

## HP JetAdvantage Security Manager 2.1

Formerly HP Imaging & Printing Security Center



- ★★★★★ Features and Productivity
- ★★★★★ Value
- ★★★★★ Administration
- ★★★★☆☆ Software Integration
- ★★★★★ Customer Support and Training



## OVERVIEW

Document and device security is a concern in every organization, and for entities such as government offices, healthcare providers, financial services firms, and law offices, it is an imperative. MFPs can often be the weak link in the document chain of custody, but managing the various security settings on each model can be confusing and time consuming. HP JetAdvantage Security Manager, formerly marketed as Imaging & Printing Security Center, centralizes and automates the process of bringing and keeping devices in compliance with an organization's preferred security policies, delivering IT administrators security-specific monitoring and management tools that go well beyond the capabilities of traditional network device management platforms.

## Strengths

- Monitors entire MFP/printer fleet for devices that are out of compliance with an organization's set security policies
- Can automatically change 150+ security settings remotely to bring devices back into compliance
- "Best practice" template provides baseline security policy based on industry and HP security expert recommendations
- Streamlines use of unique security certificates for HP output devices across the enterprise
- Intelligent policy editor keeps administrators from creating invalid policies
- Leverages the HP Instant-On Security feature of enterprise-class devices to change settings to match desired policy once the device is connected to the network
- Risk-based reports show which devices are in compliance and which are not
- Reasonable price for perpetual device licenses

## Weaknesses

- Functionality not supported on all HP output devices
- No support for non-HP devices



## BLI Recommendation



It's not often that a completely new class of document imaging solution comes along, yet this is precisely what HP has created with its JetAdvantage Security Manager. HP Security Manager is the industry's first policy-based imaging and printing compliance solution and was designed to tackle the thorny issues surrounding device security such as unauthorized access, changes to device settings, network security and more. In fact, its unique functionality earned it an "Outstanding Achievement" honor in BLI's Winter 2013 awards season.

Unlike traditional network device management utilities (such as HP's own Web Jetadmin) that are general-use tools for monitoring and managing output devices on the network, HP Security Manager is tailored to the security aspects of those devices. Functionality is divided into three logical parts: policy creation; device assessment, monitoring and remediation; and reporting. Templates and automated processes mean that administrators don't need to be trained IT security experts to use the solution. For example, when customizing the settings template to suit a particular need, the administrator can rely on HP Security Manager's Policy Editor to warn them if a particular change brings the proposed policy out of compliance with best practices, or if that change conflicts with an interrelated security setting.

Given the sheer number of settings available—more than 150, depending on the capabilities of the device—this sort of sanity check will be welcome even for experienced IT professionals.

While HP Security Manager is very well executed, there are a couple of things on our wish list. For one, while the solution is compatible with a good subset of HP output devices (for example, all enterprise-class networked LaserJet devices), it does not support all HP output devices an organization might have in use, nor does its functionality extend to non-HP devices. (HP reports that it is expanding compatibility to other devices in its portfolio with each release.) And while HP intentionally designed Security Manager to be a separate tool from WJA—the former for background security compliance monitoring, the latter for day-to-day print device administration—some IT departments might prefer to have the complementary functionality accessible in one tool. Still, HP Security Manager is a unique and important tool for any IT department charged with administering HP enterprise devices that are compatible with it.

## Product Profile

<b>Product:</b>	HP JetAdvantage Security Manager
<b>Version:</b>	2.1
<b>Software Developer:</b>	Hewlett-Packard Company
<b>Phone:</b>	650-857-1501
<b>Web:</b>	<a href="http://www.hp.com">www.hp.com</a>
<b>Supported Devices:</b>	HP enterprise-class networked LaserJet devices, select LaserJet flow devices, select HP OfficeJet Pro devices, select HP FutureSmart devices. (Current list can be found at <a href="http://www.hp.com/go/securitymanager">www.hp.com/go/securitymanager</a> .)
<b>Server Requirements:</b>	2.33-GHz dual core CPU; 3-GB RAM (32-bit systems) or 4-GB RAM (64-bit systems); 4-GB hard drive space; Microsoft Windows Server 2008, Server 2008 R2, Server 2012, Server 2012 R2, VMWare ESX/ESXi 4.0
<b>Database Support:</b>	Microsoft SQL Server 2008 R2, Microsoft SQL Server 2008 R2 Express (bundled with HP Security Manager), Microsoft SQL Server 2012, Microsoft SQL Server 2012 Express
<b>Client Requirements:</b>	1.8-GHz CPU; 2-GB RAM (32-bit systems) or 4-GB RAM (64-bit systems); Microsoft Windows Vista, Windows 7, Windows 8.x
<b>List Price:</b>	Server software and device licenses for 50 devices is \$800; for 250 devices is \$3,500; for 1,000 devices is \$12,000; and for 5,000 devices is \$50,000
<b>Availability:</b>	HP JetAdvantage Security Manager is available from HP authorized resellers and directly from HP worldwide, including in the Americas, Europe, the Middle East, Africa, Japan, and Asia-Pacific. The utility and its documentation are provided in English.



## Features and Productivity

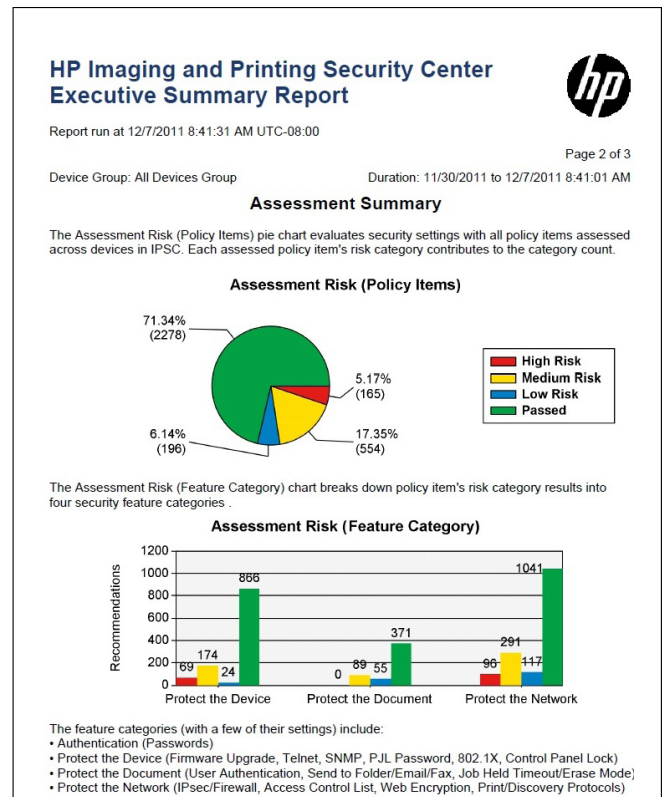
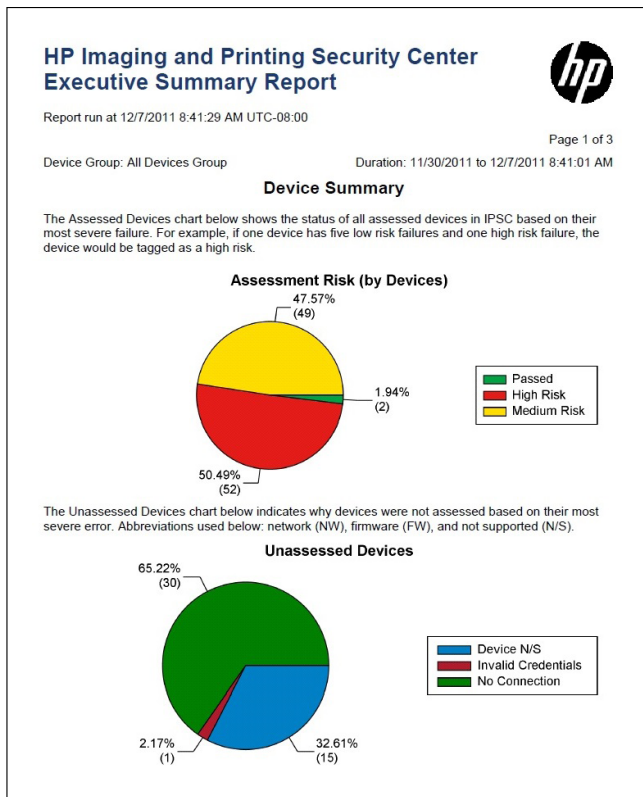


The trailblazer in an all-new class of management utilities, HP Security Manager offers features not found in the traditional device management platform—nor in other products BLI has evaluated. Features are centered around security policy creation, initial device assessment and ongoing monitoring, and remediation to keep devices in line with set policies.

For the creation of security policies for imaging devices, HP Security Manager delivers an embedded “best practice” template, based on the HP Best Practices Security Checklist as well as the U.S. National Institute of Standards and Technology. This template contains the recommended configuration for a device’s core security settings related to authentication, print and sending functions, networking and communications parameters (including NFC and Wireless Direct settings), and so on. The baseline template can then be customized to fit an organization’s particular use case. Even better, administrators do not need to be experts in security before tweaking settings: the Policy Editor used to make changes will warn the administrator if a particular change brings the proposed policy out of compliance with best practices or if that change conflicts with an interrelated security setting. The feature is like a built-in security consultant that helps keep administrators from creating policies that are invalid.

Once policies are set, HP Security Manager offers assessment features that check devices on the network to see if they are in or out of compliance with the policies. Checks can be run manually at any time (for example, as a new device is added) or can be scheduled to run automatically in the background at set intervals. HP Security Manager’s assessment reports will flag items that need attention, and the handy reports also show high-risk devices that need attention immediately.

Perhaps the most welcome features will be the program’s automated assessment and remediation tools. An assessment can be set to run at desired intervals (daily, weekly, monthly) to check all registered devices to see if they are in compliance with their assigned policies. The administrator can select whether to simply run an assessment and report the results, or to run an assessment and have HP Security Manager perform any required remediation automatically (that is, change device settings remotely to bring devices back into compliance with the assigned policy; the program will show on the report any errors that cannot be changed remotely). Conveniently, HP Security Manager leverages the HP Instant-On Security feature of the company’s enterprise-class devices. When added to the network or rebooted, such devices automatically announce themselves to the HP Security Manager server and security settings are changed to match the customer-defined policy—resulting in out of box security with no additional IT overhead.



The Executive Summary Report presents an at-a-glance view of fleet security.

HP Security Manager also handles certificate management. Certificates help protect the flow of information to and from networked devices. They are used to prove the identity of a device and encrypt data, enabling secure communication between trustworthy entities. But manually installing unique certificates on output devices can be a laborious and time-consuming task—up to 15 minutes per device—which keeps many enterprises from utilizing them. HP Security Manager's latest innovation, introduced with v2.1, streamlines this process by deploying unique identity certificates across a customer's fleet, continuously monitoring those certificates to ensure they remain valid, and automatically replacing revoked or expired certificates.

As for other features, HP Security Manager includes several reports to keep administrators informed about the state of devices and keep record of compliance for audit purposes. An Executive Summary report shows a top-level view of the current state of an organization's system, showing for the device group selected an assessment risk by device, devices that are unassessed, assessment risk by policy item, assessment risk by feature category, and a risk summary. The administrator can also see detailed reports by device group and drill down to the feature level of devices, including Assessed (which lists all of the assessed devices), Recommendations (lists all devices that have at least one recommended remediation required), Remediated (lists all of the remediated devices) and Unassessed (lists all of the devices that could not be assessed). In the Policy Item View, users can run a Fleet Assessment Summary (which summarizes the number of recommendations for a

particular policy item, and its risk in a security category) and a Policies report that lists all of the current security policies an administrator has in force.

While there is some overlap with HP WJA, the company's excellent device management tool, HP Security Manager's features complement WJA and do not aim to replace it. The difference is one of scope: Security Manager is intended to be used in the background as a security settings compliance monitoring tool, which can change settings when needed to enforce compliance. WJA is designed for day-to-day management of all aspects of a print fleet. For example, with WJA, administrators would actively control device credentials and passwords, disk erase functions, settings for Jetdirect print servers, access to MFP functions (such as digital sending) and so on. Security Manager, by contrast, is intended to keep devices in compliance with overarching security policies. Indeed, in large enterprises, the target user of the two utilities might be different: the Security Administrator (Security Manager) versus the Print Administrator (WJA).



## Value



HP Security Manager is priced according to the number of devices to be monitored, with four price tiers. The price for server software and device licenses for 50 devices is \$800; for 250 devices is \$3,500; for 1,000 devices is \$12,000; and for 5,000 devices is \$50,000. The licenses are perpetual and are not tied to a particular device, so if one monitored device is retired from the fleet, its replacement (if compatible) can be counted in the existing license. For tech support, HP JetAdvantage Security Manager requires the customer to purchase an HP Care Pack Service agreement (available in 1-year or 3-year terms); fees are based upon the product tier the customer has purchased.

BLI feels this pricing structure and the per-device license fees are very fair. All told, HP Security Manager represents an excellent value, since it delivers time-saving functionality unavailable elsewhere—and does so at a very reasonable cost.



## Administration

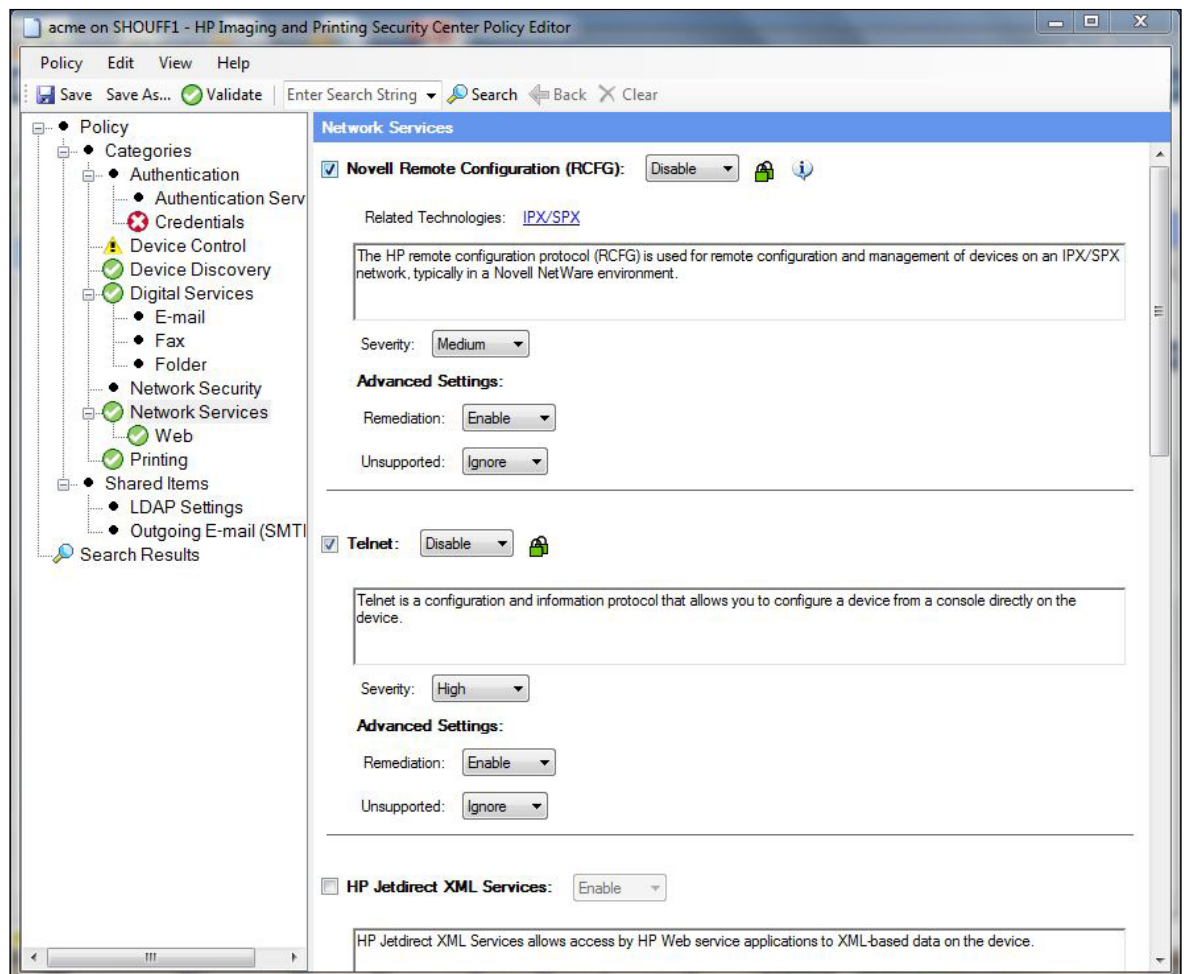


HP Security Manager is easy to install, and could be done by a customer's IT administrator, HP services, or a certified reseller. The installation package includes Microsoft SQL Server Express 2008 R2 Express to use as the database, or the solution can be pointed to an existing SQL database if the customer prefers. For monitoring thousands of devices, HP recommends the more robust Microsoft SQL Server as the database. Initial setup, consists of installing device licenses and adding devices to the system. This can be done by directly entering device IP addresses into HP



Security Manager; importing them via a text or XML file, or from a Web Jetadmin database; or discovering and adding them via the Instant-On Security feature of select HP devices.

Once devices are in the database, they can be added to groups for more streamlined monitoring and policy enforcement. Devices can be grouped by device model, capabilities (such as MFP and printer-only), location, department—whatever groupings make sense for the customer's environment—and devices can belong to more than one group.



The heart of the system is the policy editor, which walks an administrator through devising correct security setting templates.

Administering the system on an ongoing basis is made surprisingly easy thanks to the client program's intuitive layout and handy templates and policy editor. For example, the "home page" features a flowchart showing steps that an administrator might need to complete, such as adding devices or setting policies. And as noted earlier, the administration console is designed for use by an IT pro who is familiar with administering print environments, but who is not necessarily a security expert.

To that end, HP built intelligence into HP Security Manager to identify possible conflicts, linkages and potential unintended consequences: “If changing this, you might want to think about changing that.” For example, if the administrator elects to disable the Novell IPX/SPX stack, the program links to and disables the Novell RCFG stack, too, which the administrator might have otherwise overlooked.

After adding devices, the next step is to create security policies for the registered devices. Clicking on Policy opens a screen where the administrator can start with a blank policy (which can be rather intimidating, given the number of parameters available to set), open an existing policy to edit, or (even better) select the prefilled HP Best Practices Base Policy as a starting point and change that as needed. Conveniently, valid policies can be exported and then imported into a compatible version of HP Security Manager, so a reseller can have a library of common policy templates to use as starting points.

Once a policy (or policy template) is selected, a tree hierarchy in the left column of the policy editor shows all the security settings available, divided into logical groups. The administrator can then browse through those category groups, or use the search field to jump directly to a particular setting (such as “AppleTalk”). As the administrator makes changes to settings, icons indicate if the elected change is a sound choice from a security standpoint or not. A green padlock indicates that a given setting is the recommended one, a yellow padlock shows that there is a more secure setting choice available, while a red padlock indicates that the program has a recommendation for a more secure policy. The policy editor will also display other icons to guide the administrator through changes. For example, a green check indicates that all of the entries in the particular category are valid, a yellow caution triangle indicates that there are one or more items that might cause issues on some devices or in certain situations, a red x flags that information is missing from the category,.

Once a policy is created, the program’s validation feature checks the policy and flags potential problems with the desired settings. HP Security Manager will also show a policy validation error when selected settings are incomplete or incorrect. Ultimately, however, control rests with the administrator, and if a desired setting is unsupported, the administrator can tell the program to ignore it so it is not continually reported as a policy error in future reports.

Should an administrator need help along the way, HP Security Manager offers excellent documentation. In addition to the embedded help content, there is a 36-page Installation and Setup Guide and a separate 52-page user manual. Each is logically organized with clear descriptions and screenshots to illustrate all functions. There’s also an 8-page FAQ document in downloadable PDF format, and various whitepapers on the solution.





## Software Integration



While HP Security Manager is a standalone application, it can import device information from HP's Web Jetadmin if that device management utility is in use on the network. Beyond that, however, the two utilities are separate. BLI would like to see HP Security Manager more tightly integrated with WJA, so one management interface could be used to manage both the devices and their security settings.



## Customer Support and Training



HP Security Manager is designed for customers to utilize without extensive training. HP or the reseller placing the system can train the administrator or other IT personnel on how to use the utility as part of the deployment under a professional services agreement. Documents such as the Install Guide, Users Guide, and whitepapers are available resources for customers at [www.hp.com/go/securitymanager](http://www.hp.com/go/securitymanager). If needed, HP authorized resellers or HP Professional Services may provide additional onsite training or consulting to customers upon request, for a fee.

For tech support, HP JetAdvantage Security Manager requires the customer to purchase an HP Care Pack Service agreement (available in 1-year or 3-year terms); fees are based upon the product tier the customer has purchased. This Care Pack entitles the customer to maintenance upgrades and technical phone support, which is available on business days from 8:00 a.m. to 5:00 p.m. local time (call centers are located in North America, Western Europe and Singapore). Notably, support lines are staffed by dedicated engineers who are familiar with HP management tools.

### BUYERS LABORATORY LLC • North America • Europe • Asia

Gerry Stoia, CEO  
Anthony F. Polifrone,  
Managing Director  
Gerry O'Rourke, Managing  
Director, BLI International  
Patti Clyne,  
Senior VP of Sales  
Daria Hoffman,  
Managing Editor  
Dr. Simon Plumtree,  
European Managing Editor

Tracie Hines, Senior Editor,  
Competitive Analysis Reports  
Jamie Bsales,  
Senior Product Editor, Solutions  
George Mikolay,  
Senior Product Editor, A3 MFPs  
Marlene Orr, Senior Analyst,  
Printers and A4 MFPs  
Lisa Reider, Senior  
Product Editor, Scanners  
and Environmental

Carl Schell, Senior Writer  
Priya Gohil, Senior Editor  
Kaitlin Pendagast,  
Research Editor  
David Sweetnam,  
Head of European Research  
and Lab Services  
Pete Emory, Director of  
Laboratory Operations

Martin Soane,  
European Lab Manager  
Pia Beddages, Manager  
of Competitive Services  
Anthony Marchesini,  
IT Director  
T.R. Patrick, Art Director