sie sicher, dass Sie die folgenden **zwingend notwendigen** Informationen übermitteln:

- Gerätename
- Zusammenfassung des Problems
- Zusammenfassung eines Lösungsvorschlags – Wissen Sie, wie wir Ihnen helfen können?
- Ist das Problem konsistent reproduzierbar?
- Können Sie Screenshots von Popup-Fenstern oder Fehlermeldungen beifügen, um die Lösung zu beschleunigen?

Kurzanleitung – HP Wolf Pro Security