HP JETADVANTAGE SECURITY MANAGER

Frequently Asked Questions

CONTENTS

INTRODUCTION

This document provides answers to frequently asked questions about HP JetAdvantage Security Manager.

POLICY

Q. If I use the HP Best Practices Base Policy template and its default settings, will my printing and imaging devices be completely secure?

A. No. The HP Best Practices Base Policy template provides a great place to start when creating a custom policy or when used as a baseline policy. The default settings in this template are based on NIST guidelines, but do not represent complete security for your devices. HP understands that the device security requirements for each customer might differ and offers the most common NIST settings as a starting point for developing your custom or baseline policy.

Q. Will any of my third party device solutions be affected by adopting the HP Best Practices Base Policy as is?

A. Possibly. When used with third-party solutions requiring access to the device, the HP Best Practices Policy template might require changes to the default security settings. Refer to your solution documentation to determine whether policy changes are required to accommodate specific functionality. For some third party solutions, the **Command Load & Execute** and **Allow PJL** settings might require enabling. Another known setting that should be enabled for solutions to function properly is the **Legacy Firmware Upgrade** so firmware can be signed with SHA-1 for solutions use.

Q. Should I export my policies?

A. You might export policies for the following reasons:

- To back them up for possible restoration later
- To use for importing into another Security Manager server in your corporation

Q. What is the best way to use the Enter Search String field when creating or editing a policy?

A. Use this field to quickly locate a particular setting instead of browsing the setting categories. For example, a search for **Apple** displays the **Apple Bonjour** and **Appletalk** setting links. Also use this field to quickly view related technologies for a setting of interest. For example, a search for **Fax** displays **Digital Send, Fax PIN, Fax Speed Dial Lock, Send to Fax** and **User Authentication**.

Q. Why does a warning icon appear next to one of my policy setting categories after successful validation?

A. A policy can be reviewed and saved as valid with pending policy suggestions. Although not recommended, you can ignore the policy suggestions. For example, if you enable a file system access protocol without enabling the check for a file system access password, this policy is valid, but contains a warning icon next to the policy setting category.

Q. Why can't I enable remediation of Password settings in the Password category?

A. Security Manager can assess a device to see if passwords are configured, but cannot configure the appropriate password. HP is committed to addressing this limitation in a future release. In the interim, use Web Jetadmin or the device EWS to set passwords.

DEVICES

Q. At what point in the add devices process is my device actually added to the database?

A. The device is added to the database after you have input an IP address or imported a device list and selected **OK**. Prior to this, the addresses displayed in the window are not in the database nor do they have a license assigned. You can use this step in the add devices process to clean up a device list before adding to the database and assigning a node license.

Q. When selecting Verify, what information is gathered from the device and how?

A. The verify process uses the SNMP and HTTP protocols to gather pertinent device information, such as model name, serial number, firmware versions, and credentials. Additional information, such as assessment status, date assessed, and policy name, is gathered from the Security Manager database if it already exists. After a verify, the following information can be displayed and filtered in the devices window: assessment status, device status, license status, supported device status, IP address, hostname, model name, device name, date assessed, policy name, recommendations, credential use, credential status, discovered by instant-on, instant-on authorized, serial number, firmware version, network model and network firmware version.

Q. I exported a list of devices from HP Web Jetadmin in xml format. Will all the device related information in this file be imported during the add file process?

A. No. Only the device IP address or the hostname (as device identifier) are imported. HP Security Manager uses the **Resolve IP addresses to hostnames** process and the **Verify** task to update the Security Manager database with current device information.

Q. Why can't I see all of my 2200 devices in the devices window?

A. The devices window displays 1000 devices per page. To see more devices, select **Devices** from the toolbar and advance to the next range of devices.

Q. Why can't I see my filter choices when I right click on the column headings in the devices window?

A. Filters are disabled. Click on the funnel icon in the toolbar. When it changes color to green, filtering is enabled.

Q. Why didn't my node license count increment when I removed 10 devices from my custom group?

A. Even though the devices were removed from your custom group, they are still included in the **All Devices Group** and have a license assigned. Deleting the devices removes them from the database and frees the 10 licenses.

Q. I purchased more licenses to accommodate the additional printers I've added. I've loaded the new license file, but licenses are not automatically assigned to these added devices. How do I assign the new licenses?

A. If devices are added to the Security Manager database before the license file is loaded, they are set to an unlicensed status. To assign licenses, select the unlicensed devices, right-click and select **License**. You can also select **License** from the **Action** menu or simply **License** from the **All Devices Group**.

Q. I've set an EWS credential for my All Devices Group, but use a different credential for 5 high availability printers in this group. How do I set the credentials for these 5 printers in the All Devices Group?

A. Select the 5 devices and right-click for the menu. Select the **Set Credentials** option and set the credentials for the 5 devices.

Q. I've set the appropriate credentials for a custom group. Why am I receiving credential failures for the 5 devices I added to this group?

A. Devices added to a group with credentials already set do not inherit that group's credentials. You must manually set credentials on the 5 devices to match the group's credentials.

Q. My device status displays good, but I have a conflicting green check mark and red x icons. Please explain.

A. When viewing devices, there are two separate icon columns to the left of the device status column. The first icon column is referred to as the **Device Status Icon Column**. **Good, No Information** and **Error** are the potential status icons found in this column. The left most column is referred to as the **Assessment Status column** and includes the assessment status of **Passed, High Risk, Medium Risk, Low Risk** or **Not Assessed**. In the scenario above, the device has been verified for good communication and credentials (the green check mark), but assessed with at least one high risk policy setting that is out of compliance (the red x).

ASSESS & REMEDIATE

Q. Why can't I select the Assess and Remediate option in the toolbar of the Policy or Task windows?

A. There is a global device remediation setting found in the File -> Settings -> General window that disables all device remediation. When disabled, **Assess Only** is your only option. Enabling remediation at this global level allows you to select **Assess and Remediate** from the **Policies** and **Tasks** windows.

Q. I have benchmarked the performance of an Assess Only across my fleet of devices. What is the relative performance I can expect when I Assess and Remediate?

A. This depends on how much remediation is required per device, but a good guideline to follow is double the time for an assess only. This is a rough estimate and is based upon every assessed setting being out of compliance with your policy.

Q. Why won't one of my policy settings remediate?

A. Within the policy editor, an individual setting can be configured not to remediate and is most likely the cause. Open the suspect policy and select the setting that is not remediating. Make sure **Advanced Policy Settings** is selected in the view. Now, change the **Remediation** setting from **Disable** to **Enable**. If this is not the issue, then you are experiencing the proper behavior of a setting that, by design, cannot be remediated.

Q. Must I create a new task every time I want to Assess or Assess and Remediate?

A. No. There are several ways to create a new task. You can select a completed task from the **Tasks** window, right click and select **Restart**, if it is a task you want to repeat. Or, you can select a completed task, right click and edit the parameters you desire. Or, schedule the task to reoccur at a daily, weekly or monthly interval.

Q. What is the primary value of an Assess Only?

A. Performing an **Assess Only** allows you to validate the comprehensiveness of a newly created policy before remediating any out of compliance devices. **Assess Only** reports security compliance recommendations on each device assessed, which allows you to adjust the policy, if required. Once you are comfortable with your new policy, switching to **Assess & Remediate** keeps your assessed fleet compliant with that policy.

Q. After an assessment, I sometimes see a Device Error in the device recommendations. What does this error indicate?

A. Recommendations are based on the gathering of a device's setting information via an assortment of network protocols and specific ports. If Security Manager is unable to gather this information using a specific protocol in the appropriate amount of time, a Device Error is posted for that particular setting.

REPORTS

Q. Why does the Executive Summary Report show an Assessment Risk By Device pie chart with 100% High Risk?

A. This indicates that you have at least one high risk setting out of security policy compliance for every device you assessed.

Q. Does the Executive Summary Report only include Device Summary pie charts?

A. No. The **Executive Summary Report** actually includes three pages of information. Use the page advance at the top of the page to view the additional information. The additional reports are **Assessment Risk by Policy Item**, **Categorization of Risk**, and **Risk Calculations**.

Q. On the Risk Summary page of the Executive Summary Report how is the Worst Case Risk total calculated?

A. The policy used in an assessment includes enabled settings with a user assigned severity. The severity choices are high, medium, or low risk. The calculation of Worst Case risk is the total number of like severity settings in the policy, multiplied by the number of devices assessed and multiplied again by the specific risk factor multiplier. For example; a policy might have 3 high risk settings and the policy will be used to assess 3 devices. This is a potential for 9 high risk settings to be assessed as out-of-compliance with the policy applied. Utilizing the risk factor multiplier of 10 calculates to be a worst case risk of 90.

Q. Can I save reports?

A. Yes, reports can be saved as an Excel or PDF file and archived for historical purposes.

Q. Can I generate a report from a previous period of time?

A. The **Devices Change Details Report** is the only report that provides historical data. However, this historical data is limited to device remediation only. By executing the **Devices Assessed Report** and viewing the changes column, you are presented with device remediation tracking over time. The time range can be adjusted using the **Report Duration** selection, located on the toolbar. In this report, on a per device basis, you will see the remediated setting, the old value, the new value, date and time remediated, and the policy the setting was remediated against.

Q. My reports always provide information for all devices. How can I produce reports on a filtered set of devices?

A. From the **Reports** tab, you can filter devices by selecting a specific group from the **Reports, Executive Summary**, and **Detailed Reports** selections in the left-hand navigation menu. By selecting any of these report options, you will see a **Select Group** option on the toolbar. Use the **Select Group** option to filter devices before generating a report.

INSTANT-ON SECURITY

Q. To take full advantage of the Instant-On (out-of-the-box) security feature, what is the required Security Manager Server DNS name/alias?

A. hp-print-mgmt

Q. Why don't I see the Announcement Agent status on my device's JetDirect configuration page?

A. Your device might not support this feature or it might not be upgraded to the appropriate 11.3 firmware version. See the Security Manager Release Notes (www.hp.com/go/ipsc) for the actual 11.3 version numbers.

Q. Why does my device's JetDirect configuration page show Announcement Agent failed?

A. This status indicates that the printer did not establish an Instant-On connection with the Security Manager server. Possible reasons for the non-connection status are as follows:

- The Instant-On feature is not enabled on the Security Manager server.
- TCP Port 3329 might be blocked at the Windows firewall or elsewhere.
- The DNS name of hp-print-mgmt could not be resolved by the printer.

Q. How do I associate more than one security policy with the Instant-On security feature?

A. This is not possible. If you require more than one policy to be applied across your fleet, you can create a base security policy and associate it with the Instant-On security feature. Once the device is set in accordance with the base policy, a scheduled assessment and remediation with additional settings from another policy can be applied.

Q. Selecting Mutual Authentication as an Instant-On authentication option nullifies a true out-of-the-box security experience. Why would I use this option for Instant-On?

A. It is true that the Instant-On security feature was designed for a secure out-of-the-box experience. However, its usefulness extends to keeping a device secure after a cold reset. Certificates remain over a cold reset, keeping the device somewhat secure until after Security Manager assesses and remediates.

c03602074ENW, Rev. 2, September 2015