SOA Software Platform 7.0 Release Notes

SOA | software™

SOA Software Platform 7.0

Release Notes
SOA_Platform_Release_Notes_v1

Copyright

Trademarks

SOA Software, Inc.

SOA Software, Inc.
12100 Wilshire Blvd, Suite 1800
Los Angeles, CA 90025
(866) SOA-9876
www.soa.com
info@soa.com

Disclaimer

Contents

SOA Software Platform 7.0 Release Notes

The SOA Software Platform from SOA Software™ delivers security and management for XML and Web services. Web services and Service Oriented Architectures offer a promise of enabling a truly agile enterprise through service reuse and flexible application deployment. The transition to a distributed, loosely coupled application and integration architecture requires a management and security fabric. Without this fabric, many of the advantages of Web services and Service Oriented Architectures are lost.

This Release Notes document provides a summary of the changes that have taken place in the SOA Software Platform 7.0 and other associated utilities and subsystems in this release including:

- New features added to the product.
- Documentation enhancements.

What's New in 7.0?

SOA Software Platform 7.0 Features

The SOA Software Platform 7.0 release includes the following new or updated features:

64-Bit Support

The SOA Software Platform 7.0 Release supports 64-bit setup executables only. If your current SOA Software Platform deployment is running on a 32-bit machine, contact SOA Software Customer Support.

System Requirements

- Windows
  - Windows 2008
  - Windows 7
- Linux
  - Red Hat Enterprise Linux 5.2, 5.8, 6.2
- Solaris
  - Solaris 10, 11
- IBM AIX
  - AIX 5.2 and 5.3
- Database Support
  - Oracle 10g, 11g

  - Microsoft SQL Server 2008, 2012
  - IBM DB2 Universal Database V9.7, V10.5
  - MySQL 5.1
- Browser Support
  - IE 7.0, 8.0, 9.0
  - Mozilla Firefox 10+ and above
  - Google Chrome v17 and above

Processes

SOA Software introduces the new Process interface with the 7.0 release. In the Management Console, each new Organization now includes a *Processes* folder and each virtual service operation includes a *Process* and *Fault* tab.

The Process functionality allows you to define web service orchestration concepts using an XML-based graphical editor called the Process Palette. You can define the sequence of messages as they flow through Policy Manager for each virtual service operation and configure a variety of different "Activities" for achieving the results required for each operation.

A process is an ordered graph of activities that can be performed by a container that supports the virtualization capability, like the Network Director. The logic performed in a virtual service operation is defined as a process. When a message is received by the container, once the virtual service operation is identified, its process is executed. As dictated by the activities in the process, down-stream services may be invoked. As a result of process execution, a response to the original message is generated.

The new interface includes the following components:

Process Editors

- Process Editor

  The Process Editor allows you to create a process in a graphical drag-and-drop environment. The process begins by receiving a message (see the Receive Activity) and the process ends when a message is returned (see the Reply Activity) to the caller.

- Fault Sequence Editor

  The Fault Sequence Editor works exactly like the main Process Editor except that the sequence does not need to begin with a Receive Activity. The Receive from the external client has already been executed in the main process. At this point we are just executing activities within the same process context.

  When the fault sequence is executed, the reserved variable name “fault” will contain the fault message that is triggering the sequence. Activities that reference variables can use this fault variable.

- Variable Editor

  The Variable Editor is an interface for defining variables that can be used in the process. Variables can be used in different activities to dictate behavior, such as using a variable to identify the

endpoint of a service to invoke. Variables can also be used to store the output from web service invocations or provide input to web service invocations.

A variable is identified by a name and defined by a type, or syntax. The types recognized by the system are message (used for input or output of a web service invocation, request, or reply activity), string, int, long, boolean, float, or any (can hold any content). Activities that support the use of variables in their configurations will often restrict the use of variables based on type. Optionally a default value can be given to a variable. If there is a default, at the beginning of process execution the variable will be given that value.

Process Activities

The activities available to be called from within a process are available on an Activity Palette located on the upper left hand side of the editor graph. An activity icon in the palette can be selected and dragged on to the process editor graph. Activities are called in order and are linked together by directional connectors. To link two activities select the middle of the activity that will be executed first. A circle with an error should appear.

- Receive Activity

  The Receive Activity provides the entry point into the process. The caller will invoke the process by providing it with a message. That message will be stored in the variable selected in the activity's configuration screen. Only variables of type message can be used. There can only be one Receive activity in a process.

- Reply Activity

  The Reply Activity provides the exit point from a process. Every flow through the process must have one and only one Reply Activity. This means if there are multiple branches created from a Branch Activity, each branch must be terminated with a Reply Activity. The Reply Activity can return a message to the caller. It is not required for one-way operation processes. Only variables of type message can be used.

- Invoke Activity

  The Invoke Activity invokes the operation of a service registered in the system. The operation is invoked by sending a message that is specified as an input variable to the activity. The response from the operation invocation is stored in an output variable. The input and output variables can both be the same variable.

- Script Activity

  The Script Activity provides the ability to execute a script at the point in the process the activity is connected. The script can be written in either JavaScript, Jython, or BeanShell. The Script Activity includes a Script Details Editor that is organized into two separate areas, Imports and Source. The Source has a pull-down where you can select the script language. It also has a large source code editor text area.

- Branch Activity

  The Branch Activity provides a mechanism to have alternate process flows, or branches, based on boolean conditions. Drop the Branch Activity on the Process page and connect the last activity to be executed before the branch to the Branch Activity.

- Transformation Activity

  The Transformation Activity provides a mechanism for transforming XML message or string content. The transformation is based on XSLT. The input to the activity can be a message or string variable. The transformed content will replace the input variable content at the completion of the activity.

- Audit Activity

  The Audit Activity provides a mechanism for auditing a message. The audited message content is recorded and displayed as audited message content from an Auditing Policy. This information displays on the Monitoring pages of a service (i.e., Services > Monitoring). The input to the activity can be a message variable.

- Insert Content Activity

  The Insert Content Activity can be used to fill the content of a String or Message variable. The source of the content can be either statically defined content or an existing variable.

  You can define a filter using a filter expression written in a selected language. The languages supported are XPath (for XML content), JSONPath (for JSON content), or Regular Expression (for any content). The result of the filter expression applied to the input variable will be inserted. It is possible that the filter expression results in multiple elements or properties being used as input.

- Process Activity

  The Process Activity allows you to call one process from another so that you can create processes with common activities and then call those processes at an appropriate point of another process. These processes with common activities are reusable and are organized in the Processes folder of each Organization in the Policy Manager Workbench. Reusable processes can themselves have Process activities so that they can call other reusable processes.

Process Tools

The Processes interface includes a wide variety of tools to help you manage process definitions, download stored processes, export processes, save process to a database, manage activity definitions, and view process references. The SOA Software Documentation Repository (docs.soa.com), includes a topic called "Process Management" that describes all the available tools.

Scripts

- SOA Software introduces the new Scripts interface with the 7.0 release. In the Management Console, each Organization now includes a *Scripts* folder.

  The Script functionality allows you to define common functions that you may need to perform in Script objects using the **Add Script** function. You can make use of these common functions in a process Script Activity or in a QoS Script Policy.

  To make use of those common functions from the Script Activity or Script Policy the Script objects defining those functions must be imported. The Imports area is where those scripts are identified for import. The available scripts are listed in the Available Scripts tree. Any number of Scripts in that tree can be moved to the Imported Scripts list box. Only scripts that match the language type will be available for selection in the tree. The script does not return a value.

Service Management

- Service Creation Option Changes

  The service creation option in the **Create Physical Service** and **Create Virtual Service** service management functions have been simplified as follows:

  - *Create service from WSDL* option has been renamed to *Create Using WSDL*.
  - *Model service using interfaces* option has been renamed to *Create Using Existing Interfaces*.
  - *Create service from schema* option has been removed and functionality has been migrated to *Create Without Using WSDL*.
  - *Create service without WSDL* option has been replaced with *Create Without Using WSDL*.

Note: The *Virtualize existing service* option in the Create Virtual Service Wizard remains unchanged.

- Configure Policy Processing / Manage Header Propagation

  The Configure Policy Processing and Manage Header Propagation function on the Service Details Actions portlet have been removed and combined into a new function "Configure Message Processing."

Containers

- Configure Container Instance Wizard

  The Configure Container Instance Wizard now allows you to specify a custom container key when defining your instance name. If a custom key is not specified the system automatically assigns a key.

- Dynamic Container Listeners

  The container listener implementation has been upgraded and now supports dynamic listeners. This allows you to build Policy Manager plug-ins for custom listener types that can be added to the "Add Container Listener" drop-down.

Policies (New)

Threat Detection

- Message Threat Policy

  The "Message Threat Policy" is used to guard against XML based denial of service attacks. An attacker can construct XML messages in such a way that parsing them could result in overwhelming CPU and/or memory consumption. This policy can detect such situations and reject the messages immediately.

- Cross Site Scripting Detection Policy

  The Cross Site Scripting Detection Policy is an Operational policy that allows you to block potentially malicious HTML tags in the request message body using what is called a white list of tags.

- Anti-Virus Policy

The "Anti-Virus Policy" is used to direct the scanning of messages for viruses. The Network Director itself does not scan for viruses. Instead it off-loads the virus checking to an anti-virus server. The Network Director communicates with an anti-virus server using the Internet Content Adaptation Protocol (ICAP) protocol. The Anti-Virus policy dictates what messages should be scanned, how to communicate with the anti-virus server, and what action should be performed when a virus is detected.

- HTTP Malicious Pattern Detection Policy

  The "HTTP Malicious Patterns Detection Policy" is used to inspect the HTTP messages for content that could be considered dangerous to an API or web service, and reject the message returning a fault if any of the defined expressions match the content.

- WS- Malicious Pattern Detection Policy

  The "WS-Malicious Pattern Detection Policy" is very similar to the HTTP Malicious Pattern Detection Policy except that it is tailored for SOAP messages. In particular, the SOAP body and SOAP headers can be handled differently. You can use the WS-Malicious Pattern Detection Policy for SOAP message (transmitted over HTTP) but the envelope has no special meaning and would be treated as any XML content.

Schema Validation

- WS-Schema Validation / Schema Validation Policies

  A common integration problem in an SOA occurs when consumers send messages to services that don't conform to the services' message schemas. Typically this is caused by the versioning of a service's schema and a consumer sending message defined in the prior schema version. However it can also be a consumer's malicious attempt to cause a denial of service by sending invalid messages to a service. An SOA Container can aid by validating the messages exchanged between the consumers and services against the service's published schema.

  Configuring the SOA Container to perform schema validation of messages is performed by the definition of schema validation policies. The WS-Schema Validation and Schema Validation policies indicate which messages to validate.

Paging

The Paging Policy is designed to allow a client to only get a subset of a list based response. For example, if an operation is returning a list of books, and the full list is 1000 books, the client may wish to only have 100 books be returned at a time. The policy applies to both SOAP and Restful (XML) services. When the policy is attached to an operation the client can request subsets of the list.

Monitoring

- Metrics Policy

  The Metrics Policy is an Operational policy that allows you to collect roll-up data for selected services/operations that the policy is attached too. A Metrics Policy is useful for:

- **Database Space Conservation** - Roll-up data on a large number of services can take up a significant amount of database space. Designating specific services/operations where roll-up data will be captured reduces the chance of receiving out of memory database exception errors.
- **Granular View of Service Activity** - You may have a set of services that include specific operations you want to monitor at a more granular level (i.e., track service level, volume of activity, etc.).

Policies (Updates)

HTTP Security Policy

The "HTTP Security Policy" includes the following new functionality in the Modify HTTP Security Policy Wizard:

- **Cookie Response:** The "Add Cookie Response" screen allows you to add a cookie to be included in the outgoing service response. The "Modify Cookie Response" screen allows you to update the cookie response definition.
- **Generate Security Audit Data:** Captures success and failure audit data for all message exchanges.
- **Audit on Error Only:** Captures audit data only when an error occurs on a message exchange.

Authentication Policy

The "Authentication Policy" includes the following new auditing options in the Modify Authentication Policy" popup.

- **Generate Security Audit Data:** Captures success and failure audit data for all message exchanges.
- **Audit on Error Only:** Captures audit data only when an error occurs on a message exchange.

Authorization Policy

The "Authorization Policy" includes the following new auditing options in the Modify Authorization Policy" popup.

- **Generate Security Audit Data:** Captures success and failure audit data for all message exchanges.
- **Audit on Error Only:** Captures audit data only when an error occurs on a message exchange.

WS-Security Supporting Tokens Policy

The "Specify SAML Token Options" screen in the WS-Security Supporting Tokens Policy Wizard has been enhanced and now allows you to specify required claims by specifying a Claim URI.

Upgrades

- The SOA Software Platform Release supports upgrading from Policy Manager 6.1 to 7.0. Download the Policy Manager 6.1 to 7.0 Upgrade Technical Note from the SOA Software Customer Support Site (`https://support.soa.com/support`) under PolicyManager> PM70, or from the SOA Software Documentation Repository (docs.soa.com).

  Note: If you have not upgraded to Policy Manager 6.1, and have Policy Manager 6.0 or earlier, you will need to upgrade to Policy Manager 6.1 first, and then perform the 6.1 to 7.0 upgrade. Contact SOA Software Customer Support for assistance in assessing your required migration plan.

Documentation

- SOA Software Documentation Repository (docs.soa.com)

  SOA Software offers a new documentation repository website (docs.soa.com). The repository provides a centralized storage solution for SOA Software's Community Manager, API Gateway (Policy Manager, Network Director, Agents), and LifeCycle Manager product offerings. The repository is designed to provide quick access to installation, configuration, concept, and usage documentation through use of the search facility. Documentation is accessible in either PDF format (downloadable), or HTML (view / print).

  A subset of Policy Manager 7.0 documentation is currently available on the site, and we will be continually migrating online help documentation content, existing PDF guide documentation, and Technical Notes that are currently available on the SOA Software Customer Support site to the repository site over the coming months.

- Policy Manager Online Help
  - Product help has been updated to reflect the new Policy Manager 7.0 functionality. Context sensitive help can be launched from any screen in the Management Console via the upper right Help button, Question Mark icon located on portlets, or the Help button in wizards. The help can also be launched in standalone mode by launching "welcome_to_service_manager.htm" in the docs\UsersGuide folder in the Policy Manager Release Directory.
- SOA Software Platform Installation Guide
  - This guide provides instructions for installing and configuring Policy Manager 7.0 for Windows and UNIX platforms. The installation process is implemented via a platform-specific setup file that loads the "SOA Software Platform Installation Wizard." The configuration process is performed using the "Configure Container Instance Wizard" and the "SOA Software Administration Console." Silent installation and configuration instructions are also included. You can download this guide from the SOA Software Customer Support Site (`https://support.soa.com/support`) under PolicyManager> PM70, or from the SOA Software Documentation Repository (docs.soa.com).
- Policy Manager 6.1 to 7.0 Upgrade Technical Note
  - This technical note provides instructions for upgrading Policy Manager 6.1 to Policy Manager 7.0. You can download this guide from the SOA Software Customer Support Site (`https://support.soa.com/support`) under PolicyManager> PM70, or from the SOA Software Documentation Repository (docs.soa.com).
- Policy Manager API

  - The *Policy Manager API* is located in the **\sm70\docs\apiDocs** folder of the Policy Manager 7.0 Release Folder and provides a series of interfaces and classes you can use to build extensions to the Policy Manager product. You can also access it on docs.soa.com.
- Policy Manager Scripting API
  - The *Policy Manager Scripting API* is located in the **\sm70\docs\scriptDocs** folder of the Policy Manager 7.0 Release Folder and provides a series of interfaces and classes you can use to build process related scripts. You can also access it on docs.soa.com.
- Other Documentation

  The following product documentation is also available and can be downloaded from the SOA Software Customer Support Site (`https://support.soa.com/support)` under PolicyManager> PM70, or from the SOA Software Documentation Repository (docs.soa.com).

  - Policy Manager 7.0 Message Handler Programming Guide
  - Policy Manager 7.0 Delegate for Apache Axis
  - Policy Manager 7.0 Custom Actions
  - SOA Software Policy Manager Data View Description

Distribution and Installation

- SOA Software Platform Manager 7.0 provides a platform-based distribution approach for Windows, and UNIX (Linux, Solaris, and AIX) software versions. Setup files can be directly downloaded from the SOA Software Customer Support Site under PolicyManager > PM70.

Customer Support

SOA Software offers a variety of support services by email and phone. Support options and details are listed below.

Support Option	Details
Email	• support@soa.com • The Support section of the SOA Software website at https://support.soa.com/support provides an option for emailing product-related inquiries to our Support team.
Phone	1-866-SOA-9876 (1-866-762-9876)
Support Site	The Support section of the SOA Software website at https://support.soa.com/support includes many product-related articles and tips that might help answer your questions.
Documentation Updates	We update our product documentation for each version. If you're not sure you have the latest documentation, send an email request to support@soa.com. Specify the product and version you're using.

For more information, visit https://support.soa.com/support/.