Extended EMail Action Plugin

Overview

This plugin provides more flexibility when it comes to sending email action alerts. You have full control over the email message that gets send and can also specify additional filtering options e.g: just send the email when the Incident comes from a specific agent or server

Plugin Details

Author	Eugene Turetsky (Eugene.Turetsky@dynatrace.com)
dynaTrace Versions	6.1+
License	dynaTrace BSD
Support	Not Supported
Known Problems	

Release History	2013-07-05 Initial Release 0.9.5, 2013-08-07 Release 0.9.6 2013-10-10 Release 0.9.7 2013-12-27 Release 0.9.8 2014-02-26 Release 0.9.9.5 2014-07-01 Release 0.9.9.6 2014-07-22 Release 0.9.9.7 2014-09-16 Release 0.9.9.8 - 0.9.9.12 2014-10-10 Release 0.9.9.13 2014-10-27 Release 0.9.9.14 2014-11-18 Added Java utility to verify correctness of Emails-Filters Dependency File 2014-12-28 Release 0.9.9.18 2015-04-19 Release 0.9.9.19 2015-04-29 Release 0.9.9.20 2015-05-20 Release 0.9.9.21 2015-09-06 Release 0.9.10 2015-10-01 Release 0.10.0 2015-11-17 Release 0.10.1 2015-12-04 Release 0.10.2 2015-12-20 Release 0.10.3 2015-12-29 Release 0.10.4 2016-01-03 Release 0.10.5 2016-04-24 Release 0.10.6 2016-07-09 Release 0.10.7 2016-10-09 Release 0.10.8 2016-10-13 Release 0.10.9 2016-11-16 Release 0.10.10 2016-11-21 Release 0.10.11 2016-12-06 Release 0.10.12 2017-01-16 Release 0.10.13
Download	com.dynatrace.diagnostics.plugins.extendedmailreport_0.10.13.jar

New in the Release 0.10.13

Improved plugin logging.

New in the Release 0.10.12

Added new predefined runtime variables PURE_PATH_N, where N = 1, 2, 3, 4, 5, ... up to 100. The ${DYNATRACE_INCIDENTS} runtime variable contains full list of the affected PurePaths.

New in the Release 0.10.11

Fixed issue with e-mail attachments which was introduced in the release 0.10.8 of the plugin.

New in the Release 0.10.10

Rounded off to the two decimal points values of the ${VIOLATED_TRIGGER_VALUE} and ${VIOLATED_MEASURE_VALUE} runtime variables.

New in the Release 0.10.9

Added ability to use filters by application in the Emails-Filters Dependency file. See example of the XML file here. The matching XSD schema file is located here. Plugin internally validates XML file using this schema. Please use the following link to validate correctness of the XML file outside of the plugin: XML-validation-link.

New in the Release 0.10.8

Added new ${DYNATRACE_INCIDENTS} runtime variable which represents array of DT incidents and their subsequent violations with triggered values in JSON format. For details, please see next screenshots and correspondent files example-1-json-output.log and example-2-json-output.log:

New in the Release 0.10.7

Replaced old Dynatrace logo to a new one that matches to Dynatrace 6.3.

Added missing semicolon separator in the VIOLATED_MEASURE_NAME_ALL variable.

New in the Release 0.10.6

Added new parameter - 'dynaTrace Server REST Protocol'. Its values are 'HTTP' or 'HTTPS'. Value of the 'dynaTrace Server REST Port' parameter should match to the chosen value of the 'dynaTrace Server REST Protocol' parameter. Default value is 'HTTP'.

Fixed messages for measures with different units.

New in the Release 0.10.5

Fixed backward compatibility issue with older releases of the plugin.

New in the Release 0.10.4

Added ability to set quiet time intervals using the following three formats depicted below. These formats can be used equally in the “Quiet Time From/To” plugin configuration parameters or in the <from></from>/<to></to> tags of the plugin Emails-Filters Dependency File. They are listed below with examples from the plugin Emails-Filters Dependency File:

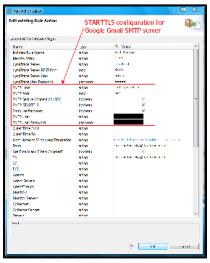
1. **“HH:mm”** - this means that quiet time is every day from HH:mm to HH:mm (implemented already).
   For example:
   <from>8:15;12:00</from>
   <to>9:00;13:00</to>
   Quiet time contains two intervals:
   a. Every day from 8:15 to 9:00
   b. Every day from 12:00 to 13:00.
2. **“<day-name-in-week> HH:mm”** – this means that quiet time is from HH:mm to HH:mm on <day-name-in-week> every week. For

example:
<from>Saturday 8:15; Sunday 12:00; Saturday 6:00</from>
<to>Saturday 9:00; Sunday 13:00; Sunday 18:00</to>
Quiet time contains three intervals:
    a. Every Saturday from 8:15 to every Saturday 9:00
    b. Every Sunday from 12:00 to every Sunday 13:00
    c. Every Saturday from 6:00 to every Sunday 18:00
3. **“MM/dd/YYYY HH:mm”** – this means that quiet time is from HH:mm to HH:mm on MM/dd/YYYY day. For example:
<from>12/26/2015 8:15; 12/27/2015 12:00</from>
<to>12/26/2015 9:00; 12/27/2015 13:00</to>-
Quiet time contains two intervals:
    a. From 8:15 on 12/26/2015 to 9:00 on 12/26/2015
    b. From 12:00 on 12/27/2015 to 13:00 on 12/27/2015

Added new configuration parameter to manage suppression of the Incident Ended notifications. New parameter name is 'Suppress Incident Ended Notification'. If the 'Suppress Incident Ended Notification' parameter is 'true' then if notification e-mail for the 'Incident Started' event was suppressed by one of the quiet time intervals then notification e-mail for the 'Incident Ended' event will be always suppressed by the plugin. If the ' Suppress Incident Ended Notification' parameter is 'false' then notification e-mail for the 'Incident Ended' event will be sent based on the quiet time intervals.

New in the Release 0.10.3

New features include:

1. Added ability to manage multiple quiet time intervals. The "Quiet Time From" and "Quiet Time To" parameters contain semicolon separated "from" and "to" times respectively in the HH:mm format, where "HH" and "mm" are using notations explained in the Date and Time Patterns section here.
   Quiet Time intervals which are set using the "Quiet Time From" and "Quiet Time To" plugin configuration parameters are always applied to all filters which are set in the "Emails-Filters Dependency" file (see next section 2).
2. Added ability to set Quiet Time intervals in filters. Now the "Emails-Filters Dependency" file has optional <quiet_time> tag which contains <from> and <to> values for quiet intervals. Please see example of the quiet time intervals in the XML file here. The matching XSD schema file is located here. Plugin internally validates XML file using this schema.
3. Enhanced support for different communication types between plugin and SMTP mail server:
    a. Now, besides plain text and SMTP over SSL communications, plugin also supports the STARTTLS type of communication. New configuration parameter "SMTP STARTTLS" was added to reflect use of the SMTP STARTTLS communication. When it is 'true' the SMTP STARTTLS communication is used, otherwise this communication type is not used. Below is an example of the STARTTLS communication for Gmail SMTP server:
    
    b. Added ability to use different flavors of SMTP communication settings by utilizing additional SMTP Custom Properties. New parameter "SMTP Custom Properties File" points to the file which contains key and value pairs that will be added by the plugin to the SMTP properties file at run time. Example of the SMTP Custom Properties file is located here.

New in the Release 0.10.2

Improved logging messages.

New in the Release 0.10.1

Improved default formatting of the Infrastructure Alerts incidents.

New in the Release 0.10.0

New features include:

- Added log messages to identify incidents which have no matching filters and hence are not sending notification e-mails.
- Added better management of the log messages.
- Fixed default message in the notification e-mail for the 'Average response time degraded' OOTB incidents.

New in the Release 0.9.10

New features include:

- Added ability to filter by application name. New parameter 'Applications' contains list of semicolon separated filters. Each filter is a Java regular expression.
  Note: if the ${APPLICATION} runtime variable is '-' (dash), plugin will ignore application filters and e-mail will be sent anyway.
- Fixed bug associated with use of the thresholds file for dynamic measures.

New in the Release 0.9.9.21

Added support for international languages.

New in the Release 0.9.9.20

Extended filtering by server name for non-server resource type of incidents.

New in the Release 0.9.9.19

New features include:

- Added EMail Priority parameter which handles priority of a notification e-mail. It has the following values: High, Medium, and Low. Default value is Medium;
- Logo image which is used in the notification e-mails was changed from Compuware to Dynatrace logo.

New in the Release 0.9.9.18

New features include:

- Plugin now supports setting up individual thresholds for the Dynatrace dynamic measures. This mitigates existing limitation of the Dynatrace plugin interface to support individual thresholds for given dynamic measures. New parameter "ThresholdsFile" was added to the plugin configuration parameters. It points to an XML file which contains list of dynamic measures and their respective thresholds. Example of the setting up parameter is here. Example of the XML file is here. Plugin internally verifies correctness of the XML file based on this XSD schema before processing request.
- Plugin now supports filtering by the violated measure names. New parameter "measureNamePatterns" was added to the plugin configuration parameters. It contains semicolon separated list of Java regular expressions, see example here.
- The following new predefined variables are added to the list of maintained by the plugin variables:
  - APPLICATION_ALL,
  - VIOLATED_MEASURE_NAME_ALL,
  - VIOLATED_MEASURE_DESCRIPTION_ALL,
  - VIOLATED_MEASURE_VALUE_ALL,
  - VIOLATED_MEASURE_UNIT_ALL,
  - VIOLATED_MEASURE_SPLITTINGS_ALL,
  - VIOLATED_MEASURE_TRESHOLD_UPPER_SEVERE_ALL,
  - VIOLATED_MEASURE_TRESHOLD_LOWER_SEVERE_ALL,
  - VIOLATED_MEASURE_TRESHOLD_UPPER_WARNING_ALL,
  - VIOLATED_MEASURE_TRESHOLD_LOWER_WARNING_ALL,
  - VIOLATED_MEASURE_METRIC_NAME_ALL,
  - VIOLATED_MEASURE_METRIC_DESCRIPTION_ALL,
  - VIOLATED_MEASURE_METRIC_GROUP_ALL,
  - VIOLATED_MEASURE_METRIC_UNIT_ALL,
  - VIOLATED_TRIGGER_VALUE_SOURCE_TYPE_ALL,
  - VIOLATED_TRIGGER_VALUE_SOURCE_NAME_ALL,
  - VIOLATED_TRIGGER_VALUE_SOURCE_HOST_ALL,
  - VIOLATED_TRIGGER_VALUE_ALL.

  Each variable from the above list contains a semicolon separated respective values (e.g. applications, violated measure names, violated measure descriptions, etc.) which are taken from violations of given incident.

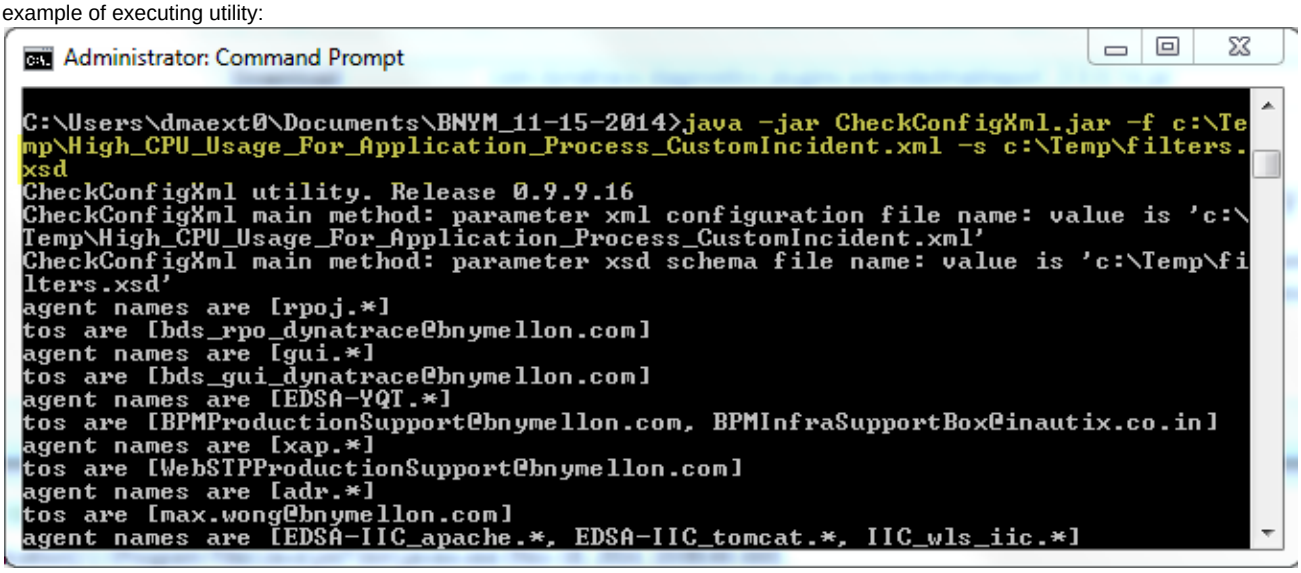
Java utility which verifies correctness of the Email-Filters Dependency File

Standalone Java utility mimic the Extended Mail Action plugin code which processes the Email-Filters Dependency XML files. It checks correctness of the Email-Filters Dependency XML file based on provided XSD schema and plugin's built-in internal rules. Below are few examples of utility usage:

- getting help about utility usage:

```
C:\Users\dmaext0\Documents\BNYM_11-15-2014>java -jar CheckConfigXml.jar -h
CheckConfigXml utility. Release 0.9.9.16
usage: java -jar CheckConfigXml.jar -f <path-to-xml-configuration-file> -s
            <path-to-xsd-schema-file>
 -f <arg>   , where arg is direct path to the xml configuration file
 -h         , will print usage
 -s <arg>   , where arg is direct path to the xsd schema file
```

- example of executing utility:



New in the Release 0.9.9.14

Fixed a filtering issue for agent groups and servers.

New in the Release 0.9.9.13

GA release.

New in the Release 0.9.9.8 - 0.9.9.12

New features include:

- Ability to send notification e-mails to different addresses depending on filters criteria. The list of filters and correspondent e-mails will be provided in the XML file. Please see example of the XML file here. The matching XSD schema file is located here. Plugin internally validates XML file using this schema. Please use the following link to validate correctness of the XML file outside of the plugin: XML-validation-link.
  There are two new parameters which define if filters/e-mails pairs are used by the plugin They are (see the following screenshot):
  - Are Emails and Filters Coupled;
  - Emails-Filters Dependency File.
- Ability to filter by agent names and by server names for the following sources (see the following screenshot for new parameters):
  - Agents;
  - Monitors;
  - Collectors.
- Mitigated issue with excessive invocations of the Action plugin setup/teardown methods by the dynaTrace engine. Two new properties are added to the extendedmailactionplugin.properties file. They are:
  - expireCacheInterval;
  - cleanupInterval.

  These parameters are taken in minutes. The *extendedmailactionplugin.properties* file is located in the 'res' subdirectory of the plugin's jar file. Example of the extendedmailactionplugin.properties file is located here.

  There are two new parameters which are added to the plugin to uniquely identify instance of the action plugin. They are:

  - Incident Rule Name;
  - Identity String.

Please see example of using these parameters here. While the first parameter is required to identify instance of the plugin which is associated with the specific incident rule, the second parameter is optional and only necessary when there are two or more instances of this plugin setup for a given incident rule. The last scenario of having two or more instances of the Extended Mail Action Plugin (as well as any action plugin) for given incident rule is *highly discouraged* if incidents are thrown frequently. If you have need in having multiple instances of the Extended Mail Action Plugin for a given incident rule, and given version of the plugin does not allow you to cover your needs with a single plugin instance, please contact us to provide your use cases. We will make this plugin (or other action plugins) to accommodate your use cases that you will have to configure just one instance of the plugin per incident rule.

- Added new configuration parameter ALL_SERVER_NAMES_CAPS: when it is "true", content of the ${ALL_SERVER_NAMES} environmental variable is in upper case letters, otherwise it is unchanged.

Note

This version of the plugin is a beta version now. It will become a GA release after successful beta testing.

New in the Release 0.9.9.7

Additional filtering of notification e-mails:

- Added new configuration parameter sendOnlyPatterns: it is a semicolon separated list of Java regular expressions. Each regular expression from the sendOnlyPatterns list will be evaluated against the following incident variables:

  - MESSAGE;
  - RULE_DESCRIPTION;
  - VIOLATION_HEADER_1;
  - VIOLATION_MESSAGE_1;
  - VIOLATION_HEADER_2;
  - VIOLATION_MESSAGE_2;
  - VIOLATION_HEADER_3;
  - VIOLATION_MESSAGE_3;
  - VIOLATION_HEADER_4;
  - VIOLATION_MESSAGE_4;
  - VIOLATION_HEADER_5;
  - VIOLATION_MESSAGE_5.

  Notification e-mail will be sent only if match is found in any of the above variables, otherwise notification e-mail will not be sent.

New in the Release 0.9.9.6

Added support for e-mail notifications from the Cloud:

- Added new configuration parameter SmtpUserPassword: when it is on, user name and password must be provided for SMTP mail server.

New in the Release 0.9.9.5

Changes include:

- Removed port from the Agent_Host/Monitor_Host/Collector_Nost/Server_Host for OOTB incidents;
- Improved content of the e-mail body for e-mails in the plain text format;
- Added application name in the Details section of the e-mail body where it is available;
- Use of incident's message in cases where violations have no meaningful content for OOTB incidents.

New in the Release 0.9.9.4

Added hosts' DNS name to IP address translation for the agents, monitors, collectors, and servers. New predefined variables are added to the list of maintained by the plugin variables:

- *AGENT_HOST_IP_ADDRESS*,
- *AGENT_HOST_IP_ADDRESS_1*,
- *AGENT_HOST_IP_ADDRESS_2*,
- *AGENT_HOST_IP_ADDRESS_3*,
- *AGENT_HOST_IP_ADDRESS_4*,
- *AGENT_HOST_IP_ADDRESS_5*,
- *ALL_AGENT_HOSTS_IP_ADDRESSES*,
- *MONITOR_HOST_IP_ADDRESS*,
- *MONITOR_HOST_IP_ADDRESS_1*,
- *MONITOR_HOST_IP_ADDRESS_2*,
- *MONITOR_HOST_IP_ADDRESS_3*,

- *MONITOR_HOST_IP_ADDRESS_4*,
- *MONITOR_HOST_IP_ADDRESS_5*,
- *ALL_MONITOR_HOSTS_IP_ADDRESSES*,
- *COLLECTOR_HOST_IP_ADDRESS*,
- *COLLECTOR_HOST_IP_ADDRESS_1*,
- *COLLECTOR_HOST_IP_ADDRESS_2*,
- *COLLECTOR_HOST_IP_ADDRESS_3*,
- *COLLECTOR_HOST_IP_ADDRESS_4*,
- *COLLECTOR_HOST_IP_ADDRESS_5*,
- *ALL_COLLECTOR_HOSTS_IP_ADDRESSES*,
- *SERVER_HOST_IP_ADDRESS*,
- *SERVER_HOST_IP_ADDRESS_1*,
- *SERVER_HOST_IP_ADDRESS_2*,
- *SERVER_HOST_IP_ADDRESS_3*,
- *SERVER_HOST_IP_ADDRESS_4*,
- *SERVER_HOST_IP_ADDRESS_5*,
- *ALL_SERVER_HOSTS_IP_ADDRESSES*

Provided write-up of the Workaround of incorrect sensitivity issue for built-in OOTB incidents for dynaTrace action plugins.

New in the Release 0.9.8

Added ability to embed into dashboard names predefined variables which will be substituted with their runtime values.

New in the Release 0.9.7

Here is list of new features:

- Added support for plain text e-mail format:
  - new parameter "HTML Mail Format" is set to "true" for HTML notifications and "false" for ASCII/Text notifications. Default value is "true".
- Plugin supports now reports in HTML, PDF, XLS, XML, CSV, and XSD formats:
  - new parameter "Dashboards Type" is set to one of the above report formats.
- Added new external variables supported by the plugin:
  - DYNATRACE_SERVER_REST_PORT
  - DASHBOARD_URL_1, DASHBOARD_URL_2,... DASHBOARD_URL_5 provide up to 5 links for dashboards' reports.
- Added support for "quiet time" when notification e-mails will not be sent. During quiet time incidents will be triggered as they would be during usual activities but notification e-mails will not be sent.
  - two new parameters "Quiet Time From" and Quiet Time To" are setting up a quiet time interval. Format of values for the "Quiet Time From" and "Quiet Time To" parameters is "HH:mm", where "HH" and "mm" are using notations explained in the Date and Time Patterns section here.

New in the Release 0.9.6

Here is list of new features:

- Significantly improved integration with the OOTB incidents;
- Added support for Java regular expressions for filtering incidents by Agents, Agent Groups, Monitors, Collectors, and Servers
- Plugin maintains new variables which capture sources of the incidents (AGENT_NAME_1, AGENT_NAME_2, etc.);
- Plugin maintains new variables which capture list of incidents' sources (ALL_AGENTS, ALL_AGENT_NAMES, ALL_AGENT_HOSTS etc.);
- Plugin provides REST filtering of the PDF reports by agent names/hosts, group names, and/or custom timeframe;
- START_TIME and END_TIME variables are set to "-" if they are not defined;
- Separator for multiple incident's sources for filtering set to semicolon (";").

Installation

Import the Plugin into the dynaTrace Server. For details how to do this please refer to the Online Documentation on Plugin Management.

Usage

The plugin was originally shared through the following discussion forum entry: Automatic Dash Report via e-mail.
The following link contains documentation for the plugin: **Extended Mail Action Plugin.**

The Extended Email Report Action Plugin has the following features:

1. Filtering of incidents based on
    a. agents
    b. agent groups
    c. monitors
    d. collectors
    e. servers
    f. sendOnlyPatterns
    g. measureNamePatterns
2. Customize Subject and Body of the e-mail
    a. Add/replace Subject and/or Body of the OOTB e-mail which is generated by the Email Alert Action plugin
3. Embed predefined variables into the customized text in order to provide incident's details at runtime in the Subject and/or Body of the e-mail. This list consist of the following variables:

    - *AGENT_NAME*,
    - *AGENT_NAME_1*,
    - *AGENT_NAME_2*,
    - *AGENT_NAME_3*,
    - *AGENT_NAME_4*,
    - *AGENT_NAME_5*,
    - *AGENT_HOST*,
    - *AGENT_HOST_1*,
    - *AGENT_HOST_2*,
    - *AGENT_HOST_3*,
    - *AGENT_HOST_4*,
    - *AGENT_HOST_5*,
    - *AGENT_HOST_IP_ADDRESS*,
    - *AGENT_HOST_IP_ADDRESS_1*,
    - *AGENT_HOST_IP_ADDRESS_2*,
    - *AGENT_HOST_IP_ADDRESS_3*,
    - *AGENT_HOST_IP_ADDRESS_4*,
    - *AGENT_HOST_IP_ADDRESS_5*,
    - *ALL_AGENT_NAMES*,
    - *ALL_AGENT_HOSTS*,
    - *ALL_AGENT_HOSTS_IP_ADDRESSES*,
    - *ALL_AGENTS*,
    - *AGENT_GROUP_NAME*,
    - *AGENT_GROUP_NAME_1*,
    - *AGENT_GROUP_NAME_2*,
    - *AGENT_GROUP_NAME_3*,
    - *AGENT_GROUP_NAME_4*,
    - *AGENT_GROUP_NAME_5*,
    - *ALL_AGENT_GROUP_NAMES*,
    - *MONITOR_NAME*,
    - *MONITOR_NAME_1*,
    - *MONITOR_NAME_2*,
    - *MONITOR_NAME_3*,
    - *MONITOR_NAME_4*,
    - *MONITOR_NAME_5*,
    - *MONITOR_HOST*,
    - *MONITOR_HOST_1*,
    - *MONITOR_HOST_2*,
    - *MONITOR_HOST_3*,
    - *MONITOR_HOST_4*,
    - *MONITOR_HOST_5*,
    - *MONITOR_HOST_IP_ADDRESS*,
    - *MONITOR_HOST_IP_ADDRESS_1*,
    - *MONITOR_HOST_IP_ADDRESS_2*,
    - *MONITOR_HOST_IP_ADDRESS_3*,
    - *MONITOR_HOST_IP_ADDRESS_4*,
    - *MONITOR_HOST_IP_ADDRESS_5*,
    - *ALL_MONITOR_NAMES*,
    - *ALL_MONITOR_HOSTS*,
    - *ALL_MONITOR_HOSTS_IP_ADDRESSES*,
    - *ALL_MONITORS*,
    - *COLLECTOR_NAME*,
    - *COLLECTOR_NAME_1*,
    - *COLLECTOR_NAME_2*,
    - *COLLECTOR_NAME_3*,
    - *COLLECTOR_NAME_4*,
    - *COLLECTOR_NAME_5*,
    - *COLLECTOR_HOST*,
    - *COLLECTOR_HOST_1*,

- *COLLECTOR_HOST_2*,
- *COLLECTOR_HOST_3*,
- *COLLECTOR_HOST_4*,
- *COLLECTOR_HOST_5*,
- *COLLECTOR_HOST_IP_ADDRESS*,
- *COLLECTOR_HOST_IP_ADDRESS_1*,
- *COLLECTOR_HOST_IP_ADDRESS_2*,
- *COLLECTOR_HOST_IP_ADDRESS_3*,
- *COLLECTOR_HOST_IP_ADDRESS_4*,
- *COLLECTOR_HOST_IP_ADDRESS_5*,
- *ALL_COLLECTOR_NAMES*,
- *ALL_COLLECTOR_HOSTS*,
- *ALL_COLLECTOR_HOSTS_IP_ADDRESSES*,
- *ALL_COLLECTORS*,
- *SERVER_NAME*,
- *SERVER_NAME_1*,
- *SERVER_NAME_2*,
- *SERVER_NAME_3*,
- *SERVER_NAME_4*,
- *SERVER_NAME_5*,
- *SERVER_HOST_IP_ADDRESS*,
- *SERVER_HOST_IP_ADDRESS_1*,
- *SERVER_HOST_IP_ADDRESS_2*,
- *SERVER_HOST_IP_ADDRESS_3*,
- *SERVER_HOST_IP_ADDRESS_4*,
- *SERVER_HOST_IP_ADDRESS_5*,
- *ALL_SERVER_HOSTS_IP_ADDRESSES*
- *ALL_SERVER_NAMES*,
- *DYNATRACE_SERVER_NAME*,
- *DYNATRACE_SERVER_REST_PORT,*
- *MESSAGE*,
- *RULE_NAME*,
- *RULE_DESCRIPTION*,
- *SENSITIVITY*,
- *SESSION_ID*,
- *SESSION_NAME*,
- *START_TIME*,
- *END_TIME*,
- *DURATION*,
- *IS_OPEN*,
- *IS_CLOSED*,
- *SEVERITY*,
- *KEY*,
- *STATE*,
- *SYSTEM_PROFILE*,
- *APPLICATION*,
- *VIOLATED_MEASURE_NAME*,
- *VIOLATED_MEASURE_DESCRIPTION*,
- *VIOLATED_MEASURE_VALUE*,
- *VIOLATED_MEASURE_UNIT*,
- *VIOLATED_MEASURE_SPLITTINGS*,
- *VIOLATED_MEASURE_TRESHOLD_UPPER_SEVERE*,
- *VIOLATED_MEASURE_TRESHOLD_LOWER_SEVERE*,
- *VIOLATED_MEASURE_TRESHOLD_UPPER_WARNING*,
- *VIOLATED_MEASURE_TRESHOLD_LOWER_WARNING*,
- *VIOLATED_MEASURE_METRIC_NAME*,
- *VIOLATED_MEASURE_METRIC_DESCRIPTION*,
- *VIOLATED_MEASURE_METRIC_GROUP*,
- *VIOLATED_MEASURE_METRIC_UNIT*,
- *VIOLATED_TRIGGER_VALUE_SOURCE_TYPE*,
- *VIOLATED_TRIGGER_VALUE_SOURCE_NAME*,
- *VIOLATED_TRIGGER_VALUE_SOURCE_HOST*,
- *VIOLATED_TRIGGER_VALUE*,
- *VIOLATION_HEADER_1*,
- *VIOLATION_MESSAGE_1*,
- *VIOLATION_HEADER_2*,
- *VIOLATION_MESSAGE_2*,
- *VIOLATION_HEADER_3*,
- *VIOLATION_MESSAGE_3*,
- *VIOLATION_HEADER_4*,
- *VIOLATION_MESSAGE_4*,
- *VIOLATION_HEADER_5*,

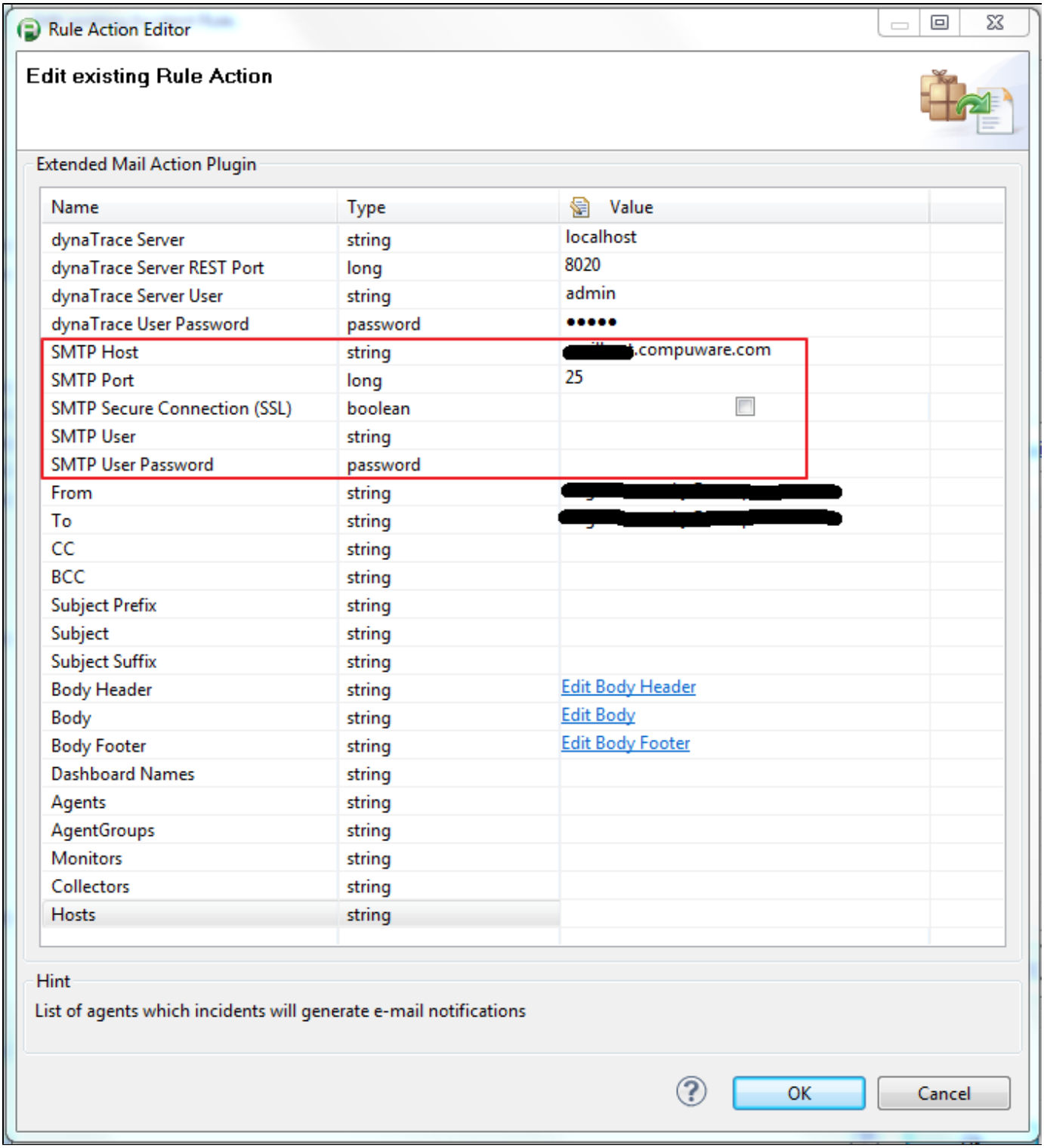
- *VIOLATION_MESSAGE_5*,
- *INCIDENT_STARTED_ENDED*,
- *IMAGE_WARNING_OK,*
- *DASHBOARD_URL_1,*
- *DASHBOARD_URL_2,*
- *DASHBOARD_URL_3,*
- *DASHBOARD_URL_4,*
- *DASHBOARD_URL_5,*
- APPLICATION_ALL,
- VIOLATED_MEASURE_NAME_ALL,
- VIOLATED_MEASURE_DESCRIPTION_ALL,
- VIOLATED_MEASURE_VALUE_ALL,
- VIOLATED_MEASURE_UNIT_ALL,
- VIOLATED_MEASURE_SPLITTINGS_ALL,
- VIOLATED_MEASURE_TRESHOLD_UPPER_SEVERE_ALL,
- VIOLATED_MEASURE_TRESHOLD_LOWER_SEVERE_ALL,
- VIOLATED_MEASURE_TRESHOLD_UPPER_WARNING_ALL,
- VIOLATED_MEASURE_TRESHOLD_LOWER_WARNING_ALL,
- VIOLATED_MEASURE_METRIC_NAME_ALL,
- VIOLATED_MEASURE_METRIC_DESCRIPTION_ALL,
- VIOLATED_MEASURE_METRIC_GROUP_ALL,
- VIOLATED_MEASURE_METRIC_UNIT_ALL,
- VIOLATED_TRIGGER_VALUE_SOURCE_TYPE_ALL,
- VIOLATED_TRIGGER_VALUE_SOURCE_NAME_ALL,
- VIOLATED_TRIGGER_VALUE_SOURCE_HOST_ALL,
- VIOLATED_TRIGGER_VALUE_ALL,
- DYNATRACE_INCIDENTS*,*
- PURE_PATH_1,
- PURE_PATH_2,
- PURE_PATH_3,
- PURE_PATH_4,
- PURE_PATH_5.

4. Attach multiple custom and/or OOTB dashboards in PDF format
    a. Filter reports using agent-names/agent-hosts, agent-groups, and/or custom timeframe
5. Customize To, CC, and BCC fields of the e-mail by providing lists of e-mail addresses
6. Set From e-mail address
7. Set specific SMTP mail server
8. Supports setting up individual thresholds for the Dynatrace dynamic measures

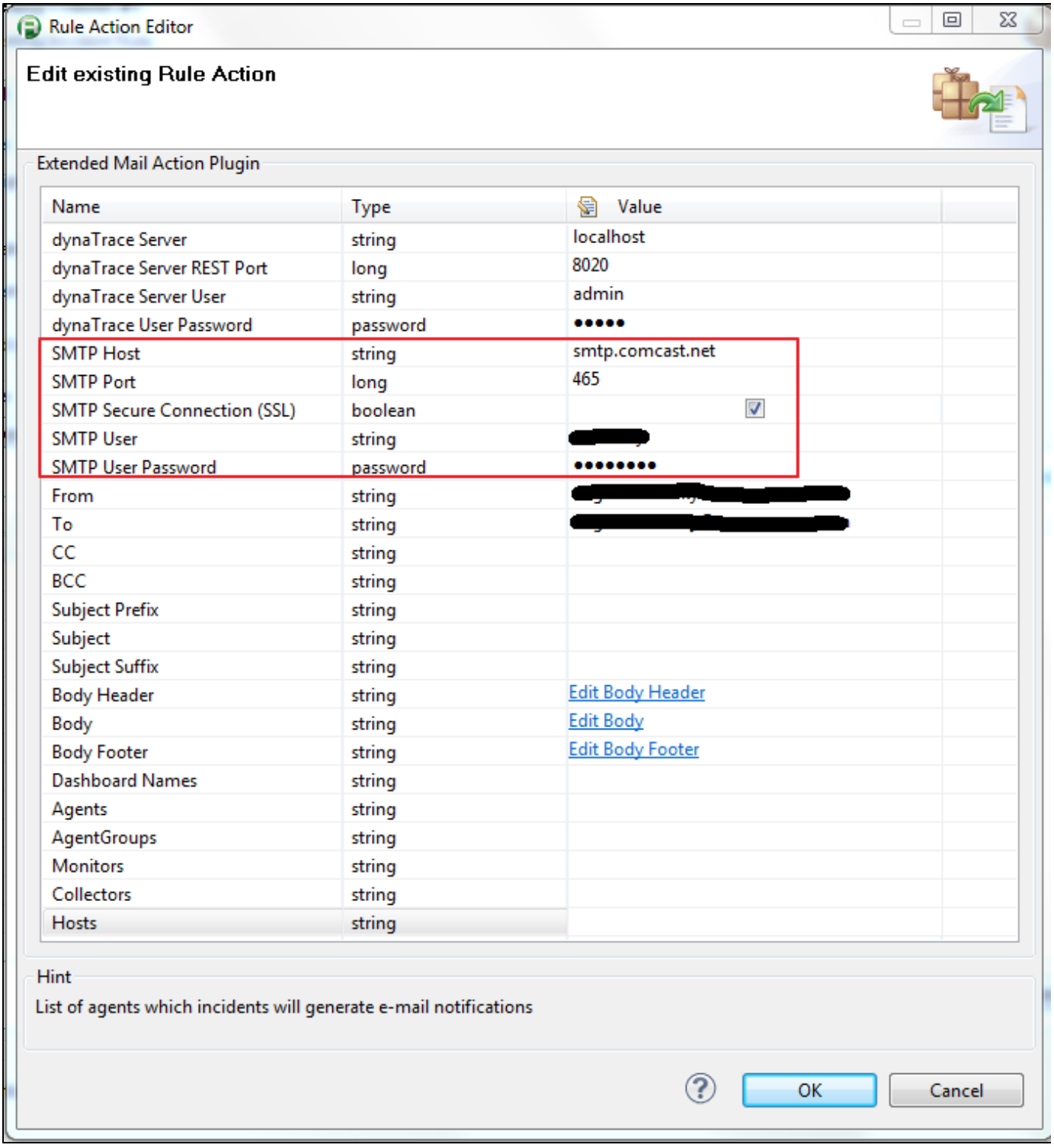
The plugin provides a great extension to the default Email Alert Action plugin.

Configuration

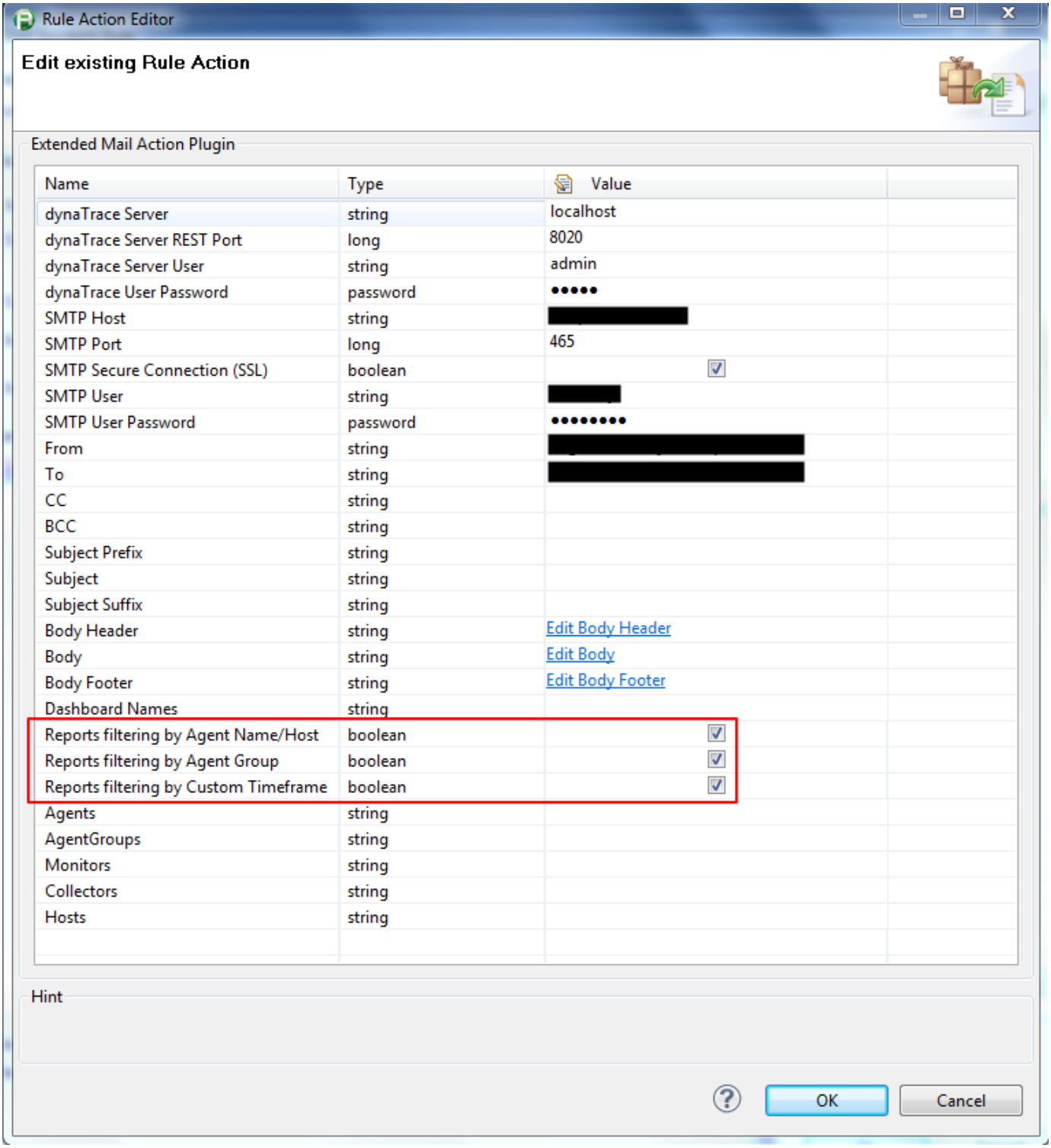
The following screenshot shows an example configuration for non-SSL SMTP server.



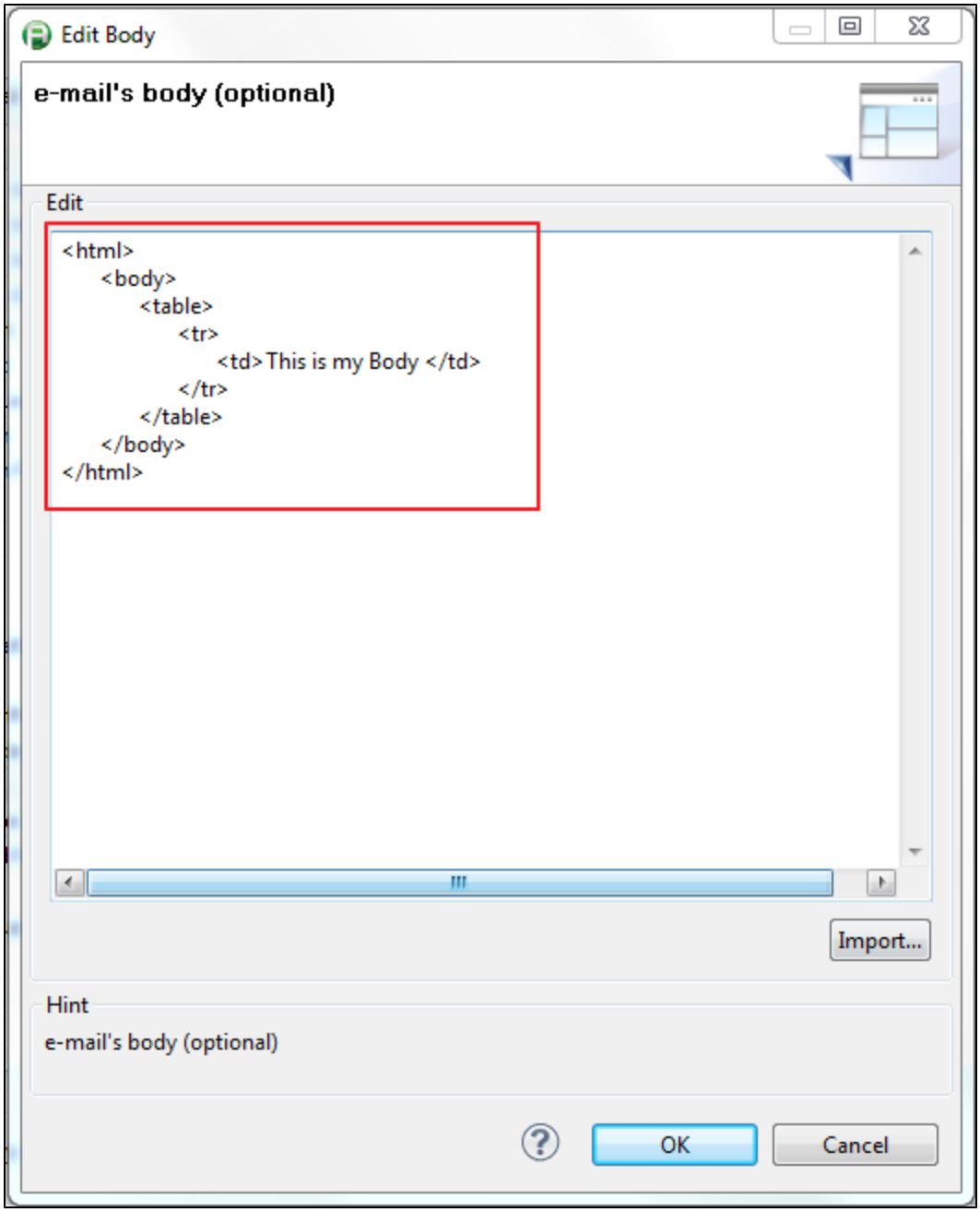
Next screenshot shows an example configuration for SSL SMTP server:



Next screenshot shows Report Filtering by Agent Name/Agent Host, Agent Group, and Custom Timeframe:



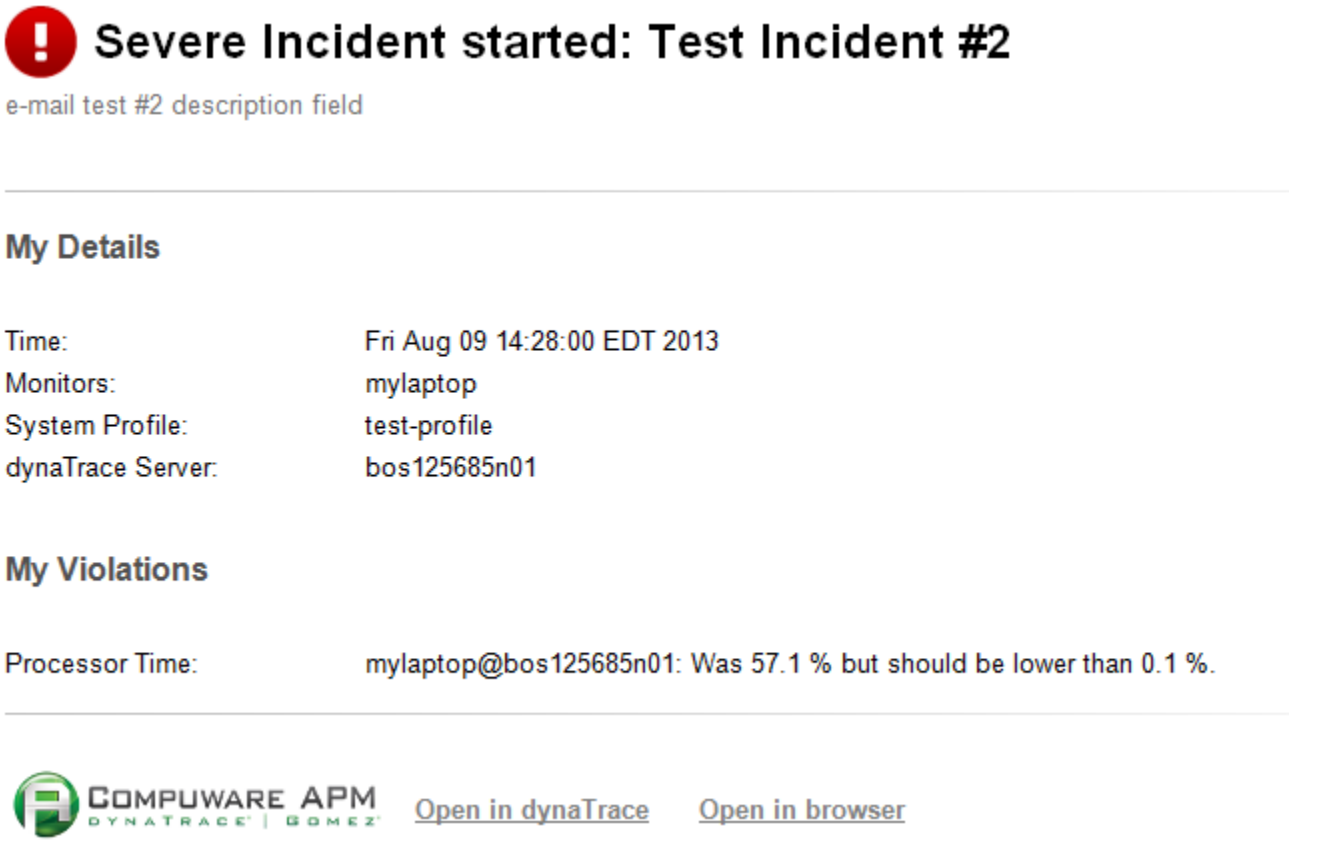
Next screenshot shows an example configuration of the Body parameter:



Next screenshot contains more complex example of the Body parameter (full content of the Body parameter is here):

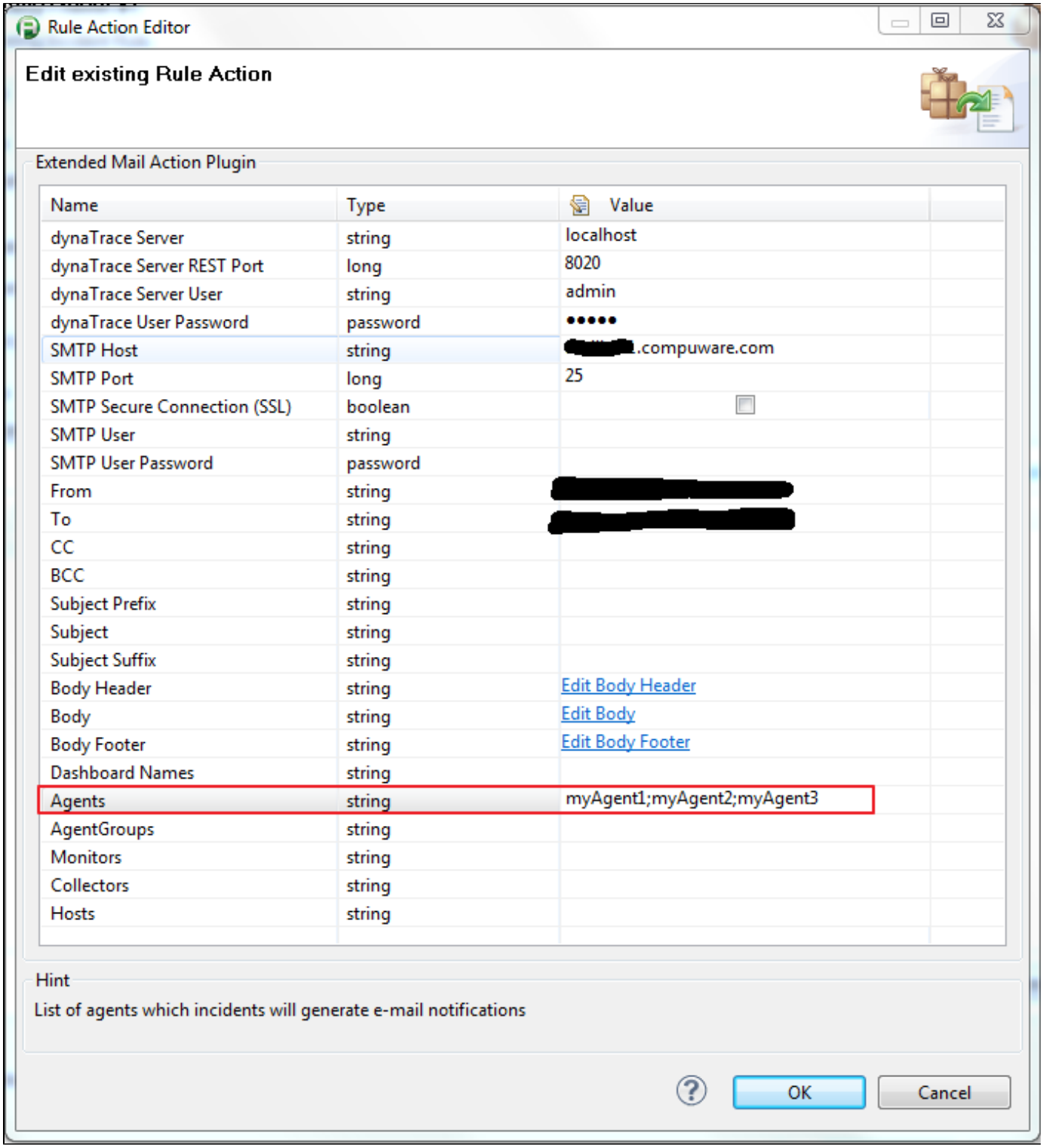
```
<table style="border: 0px;" cellpadding="0" cellspacing="0">
    <tr>
        <td style="width: 5px; margin-right: 8px;"><img src="dtbundleresource:${IMAGE_WARNING_OK}" /></td>
        <td style="width: 795px;"><div style="font-size: 1.5em; font-weight: bold;">${SEVERITY} Incident ${INCIDENT_STARTED_ENDED}: ${RULE_NAME}</div></td>
    </tr>
    <tr>
        <td colspan="2"><div style="font-size: 0.8em; color: #737373; margin-top: 5px; width: 800px;">${RULE_DESCRIPTION}</div></td>
    </tr>
</table>
<br>
<div>
    <img style="margin-top: 20px;" src="dtbundleresource:res/separator.png">
</div>
<br>
<div style="font-weight: bold;">My Details</div>
<table style="border: 0px; margin-top: 5px;" cellpadding="0" cellspacing="0">
    <tr>
        <td style="vertical-align: top; width: 180px;"><div style="font-size: 0.8em;">Time:</div></td>
        <td><div style="font-size: 0.8em;">${START_TIME}</div></td>
    </tr>
    <tr>
        <td style="vertical-align: top; width: 180px;"><div style="font-size: 0.8em;">Monitors:</div></td>
        <td><div style="font-size: 0.8em;">${MONITOR_NAME}</div></td>
    </tr>
    <tr>
        <td style="vertical-align: top; width: 180px;"><div style="font-size: 0.8em;">System Profile:</div></td>
        <td><div style="font-size: 0.8em;">${SYSTEM_PROFILE}</div></td>
    </tr>
    <tr>
        <td style="vertical-align: top; width: 180px;"><div style="font-size: 0.8em;">dynaTrace Server:</div></td>
        <td><div style="font-size: 0.8em;">${SERVER_NAME}</div></td>
    </tr>
</table>
<br>
<br>
<div style="font-weight: bold;">My Violations</div>
<table style="border: 0px; margin-top: 5px;" cellpadding="0" cellspacing="0">
    <tr>
        <td style="vertical-align: top; width: 180px;"><div style="font-size: 0.8em;">${VIOLATION_HEADER_1}:</div></td>
        <td><div style="font-size: 0.8em;">${VIOLATION_MESSAGE_1}</div></td>
    </tr>
</table>
<div>
    <img style="margin-top: 20px;" src="dtbundleresource:res/separator.png">
</div>
<table>
    <tr>
        <td style="width: 200px;"><div>
            <img style="margin-top: 20px;" src="dtbundleresource:res/logo.png">
        </div></td>
        <td style="width: 140px;"><div>
            <a style="a: link:text-decoration:underline; font-size: 0.8em; font-weight: bold; color: #505050; a: visited:text-decoration:underline;
            font-size: 0.8em; font-weight: bold; color: #505050; a: hover:text-decoration:underline; font-size: 0.8em; font-weight: bold; color: #808080;"
            href="http://127.0.0.1:8020/webstart/Client/client.jnlp?&amp;argument=-reuse&amp;argument=-incident&amp;argument=${SYSTEM_PROFILE}&amp;argument=${KEY}">Open in dynaTrace</a>
        </div></td>
        <td style="width: 125px;"><div>
            <a style="a: link:text-decoration:underline; font-size: 0.8em; font-weight: bold; color: #505050; a: visited:text-decoration:underline; font-size: 0.8em;
            font-weight: bold; color: #505050; a: hover:text-decoration:underline; font-size: 0.8em; font-weight: bold; color: #808080;"
            href="http://127.0.0.1:8020/rest/html/management/dashboards">Open in browser</a>
        </div></td>
    </tr>
</table>
```

Next screenshot shows e-mail which was created by the Body depicted in the previous screenshot:



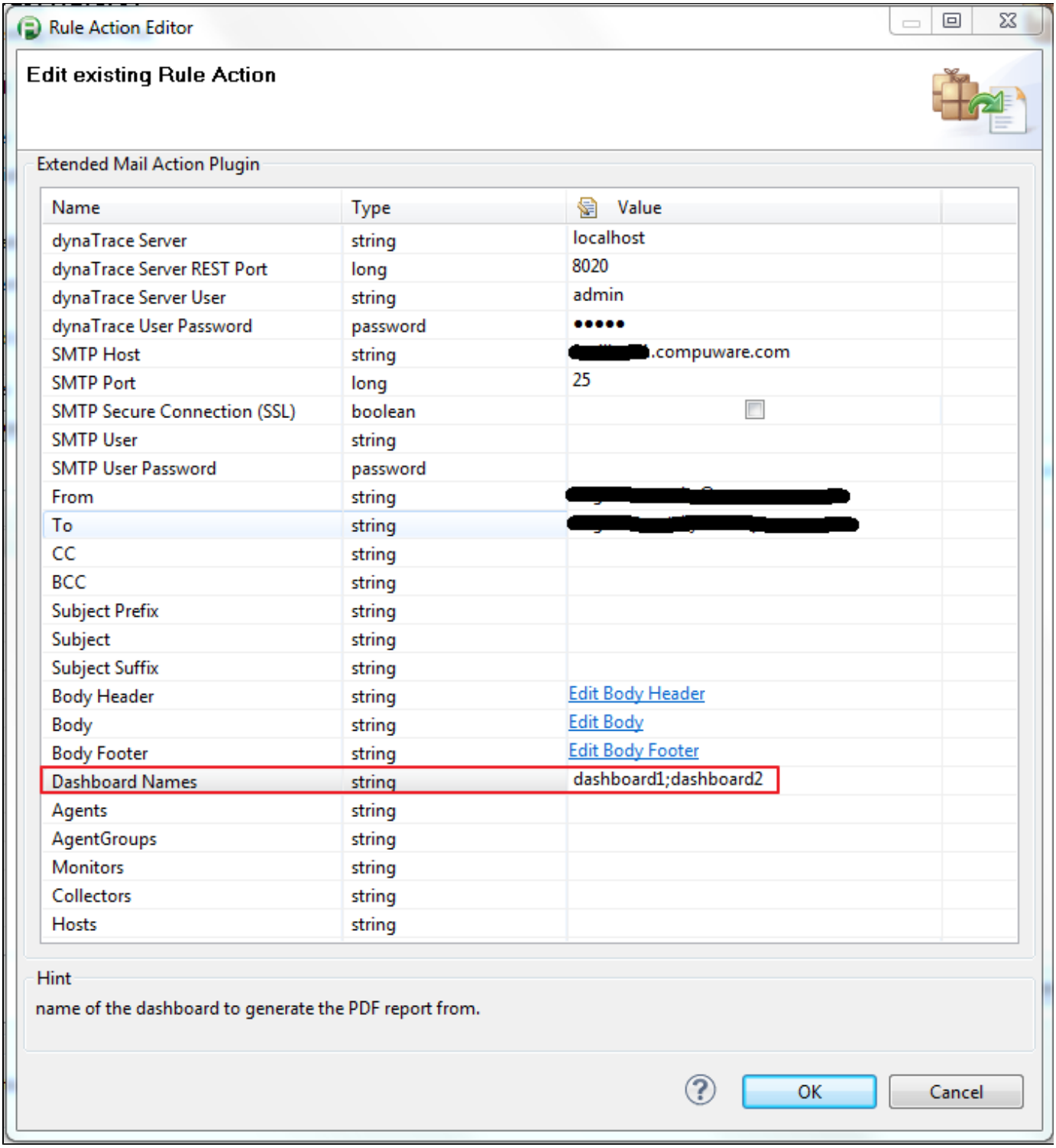
For more examples of Body, Body Header, and Body Footer parameters please see pages 11 - 13 of the **Extended Mail Action Plugin** document.

Next screenshot shows an example configuration of filtering by agents:



For more details about filtering see section 2 on page 7 of the **Extended Mail Action Plugin** document.

Next screenshot shows an example configuration for generating and attaching PDF files to the e-mail:



Custom Text

The following notation is used to embed predefined variables in the text:

- ${variable-name}, where variable-name is one of the names from the list of predefined variables.

Next is an example of custom text:

"I do not like incidents, especially when they are coming from the agent ${AGENT_NAME} which is running on the host ${AGENT_HOST}"

For more examples see section 4 on page 9 of the **Extended Mail Action Plugin** document.

Feedback

Please provide feedback on this plugin either by commenting on this page or by comments on the Community Plugins and Extensions

Contribution

Feel free to contribute any changes on Github

Comments

Please post comments in AppMon & UEM Plugins

Looking for old comments? Find them here (this page is loading very slow!)