Avaya Endpoint Access Control Agent Administrator's Guide

5.0
NN47230-601, 02.03
May 2011

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: Introduction

The Avaya Endpoint Access Control (EAC) Agent checks that the components (executables, DLLs, configuration files) required to comprise a personal firewall are installed and active on the remote user's machine.

The Avaya EAC Agent Administrator's Guide provides information to configure the Avaya EAC Agent applet and SRS rules.

Navigation

Related publications

For more information about AVG, NVR or SNAS, see the following publications:

- VPN Gateway - Administrator Guide
- VPN Router Administration
- Release Notes for Avaya Ethernet Routing Switch 5500 Series, Software Release 5.0.1
- Release Notes for the Ethernet Routing Switch 8300, Software Release 2.2.8
- Release Notes for the Secure Network Access Solution, Software Release 1.6.1
- Release Notes for Enterprise Switch Manager, Software Release 5.2
- Using Enterprise Switch Manager Release 5.1
- Secure Network Access Solution Guide
- Secure Network Access Switch 4050 Installation Guide
- Secure Network Access Switch 4050 User Guide for the CLI

To print selected technical manuals and release notes, see http://www.avaya.com/support, find the product for which you need documentation, then locate the specific category and model or

version for your hardware or software product. Use Adobe Reader to open the manuals and release notes, search for the sections you need, and print. To download Adobe Reader, see http://www.adobe.com/ .

Customer Service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. See www.avaya.com or one of the pages listed in the following sections.

Navigation

- Getting technical documentation on page 6
- Getting product training on page 6
- Getting technical support from the Avaya Web site on page 6

Getting technical documentation

To download and print selected technical publications and release notes, see www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, see www.avaya.com/support. The training contacts link is located on the left-hand navigation pane.

Getting technical support from the Avaya Web site

You can access technical support for Avaya products from the Avaya Technical Support Web site, see www.avaya.com/support.

Chapter 2: Avaya EAC Policy Administrator interface fundamentals

Navigation

Avaya EAC Policy Administrator user interface

This section describes the Avaya EAC Policy Administrator user interface.

Launching Avaya EAC Policy Administrator

The Avaya EAC Policy Administrator allows you to enable Avaya EAC Agent and to configure global Avaya EAC Agent settings for the selected Domain.

The Avaya EAC Policy Administrator is accessible through the Browser-based interface (BBI) in two ways

1. a. Log on to BBI.
   b. Click the **Config** tab.
   c. Select VPN Gateways\<VPN Name>\EACA\SRS Rules.

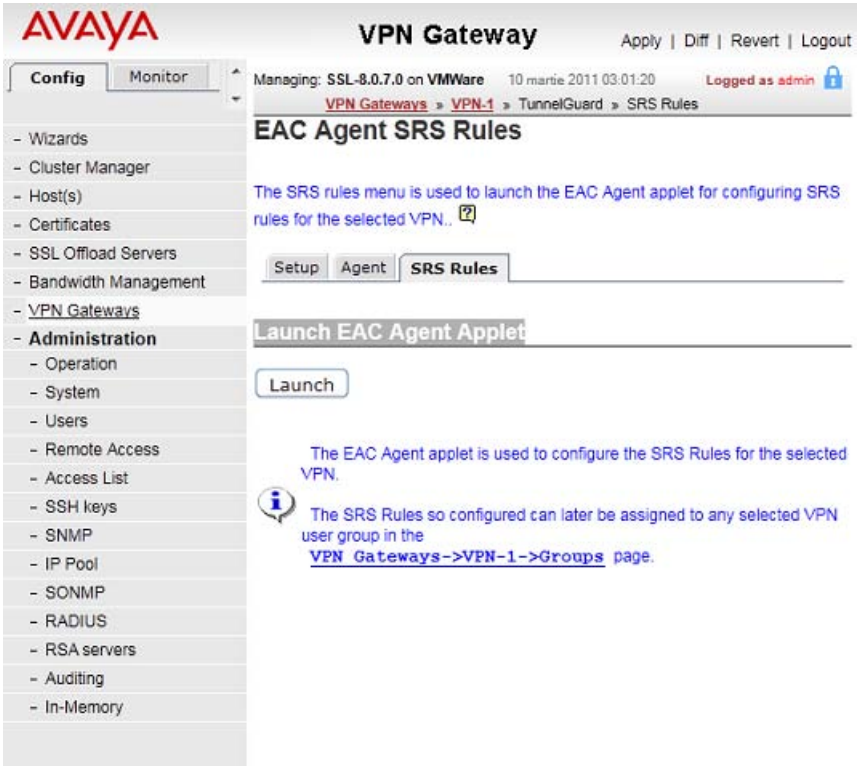
The Avaya EAC Policy Administrator screen appears.

Important:

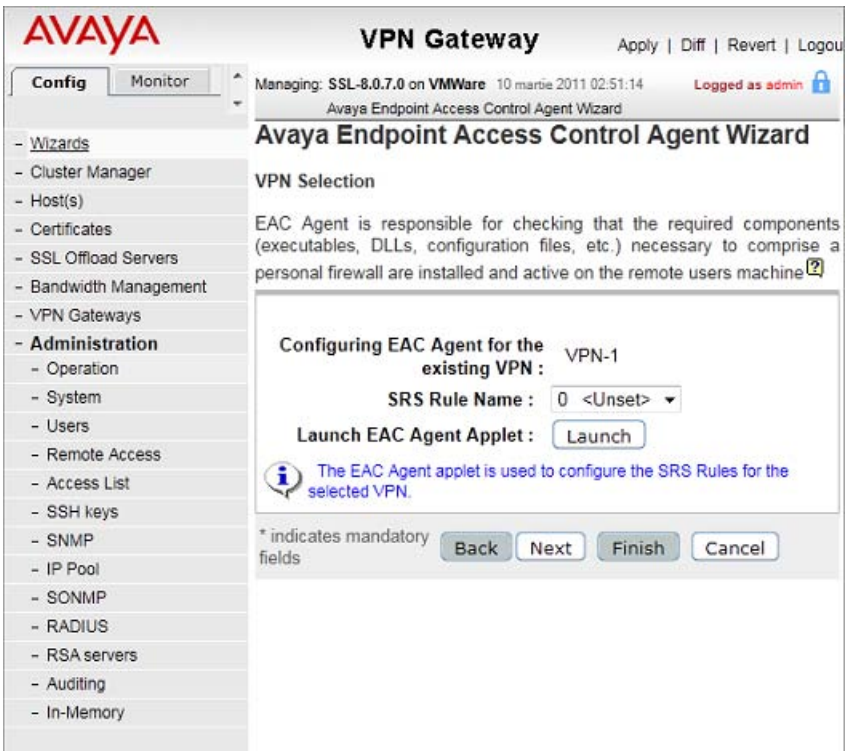
The Avaya EAC Policy Administrator configures SRS Rules for the selected Domain.

d. Click **Launch**.

The Avaya EAC Policy Administrator window appears.

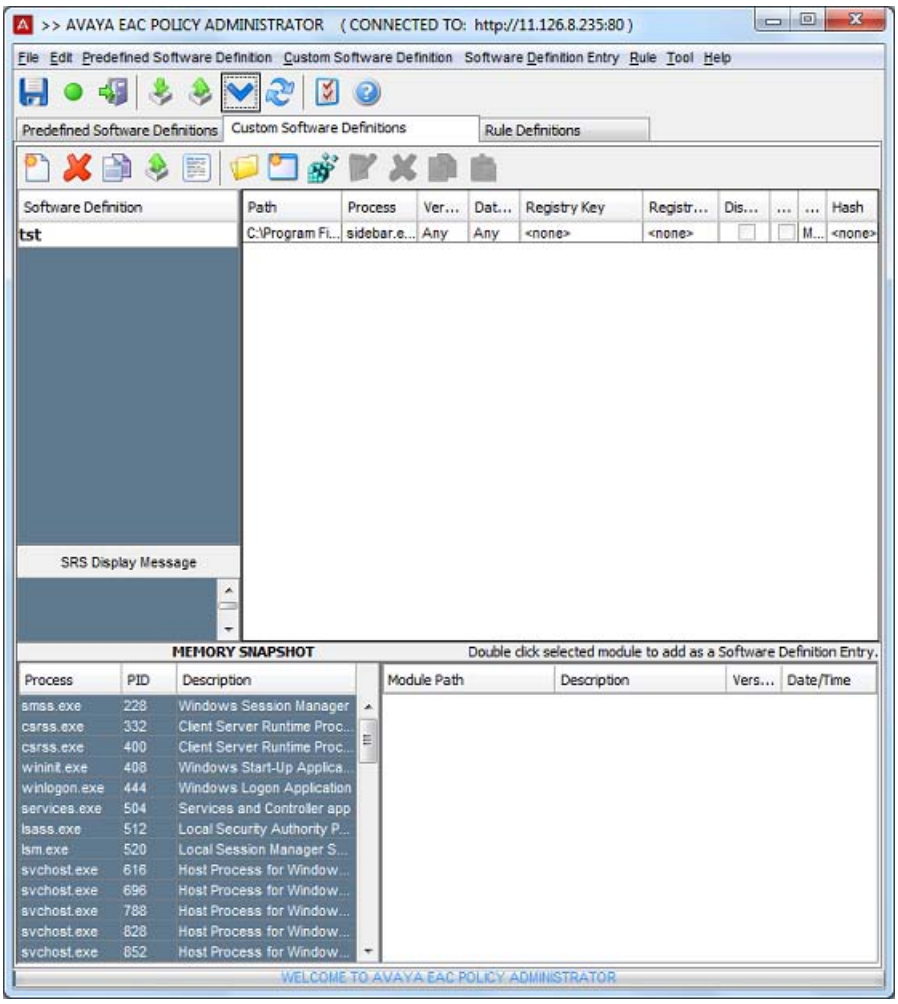


2. Click Launch button in section Config->Wizards->Avaya Endpoint Access Control Agent Wizard->Launch EAC Agent Applet.



Avaya EAC Policy Administrator user interface navigation

Once the Avaya EAC Policy Administrator Applet launches, the application home screen appears:



Software Definition Entry components table

Click the Custom Software Definitions tab. The right pane lists the Software Definition Entries. The following table describes the Software Definition Entry components.

Table 1: Software Definition Entry components table

Item	Description
Path	Shows the full directory path to the file location.
Process	Shows the process name, in which the component runs. For files that only exist on disk, this column does not apply.
Version	Shows version information of the component.
Date/Time	Shows the last modified time of the component.
Registry Key	Shows the registry key entry.
Registry Expression	Shows a regular expression used to match a registry key value.

Item	Description
DiskOnly	If selected, the file is not loaded in memory. If this option is combined with the API option, the file is loaded and the API called.
API	If checked, means that the component contains a third party API for further checking.
HashAlg	Shows the hash algorithm used to generate the hash.
Hash	Shows the hash value of the file.

Memory snapshot

The memory snapshot section in the lower half of the Avaya EAC Policy Administrator Software Definition screen displays all processes currently running on the administrator system. On Windows 7 and Windows Vista, it displays only the processes running in current user context.

Note:

For Windows Vista and Windows 7 systems you must run the internet browser as an administrator for Avaya EAC Agent to display all running processes.

If you launch the applet on a 64 bit system, 32 bit processes list with a ”*32" suffix to help distinguish 32 bit processes from 64 bit processes with the same name. The ”*32" text specifies that the process runs in a 32 bit context. The display list is similar to the Task Manager process list on Windows 64 bit architectures.

To create a rule use the original process name without the suffix. For example, if the process appears in the list as ”MyProcess.exe *32", use ”MyProcess.exe" as the process name.

You can select and add any process currently running and loaded into the memory snapshot to the SRS set or use the Add a selected memory module menu command.

Important:

You can access memory snapshot at startup or from the Tools menu.

The following table shows a list of the memory snapshot items.

Table 2: Memory snapshot item descriptions

Item	Description
Process	Specifies the name of the process or file currently in memory.
PID	Specifies the unique system process ID for each running process.
Description	Specifies a text description, if one is available, for each process.
Module Path	Specifies the module path for the software definition entry.

Item	Description
Version	Specifies a particular version for the software definition entry.
Date/Time	Specifies the last modified date/time of the software definition entry.

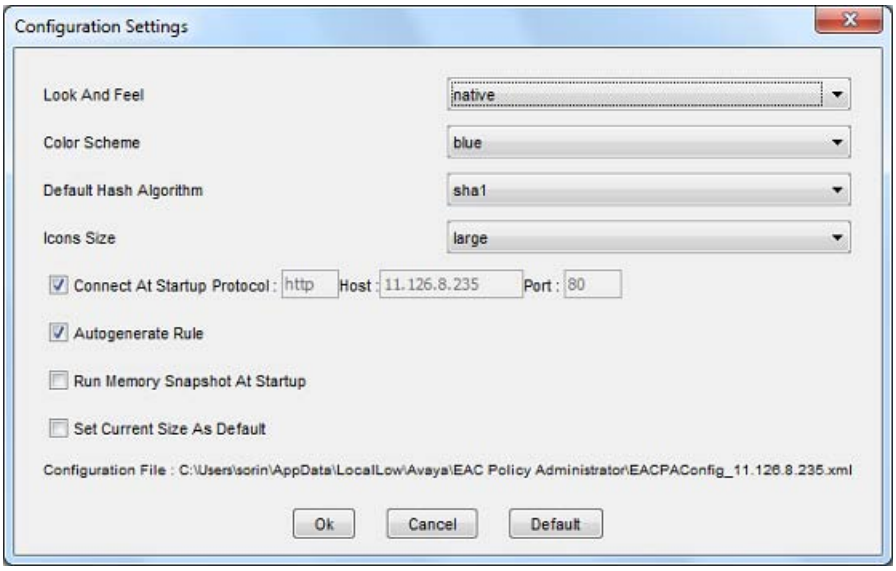
Configuring preferences

Configure the preferences for the Avaya EAC Policy Administrator.

Procedure steps

1. Launch the Avaya EAC Policy Administrator screen.
2. From the Edit menu, choose the **Preferences** option.

   The Configuration Settings window appears.



3. From the **Look and Feel** list, choose **native** or **cross platform**.
4. From the **Color Scheme** list, choose **red**, **gradient**, **orange**, **purple**, **teal**, or **blue**.
5. From the **Default Hash Algorithm** list, choose **sha1** or **md5**.
6. From the **Icons Size** list, choose **large** or **small**.
7. Select the **Connect At Startup** check box, and specify the values for **Protocol**, **IP address**, and **Port** to start the Applet.
8. Select the **AutoGenerate Rule** check box to generate the Rule automatically.
9. Select the **Run Memory Snapshot At Startup** check box to run the snapshot during the startup of the EAC Agent applet.

10. Select the **Set Current Size As Default** check box to retain the current size of the applet as the default size.
11. Click **OK** to apply the preferences.

    OR

    Click **Default** to use the default preferences.

Registry based SRS Entries

Avaya EAC Policy Administrator supports checking of on-disk files, running processes, hash checking and version numbers to verify installed software packages. You can also read the registry settings on a client's PC to check software packages and installed state.

The following sections provide details on registry-based rules:

- Registry only SRS entry on page 13
- Registry-based File or Module on page 15

Registry only SRS entry

Both Avaya EAC Agent and Avaya EAC Policy Administrator support registry-checking functionality. The administrator tool applet is used to add registry key checks into SRS entries. You can check for the existence of certain registry keys and enforce the values on a desktop PC before allowing access to the network. One SRS entry holds any number of registry key checks, just as one SRS entry holds any number of file checks. Contrary to file and process checks, registry key checks do not check hash, date, and version number checking enabled. However, you can combine registry key checking entry with any other type of checking, such as process check or on-disk entry check.

Registry-based rules are useful in instances where rules are created based on Registry Key Values. Avaya EAC Policy Administrator supports simple regular expressions-based rules for Registry Key Values.

Avaya EAC Policy Administrator is a Java-based application that uses the pattern and the regular expression support available in JRE. It provides all of the relevant pattern-matching facility based on regular expressions provided by JRE.

Registry Key Values of type string and integer are supported. Binary data type for Registry Key Values is not supported.

The following table describes supported operands for integer values.

Table 3: Supported integer operands

Operand	Description
>=	greater than or equal to

Operand	Description
<=	less than or equal to
==	equal to
!=	not equal to
<	less than
>	greater than

The following are examples of regular expressions for integer Registry Key values:

- >= 20—matches integer values that are greater than or equal to 20
- = 100—matches integer values that are exactly equal to 100
- < 50—matches integer values that are less than 50
- != 200—matches all integer values that are not equal to 200

The following table describes supported constructs for string-based regular expressions.

Table 4: Constructs for string-based regular expressions

String regular expression	Description
x	the character x
.	any character
\\	the backslash characters
\0 *n*	the character with octal value 0 *n* (0 <= n <= 7)
\	the character with the hexidecimal value 0xhh
\t	the tab character ('\u0009')
\n	the newline (line feed) character ('\u000A')
\d	a digit: [0-9]
\D	a nondigit: [^0-9]
\s	a whitespace character: [\t\n\x0B\f\r]
\S	a non=whitespace character: [^\s]
\w	a word character: [a-zA-Z_0-9]
\W	a nonword character: [^\w]
[abc]	a, b, or c
[^abc]	not a, b, or c
[a-z]	any character a through z
[a-d[m-p]]	a through d, or m through p: [a-dm-p] (union)
[a-z&&[def]]	d, e, or f (intersection)

String regular expression	Description
[a-z&&[^bc]]	a through z, except for b and c: [ad-z] (subtraction)
X?	X, once or not at all
X*	X, zero or more times
X+	X, one or more times
X{*n*}	X, exactly *n* times
X{*n*,}	X, at least *n* times
X{*n,m*}	X, at least *n* but not more than *m* times
\	nothing, but quotes the following character
\Q	nothing, but quotes all characters until \E
\E	nothing, but ends quoting started by \Q
^	the beginning of a line
$	the end of a line
\b	a word boundary

The following are examples of regular expressions for string-based Registry Key values:

- ^Avaya .*Inc — matches anything that starts with Avaya and ends with Inc
- \w* — matches Avaya EAC Agent_2; does not match Avaya EAC Agent_2.0.0 (word definition includes_but not ".")
- [a-z] {2}_[\.\d]+ — matching tg_2.0.0; does not match Tg_2.0.0; does not match tg_; does not match tg_two; does not match tug_2.0.0

Registry-based File or Module

If the File/Module path or name is not known to the administrator or is not static for SRS rule creation, the file name or module is sometimes available as Registry Key Value data. Administrators can define a Registry Key to look for and derive a File/Module path and name from the Registry Key Value data. This path is then treated exactly as any other OnDisk entry or Memory Module entry.

File age check

Most PCs contain antivirus software with virus-definition files that update weekly, biweekly, or monthly. You can create a rule that the Avaya EAC Policy Administrator check fails if the users contain virus definitions older than a specified time period.

The administrator tool applet's Set Date/Time Range allows you to specify a "Relative Date/ Time Range" option. If you select this option, To and From dates are automatically cleared.

Software definition display message

The software definition display message appears on the left bottom side of the Avaya EAC Policy Administrator window in the "Custom Software Definition" or "Predefined Software Definition" tab.

This message displays along with SRS name when the SRS fails. This displays Software Definition specific messages to the end user. For example, you can configure one Software Definition Message for Antivirus and another for Firewall. If Firewall and Antivirus software definitions are both part of the rule and one fails, then the specific Firewall or Antivirus message displays to the end user.

Network Access Protection

The Avaya Endpoint Access Control solution integrates the Avaya NAP Enforcement Client module to check administrator's defined rules.

Network Access Protection (NAP) is a set of operating system components that provide a platform for protected access to private networks. The NAP platform provides an integrated evaluation of the system health state of a network client attempting to connect to or communicate on a network. The NAP can restrict the access of the network client until health policy requirements are met

NAP allows network administrators to define granular levels of network access based on who a client is, the groups a client belongs, and the degree a client is compliant with corporate governance policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client to compliance and dynamically increase the clients level of network access.

For information on how to configure NAP, see Network Access Protection section in the Avaya VPN Gateway BBI Application Guide.

Avaya EAC Policy Administrator support for API calls

The Avaya EAC Policy Administrator can interact with other software vendor applications. In addition to its own checks, you can configure Avaya EAC Policy Administrator to communicate with other applications and ask for their status. The result of the status check is treated the same as other checks and is reported back to the server. An administrator can use the Avaya

EAC Policy Administrator to retrieve status from other software packages, such as personal firewalls and virus checkers, to ensure they are running properly.

Making API calls

Avaya EAC Policy Administrator requires a Windows Platform DLL that implements at least one common entry point as described in the following:

Windows

```
#include <windows.h>
/*  return values */
#define STATUS_SUCCESS 0
#define STATUS _FAILURE  -1
#define STATUS_REQUIRES_UPDATE 1
/* simple check */
int WINAPI CheckStatus(void);
```

This API blocks until one of the required status is returned in 10 seconds or less. If an answer is not returned in 10 seconds, the software is assumed unavailable, the call times out and an error message displays.

Rule Definitions screen

Click the Rule Definitions tab to access the rule definitions screen. You can use this screen to create and manage rules. The Rule Definitions toolbar appears at the top of the screen.

Rule Definitions toolbar

The following figure shows the Rule Definitions toolbar.

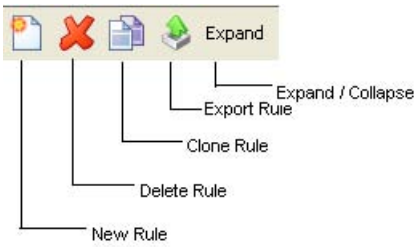


Figure 1: Rule Definitions toolbar

You can use the Rule Definitions toolbar icons to:

- define a new rule
- delete the selected rule
- clone the selected rule
- export the selected rule
- expand or collapse the rules

SRS rule list

The SRS Rule list shows the existing SRS rules. The Avaya EAC Policay Administrator applet retrieves rules from the SNAS at start-up

The following table provides SRS rules information.

Table 5: SRS Rule information

Item	Description
Avaya EAC Agent Rule Name	Shows the name of the rule.
Rule Expression Editor	Provides the rule expression.
Display Message Editor	Shows any comments related to the rule.
Trigger Action Editor	Specifies the trigger actions.

SRS Rule Expression Constructor

You can use this section to define SRS rule expressions. For more information on Rules and expressions, see Management of custom software definition on page 31.

Available Expression list

The Available Expression list contains the elements you need to construct the Boolean expression. The expressions can be basic SRS definitions or user defined ones.

Rule Expression Constructor

You can group multiple SRS Rule expressions into more compound expressions using the AND, OR, or NOT operators.

Form Avaya EAC Policy Administrator rule expression

Select this option to put the expression you create into the Available SRS Rule Expression list.

Once the expression is formed, it is available for rule definitions. Any unused expressions are not saved on the SNAS and are not available once the Avaya EAC Policy Administrator applet closes.

Logical Expression

You can create a logical expression to specify an SRS rule that comprises a number of different requirements. The logical expression must contain the conditions that must be true for the Avaya EAC Policy Administrator checks to pass. For example, a logical expression can define several applications that must be present on the client computer, or that either of two applications must be present.

Once you create a logical expression with the desired conditions, select the expression for the Avaya EAC Policy Administrator SRS rule.

The Avaya EAC Policy Administrator SRS rule can now be mapped to the desired user group. You can create a new software definition if required. The expression created for the software definition can be used to form a new logical expression, including both the new and the existing expression. For more information, see Creating logical expressions on page 43.

Display message for a rule

You can add a display message to an Avaya EAC Policy Administrator rule to provide important information for the user. For example, a message to display the reason the Avaya EAC Policy Administrator checks failed and the recommended actions. The display message information is included in the <*var:tgFailureReason*> variable, along with the Rule expression name. In teardown mode, the display message automatically displays on the Portal Login page.

Chapter 3: Avaya EAC Policy Administrator menu commands

This chapter describes the menu commands available in the Avaya EAC Policy Administrator application.

Navigation

File menu

The File menu commands table describes the File menu commands.

Table 6: File menu commands table

Item	Description
Save	Saves the software requirement set (SRS) definition settings.
Connect to	Establishes the new connection to the SNAS box by changing the configuration settings.
Import File	Imports the file in xml format.
Export All	Exports files in xml format.
Exit	Closes the Avaya EAC Policy Administrator window.

Edit menu

The Edit menu commands table describes the Edit menu commands.

Table 7: Edit menu commands table

Item	Description
Preferences	Allows to configure the settings as desired.

Predefined Software Definition menu

The Predefined Software Definition menu commands table describes the Predefined Software Definition menu commands.

The same menu functions are also available by selecting a created predefined software definition and right-clicking with your mouse.

Table 8: Predefined Software Definition menu commands table

Item	Description
New Definition	Creates a new definition.
Delete Definition	Deletes the selected definition.
Clone Definition	Clones the selected definition.
Export Definition	Exports a definition to an XML-formatted file.
Edit Definition Display Message	Edits the comment for the selected definition. The SRS display message appears on the left side bottom area of Avaya EAC Policy Administrator window.

Custom Software Definition menu

The following table describes the Custom Software Definition menu commands.

Table 9: Custom Software Definition menu commands table

Item	Description
New Software Definition	Creates a new software definition.

Item	Description
Delete Software Definition	Deletes the selected software definition.
Clone Software Definition	Clones a copy of the currently selected software definition.
Export Software Definition	Exports a software definition to an XML-formatted file.
Edit Software Definition Display Message	Adds or edits the comment for the selected software definition. If the check fails, the specified comment is written to the log. The SRS display message appears on the left side bottom area of Avaya EAC Policy Administrator window.

The same menu functions are also available by selecting a created custom software definition and right-clicking with your mouse.

Figure 2: Custom Software Definition toolbar

Software Definition Entry menu

The following table describes the Software Definition Entry menu commands.

Table 10: Software Definition Entry menu commands table

Item	Description
New Disk Entry	Select a file from the local file system (in "C:\Program Files\Avaya" format) and add it as one component of the SRS, for example, a text configuration file or a DLL. By doing this, you can make an API call to a DLL that is not yet loaded by Avaya EAC Policy Administrator or the application.
New Memory Module Entry	Add the selected memory module from the current memory snapshot as a required entry.
New Registry Entry	Add the registry key entry.

Item	Description
Edit SRS Entry	Edit the selected entry.
Delete Entry	Delete the selected component.
Copy Entry	Copy the selected component.
Paste Entry	Paste a component (from one SRS definition to another).

The same menu functions are also available after selecting a software definition entry and right-clicking with your mouse.

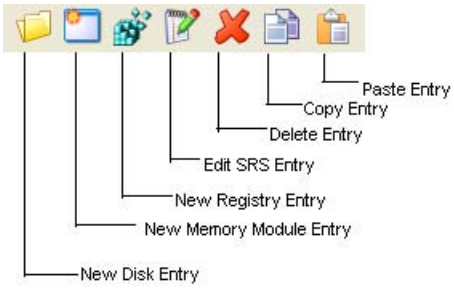


Figure 3: Software Definition Entry toolbar

Rule menu

The Rule menu commands table describes the Rule menu commands.

Table 11: Rule menu commands table

Item	Description
New Rule	Creates a new rule.
Delete Rule	Deletes the selected rule.
Clone Rule	Clones the selected rule.
Export Rule	Exports the selected rule.

Tool menu

The Tool menu commands table describes the Tool menu commands.

Table 12: Tool menu commands table

Item	Description
Show Memory Snapshot	Displays the list of processes in the Memory Snapshot area.
Refresh Memory Snapshot	Refreshes the list of processes shown in the Memory Snapshot area of the main screen. You can refresh the view if you launch other applications while running the Avaya EAC Policy Administrator or if other processes are started after the Avaya EAC Policy Administrator started.

Help menu

The Help menu commands table describes the Help menu commands.

Table 13: Help menu commands table

Item	Description
About Avaya EAC Policy Administrator	Opens the About Avaya EAC Policy Administrator window, which contains the Version, Server, and Creation date information of the software.
Avaya EAC Policy Administrator Help	Opens the Avaya EAC Policy Administrator Help window.

Chapter 4: Predefined software definition management

Navigation

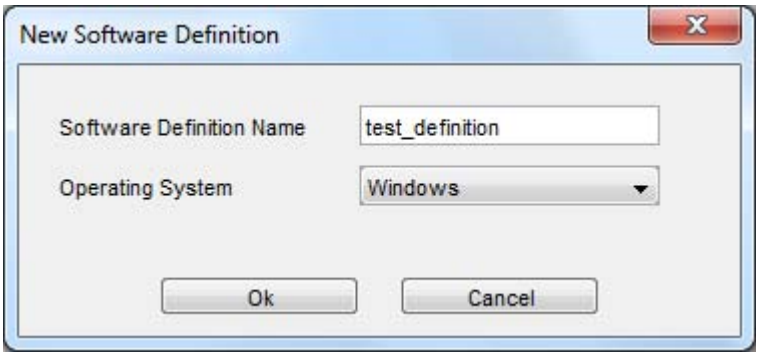
Creating a predefined software definition

Predefined software definitions can be found in the section where all antivirus, firewall and other application SRSs are predefined. The user can select and configure software definitions as desired.

Procedure steps

1. Launch the Avaya EAC Policy Administrator screen.
2. Click the **Predefined Software Definitions** tab, and click the New Software Definition menu icon.

   The New Software Definition dialog box appears.



3. In the **Software Definition Name** field, type a name.

   For example, to create a software definition specifying the antivirus modules that must be present on the client system, type the name Antivirus.

4. In the **Operating System** field, choose the Operating System from the list.
5. Click **OK**.

   The new software definition is added in the Software Definition section.

Mapping predefined software definition to available software definition

Use the following procedure to map a predefined software definition to an available software definition.

Procedure steps

1. Launch the Avaya EAC Policy Administrator screen.
2. Click the **Predefined Software Definitions** tab, and select the name of the predefined software definition entry for which you want to map the available software definition.

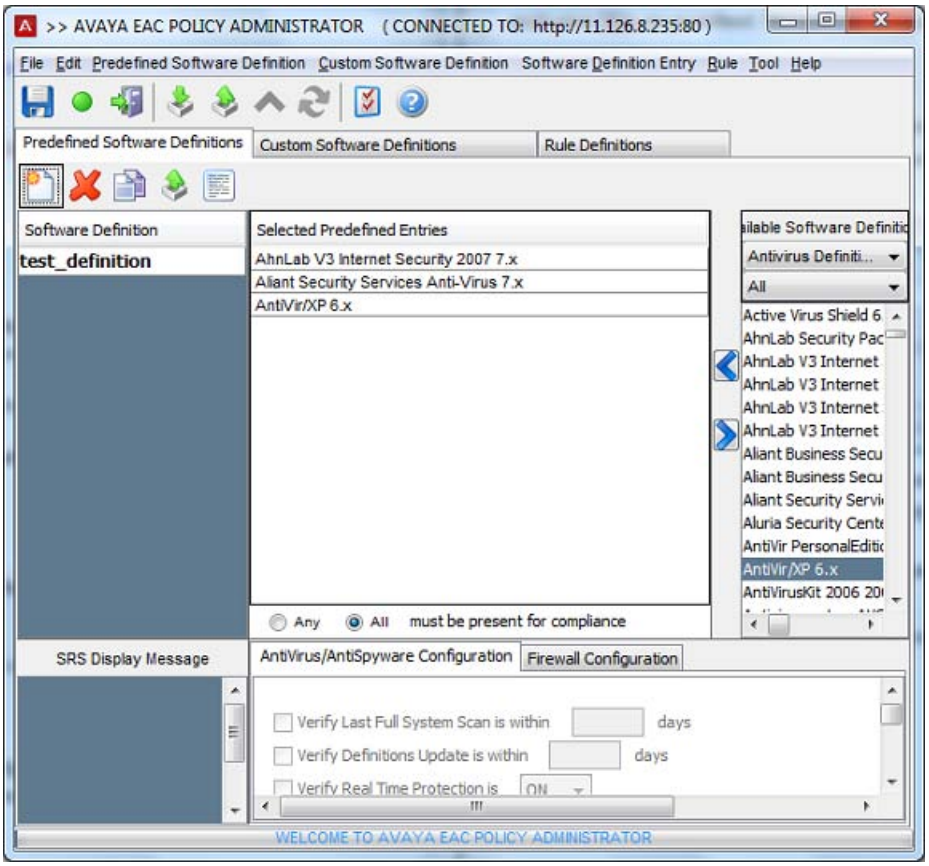


Figure 4: Predefined software definitions

3. From the **Available Software Definition** column on the right pane, choose the software definition.
4. Click **Add Selected Entries (<)** to add the selected software entry.

   The selected software definition entry is added in the Selected Predefined Entries column.
5. Click **Remove Selected Entries (>)** to remove the selected software entry.
6. Choose the **Any** option to validate any of the predefined entries.

   OR

   Choose the **All** option to validate all of the predefined entries.
7. Specify the parameters under the **AntiVirus\Antispyware Configuration** and **Firewall Configuration** tabs for the selected entry.

   Important:
   Depending upon the entry selected, the parameters of the Antivirus/Antispyware Configuration and Firewall Configurations can differ.
8. Click **Save** to save the changes.

Chapter 5: Custom software definition management

Navigation

Management of custom software definition

Once you launch the Avaya EAC Policy Administrator, all processes currently running on the local system, or for Windows Vista and Windows 7, the current user's processes display in the memory snapshot section at the bottom of the screen. Select a process in the left pane of the Memory Snapshot section to display included files and modules on the right pane.

Prerequisites

- You can use the Avaya EAC Policy Administrator to create or modify SRS rules. Creation of SRS rules is not available from the CLI.
- You can use the Avaya EAC Agent quick setup wizard from the CLI, SREM, or BBI to create a test rule, for example, srs-rule-test. You can also subsequently modify these rules with the Avaya EAC Policy Administrator.

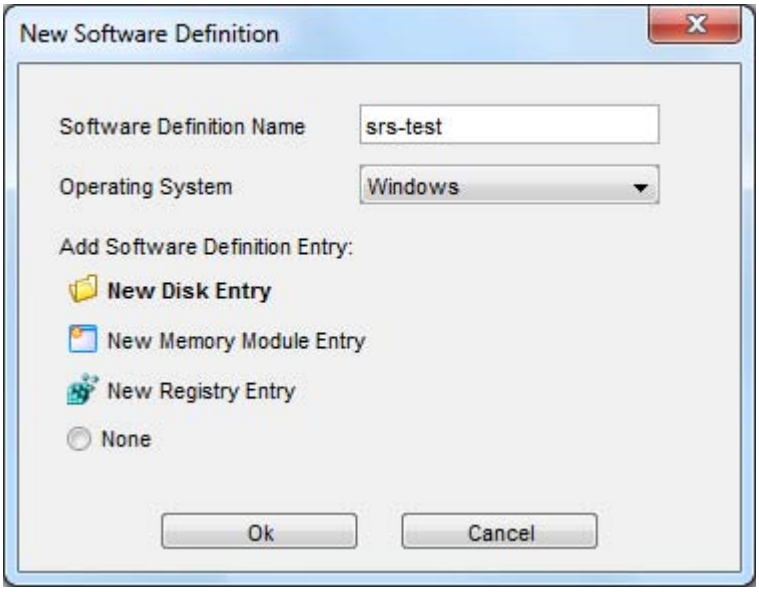
Creating a custom software definition

Create a custom software definition to specify the modules that must be present on the client system.

Procedure steps

1. Launch the Avaya EAC Policy Administrator screen.
2. On the **Custom Software Definitions** menu, select **New Software Definition**.

   The New Software Definition dialog box appears.



3. In the **Software Definition Name** field, type a name.

   For example, to create a software definition specifying the antivirus modules that must be present on the client system, type the name Antivirus.
4. In the **Operating System** field, select the operating system.
5. Click **OK**.

   The new software definition is added in the Software Definition area.

Adding entries to a custom software definition

The following sections describe the various ways you can specify files and software executables to run on the client system.

- Creating a Memory Module entry on page 33
- Creating an On Disk file entry on page 35
- Creating a registry entry on page 37

Important:

The administrator tool applet provides On Disk, Memory Module and Registry Entries buttons to create custom SRS entries and rules for your PC. You must know the name of the executables or files to be checked to create these rules.

Creating a Memory Module entry

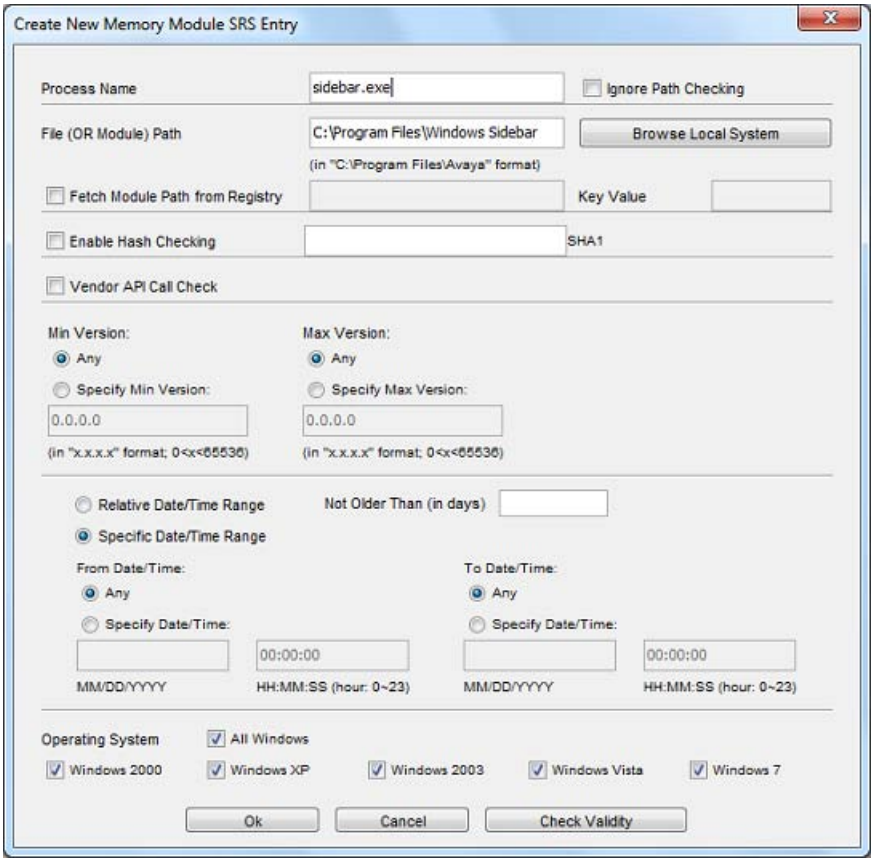
Use the following procedure to create a Memory Module entry for inclusion in the software definition.

Procedure steps

1. Launch the Avaya EAC Policy Administrator screen.
2. On the Custom Software Definition screen, in the **Process** list at the bottom left, select the application or process to include in the software definition.

   All processes that are currently running on your local PC system appear, except for Windows Vista and Windows 7 where the current user's processes are listed. Once you select a process or application, all the associated modules list to the right.
3. On the right pane, under the **Module Path** heading, double-click a module that must be included as an entry in the current software definition.

   The Create New Memory Module SRS window appears.



4. In the **Process Name** field, type the name of the process for which you wish to add the module as a software definition entry.

   The name of the selected process is displayed by default.

5. To ignore path checking, select the **Ignore Path Checking** check box.

   If enabled, the client system searches for the specified file name, irrespective of path to folder.

6. In the **File (OR Module Path)** field, verify that the correct file or module is selected.
7. If you want to add another file or module to the current software definition, click **Browse Local System** and find the desired file.
8. Select the **Fetch Module Path from Registry Entry** check box to fetch the module name from the local registry entry on the PC. In the key path and Key Value fields, type the values. Use this option if a module name varies in other configurations and is available in a registry key.
9. Select the **Enable Hash Checking** check box to enable hash value checking of the current SRS entry.

   Then paste the hash value to be checked in the Hash Value field. The hash value of a selected file/module (if any) is displayed by default.

10. Select the **Vendor API Call Check** check box to invoke a 3rd-party API call for doing additional checking of the software.

    You can use the Avaya EAC Policy Administrator to specify an API that you want to use to check a file, such as an executable. Avaya EAC Policy Administrator supports the use of API calls that check at startup, when the component (for example, an executable or DLL) is launched from a file on disk or during runtime, or when a component is already launched and running in memory.

    For more information, see Making API calls on page 17.

11. In the **Min Version** section, select **Specify Min Version**, and specify a minimum range.

    If there are no restrictions for the minimum version, select **Any**.

12. In the **Max Version** section, select **Specify Max Version**, and specify a maximum range.

    If there are no restrictions for the maximum version, select **Any**.

13. Choose one of the following options:

    - Select the **Relative Date/Time Range** and specify a number in the **Not Older Than (in days)** field.
    - Select the **Specific Date/Time Range** and specify the date/time range for when the file was last created or modified.

14. Choose one of the following options:

    - Select the **From Date/Time** and specify the date in (MM/DD/YYYY) format and time in (HH:MM:SS hour 0~23) format.
    - Select the **To Date/Time** and specify the date in (MM/DD/YYYY) format and time in (HH:MM:SS hour 0~23) format.

Note:

If there are no restrictions for the time, select **Any**.

15. In the **Operating System** section, select the operating system check box. You can select, All Windows, Windows 2000, Windows XP, Windows 2003, Windows Vista and Windows 7)
16. Choose one of the following options:
    - Click **OK** for the file/module to be added as an entry in the selected software definition.
    - Click **Save and More** for the entry to be saved. The Create New Memory Module SRS window remains open for you to add more entries to the current software definition.
    - Click **Check Validity** to check for syntax errors on the defined path. It does not check the actual file.

Note:

The file/module path can include variables such as *<REG>registry key</REG>* so the end user can create a fully customizable file/module path with input from the registry key. For example, you can create the path:

`C:\Program Files\<REG>HKLM\Software\Avaya\EACA\Reg1</REG>\abc.exe`. If registry Reg1 on the PC contains a value "Folder", then path becomes `C:\Program Files\Folder\abc.exe`.

Creating an On Disk file entry

You can use the on disk file entry method to add files that are not shown in the memory snapshot. Select a file from the local file system, for example, a text configuration file, and add it as a software definition entry. You can also add files that are not present on your file system, such as malicious files. By using the NOT operand when forming logical expressions, you can instruct Avaya EAC Policy Administrator to verify that certain files are not present on the client system.

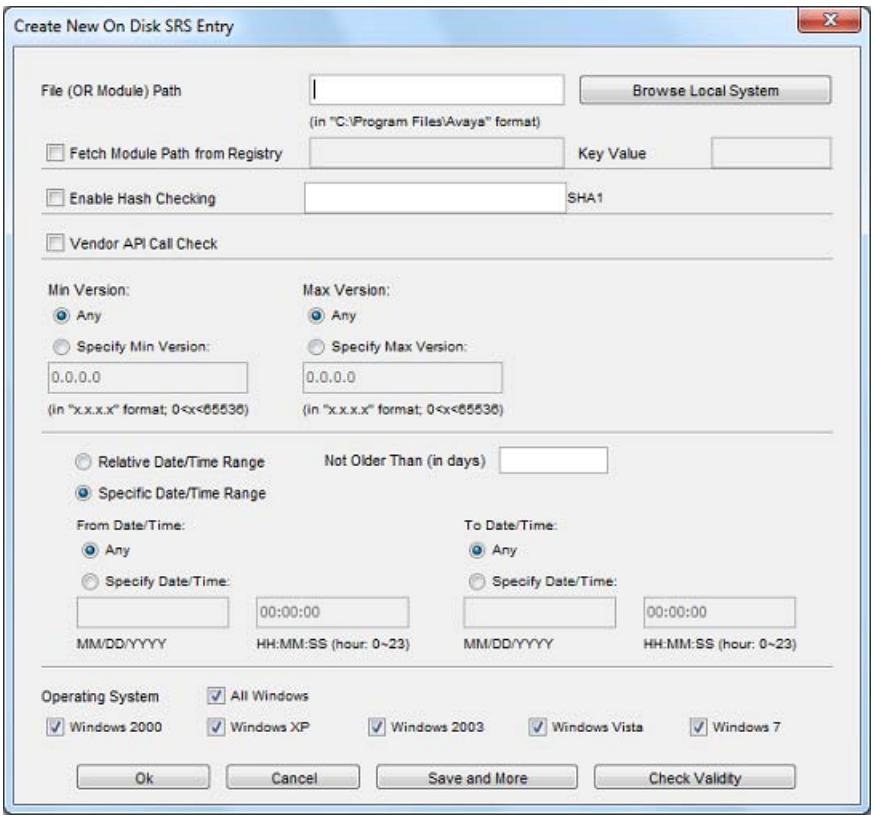
Use the following procedure to create a software definition entry for a file that is not shown in the memory snapshot.

Procedure steps

1. Launch the Avaya EAC Policy Administrator screen.
2. On the Software Definition Entry menu, select **New Disk Entry**.

   To include the file in a new software definition, first create the new software definition (select New Software Definition from the Software Definition menu).

   The Create New On Disk SRS Entry window appears, as shown in the following figure.



3. In the **File (OR Module Path)** field, type the path to the file.

   OR

   Click **Browse Local System**, to add a file from your local system.

4. Select the **Fetch Module Path from Registry Entry** check box to fetch the module name from the local registry entry on the PC.

   In the key path and Key Value fields, type the values. Use this option if a module name varies in other configurations and is available in a registry key.

5. Select the **Enable Hash Checking** check box to enable hash value checking of the current SRS entry.

   Paste the hash value to be checked in the Hash Value field. The hash value of a selected file/module (if any) displays by default.

6. Select the **Vendor API Call Check** check box to invoke a 3rd-party API call for additional checking of the software.

7. Specify the desired limitations regarding version and file age.

8. In the **Min Version** section, select **Specify Min Version**, and specify a minimum range.

   If there are no restrictions for the minimum version, select **Any**.

9. In the **Max Version** section, select **Specify Max Version**, and specify a maximum range.

If there are no restrictions for the maximum version, select **Any**.

10. Choose one of the following options:
    - Select the **Relative Date/Time Range** and specify a number in the **Not Older Than (in days)** field.
    - Select the **Specific Date/Time Range** and specify the date/time range.
11. Choose one of the following options:
    - Select the **From Date/Time** and specify the date in (MM/DD/YYYY) format and time in (HH:MM:SS hour 0~23) format.
    - Select the **To Date/Time** and specify the date in (MM/DD/YYYY) format and time in (HH:MM:SS hour 0~23) format.

    Note:
    If there are no restrictions for the time, select **Any**.
12. In the **Operating System** section, select the operating system check box. You can select all check boxes (Windows, Windows 2000, Windows XP, Windows 2003, Windows Vista and Windows 7)
13. Choose one of the following options:
    - Click **OK** for the file/module to be added as an entry in the selected software definition.
    - Click **Save and More** for the entry to be saved. The Create New Memory Module SRS window remains open so you can add more entries to the current software definition.
    - Click **Check Validity** to check for syntax errors on the defined path. It does not check the actual file.

    Note:
    The file/module path can include variables like *<REG>registry key</REG>* so the end user can create a fully customizable file/module path with input from the "registry key". For example, you can create the path:

    `C:\Program Files\<REG>HKLM\Software\Avaya\EACA\Reg1</REG>\abc.exe`. If registry Reg1 on the PC contains a value "Folder", then the path becomes `C:\Program Files\Folder\abc.exe`.

Creating a registry entry

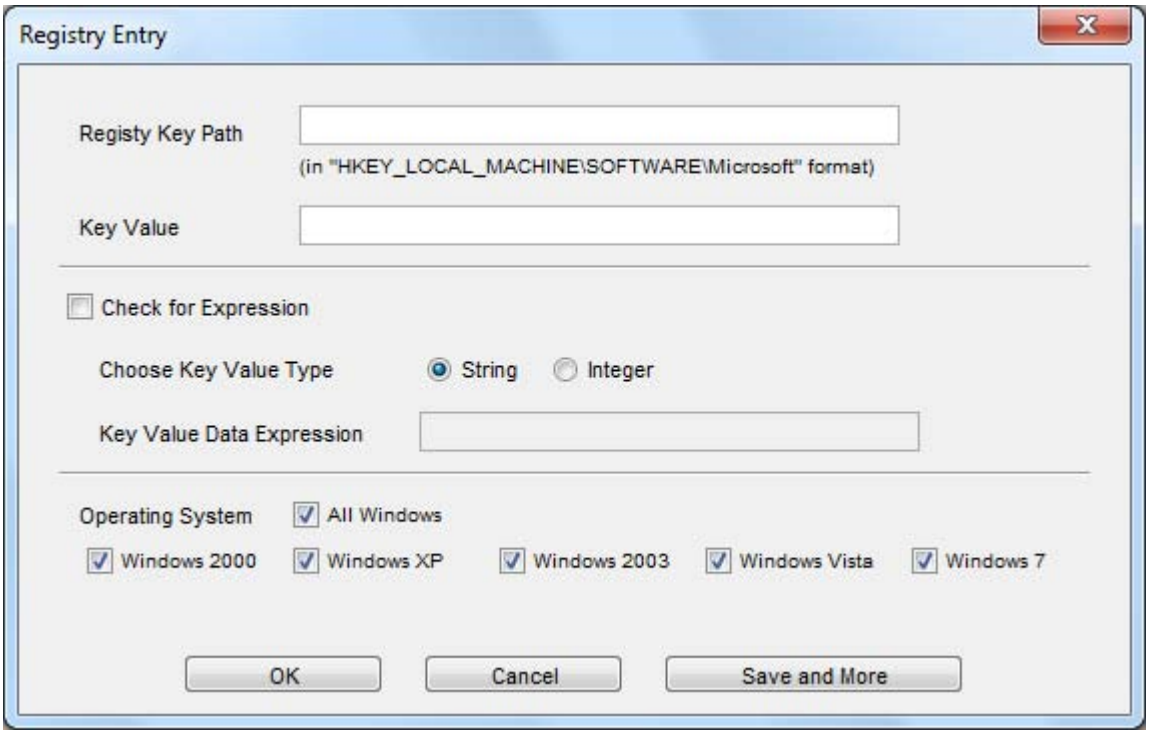
Use the following procedure to create a registry entry for inclusion in the software definition.

Procedure steps

1. Launch the Avaya EAC Policy Administrator screen.
2. Click the **Software Definitions** tab.

3. From the **Software Definition Entry** menu, choose **New Registry Entry**.

   The Registry Entry dialog appears.



4. Select the **Registry Key Path** from the Registry Editor.
5. Select the **Key Value** type.
6. Type the **Key Value Data Expression**.
7. Click **OK**.

   OR

   Click **Save and More** for the entry to be saved. The Registry entry windows remains open for you can add more entries.

Creating Rules for 64 bit architectures

Avaya Endpoint Access Control (EAC) Administrator supports 64 bit platforms starting with version 5.3 released with Avaya VPN Gateway v8.0.5. For AVG upgrade procedure, please refer to VPN Gateway - Administrator Guide document.

Note:

The full path of a disk entry or a registry entry must be provided when creating a rule. Paths in rules must be **explicit**.

Not all paths on 64 bit platforms exist on 32 bit platforms. See the following examples of installing an application, called ”MyApp.exe”.

1. 32 bit application

    a. On 32 bit Operating System

    - Install Path: *C:\Program Files\MyCompany\MyApp.exe*
    - Registry Key: *HKEY_LOCAL_MACHINE\Software\MyCompany*

    b. On 64 bit Operating System

    - Install Path: *C:\Program Files (x86)\MyCompany\MyApp.exe*
    - Registry Key: *HKEY_LOCAL_MACHINE\Software \WOW6432Node\MyCompany*

2. 64 bit application

    On 64 bit Operating System

    - Install Path: *C:\Program Files\MyCompany\MyApp.exe*
    - Registry Key: *HKEY_LOCAL_MACHINE\Software\MyCompany*

Note:

Rules must be **specific** for each architecture, otherwise the rule fails. You must be aware of what type of system the rule checks.

Avaya EAC Agent does not include built-in rules for 32 bit/64 bit platform checks. You must define the 32bitOSCheck and 64bitOSCheck rules by defining Registry check rules. You can define 32 or 64 bit by checking the Registry entries under HKLM\HARDWARE\DESCRIPTION \System\CentralProcessor. Please refer to Microsoft KB for more details: http://support.microsoft.com/kb/556009

The following are examples of how to create specific rules for each platform.

1. Enforce an SRS Rule **My32bitRule** on 32 bit only:

    Rule Expression: (**My32bitRule** AND 32bitOSCheck) OR (64bitOSCheck)

    Explanation: Avaya EAC Agent enforces **My32bitRule** checking on 32 bit platform only and will bypass the check on 64 bit platforms.

2. Enforce an SRS Rule **My64bitRule** on 64 bit only:

    Rule Expression: (**My64bitRule** AND 64bitOSCheck) OR (32bitOSCheck)

    Explanation: Avaya EAC Agent enforces **My64bitRule** checking on 64 bit platform only and will bypass the check on 32 bit platforms.

3. Enforce an SRS Rule **MyGeneralRule** on both 32 bit and 64 bit platforms:

    Rule Expression: **MyGeneralRule**

Explanation: Avaya EAC Agent enforces **MyGeneralRule** checking on both 32 bit and 64 bit platforms.

The following two examples describe how to configure rules for 64 bit platforms.

- Generate an SRS rule for an application (MyApp.exe) that runs as a 32-bit program on 32-bit platforms and a 64-bit program on 64-bit platforms, and enforce the rule on both 32 bit and 64 bit platforms.

  The rule can be defined as:

  CheckMyApp

  where **CheckMyApp** checks for existence of “C:\Program Files\MyCompany \MyApp.exe”

- Generate an SRS rule for an application (MyApp.exe) that runs as a 32 bit program on 32 bit platforms and also as a **32 bit** program on 64 bit platforms and enforce the rule on both 32 bit and 64 bit platforms.

  The rule can be defined as:

  (CheckMyAppOn32 AND 32bitOSCheck) OR (CheckMyAppOn64 AND 64bitOSCheck)

  where

  CheckMyAppOn32 checks for existence of “C:\Program Files\MyCompany\MyApp.exe”

  CheckMyAppOn64 checks for existence of “C:\Program Files (x86)\MyCompany \MyApp.exe”

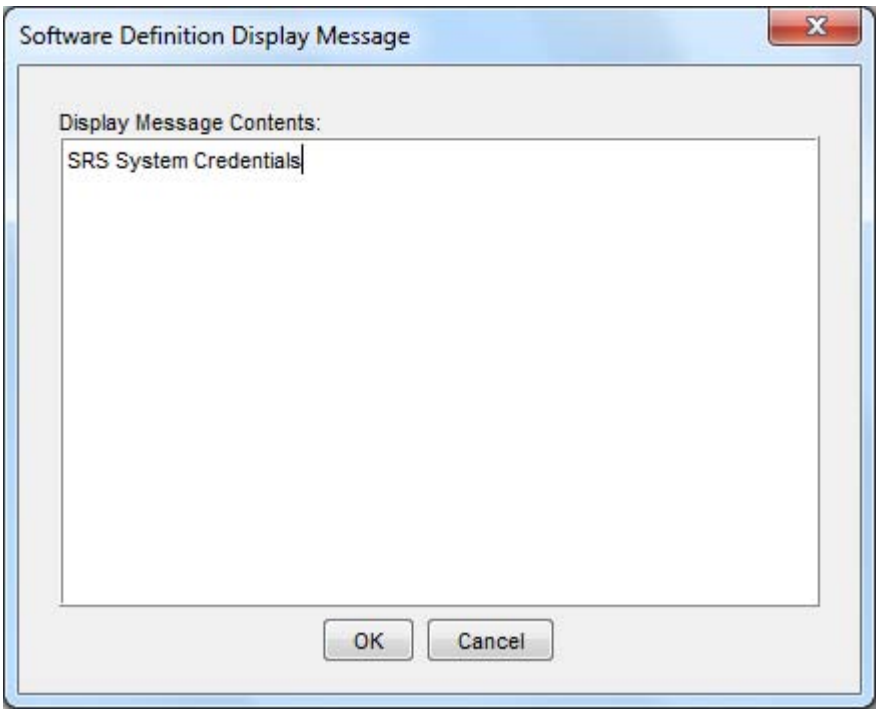
Adding a software definition display message

Use the following procedure to add a custom software definition display message to display Software Definition specific messages to the end user.

Procedure steps

1. Launch the Avaya EAC Policy Administrator screen.
2. Click the **Custom Software Definition** tab.
3. From the **Custom Software Definition** menu, choose **Edit Software Definition Display Message**.

   The Software Definition Display Message window appears.



4. Type a message, and click **OK**.

Deleting SRS rules and their components

To delete SRS rules and component elements use one of the following procedures.

- Deleting a custom software definition on page 41
- Deleting a custom software definition entry on page 42

Deleting a custom software definition

Use the following procedure to delete a custom software definition from the existing software definitions.

Procedure steps

1. Launch the Avaya EAC Policy Administrator screen.
2. Click the **Custom Software Definition** tab.
3. In the **Custom Software Definition** column, select the desired software definition.
4. Click the Delete Software Definition symbol on the Custom Software Definition tool bar.

Important:

You cannot delete a custom software definition if it is used in a Rule. You must first delete the Rule.

Deleting a custom software definition entry

Use the following procedure to delete a custom software definition entry. A software definition entry is a file that lists on the right pane of the Software definition tab (for example, a file that is included in the current software definition).

Procedure steps

1. Launch the Avaya EAC Policy Administrator screen.
2. Click the **Custom Software Definition** tab.
3. In the **Software Definition** column, select the required software definition.
4. On the right pane, select the software definition entry.
5. Click the **Delete** symbol on the Custom Software Definition toolbar.

Chapter 6: Rule definition management

This chapter provides detailed procedures on how to configure Rule definitions.

You can assign Rule definitions to software definitions and use Rule definitions to create logical expressions.

Navigation

Creating logical expressions

Use the following procedure to create a logical expression that specifies an SRS rule which comprises a number of different requirements.

Important:

Rules automatically create if the autogenerate rule is selected. The autogenerate rule is selected by default. You can clear the autogenerate rule by selecting Edit > Preferences and clearing the checkbox.

Procedure steps

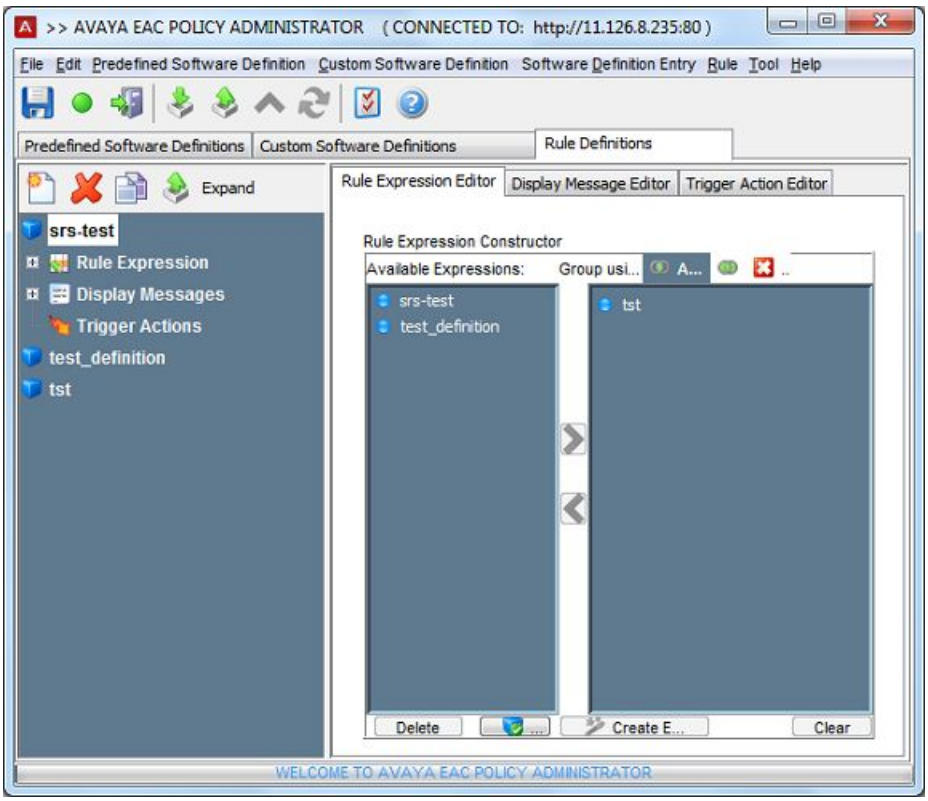
1. On the Avaya EAC Policy Administrator screen, click the **Rule Definitions** tab.

   Important:

   Create the desired software definitions.

   For example, you can create a software definition for an antivirus program, another one that identifies a certain executable and a third one that identifies a certain dll file. For instructions on how to create a software definition, see Creating a custom software definition on page 31.

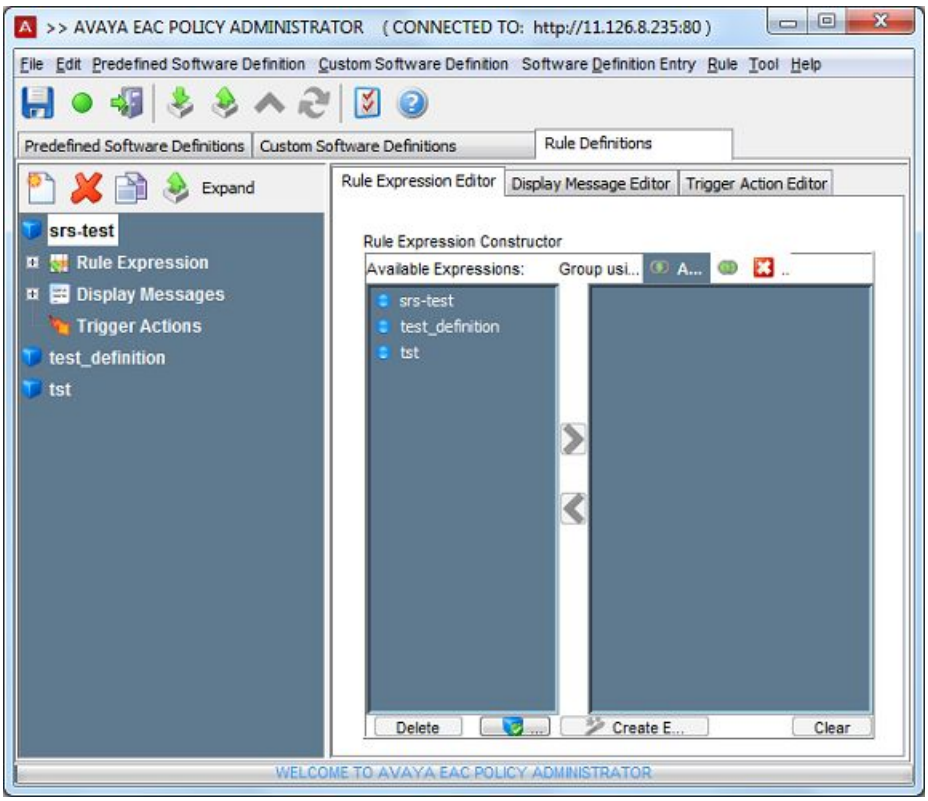
   Rules and expressions with the same names as the software definitions are created and appear on the **Rule Definitions** tab.



In the preceding figure, two Avaya EAC Policy Administrator rules are created, each defining an unique application. To create one Avaya EAC Policy Administrator rule comprising both applications, you must start by creating a new logical expression.

2. Click the **Rule Expression Editor** tab.

   A new expression is created and copied to the Available Expressions area.



3. In the **Available Expressions** section, select the expression, and click the right arrow.

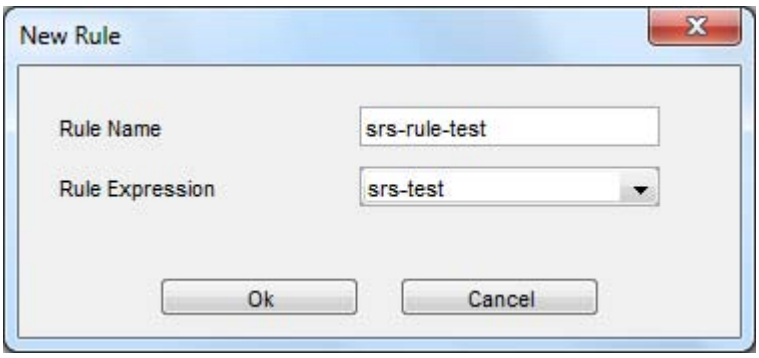
   The expression is copied to the Rule Expression Constructor table.

4. Choose another expression to form a new logical expression in combination with the first.
5. In the **Group Using** section, choose from the options **AND**, **OR**, or **NOT**.

   For example, you can use the AND expression to construct a logical expression where both conditions must be met for the Avaya EAC Policy Administrator checks to pass. You can use the OR expression to construct an expression where either of the conditions must be met for the Avaya EAC Policy Administrator checks to pass. You can use the NOT operand to construct an expression where the condition must not be met for the Avaya EAC Policy Administrator checks to pass. For example, the file or files in the software definition must not be found on the client systems.

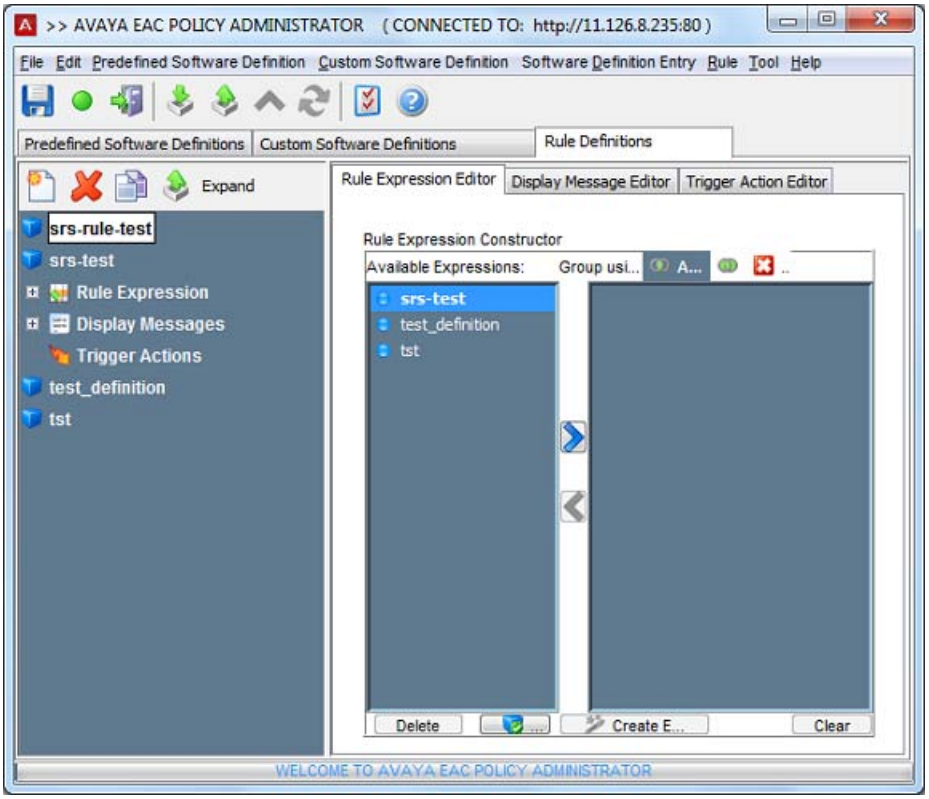
6. Press the "Create Expression" button to combine the selected software definitions.
7. On the Rule menu, choose **New Rule**.

   The New Rule window appears.



8. In the **Rule Name** field, type a name for the Rule.
9. In the **Rule Expression** field, choose a Rule Expression from the list.
10. Click **OK**.

    The new rule name appears in the Rule Name column.



11. Click the **Rule Expression Editor** tab.
12. Choose the expression you want to associate with this rule.

    You can use any logical expression you create in a new logical expression, for example, to construct more complex conditions.
13. Click **Assign to Rule**. You can add multiple SRS or expressions in one **AND** or **OR** expression. You can only choose one expression/srs to create a **NOT** expression.

Deleting an expression

Use the following procedure to delete an expression and remove an expression from the Available Expressions area.

Procedure steps

1. On the Avaya EAC Policy Administrator screen, click the **Rule Definitions** tab.
2. In the **Available Expressions** section, select the expression, and click **Delete**.

Important:
You cannot delete an expression if it is used in a Rule.

Adding a display message to a Rule

Use the following procedure to add a display message Rule to appear on the portal page and the Avaya EAC Agent pop-up window on a rule failure. You can include URLs, email, and ftp links in the display message to assist the user with rule failure remediation.

Procedure steps

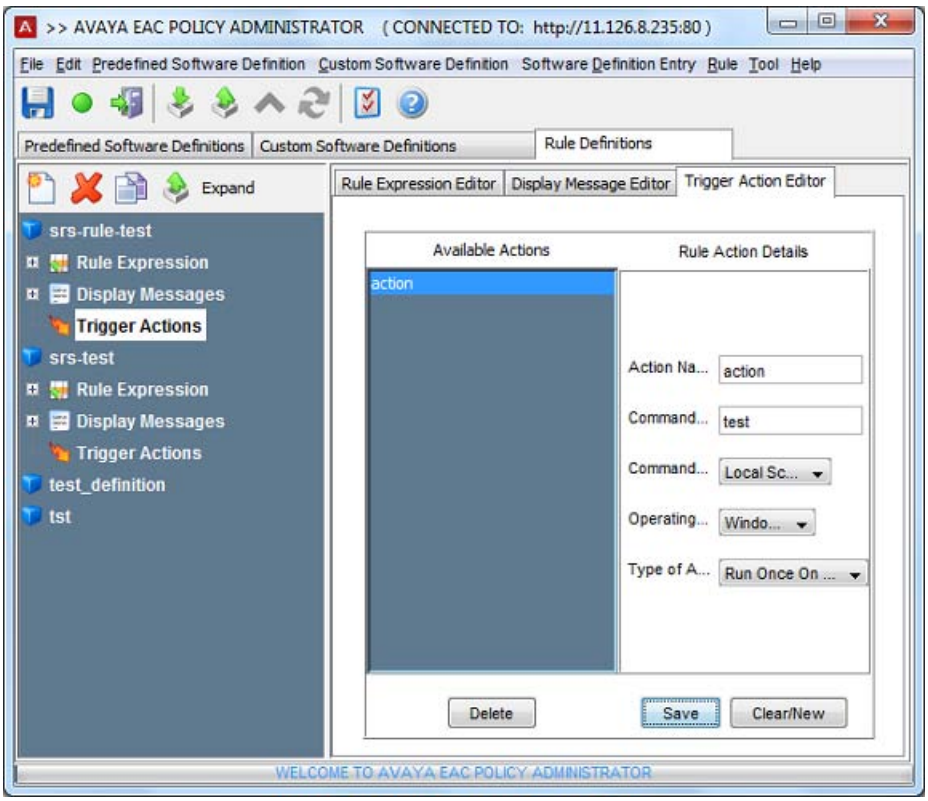
1. Launch the Avaya EAC Policy Administrator screen.
2. Click the **Rule Definitions** tab.
3. Select rule you want to add a Display Message to.
4. Click the **Display Message Editor** tab.
5. In the Display Message Contents section, type the message text.
6. Click **Set**.

Configuring trigger action

Use the following procedure to configure a trigger action for the selected rule and edit the command type and type of action for the rule.

Procedure steps

1. On the Avaya EAC Policy Administrator screen, click the **Rule Definitions** tab, and the **Trigger Action Editor** tab.



2. Complete the Rule Action Details section.
3. Click **Save**.

   The created action appears in the Available actions section.

Variable definitions

Use the data in the following table to set the trigger action.

Variable	Value
Action Name	Specifies the action name.
Command Text	Specifies the name of the executable or batch file to run, along with arguments to pass onto the executable. The executable must be available on the PC that rules are executed on either locally or available over the network. Values: enabled and disabled. The default is disabled.
Command Type	Specify the command type. Values: Local Script
Operating System	Specify the operating system. Values: Windows
Type of Action	Specify the type of action. Values: Run Once On Success and Run Once On Failure.

Variable	Value
	Run Once On Success—This action executes only once, after compliance success and vlan transition (if any). **Run Once On Failure**—This action executes only once on compliance failure and vlan transition (if any). You can configure only one action of each type for a particular rule.

Deleting a Rule

Use the following procedure to delete a rule and remove an Avaya EAC Agent Rule name.

Procedure steps

1. Launch the Avaya EAC Policy Administrator screen.
2. Click the **Rule Definitions** tab.
3. Select the rule to delete in the left pane, and click the delete symbol on the Rule Definitions toolbar.

Note:
You cannot delete a Rule if it is assigned to a group. Remove the assignment first.

Index