Technical white paper

HP JetAdvantage Security Manager

Automatic Email Notification and Policy Change Notification for Remediation Tasks

Table of Contents

Overview

HP JetAdvantage Security Manager can run unattended scheduled tasks. A user schedules these tasks to occur periodically. The Automation Email feature sends a preconfigured tickler email when an Assessment/Remediation task is complete and when a policy is changed which has been changed since the task ran last time.

Configure the Automated Email feature

The Automation Output feature must be configured before it can be used. Configuration is performed on the Automated Output tab on the global Settings dialog. To access this dialog, go to Settings on the Security Manager client application by clicking on the lines next to the user icon:

After clicking on the icon select the **Settings** menu as shown in next screen
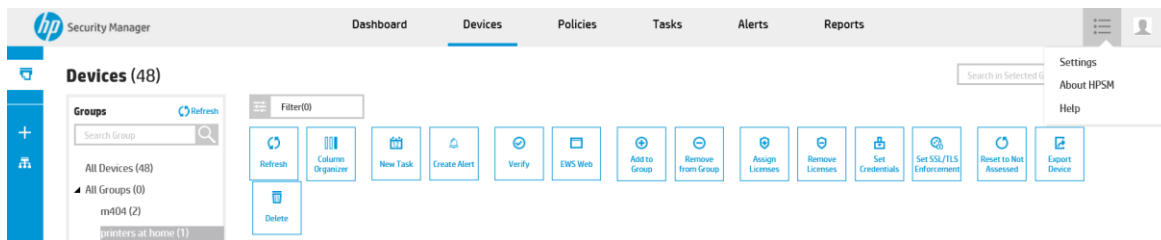
The **Automated Email** settings are used to configure both the **Email Server Settings** used to send the email as well as **Automatic Email Notification Settings**.

Configure the Email Server Settings

The E-mail Settings group contains settings that identify the email server used to send emails and how to authenticate if required. These settings include the following:

SMTP Server—The hostname or IP address of the email server.

Port—The network port used to contact the email server.

Enable SSL—Enables or disables the use of SSL when working with the email server.

Specify Credentials—Specifies if user credentials are required. If selected, the Username, Password, and Domain fields are enabled.

Username—The username used to log in to the SMTP (email) server.

Password—The password used to log in to the SMTP server. This is a password text box, so the characters are hidden as they are entered.

Domain—If the username is related to a domain, the domain is required to qualify the username. This value is optional.

Complete the configuration

All the settings are saved to the database when the **Save** button is clicked.

Configure the Automatic Notification Settings

The settings for the email message include the following:

Email Subject—The subject used in the email.

Recipient(s)—One or more recipient email addresses. If more than one address is specified, they must be separated by a space, comma, or semicolon.

From Address—The email address used for the sender in the email.

Send Test Email - A test email can be sent by clicking the Send Test E-mail button. This might take a second or two to complete.

Complete the configuration

All the settings are saved to the database when the **Save** button is clicked.

Automated Emails

Automated Emails can be generated for remediation tasks (called Assess and Remediate) and for Policy Change Notification.

Assessment/Remediate notifications

Automation Emails are supported for Assess and Remediate tasks (not for Assess Only tasks). These tasks can be scheduled when creating a New Task

If the **Email Results** checkbox is selected, an email will be sent when the task completes. This checkbox is visible only if the following occur:

A valid SMTP server name is entered in the global Settings dialog.

The task type is Assess and Remediate.

Policy Change Notification

The default audit logging will log when a user has changed a policy. However, in order to detect this change, the HPSM administrator will have to go through the HPSM_WebAudit.log (see HP JetAdvantage Security Manager – Reporting, Email Alert Subscriptions & Remediation Summary, Auditing & Syslog Functionality) in order to detect this. This is very cumbersome, while it's very important to know when a policy has been changed which is used in a re-occuring task. To simplify this policy change notification was added in HPSM 3.4: when a task is running and it's using a policy which has been changes since the task ran last time, then HPSM will report this. When enabled, this reporting is done in the following ways:

- An event is logged in the windows event log
- A report is created and stored in the directory

    ```
    C:\Program Files (x86)\HP JetAdvantage Security Manager\Reports
    ```

- Optional: An email will be send out an email to the configured email recipients and the email will have the Report attached. The Email Recipients have to be configured under Settings, Automated Email. See Appendix A for details.

Example of Policy Change Notification for a policy setting which was removed from the policy:

Example of a Policy Change Notification for a policy setting which had been configured with a different value:

Enabling/Disabling Policy Change Notification

In HPSM 3.5 this functionality is disabled by default. This can be enabled by updating the following entries in HPSM service configuration file (HPSM_service.exe.config) to false:

```
<!-- Enable/Disable Policy Change Notification-->
<add key="enablePolicyChangeNotification" value="false" />
<add key="emailPolicyChangeNotification" value="false" />
```

After making the changes the HP Jetadvantage Security Manager service will have to be restarted.

The option enablePolicyChangeNotification enables/disables the Policy Change Notification, the event viewer entries and the pdf files in the Reports directory. On top of that the emailPolicyChangeNotification can be enabled (set to true). The email Policy Change Notifications will only occur if both options are set to true.

Contents of the email message

The email message is intended to be a tickler to remind an administrator that a remediation ran or that a policy which is used in a scheduled task has been changed. These message, like all emails, typically go over the network in clear text, so only minimal information is included in the email. The email contains Task Details (task name, policy name, and device group) and Assessment & Remediation Results.

Sample Email Notification

The email can list the following under the **Assessment & Remediation Results** heading:

X Device(s) were unassessed, of these:

  X1– No Information

  X2– Network Connection Error

  X3– Device(s) Not Supported

  X4– Connection Refused

  X5– Credentials Failed

  X6– Device(s) Not Authorized

  X7– License Required for Assessment

  X8– Hostname Resolution Error

  X9– General Error

  X10– Good

Y Device(s) with Low Risk Issues remaining

Z Devices(s) with Medium Risk Issues remaining

W Device(s) with High Risk Issues remaining

If X,Y or Z is zero, then the corresponding line will not be displayed.