KEYPOINT INTELLIGENCE | Buyers Lab

SERVICE AREA:

Security Testing

ANALYSIS

PRIVATE TEST REPORT

PRINTER & MFP SECURITY VALIDATION TESTING: POLICY COMPLIANCE

JULY 2020

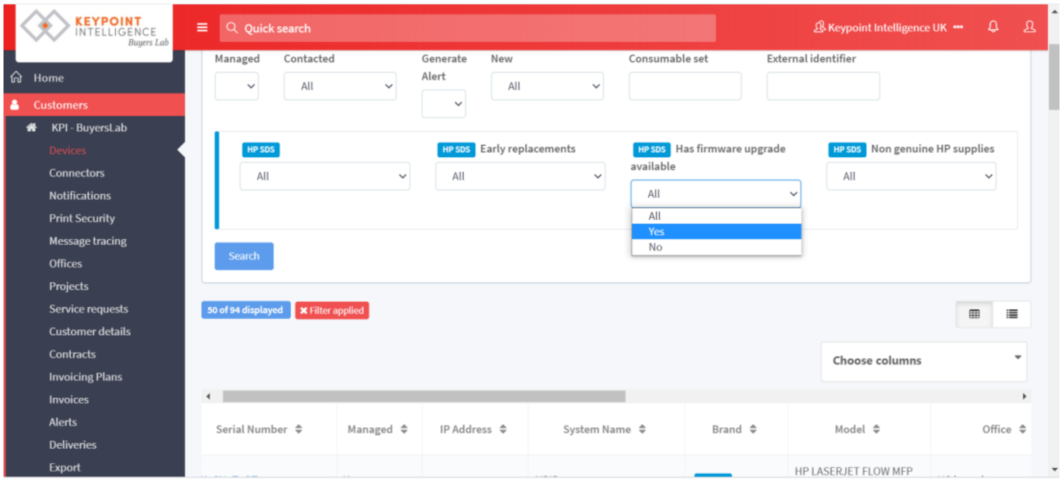
Executive Summary

For this report, Keypoint Intelligence-Buyers Lab was commissioned by MPS Monitor, s.r.l. to conduct validation testing to determine if the company's MPS Monitor 2.0 platform—when used in conjunction with compatible devices—satisfied the functional requirements put forward in Buyers Lab's Printer & MFP Security Validation Testing: Policy Compliance test methodology [July 2020 revision].

Key Findings

Through a combination of hands-on testing by Buyers Lab software technicians and real-time observation of demonstrated functionality by MPS Monitor personnel, Buyers Lab analysts verified the claimed features and effectiveness of the MPS Monitor 2.0 platform in satisfying the test methodology criteria indicated below, when used to manage HP Inc. printers and MFPs fully supported by the HP SDS platform:

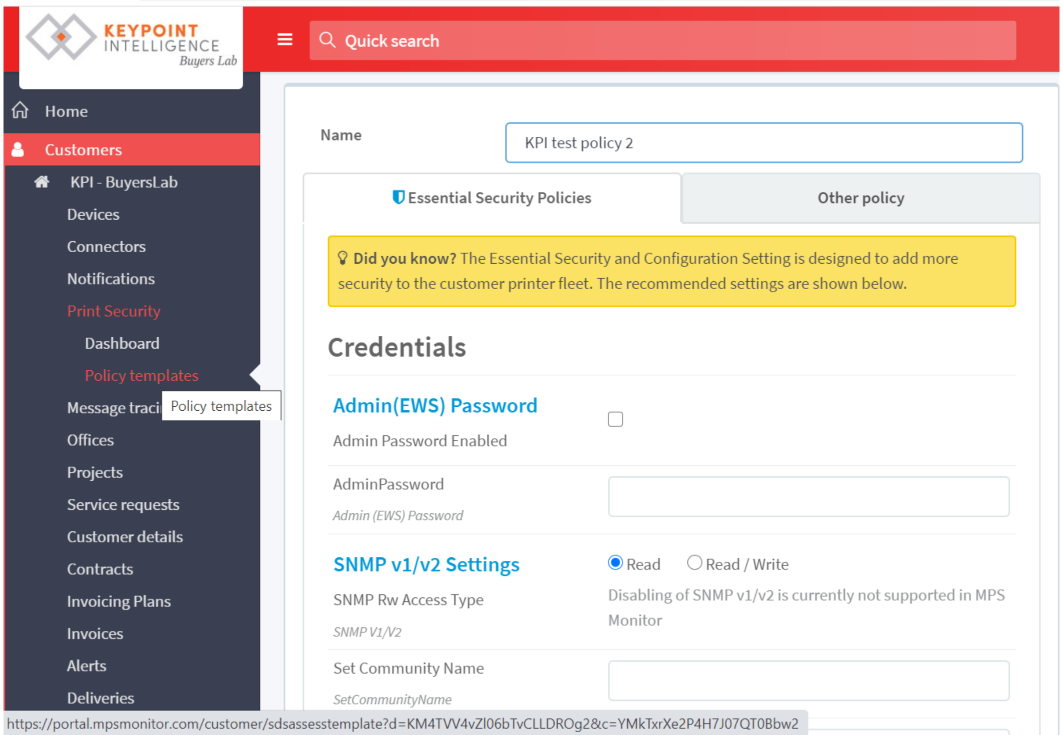
- Discover and highlight at-risk firmware (that is, out-of-date firmware with known and/or likely vulnerabilities) that are still in use on devices
  - ✓ Confirmed: Devices | Show Filters | Has firmware upgrade available filed set to "Yes"
  - ▪ Recommended improvement: Add "Firmware update available" choice to the Notifications | Create notification | Notification type" functionality



Identify models with a firmware update available

- Provide fleet-scalable, secure firmware update capability
  - ✓ Confirmed. Batch Operations | Firmware update. Select devices, enter a scheduled time

- Ensure a customer's devices are secured to a vendor's and/or customer's recommended settings (via templates, policies, or similar mechanism)
  - ✓ Confirmed: Select a customer, then Print Security | Dashboard (or Policy templates) | Select an existing policy template to edit or click on "+ Create new" button to create a new template



Name: KPI test policy 2

Did you know? The Essential Security and Configuration Setting is designed to add more security to the customer printer fleet. The recommended settings are shown below.

Credentials

Admin(EWS) Password
Admin Password Enabled ☐

AdminPassword
Admin (EWS) Password

SNMP v1/v2 Settings
SNMP Rw Access Type ● Read ○ Read / Write
SNMP V1/V2
Disabling of SNMP v1/v2 is currently not supported in MPS Monitor

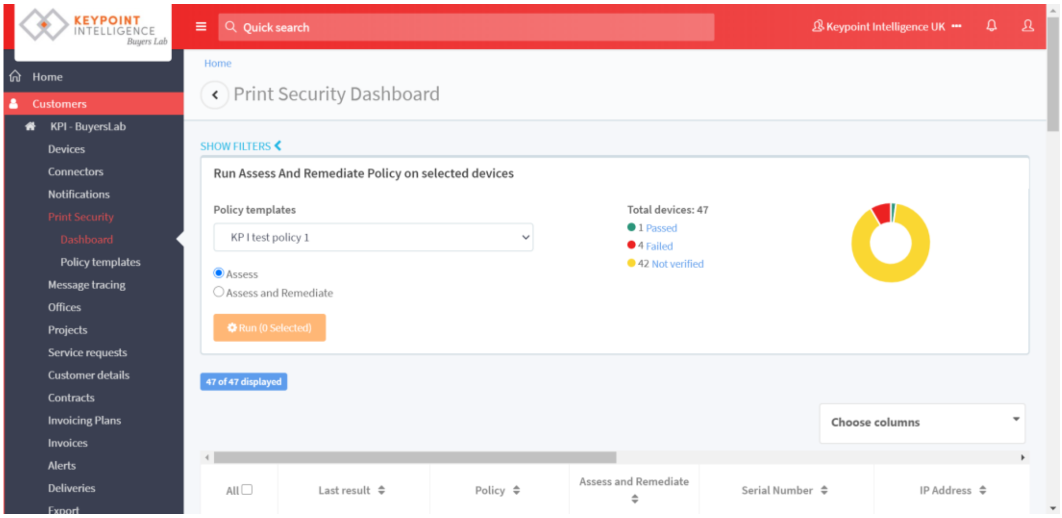
Set Community Name
SetCommunityName

https://portal.mpsmonitor.com/customer/sdsassesstemplate?d=KM4TVV4vZI06bTvCLLDROg2&c=YMkTxrXe2P4H7J07QT0Bbw2

Create, edit, and save security-settings templates

- Provide a method to discover out-of-compliance devices
  - ✓ Confirmed: Customer | Print Security | Dashboard | select "Assess" or "Assess and Remediate" and then Run

- Generate a report (or dashboard view) showing at-risk devices
  - ✓ Confirmed: Customer | Print Security | Dashboard shows Passes/Failed/Not Verified devices (after an assessment has been run)



Print Security Dashboard

Run Assess And Remediate Policy on selected devices

Policy templates: KP I test policy 1

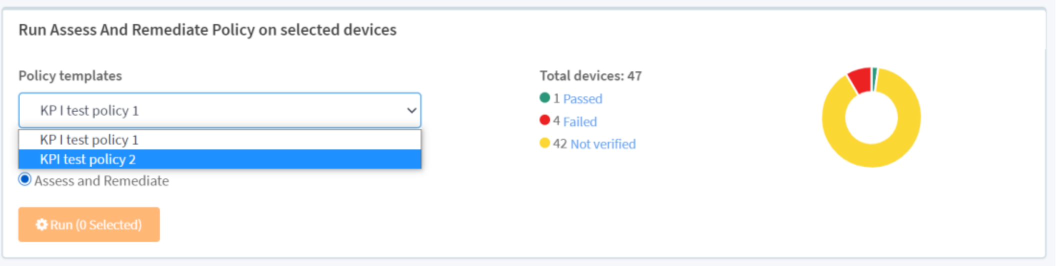
● Assess
○ Assess and Remediate

Total devices: 47
● 1 Passed
● 4 Failed
● 42 Not verified

All □	Last result	Policy	Assess and Remediate	Serial Number	IP Address

Dashboard shows at-risk devices that are out of compliance with a security policy

- Provide a way to automatically apply the desired settings to bring devices back into compliance
  - ✓ Confirmed: Customer | Print Security | Dashboard | in the “Run Assess and Remediate Policy on selected devices, select the template from the Policy Templates drop-down menu, select the Assess and Remediate radio button and click the Run button.



Run Assess And Remediate Policy on selected devices

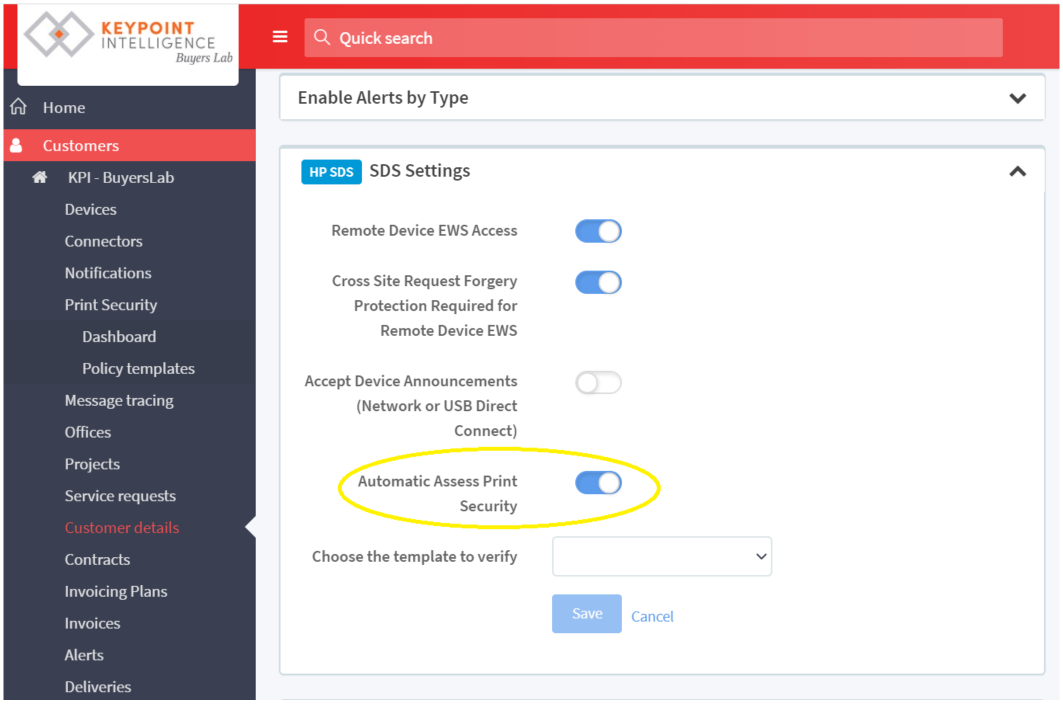
Policy templates: KP I test policy 1
KP I test policy 1
KPI test policy 2

● Assess and Remediate

Total devices: 47
● 1 Passed
● 4 Failed
● 42 Not verified

Assess and remediate task applies the desired policy to selected devices

- Provide on-going checks to ensure the devices are still in compliance with the recommended settings
  - ✓ Confirmed: Customer | Customer details | SDS Settings | set “Automatically Assess Print Security” slider to “on”



Enable Alerts by Type

HP SDS SDS Settings

Remote Device EWS Access	☑
Cross Site Request Forgery Protection Required for Remote Device EWS	☑
Accept Device Announcements (Network or USB Direct Connect)	□
Automatic Assess Print Security	☑
Choose the template to verify	

Automatically run security-assessment checks to find devices that are out of compliance

- Automatically detect newly connected but un-configured device(s) attached to the network and automatically apply the policy designated by the administer for new devices
  - ✓ Confirmed: The platform can be set to run the Assess and Remediate task automatically after a Discovery task has run, and apply a default policy to newly discovered devices.
  - ▪ NOTE: MPS Monitor reports that it has opted to disable this capability in the platform's default configuration. The decision as to whether or not to implement the feature is a decision left to MPS Monitor customers.

With the validation of the functionality checked above, the MPS Monitor 2.0 platform has earned the *BLI Security Validation Testing: Policy Compliance* seal, which applies to the tested product for the period commencing July 31, 2020, and ending August 1, 2022. (Use of the seal by MPS Monitor s.r.l., if licensed, is governed by the conditions stipulated in the separate licensing agreement.)

authors

Jamie Bsales

Director, Solutions & Security Analysis

jamie.bsales@keypointintelligence.com

✉

Jamie Bsales is an award-winning technology journalist who has been covering the high-tech industry for more than 25 years, 12 of those at Buyers Lab and Keypoint Intelligence. In his role as Director, Solutions& Security Analysis, Jamie is responsible for Keypoint Intelligence's coverage of document imaging software, security, and related services.