HP Wolf Pro Security
Getting Started Guide

Version 1.0

Getting Started Guide – HP Wolf Pro Security

Contents

Introduction

HP Wolf Pro Security (WPS) is comprised of 3 main protection capabilities. You will be eligible on any supported computer to enable all 3 technologies.

1. Threat Containment – Hardware-backed file isolation and containment into full-stack virtual machines.
2. NGAV – Signature-based and behavior-based protection – Quarantine malicious content utilizing AI and deep-learning tools.
3. Credential Protection – Credentials are blocked from being entered on known bad sites and user warned on unknown sites

Since the most frequent source of attack against endpoint PCs occur through downloads from email attachments, malicious websites, and infected links, Threat Containment opens untrusted content in isolated VMs that allow the malware to detonate inside a hardware-enforced virtual machine. This approach keeps the threat from infecting the endpoint or spreading across the network. It also allows the behavior of the content to be monitored for suspicious behavior. Because files are opened in isolation, even zero-day threats are contained. Adding in a next-gen AV and powerful Credential Protection capabilities, you have a complete suite to protect your Windows PCs from the most advanced threats.

Apart from the industry's best security technology, server and agent upgrades as well as automated monitoring for platform integrity are all included. Onboarding is a simple process and troubleshooting help is just a call or email away. You have HP Security Experts waiting to assist you during your engagement.

Targeted Audience

So far you should have either submitted a trial (POC) request form or purchased the WPS product. After approval you would have received an email with instructions on the next steps.

Note: It is critical that a correct email address be entered while placing an order, as the activation email will be sent to that email address.

If you can't find that email or the person who requested access to our service is unreachable, see https://support.hpwolf.com for contact options. Once you have your acceptance email, please navigate to the Onboarding section.

This guide should answer most of your initial questions. Please contact your partner support if you run into issues.

The first part of this document is for *IT and Cyber Security Administrators*. It details:

- Summaries of the product from a technical viewpoint
- An overview of how the IT and Cyber Security Administrators will interact with the Wolf Pro Controller
- What communications they can expect with the service.
- Support portal overview

The second part of this document will review the HP Wolf Pro experience for *end users*:

- Desktop UI
- Health status
- System pop-ups and interactions with the product.
- How to submit a request for assistance.

Quick Links

Accessing your controller instance

Sign-in using your HPID here:

https://portal.hpwolf.com

System Requirements - Hardware and Software

Our products must be installed with a minimum set of hardware and software to function properly, learn more:

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

Technical Support and FAQ

Do you have questions? Maybe the answer is here:

https://support.hpwolf.com

Contacting support

To find out how to contact us, see: https://support.hpwolf.com/s/contact

For IT and Cyber Security Administrators

Product Terminology

The HP Wolf Pro Security solution consist of 2 primary components:

- HP Wolf Security Controller is your HP-cloud-hosted "controller" for administrators to manage the endpoint "agents"
- HP Wolf Security is an "agent" that consists of several software features that are installed on individual end-user computers.
    - HP Wolf Pro Security Protection features
    - HP Wolf Security "Desktop Console" to review agent status or enable/disable features on a local device.
    - HP Sure Click Pro Secure Browser, a browser that uses Threat Containment features to open pages isolation. Additional browser extensions and an Outlook plug-in are also automatically installed

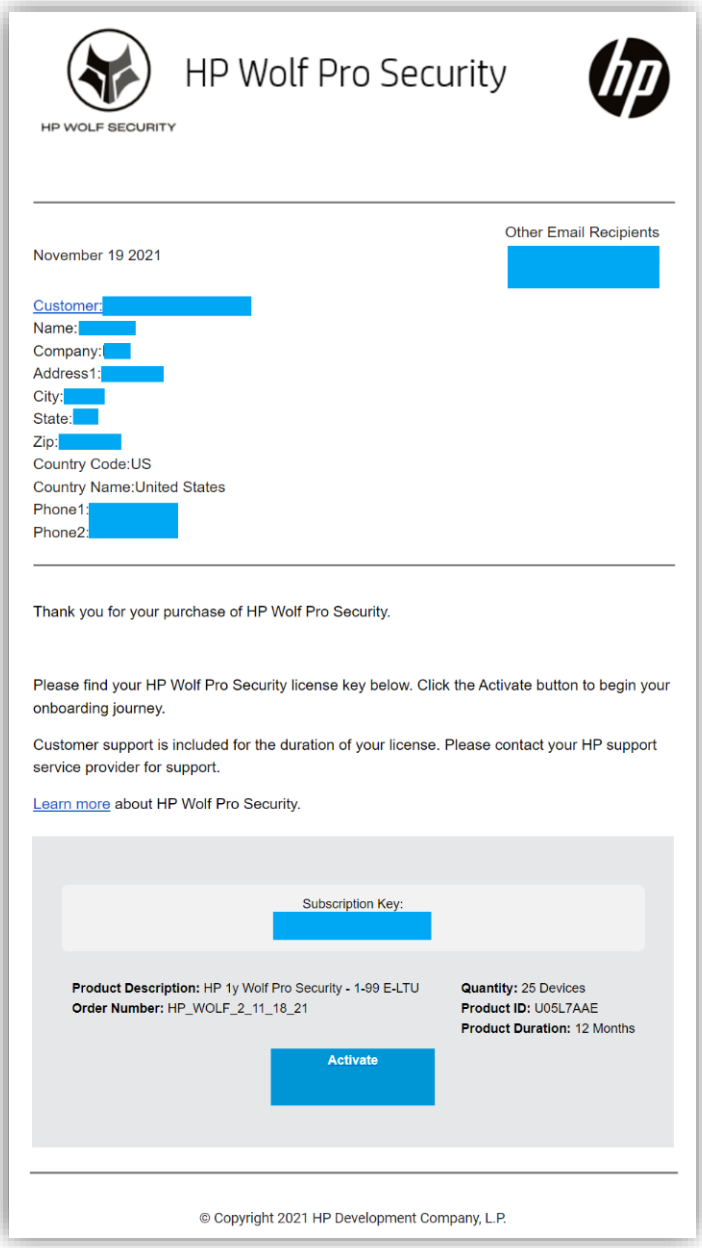
Self-Onboarding and Activation

The journey to get WPS installed and protecting your endpoints begins with the activation and onboarding step.

In certain cases, depending on how you purchased WPS, your managed service partner might do this step for you. Please check with your MSP.

Activation Email

Whether a POC request has approved or WPS has been purchased, the initial journey begins with the customer (or MSP) receiving an email from HP. This email contains the license key, SKU information and an activation link.



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.

Clicking on the activation link will begin the onboarding flow.

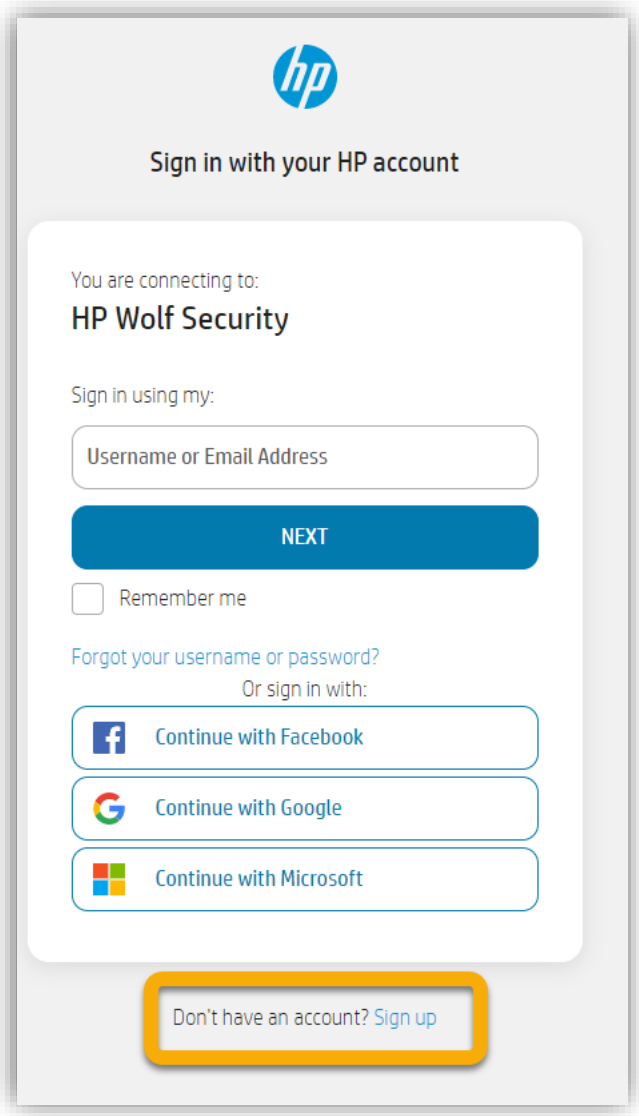
Onboarding wizard

There are a few simple steps that need to be taken to activate WPS.

Step 1: Login with your HPID

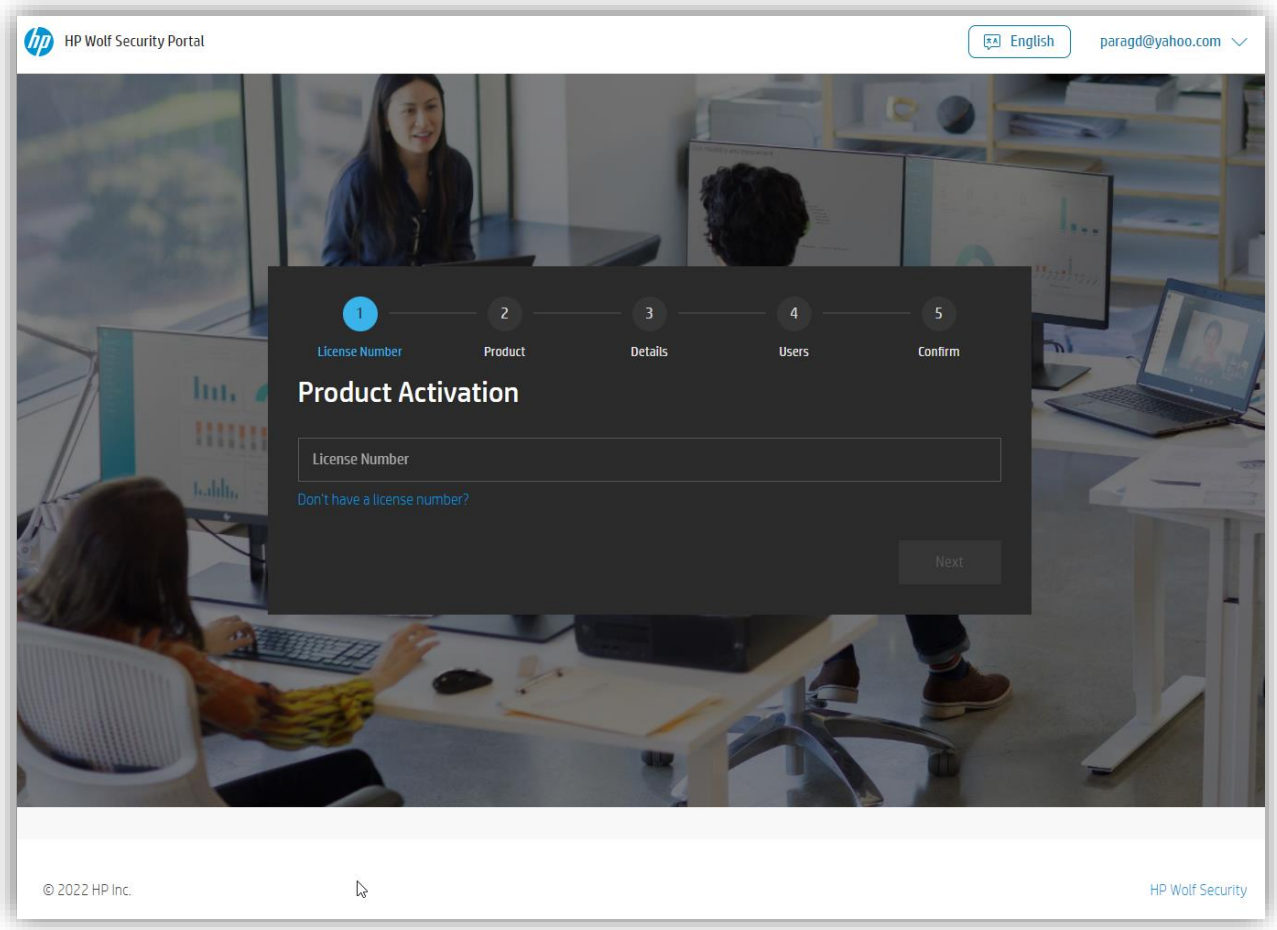
Clicking the Activate link will first ask for your HPID login.

1. If you already have an account with HPID then proceed to enter your credentials.
2. If you do not have an HPID account, follow these steps.
3. Select Sign up at the bottom of the page.



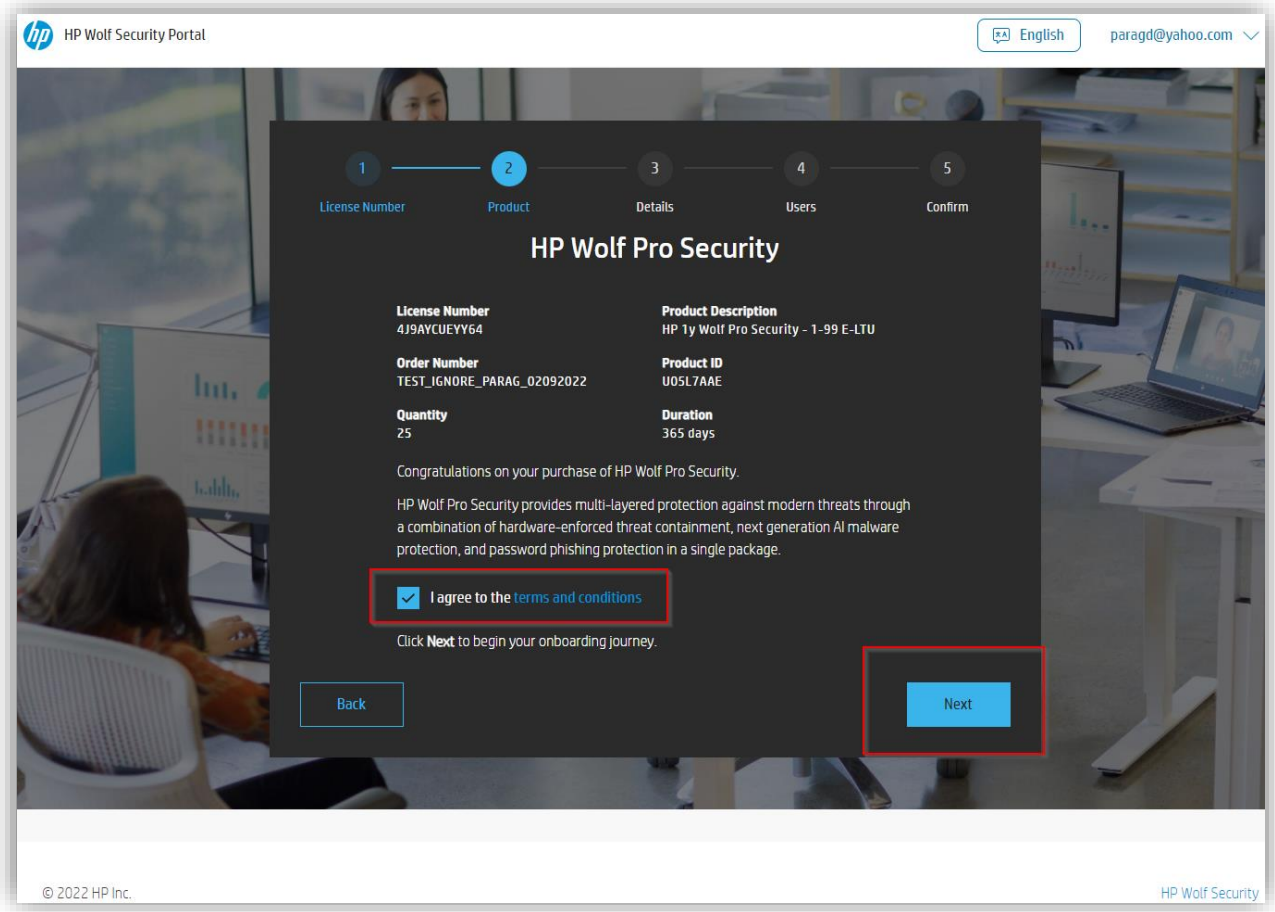
4. Fill in your account information and select Create Account.
5. There will be a 2FA step where you are required to enter a code that is sent to the email address that was entered.
6. Once the account is successfully created, you will be automatically re-directed to your controller and should see the view below:

Step 2: License Validation



In most cases, the license number will be automatically filled in. If not, please copy and paste the license number that was sent as part of the email message and click NEXT.

When the license has been successfully validated, you will see the following screen:



Please make sure you read and accept the terms and conditions, which also contains a link to the privacy policy and a data FAQ document.

Unless the terms are accepted, the NEXT button is not usable.

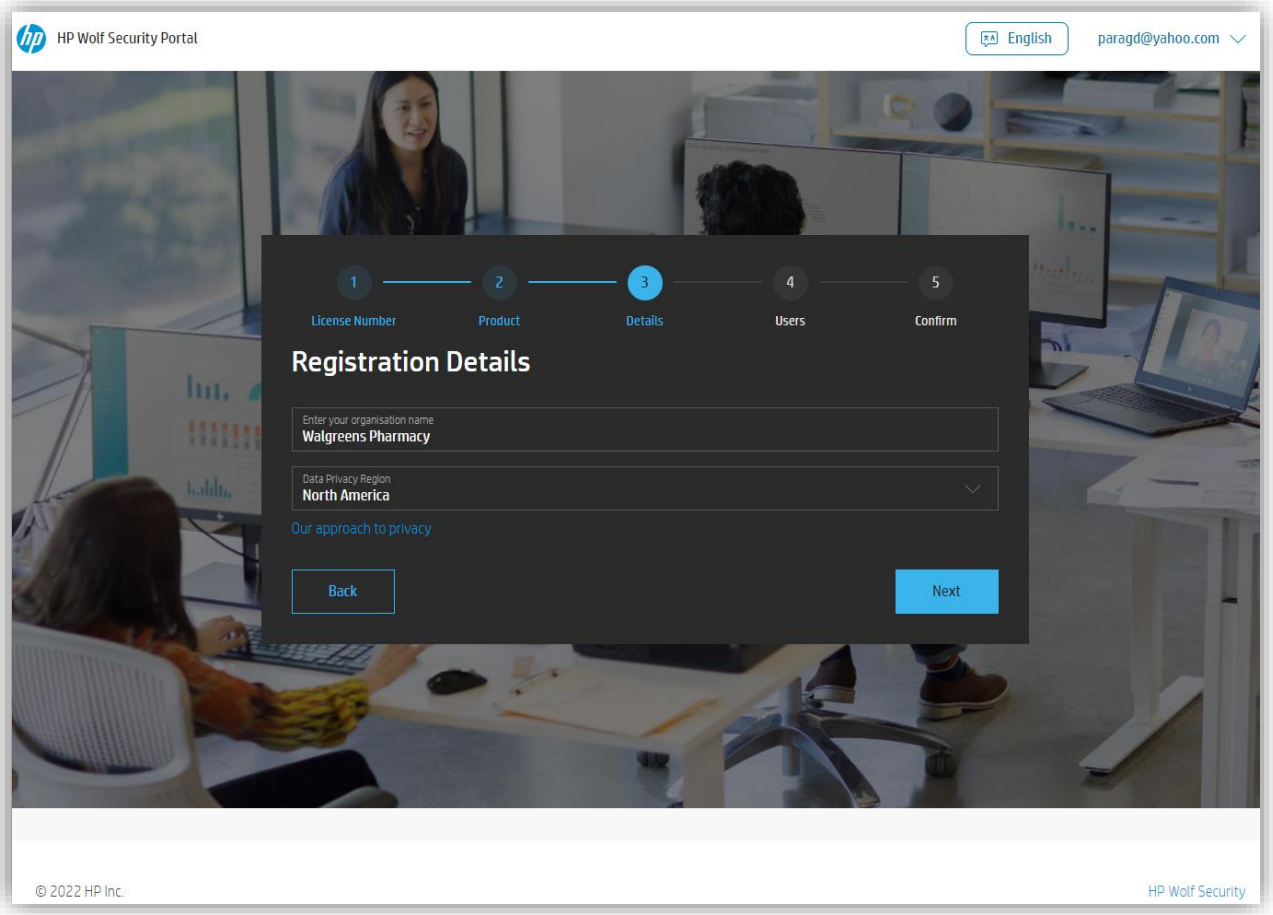
Once you read and accept terms, please click the next button.

Step 3: Tenant Information

The next step is to enter your tenant's name and select the data region. This determines where your tenant is created, and your data stored. At the time of writing, there are only two options:

EU and North America.

For countries outside the EU, please select North America. More data regions will be created as needed to satisfy any regional and other privacy restrictions.

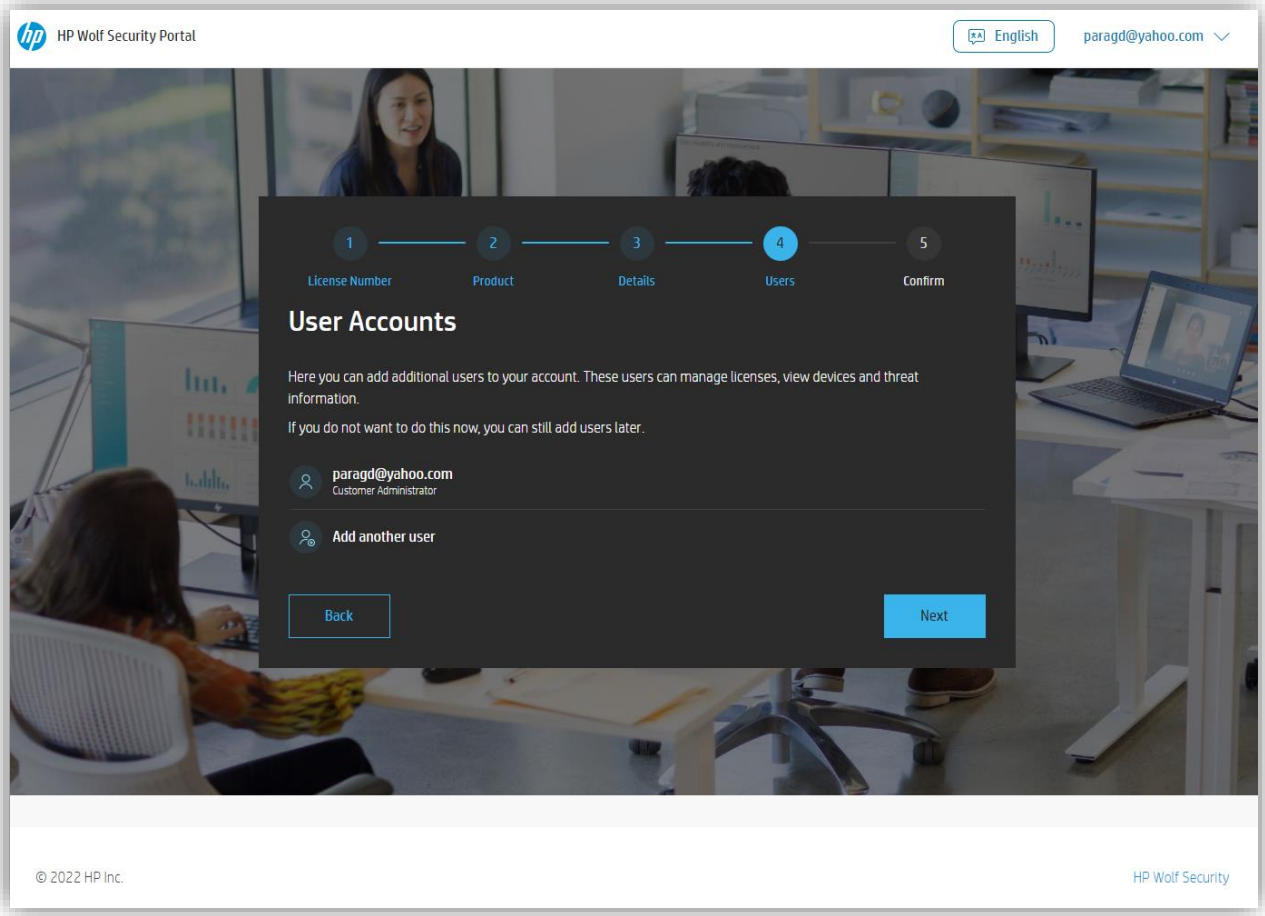


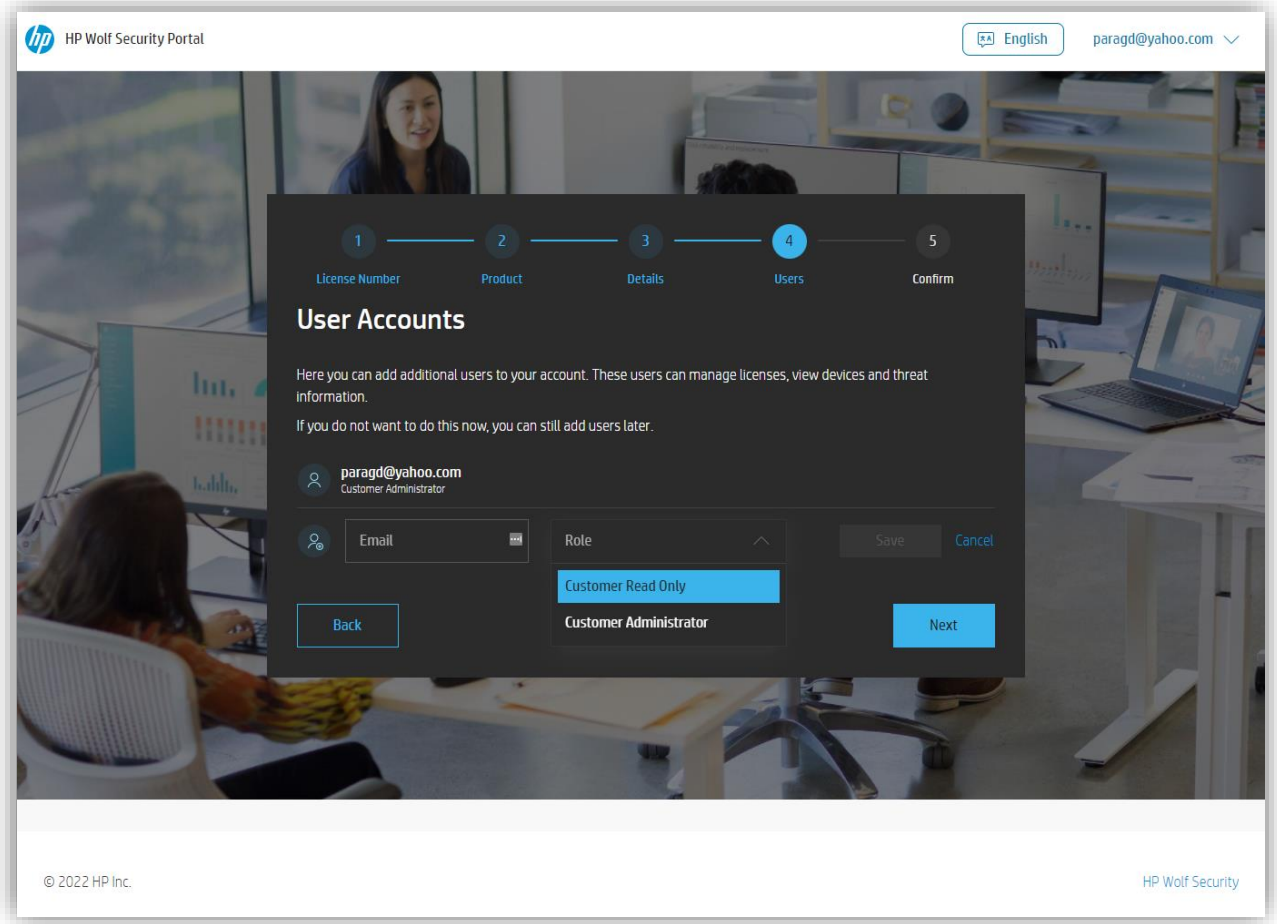
Step 3: Adding users

The HPID that was used for onboarding is created with a default Customer Administrator role. If needed, add additional users that need access to the tenant here. At this point, there are only two options.

Customer Administrator – Administrator can make changes in the Controller.

Customer Read Only – Can only view the Controller settings and reports.


HP Wolf Security Portal
English
paragd@yahoo.com
1
License Number
2
Product
3
Details
4
Users
5
Confirm
User Accounts
Here you can add additional users to your account. These users can manage licenses, view devices and threat information.
If you do not want to do this now, you can still add users later.
paragd@yahoo.com
Customer Administrator
Add another user
Back
Next
© 2022 HP Inc.
HP Wolf Security



If you are an MSP that is onboarding your customer or activating the software on behalf of your customer, this is where you might enter the customer IT admin or equivalent authorized users email address. Similarly, if you are a customer who is self-onboarding and need to give access to your managed service partner, you would enter your partner's email address here.

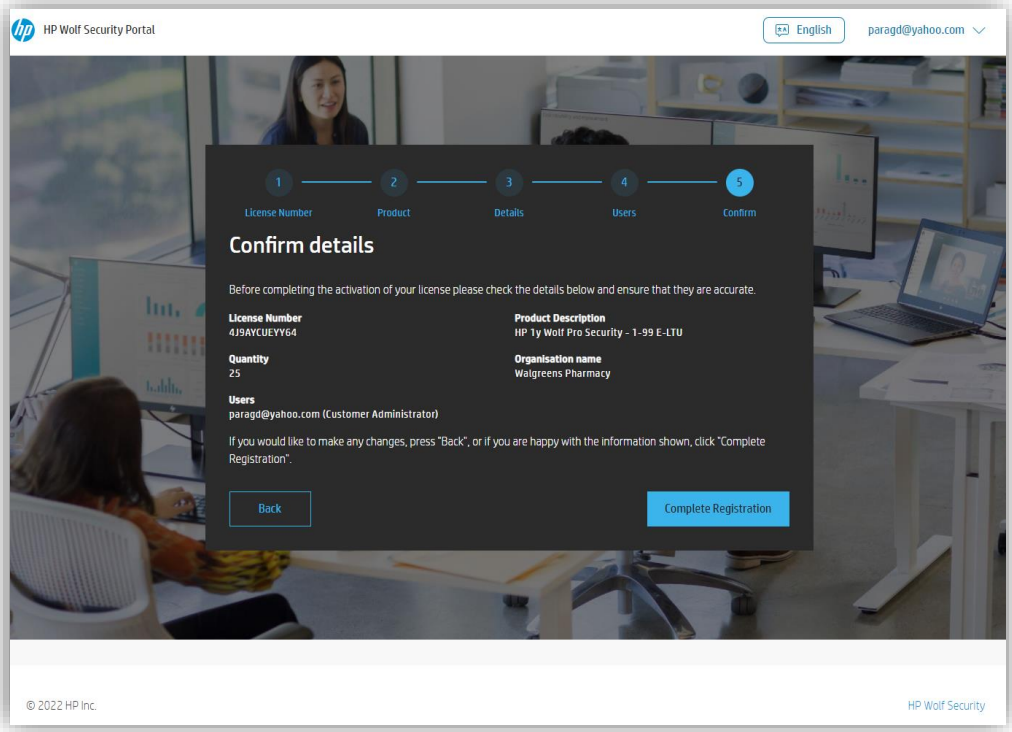
These additions can be done later as well.

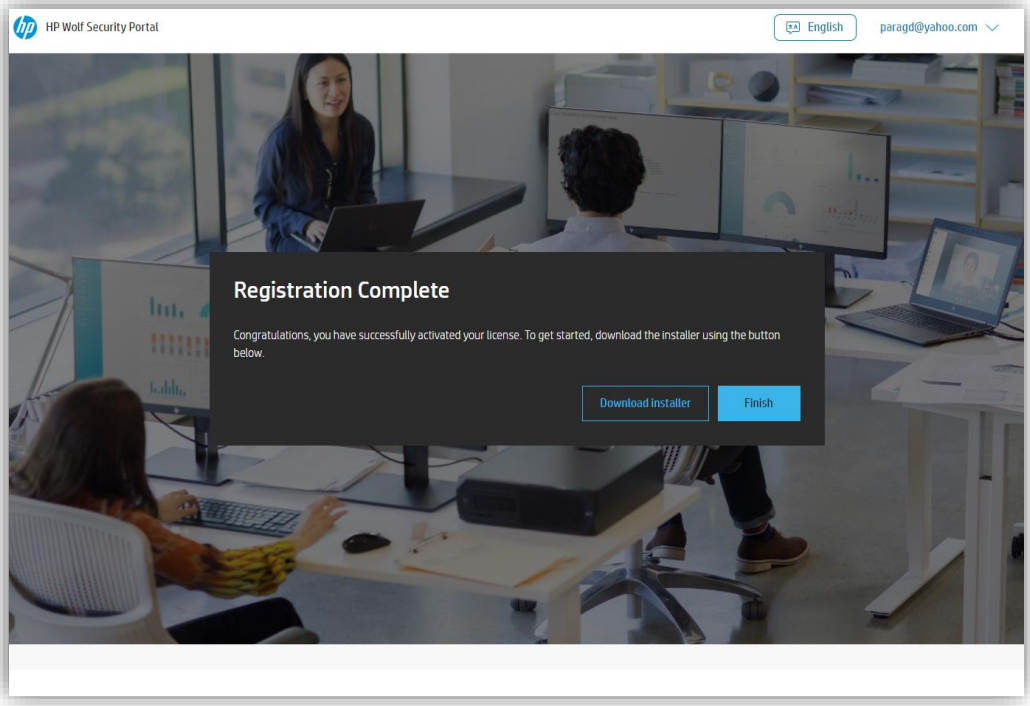
Once you have added the required users, move onto the next step.

Step 4: Complete registration

Next you will be shown a confirmation page. Make sure all the details are correct. Go back and make changes if needed. If not, complete the registration:

Getting Started Guide – HP Wolf Pro Security



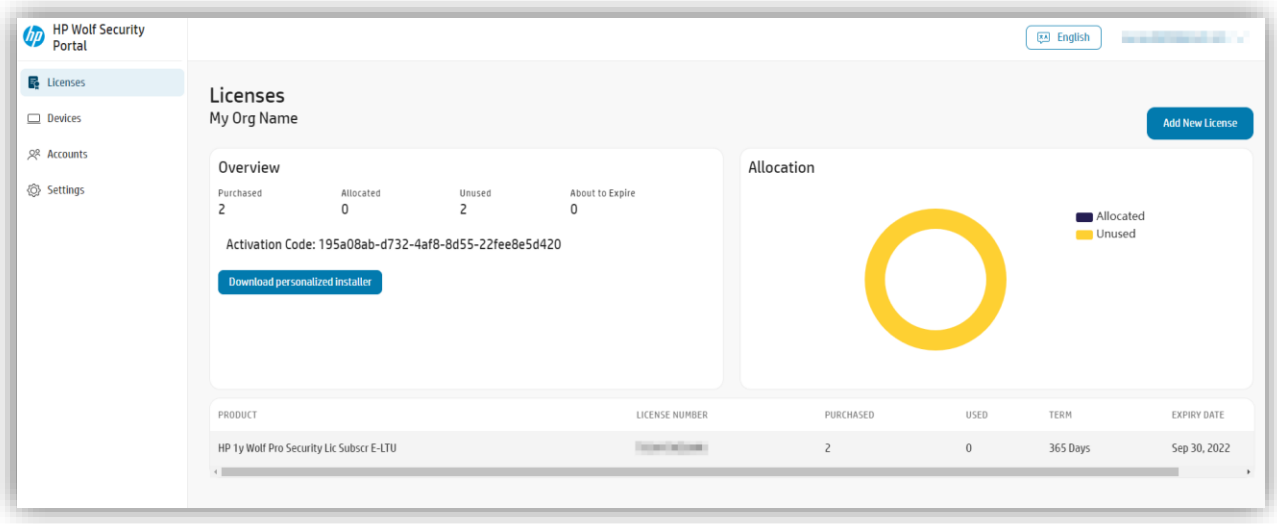


Step 5: Setup Cloud Features

All customers get access to a cloud console. However, there are some key differences

Less than 25 seats purchased

If you have bought a license for less than 25 seats, then you will see this screen right after you complete the registration in the previous step:

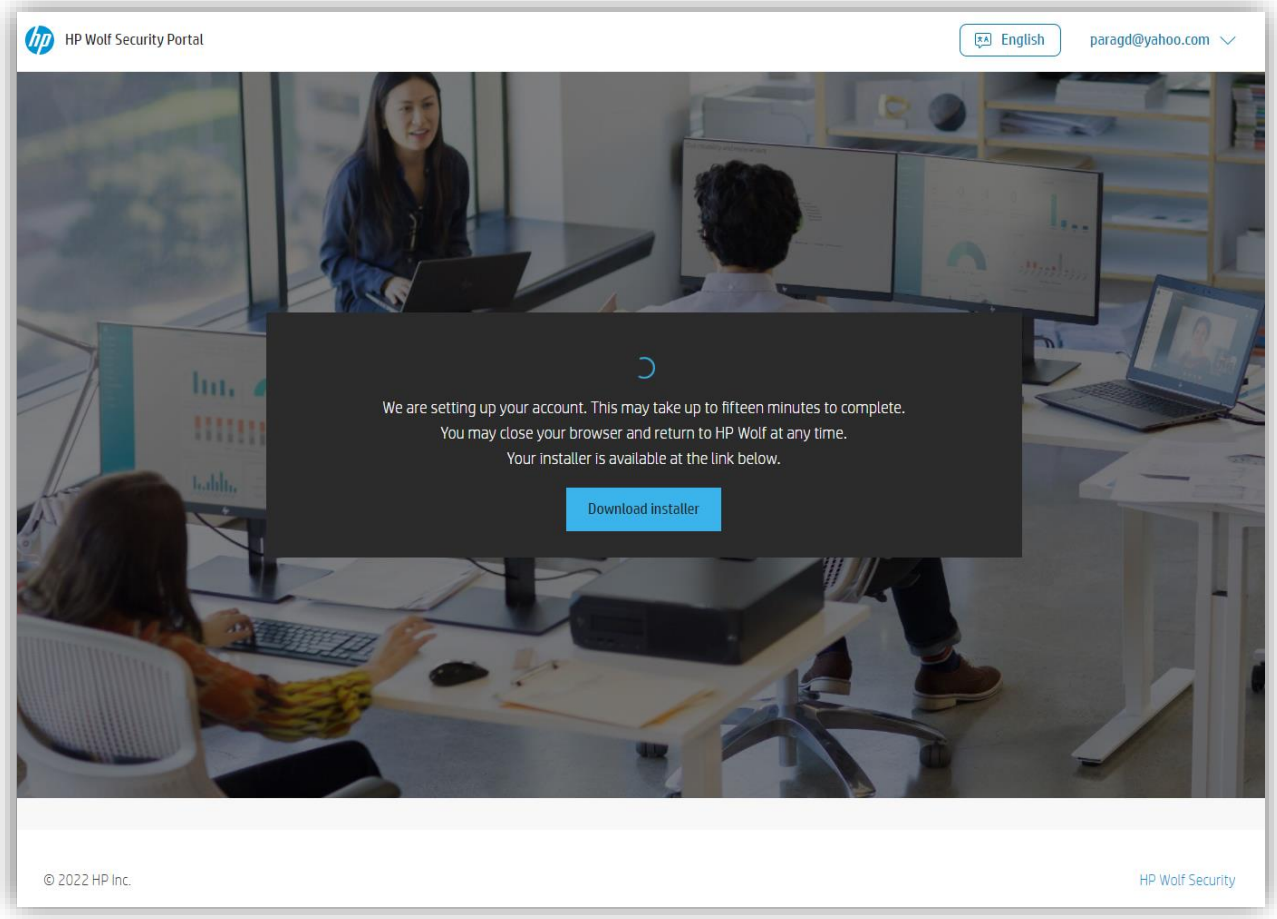


This console allows you to view and manage licenses and user accounts and see basic details of devices connected to the tenant. To unlock full management features, 25 or more seats need to be connected to the tenant.

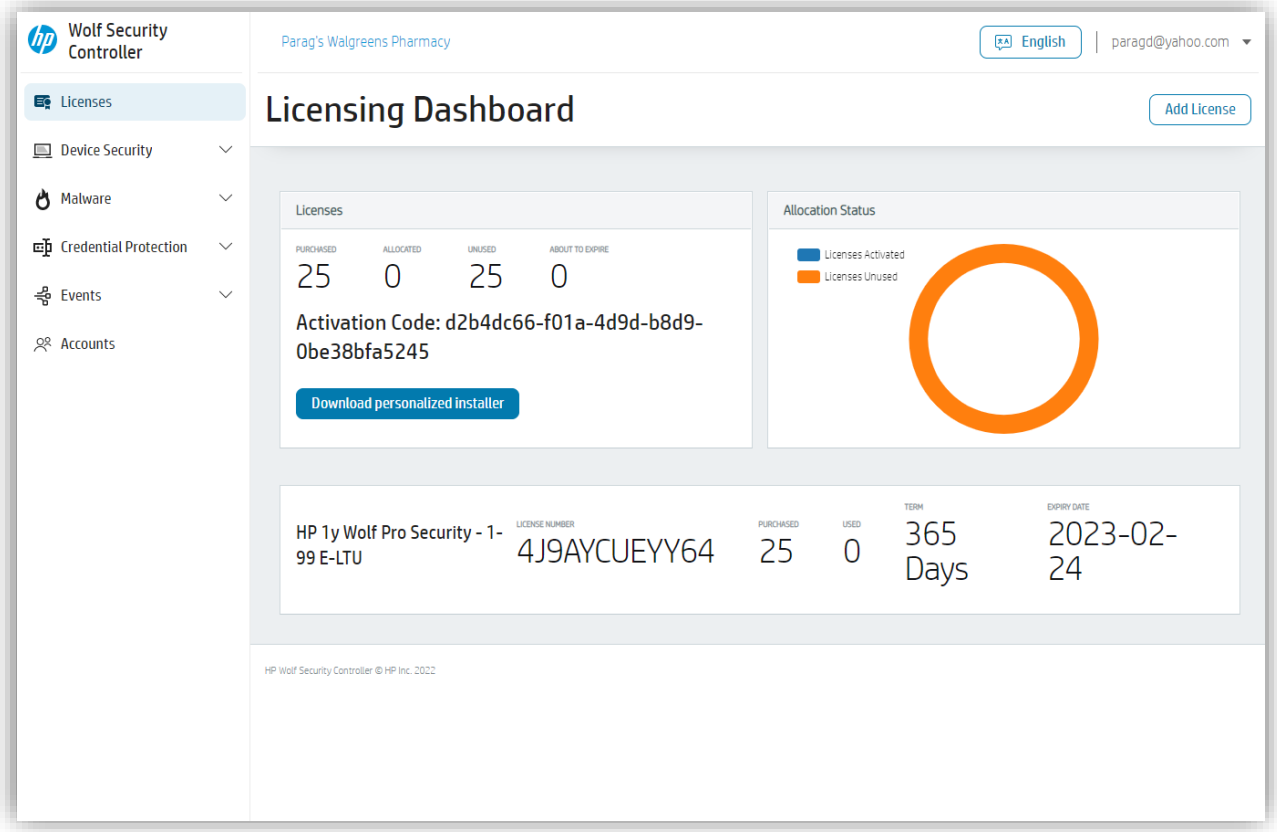
In case additional seats are purchased and connected to this tenant (that takes the total above 24) or a license is activated for a new tenant with more than 24 seats, this will automatically activate full management capabilities of the tenant. See below.

25 or more seats purchased

If more than 24 seats have been purchased, or if the activation of this license on an existing tenant results in a total of 25 or more seats allocated, this next step will result in the unlocking of full management capabilities. This step can take anywhere from a few minutes to 15 minutes, as WPS takes steps to ensure complete and comprehensive data separation between tenants. Clicking on the 'Finish' button in the registration screen above will show the following:



Once the tenant has been created, you will be automatically redirected into your tenant, and should see something like this:



Installing the endpoint agent

The product installer is available for download as soon as the tenant is setup and before the controller instance has been created.

HP recommends that the installer be run only after the controller has been fully created. This is because the installer needs to download certain product information and packages from the controller.

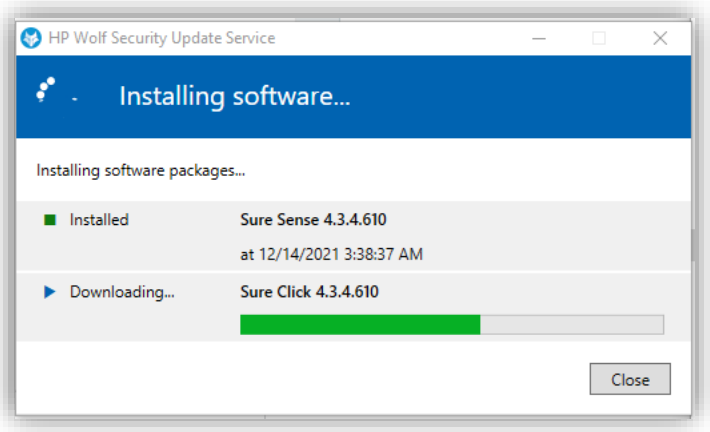
The installer for our product can be found when logged into the controller and on the Licenses page. If you already download the installer in prior steps (before the controller instance was created), you do not need to download it again.

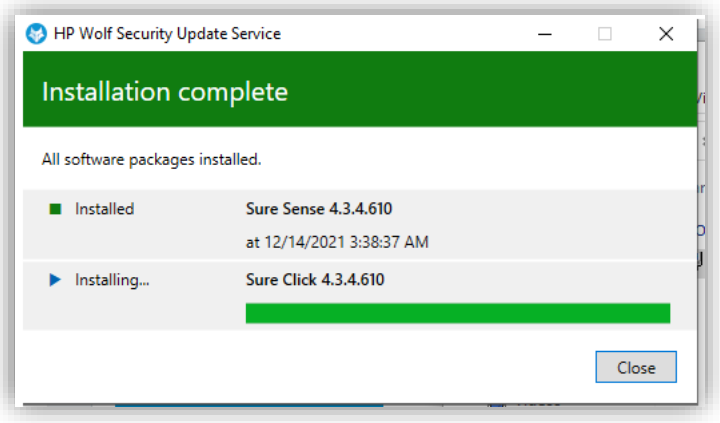
This installer, named *HPSecurityUpdateService – [your tenant's name will be here].msi*, is only around 2MB in size and will quickly install on the computer. The installer will perform a series of checks and begin to download and install the agent to your computer shortly after you run it.

Installing on a single device

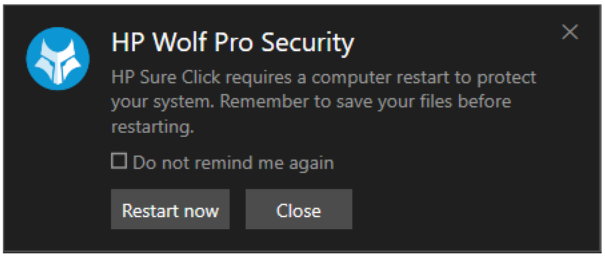
- Right click the installer and select Install.
- Note: The installer will automatically connect to the right cloud tenant. You do not need to run the installer with any special command lines unless you want to install the agent silently.

- You will need to enter administrative credentials if you are currently a limited user of the computer.
- The installer is interactive when run this way and you will watch the applications download and install one at a time. Based on your computer's available resources, this process can take up to 10 minutes but will likely by faster than that



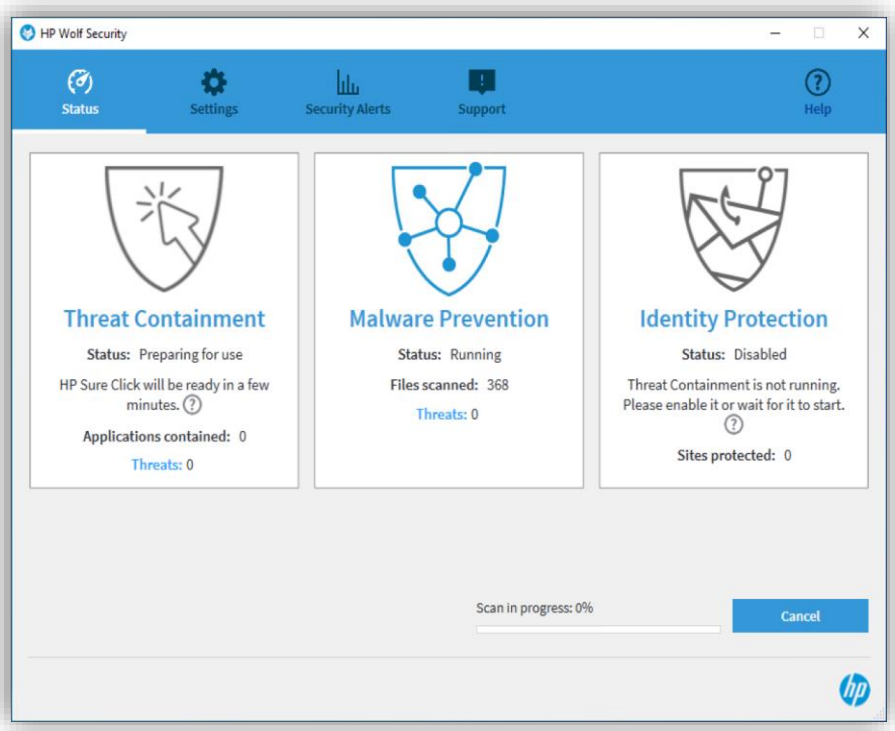


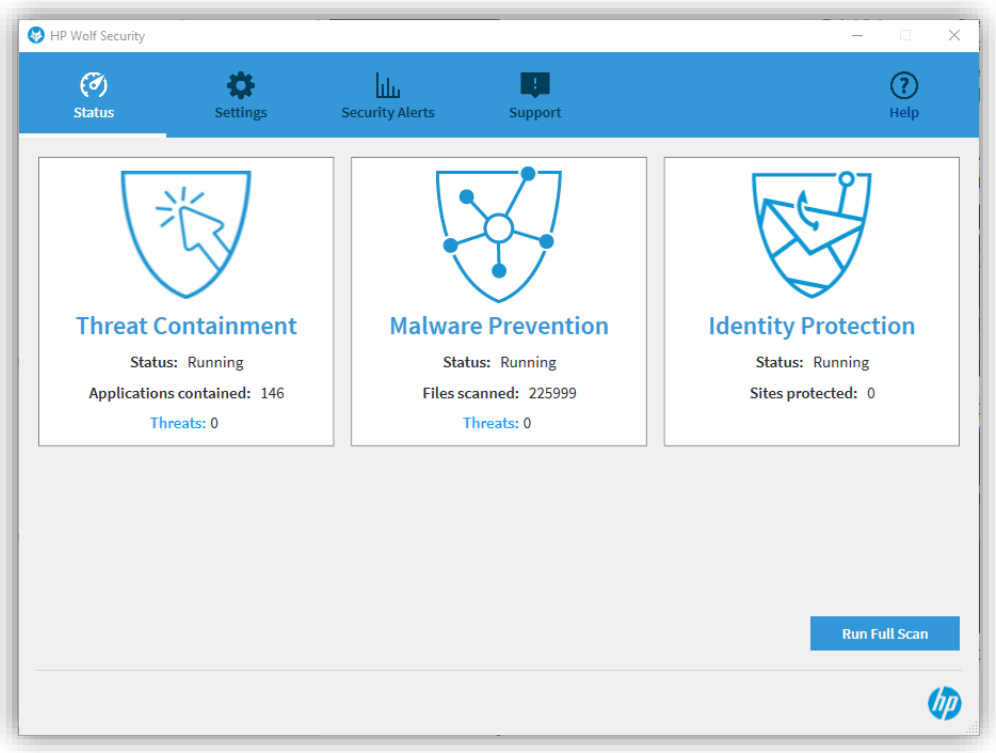
You will see a pop up in the lower right of your view instructing you to restart the computer to finalize the installation. You can restart using the "Restart now' button on the alert restart later. To restart later, click the Windows icon in the corner of your Start tray and select Power | Restart. (Do not choose Shutdown.)



After the computer restarts, you will be able to find the HP Wolf icon in the system tray  as well as the new applications in the Start menu.

The agent will do a few house-keeping steps. This includes initial setup, establishing a connection with the cloud tenant, and running a full scan to check for any existing malicious content on the PC. During this time, opening the "HP Wolf Security" console above will show something like this:





Deploying to multiple devices

You can deploy the installer from any centralized deployment solution such as SCCM or BigFix. You can also easily deploy this via GPO and a file share.

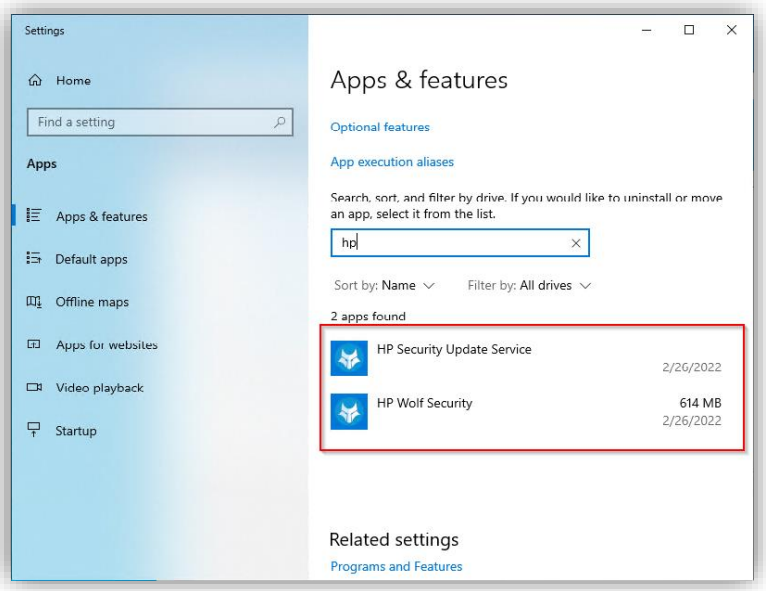
Since this is an *msi* package you can use all the standard *Msiexec.exe* flags such as silent installation or log to file.

Uninstalling the Agent

The uninstall operation will remove HP Wolf Pro Security from the PC.

Note: All the components shown below need to be uninstalled, to avoid unexpected outcomes. For e.g.: If the HP Security Update Service is not uninstalled, it will try to download and install the agent again. Please uninstall all the components below for a full uninstall.

- Open the "Add or Remove Programs" in Windows settings.
- Uninstall both **HP Wolf Security** and **HP Security Update Service** applications.


Settings
Home
Find a setting
Apps
Apps & features
Default apps
Offline maps
Apps for websites
Video playback
Startup
Apps & features
Optional features
App execution aliases
Search, sort, and filter by drive. If you would like to uninstall or move an app, select it from the list.
hp
Sort by: Name
Filter by: All drives
2 apps found
HP Security Update Service
2/26/2022
HP Wolf Security
614 MB
2/26/2022
Related settings
Programs and Features

Getting Started Guide – HP Wolf Pro Security

HP Wolf Security Controller Overview

Note: The HP Wolf Security Controller is only available for installations with 25 or more seats. If you are not eligible for a controller, most of the features described below will be unavailable.

The HP Wolf Security Controller is your gateway to interacting with your security service. This controller is a dedicated controller and is not shared by any other customers. This ensures true separation of data. While some threat data is anonymized and aggregated to improve monitoring and alerting processes, this data stays within the service and is never shared with vendors or 3rd parties. The dedicated HP Wolf support team can access to your controller for support purposes. HP meets or exceeds ISO and SOC compliance standards for user and administrator access.

Learn more about HP's privacy policy here. Also click here to view the Hp Wolf Pro Security data FAQ.

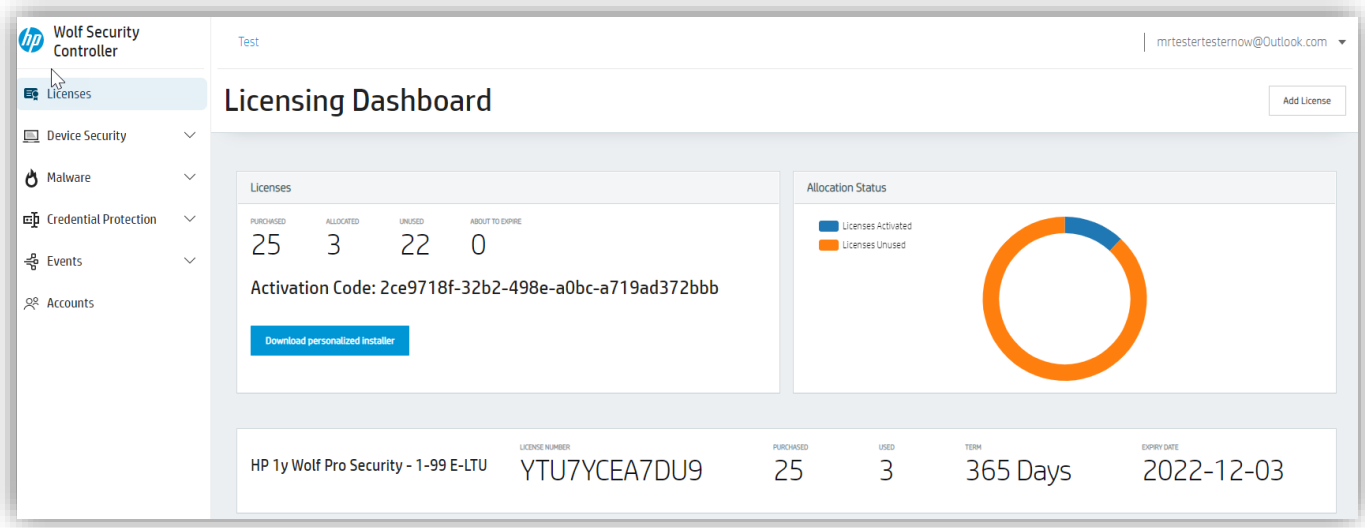
This guide assumes you have already had your controller prepared and you have access to it.

Login

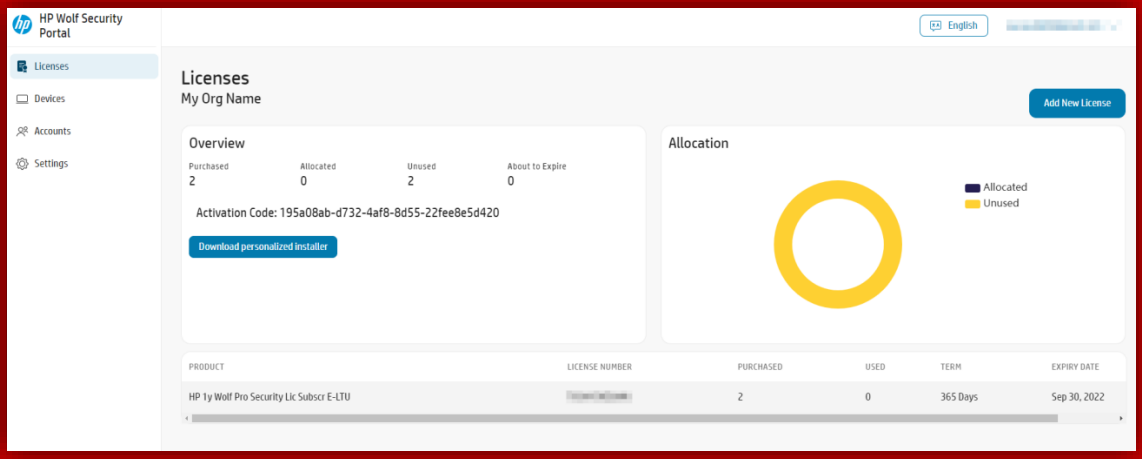
Access to your controller is found at:

https://portal.hpwolf.com

When you first login to the controller you will see the view below. Starting from the top option on the left-hand menu is the **Licenses** page.



Note: If you have less than 25 seats connected to the tenant, only the Licenses and Accounts sections below will apply to your tenant. You can enable the full management feature set by purchasing additional licenses.



Licenses

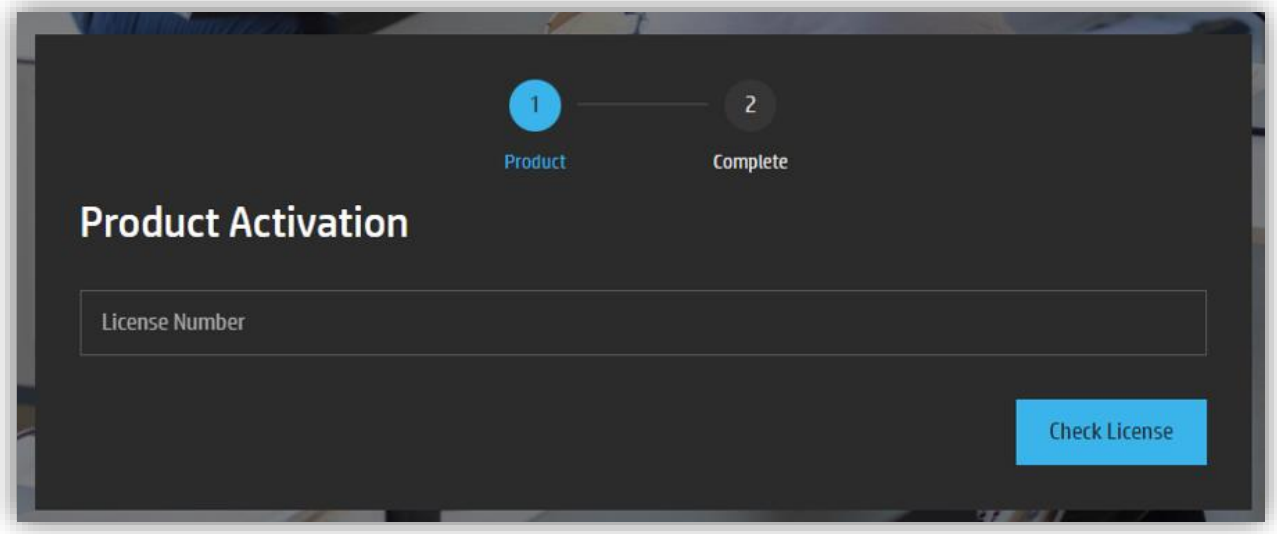
The **Licenses** page contains all the administrative data you need to review your account. Number of licenses Purchased, Allocated, Unused and About to Expire is shown at the top.

Here you can also download the HP Wolf Pro Security installer (.msi) which is specific to your controller and cannot be used with any other products or controller environments. We will cover this in detail in the Installation section below.

The **Licenses** page is also where you will come to view your license number, days remaining of licensed product and can apply new licenses keys.

Applying new license keys to the same tenant

Click the Add License option in the upper-right corner of the page. Enter the license key provided by HP and select Check License.

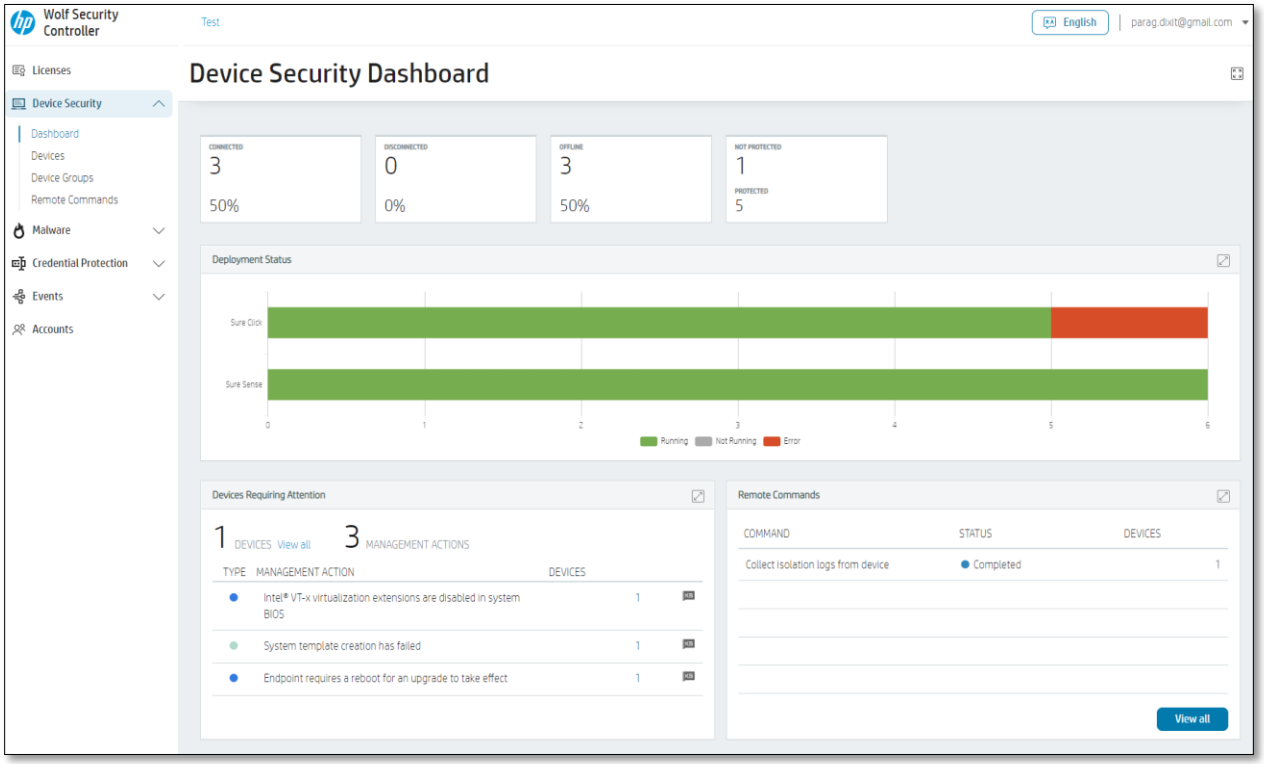


Once this step is complete, the controller Licenses page will automatically reflect the new license and the number of additional seats and term available.

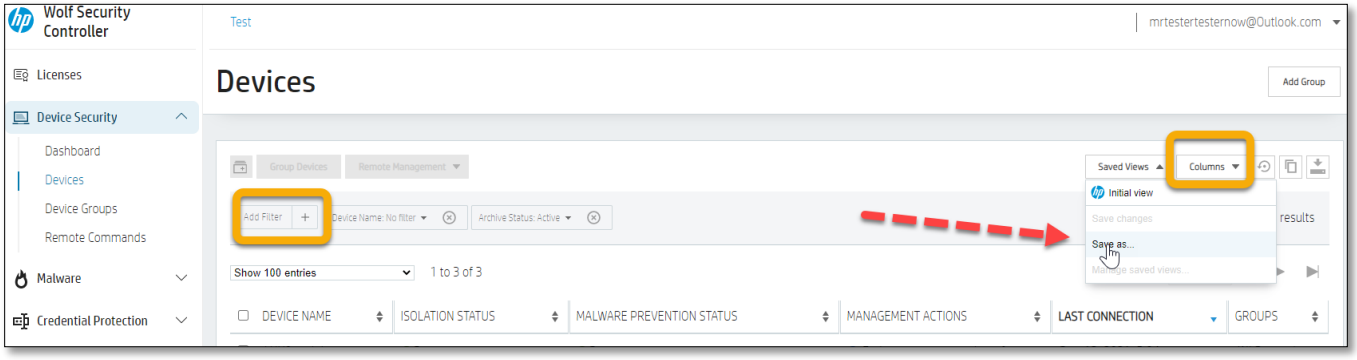
Device Security

This section is helpful for the device administrator or security specialist responsible for keeping track of metrics related to the health of the agent fleet, current deployment, or general questions such as “How many devices are fully protected?” or “Which devices need to be reviewed?”

- **Dashboard** gives you an overview of the devices that are running the product. From the dashboard, you can track key device health stats, overall deployment status and the results of remote commands. The dashboard is very interactive, and you can click on any relevant box or item in the dashboard to be shown more details about the item in question



- **Devices** lists all the devices connected to this tenant. It will be a very helpful page in that you can save custom device views so there is no need to keep looking for items you are interested in. Set the columns and filters as you would like to see them each time that you come to this page and select *Save As*. Name each saved view, so you know what they represent at any given time.

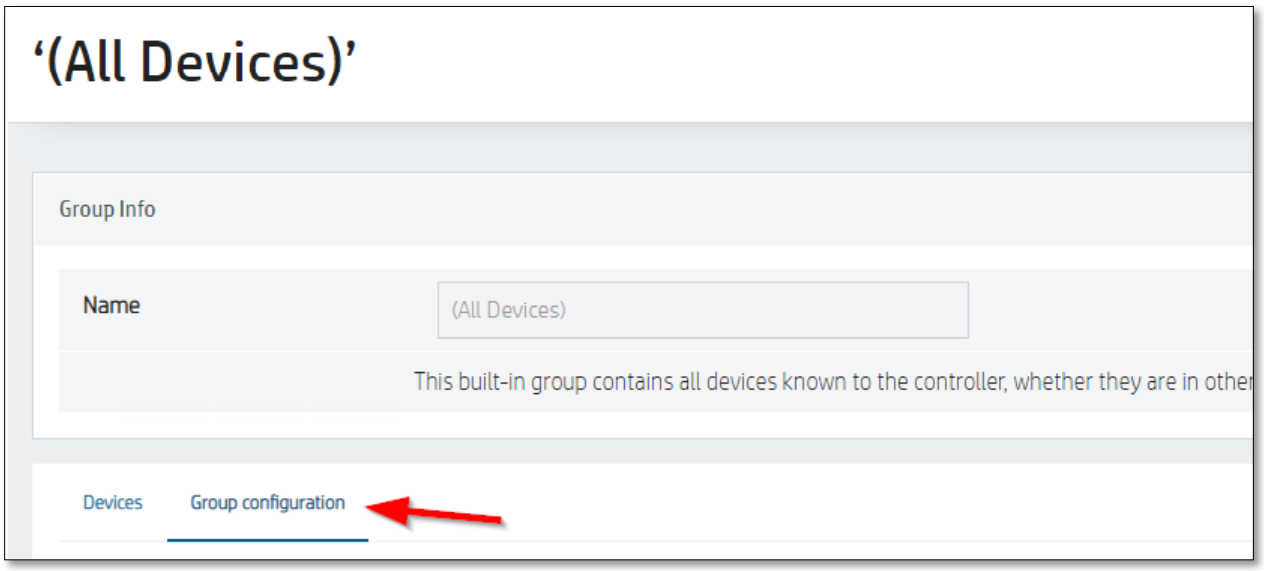


(All Devices) group and policy

WPS allows you to set certain policy values that determine product behavior. It is highly recommended that you build your ***company-wide*** policy in the (All Devices) group. Any new device being onboarded to this tenant automatically gets this policy applied.

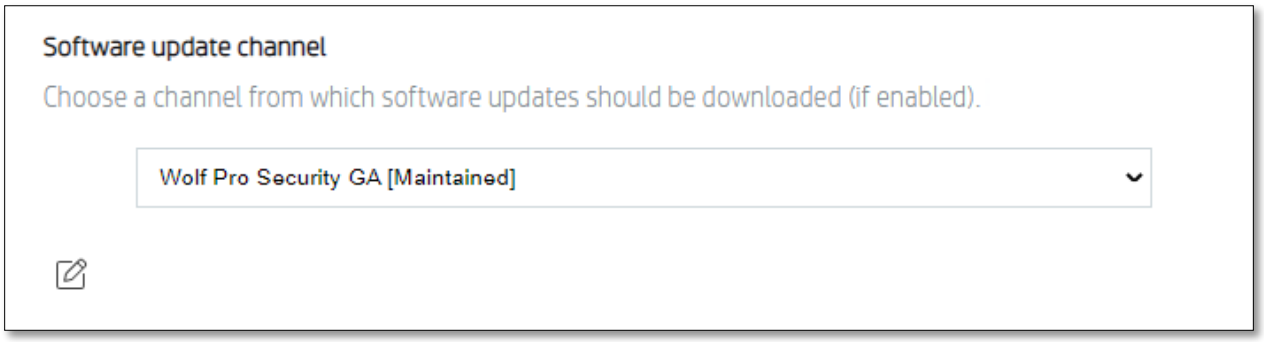
Let's look at the policy settings and how they affect endpoint product behavior:

Begin by clicking on the ***(All Devices)*** group in the **Device Groups** page and click on **Group Configuration**



Sure Click Policy settings

Software Update channel



Select the software update channel that will be used to update the endpoint software. In most cases, this would be left as the default selection for HP to manage software updates.

In cases where a new test or POC build might be required, it's always better to do it by first creating a new device group, adding the required devices to that group, and assigning a policy to that group that changes its software channel. See the next section "Custom device groups and policy" for more information

Trusted Websites

Add sites here that will be opened by the secure browser without isolation. This is useful in case there are internal or known trusted domains that do not need to be opened in a secure virtual machine.

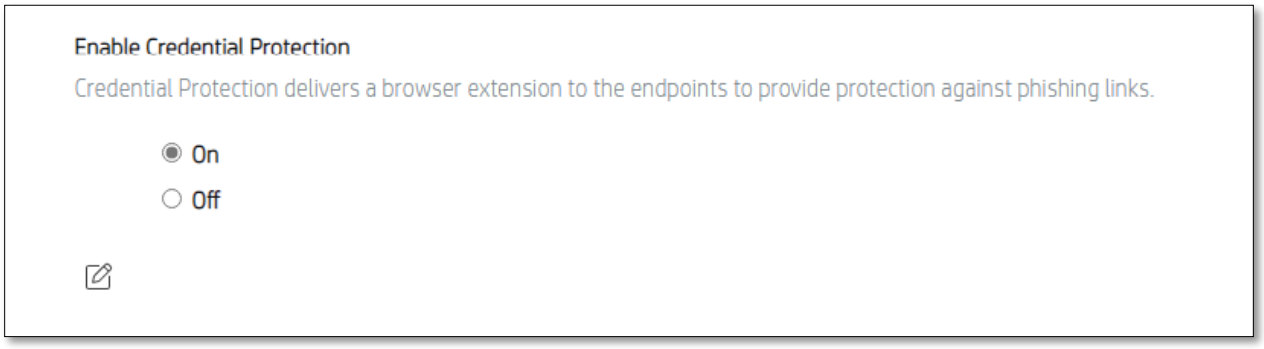
Be very specific here, otherwise all subdomains of a TLD will also open without protection.

For e.g.:

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

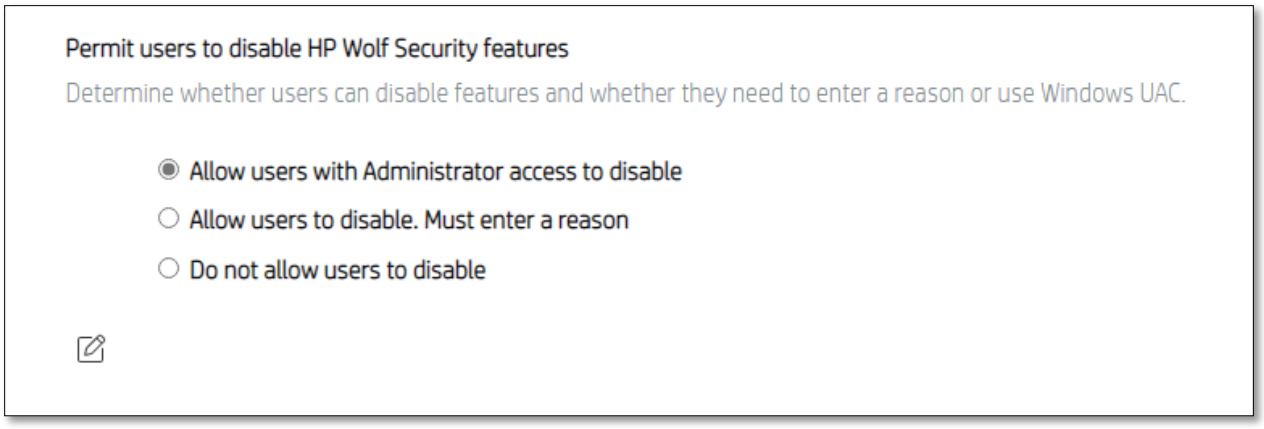
NOT SECURE: https://sharepoint.com

Enable Credential Protection



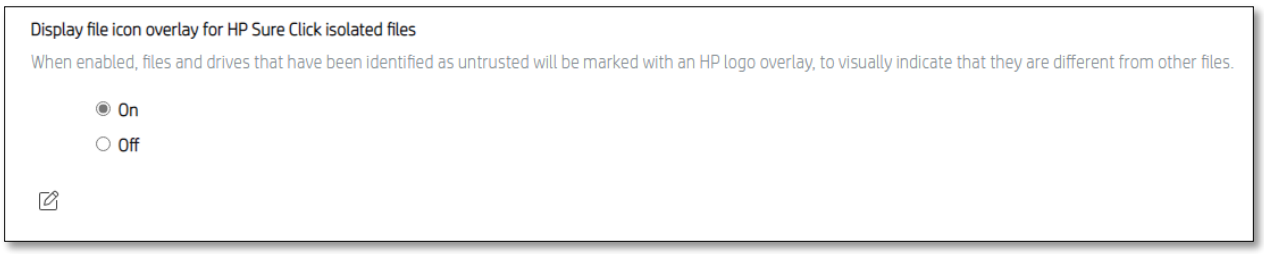
This turns on or off the Credential Protection feature. If this is turned OFF, users on the endpoint cannot turn it back ON.

User control of WPS endpoint features



Use this setting if you want to enact strict end-user behavior and don't wish to allow end users to disable any protection features, or only disable features if they are a local administrator. You can also allow standard windows users to disable, but they must enter a reason. These reasons can be tracked in the 'Events' section described below.

Icon overlay control

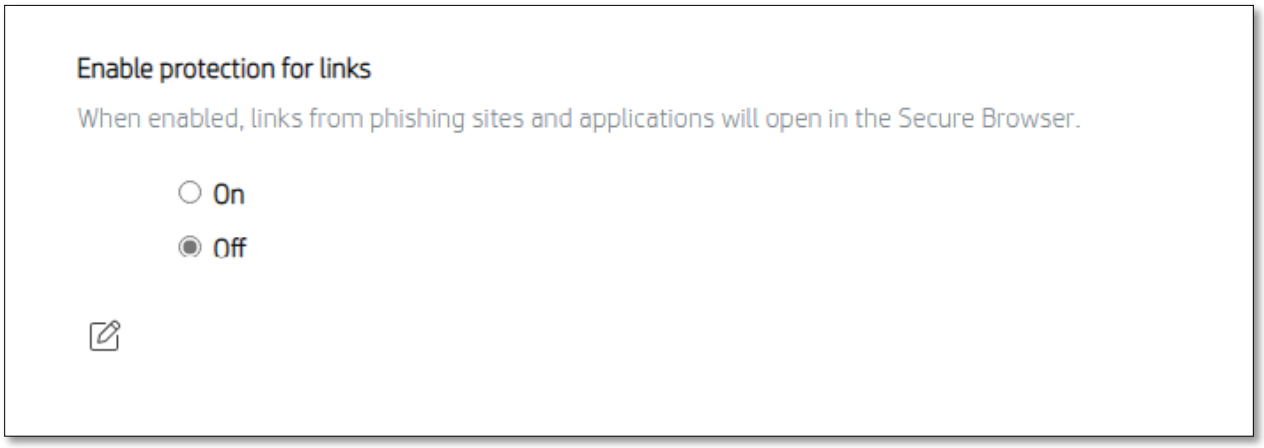


When a file is deemed *untrusted* by WPS, which means it was downloaded off the internet or was an email attachment from a non-internal sender or from various other ingress points, a small Wolf overlay icon is shown on the file. This indicates to the end-user that the file is protected by WPS and will always be opened in isolation.

This policy setting removes this overlay icon.

Note: This setting is useful if your employees have gotten into a habit of removing protection from files before they work on them. Removing protection from documents is not necessary in almost all cases because WPS allows users to edit documents and save them locally while the document is opened in an isolated container.

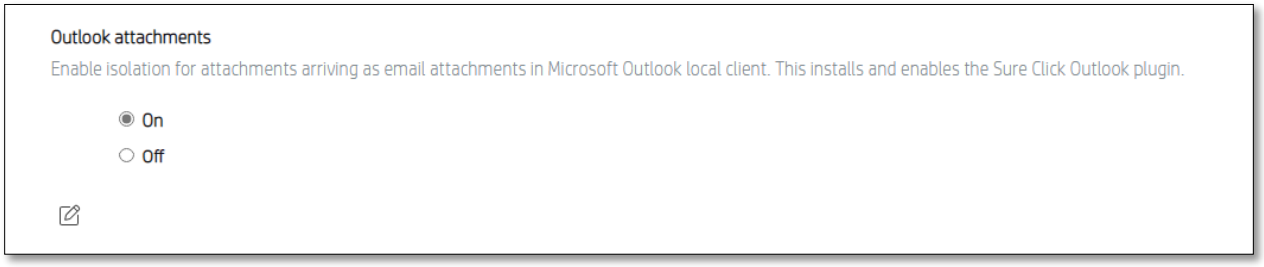
Link protection



Link protection works in conjunction with the trusted sites list. If this setting is turned ON, then any links clicked from email, chats or other link ingress points will open in a secure browser, regardless of what the users default browser is set as. If the link is in the trusted sites list, it will open in the default browser.

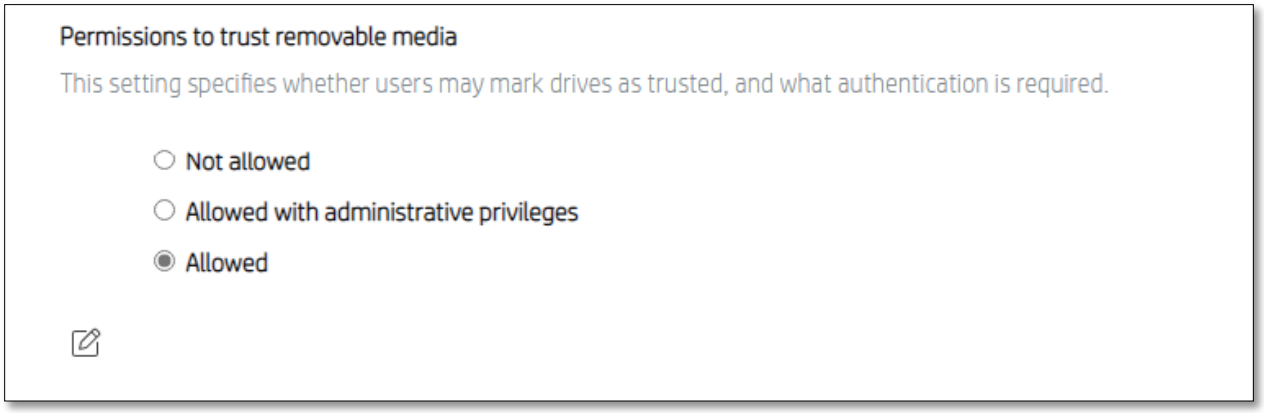
Note: Use this setting with caution. It's usually not needed, because most malware ingress points today are documents that are downloaded from malicious websites. Regardless of this setting or the trusted sites list, downloaded files are always considered untrusted.

Outlook attachments



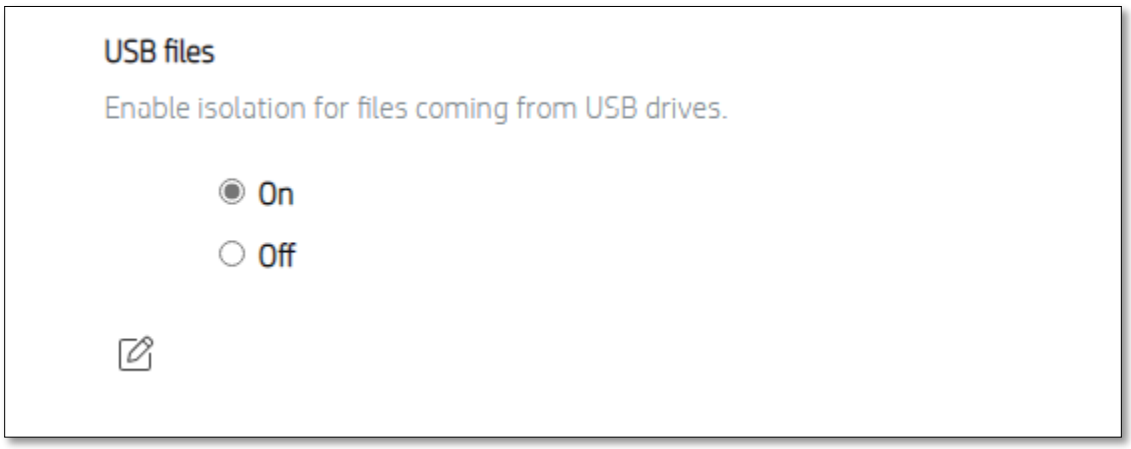
This setting is specific to Microsoft Outlook. Use this if you want to enable isolation for files that arrive as attachments in Outlook emails. The recommendation is to leave this setting ON.

Removable media settings



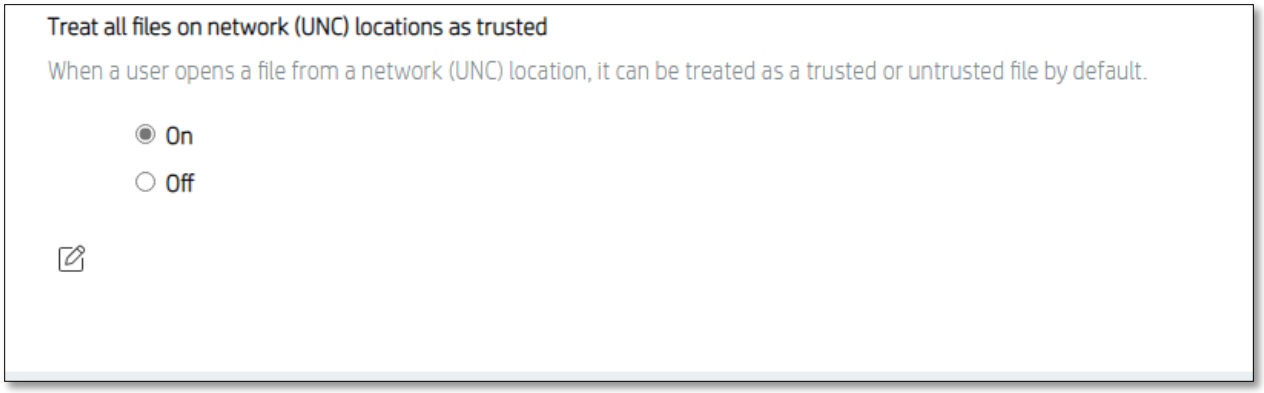
Note that this setting is not a substitution for device control. This simply allows end-users the ability to trust removable media connected to their PC. By default, files on the media will be untrusted and so will open in isolation. If you want a tighter security posture, set this to Not allowed or allowed only with local admin privileges.

USB Drive control



This setting determines whether USB devices are to be trusted. If left ON, and files that are opened from or copied to the end-user PC from a USB drive will be considered untrusted and will open in isolation.

Network (UNC) drive control



When a file is opened from a network location, it can be opened in isolation if this setting is ON

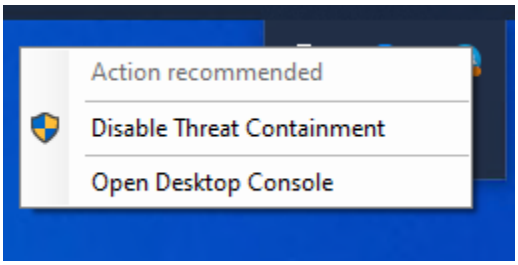
Sure Sense Policy settings

The following policy settings are configurable for the NGAV portion of WPS

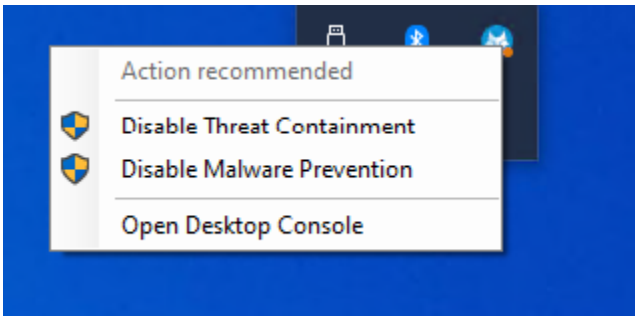
Enable/Disable Sure Sense

This allows you to configure the status of NGAV on the endpoint. If set to **Enable** or **Disable** via this policy, then NGAV on the endpoint will remain either Enabled or Disabled, and the user cannot change that state.

When set to either **Enable** or **Disable** via this policy, the user option to enable or disable malware prevention on the endpoint will automatically be hidden.



When this setting is set to 'Allow endpoint local admin to enable/disable', then the last endpoint setting of malware prevention is preserved and the user gets to option to enable or disable it at will.

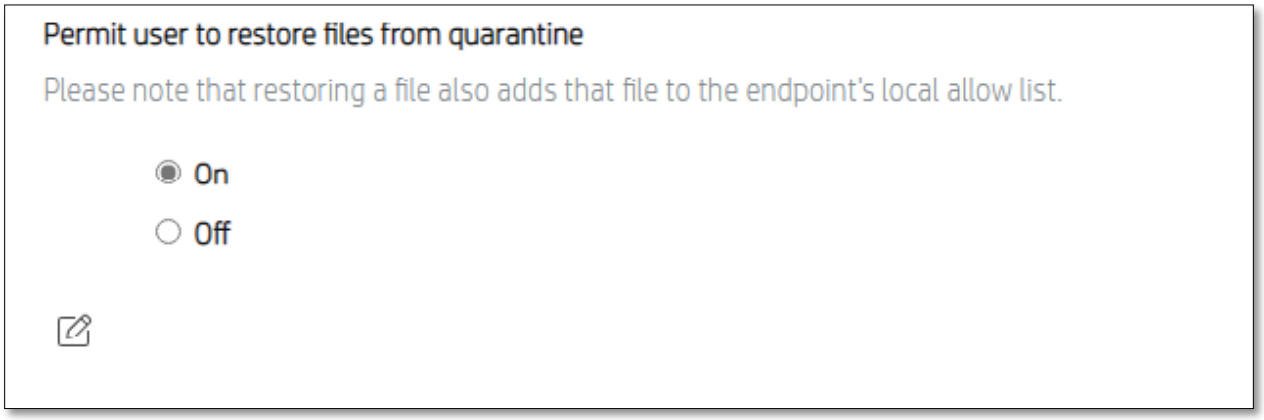


Local exclusion list control

This setting controls whether the user is allowed to edit the NGAV exclusion lists on their endpoint. Use this if you suspect that users might be adding process or folders that they should not in the exclusion lists (like c:\).

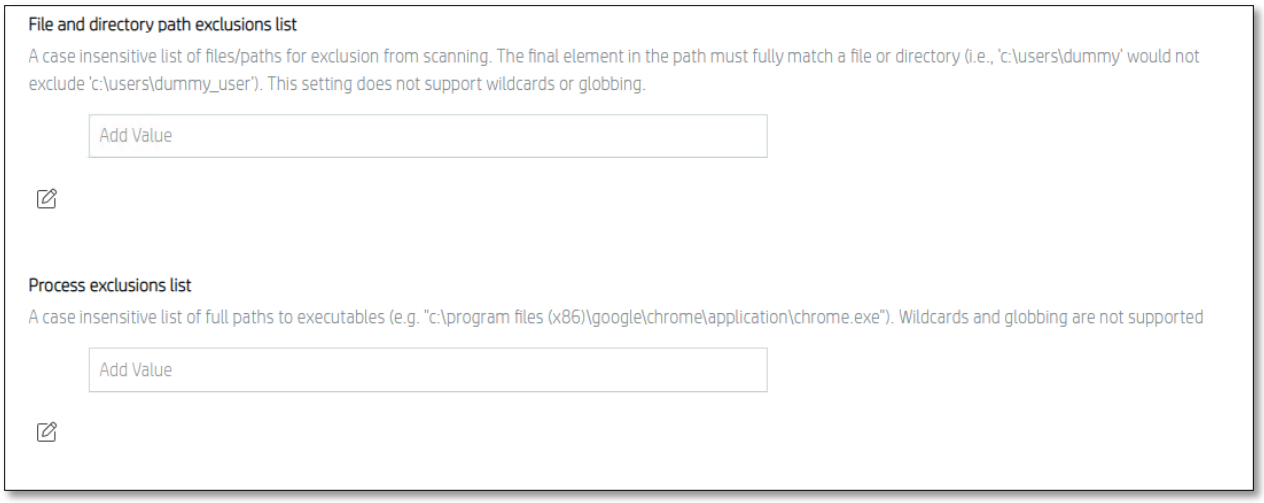
When this is set to OFF, the Exclusions tab in the Setting page on the local desktop console disappears and the user is not allowed to set any exclusions.

Local quarantine list control



With this set to Off, the user is not allowed to restore an already quarantined file on the endpoint. The file will remain in the quarantined list.

Exclusions list control



This allows the IT admin to add file, folder and process exclusions via policy, so that they are applied to all devices in the group to which this policy applies. The files, folders or processes specified here will be excluded from any NGAV scanning.

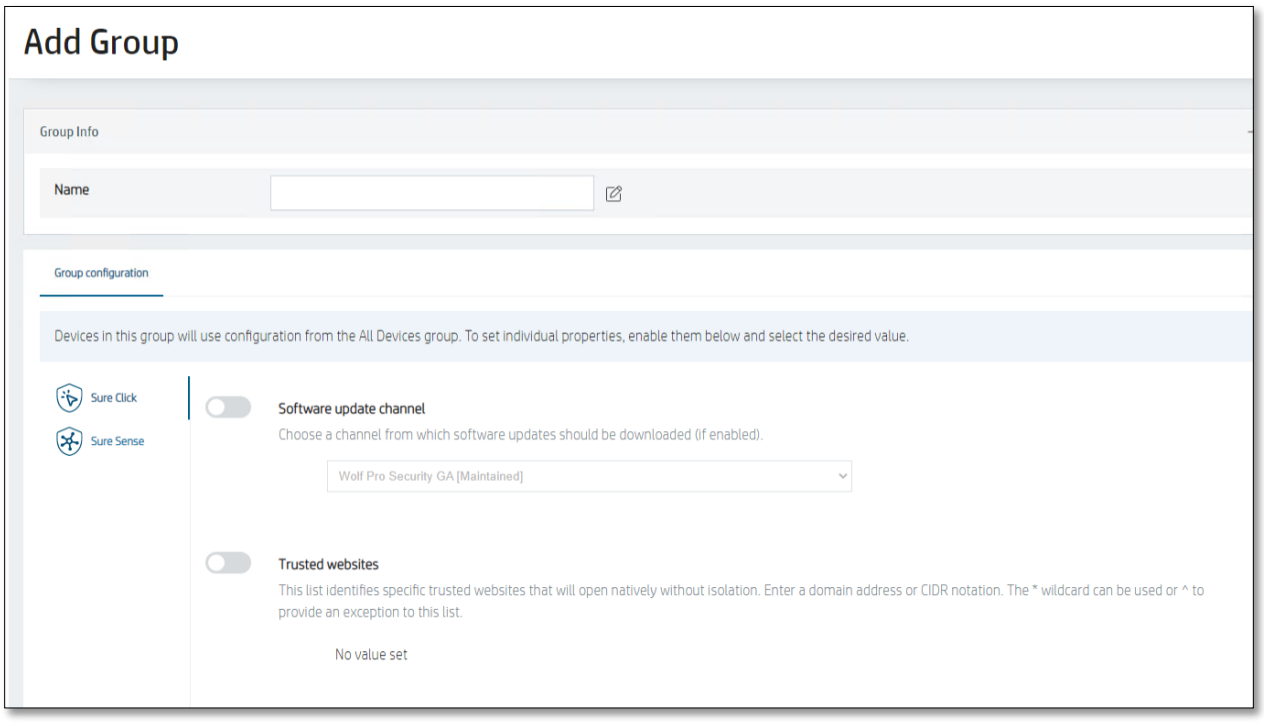
Subgroup Policy settings

The section above covered how to configure a policy for all devices. This should be your company-wide policy.

However, there would be situations where these policy settings might need to be different for certain specific devices, or a selected group of devices.

The Devices section/page will also help you to create your Device Groups which can have a specific policy applied. You can begin by selecting Add Group.

The Add Group page allows you to create a group with a new name and policy.

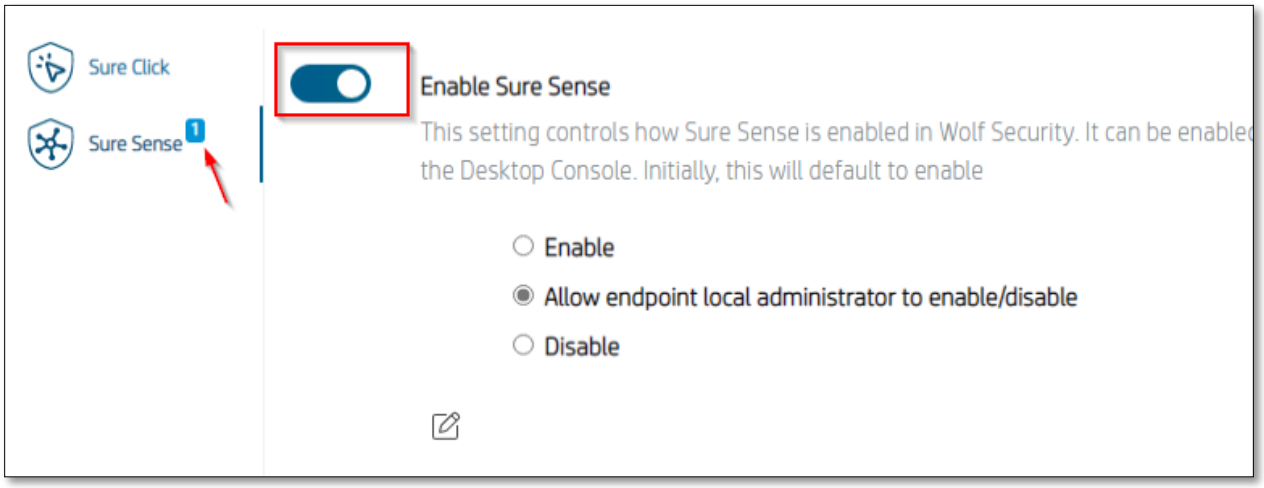


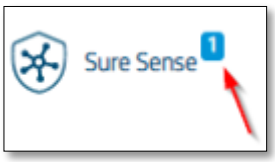
If you just want to add devices to a group without setting any policy values (e.g.: maybe you just want to track the health of a subset of devices), just name the group in the above page, save the group, and then start adding devices to the group.

Setting a policy for a new group is optional.

If no policy is set, devices in the group will automatically inherit policies from the (All Devices) group.

If you want to set a policy from for the group, indicate which policy setting you want to override from the (All Devices) group by toggling the switch as below and set the new value:

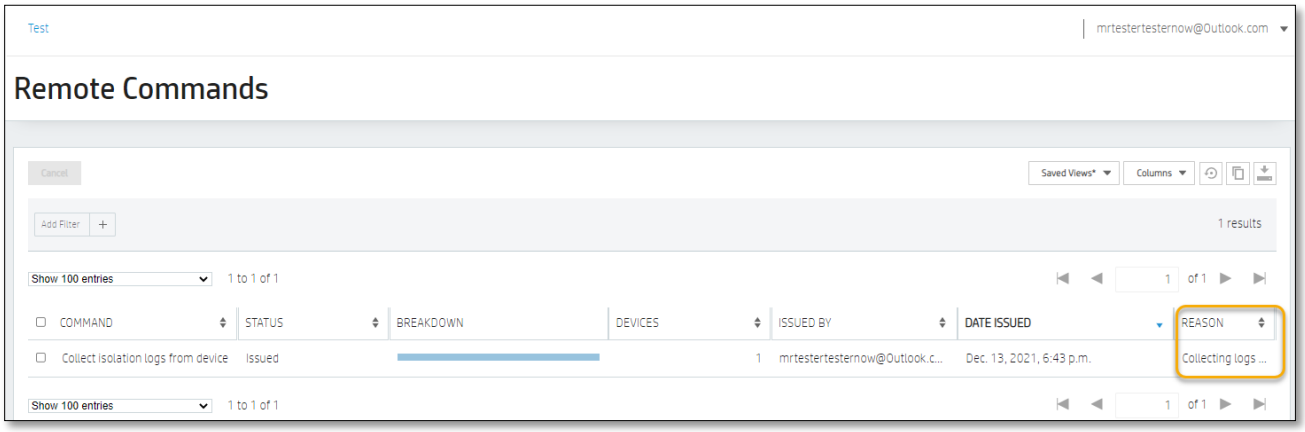


All other policy settings can be left untouched. The call out 

will indicate how many policies have been enabled in the new group

Remote Commands

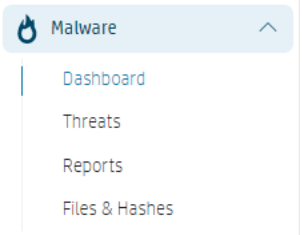
Remote Commands is where you will see all past and presently queued *commands* issued by this controller. HP will always put in a case number and date in this field for auditing purposes. You must select Columns and select Reason to add this into your view. You can also save this view, so you do not need to add it again. More details concerning Remote Commands is found in **Remote Commands Explained** below.

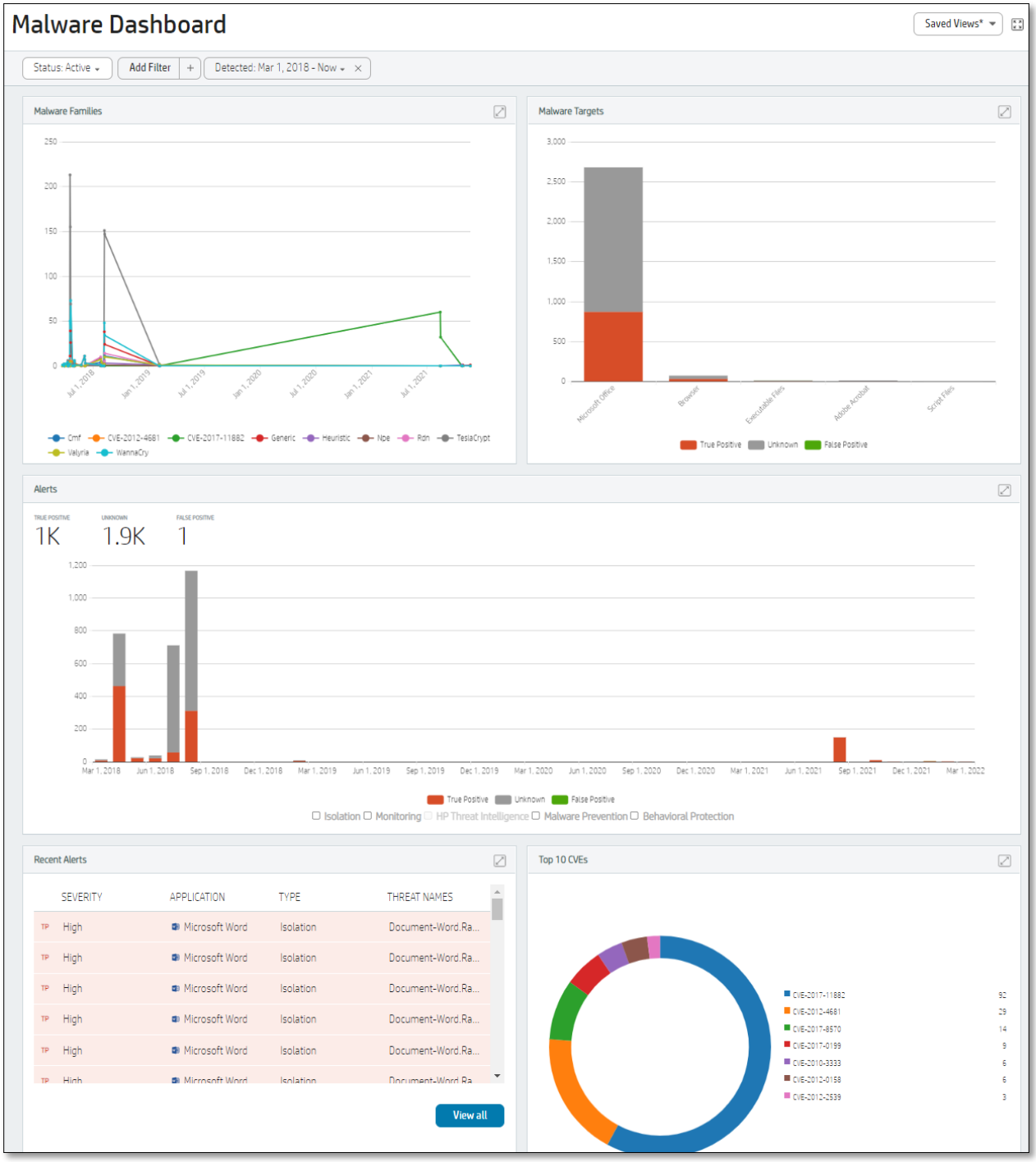


Malware

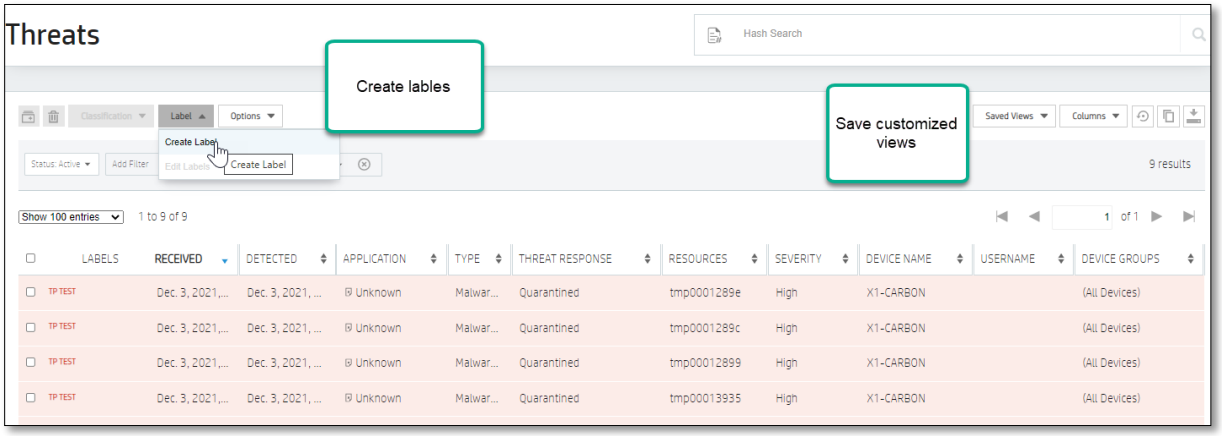
The malware section is helpful to the security analyst or IT administrator responsible for security within the company. All our technologies create threat-based events that you can open and analyze.

- **Dashboard** gives you a view of threats seen in the environment and computers at risk.

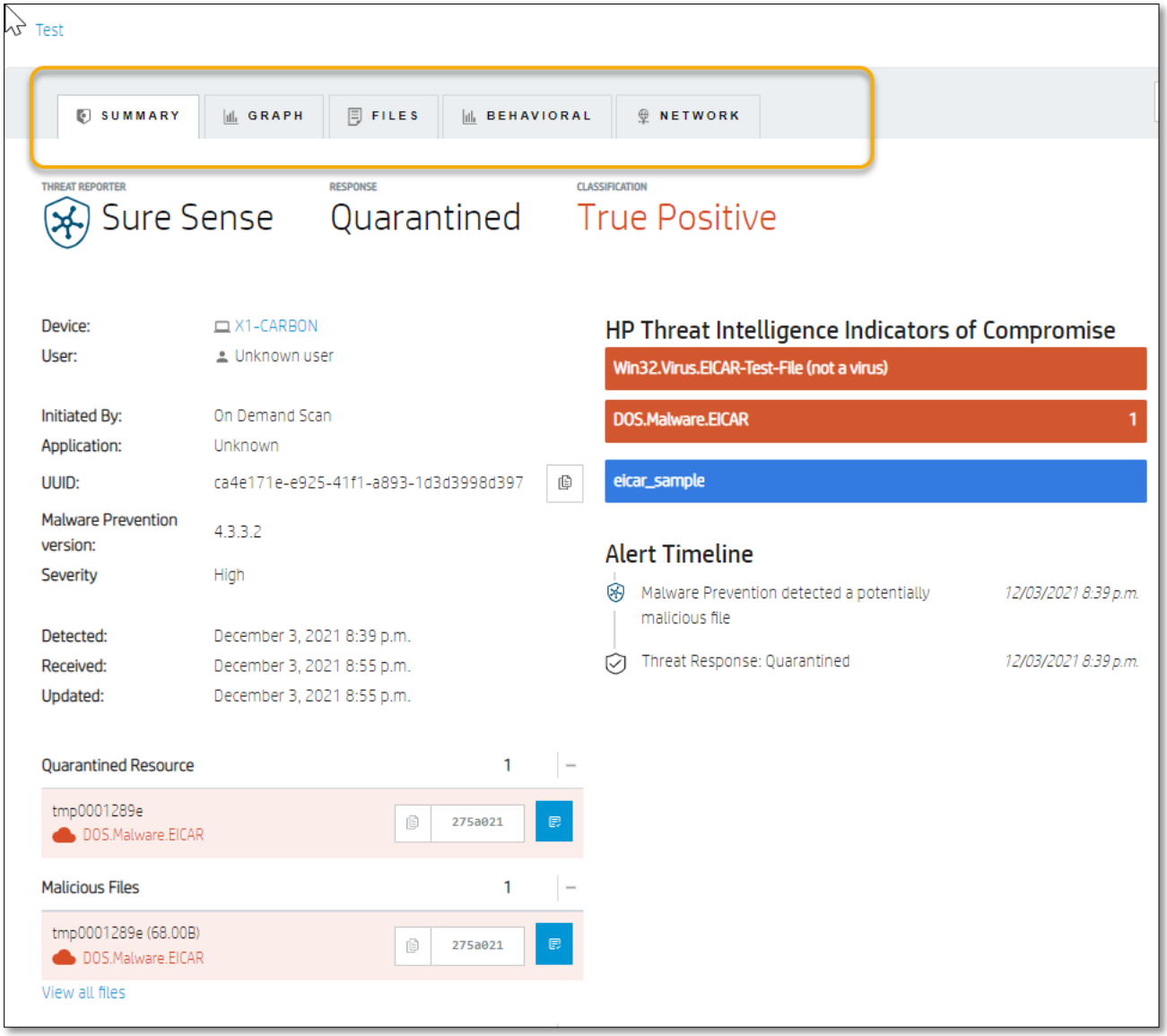




- **Threats** gives you a list view with the ability to sort and save views. This is where the analyst will spend most of their time reviewing events. You can make labels such as “Needs investigating” and apply that to a threat to help the internal team keep track of items that have been addressed.



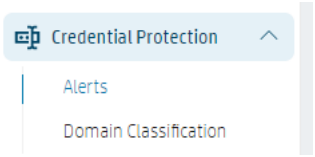
- **Threats** will also allow you to click and investigate. While in an event you can use the information to investigate deeper into the threat.



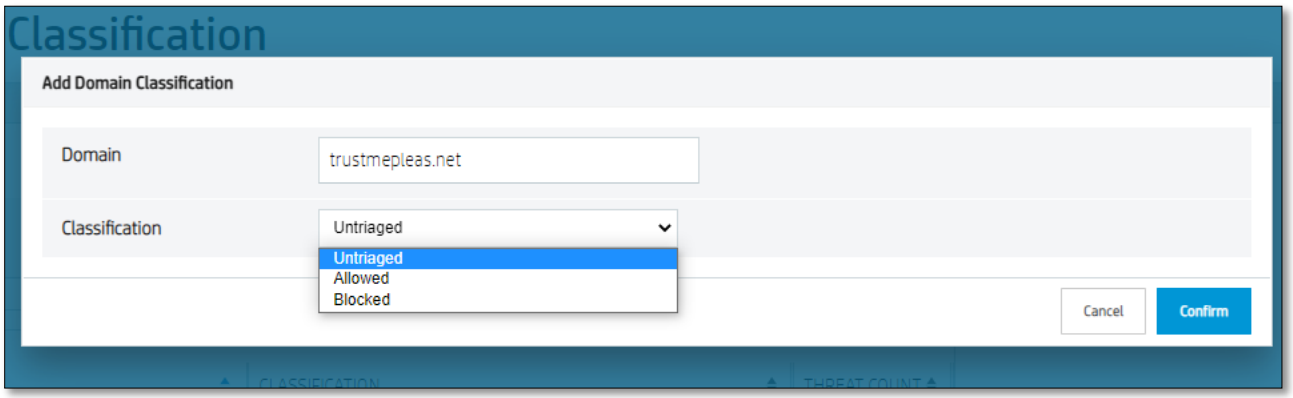
- **Reports** currently gives you the ability to create and view a security report that highlights threats that you have seen in the environment.
- **Files & Hashes** will give you a list of all whitelists that have been placed in your controller. Good for a list to audit.

Credential Protection

Credential protection will be useful to anyone who may work with third parties and is a target for phishing. This will provide you with the ability to see what has been flagged or blocked by Credential Protection within your company by phishing attempts

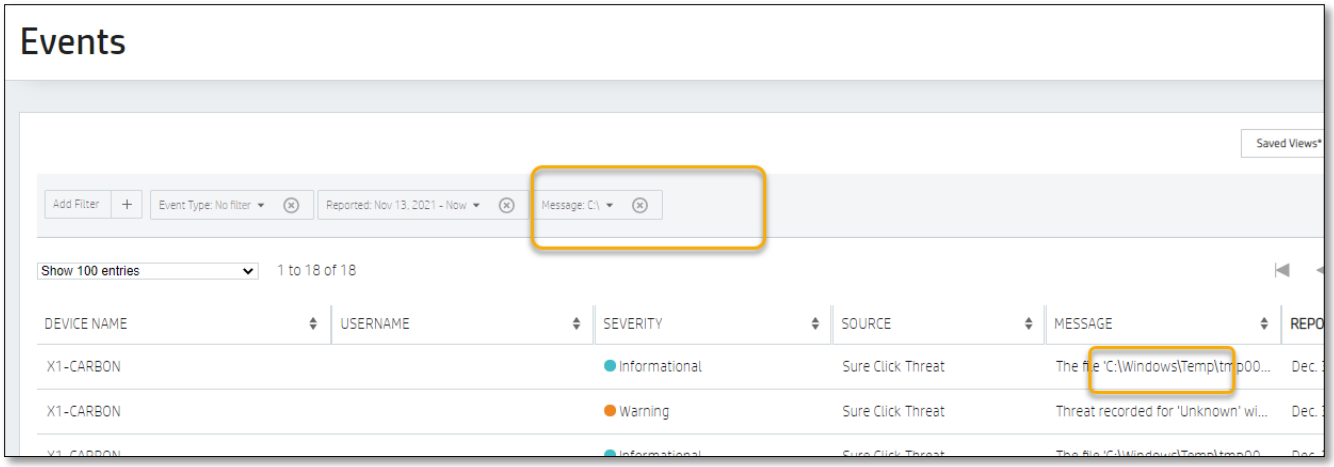


- **Alerts** will give you the ability to see a list view of all the detections or blocks within your company. You can also create saved views based on the information you want to see.
- **Domain Classification** will give you the ability to override sites which may be miscategorized or you want to allow, such as an internal portal login. You can change the classification here.



Events

This section is helpful for the device administrator or security specialist responsible for keeping track of metrics related to the health of the agent fleet, current deployment, or specific questions such as “When was the last time a computer initialized?” or “How many devices have trusted a file located at C:\Windows\temp?”



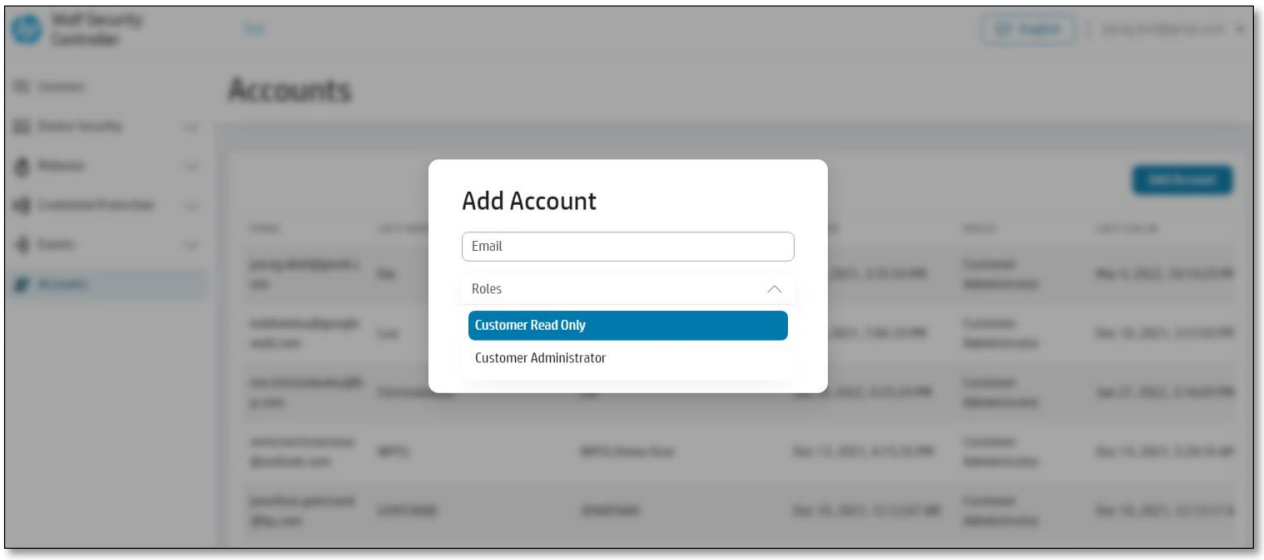
Accounts

When you initially setup your controller (HP or a Partner may have initiated this on your behalf) you had the option to add users. You can still add users at any time if your access has "Customer Administrator" power. Simply navigate to the **Accounts** page and select Add Account. Provide an email address for the new user and the level of access you would like to grant.

There are 2 levels of access you can assign.

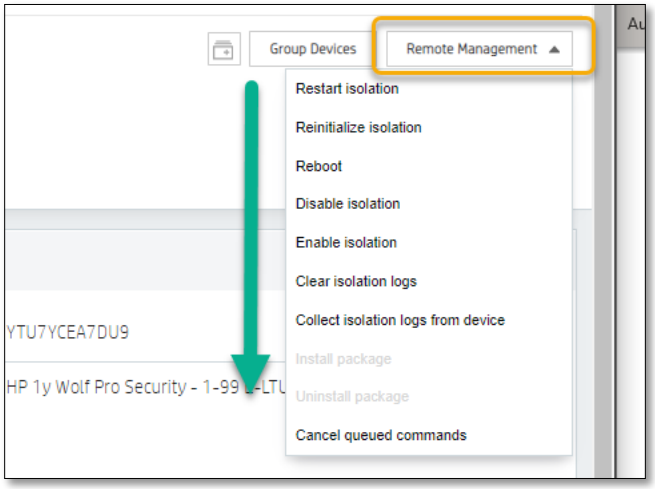
Customer Administrator – Administrator can make changes in the Controller.

Customer Read Only – Can only view the Controller settings and reports.



Remote Commands Explained

Remote commands are one way to manage your deployed computers from the controller. Here is an overview of which ones you will use to manage your computers. Remote Management options can be found in several of the already covered pages. Just select the dropdown to find your command.



- Restart isolation – Is specific to Threat Containment, this can clear up issues that the software on the computer may be having. It is rare to select this command.
- Reinitialize isolation – Is specific to Threat Containment, this should be run on any device having issues as a first troubleshooting step.
- Reboot – WARNING! This command forces a Windows Restart on the end-user's computer without warning and any unsaved work will be lost on that device. The user is unable to prevent or delay the immediate restart.
- Disable isolation – This is the same from the remote command as it is from the computer desktop console. It disables the Threat Containment feature for troubleshooting purposes typically.
- Enable isolation – The reverse of Disable. Can also be done on the computer desktop console.
- Clear isolation logs – This can be requested by support to be run prior to starting a troubleshooting session on specific issues.
- Collect isolation logs from device – This will upload the agent logs to the controller which can be retrieved later by support.
- Cancel queued commands – This can be useful if you issued a remote command to a large fleet and want to end the original command due to timing issues.

Troubleshooting Tips

Below is a collection of steps you can take as an IT Administrator to help your end users troubleshoot an issue.

First find out what feature is causing the issue

Determining what product is causing trouble is usually done quickly. Follow the flows below to determine the product and prepare for requesting support if needed.

If you are having issues with office documents or opening documents in VMs, a generally quick way to resolve this is to 'Reinitialize'. You could first check by disabling Threat containment.

Threat Containment Triage Flow

Disable Threat Containment.

Does this resolve the issue?

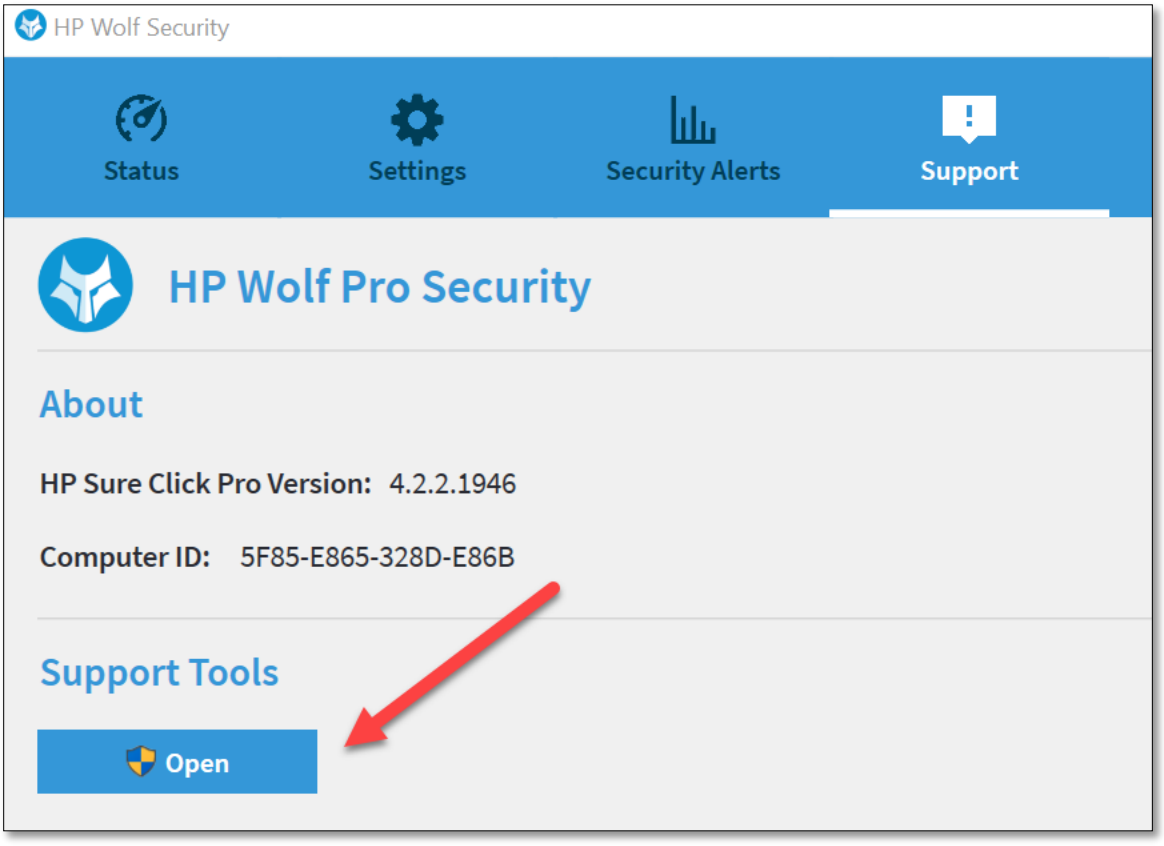
Yes, now let's see if we can fix it. Continue with steps below.

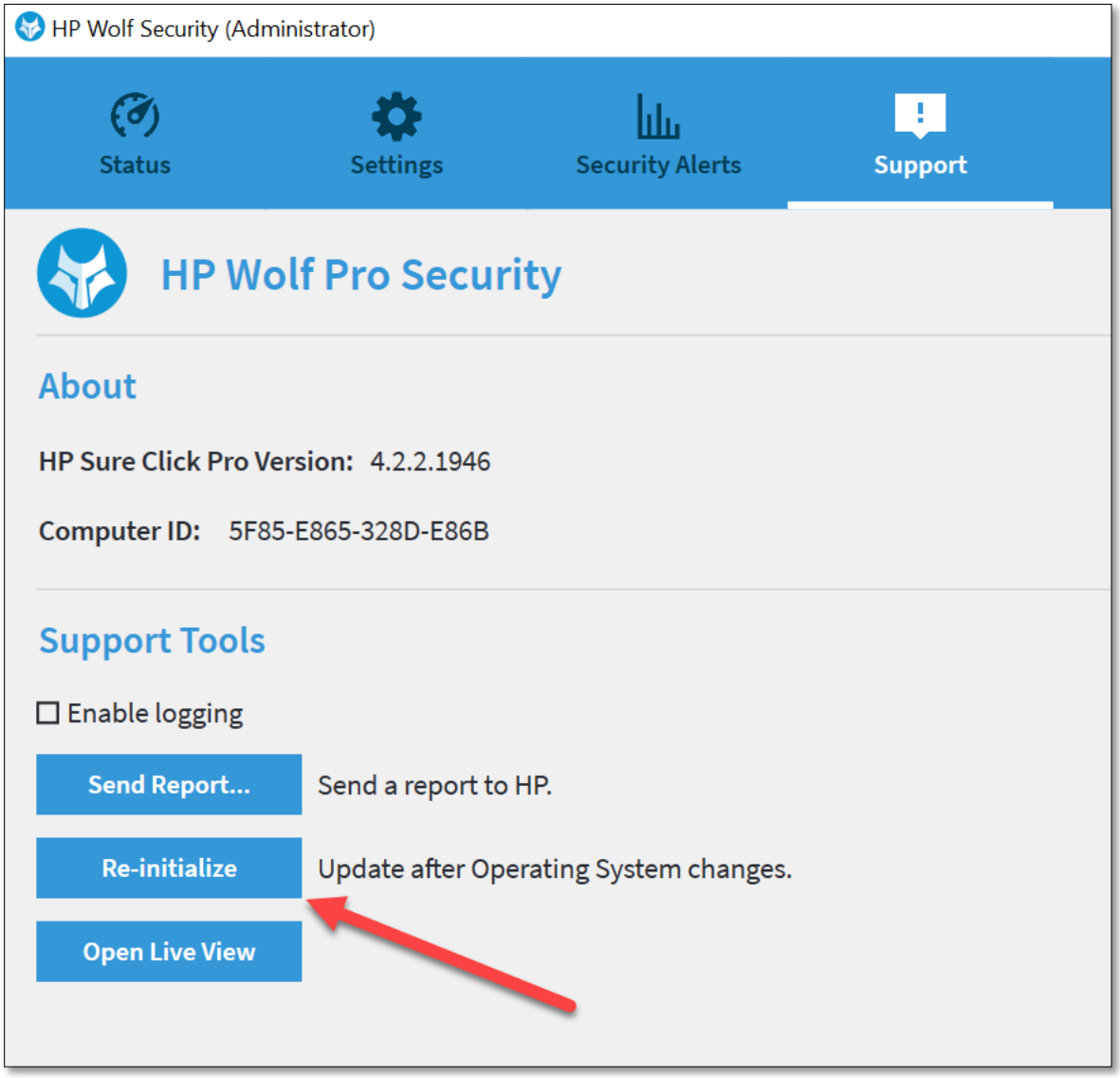
No, skip to Malware Prevention Triage Flow

Enable Threat Containment

Restart the computer

After restarting, open the Wolf Desktop Console and re-initialize





Malware Prevention Triage Flow

Disable Malware Prevention

Does this resolve the issue?

Yes, now let's see if we can fix it. Continue with steps below.

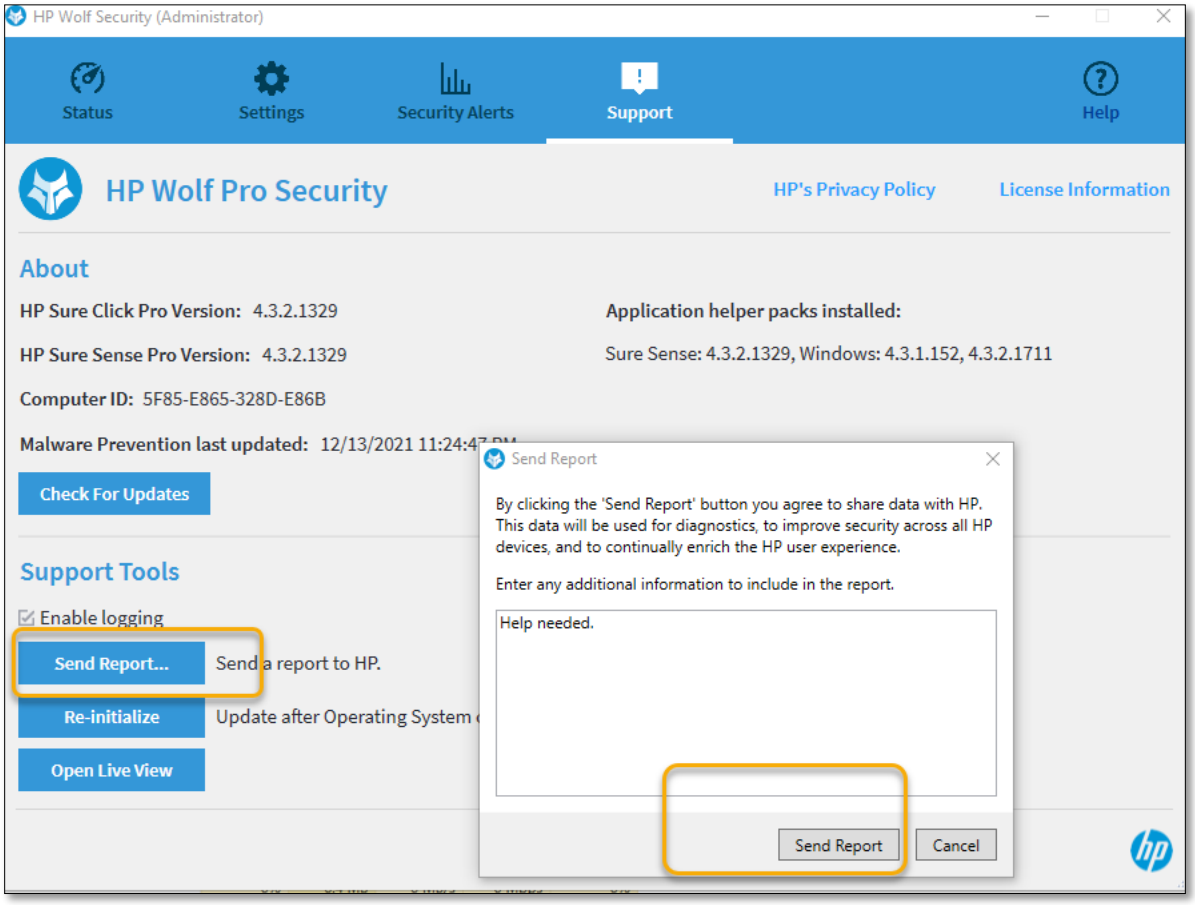
No, either you are not having issues with our product, or the issue needs a customer support case created to resolve.

Leave Malware Prevention disabled and check exclusions for any conflicting products such as 3rd party AV solutions. Restart the computer after you apply any needed exclusions.

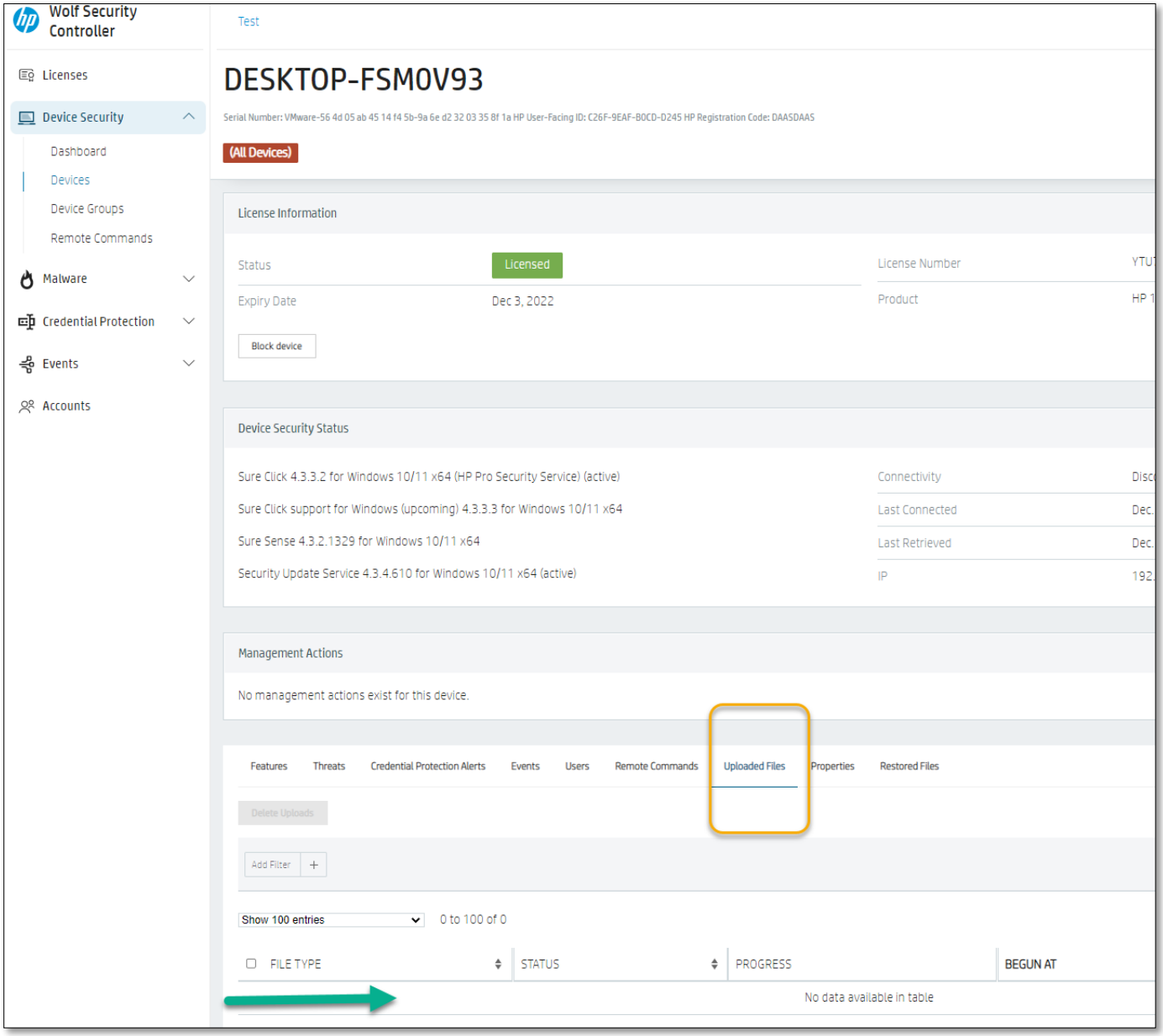
Collecting Log Bundles for Support

When opening a case with support it's a great idea to have a log bundle ready from the device in question. You can also send this in with your initial email request.

- To generate a log bundle, you can either request it via a remote command from the controller or have the end user send it in when it is convenient.

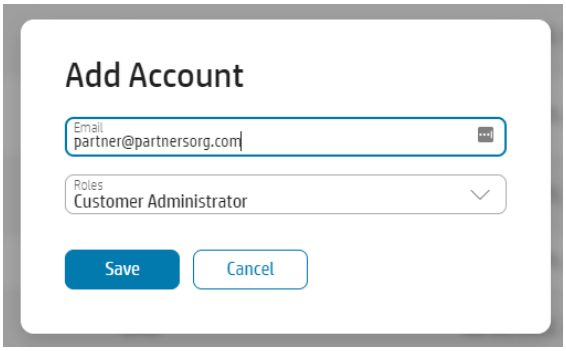
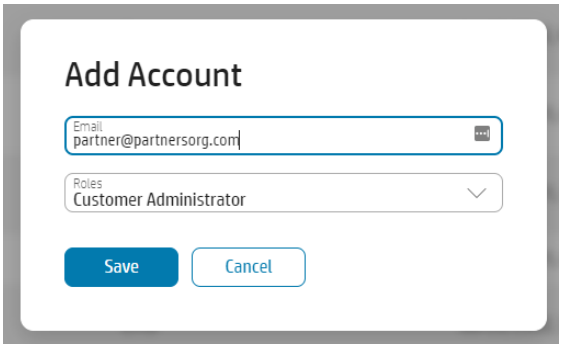


- You can view the uploaded log bundle in your controller under the Device information page.

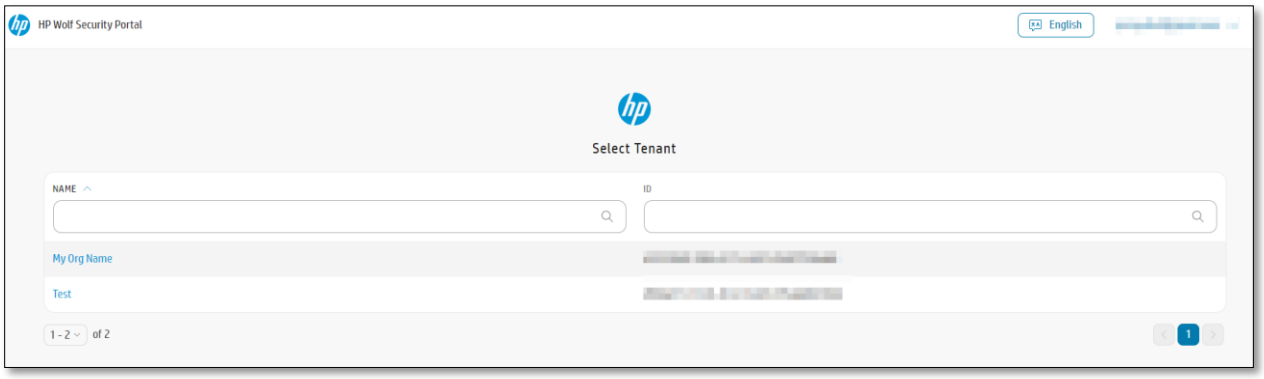


For Partners: Managing multiple customers

Partners will have the ability to manage multiple customers using a basic partner console. In order to enable this partner view, the partner will have to make sure that partner rep's email address (or the email address of whomever is assigned to help the customer) is added as an Admin user to the customer's tenant.

Customer A	Customer B
	

When the same HPID account is granted access to two separate tenants, then logging in with that HPID will result in this view when that HPID logs in:



This allows the partner to **single-sign-on** to the customer account using this page and allow basic features like searching for the customer by name and/or ID if the partner is managing a large number of customers.

Communication and Support Requests

There are two ways in which you can easily submit a support request.

- If you are in the POC phase of your service deployment you will email your assigned HP Security Service Expert with your question or issue.
- If you are a paid customer and no longer in the POC phase of your service, see the customer portal for contact options: https://support.hpwolf.com/s/contact

Communications

HP will contact you under the following circumstances:

- HP will respond to an email you submit requesting support.
- HP will send communications when upgrades are scheduled.

Information Gathering/Submitting a Support Ticket

If you would like assistance with or have questions about an issue, contact HP Support at https://support.hpwolf.com/s/contact with the below information. We will also need the customer information and reason for your submission.

Submitting Customer Information

Before submitting any service request for root cause analysis, it is important to collect information pertaining to the individual and organization.

Please ensure that you submit the following **mandatory** information:

- Customer's name
- Customer's email address
- Customer's contact number
- Customer's geographic location and time zone
- Customer's HP internal primary contact and/or partner information

Gathering General Information

Some information is necessary to explain the issue being reported or the possible resolution.

Please ensure that you submit the following **mandatory** information:

- Device name
- Summary of the issue
- Summary of a suggested resolution suggestion. Do you know how we can help you?
- How many people are affected?

- Is the issue consistently reproducible?

Gathering additional details

Please ensure that you try answering the following questions – **optional but helpful**:

- Was a file isolated?
  - Do you feel this site should be trusted automatically? Why?
  - Do you have any error messages that will help in resolving the issue?
  - Any screenshots of the HP Wolf Pro Security Desktop Console
    - Status page
    - Support page
- Is there poor performance?
  - Screenshot of the desktop at time of trouble
  - Screenshot of the task manager process tab
  - Screenshot of the HP Wolf Pro Security Desktop Console
    - Status page
    - Support page
- Can you suggest a possible resolution?
- Do you know how we can help you?
  - Do you need to have a file unblocked?
  - Do you need to have a site trusted?
  - Do you need to disable the agent for troubleshooting performance issues?
- Can you provide the device serial number?
- Can you provide the logged-on username?
- What testing/troubleshooting has the customer performed so far?
- What is the priority of this issue? Critical, High, Medium, Low –
  Note: This in no way dictates the service level objective (SLO) for resolution, this is just a quick indicator when we are looking over the ticket how we will respond.

HP Wolf Pro Security also manages a minimum of 2 agent upgrades per calendar year.

- Agent Upgrades – A minimum of 2 agent upgrades will occur each year. This is typically times around the Microsoft OS release calendar. These upgrades are done remotely from the controller, and you don't need anything for this to take place. We will send a communication letting you know the schedule for QA and Production releases. If there are issues, please submit a support email with the details. Furthermore, if we see issues, we may open a case and contact you to help us resolve them or just provide feedback on what we are seeing. Any issues may delay the upgrade.

For Users

This section is meant for the end-users of HP Wolf Pro Security. However, it is recommended that IT admins also go through this section to better triage issues and address end-user concerns.

Understanding HP Threat Containment

HP Threat Containment protects you by isolating potentially malicious content in files downloaded from an untrusted source outside your organization.

Your IT Department has already defined sites as *Trusted* from which you can download files. Typically, all your organization's internal file-sharing sites, as well as enterprise Web apps, will be trusted for downloads. Files downloaded from these trusted sites will continue to open like they do today. The process of trusting internal sites, Web apps, and email addresses is known as whitelisting.

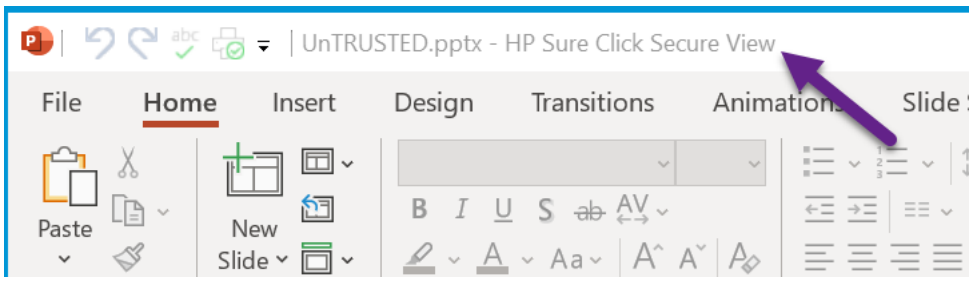
Your IT Department has also defined internal email addresses as trusted sources for attachments. Files that are created internally or downloaded from trusted sites can be attached to emails to colleagues in your organization. These files will be trusted and will open normally.

Downloaded files and email attachments from anywhere else will be untrusted. Any untrusted files that are received by email and that open in Microsoft Word, Excel, PowerPoint, or Adobe Acrobat Reader, can still be opened, viewed, edited, printed, and saved. HP Threat Containment automatically isolates any malicious activity from untrusted files.

So, HP Threat Containment also protects your computer from files you may download:

- Files downloaded from the Internet or saved from email are marked as untrusted.
- Untrusted files are isolated and opened inside Threat Containment.
- Isolated files are still fully functional and can be saved, copied, edited, and shared.

If you save an untrusted file, the file will have an untrusted status. If you send untrusted files to people in your organization who use Wolf Pro Security, these files will be marked as untrusted. If you want to check if HP Threat Containment is protecting a file you open, look for the words HP Sure Click Secure View in the title bar at the top of the application window (as pictured below). This indicates you are working with the file in the safest way.



If you believe a website or email address should be trusted, then contact your IT department for a security review of the site or email address. Your IT department will get the site or email added if they approve the business case.

Removing HP Threat Containment protection

Devices are often exploited when malicious files are downloaded from the Internet. HP Threat Containment overcomes exploits by opening untrusted sites and files inside a virtual environment.

The following are some reasons why you may want to whitelist trusted sites:

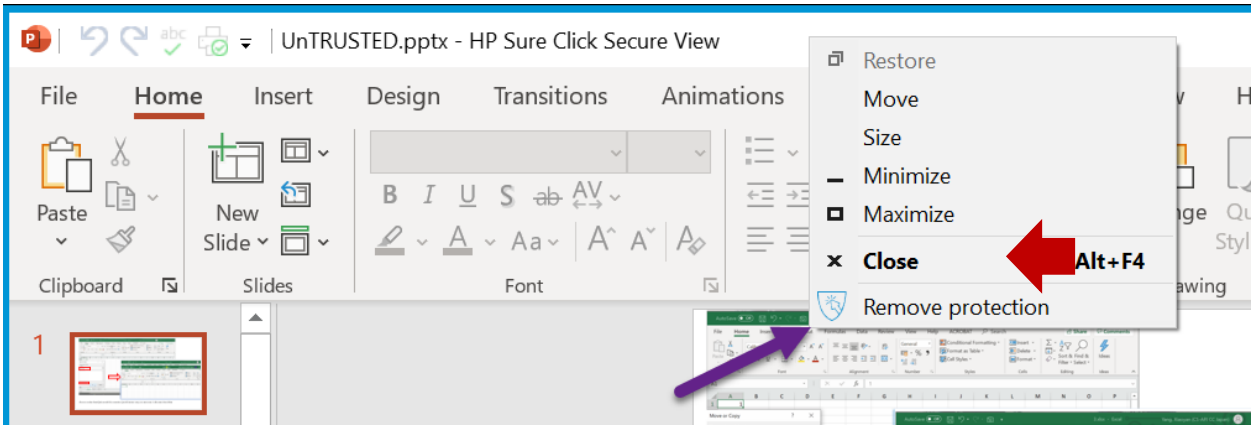
- Simplify user workflows
- Support authentication of Web-based applications
- Avoid repetitive MVM isolation of safe sites

Also, some features are not fully enabled in MS Office or Adobe Acrobat Reader when a file is being protected by HP Threat Containment. For example, Excel Add-ins or PowerPoint Presenter View will be disabled. If you have a valid business justification and the file is not malicious, then you can remove Threat Containment protection from the file. In most cases, you should contact your IT department to remove protection by whitelisting websites and email addresses; however, Threat Containment protection can be removed from individual files if needed so the files become trusted.

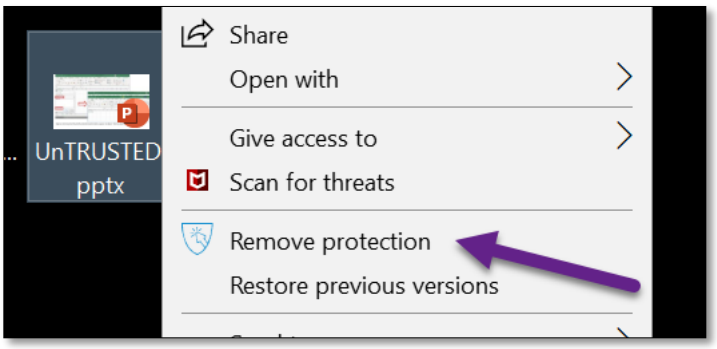
Note: Removing containment protection from a file will result in a notification being sent to the controller

Following are two ways you can remove protection:

- If a file is open inside Threat Containment, right click on the **HP Sure Click Pro Secure View** at the top of the application. Then, click **Remove Protection**.



- Right-click the file in Windows Explorer, then select **Remove Protection.** A new window appears. Select **Remove Protection** again.



Please note, the file will be analyzed by HP Threat Containment before protection is removed. The file will open from that point forward in MS Office or Adobe Acrobat Reader without protection. If you save a trusted file and open it again, the file will remain trusted. If the file is sent by-email outside of your organization to an untrusted party, the file will automatically be reset with an untrusted status.

If HP Threat Containment detects suspicious content in an MS Office, Adobe .PDF, or executable .EXE file, the file will not be trusted. You should safely close the file. If you need additional help, please contact your IT department for additional instructions.

Understanding Malware Prevention

The Malware Prevention feature of the HP Wolf Pro Security software is like a traditional Anti-Virus software you have used in the past. It is always running and if it sees something it will quarantine it and block it. Based on your company's policy you may be able to release items from quarantine without help from additional support. If you would like to see items that have been quarantined, you can open the Desktop Console from the system tray and view the Security Alerts page. If allowed by policy, you can also disable the Malware Prevention if needed for troubleshooting. This will stay disabled until it is enabled again.

Credential Protection

Credential Protection, also referred to below as Identity Protection, will help prevent users from entering passwords on known bad websites and warn users on potentially bad websites.

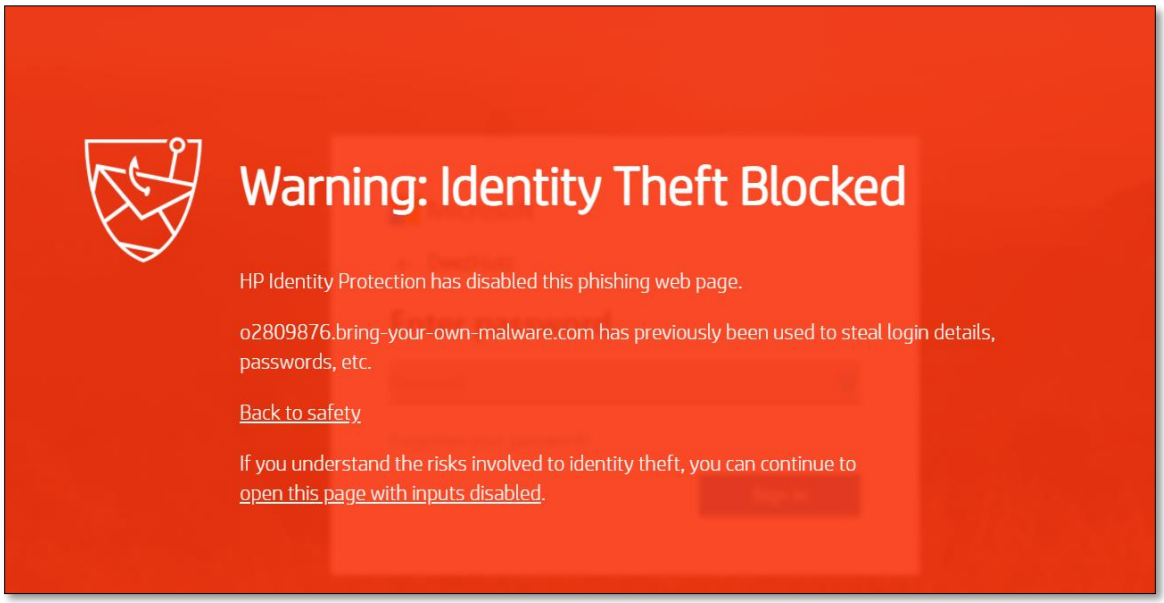
Supported browsers

The Identity Protection extension is currently supported on the latest releases of the Google Chrome, Mozilla Firefox and Microsoft Edge (Chromium-based) web browsers. It is also available on the HP Sure Click Pro Secure Browser.

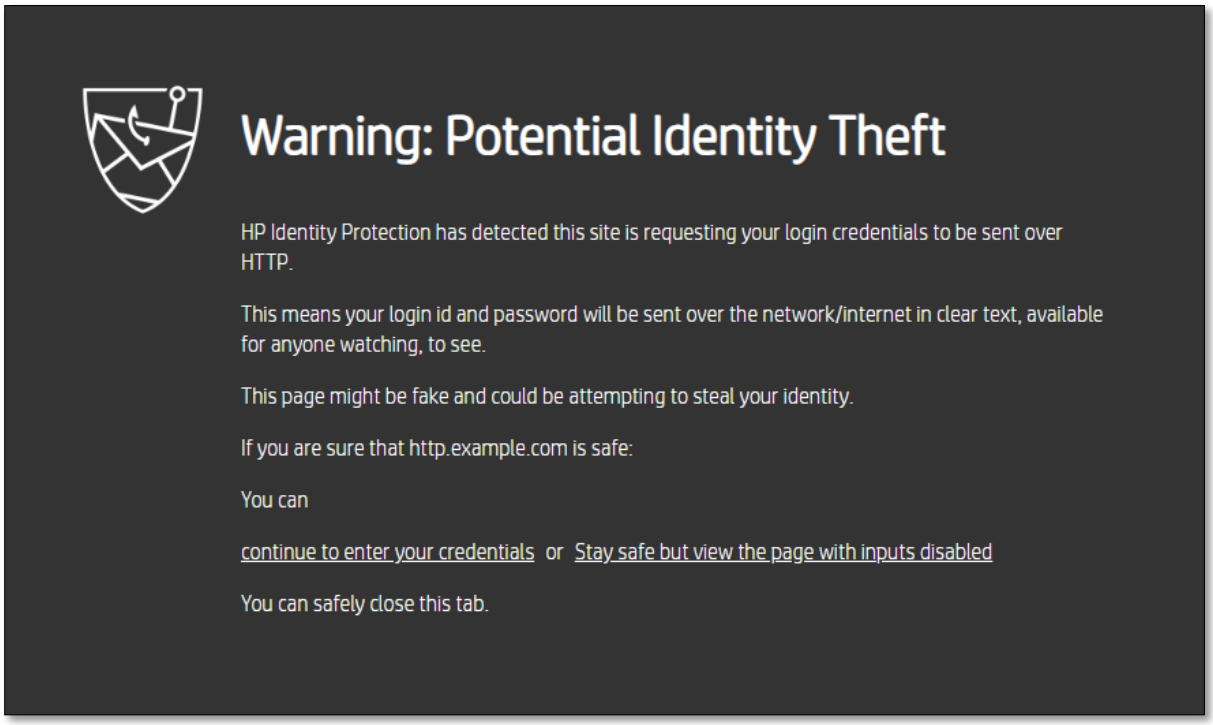
Protection behavior

On devices where the feature is enabled, when a user attempts to enter a password into a suspicious or known malicious website from a protected browser, then a warning message will be triggered on the page.

If the website risk is assessed as High, then the user will see a red warning screen as shown. The user will be warned and will not be able to bypass the warning, their access to the site will be restricted so that the login controls are disabled on the login form.



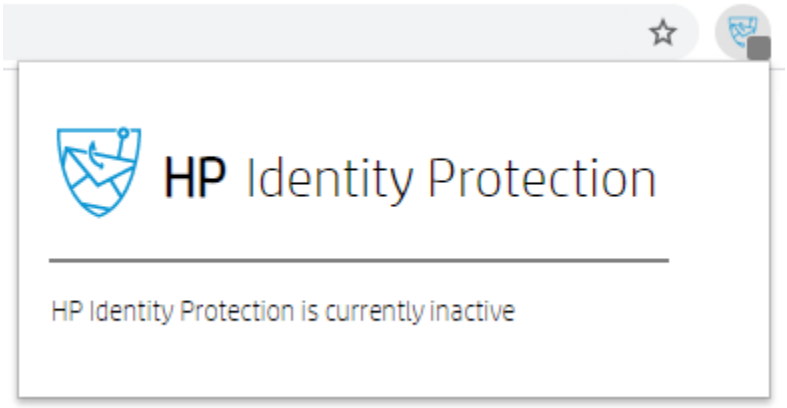
If a site is assessed as medium risk (suspicious), then the user will see a gray warning screen as shown below:



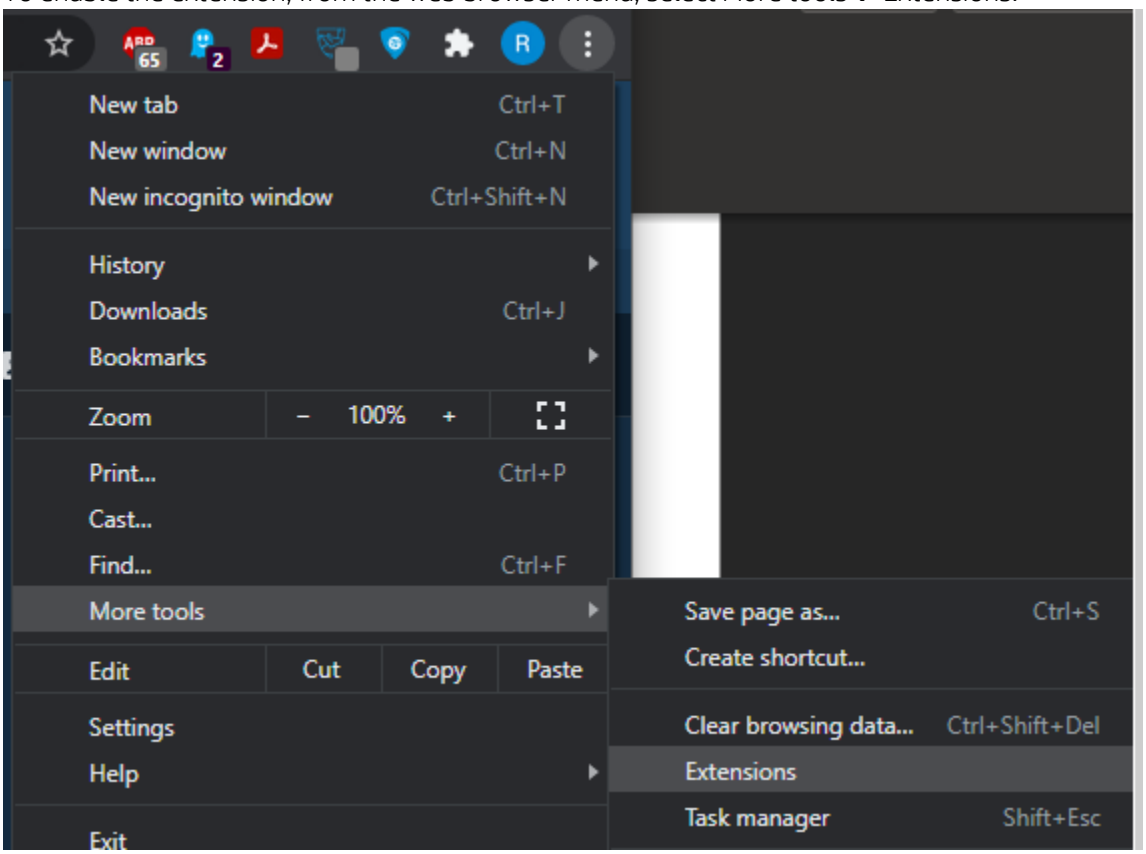
Since these sites are not confirmed as malicious in intent, then the user will have the option to either continue to enter their credentials, or continue to the website, but disable the login fields on the site so the user cannot mistakenly enter their password. In addition, if the user selects the option to continue to enter their credentials on the web page, then the site will be added to the end user's list of trusted login sites, and no additional warnings for the page will be shown.

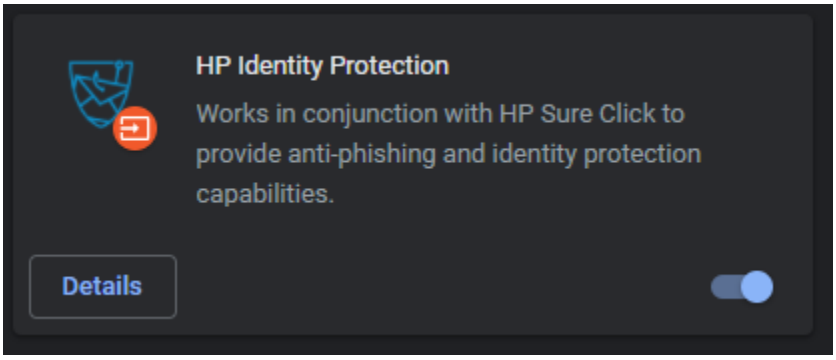
How to enable the Identity Protection extension

To verify whether Identity Protection is enabled, from the web browser extension toolbar icon, click on the HP Identity Protection extension icon. If the extension is not enabled on the user's browser profile, then the following popup will be displayed.



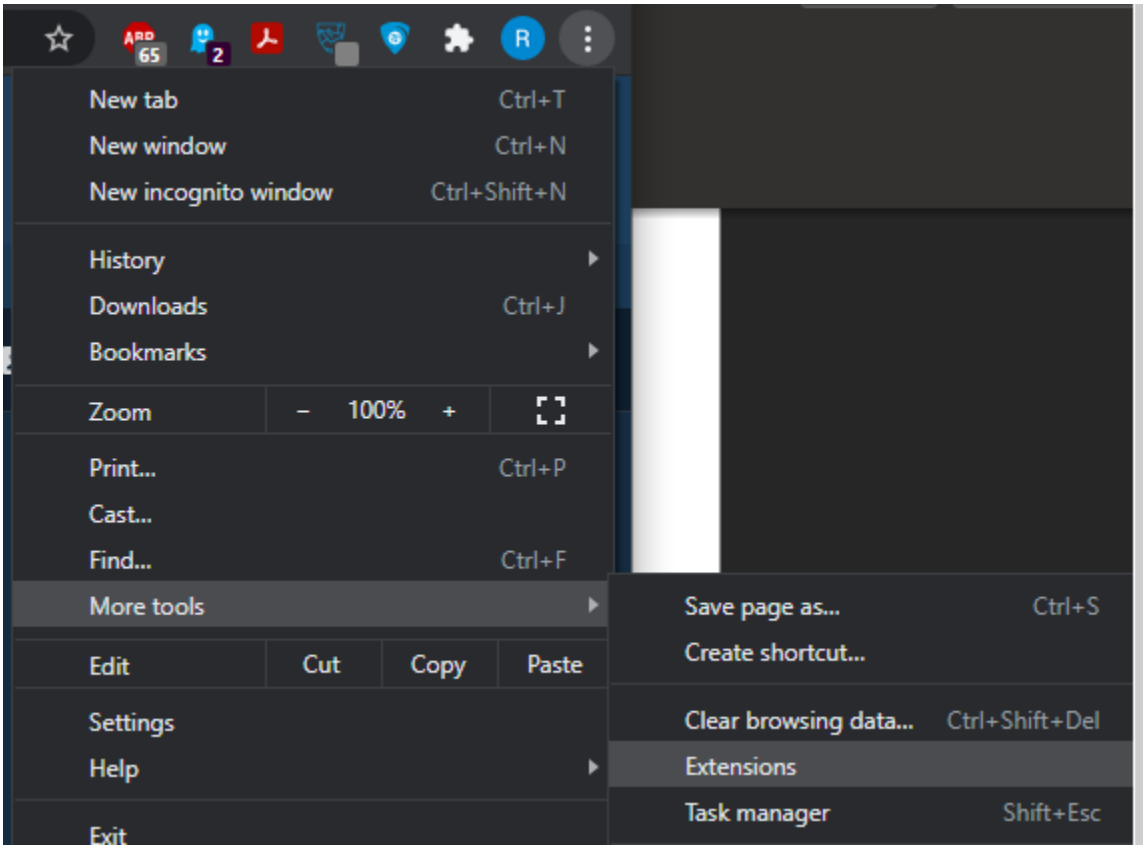
To enable the extension, from the web browser menu, select More tools→ Extensions.



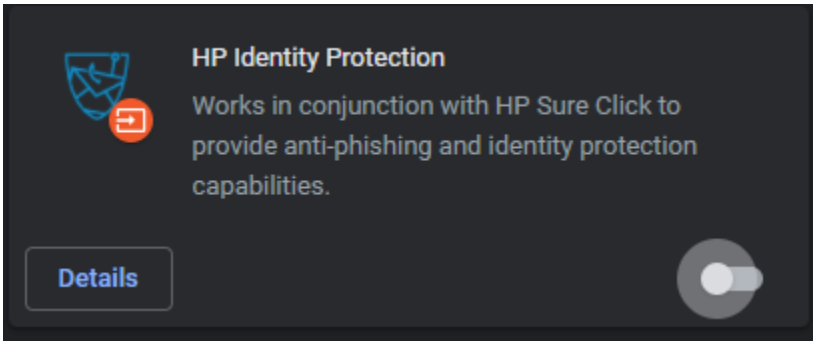


How to disable the Identity Protection extension

To disable the Identity Protection extension, navigate to the Extensions menu item for your browser and toggle the extension "Off" to disable the feature. In Google Chrome and Microsoft Edge (Chromium) browsers, this is in the browser menu under More Settings→ Extensions.

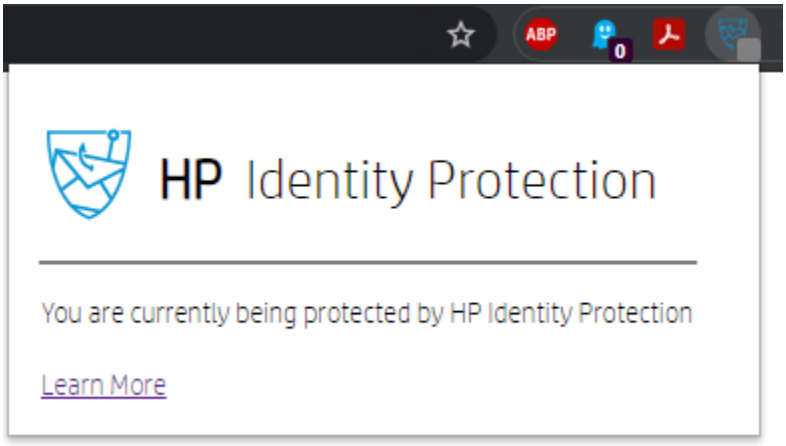


When the extensions list loads, find the HP Identity Protection extension tile and then toggle the feature Off.



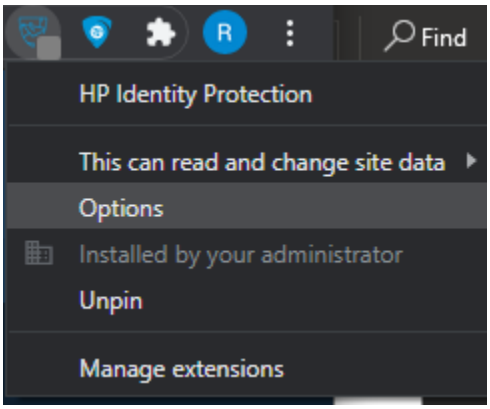
How to confirm whether the HP Identity Protection browser extension is enabled

After it is enabled, one can verify the extension is active by clicking on the HP Identity Protection extension icon in the browser menu bar.

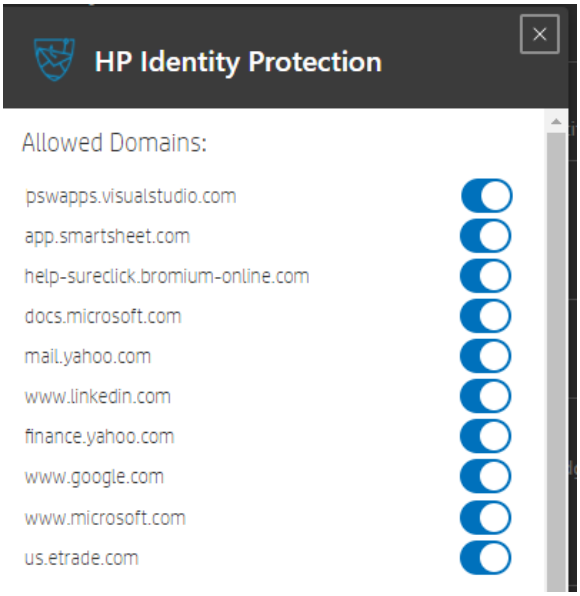


How to manage user-defined login page exclusions

To manage the list of allowed or blocked login pages, right-click on the HP Identity Protection browser extension icon in the browser menu bar, and then select Options.



From this menu, the user can choose whether to change the trust settings of the allowed websites. Note this may be restricted by your organization.

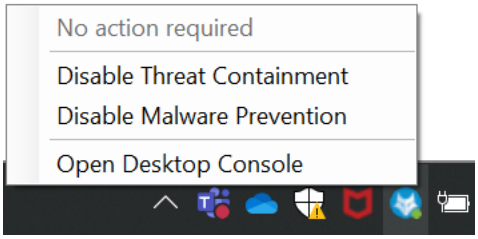


Local management (Desktop Console)

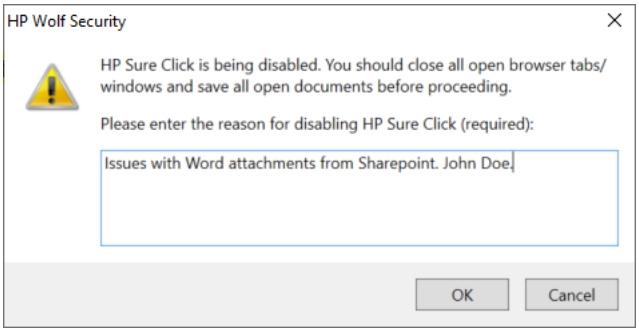
This section describes how the end user interacts with the HP Wolf Pro Security agents and service.

Locate the Desktop Console

The desktop console (user interface) is displayed after clicking the HP Wolf Pro Security icon next to the clock in the Taskbar, as pictured below.

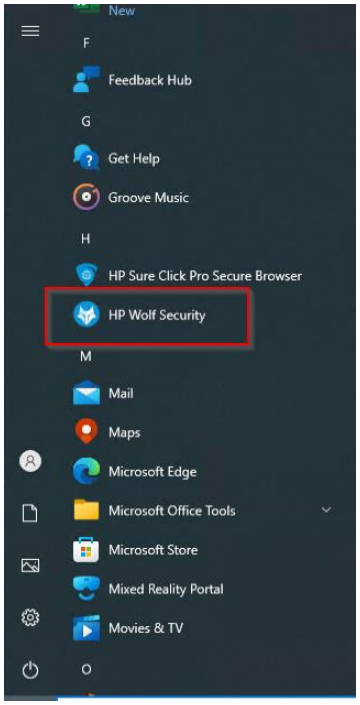


- Overall Status lets you know if any action is needed.
- Disable Threat Containment or Enable Threat Containment can be done by clicking on that option. This will disable the Threat Containment technology.
- Disable Malware Prevention or Enable Malware Prevention can be done by clicking on that option. This will disable the Sure Sense technology.
    - Any time you disable a feature you should put in a reason why and your name. This could help resolve any issue that may be affecting other users faster.



- Open Desktop Console will open the user interface.

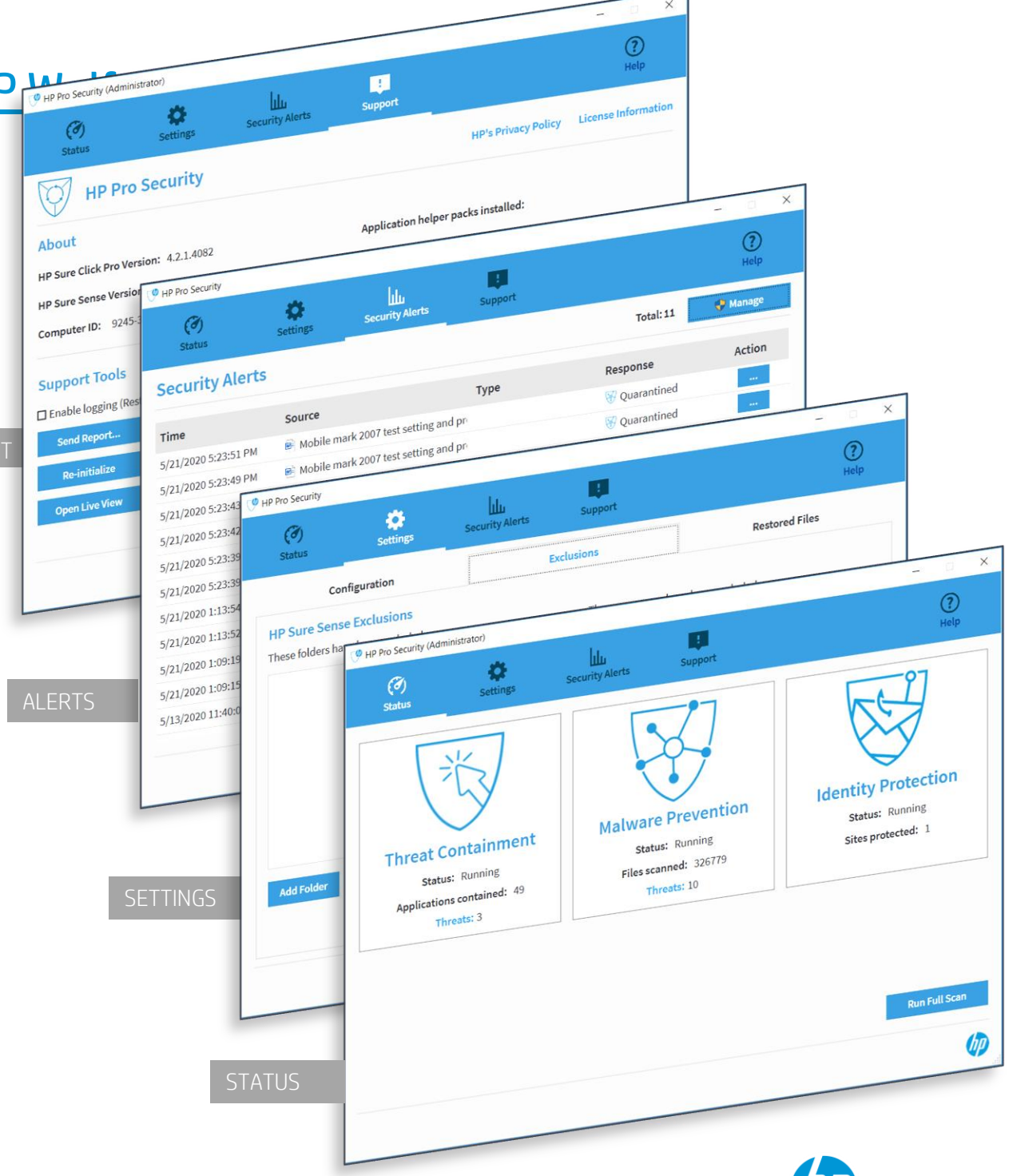
The desktop console can also be opened by clicking on the start menu and looking for HP Wolf Security



Getting Started Guide – HP W...

Desktop Console Details

- Status
  - Active Health status, error messages, number of threats encountered and mitigated, number of files scanned.
- Settings
  - Status – Endpoint Connection to controller
  - Set local file and folder exclusions, take actions on files restored from quarantine
- Alerts
  - Event list of detected malicious files, websites, and credential phishing attacks encountered
  - Correct and act on a quarantined file, using isolation technology to safely open quarantined files
- Support
  - About Info – Version number, PC #
  - Advanced Tools
    - Logging, Reinitialize VMs, Live View



Getting Started Guide – HP Wolf Pro Security

After launching the **HP Pro Security** dashboard via the Windows Start Menu, the Dashboard will open to the ***Status*** page. Below are descriptions for each of the 3 Protection mechanisms HP Pro Security includes. Clicking across the icons on the top (Status, Settings, Security Alerts and Support) will present settings and information for each of the attributes of the Software.

Status – Indicates protection is active, protecting the user against malicious websites and suspicious email attachments. If the icon appears Yellow or Red, it

Applications Contained – Documents/Websites opened in a Secure View.

Threats – Files/Websites blocked and quarantined (see Security Alerts page for details on names and types of threats).

Malware Prevention – Deep-learning AI – anti malware protection.

Status - Indicates the AI protection agent is active, protecting and isolating the PC from malicious files which land on the PC.

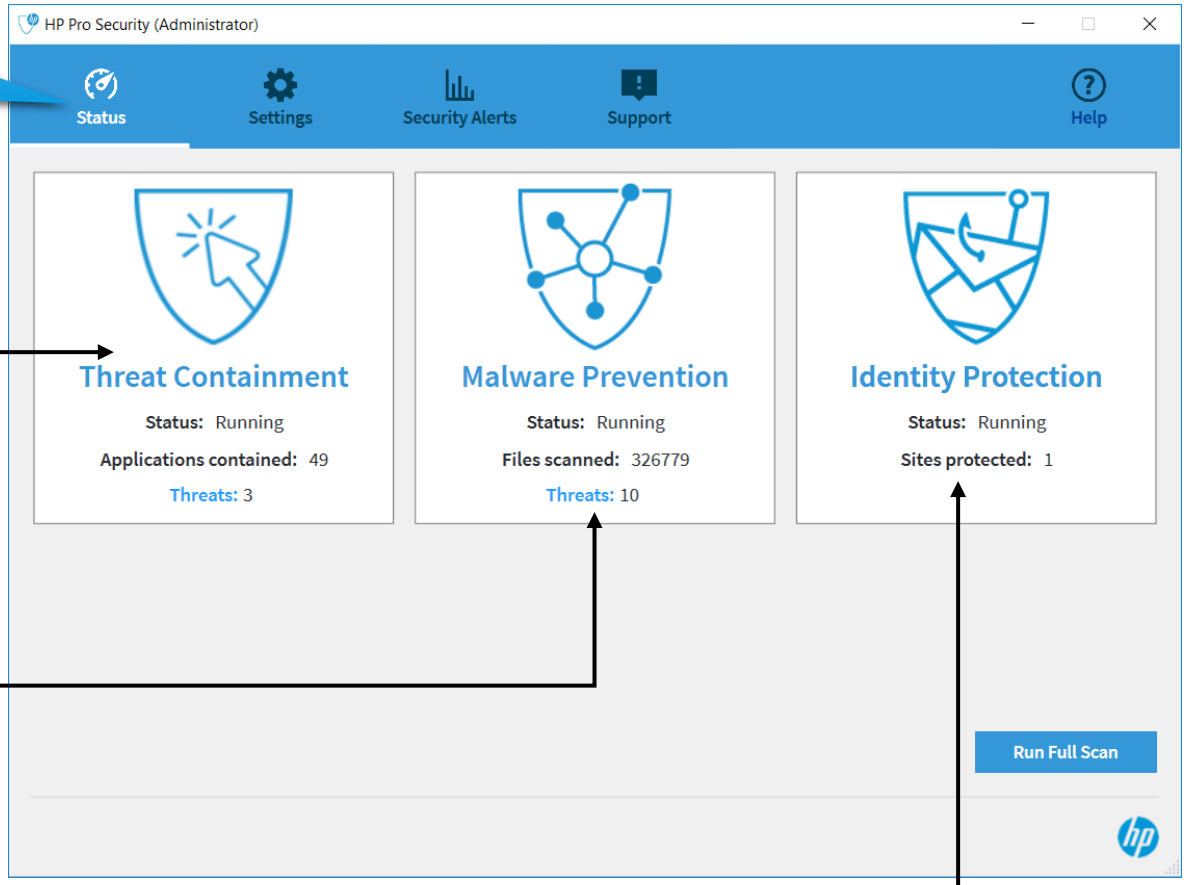
Files Scanned – Documents/Websites scanned by the agent. Note- when the agent is active it is scanning all file types that land on the PC.

Threats – Files/Items blocked (see Security Alerts page for details on names and types of threats).

Identity Protection – The anti-phishing engine with the ability to warn or stop users from entering passwords on suspicious websites

Status - Indicates HP's anti-phishing protection is active or inactive.

Sites protected– Indicates the number of websites that attempted to steal credentials (user login, password)

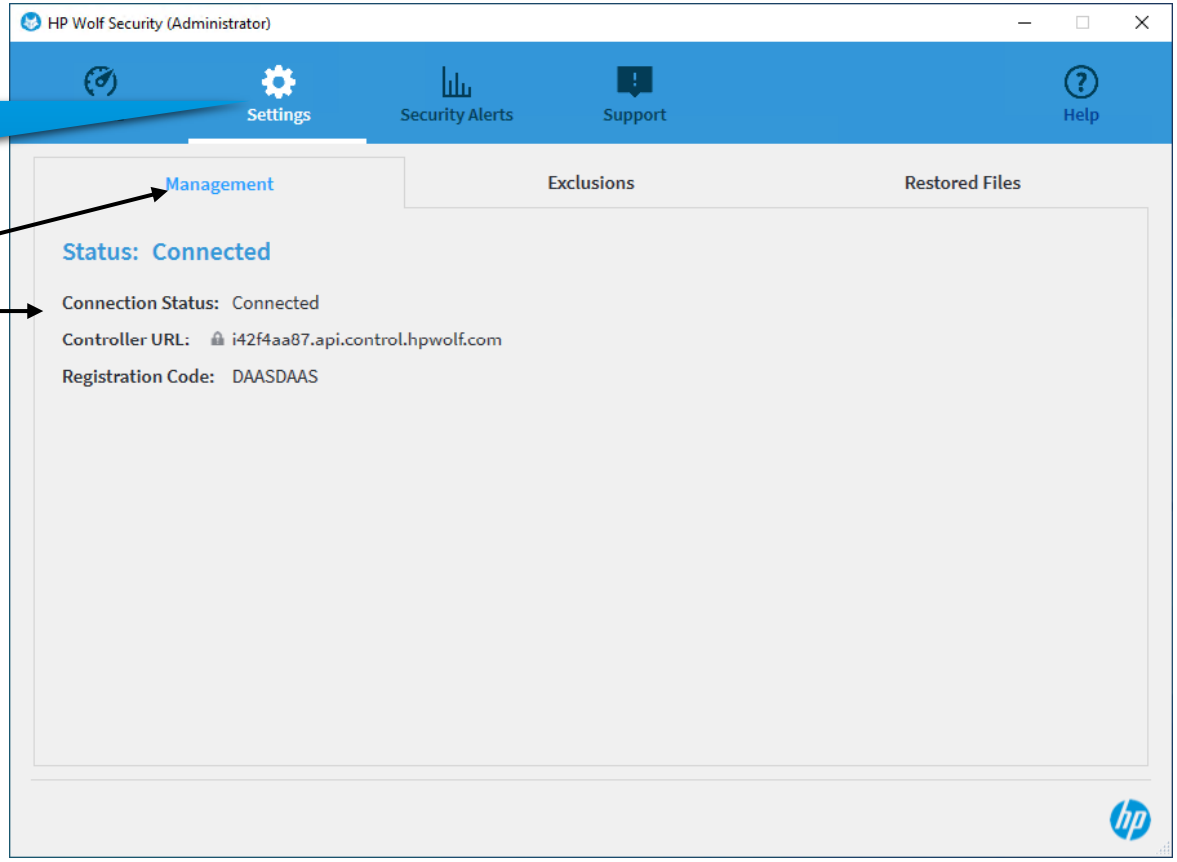


Getting Started Guide – HP Wolf Pro Security

After launching the **HP Pro Security** dashboard via the Windows Start Menu, the Dashboard will open. Selecting the ***Settings*** icon will reveal 3 tabbed pages of features that can be controlled in the software: Settings, Exclusions and Restored Files.

Management: Tab 1 of 3 on this (Settings) Page

Management: 'Status' – Displays the status of the endpoint's connection to the controller.



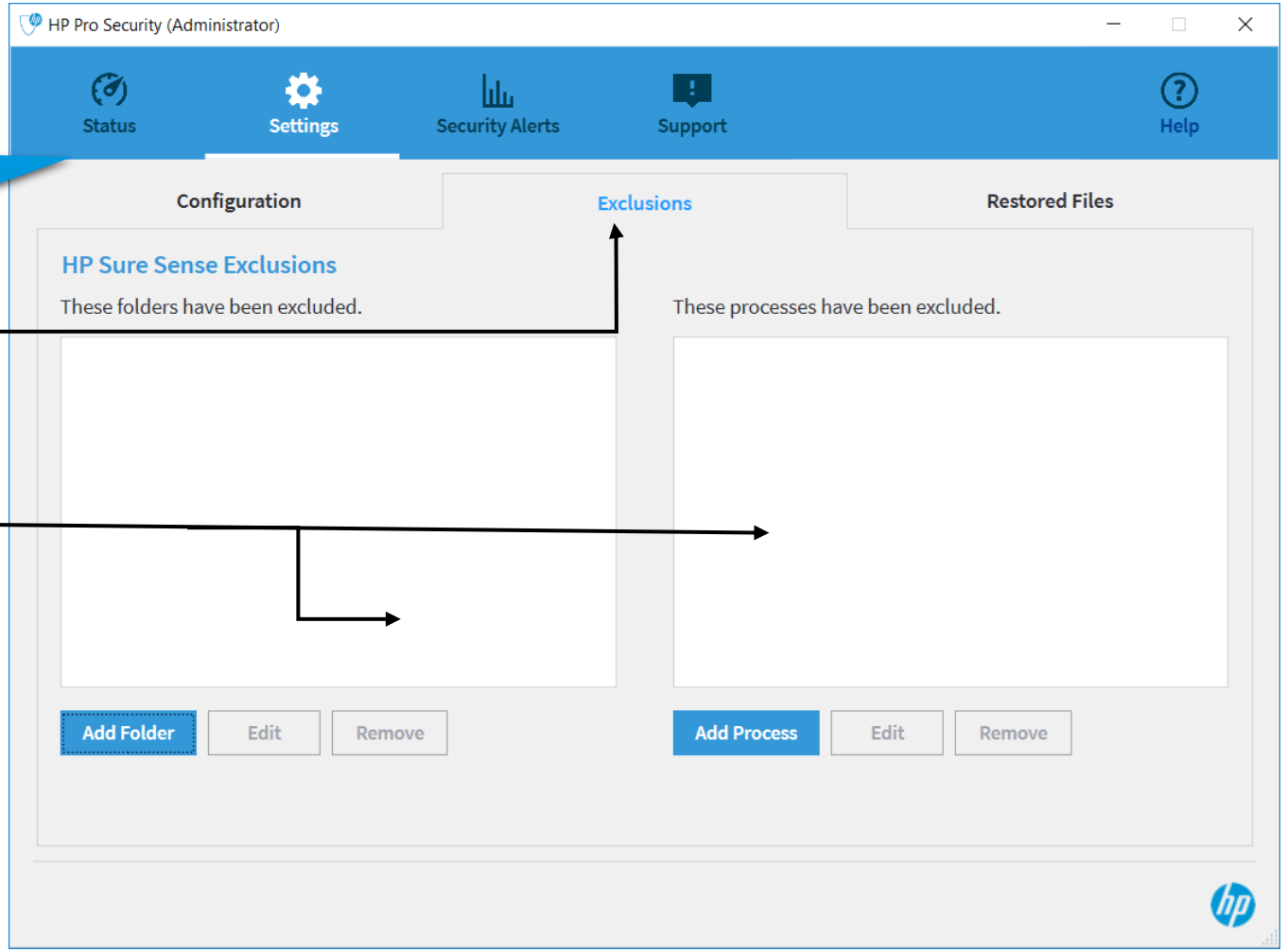
Getting Started Guide – HP Wolf Pro Security

After launching the **HP Pro Security** dashboard via the Windows Start Menu, the Dashboard will open. Selecting the ***Settings*** icon ***will*** reveal 3 tabbed pages of features that can be controlled in the software: Configuration, Exclusions and Restored Files.

Exclusions: Tab 2 of 3 on this (Settings) Page

Exclusion: Lists of folders and or processes that are known-safe folders, files, or processes. Adding a folder (containing a file) or a process-name to either list on this page will be bypassed (considered 'safe') when HP Pro Security *performs security scans.*

Adding this custom application to the Exclusions list will exclude the file from any future Malware scans.



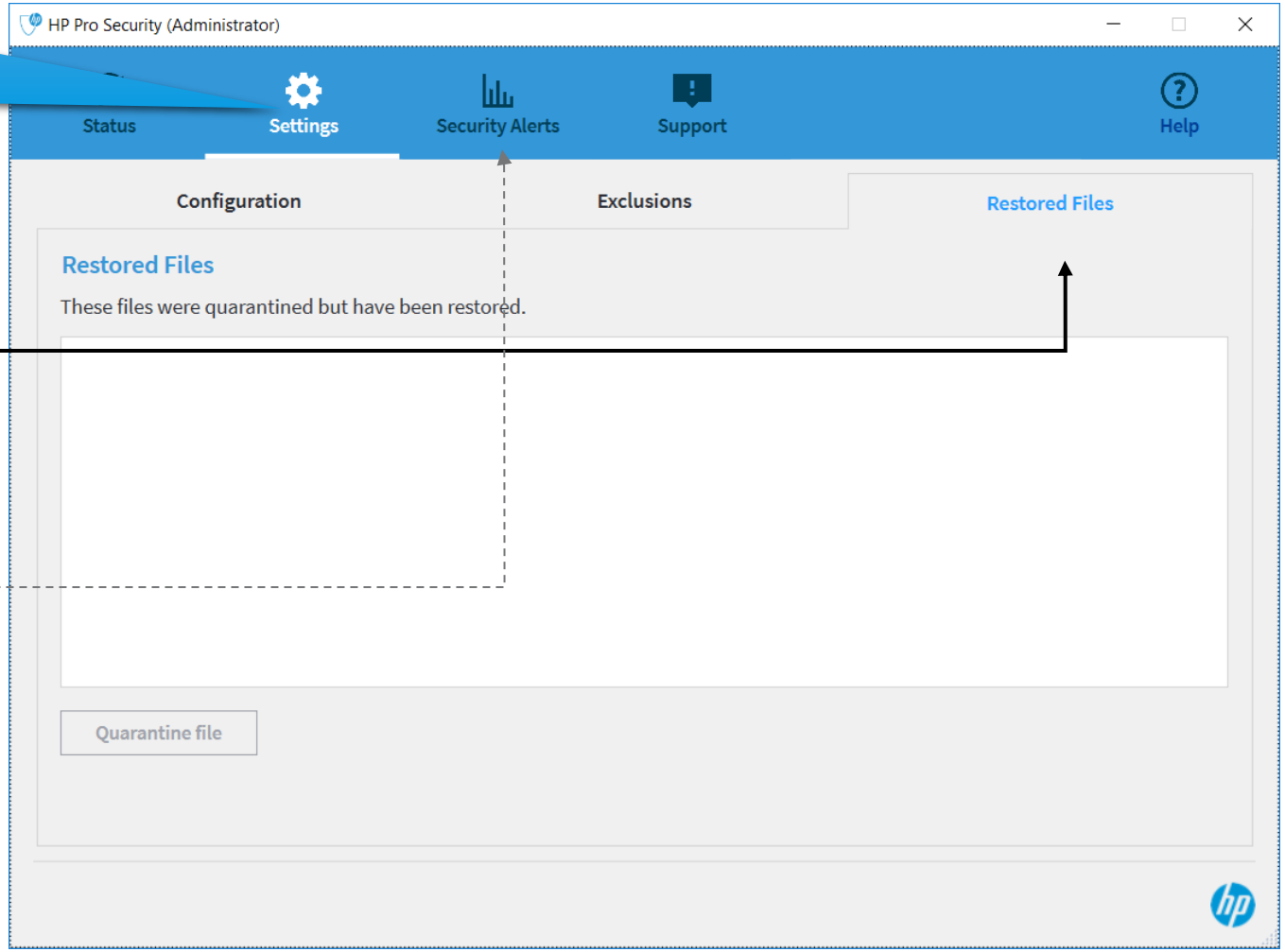
Getting Started Guide – HP Wolf Pro Security

After launching the **HP Pro Security** dashboard via the Windows Start Menu, the Dashboard will open. Selecting the ***Settings*** icon will reveal 3 tabbed pages of features that can be controlled in the software: Configuration, Exclusions and Restored Files.

Restored Files: Tab 3 of 3 on this (Settings) Page

Restored Files: This page maintains an active list of files HP Wolf Pro Security initially flagged as malicious, however, the user elected to mark the file as Safe. Typically, a safe file will have come *from a trusted source and the user took action to mark as safe.*

NOTE: Files that were flagged as un-safe have been captured and logged on the *Security Alerts* page



Getting Started Guide – HP Wolf Pro Security

After launching the **HP Pro Security** dashboard via the Windows Start Menu, the Dashboard will open. Selecting the ***Security Alerts icon*** will reveal a list of filenames and/or websites that were *quarantined* or flagged as malicious.

Attack data includes *Time, Source, Type (of attack), Response* and *Action.*

Time: Month, Day, Year and Time the threat was detected.

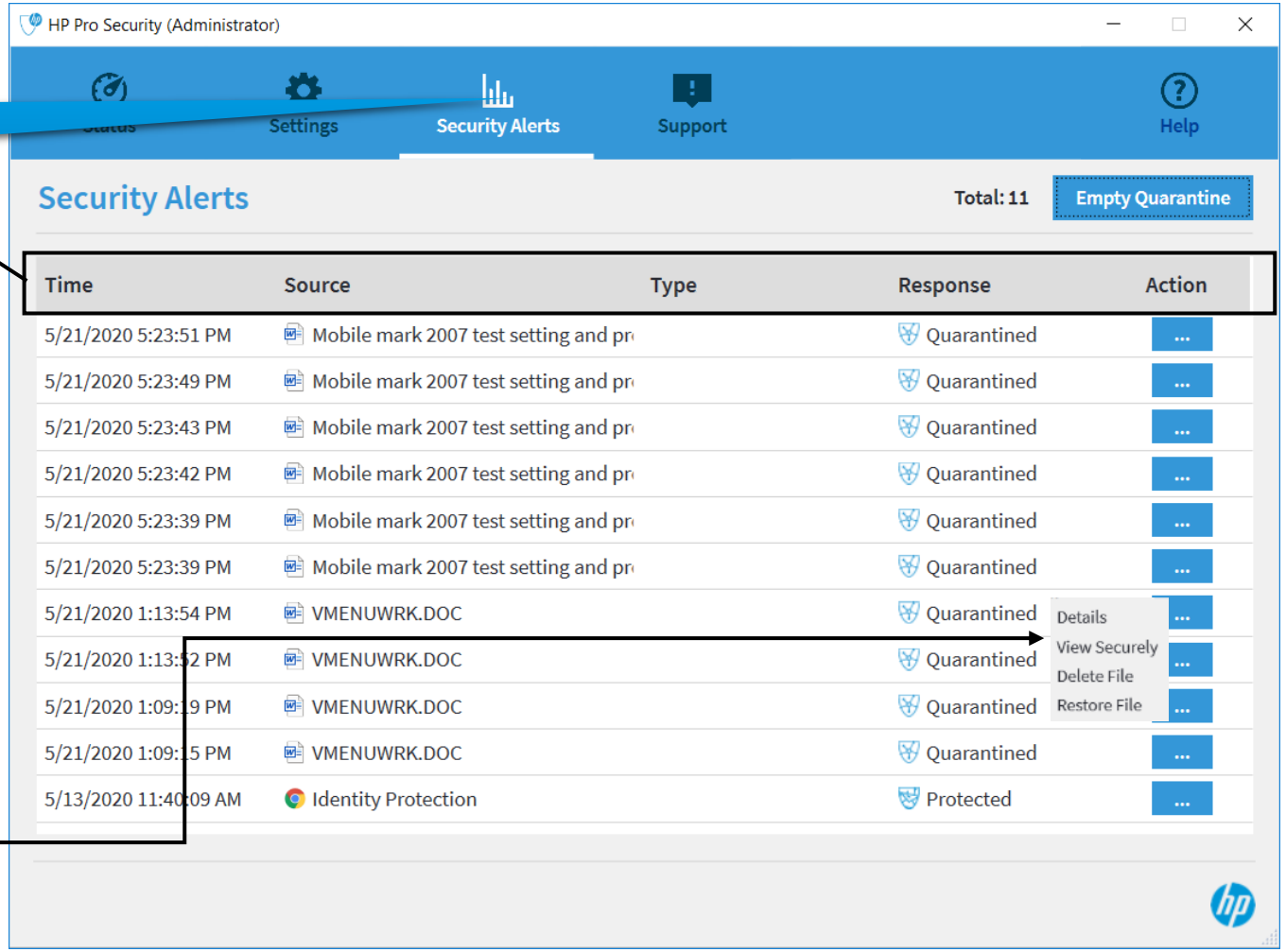
Source: Indicates the file type categorized and quarantined as a potentially malicious file. Typically, the icon will inform the user if the suspicious file was a document (e.g., Word, Excel) or an encounter via web-browser, flagging a website attempting to steal credentials.

Type: Some malware types can be categorized (e.g., Ransomware) and if able, HP Pro Security will display information in this column.

Response: The action taken by HP Pro Security when encountering a malicious file or website.

Action: The action … button provides multiple user options.

1. On a Quarantined file, the user is presented 4 options
   i. Details of the file- the location, time, and hash value.
   ii. View Securely – to open and view the file in a protected Virtual Machine and determine if file is safe or should remain quarantined.
   iii. Delete the file from PC
   iv. Restore – changes the file to a 'trusted' state.
2. On a Protected file, the user can view details of the website identified as a Phishing location.
   i. View Details of the file- the URL location, time, and hash value.



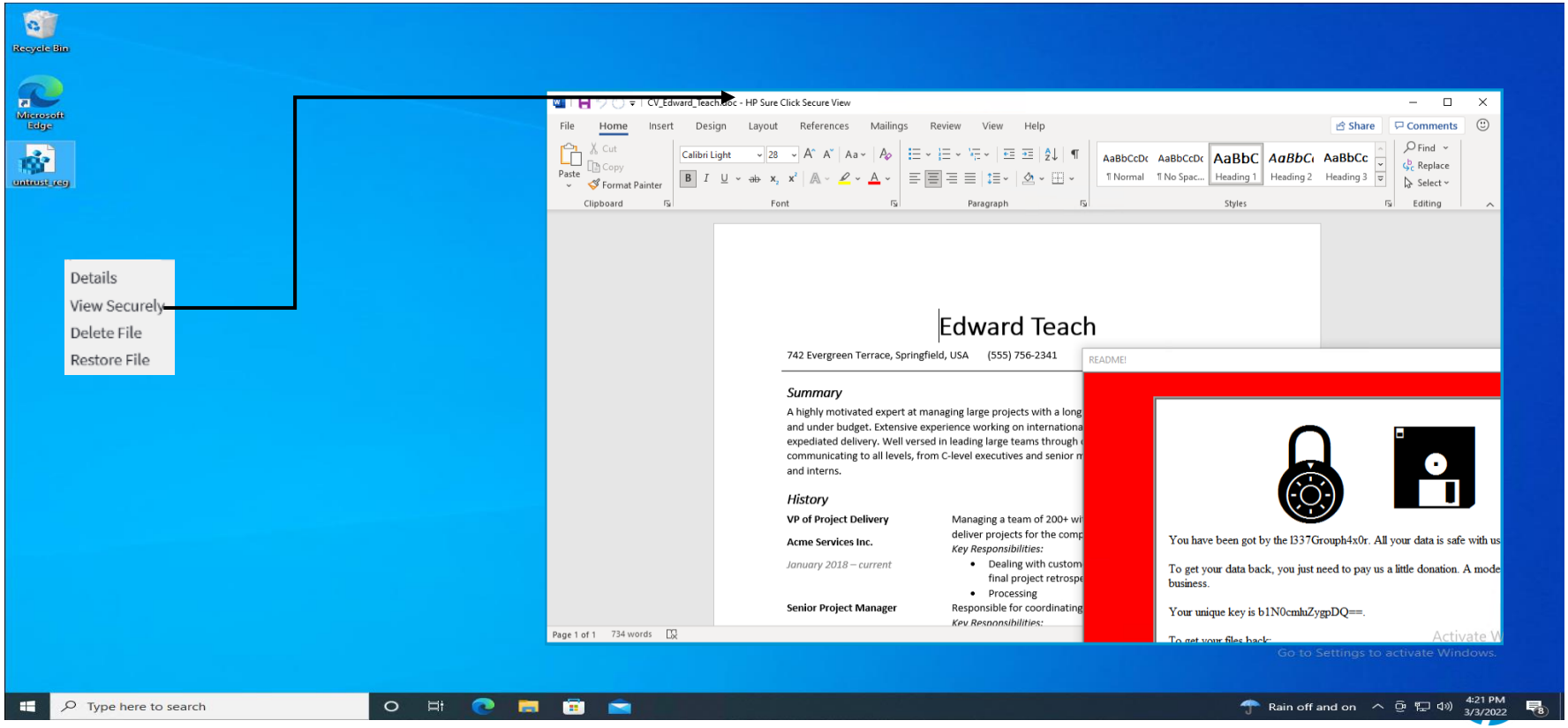
This is an industry-unique quarantine workflow specified in more detail below.

Unique workflow for quarantined files

The combination of hardware-backed isolation and NGAV allows WPS to present quarantine workflows that are unique in the industry. In the case of most NGAVs, the standard response to a potentially malicious quarantined file is to delete it or securely upload it for analysis in case the end-user is convinced that the detection is a false-positive. This leads to workflow disruptions, especially in the case of false positives because the file is not even allowed to be viewed. Depending on the file that is quarantined (and hence no longer accessible to the user), the disruptions can be severe.

WPS circumvents this issue entirely by allowing the quarantined file to be opened securely in isolation if the filetype is isolation-supported. The user does not need to care whether the file is malicious or not, they can view it securely. In case the file is malicious, the malware triggers in isolation and is destroyed as soon as the document is closed. The end-user device is completely unaffected.

Below is an example of a malicious resume containing ransomware that has already been quarantined, but the end-user is not sure if it's really malicious or not. The user can still view it securely, and it will open in fully isolated VM. Even if it turns out to be really malicious, as seen below, the malware is fully contained within the VM and is destroyed when the Word document is closed.



Getting Started Guide – HP Wolf Pro Security

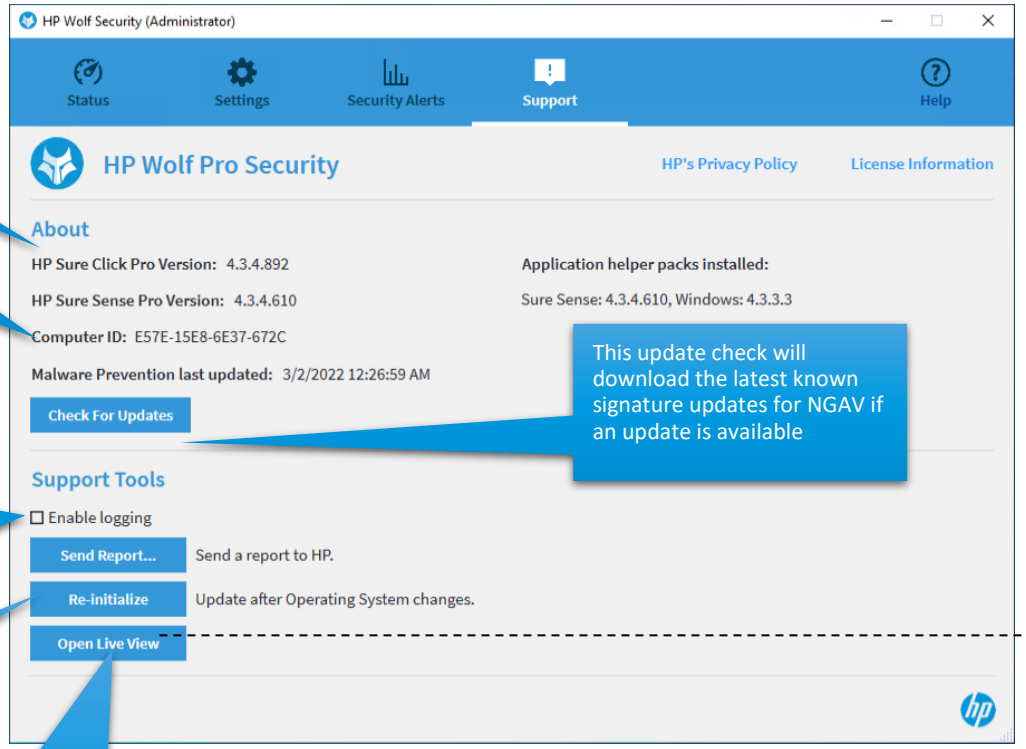
HP Sure Click Pro and HP Sure Sense Pro together provide the features that are part of WPS. Each application may receive updates separately from the HP Cloud. The **version numbers** will not be the same.

The **Computer ID** is a unique ID assigned to this endpoint. It is used to identify this endpoint on the controller and is also useful for support.

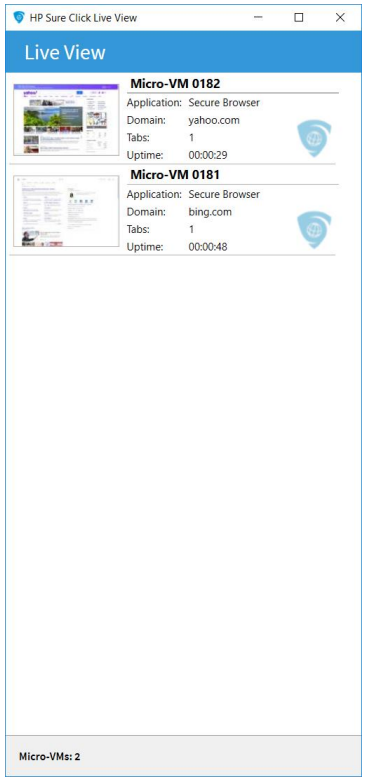
Enable Logging will create .zip log file in a user defined PC directory (e.g., 'Desktop') for the purpose of providing information to support. The "Send Report" button will transmit the log file to the controller for further triaging

"Reinitialize" is useful in certain situations when Threat Containment runs into unexpected errors. This button will recreate the virtual machine templates that are used to isolate malicious content.

Open Live View is an advanced feature useful for support. Pressing the Open Live View button will create a dialog-window (example, far right) and display the currently running virtual machines on the PC.



This update check will download the latest known signature updates for NGAV if an update is available



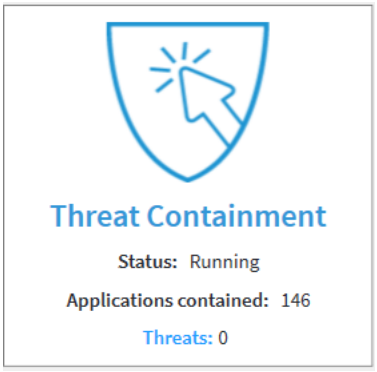
Getting Started Guide – HP Wolf Pro Security

Desktop Console status cards

Threat Containment

There are three statuses for isolation and monitoring:

- Running– Everything is normal and healthy.
- Action recommended – The application is not healthy and should be investigated.
- Disabled – This means that the agent has been disabled and is not protecting the computer.
- You can see how many items have been analyzed
- You can see how many threats have been prevented



The following status messages could be shown on this tile:

Status	Description
Waiting for HP Sure Click	If HP Sure Click remains in this state, try restarting your computer.
HP Sure Click is running	HP Sure Click is protecting you from websites and documents containing malware.
Enable HP Sure Click to protect your system	HP Sure Click is disabled. Select Enable Threat Containment from the system tray icon menu to enable it.
HP Sure Click is not running	HP Sure Click is not running. Try restarting your computer.
HP Sure Click requires initialization	HP Sure Click has not been initialized. To initialize, press the Initialize button on the Support page.
Checking HP Sure Click requirements...	This message may be shown briefly when HP Sure Click is starting.
Checking HP Sure Click status...	This message may be shown briefly when HP Sure Click is starting.
Checking for HP Sure Click updates...	HP Sure Click may need to download updates before it can run. Please wait for this process to complete.
Waiting to receive configuration	HP Sure Click needs to download configuration from the Controller before it can run. Please wait for this process to complete.
Failed to fetch configuration. Please check your network connection.	HP Sure Click needs to download configuration from the Controller before it can run. Please check that your computer is connected to the internet.

Please check that your computer is connected to the internet	Please check that your computer is connected to the internet
HP Sure Click will be ready in a few minutes	HP Sure Click is preparing for use. Please wait for this process to complete.
Initialization in progress	HP Sure Click is capturing the computer's current system state. Please wait for this process to complete.
Initialization required / Initialization paused	HP Sure Click needs to capture the computer's current system state. This should happen when the system becomes idle. Alternatively, you can press the 'Initialize' button on the 'Support' page to start this process.
Re-initialization in progress	HP Sure Click is capturing the computer's current system state. HP Sure Click is still running so you are still protected during this process.
Re-initialization required / Re-initialization paused	HP Sure Click needs to capture the computer's current system state. This should happen when the system becomes idle. Alternatively, you can press the 'Re-initialize' button on the 'Support' page to start this process. HP Sure Click is still running so you are still protected during this process.
HP Sure Click requires a computer restart for an upgrade to take effect	Updates to HP Sure Click have been installed. Restart your computer to switch to the updated version.

The following error messages could be shown on this tile

Error messages	Description
HP Sure Click does not support this CPU	HP Sure Click does not support this CPU and therefore is unable to run.
HP Sure Click requires a VT-x capable system	The CPU does not support VT-x virtualization extensions (or equivalent) and therefore cannot run HP Sure Click.
HP Sure Click requires VT-x to be enabled	VT-x virtualization extensions (or equivalent) are disabled in the system BIOS. You need to enable VT-x in the system BIOS to allow HP Sure Click to run. See How to enable Virtualization Technology in the BIOS.
HP Sure Click requires Extended Page Tables (EPT) to be enabled	Extended Page Table virtualization extensions are disabled in the system BIOS. You need to enable EPT in the system BIOS to allow HP Sure Click to run.
Unsupported AMD CPU family	The computer has an AMD processor that is not supported by HP Sure Click.
HP Sure Click memory requirements have not been met	HP Sure Click has detected that it is short of memory. Please close some programs to make more memory available.
Not enough free memory. Please provide more by closing some programs	HP Sure Click has detected that it is short of memory. Please close some programs to make more memory available.

Provide more free disk space and then restart the computer	HP Sure Click initialization requires at least 1.5GB of free space on the system disk. Please make sure 1.5GB of disk space is available and then restart the computer.
HP Sure Click is incompatible with systems using Gladinet	HP Sure Click is not compatible with Gladinet software.
HP Sure Click is active in another user session	HP Sure Click is not configured to support multiple users logged into the same computer at the same time.
HP Sure Click requires a computer restart to protect your system	The computer must be restarted before HP Sure Click will run.
HP Sure Click requires updates to support the installed version of Windows. Restart your computer to allow these updates to be installed.	HP Sure Click requires an additional component to support this version of Windows. The system must be restarted to allow this component to be installed.
HP Sure Click is unable to download updates required to support the installed version of Windows. Please check your internet connection.	HP Sure Click requires an additional component to support this version of Windows. The system has been unable to download the necessary components. Please check your system is connected to the internet and then wait for the download to complete.
HP Sure Click requires updates to support the installed version of Windows. Please wait for the updates to be installed.	HP Sure Click requires an additional component to support this version of Windows. Please wait for the system to complete installation of this component.
HP Sure Click requires updates to support the installed version of Windows	HP Sure Click requires an additional component to support this version of Windows.
No supported Windows language pack is installed	HP Sure Click requires you to install a Windows language pack.
The user's Windows display language is not supported	The user's Windows display language is not supported
Restart the computer to install pending Windows updates	HP Sure Click cannot initialize because the computer needs to restart to apply Windows updates. Please restart the computer, wait for the updates to apply, and then press the 'Initialize' button to start the initialization process
Windows Update is in progress	HP Sure Click cannot initialize because Windows update is in progress. Please wait for it to finish or restart the computer. Then press the 'Initialize' button to start the initialization process.
HP Sure Click requires the VBA component to be installed with Microsoft Office	HP Sure Click requires Visual Basic for Applications to be installed with Microsoft Office. Please install the VBA component and then press the 'Initialize' button to start the initialization process.
Office is not activated	HP Sure Click requires that Microsoft Office be activated. Please activate Microsoft Office, and then press the Initialize button to start the initialization process.
No supported Office UI language pack is installed	HP Sure Click requires one of the following Microsoft Office UI language packs to be installed

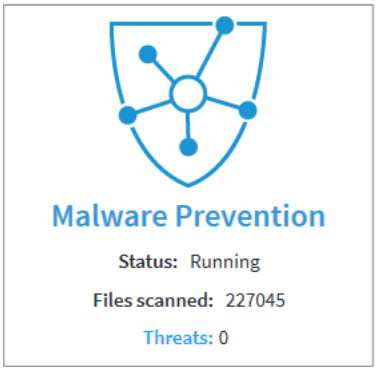
HP Sure Click is unable to support Hyper-V on this computer	To allow HP Sure Click to run, either disable Hyper-V or enable Windows Hypervisor Platform (see Windows Hyper-V Support).
HP Sure Click requires UEFI boot in order to support Hyper-V	UEFI boot was not detected. To allow HP Sure Click to run, either disable Hyper-V or enable Windows Hypervisor Platform (see Windows Hyper-V Support).
HP Sure Click requires Windows 10 or later in order to support Hyper-V	An unsupported operating system version was detected. Disable Hyper-V to allow HP Sure Click to run.
HP Sure Click does not support this CPU when Hyper-V is enabled	An unsupported CPU was detected. To allow HP Sure Click to run, either disable Hyper-V or enable Windows Hypervisor Platform (see Windows Hyper-V Support).
HP Sure Click requires the Secure Boot third party key in order to support Hyper-V	In the system BIOS open the 'Secure Boot Configuration' menu. Select 'Enable MS UEFI CA key' to allow HP Sure Click to run.
HP Sure Click requires a CPU capable of VMCS shadowing in order to support Hyper-V	The CPU does not support VMCS Shadowing. To allow HP Sure Click to run, either disable Hyper-V or enable Windows Hypervisor Platform (see Windows Hyper-V Support).
HP Sure Click failed to enable support for Hyper-V	Please contact HP Support to fix this issue.
Micro-virtualization blocked while enabling support for Hyper-V	Please contact HP Support to fix this issue.
BitLocker must be suspended before the computer is shutdown/ restarted	You must suspend BitLocker before the computer is restarted. From the Windows Control Panel, select BitLocker Drive Encryption, then Suspend Protection/
HP Sure Click unable to configure the UEFI boot order when enabling support for Hyper-V	Please contact HP Support to fix this issue.
HP Sure Click unable to determine the boot device when enabling support for Hyper-V	Please contact HP Support to fix this issue.
Last initialization canceled	HP Sure Click's initialization process was canceled so did not complete.
Last initialization blocked	HP Sure Click was unable to complete the initialization process. Try pressing the 'Initialize' button on the 'Support' page to start the initialization process again. If that fails please contact HP Support.
Last initialization attempt failed	HP Sure Click was unable to complete the initialization process. Try pressing the 'Initialize' button on the 'Support' page to start the initialization process again. If that fails please contact HP Support.
Last initialization attempt unsuccessful	HP Sure Click was unable to complete the initialization process. HP Sure Click has previously initialized so is still able to protect you computer. Try pressing the 'Re-initialize' button on the 'Support' page to start the initialization process again.

Unsupported configuration. Please contact support.	Please contact HP Support to fix this issue.
Internal error, please restart the computer	To resolve this issue, restart the computer. If that does not resolve it please contact HP Support.
Micro-VM could not be loaded. Restart the computer and if the condition persists contact support.	A problem occurred which prevented HP Sure Click from correctly loading micro-VMs. Try restarting the computer and consult HP Support if the problem reoccurs.
The HP Sure Click installation has been corrupted and needs to be repaired	Some files are missing from the HP Sure Click installation. This may be a result of doing a Windows System Restore. Download and install the latest version of the product to fix the corruption - see Download Latest Version.

Malware Prevention

There are three statuses for this feature:

- **Running**– Everything is normal and healthy.
- **Action recommended** – The application is not healthy and should be investigated.
- **Disabled** – This means that the agent has been disabled and is not protecting the computer.
- You can see how many items have been scanned
- You can see how many threats have been prevented



The following **status messages** could be shown on this tile:

Status message	Description
HP Sure Sense is running	HP Sure Sense is protecting you from malicious files.
Enable HP Sure Sense to protect your system	HP Sure Sense is disabled. Select Enable Malware Prevention from the system tray icon menu to enable it.

HP Sure Sense will be ready in a few minutes	HP Sure Sense is preparing for use. Please wait for this process to complete.
HP Sure Sense requires a computer restart for an upgrade to take effect	Updates to HP Sure Sense have been installed. Restart your computer to switch to the updated version.
HP Sure Sense is not accessible	HP Sure Sense appears to be installed but HP Wolf Pro Security is unable to access it. Please try restarting your computer.
Failed to download updates	HP Sure Sense needs to download updates before it can run. Please check that your computer is connected to the internet.
Behavioral Protection is disabled because an incompatible product is present	To enable Behavioral Protection please remove any product which is known to be incompatible with it.
Waiting to receive configuration	HP Sure Sense needs to download configuration from the Controller before it can run. Please wait for this process to complete.
Failed to fetch configuration. Please check your network connection.	HP Sure Sense needs to download configuration from the Controller before it can run. Please check that your computer is connected to the internet.
Unknown Error	Please contact HP Support to fix this issue.

Identity Protection

There are three statuses for Identity Protection:

- No action required– Everything is normal and healthy.
- Action recommended – The application is not healthy and should be investigated.
- Disabled – This indicates either the Add-In in the browser is disabled or the protection as a whole is disabled.
- You can see how many sites you have been protected from

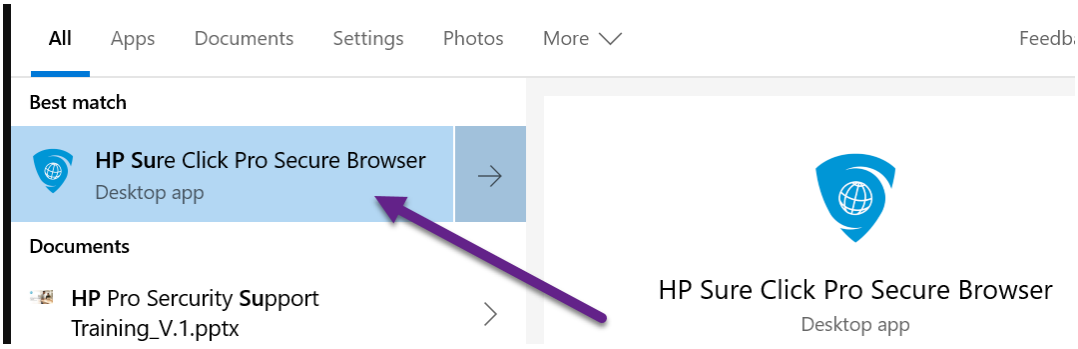
The following **status messages** could be shown on this tile:

Status	Description
Identity Protection is running	HP Identity Protection is protecting you from identity theft attacks.
The HP Sure Click Secure Browsing extension appears to be disabled in your default browser. Please enable it.	When you open your default browser you may be prompted to enable the HP Sure Click Secure Browsing extension. In your default browser you can also select the Extensions menu item to open the Extensions page. Then locate the HP Sure Click Secure Browsing extension and enable it.
Threat Containment is not running. Please enable it or wait for it to start.	The HP Sure Click Secure Browsing extension requires HP Sure Click Pro to be running. If it is disabled, then please enable it. If it is preparing for use, then please wait for it to finish.
The HP Sure Click Secure Browsing extension is not supported by your default browser	The HP Sure Click Secure Browsing extension is available in HP Sure Click Secure Browser, Google Chrome, Mozilla Firefox and new Microsoft Edge. You can change your default browser to one of these by searching for 'Default Web Browser' in the Windows Start menu.
Identity Protection is unable to run	HP Identity Protection is not able to run. Please try restarting your computer.

Secure Browsing

You can open the HP Secure Browser directly if you know you will be browsing high-risk sites.

Follow these steps to begin:



The Secure Browser will open. Begin browsing the Web as you would with any other browser. This browser is chromium based, and every tab you open will be opened in an isolated container. Use the browser to directly browser to suspicious websites if your workflow calls for it. If link protection is enabled by policy, WPS will automatically open untrusted links in this browser.

Getting Support

Gathering Information

Some information will be needed to explain the issue being reported or the possible resolution. To help resolve your issue quickly please forward the information below to your IT Administrator or Security Team so they can submit a request on your behalf.

Please ensure that you submit the following **mandatory** information:

- Device name
- Summary of the issue
- Summary of a resolution suggestion - Do you know how we can help you?
- Is it consistently reproducible?
- Can you include any screenshots of pop-ups or errors that will help to expedite the resolution?

Excerpts from this guide are provided with permission from third parties and redistributed as required with HP software solutions.

© Copyright 2022 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.