HP WOLF SECURITY

Protect your fleet with simple, policy-based print security

Grow your business the secure way- with HP Security Manager

An HP Wolf Pro/Enterprise Security Solution

Stay one step ahead of evolving threats

Your company is continuously creating confidential, valuable data that's crucial to running your business. And you're probably using multiple security methods—including authentication, encryption, and monitoring—to protect this data on your PCs, networks, and servers. But is your printing and imaging environment as secure as the rest of your infrastructure?

Print security can be complicated. HP Security Manager[1] makes it simple to take device management off your to-do list and protect at-risk printers by establishing policies, automating fixes, and maintaining ongoing compliance.

To help keep your business protected, you need a solution that simplifies and strengthens security throughout your printing and imaging environment, saving your business time and money that can be better spent elsewhere.

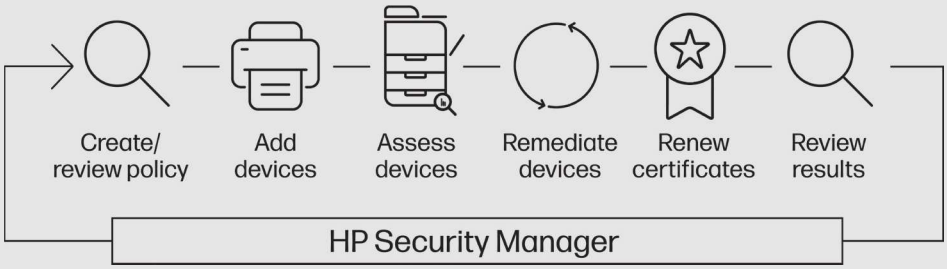
Bring clarity to compliance

Strengthen your security posture and make it consistent across your entire fleet of devices. HP Security Manager[1] lets you monitor, manage, and automatically restore critical settings that make maintaining compliance simple.

HP Security Manager[1] offers a simple, intuitive process for securing your fleet. Efficiently deploy and monitor devices by applying a single security policy across the fleet, and secure new HP devices as soon as they are added to your network with HP Instant-on Security.[2] Actively maintain and verify compliance with your defined security policies using HP Security Manager's automated monitoring and risk-based reporting. Rely on the automatic deployment and updating of identity certificates that strengthen information security while significantly reducing administrative overhead.

How HP Security Manager secures your fleet

HP Security Manager[1] offers a simplified approach to HP fleet security that strengthens compliance and reduces risk.



Provide fleet security with effortless policy creation

The easy-to-use HP Policy Editor simplifies policy creation with an intuitive rules engine that provides guidance, and helps create a comprehensive policy for your environment. Easily modify your security policies to best suit changing company needs, regulations, or industry standards.

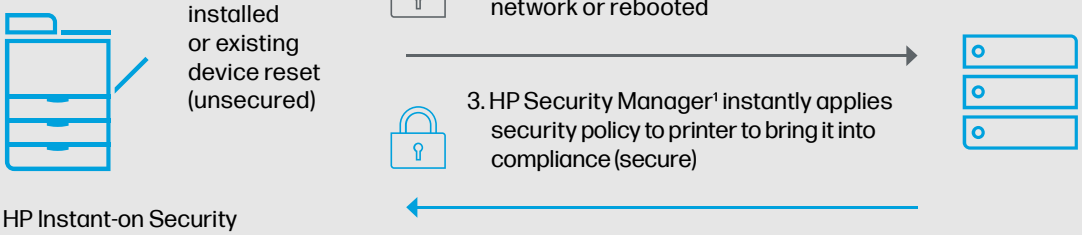
HP Security Manager Base Policy template

Easily create a security policy for your print environment using the HP Security Manager[1] Base Policy template. The template provides a baseline approach for securing a common enterprise printing environment, but is easily tailored to meet individual security policy requirements. The template combines settings from the U.S. National Institute of Standards and Technology and HP Security Best Practices Checklist with customer input on the security settings necessary to create a secure—yet productive—print environment.

Connect devices to your policy in a variety of ways

It's easy to add HP devices to HP Security Manager[1].

- **Auto-Discovery:** Let Security Manager[1] discover your HP devices through auto-discovery. Set it to look over a certain number of network hops or within a specific IP address range. Then choose which devices you want to manage from the list.
- **.txt or .xml file:** Add an existing list of devices by importing a .txt or .xml file with device IP addresses or host names, including .xml exports from HP Web Jetadmin.[4]
- **Instant-on Security:** Use the HP Instant-on Security feature to automatically add each HP device into Security Manager[1] as soon as it is connected to your network (or after a cold reset) without any IT intervention. Unique to HP Security Manager[1], HP Instant-on Security immediately configures devices to be compliant with your specific corporate security policy—saving you time and minimizing risk.[2]



HP Instant-on Security

Maximize your investments with proactive compliance

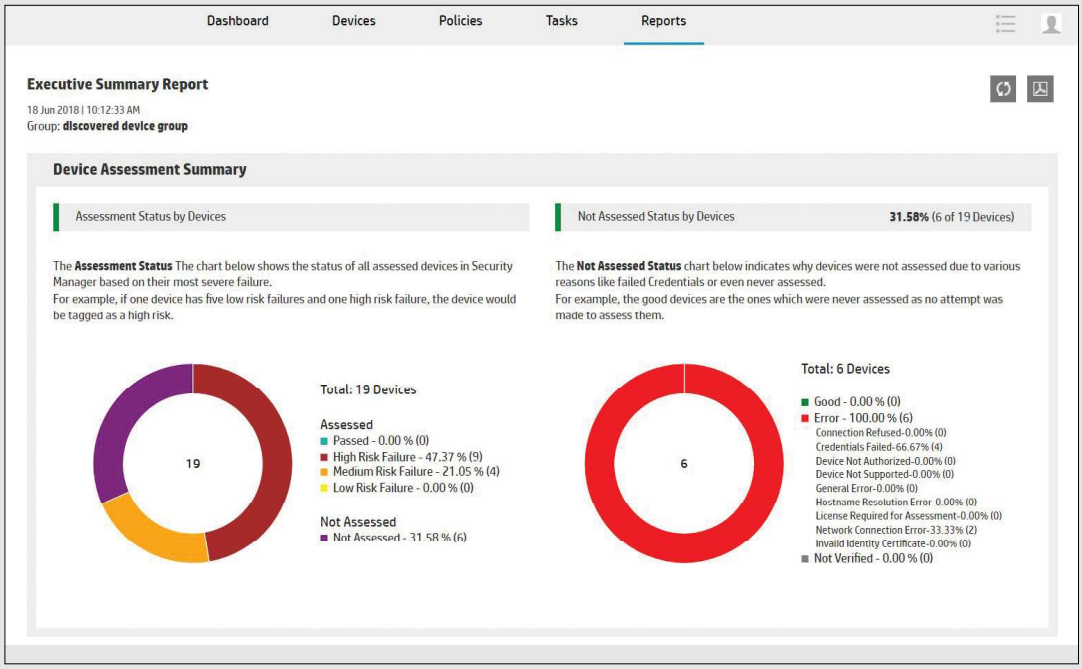
HP Security Manager[1] helps maintain compliance with ongoing assessments and automated remediation. You decide how often you want to assess and remediate your devices. Daily, weekly, or monthly—it's up to you.

- **Assessment:** During an assessment, HP Security Manager[1] runs in the background and verifies your fleet's security settings against a specific policy. The assessment process then reports anynoncompliant features.
- **Remediation:** HP Security Manager[1] can also automatically apply the correct policy settings to any noncompliant features recognized during the assessment. The corrected setting is assessed again to confirm it was applied successfully.

Reduce risk with comprehensive fleet security reporting

Protect your information with built-in reporting. Users can run summary reports on the overall risk level of the fleet, and then drill down into specific risks by device or security settings. High-level emailed reports can also be sent after each auto-scheduled assessment and remediation.

HP Security Manager[1] can also provide a risk assessment to help you identify less secure devices. Less secure devices may not have the most recent device firmware, may not have Jetdirect firmware, or may not be enabled with Sure Start, run-time intrusion detection, or whitelisting capabilities.



Protect your workflow with fleet-wide certificate management

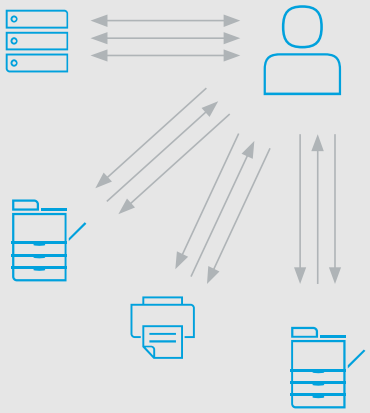
Certificates are vital to protecting the flow of information to and from your devices. They are used to prove identity and encrypt data, enabling secure communication between trustworthy entities. Manually installing unique certificates can be an error-prone, laborious, and time-consuming task—up to 15 minutes per device. This causes many customers to opt out of using certificates entirely, or maintaining them properly.

HP Security Manager's latest innovation streamlines this process by deploying unique identity certificates across your fleet, continuously monitoring them to ensure they remain valid, and automatically replacing revoked or expired certificates.

HP Security Manager[1] efficiently implements and updates both ID and CA certificates—helping increase the security of your infrastructure, applications, and device communications.

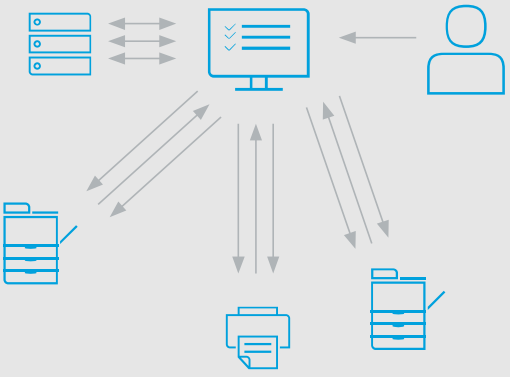
Before

Manual, time-consuming, and error-prone process required on each device

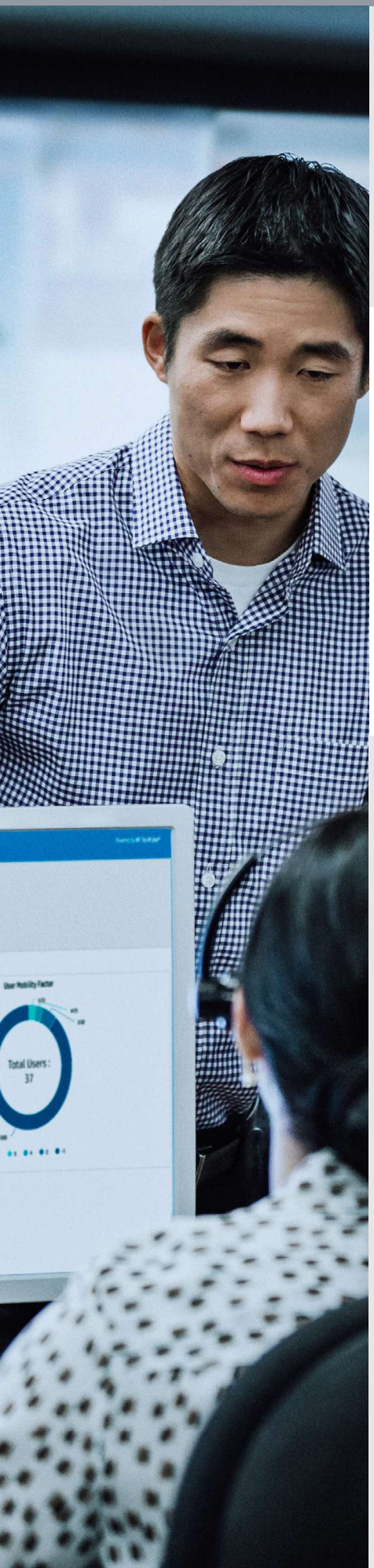


After

Simple, efficient, one-time setup for the entire fleet with HP Security Manager[1]



How can this easy-to-use solution benefits you?



HP Security Manager[1] is a versatile security solution that can apply to a variety of contexts and business situations.

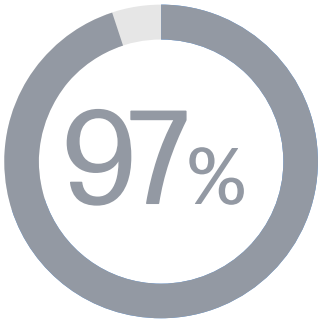
For example, financial services firms know that protecting client information is crucial to the success of their business, and is required by industry regulations. However, with print fleets that often number in the thousands, maintaining security consumes a substantial amount of administration overhead.

With HP Security Manager[1], financial services firms can save time and money by scheduling a daily assessment and remediation of their HP printing and imaging fleet. This helps ensure that the fleet remains compliant with a company's security policy while freeing up the IT team to focus on other activities. Administrators can also print or save built-in fleet, device, or feature-level reports for proof-of-policy compliance, making it easy to verify that client information is safe and secure.

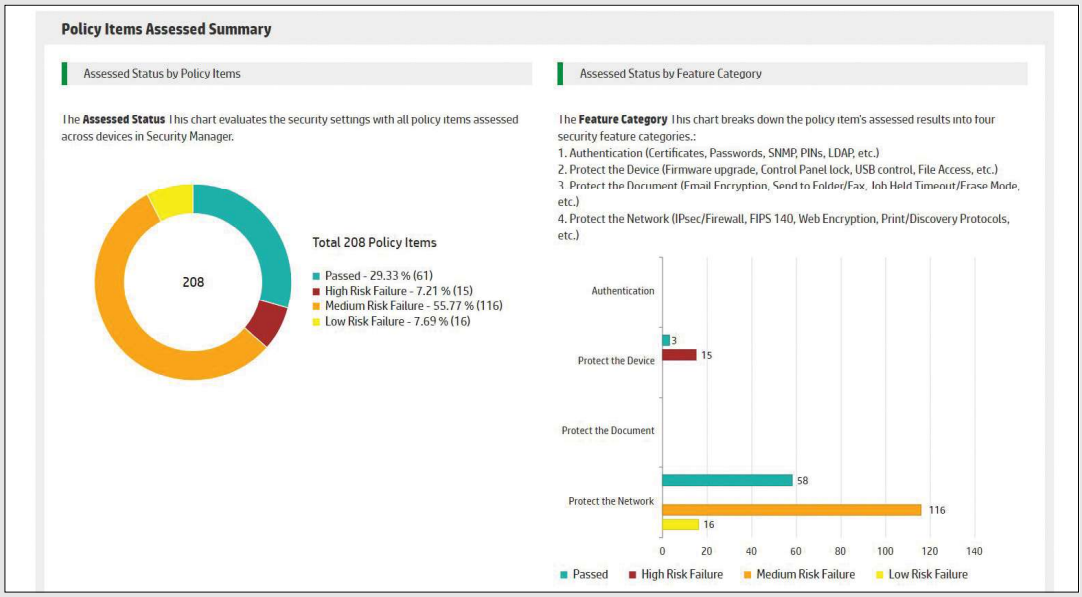
Before HP Security Manager

Less than 25% of the fleet complied with the security policy

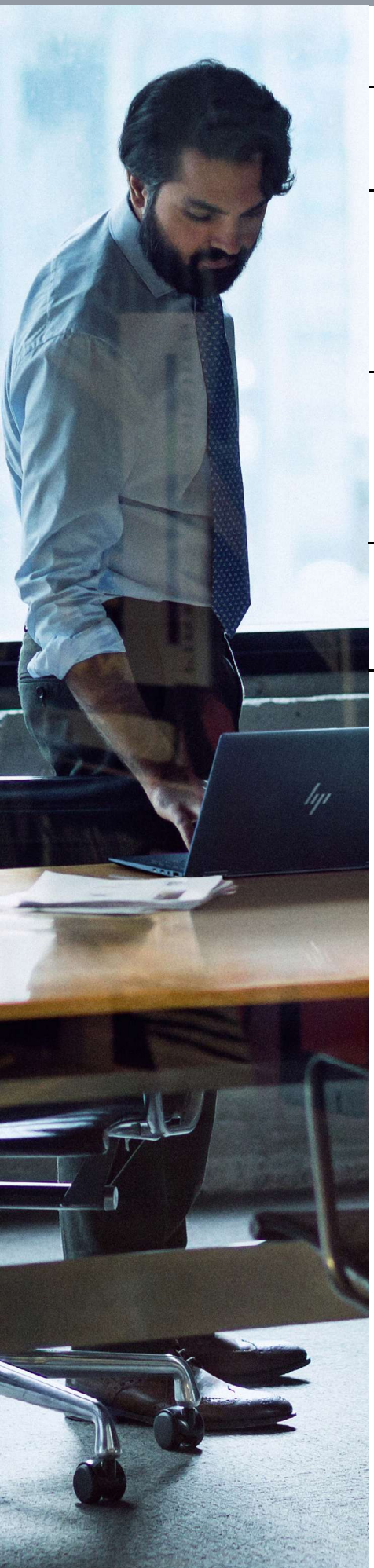
After HP Security Manager



More than 97% of the fleet complies with the security policy



System requirements



The following are the basic requirements for installing the newest version of Security Manager

- Internet Information Services (IIS) 7.5 or newer versions.
- Microsoft NET Framework 4.8 or newer version.

Note: If the HP Security Manager installer does not detect the .NET Framework 4.8 or newer versions. the installer provides the appropriate iistallation instructions and Microsoft URL to download the NET Framework.

Note: Security Manager supports platforms that have Microsoft Windows and NET Framework high-priority updates.

- **Database:** Security Manager installs Microsoft SOL Server 2022 Express.
- For a full list of supported databases, see the Security Manger Release Notes at HP Security Manager product support page.
- A supported Microsoft Windows computer
- **Operating Systems:** Supports the following Microsoft Windows 64-bit operating systems:

Note: IHP no longer supports or tests Microsoft operating systems released for prior HP Security Manager installations. Support will only be provided for the latest Security Manager release versions. HP recommends to use a supported Windows Server with Windows 10 and 11 for optimal performance.

1. Windows Server 2022
2. Windows Server 2019
3. Windows Server 2016
4. Windows Server 2012 R2
5. Windows Server 2012
6. Windows 11
7. Windows 10

- **Server Hardware:** HP recommends the following hardware configuration for the server:

  1. 4 or more processor cores
  2. 2.8 GHz or higher processor speed
  3. 12 GB or more of RAM
  4. 4 GB of available storage

- **Supported browsers:** Security Manager supports the following browsers:

Note: HP Security Manager is supported in VMWare and Hyper-V environments with the Windows versions listed previously. Hyperthreading is optional for VMware and Hyper-V. Reserve memory is required for Hyper-V.

Note: If installing Security Manager on a VMware instance, you must use the hardware (MAC) address of that virtual adapter during the ordering of the license file. Be aware that VMware dynamically generates the virtual adapter MAC address and does not guarantee it will remain static during session restarts or power toggling. If the MAC address changes, the print license service will fail to operate properly. Refer to VMware help documentation for instructions on how to configure a static MAC address or how to change the modified MAC address back to original.

Note: Importing a license file might fail on VMware VM's. If this occurs, reboot the virtual machine.

Note: SQL 2017 or 2019 is recommended on VMware because testing with older versions and partially disabled TLS settings resulted in random database connectivity issues. However, SQL 2022 is recommended to avoid vulnerability issues with earlier versions of SQL server.

1. Chrome version 60 or newer
2. Microsoft Edge (Chromium-based) version 79 or newer

Sign up for updates hp.com/go/getupdated

HP WOLF SECURITY

1. HP Security Manager must be purchased separately. For details, see hp.com/go/securitymanage.
2. Available on select product models and firmware versions.
3. This tool is provided for general comparison only. This information is based on manufacturers' published and internal specifications, and proprietary data and algorithms.

The information is not guaranteed accurate by HP Development Company. Users can customize the security policies used in the analysis, which will affect the results. Actual results may vary.

4. HP Web Jetadmin is available for download at no additional charge at hp.com/go/webjetadmin.

4AA3-9275ENW, March 2024