SOA Software: Policy Manager Configuration Categories and Settings

SOA | software™

SOA Software Policy Manager

Policy Manager Configuration Categories and Settings
1.1 / 6.1
October, 2013

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

Chapter 1 | Introduction

This document provides general information and instructions to help you troubleshoot issues that might come up with your SOA software products. It also includes detailed information about the configuration categories and settings.

This chapter includes:

- Document Summary
- Customer Support
- Troubleshooting Resources and Tips
- Product Documentation

Document Summary

The table below provides a summary of the information in this publication and how it is organized.

This chapter…	Provides this information…
1: Introduction	General information about information resources available, information about working with Support, general information about basic troubleshooting tools.
2: Configuration Categories and Settings	Information about each configuration category and its settings.

Customer Support

This section provides information about working with SOA Software technical support, including:

- Contacting Technical Support
- Logging a Support Ticket
- Support Tickets: Customer Responsibilities
- Notes for Support Customers

Contacting Technical Support

If you experience an issue with an SOA product, you can contact SOA Support. SOA Software offers a variety of support services by email and phone. Support options and details are listed in the table below.

Support Option	Details
Email (direct)	support@soa.com
Phone	1-866-SOA-9876 (1-866-762-9876)
Email (via the website)	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. It also 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/.

Logging a Support Ticket

There are two ways to log a support ticket:

- Submit a ticket directly from the SOA Software Support site at https://support.soa.com/support.
- Send an email to support@soa.com.

When you log a support ticket, provide clear and specific details about the issue you are having, with as much background information as possible. Include the appropriate log files based on the type of issue being reported.

To log an SOA support ticket

1 Log in to the SOA Support site, using the credentials provided to your organization, at this address:

```
http://support.soa.com
```

2 On the Support home page, click **Submit a Ticket**.

3 Under **Select Department**, choose the product you need help with and then click **Next**.

4 Select the Priority/Severity of the issue. For definitions and guidance, refer to the general support policy, available at: https://support.soa.com/docs/index.php?download=SupportOverview.doc.

5 Provide all the required information. The specific information required might vary depending on the product for which you're reporting an issue. For example, you might need to provide:

   - Product version and update
   - Database version
   - Operating system (32/64-bit)

6 Provide a clear subject and description of the issue. If possible, include steps to reproduce your issue so that Support can troubleshoot it more effectively.

7 Attach log files, screen captures, or any other related files.

Support Tickets: Customer Responsibilities

When logging a support ticket, please bear in mind these additional points and customer responsibilities:

- Please make sure that the issue is related to the SOA product. In some cases, issues are caused by other factors such as network, firewall, or security certificates.

- In case of a Production Critical issue, you can contact SOA Support immediately and one of our knowledgeable support staff will help you troubleshoot your problem and collect information for further diagnosis. If you are reporting the issue by email, specify in the subject line that it is Production Critical. A production critical issue is defined as follows:
  - Actual or potential complete failure of traffic on a critical route due to failure of a system or network element.
  - Complete or partial loss of visibility/control of network elements.
  - Loss or impairment of control/monitoring equipment.
- Document the scenario/steps to reproduce the issue. If it's not possible to reproduce the issue, explain what was happening at the time you experienced the issue and what then occurred.
- Provide the appropriate log files from all SOA containers that are involved in the request flow.
- Collect any other information that you think will be useful for SOA engineers to understand and troubleshoot the issue.
- Report the issue to SOA Support using one of the options listed earlier in this chapter.

Notes for Support Customers

1 For the response time and actions taken based on ticket priority, refer to the Response Times table in the general Support Policy section of the Support Site.

2 If you urgently need a quick response (for example, in the case of a Production Critical issue), please call SOA Support, or submit a ticket and indicate it on the ticket.

3 If screen sharing or an online session is needed, please specify this in the ticket so that SOA Support can be prepared.

4 In the case of screen sharing or an online session, SOA Support may need to control the console to demonstrate how to resolve the issue.

5 If you allow SOA support to access your system directly, remember to also provide the needed access information such as VPN or authentication information.

Troubleshooting Resources and Tips

This section provides information on basic tools and resources you can use, and steps you can take, to help determine the exact cause of an issue or to provide more information to SOA Support. It includes the following subsections:

- Monitoring Tabs: Alerts and Logs
- Log Files
- Knowledge Base
- Release Notes
- Monitoring Tool
- Restarting the Container: General Information

Monitoring Tabs: Alerts and Logs

Monitoring information, including alerts and logs, is available at the following levels:

- For the entire organization
- For each container
- For each service
- For each contract

At each level, a monitoring tab gives you access to alerts, logs, and other information so that you can view the state of functions in real time.

Organization Monitoring Tab

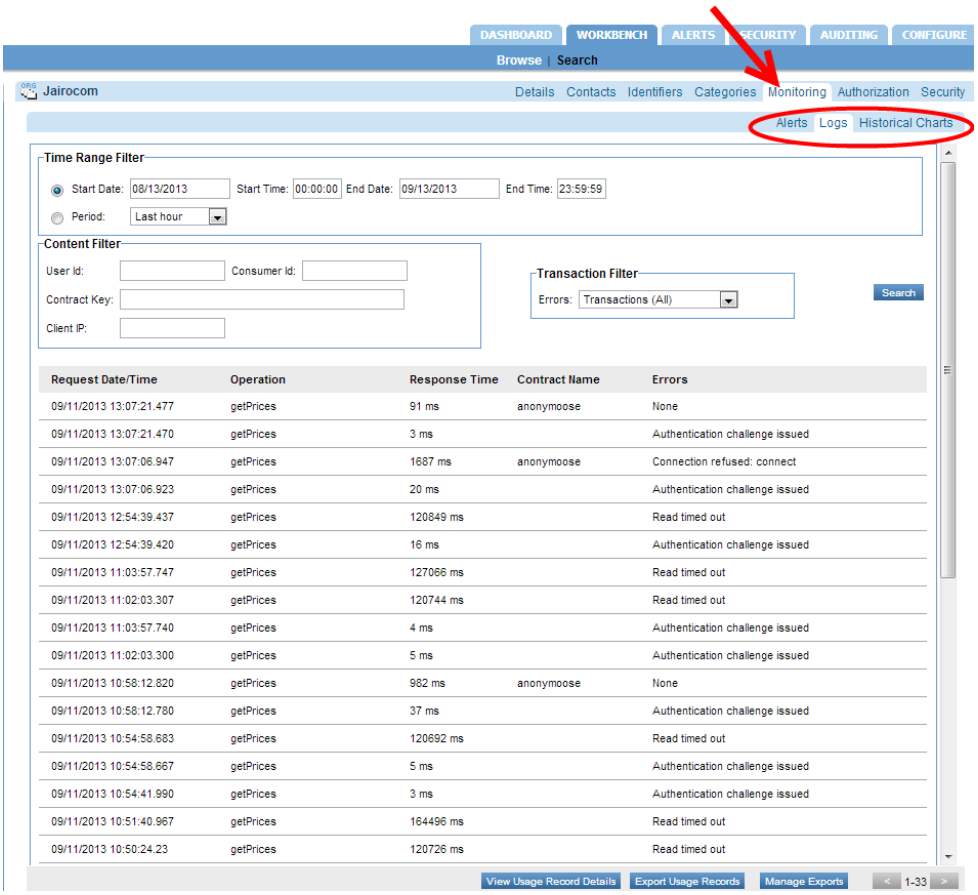
The highest level of monitoring information is available via the monitoring tab for an organization. This lets you view all logs and alerts sent by services and sub-organizations within the organization you are viewing.

This tab includes three types of alerts:

- Service Alerts
- SLA Alerts
- Container Alerts

If there is an error with one of your services, the monitoring tab is a good place to look first, to see if the alerts and log entries can help you identify the problem.

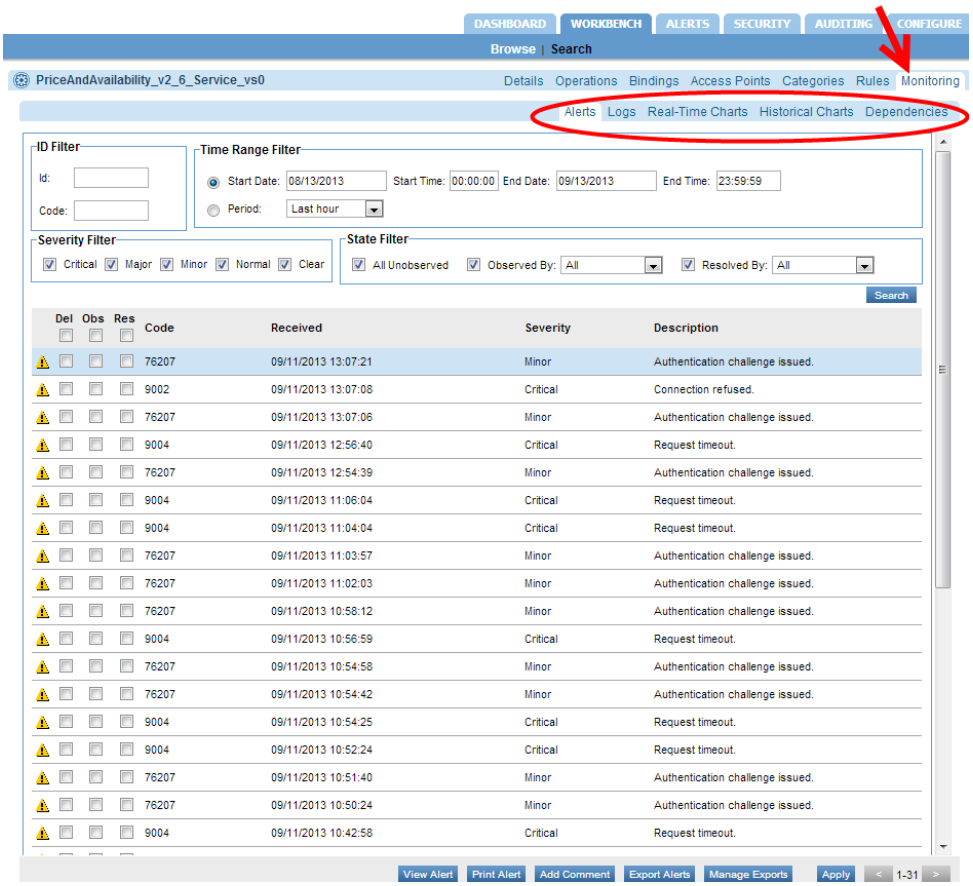
An example of the monitoring tab for an organization is shown below.



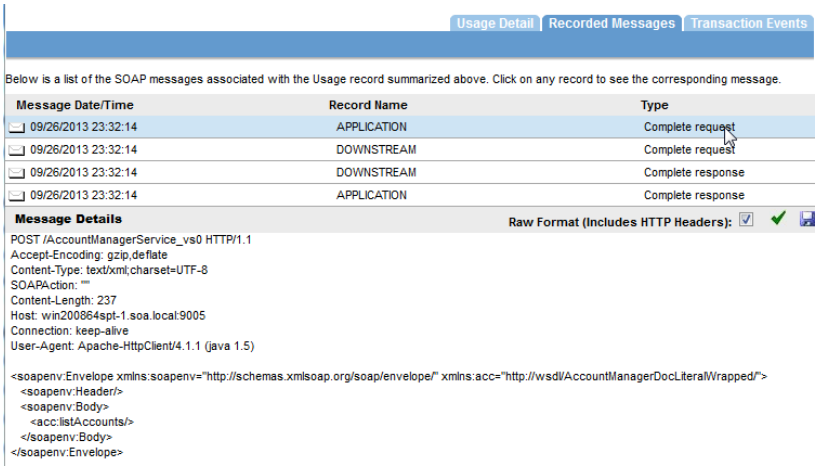
Service-Level Monitoring Tab

Each service also has its own monitoring tab, with alerts and logs relating only to that service and its operations, as shown below.

If the basic auditing policy is being used, the Monitoring -> Logs tab also shows usage data for the service. However, as a best practice this should only be used while troubleshooting or in non-production environments as the payload data is stored in the database.



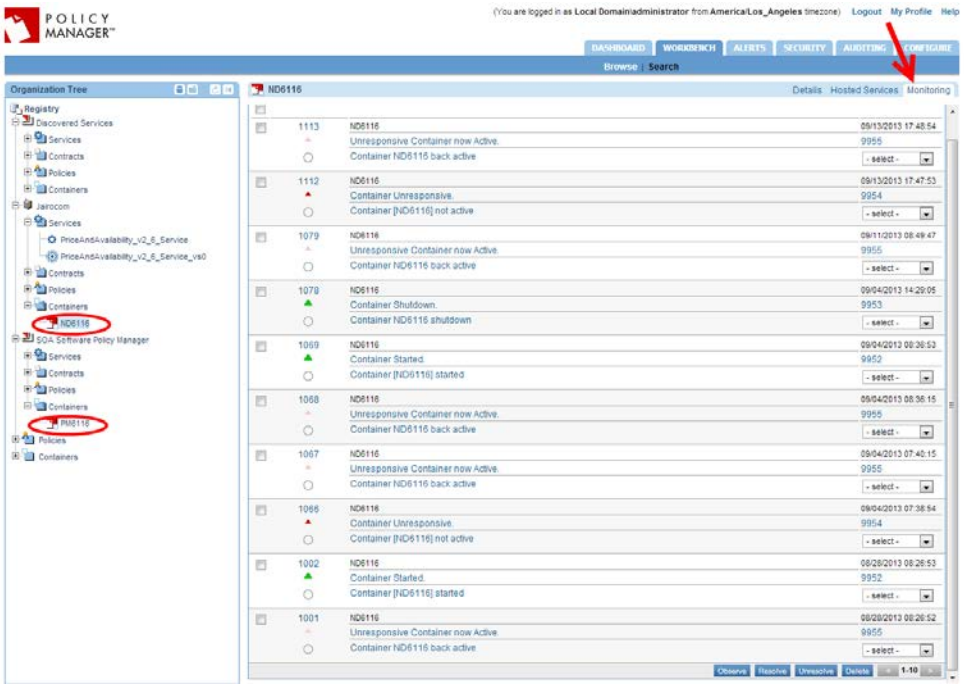
If the detailed auditing policy is being used, you can also view the request and response payload in the Logs tab. Double-click a specific message to see the Usage Data Details overlay. This includes usage detail, recorded messages, and transaction events. In the Recorded Messages tab you can see the individual request and response message. You can also choose to view Raw Format, which includes the HTTP headers. An example is shown below.



Monitoring Tab for the Container

If there is an issue with a specific container, alerts are displayed in the container's monitoring tab as well. You also see the container alerts when you log in to the Policy Manager console.

The example below shows the monitoring tab for a container.



In some cases the information on the monitoring tab can help you discover a deeper error occurring within the container or service.

The next step in troubleshooting an instance is to make use of the logging system.

Monitoring Tab for the Contract

A monitoring tab is also available for each contract, giving access to the logs applicable to the contract.

Log Files

By default, Policy Manager and Network Director only log errors (exceptions) that happen over the course of normal usage. If you are having any runtime processing errors or issues while performing some action in the Policy Manager console, applicable errors will generally be logged in the log file for the applicable container.

This section includes the following information about log files:

- File Location
- Modifying the Default Logging Behavior
- Turning Trace Logging On
- Determining Where to Look for Error Information

Note: There is another type of log that you can enable if needed. In the Policy Manager Admin Console, Configuration tab, choose the configuration category of com.soa.transport.jetty and enable the NCSA Access log (set the ncsa.access.log.enable property to **true**). Then, in the ncsa.access.log.filename field, specify the location for the log file. After that, access to any page in the Policy Manager Console or Admin Console generates an entry to the specified log file.

File Location

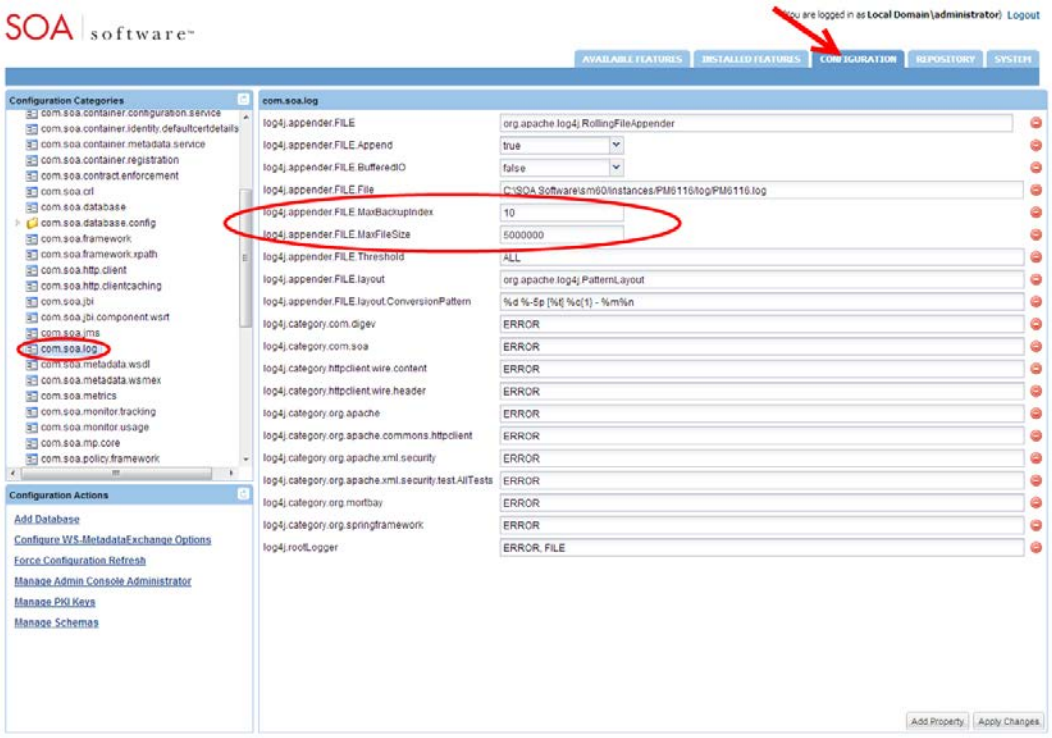
Each instance has its own set of logs at the following default location:

```
<installation directory>/sm60/instances/<instance name>/log
```

The default behavior for the logging system is to have a maximum of ten backup logs at 4.7 MB (5000000 bytes) each. When a log reaches 4.7 MB in size, the logging information rolls over into the next file. Once the total number of log files reaches 10, the oldest file is deleted when the new one starts.

Modifying the Default Logging Behavior

You can modify the default settings for logging behavior, along with the level of logging and other customization, in the Policy Manager Admin Console and in the Network Director Admin Console.



To modify the default logging behavior

1 Log in to the Policy Manager Admin Console or Network Director Admin Console.

2 Click the **Configuration** tab.

3 From the configuration categories on the left, find **com.soa.log**.

4 In the properties panel on the right, the two properties below control the number of backups and/or the maximum size for each log file. Modify as needed:

   – log4j.appender.FILE.MaxBackupIndex: the number of backup files that are kept

   – log4j.appender.FILE.MaxFileSize: the maximum size for each file

5 Click Apply Changes.

Turning Trace Logging On

If a problem with a container persists, you could enable trace logging in the Admin Console. Trace logging is enabled dynamically and does not require a container restart.

Depending on the category for which trace logging is enabled, detailed information is collected in the log file, including such activity as:

- Internal SOA to SOA container communication
- Database queries
- Incoming requests
- Certificate information
- Scheduled jobs

When the troubleshooting is complete, trace logging for the specific category should set back to the default setting of **error**.

A good practice is to figure what action is causing specific symptoms in the container, and turn on trace logging only while that action is occurring. For example, if a service detail page is coming up blank, you might want to see what Policy Manager is doing when you click on the service detail page. You would set the logging level to **trace**, click on the service detail page, and then change the level back to **error** and analyze the logs.

To turn trace logging on or off

1 Log in to the Policy Manager Admin Console or Network Director Admin Console.

2 Click the **Configuration** tab.

3 From the configuration categories on the left, find **com.soa.log**.

4 In the properties panel on the right, modify this property to enable or disable trace for all runtime activity on the container:

- To enable: log4j.category.com.soa: Switch from ERROR to TRACE
- To disable: log4j.category.com.soa: Switch from TRACE to ERROR

5 Click Apply Changes.

stdout.txt File

If there is an issue with the bundles not starting, you can check the stdout.txt file to get additional information for troubleshooting purposes.

This file is created whenever the container starts up. It is stored in the instances folder (instances/<container name>/log/stdout.txt).

Normally the file contains a one-line message stating that the bundles have started. However, if the bundles fail to load, the errors that occur during the container initialization process are recorded in this file. Errors relating to bundles loading do not appear in the Policy Manager log files, since logging of messages starts when the container has started.

Monitoring Tool

All Policy Manager 6.x containers include an optional Monitoring Tool to help troubleshoot issues related to the container resources. It is not installed by default but you can easily install it. You can use this tool to monitor and analyze the following:

- Incoming HTTP connections (com.soa.transport.httpclient)
- Database thread pool (com.soa.database.config.<db-config-id>-mon)
- Active/idle Policy Manager processes (com.soa.framework)
- Container memory usage (com.soa.vmstats)
- Outgoing HTTP connections (com.soa.transport.jetty)
- Monitoring queues (com.soa.usage)
- JMS connections (com.soa.transport.jms)

To install the monitoring tool

1 Log in to the Policy Manager Admin Console or Network Director Admin Console.

2 Click the Available Features tab.

3 From the **Filter** drop-down list at the top of the left panel, choose **Tool**.

4 Click the checkbox for the SOA Software Admin Monitoring Tool and click **Install Feature**.

5 Restart the container.

6 After restart, verify that the Monitoring tab is now present in the Admin Console, as shown below.

Note: This tool does not require additional machine or container resources to run. Before closing the tool, set the polling interval to 0.

Restarting the Container: General Information

Some types of changes that you might make will require restarting of the container before the changes go into effect. Other types of changes are effective immediately, without restarting the container.

In most cases, specific procedures and issue resolution notes in this document state whether you need to restart the container or not. In general, configuration changes do not require restart unless they include changes to the container listener or database. If you add or remove container features you'll need to restart the container for the changes to go into effect.

Examples of changes that require restart:

- Adding the monitoring tool in the Policy Manager Admin Console
- Changing database properties such as username, password, or hostname
- Changing the port number for the container listener (for Policy Manager versions 6.0 and prior)

Examples of changes that do not require restart:

- Increasing the log level to **TRACE**
- Adding an HTTP route configuration file to the /instances/<ND>/deploy folder
- Adding an identity system such as LDAP to the Policy Manager Workbench
- Changing the port number for the container listener (for Policy Manager version 6.1)

Determining Where to Look for Error Information

When trying to narrow down information for troubleshooting purposes, it might be useful to know what symptoms are likely to relate to which container types.

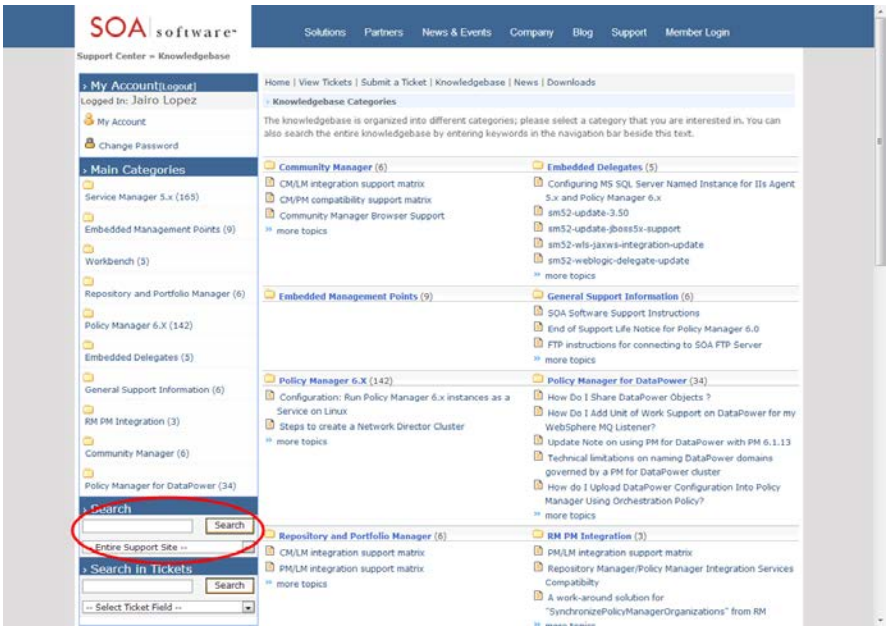
You might find info about these types of errors…	In this location…
Issues with the Policy Manager (for example, usage writer or container configuration), user interface issues, search results, and some database issues.	Policy Manager log files. These types of issues are generally a problem with the Policy Manager instance.
404 when invoking a service, bad context paths, virtual service authentication errors, authorization errors, or routing issues.	Network Director log files. Possibly also Policy Manager log files. These issues are likely to relate to the Network Director. However, since the Network Director communicates with the Policy Manage to retrieve information, in many cases the Policy Manager logs are helpful as well.
Container initialization.	stdout console or the stdout file. Any errors that occur during the container initialization process are written to stdout.

Knowledge Base

The SOA Software knowledge base, http://support.soa.com, includes many type of information such as:

- Configuration settings
- Specific problems and their resolution
- Supported versions
- Tuning information
- Known issues and workarounds
- Tips and tricks

The knowledge base home page is shown below.

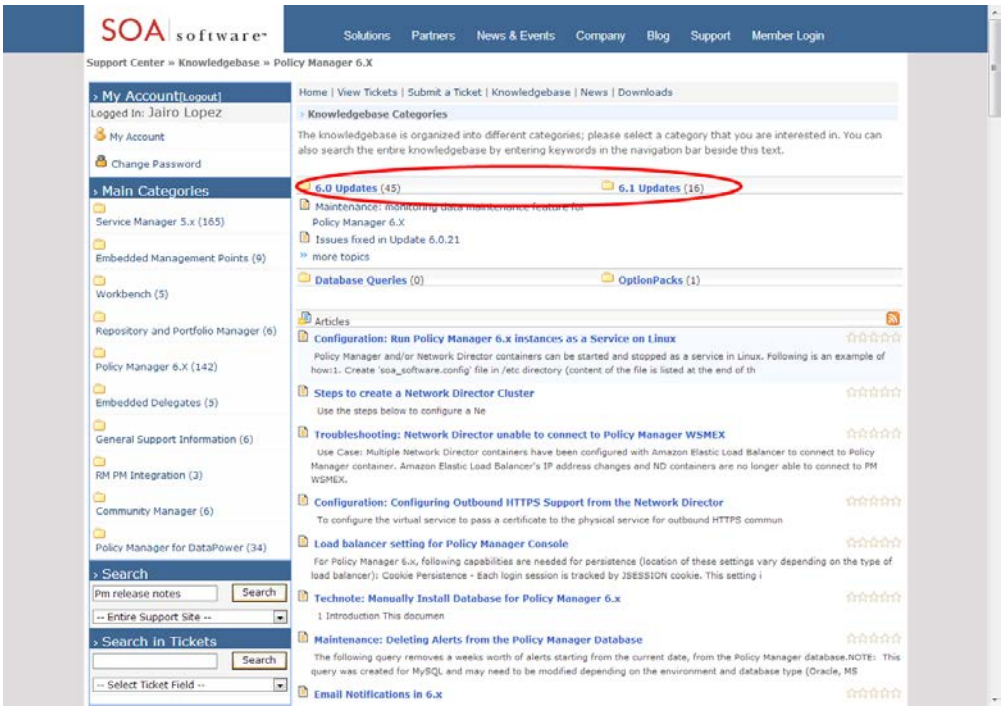


Release Notes

It's possible that you could encounter a bug that might have been resolved in a later version of the product. For this and other reasons, it's a good idea to check the release notes for versions later than yours.

The release notes for each product version include information about the bugs/issues that have been fixed in that version, as well as information about new product features and enhancements. You might find that the problem you encountered was resolved in a later version.

To view release notes, go to the knowledge base at http://support.soa.com. Click on the category for your product—for example, Policy Manager 6.x—and choose the applicable version update section, as shown below.



You will see a summary of the release notes for every version. Just browse through any versions newer than yours to see if the issue has been fixed in an upgrade.

In addition, a summary of the issues that were fixed in each update is included in a text file located in the ./sm60/docs directory.

Product Documentation

When you download your installation executable files, make sure you get and read the product documentation. The documentation for each product includes general information about installation and often includes troubleshooting information for the specific product.

Updates to documents are available from time to time on the Support site.

Chapter 2 | Configuration Categories and Settings

This section provides a brief explanation of the various configuration categories and settings in Policy Manager. In many cases, the solution to a specific issue is to modify a configuration setting. This section describes the settings that are available.

To access the configuration settings

1 Log in to the Policy Manager Admin Console.

2 Click the **Configuration** tab.

The configuration settings are in the left panel.

com.soa.auz.client

Configuration of the authorization client.

cached.auz.decision.service.cacheTimeout

The time, in seconds, for which authorization decisions will be cached/refreshed.

Default: 60

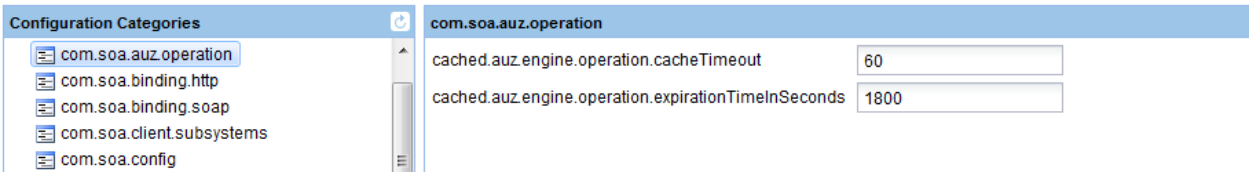
cached.auz.decision.service.expirationTimeInSeconds

The time, in seconds, after which authorization decisions are expired if not used even once.

Default: 1800

com.soa.auz.operation

Configuration settings for caching in the authorization engine. These settings control caching, so they are important for speed of message handling.



cached.auz.engine.operation.cacheTimeout

Cache Timeout: The time, in seconds, after which authorization decisions will timeout.

Default: 60

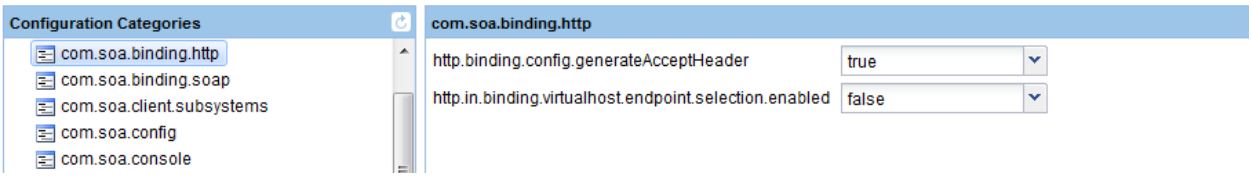
cached.auz.engine.operation.expirationTimeInSeconds

Cache Timeout: The time, in seconds, after which authorization decisions are expired if not used.

Default: 1800

com.soa.binding.http

Configuration of the HTTP binding components. These settings are used when sending or receiving HTTP messages.



http.binding.config.generateAcceptHeader

Enables or disables generation of Accept headers to downstream services based on the WSDL of the target service.

Default: true

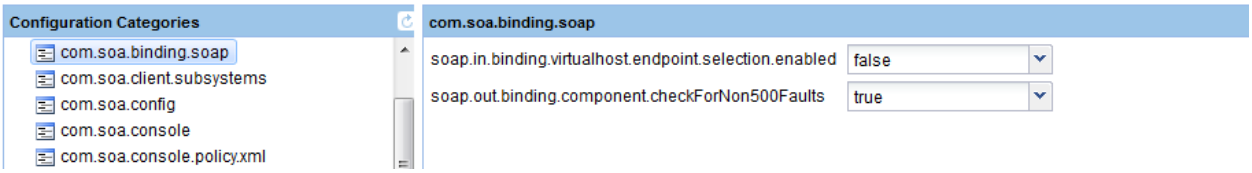
http.in.binding.virtualhost.endpoint.selection.enabled)

Enables or disables support for using virtual hosts to distinguish between HTTP endpoints. If set to true, two HTTP operations can both use the same path with a different host name; for example, http://myhost.com/api and http://yourhost.com/api.

Default: false

com.soa.binding.soap

Configuration settings for SOAP binding components. These settings are used when sending or receiving SOAP messages.



soap.in.binding.virtualhost.endpoint.selection.enabled

Enables or disables support for using virtual hosts to distinguish between SOAP endpoints. For example, two SOAP services can both use the same path with a different host name; for example, http://myhost.com/service and http://yourhost.com/service.

Default: false

soap.out.binding.component.checkForNon500Faults

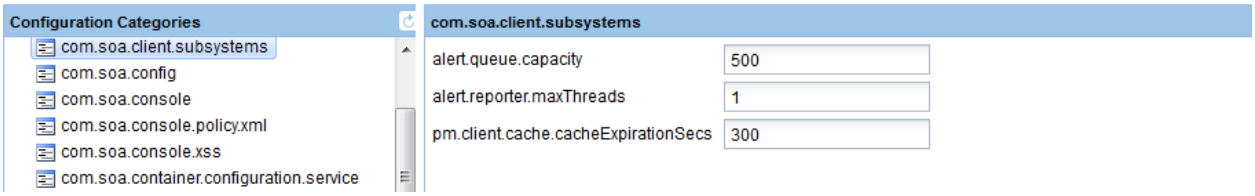
Checks for faults in messages other than 500. Per the SOAP specification, fault messages should have a status code of 500; this setting is here for interoperability purposes. Indicates that the system should check for faults returned in messages with status codes other than 500. If this setting is changed, the system must be restarted for the change to take effect.

Default: true

com.soa.client.subsystems

Configuration settings for communications with the Policy Manager and Alert Manager services.

When alerts are generated, they are sent to Policy Manager in an out of band thread so that we don't log the request and then send the alert. We log alerts to a different queue. If there are issues with alerts you might need to modify these settings.



Alert Queue Size (alert.queue.capacity)

The size of the alert queue. Alerts are delivered asynchronously.

Default: 500

Alert Writer Threads (alert.reporter.maxThreads)

The number of threads available for writing alerts.

Default: 1

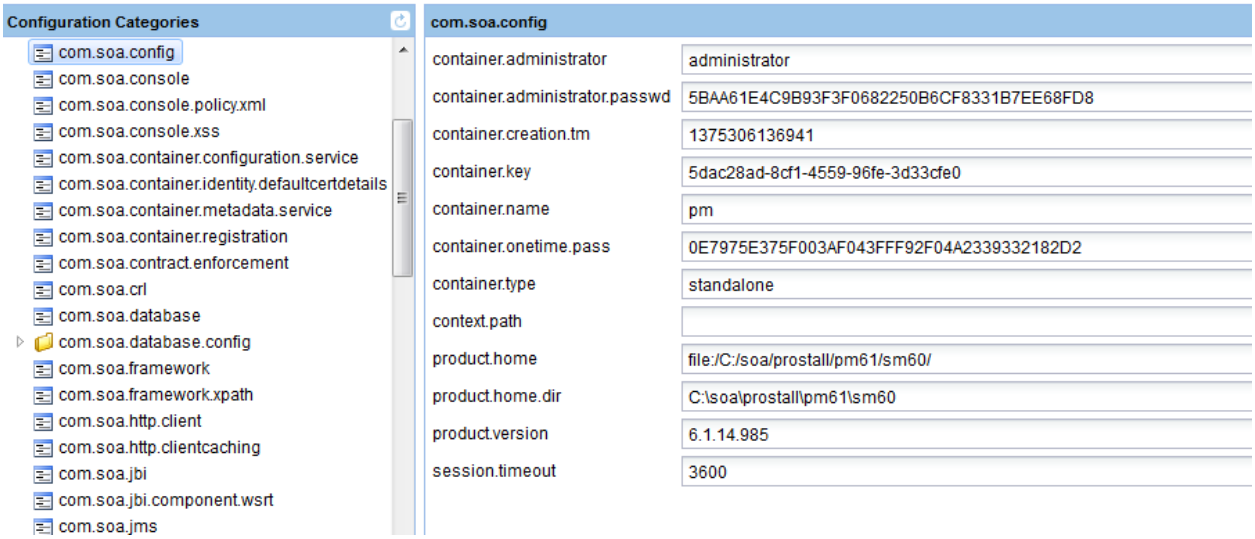
PM Client Cache Expiration in Seconds (pm.client.cache.cacheExpirationSecs)

The time, in seconds, before a cached security credential (such as a certificate or SAML assertion) that is returned from the Policy Manager service expires and must be refreshed.

Default: 300

com.soa.config

General configuration settings. These are only for viewing; do not change these settings.



container.administrator

The user ID for the Admin Console.

The Admin Console has a temporary local internal identity store of its own, containing one administrator account. You need the username and password to log into the Admin Console, and

you must log into the Admin Console to configure the database. The Admin Console identity store allows a way for you to reset the password should the only admin login be lost or forgotten.

In general usage, it's best to use the local domain user IDs, and reserve this user ID and password only for the Admin Console.

container.administrator.passwd

The password for the Admin Console. See above.

container.creation.tm

The container creation timestamp.

container.key

The container key.

container.name

The name of the container.

container.onetime.pass

The one-time password used for initial login by the Admin user.

container.type

The type of the container; for example, standalone.

context.path

The context path of the Admin Console (prefix to the /admin path).

product.home

The installation location for the product, expressed as a URL.

product.home.dir

The installation location for the product, expressed as a filesystem path.

product.version

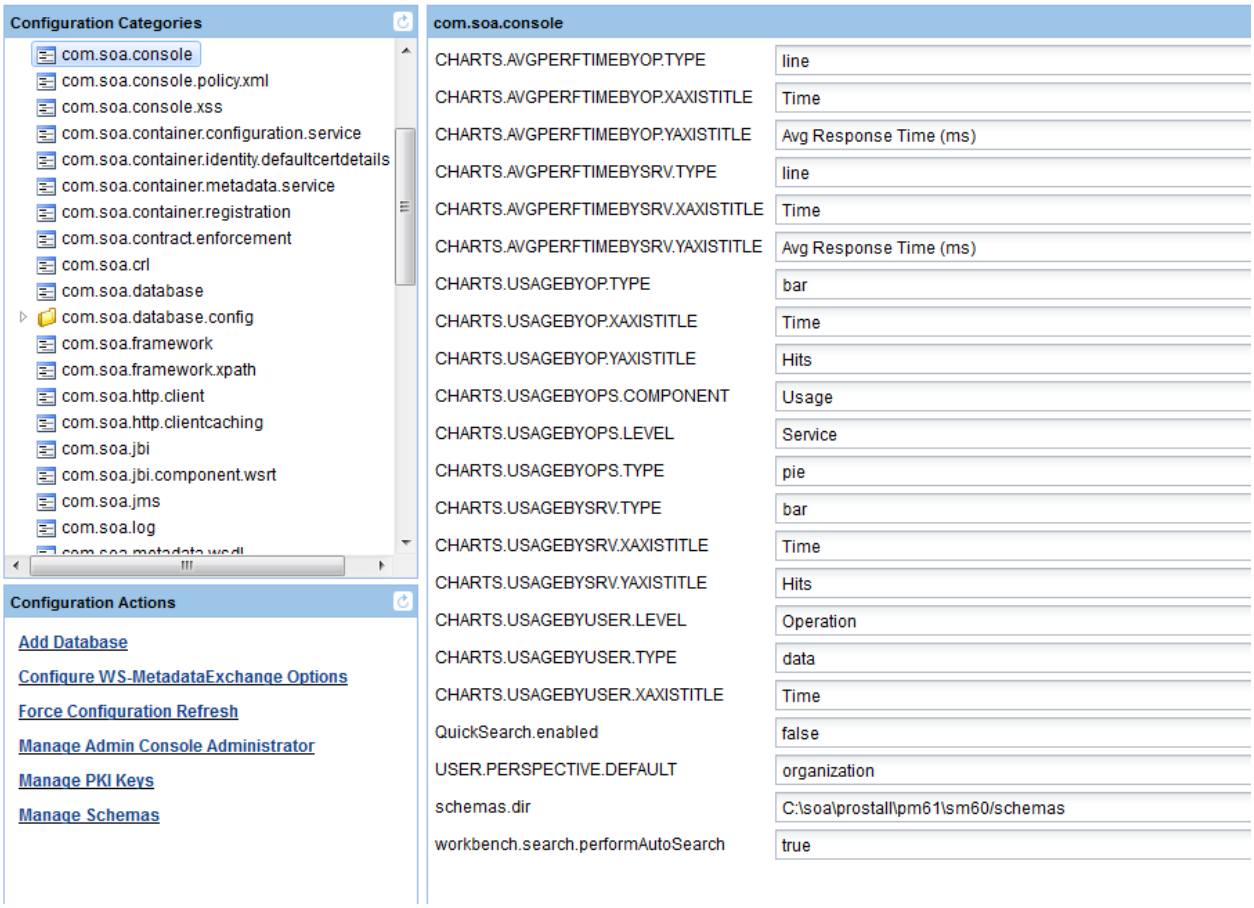
The product version number, including the build number.

session.timeout

Session timeout value, in milliseconds, for the Admin Console.

com.soa.console

Configuration settings relating to the Policy Manager console.



CHARTS.AVGPERFTIMEBYOP.TYPE

No longer used.

CHARTS.AVGPERFTIMEBYOP.XAXISTITLE

No longer used.

CHARTS.AVGPERFTIMEBYOP.YAXISTITLE

No longer used.

CHARTS.AVGPERFTIMEBYSRV.XAXISTITLE

No longer used.

CHARTS.AVGPERFTIMEBYSRV.YAXISTITLE

No longer used.

CHARTS.USAGEBYOP.TYPE

No longer used.

CHARTS.USAGEBYOP.XAXISTITLE

No longer used.

CHARTS.USAGEBYOP.YAXISTITLE

No longer used.

CHARTS.USAGEBYOPS.COMPONENT

No longer used.

CHARTS.USAGEBYOPS.LEVEL

No longer used.

CHARTS.USAGEBYOPS.TYPE

No longer used.

CHARTS.USAGEBYSRV.TYPE

No longer used.

CHARTS.USAGEBYSRV.XAXISTITLE

No longer used.

CHARTS.USAGEBYSRV.YAXISTITLE

No longer used.

CHARTS.USAGEBYUSER.LEVEL

No longer used.

CHARTS.USAGEBYUSER.TYPE

No longer used.

CHARTS.USAGEBYUSER.XAXISTITLE

No longer used.

QuickSearch.enabled

If set to true, the QuickSearch feature in the Policy Manager Console (at the top of the Organization Tree) is automatically enabled.

USER.PERSPECTIVE.DEFAULT

Default workbench tree perspective. Valid values: **organization** or **category**.

schemas.dir

Directory location for the default out-of-box schemas loaded during startup.

workbench.search.performAutoSearch

If set to true, the Workbench search feature is automatically enabled.

com.soa.cluster

Configuration of cluster node synchronization.

Enable Cluster Replication (cluster.replication.enabled)

Indicates whether cluster replication is enabled for the node.

Default: false

Master Node Hostname (master.node.hostname)

The master node hostname or IP. This is used by slave nodes to contact the master in order to retrieve synchronization data.

Master Node Port (master.node.port)

The master node port used to retrieve the node descriptor.

Excluded Configurations (excluded.configs)

The config admin PIDs that should not be exposed to other cluster members or consumed by this node. Note that changing these values can have serious consequences for the behavior of a container in the SOA framework.

Default: com.soa.log com.soa.container.identity* com.soa.admin.console*

Node Descriptor Path (node.descriptor.path)

The path on the master node used to publish and consume node descriptors.

Default: /admin/cluster/publish/state

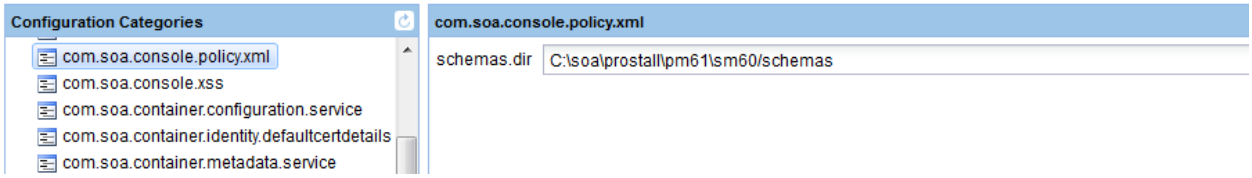
Poll Interval (poll.interval)

The poll interval for slave nodes, in milliseconds. This determines how often the slave polls the master for state information.

Default: 4000

com.soa.console.policy.xml

Configuration of the XML policy handler.



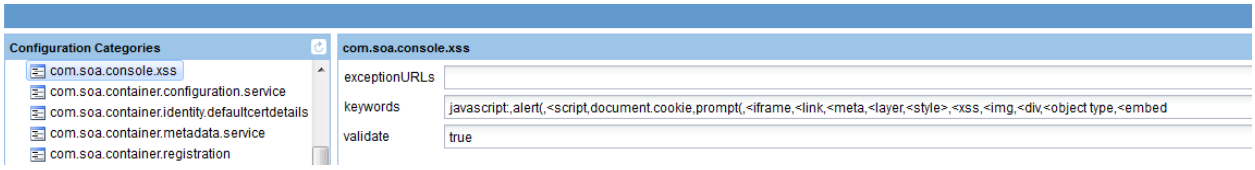
schemas.dir

The filesystem directory containing the XML schema files.

Default: ${product.home.dir}/schemas

com.soa.console.xss

Configuration settings for cross-site scripting for the Workbench console.



exceptionURLs

The URLs that are acceptable for cross-site scripting.

keywords

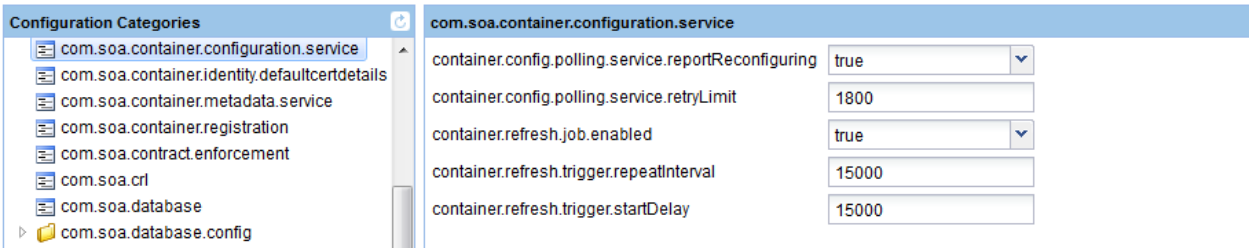
Keywords that it will search for, and will reject if the request parameters have any of these keywords.

validate

Indicates whether cross-site scripting is enabled.

com.soa.container.configuration.service

Configuration of the container refresh properties.



Report Reconfiguring Container State (container.config.polling.service.reportReconfiguring)

Indicates container reconfiguring should be reported. If set to false, once initial configuration is completed the container config job will always report com.soa.container.configuration.configured.

Default: true

Retry Time Limit (container.config.polling.service.retryLimit)

Timeout (in seconds) controlling how long a failure to obtain configuration data from Policy Manager should be retried.

For example, let's say Network Director is started but Policy Manager is shut down while Network Director is retrieving its configuration data. Some virtual services may not be deployed due to errors while the Policy Manager is restarting. By default, it keeps trying to retrieve the required information to deploy the failed virtual services for 30 minutes. After 30 minutes it gives up.

Default: 1800

Enable Refresh (container.refresh.job.enabled)

Indicates whether the refresh job is enabled or disabled. If the refresh job is disabled, service policy and other configuration information will not be updated for this container.

Default: true

Refresh Interval (container.refresh.trigger.repeatInterval)

The interval in milliseconds between configuration updates.

By default, Network Director keeps polling for the container configuration every 15 seconds. If the container configuration rarely changes you can make this interval longer.

Default: 15000

Start Delay (container.refresh.trigger.startDelay)

The time in milliseconds between when the container is started and when container updates will begin.

Default: 15000 (15 seconds)

com.soa.container.identity

Configuration of the container identity. These are only for viewing; do not change the settings.

Private Key (privatekey)

The container private key as a Base64-encoded value.

Container Public Key (publickey)

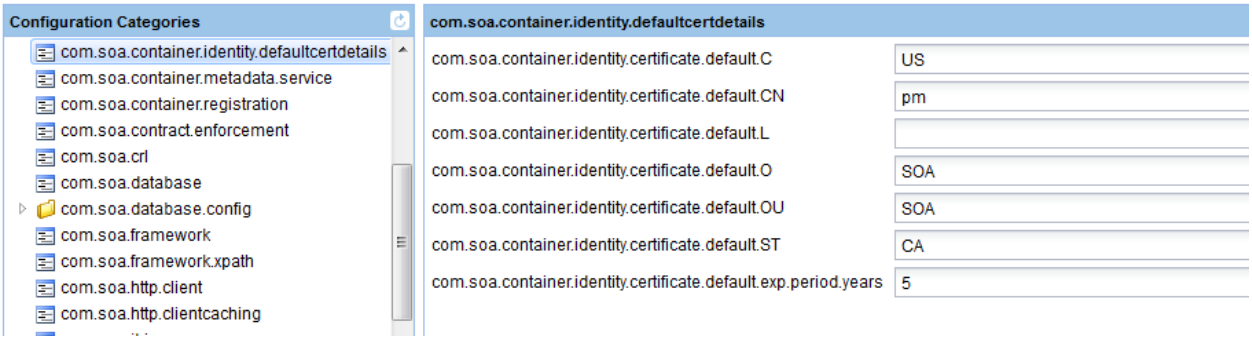
The container public key as a Base64-encoded value.

Certificate Chain (cert)

The container certificate chain. Each certificate is Base64-encoded. Certificates are separated by a comma character (,).

com.soa.container.identity.defaultcertdetails

Configuration information for the default values used when creating the container certificate.



com.soa.container.identity.certificate.default.C

The default country.

com.soa.container.identity.certificate.default.CN

The default common name.

com.soa.container.identity.certificate.default.L

The default locality.

com.soa.container.identity.certificate.default.O

The default organization.

com.soa.container.identity.certificate.default.OU

The default organization unit.

com.soa.container.identity.certificate.default.ST

The default state.

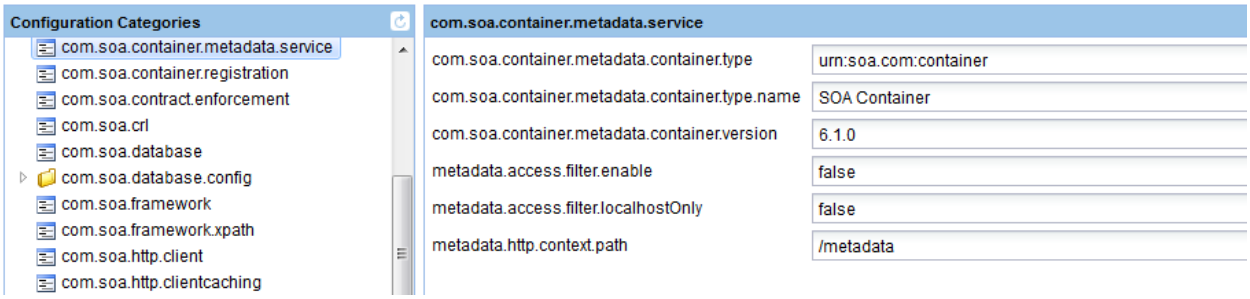
com.soa.container.identity.certificate.default.exp.period.years

Default expiration period, in years, for the container identity certificate.

com.soa.container.metadata.service

Configuration of properties for the container metadata service.

Container metadata describes the capabilities of the container. These capabilities are used in Policy Manager to guide the actions that can be taken on the container, such as hosting a virtual service or creating a listener of a certain protocol.



Container Type (com.soa.container.metadata.container.type)

The container type URI.

Default: urn:soa.com:container

Container Type Name (com.soa.container.metadata.container.type.name)

The container type name.

Default: SOA Container

Container Metadata Version (com.soa.container.metadata.container.version)

The container metadata version.

Default: 6.0

Container Metadata Service Access Toggle (metadata.access.filter.enable)

The switch for enabling or disabling the security filter for the metadata service.

Default: false

Container Metadata Service Local Access Toggle (metadata.access.filter.localhostOnly)

The switch for enabling or disabling access to the metadata service from different hosts. If set to true, it can only be accessed from localhost. This property requires the metadata.access.filter.enable property to be set to true.

Default: false

HTTP Context Path (metadata.http.context.path)

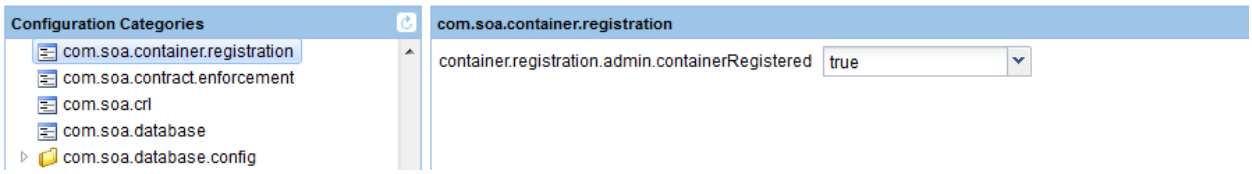
The path for where the metadata for this container is stored. You can use this path to read the metadata from this container using HTTP (precede the path with any root context for the container's HTTP listeners).

The metadata file includes information such as container type, container name, container certificate, and the features installed in the container (the capabilities it supports).

Default: /metadata

com.soa.container.registration

Configuration of container registration.



container.registration.admin.containerRegistered

Indicates whether the container is considered to have been registered in Policy Manager. As long as this value is set to false, the Network Director continues to check with Policy Manager to see if the container is registered. Only when the container is successfully registered does the Network Director begin pulling the container's configuration.

This property need not be set manually unless you would like the Network Director to recheck that it has been registered.

Default: false

com.soa.container.state

Configuration of container state reporting.

container.state.reporter.enabled (container.state.reporter.enabled)

Enable or disable the reporting of container state. If the container does not reflect state, it will appear as not started or unresponsive in Policy Manager.

Default: true

container.state.refresh.trigger.repeatInterval (container.state.refresh.trigger.repeatInterval)

The interval in milliseconds between configuration updates.

Default: 60000

container.state.refresh.trigger.startDelay (container.state.refresh.trigger.startDelay)

The time in milliseconds before container updates will begin when the bundle is started.

Default: 30000

container.state.refresh.job.enabled (container.state.refresh.job.enabled)

Enable or disable the refresh job.

Default: false

com.soa.contract.enforcement

Configuration for contract enforcement.

Contract Cache Timeout in Seconds ()

Cache timeout value for contracts, in seconds.

Contract Idle Expiration (contract.handler.framework.idleExpiration)

The number of seconds a cached contract will remain in the cache without being authorized against.

Default: 300

Contract Refresh Interval (contract.handler.framework.maxRefreshInterval)

The number of seconds a contract should remain in the cache before requiring a refresh.

Default: 120

Contract Cache Refresh Interval (contract.refresh.trigger.repeatInterval)

The interval in milliseconds between contract cache refresh checks, controlling how often this job should run.

Default: 15000

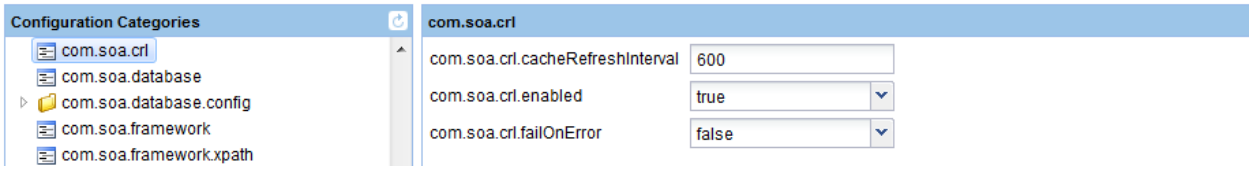
Contract Cache Refresh Start Delay (contract.refresh.trigger.startDelay)

The time in milliseconds before contract cache refreshes will begin when the system is started.

Default: 15000

com.soa.crl

Configuration properties for the certificate revocation list.



com.soa.crl.cacheRefreshInterval

Interval in seconds to refresh the CRL cache.

Default: 600

com.soa.crl.enabled

Indicates whether CRL check is enabled for all X.509 certification verification.

Default: true

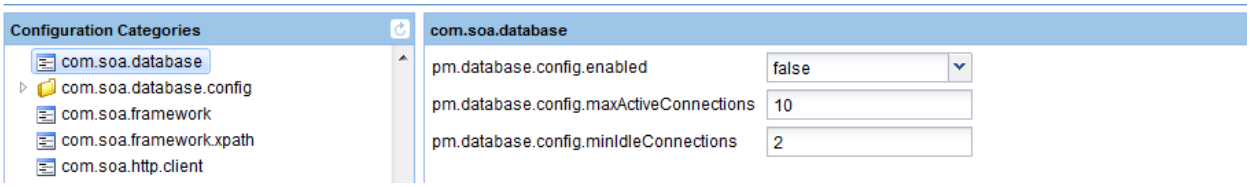
com.soa.crl.failOnError

Fail on error: If set to true, if there is any error when retrieving a CRL list for an issuer then all corresponding certificates will be revoked.

Default: false

com.soa.database

Configuration parameters for a remote database. The remote configuration holds the database connection parameters. The local thread pool is configured here.



Use Policy Manager Database Configuration (pm.database.config.enabled)

If set to true, database configuration is retrieved from Policy Manager rather than retrieved locally; whenever a Policy Manager client is registered with the system, the central database configuration is retrieved and a new data source is published based on that configuration.

This setting should only be enabled for Network Director configurations.

Default: false

Max Active Connections (pm.database.config.maxActiveConnections)

The maximum number of active connections in the connection pool.

Default: 10

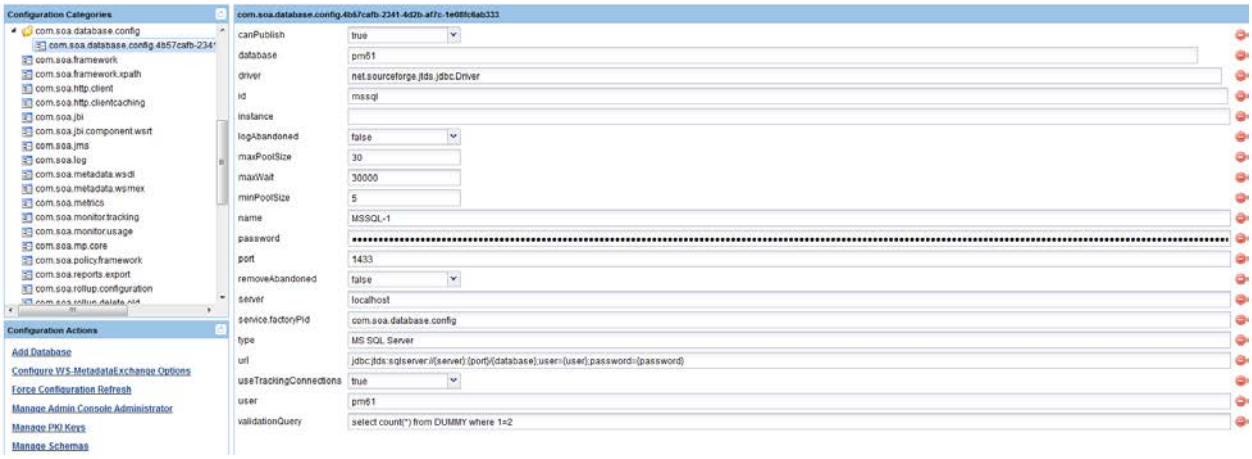
Min Idle Connections (pm.database.config.minIdleConnections)

The minimum number of idle connections in the connection pool.

Default: 2

com.soa.database.config

Configuration for the Policy Manager database connection, including some general properties and some properties specific to certain database types.



Publish This Configuration (canPublish)

A flag indicating whether the configuration can be published. When set to true, indicates that the configuration is complete and can be published as a DataSource service into OSGi.

database

The database name.

driver (driver)

The filename for the database driver.

id (id)

ID of the database (type of database).

instance

Named Instance name (SQL Server only)

Log Abandoned Connections (logAbandoned)

If set to true, abandoned connections are logged to a log file.

Max Active Connections (maxPoolSize)

The maximum number of active connections in the connection pool.

Max Connection Wait Time (maxWait)

The maximum time to wait, in milliseconds, to get a connection from the pool.

Min Active Connections (minPoolSize)

The minimum number of active connections in the connection pool.

Name (name)

The name of the database.

Database Password (password)

The password for the database connection.

port

The database server port.

Remove Abandoned Connections (removeAbandoned)

If set to true, removes abandoned connections from the pool.

server

Database server hostname.

type (type)

The type of database, in text.

url (url)

URL for the database.

Use Tracking Connections (useTrackingConnections)

If set to true, if there is a connection leak a message is generated stating that a connection was opened and not closed.

user

Database username.

Validation Query (validationQuery)

Optional validation query to validate each of the connections.

Admin Username (adminUsername)

Administrator username, if different from the regular user. Not used at runtime.

Encrypt Values (encryptValues)

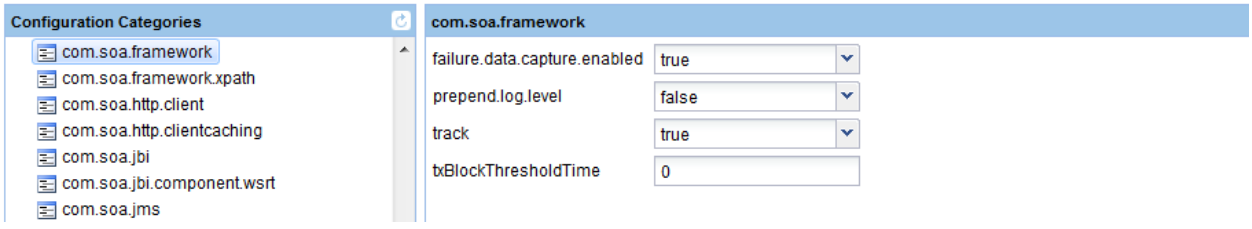
Encrypts database password.

Database User Name (username)

The user name for the database connection. Not used at runtime.

com.soa.framework

Configuration of the core framework utilities.



Nested Diagnostic Context Logging (failure.data.capture.enabled)

Captures formatted logging information. If set to true, data added to the log file is indented based on the logging context. This is often referred to as Nested Diagnostic Context (NDC) logging. With this type of logging, all log entries for a thread are grouped together. Even if log levels are not set to TRACE, trace information is stored in memory in case of an error. If an error is reported, all TRACE

information is logged. This demands more memory resources at runtime but adds to the readability of the resulting log information.

If this value is set to false, logging is not indented, and log entries for different threads might be mixed together. Only log statements that meet the configured log level will appear. However, in exchange for this, some small performance gains will be seen and memory consumption will be lower.

Default: true

Prepend Log Level (prepend.log.level)

Prepends log level to log messages. This feature is useful if log entries are long. When this value is set to true, information is prepended to each line in the log file indicating whether the line is trace, error, or info.

Default: false

Tracks Logging Frames (track)

Tracks Logging Frames. Useful when searching for leaks. When set to true, this initiates a thread that checks logs to verify that every log start includes a log end. If there is a log start without an end, indicating a memory leak, a message is generated to indicate a potential bug. This is only relevant when failure.data.capture.enabled is set to true.

Default: true

threshold in milliseconds to force log even when trace is disabled (txBlockThresholdTime)

Write log to log file for successful transactions even when trace is disabled if complete transaction takes more than the provided milliseconds.

This setting can be useful in tracking down performance issues. Generally, a log is flushed to the log file only if a request fails. However, when this setting is turned on (value other than 0 specified), a request that takes beyond the specified time is logged, even if it is successful.

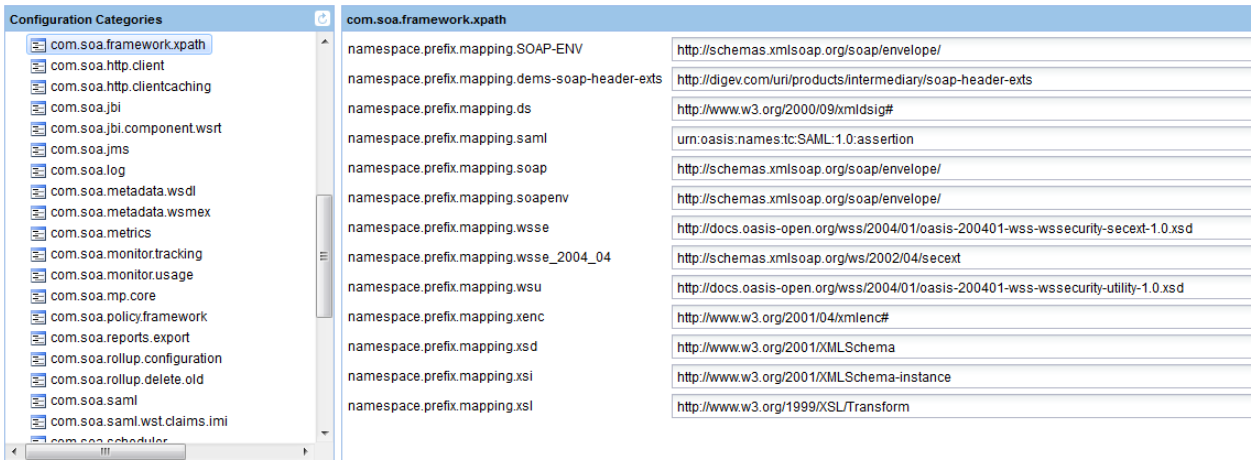
Using this setting can help you find performance issues. Note that some processes might legitimately take a longer time, and might be logged even though there is no issue. This setting is only relevant when failure.data.capture.enabled is set to true.

Default: 0

com.soa.framework.xpath

Settings to map the namespace.

By mapping the namespace URI, you can write concise XPath statements by using pre-existing or known prefixes with XPath.



namespace.prefix.mapping.SOAP-ENV

Namespace prefix mapping for SOAP 1.1 envelopes.

namespace.prefix.mapping.dems-soap-header-exts

Namespace prefix mapping for legacy proprietary SOA Software SOAP headers.

namespace.prefix.mapping.ds

Namespace prefix mapping for XML digital signatures.

namespace.prefix.mapping.saml

Namespace prefix mapping for SAML 1.0.

namespace.prefix.mapping.soap

Namespace prefix mapping for SOAP 1.1.

namespace.prefix.mapping.soapenv

Namespace prefix mapping for SOAP 1.1 envelopes.

namespace.prefix.mapping.wsse_2004_04

Namespace prefix mapping for WS-Security.

namespace.prefix.mapping.wsu

Namespace prefix mapping for WS-Utility.

namespace.prefix.mapping.xenc

Namespace prefix mapping for XML encryption.

namespace.prefix.mapping.xsd

Namespace prefix mapping for XML schemas.

namespace.prefix.mapping.xsi

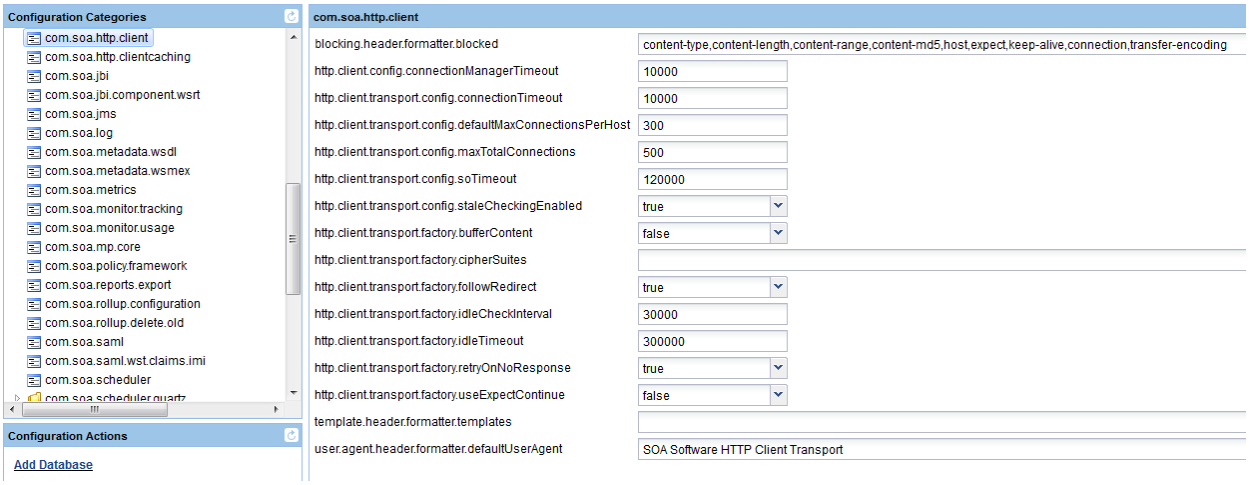
Namespace prefix mapping for XSI.

namespace.prefix.mapping.xsl

Namespace prefix mapping for XSL.

com.soa.http.client

HTTP client configuration properties. These settings allow you to tune the HTTP outbound connections.



Blocked Headers (blocking.header.formatter.blocked)

A list of HTTP headers that will not be forwarded through the transport. The value is a comma-separated list of HTTP header names. Be careful when changing these values since most are generated internally by the transport and changes could result in conflicts.

Default: content-type,content-length,content-range,content-md5,host,expect,keep-alive,connection,transfer-encoding

Connection Pool Timeout (http.client.config.connectionManagerTimeout)

The time in milliseconds indicating how long a thread should wait for a connection from the connection pool. If the pool is empty and it cannot get the connection within this time, it will fail.

Default: 10000 (10 seconds)

Connection Timeout (http.client.transport.config.connectionTimeout)

The timeout in milliseconds to allow when establishing a connection. This value is passed directly to Socket.connect(address, timeout). A value of 0 means an indefinite wait with no timeout.

Default: 10000

Maximum Connections Per Host (http.client.transport.config.defaultMaxConnectionsPerHost)

The maximum number of outbound connections that will be maintained for one specific host.

Default: 300

Maximum Total Connections (http.client.transport.config.maxTotalConnections)

The total maximum number of outbound connections in the client connection pool.

Default: 500

Socket Timeout (http.client.transport.config.soTimeout)

The I/O timeout in milliseconds. This translates to the default SO_TIMEOUT for a socket. Generally, this setting is overridden by a value for the endpoint configured in Policy Manager.

Default: 120000

Stale Checking (http.client.transport.config.staleCheckingEnabled)

Enable or disable stale connection checking for the HTTP client. Stale checking determines if a server has closed a connection while the connection is pooled on the client side. This introduces a test when connections are retrieved from the connection pool, and has performance implications.

Default: true

Disable Chunked Encoding (http.client.transport.factory.bufferContent)

This flag controls chunking of all outgoing content while still using HTTP 1.1. This can be used in situations where a server may have bad chunking support, but HTTP 1.1 features such as persistent connections are still required. If turned on, this setting impacts all outgoing HTTP connections and can lead to memory scaling problems.

Default: false

Cipher Suites (http.client.transport.factory.cipherSuites)

The cipher suites to use on outgoing SSL connections. This is a comma-separated string.

Indicates cipher suites, such as 40-bit or 128-bit ciphers, to enable for outbound messages. The same value for inbound messages is set elsewhere.

Follow Redirects (http.client.transport.factory.followRedirect)

This flag controls whether or not redirects will be followed.

Default: true

Idle Connection Check Interval (http.client.transport.factory.idleCheckInterval)

The interval between checks for idle connections, in milliseconds.

Default: 30000

Idle Connection Timeout (http.client.transport.factory.idleTimeout)

The maximum time, in milliseconds, that an outbound connection can remain idle before it is closed.

Default: 300000

Retry On No Response (http.client.transport.factory.retryOnNoResponse)

This flag enables or disables a single retry when the client generates a NoHttpResponseException on a GET operation.

Default: true

Use Expect/Continue (http.client.transport.factory.useExpectContinue)

If this setting is enabled, the HTTP client will issue a request to the server that includes an “Expect” header. The message content will not be sent until the server responds with a “Continue” status. This adds overhead but avoids problems where the server is available but cannot accept a request for some reason.

Default: false

Header Templates (template.header.formatter.templates)

Headers that will be generated based on the value of an exchange or message property. Valid property names are: incoming.scheme, incoming.hostname, incoming.port, incoming.path, incoming.uri, outgoing.scheme, outgoing.hostname, outgoing.port, outgoing.path, outgoing.uri, or the name of any available header (case-insensitive).

If a property in a template cannot be found, the header is not sent. Some of these properties may not be available in some scenarios. Note that blocked header rules are applied after these headers are set, which may result in removal. Values may be preceded by “append=” or “replace=” to indicate whether the header should be appended to an existing value or should replace an existing value. By default, any generated value is appended to any existing value.

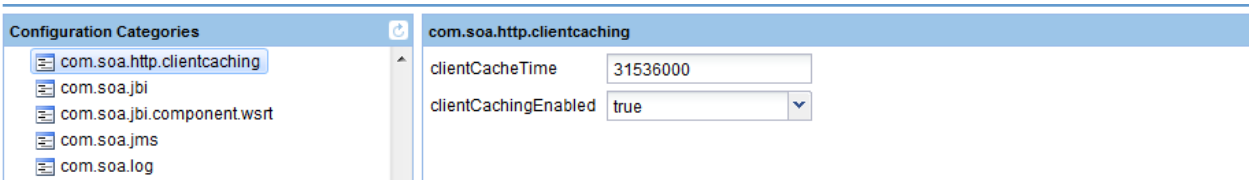
User Agent (user.agent.header.formatter.defaultUserAgent)

The default user agent header value to be used if none is specified. If there is an existing User-Agent header, this will not override the existing value.

Default: SOA Software HTTP Client Transport

com.soa.http.clientcaching

Configuration of client caching.



clientCacheTime

Sets the length of time for client to cache static resources. This is reflected in the Expires and Cache-Control headers.

Default: 31536000 (1 year)

clientCachingEnabled

Turns client caching on or off for static resources.

Default: true

com.soa.http.proxy

HTTP client proxy configuration properties. Each proxy has a set of these properties.

Target URL Pattern (url)

The URL for this proxy mapping. The URL can include an asterisk character (*) as the last character in the string. This will match any characters in the requested URL.

Proxy Server (proxy)

The proxy server address for this URL mapping.

Proxy Username (username)

The username for authenticating to the proxy server. Optional.

Proxy Password (password)

The password for authenticating to the proxy server. Optional.

Password Encrypted (isPasswordEncrypted)

Indicates whether or not the password has been encrypted.

Proxy Domain (NTLM) (domain)

The domain to authenticate within. If this property is defined, NTLM authentication is used with the proxy.

Proxy Host (NTLM) (host)

The host the authentication request is originating from. Essentially, this is the computer name for this machine. Required only for NTLM authentication.

Exclude Url (excludeurls)

The comma-separated list of patterns of URLs to exclude.

com.soa.http.resources

Configuration for a directory on the filesystem to be published as an HTTP resource.

HTTP Context Path (path)

The HTTP context path. This is a servlet path spec.

Resource Location (location)

The filesystem location of the resources to publish. This must point to a directory.

Context (context)

The application context for these resources. If omitted, the slash character (/) is used.

MIME Type Suffix Mapping (mimetypes)

Mapping of additional suffixes to MIME types. The value is a comma-separated string where each value has the form <mimetype>=<suffix> [<suffix>]*. This is optional. A small set of defaults are pre-defined.

The default is equivalent to the following MIME type list: text/css=css, text/html=htm html,text/javascript=js,text/plain=txt text,image/jpeg=jpeg jpg,image/png=png,image/tiff=tif tiff,application/json=json.

com.soa.http.route

Simple low-level client routing.

URL Pattern (pattern)

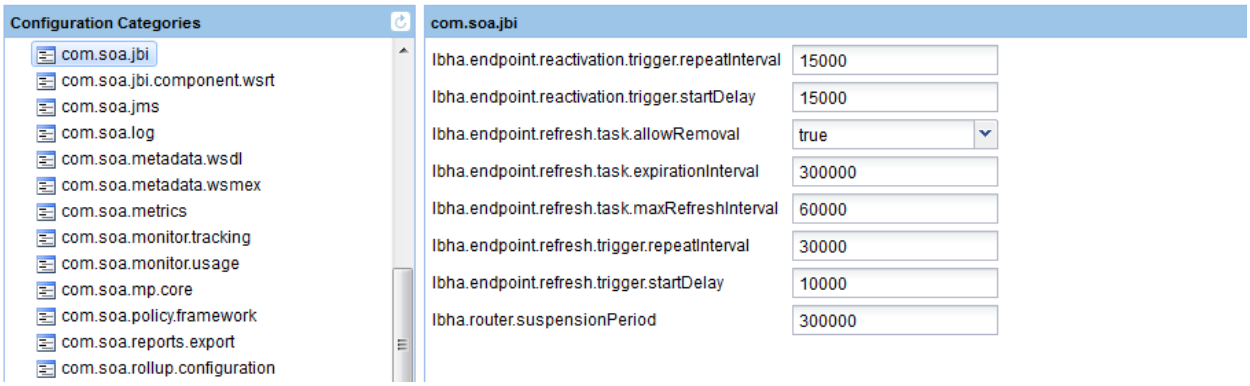
The URL pattern for this route. The URL may include an asterisk character (*) as the last character in the string. This matches any characters in the requested URL.

Target URL (url)

The target URL for this mapping.

com.soa.jbi

Configuration of the JBI router properties.



Endpoint Reactivation Interval (lbha.endpoint.reactivation.trigger.repeatInterval)

The interval in milliseconds between endpoint reactivation scans.

Default: 15000

Reactivation Start Delay (lbha.endpoint.reactivation.trigger.startDelay)

The time in milliseconds after which endpoint reactivation scans will begin, after the bundle has started.

Default: 15000

Endpoint Refresh Check Interval (lbha.endpoint.refresh.trigger.repeatInterval)

The interval in milliseconds between endpoint refresh scans.

Default: 30000

Endpoint Refresh Start Delay (lbha.endpoint.refresh.trigger.startDelay)

The time in milliseconds after which endpoint refresh scans will begin, after the bundle has started.

Default: 10000

Endpoint Suspension Interval (lbha.router.suspensionPeriod)

The time that an endpoint will be suspended for when it is marked as failed.

Default: 300000

Maximum Endpoint Refresh Interval (lbha.endpoint.refresh.task.maxRefreshInterval)

The maximum amount of time in milliseconds before the refresh of endpoints. During an endpoint refresh scan, if the max refresh interval has been reached the endpoints will be refreshed.

Default: 60000

Endpoint Expiration Interval (lbha.endpoint.refresh.task.expirationInterval)

The time in milliseconds that an endpoint can be inactive (not called) before it is removed from the router cache.

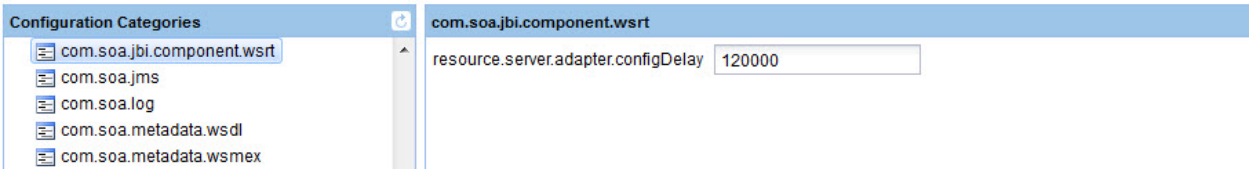
Default: 300000

Remove Inactive Endpoints (lbha.endpoint.refresh.task.allowRemoval)

A flag indicating whether inactive endpoints should be removed.

com.soa.jbi.component.wsrt

Configuration of the WS-ResourceProvider framework.



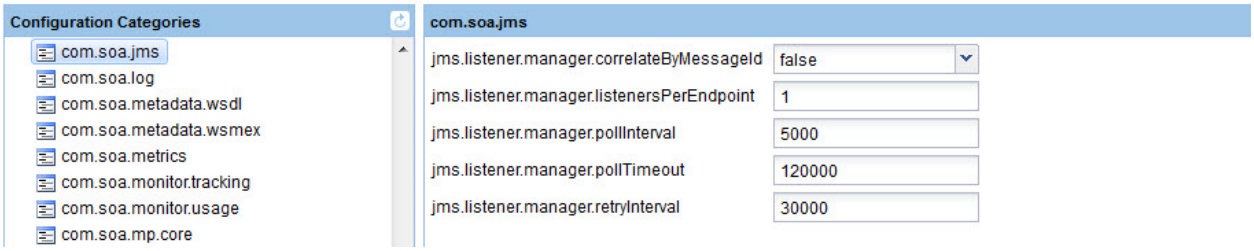
Configuration Delay (resource.server.adapter.configDelay)

The time in milliseconds that the framework will wait for providers to register before queries result in error.

Default: 120000

com.soa.jms

JMS configuration properties.



Correlate by Message ID (jms.listener.manager.correlateByMessageId)

Controls whether responses are sent with the correlation ID of the incoming request or with the request message ID.

Default: false

Listeners Per Endpoint (jms.listener.manager.listenersPerEndpoint)

The number of listener threads per endpoint. This is the number of polling threads that will be created for each listener. Note that each request is handled in a separate thread.

Default: 1

Listener Poll Timeout (jms.listener.manager.pollInterval)

The timeout value for each polling thread when attempting a read operation; the frequency with which the listener polls for a message.

Default: 5000

Poll Timeout (jms.listener.manager.pollTimeout)

The amount of time that the polling thread will wait before tearing down the connection and rebuilding it when there is no activity. This is useful for clients that do not report server restarts properly. A value of 0 disables this behavior.

Default: 120000

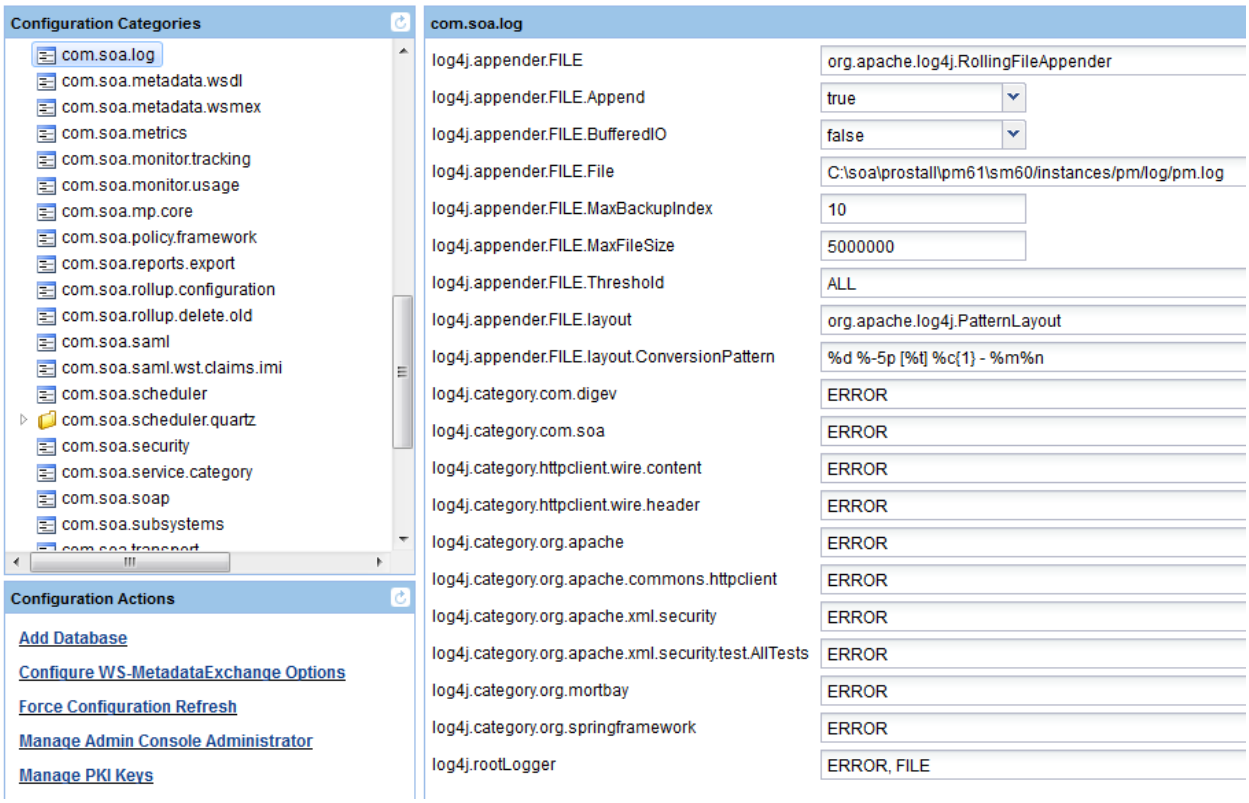
Read Retry Interval (jms.listener.manager.retryInterval)

The time in milliseconds between read operations when there is a failure.

Default: 30000

com.soa.log

Configuration settings for logging. All settings are based on Log4J configuration.



File Appender (log4j.appender.FILE)

Log class for file appender.

Default: org.apache.log4j.RollingFileAppender

Append (log4j.appender.FILE.Append)

Append to file.

Default: false

Buffered (log4j.appender.FILE.BufferedIO)

I/O Buffering.

Default: false

Logs location (log4j.appender.FILE.File)

Location for the log files.

Default: ${product.home.dir}/instances/${container.name}/log/${container.name}.log

Maximum files (log4j.appender.FILE.MaxBackupIndex)

Maximum number of backup files.

Default: 10

Maximum file size (log4j.appender.FILE.MaxFileSize)

Maximum file size.

Default: 5000000

File Appender Threshold (log4j.appender.FILE.Threshold)

File appender threshold.

Default: ALL

File Appender Layout (log4j.appender.FILE.layout)

File appender layout.

Default: org.apache.log4j.PatternLayout

File Appender Pattern (log4j.appender.FILE.layout.ConversionPattern)

File appender pattern.

Default: %d %-5p %t %c{1} - %m%n

com.digev logging (log4j.category.com.digev)

com.digev package logging setting.

Default: ERROR

com.soa logging (log4j.category.com.soa)

com.soa package logging setting.

Default: ERROR

log4j.category.httpclient.wire.content

Log category for HTTP client wire content logging. When set to DEBUG, the httpclient.wire.content and httpclient.wire.header contexts provide low-level logging of HTTP body content and headers.

log4j.category.httpclient.wire.header

Log category for HTTP client header logging. When set to DEBUG, the httpclient.wire.content and httpclient.wire.header contexts provide low-level logging of HTTP body content and headers.

log4j.category.org.apache

Log category for logging from Apache libraries.

log4j.category.org.apache.commons.httpclient

Log category for HTTP client.

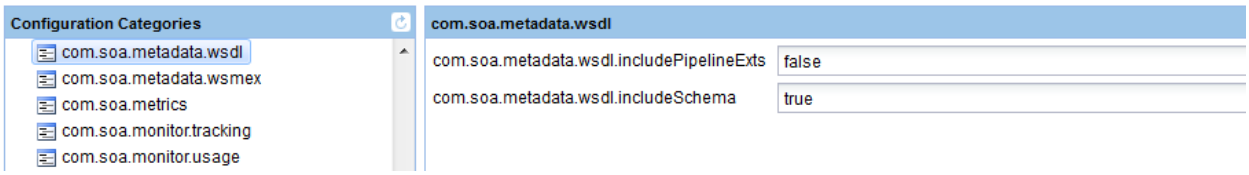
rootLogger (log4j.rootLogger)

Root loggers.

Default: ERROR FILE

com.soa.metadata.wsdl

Configuration of the metadata client.



Include Schema in WSDL (com.soa.metadata.wsdl.includeSchema)

Indicates whether schemas should be downloaded with WSDL definitions.

Default: true

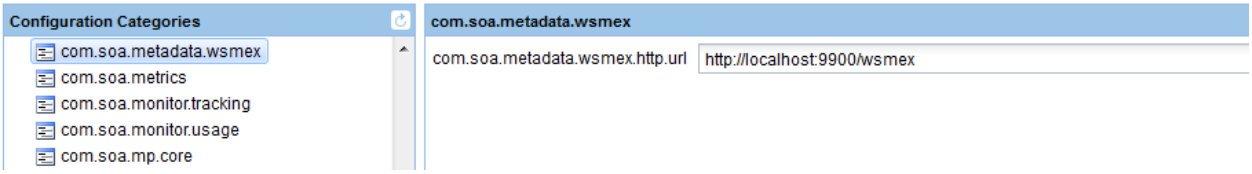
Include Pipeline Extensions in WSDL (com.soa.metadata.wsdl.includePipelineExts)

Indicates whether pipeline extensions should be downloaded with WSDL definitions.

Default: false

com.soa.metadata.wsmex

WS-Mex client configuration.



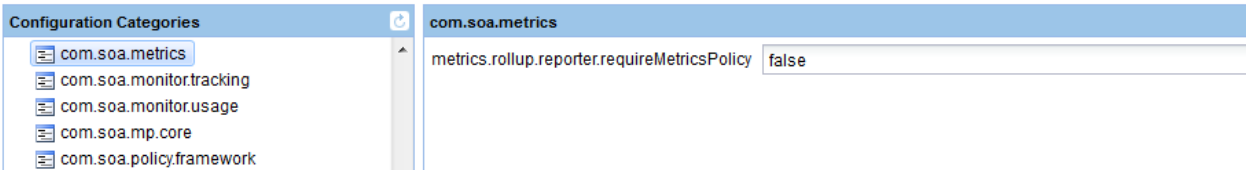
WS-Mex Service URL (com.soa.metadata.wsmex.http.url)

The WS-Mex service URL. This is the basic URL that bootstraps communication from Network Director to Policy Manager. If the Network Director hostname is ever changed, it must be changed here also.

Default: http://localhost:9900/wsmex

com.soa.metrics

Configuration of metric information.



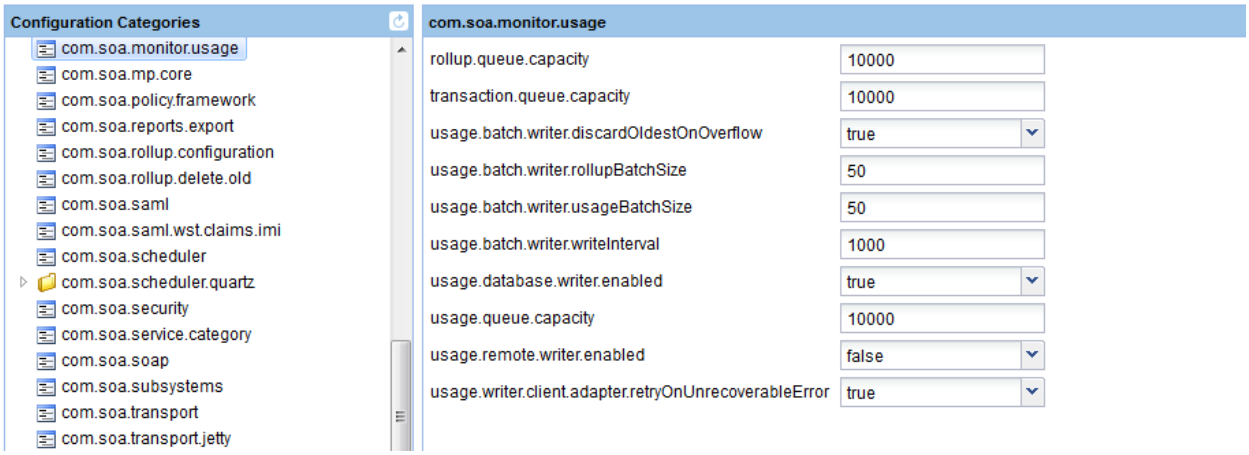
metrics.rollup.reporter.requireMetricsPolicy

Indicates whether metrics rollup information is loaded into the database automatically (false) or requires a policy in place (true).

Default: false.

com.soa.monitor.usage

Configuration for the usage monitoring services. Controls database writers, usage writers, and the container to write the counters and logs.



Rollup Queue size (rollup.queue.capacity)

The maximum number of entries in the rollup queue.

Default: 10000

Transaction Queue size (transaction.queue.capacity)

The maximum number of entries in the transaction queue.

Default: 10000

Discard Oldest on Overflow (usage.batch.writer.discardOldestOnOverflow)

Indicates whether the oldest queue entry should be discarded on queue overflow. If set to false, the newest entry is discarded when the queue is full.

Default: true

Rollup Batch Size (usage.batch.writer.rollupBatchSize)

The batch size for rollup recording. A batch is written if it reaches this limit or if the write interval has been exceeded.

Default: 50

Usage Batch Size (usage.batch.writer.usageBatchSize)

The batch size for usage recording. A batch is written if it reaches this limit or if the write interval has been exceeded.

Default: 50

Batch Write Interval (usage.batch.writer.writeInterval)

The maximum interval between batch writes, in milliseconds.

Default: 1000

Database Writer Enabled (usage.database.writer.enabled)

Indicates whether the database usage writer is enabled.

Default: true

Usage Queue size (usage.queue.capacity)

The maximum number of entries in the usage queue.

Default: 10000

Remote Writer Enabled (usage.remote.writer.enabled)

Indicates whether the remote usage writer is enabled.

Default: false

Retry on Unrecoverable Error (usage.writer.client.adapter.retryOnUnrecoverableError)

Indicates whether a remote written batch should be retried if an unrecoverable error is encountered. Recoverable errors include HTTP connection failures; unrecoverable errors include HTTP 404 Unrecoverable and others.

Default: true

com.soa.monitoring.tracking

Configuration for transaction tracking.

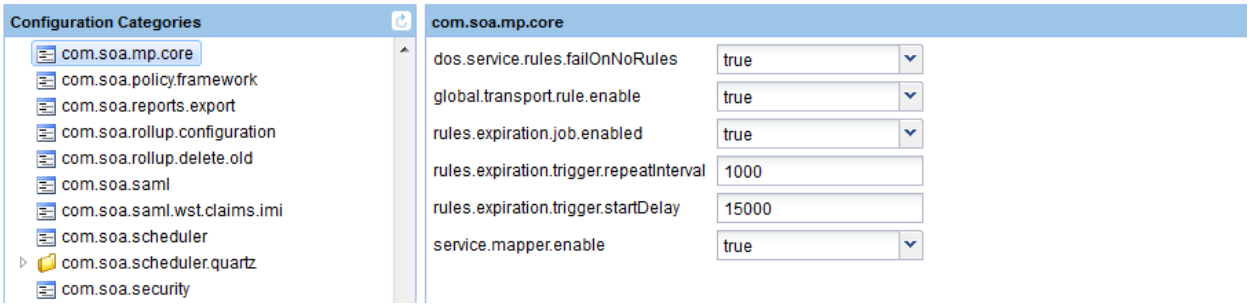
Enable Transaction Correlation (service.correlation.job.enabled)

Indicates whether the transaction correlation job is enabled. If this setting is enabled, database connections that take longer than expected can be written to the system log file.

Default: true

com.soa.mp.core

Configuration of the DoS rules properties, including when to refresh and when to expire.



Fail if no Rules Defined (dos.service.rules.failOnNoRules)

Fail if no rules are defined for a service. Has no impact if the transport rules are disabled.

Default: true

Enable Transport Rules (global.transport.rule.enable)

Indicates whether execution of the transport rules is enabled.

Default: true

Enable Expiration checking (rules.expiration.job.enabled)

Enables or disables the expiration checking job. If the expiration job is disabled, any DoS rules, specifically blacklists, will not expire.

Default: true

Expiration Checking Interval (rules.expiration.trigger.repeatInterval)

The interval, in milliseconds, between checks for rules expiration.

Default: 1000

Start Delay (rules.expiration.trigger.startDelay)

The time, in milliseconds, before expiration checks will begin when the bundle is started.

Default: 15000

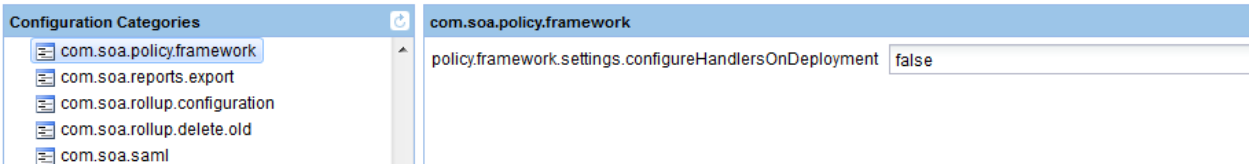
Enable Transport Rule Service Mapper (service.mapper.enable)

Indicates whether the rule service mapper is enabled.

Default: true

com.soa.policy.framework

Configuration of the policy framework.



policy.framework.settings.configureHandlersOnDeployment

If set to true, all policy handlers are initialized at the time of deployment. If set to false, policy handlers are initialized on first request.

If true, deployment will take longer and more memory consumption may be seen, but no messages will suffer performance penalties while waiting for policy handlers to be initialized. If false, the first message to a virtual service option will see some additional latency for policy handler initialization, but deployment time and overall container memory consumption will be reduced.

Default: false

com.soa.provision

Provisioning of bundles and/or configuration.

Poll Interval (com.soa.provision.poll)

The poll interval in milliseconds.

Default: 2000

No Initial Delay (com.soa.provision.noInitialDelay)

Indicates whether the scanners should be initialized immediately on startup or in the scanning thread. This allows configuration events to be handled synchronously (true) or asynchronously (false).

Default: true

Monitored Directory (com.soa.provision.file.dir)

The directory to monitor for filesystem scanners. If this property exists, a filesystem scanner will be created.

File Filter (com.soa.provision.file.filter)

An optional filter that may be used to control what files are processed. This is a regular expression that follows the rules for String.match().

OBR Descriptor URL (com.soa.provision.obr.repository)

The location (URL) of an OBR descriptor file that will be used to locate resources to be provisioned. If this property exists, an OBR scanner will be created. Note that either this or com.soa.provision.file.dir should be used; one or the other but not both. They cannot be used simultaneously.

OBR Exclude List (com.soa.provision.obr.exclude)

A list of configuration PIDs that should be ignored by the OBR scanner. This is a space-separated list. Each value may end with an asterisk wildcard (*) which will match any characters.

com.soa.reports.export

Usage and alerts export configuration.

maximum number of records to fetch in single query when exporting (usagelog.export.dao.blockSize)

The maximum number of records for one query.

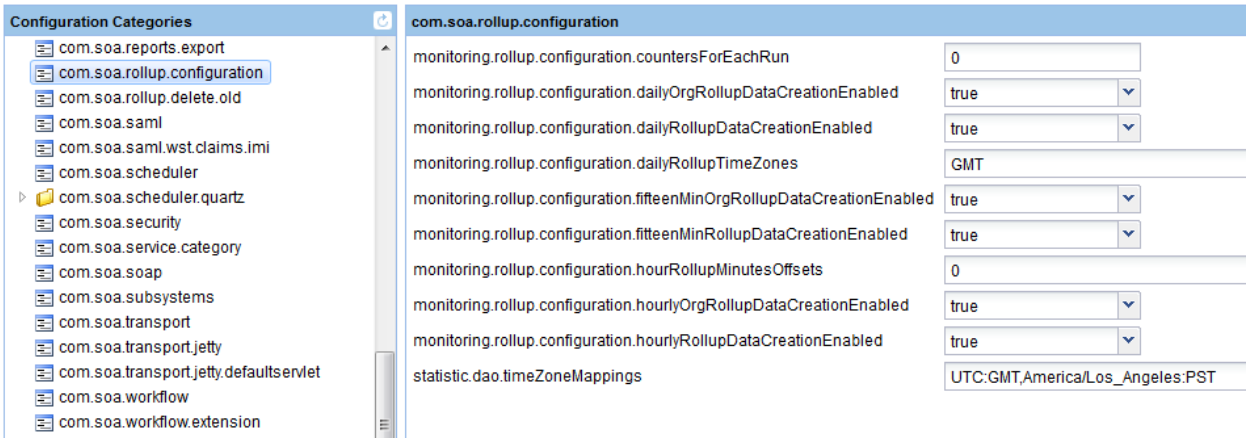
Default: 10000

com.soa.rollup.configuration

Configuration of rollup metrics.

It's important to get time zone settings correct if you want to get hourly or daily charts for more than one time zone.

For example, some parts of the world such as India are in a time zone that differs from GMT not just in one-hour increments, but in a half-hour. 6am in Los Angeles in 6:30pm in Mumbai. To get accurate rollup metrics for these different time zones, you would need to configure the time zones and keep data for the half-hour increments.



Counters for Each Run of Historical Rollups (monitoring.rollup.configuration.countersForEachRun)

Counters for Each Run of Historical Rollup Jobs. 0 means unlimited.

Default: 0

Enable Daily Organization Rollups (monitoring.rollup.configuration.dailyOrgRollupDataCreationEnabled)

Enable/disable daily organizational rollups.

Default: true

Enable Daily Rollups (monitoring.rollup.configuration.dailyRollupDataCreationEnabled)

Enable/disable daily rollups.

Default: true

Daily Rollup Timezones (monitoring.rollup.configuration.dailyRollupTimeZones)

Time zones for daily rollups. You can add additional time zones.

Default: GMT

Enable Fifteen Minute Organization Rollups (monitoring.rollup.configuration.fifteenMinOrgRollupDataCreationEnabled)

Enable/disable 15-minute organizational rollups.

Default: true

Enable Fifteen Minute Rollups (monitoring.rollup.configuration.fitteenMinRollupDataCreationEnabled)

Enable/disable 15-minute rollups.

Default: true

Hourly Rollup Offset (monitoring.rollup.configuration.hourRollupMinutesOffsets)

Hourly rollup minutes offset. For example, if you want rollup information for a time zone that has an offset of a half-hour, such as India, you would write: **0,30**.

Default: 0

Enable Hourly Organization Rollups (monitoring.rollup.configuration.hourlyOrgRollupDataCreationEnabled)

Enable/disable hourly organizational rollups.

Default: true

Enable Hourly Rollups (monitoring.rollup.configuration.hourlyRollupDataCreationEnabled)

Enable/disable hourly rollups.

Default: true

Timezone Mappings (statistic.dao.timeZoneMappings)

Time zone mappings. Some defined time zones are the same as others. You can support multiple time zones that have the same definition by mapping. For example, Los Angeles and PST are officially two different time zones but have the same definition, so they are mapped. One set of rollup metrics can then serve for both time zones. You can add additional time zone mappings following the format of the default.

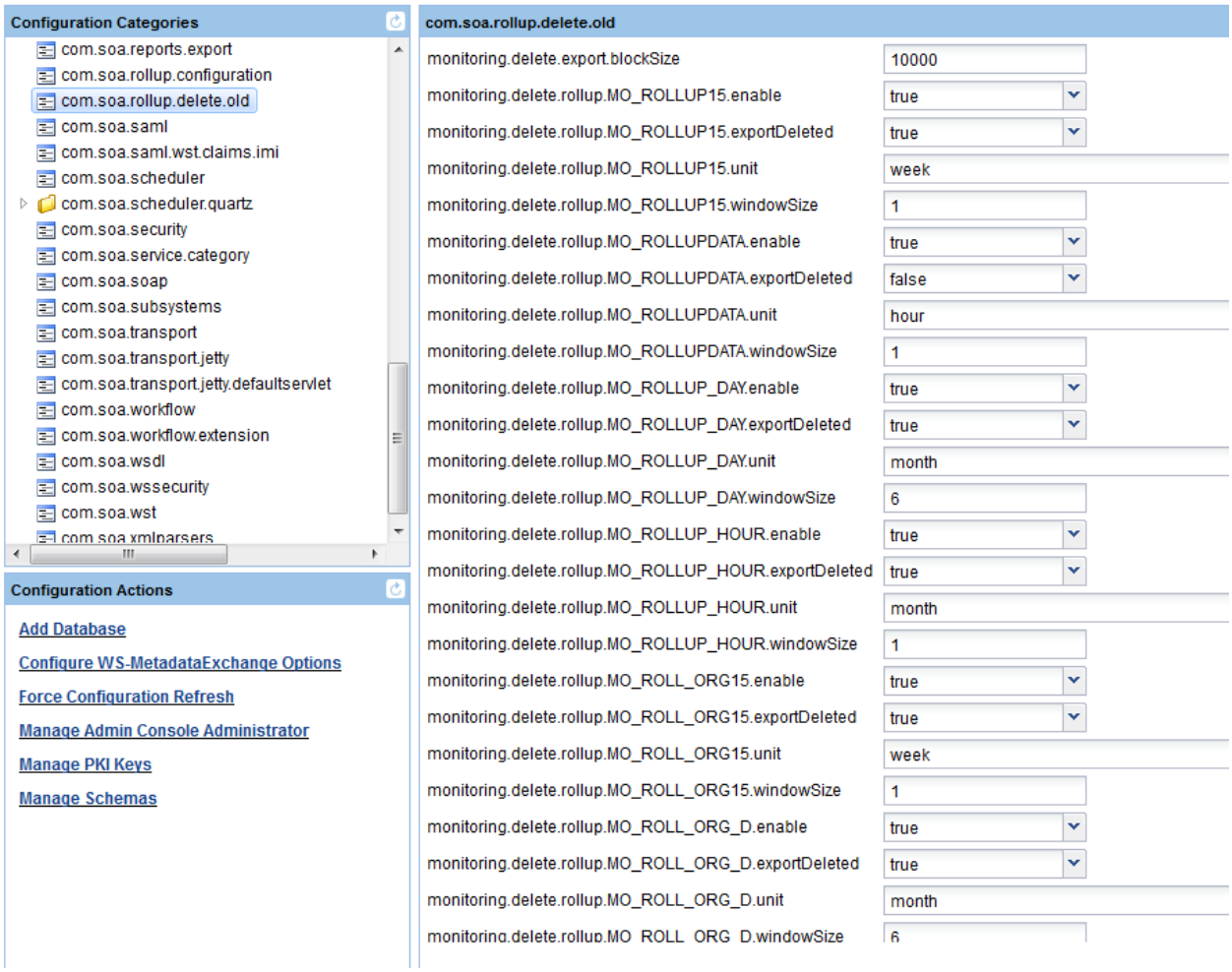
Default: UTC:GMTAmerica/Los_Angeles:PST

com.soa.rollup.delete.old

Configuration settings for metric rollup deletion. These settings control when and how often the rollup data is deleted, and which data is deleted.

WARNING: in process rollup deletion can be very expensive and even disruptive if database tables have already filled and have large volumes of data. It is best to enable this feature only when the tables have already been purged.

Note: Before deleting, it's a good idea to export a copy of the data or back up the database.



enable usage data deletion (monitoring.delete.usage.enable)

Allows deletion of data. If set to false, no data is deleted.

Default: true

frequency of usage data deletion (monitoring.delete.usage.windowSize)

Default: 1

enable export of deleted usage records (monitoring.delete.usage.exportDeleted)

monitoring.delete.usage.unit=week

Default: true

include message when exporting deleted usage records (monitoring.delete.usage.includeMessages)

Default: true

enable deletion from MO_ROLLUPDATA (monitoring.delete.rollup.MO_ROLLUPDATA.enable)

Default: true

frequency of roll-up deletion from MO_ROLLUPDATA (monitoring.delete.rollup.MO_ROLLUPDATA.windowSize)

Default: 1

enable export of deleted records from MO_ROLLUPDATA (monitoring.delete.rollup.MO_ROLLUPDATA.exportDeleted)

monitoring.delete.rollup.MO_ROLLUPDATA.unit=hour

Default: false

enable deletion from MO_ROLLUP15 (monitoring.delete.rollup.MO_ROLLUP15.enable)

Default: true

frequency of roll-up deletion from MO_ROLLUP15 (monitoring.delete.rollup.MO_ROLLUP15.windowSize)

Default: 1

enable export of deleted records from MO_ROLLUP15 (monitoring.delete.rollup.MO_ROLLUP15.exportDeleted)

monitoring.delete.rollup.MO_ROLLUP15.unit=week

Default: true

enable deletion from MO_ROLL_ORG15 (monitoring.delete.rollup.MO_ROLL_ORG15.enable)

Default: true

frequency of roll-up deletion from MO_ROLL_ORG15 (monitoring.delete.rollup.MO_ROLL_ORG15.windowSize)

Default: 1

enable export of deleted records from MO_ROLL_ORG15 (monitoring.delete.rollup.MO_ROLL_ORG15.exportDeleted)

monitoring.delete.rollup.MO_ROLL_ORG15.unit=week

Default: true

enable deletion from MO_ROLLUP_HOUR (monitoring.delete.rollup.MO_ROLLUP_HOUR.enable)

Default: true

frequency of roll-up deletion from MO_ROLLUP_HOUR (monitoring.delete.rollup.MO_ROLLUP_HOUR.windowSize)

Default: 1

enable export of deleted records from MO_ROLLUP_HOUR (monitoring.delete.rollup.MO_ROLLUP_HOUR.exportDeleted)

monitoring.delete.rollup.MO_ROLLUP_HOUR.unit=month

Default: true

enable deletion from MO_ROLL_ORG_H (monitoring.delete.rollup.MO_ROLL_ORG_H.enable)

Default: true

frequency of roll-up deletion from MO_ROLL_ORG_H (monitoring.delete.rollup.MO_ROLL_ORG_H.windowSize)

Default: 1

enable export of deleted records from MO_ROLL_ORG_H (monitoring.delete.rollup.MO_ROLL_ORG_H.exportDeleted)

monitoring.delete.rollup.MO_ROLL_ORG_H.unit=month

Default: true

enable deletion from MO_ROLLUP_DAY (monitoring.delete.rollup.MO_ROLLUP_DAY.enable)

Default: true

frequency of roll-up deletion from MO_ROLLUP_DAY (monitoring.delete.rollup.MO_ROLLUP_DAY.windowSize)

Default: 6

enable export of deleted records from MO_ROLLUP_DAY (monitoring.delete.rollup.MO_ROLLUP_DAY.exportDeleted)

monitoring.delete.rollup.MO_ROLLUP_DAY.unit=month

Default: true

enable deletion from MO_ROLL_ORG_D (monitoring.delete.rollup.MO_ROLL_ORG_D.enable)

Default: true

frequency of roll-up deletion from MO_ROLL_ORG_D (monitoring.delete.rollup.MO_ROLL_ORG_D.windowSize)

Default: 6

enable export of deleted records from MO_ROLL_ORG_D (monitoring.delete.rollup.MO_ROLL_ORG_D.exportDeleted)

monitoring.delete.rollup.MO_ROLL_ORG_D.unit=month

Default: true

Archive Deleted Rollups in ZIP (monitoring.delete.saveAsZip)

Indicates whether deleted rollups should be saved in a ZIP file

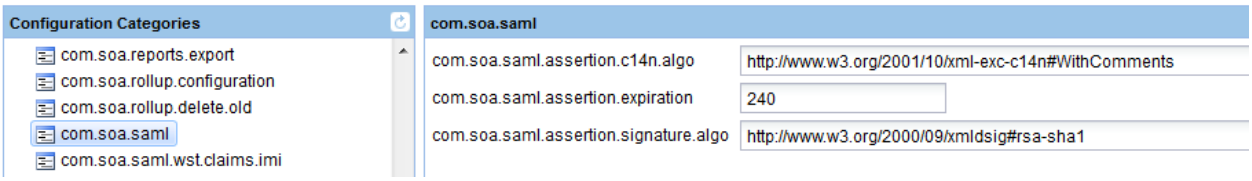
Default: true

maximum number of records to fetch in single query when exporting (monitoring.delete.export.blockSize)

Default: 10000

com.soa.saml

SAML generation configuration.



SAML Expiration (com.soa.saml.assertion.expiration)

SAML Assertion expiration time in minutes.

Default: 240

SAML Signature Algorithm (com.soa.saml.assertion.signature.algo)

Default signature algorithm used for signing SAML assertions.

Default: http://www.w3.org/2000/9/xmldsig#rsa-sha1

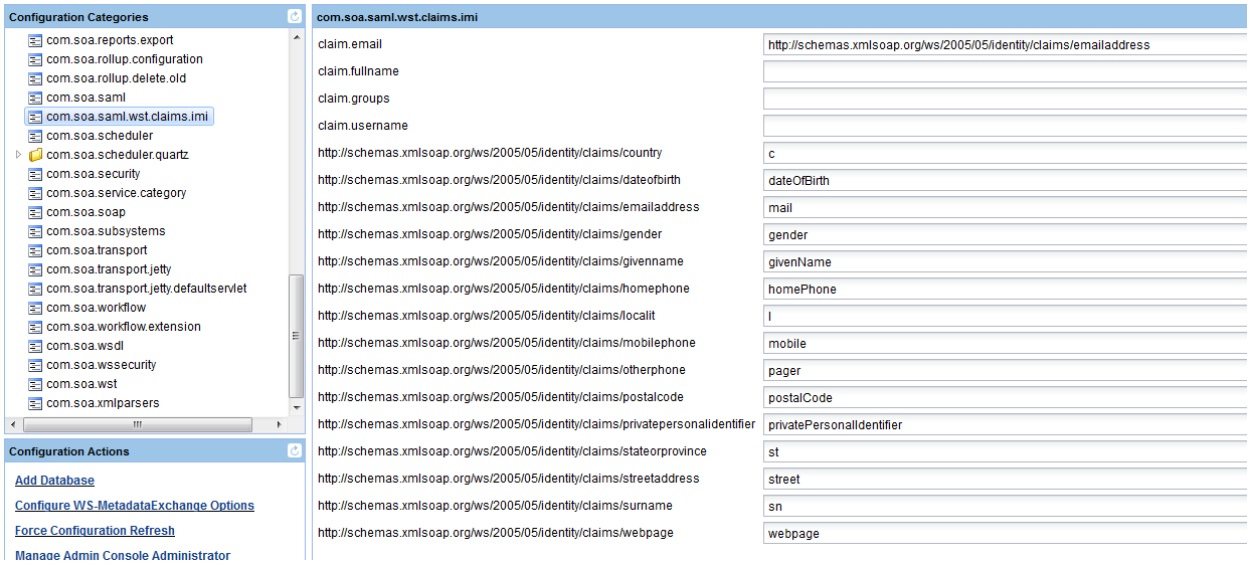
SAML C14N Algorithm (com.soa.saml.assertion.c14n.algo)

Default canonicalization algorithm used for signing SAML assertions.

Default: http://www.w3.org/2001/10/xml-exc-c14n#WithComments

com.soa.saml.wst.claims.imi

Configuration of SAML claims.



claim.email

Claim URI for an email address.

claim.fullname

Claim URI for a full name.

claim.groups

Claim URI for a list of groups.

claim.username

Claim URI for a user name.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/country

Identity system attribute name to fill the country claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dateofbirth

Identity system attribute name to fill the date of birth claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Identity system attribute name to fill the email address claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/gender
Identity system attribute name to fill the gender claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Identity system attribute name to fill the given name claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/homephone
Identity system attribute name to fill the home phone claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/locality
Identity system attribute name to fill the locality claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone
Identity system attribute name to fill the mobile phone claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone
Identity system attribute name to fill the other phone claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcode
Identity system attribute name to fill the postal code claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier
Identity system attribute name to fill the private personal identifier claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/stateorprovince
Identity system attribute name to fill the state or province claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddress
Identity system attribute name to fill the street address claim with.

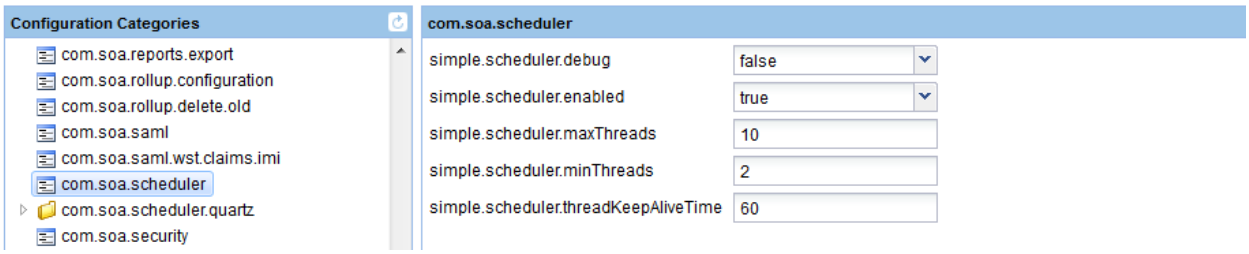
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Identity system attribute name to fill the surname (last name) claim with.

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/webpage
Identity system attribute name to fill the webpage claim with.

com.soa.scheduler

General Simple Scheduler configuration. You can optimize these settings but otherwise we recommend you do not change them.

The cache uses the Simple Scheduler, so it's important that it is not disabled.



Simple Scheduler Debug (simple.scheduler.debug)

Indicates whether debug information about the executed job should be printed to System.out.

Default: false

Disable scheduled Jobs (simple.scheduler.enabled)

Stops scheduled jobs from running. Although this setting can be disabled, it is not recommended.

Default: true

Minimum number of threads (simple.scheduler.minThreads)

The minimum number of threads.

Default: 2

Maximum number of threads (simple.scheduler.maxThreads)

The maximum number of threads.

Default: 10

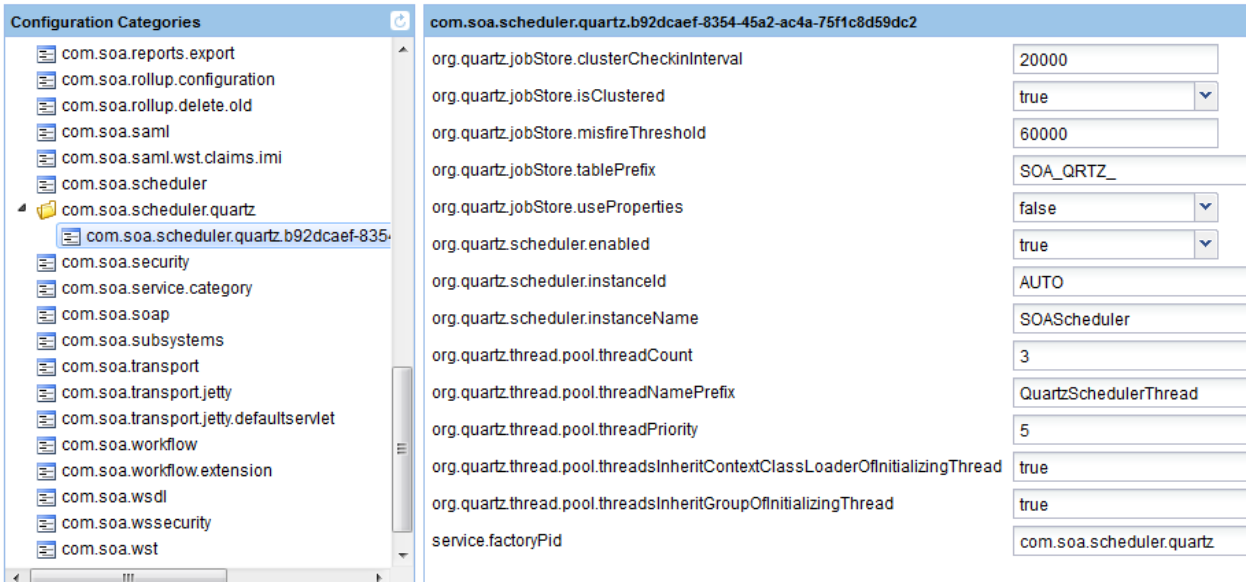
Number of seconds to keep idle threads in the pool (simple.scheduler.threadKeepAliveTime)

The number of seconds to keep idle threads in the pool.

Default: 60

com.soa.scheduler.quartz

The SOA Software Scheduler Service: Quartz scheduler configuration for the subsystems scheduler. These jobs can be disabled on a short-term or long-term basis if needed.



Instance Name (org.quartz.scheduler.instanceName)

The Quartz scheduler instance name.

Default: SOAScheduler

Node Instance ID (org.quartz.scheduler.instanceId)

The instance ID for this node in the Quartz cluster. By using the default setting, AUTO, Quartz will generate one.

Default: AUTO

Quartz Table Prefix (org.quartz.jobStore.tablePrefix)

Quartz table prefix. This string is prefixed to database table names used by Quartz.

Default: SOA_QRTZ_

Use Properties (org.quartz.jobStore.useProperties)

This instructs the JDBCJobStore that all values in JobDataMaps will be Strings and therefore can be stored as name-value pairs rather than storing more complex objects in their serialized form in the BLOB column.

Default: false

Clustered (org.quartz.jobStore.isClustered)

Indicates whether clustered scheduling is enabled (true) or disabled (false).

Default: true

Cluster Checkin Interval (org.quartz.jobStore.clusterCheckinInterval)

The time in milliseconds between polls to check on the state of the cluster. This determines the responsiveness to failed cluster members.

Default: 20000

Misfire Threshold (org.quartz.jobStore.misfireThreshold)

The number of milliseconds the scheduler will tolerate a trigger to pass its next-fire-time by before being considered “misfired.”

Default: 60000

Disable scheduled Jobs (org.quartz.scheduler.enabled)

Stops scheduled jobs from running.

Default: true

Persistent Scheduler Threads (org.quartz.thread.pool.threadCount)

The number of threads in the persistent job pool.

Default: 3

Persistent Thread Priority (org.quartz.thread.pool.threadPriority)

The priority of scheduled threads associated with the persistent scheduler.

Default: 5

Inherit Parent Thread ClassLoader (org.quartz.thread.pool.threadsInheritContextClassLoaderOfInitializingThread)

Indicates whether persistent job threads should inherit the parent context classloader.

Default: true

Inherit Parent Thread Group (org.quartz.thread.pool.threadsInheritGroupOfInitializingThread)

Indicates whether persistent job threads should inherit the parent group.

Default: true

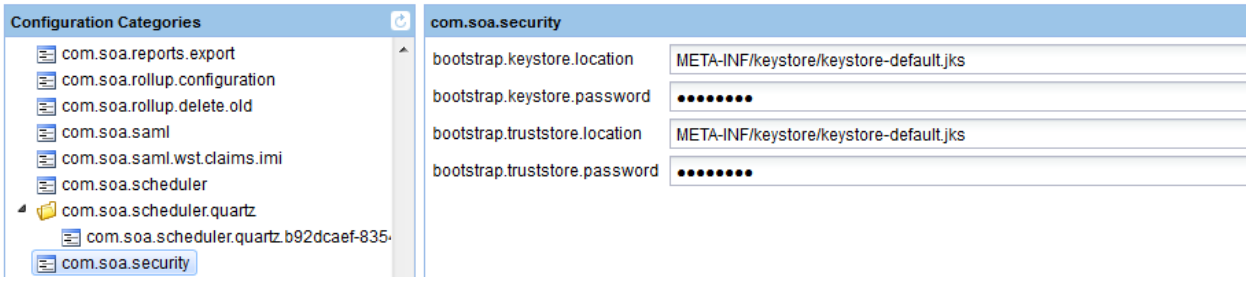
Thread Group Name (org.quartz.thread.pool.threadNamePrefix)

Thread Group Name.

Default: QuartzSchedulerThread

com.soa.security

Configuration of default key store and trust store properties.



Key Store location (bootstrap.keystore.location)

The key store location.

Default: META-INF/keystore/keystore-default.jks

Key Store Password (bootstrap.keystore.password)

The key store password.

Default: changeit

Trust Store location (bootstrap.truststore.location)

The trust store location.

Default: META-INF/keystore/keystore-default.jks

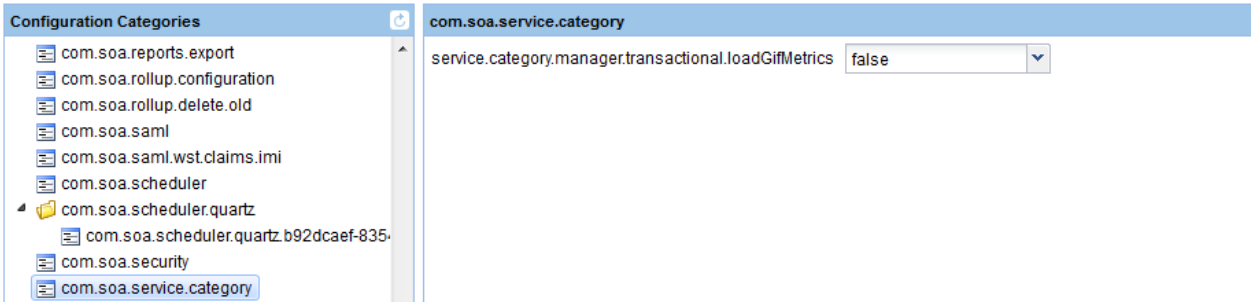
Trust Store Password (bootstrap.truststore.password)

The trust store password.

Default: changeit

com.soa.service.category

Configuration of service category. This property is not generally used, but can be used in combination with turning off some rollup data settings.



service.category.manager.transactional.loadGifMetrics

Category Manager GIF metrics calculation.

Default: false

com.soa.soap

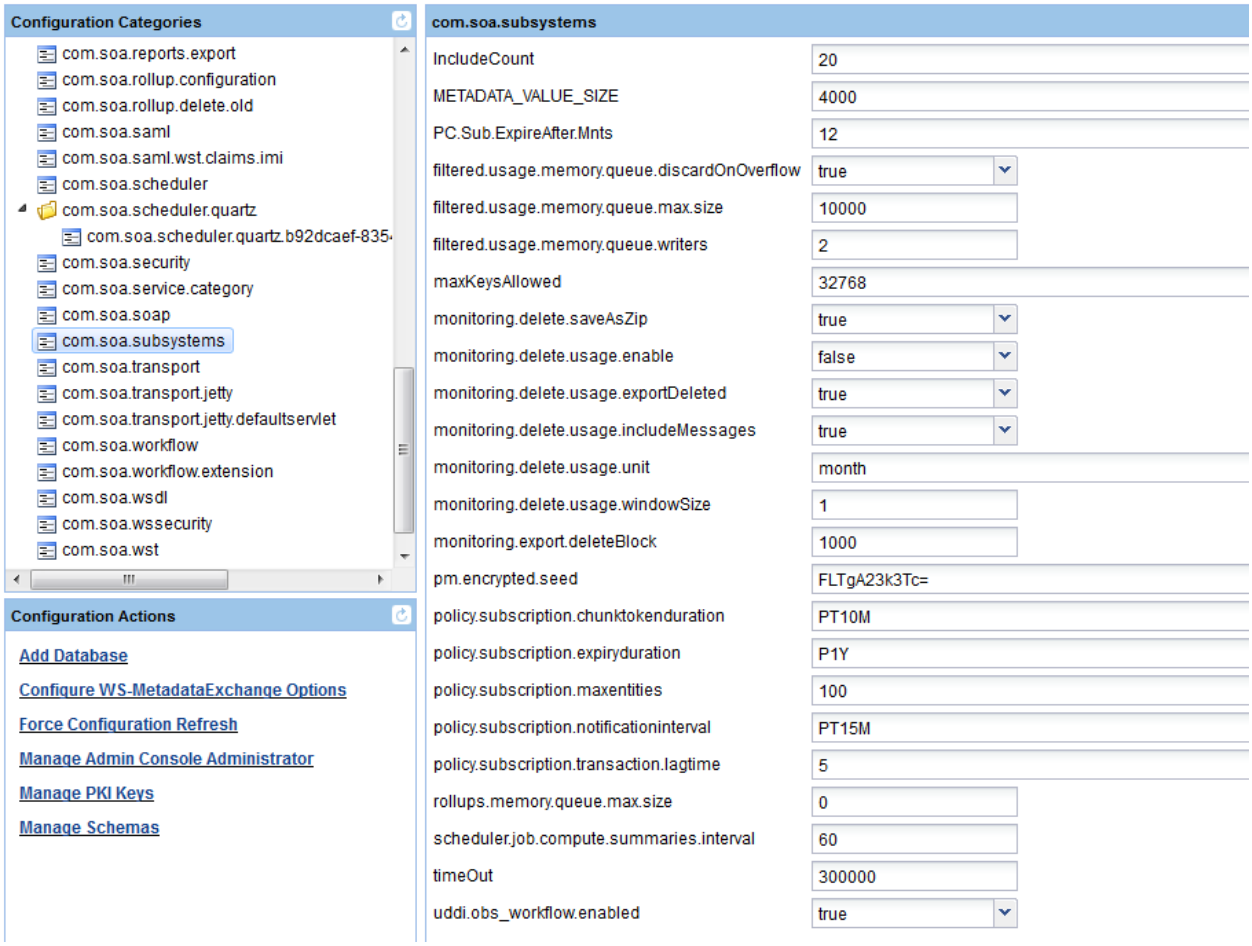
Configuration of SOAP settings.

soap.action.selector.supportNonUniqueSOAPActions

Indicates whether non-unique SOAP actions are supported.

com.soa.subsystems

SOA Software System Services: configuration of subsystems such as monitoring and policy.



Max Usage Queue Size (filtered.usage.memory.queue.max.size)

Maximum number of entries in the filtered queue.

Default: 10000

Max Rollup Queue Size (rollups.memory.queue.max.size)

Maximum number of entries in the rollup queue.

Default: 0

Discard Usage on Overflow (filtered.usage.memory.queue.discardOnOverflow)

Indicates whether additional entries should be dropped when the number of entries in the usage queue reaches the limit. If set to false, the attempt to add to the queue is blocked. Blocking could have significant performance implications.

Default: true

Usage Writer Threads (filtered.usage.memory.queue.writers)

The number of threads dedicated to writing usage data to the database.

Default: 2

Compute Summaries Interval (scheduler.job.compute.summaries.interval)

The interval in seconds for the compute summaries job.

Default: 60

Enable workflow for OBS (uddi.obs_workflow.enabled)

Controls whether security and workflow is enabled for UDDI APIs.

Default: true

Federated Search Timeout (timeOut)

Federated UDDI search timeout in milliseconds.

Default: 300000

Truncate Usage Tables (monitoring.delete.usage.enable)

If set to true, the usage log tables are periodically truncated by deleting the oldest records.

Default: false

Export Truncated Usage Data (monitoring.delete.usage.exportDeleted)

If set to true, the data deleted from the usage tables is exported to the file system. This property only applies if truncation of usage tables is enabled.

Default: true

Export Truncated Messages (monitoring.delete.usage.includeMessages)

If set to true, the audited messages will also be exported when deleted. This property only applies if exporting of truncated usage data is enabled.

Default: true

monitoring.delete.usage.unit (monitoring.delete.usage.unit)

Identifies the unit of measure of the window of usage records that will be kept in the database (see monitoring.delete.usage.windowSize). This property only applies if monitoring.delete.usage.enable is set to true.

Default: month

Usage Record Window Size (monitoring.delete.usage.windowSize)

Specifies the window size in units (see monitoring.delete.usage.unit) of usage records that will be kept in the database. This property only applies if truncation of usage tables is enabled.

Default: 1

Archive Deleted Rollups in ZIP (monitoring.delete.saveAsZip)

Indicates whether deleted rollups should be saved in a ZIP file.

Default: true

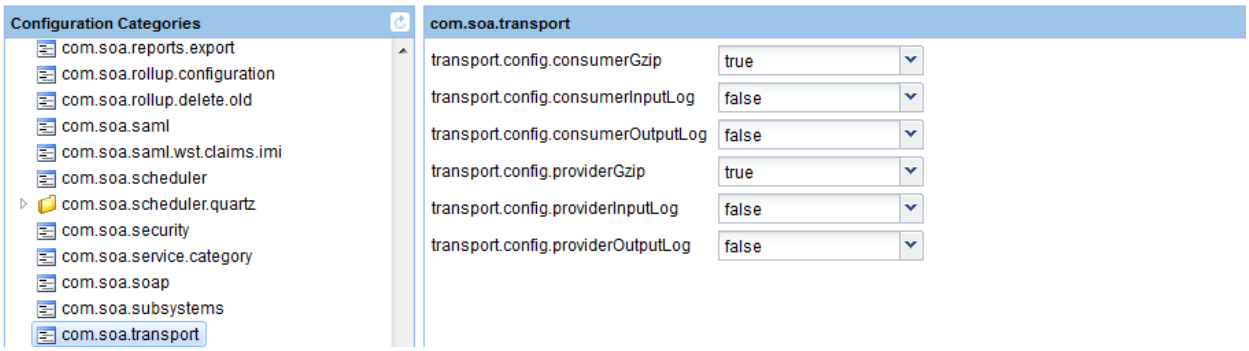
Rollup Delete Batch Size (monitoring.export.deleteBlock)

The number of rollup records that should be deleted in one call to the database.

Default: 1000

com.soa.transport

Configuration of transport properties.



Consumer gzip Support (transport.config.consumerGzip)

Enable or disable client-side gzip encoding/decoding support.

The Accept-Encoding gzip format means that the response can be zipped to save bandwidth. This value indicates whether gzip is supported.

Default: true

Provider gzip Support (transport.config.providerGzip)

Enables or disables server-side gzip encoding/decoding support.

Default: true

Consumer Logging Support (transport.config.consumerInputLog)

Enables or disables client-side input logging support.

Default: false

Provider Logging Support (transport.config.providerInputLog)

Enables or disables of server-side input logging support.

Default: false

Consumer Output Logging Support (transport.config.consumerOutputLog)

Enables or disables client-side output logging support.

Default: false

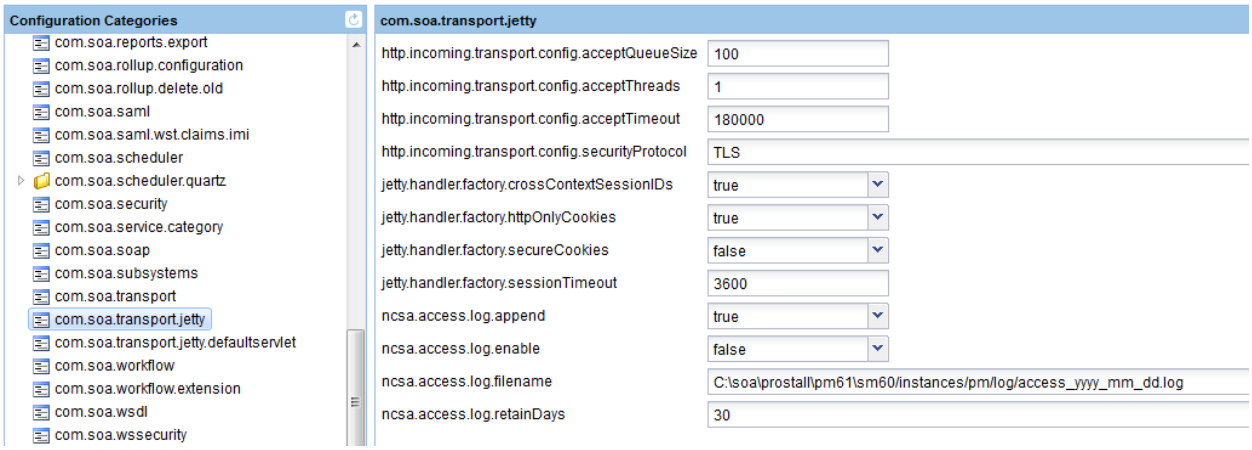
Provider Output Logging Support (transport.config.providerOutputLog)

Enables or disables of server-side output logging support.

Default: false

com.soa.transport.jetty

Configuration properties for the Jetty transport (server-side listener parameters).



Allow Cross-Context Session IDs (jetty.handler.factory.crossContextSessionIDs)

Indicates whether sessions are allowed to be used in multiple contexts/applications. This applies only to web applications.

Default: true

Allow Http Only Cookies (jetty.handler.factory.httpOnlyCookies)

Prevents cookies from being accessed from JavaScript in modern browsers. Safeguards against cross-site scripting.

Default: true

Allow Secure Cookies (jetty.handler.factory.secureCookies)

Encrypts cookies when browser uses HTTPS. If a cookie was set up by an HTTPS request, it should only be used for an HTTPS request, not for an HTTP request.

Default: false

Session Idle Timeout (jetty.handler.factory.sessionTimeout)

The session idle timeout in seconds. This applies only to web applications.

Default: 3600

Accept Backlog (http.incoming.transport.config.acceptQueueSize)

The size of the accept socket queue. This is also known as the “backlog”.

Default: 100

Accept Threads (http.incoming.transport.config.acceptThreads)

The number of accept threads.

Default: 1

Accept Socket Timeout (http.incoming.transport.config.acceptTimeout)

The accept socket timeout in milliseconds. This is also used as the SO_TIMEOUT for incoming data sockets. Warning: setting a small value for this may result in frequent recycling of the accept socket, which could cause dropped connections.

Default: 180000

Security protocol (http.incoming.transport.config.securityProtocol)

The default SSL protocol. With IBM stacks this should normally be set to SSL or SSL_TLS.

Default: TLS

Enable NCSA Access Log (ncsa.access.log.enable)

Enable/disable the NCSA access log.

Default: false

NCSA Access Log Filename (ncsa.access.log.filename)

The filename to use for the NCSA access log. The filename should include the string yyyy_mm_dd which is replaced with the actual date when creating and rolling over the file.

Default: ${product.home.dir}/instances/${container.name}/log/access_yyyy_mm_dd.log

NCSA Access Log Retention (ncsa.access.log.retainDays)

The number of days to retain log files for the NCSA access log.

Default: 30

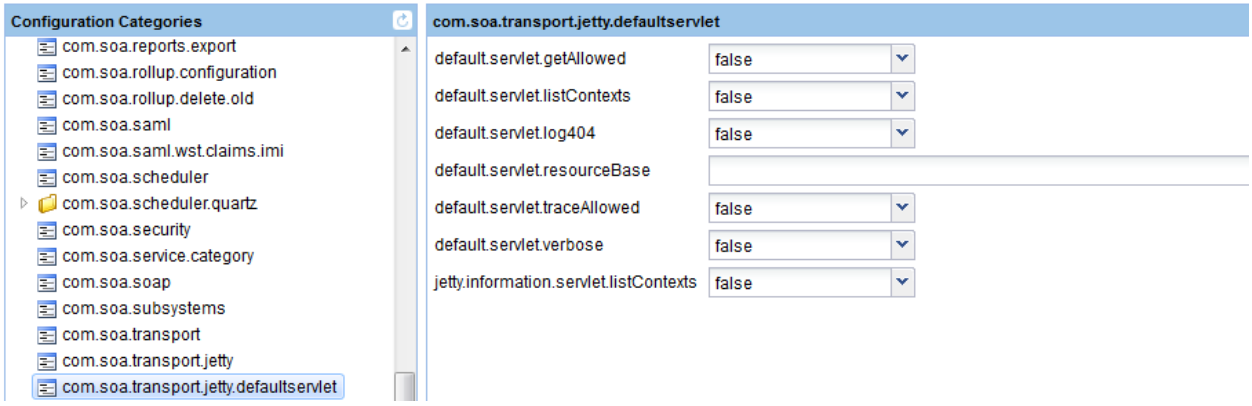
NCSA Access Log Append (ncsa.access.log.append)

Control whether to append or overwrite log files for the NCSA access log.

Default: true

com.soa.transport.jetty.defaultservlet

Configuration properties for the Jetty default servlet.



Log 404 Errors (default.servlet.log404)

Indicates whether 404 errors should be logged.

Default: false

Allow List Contexts (default.servlet.listContexts)

Indicates whether context contents can be browsed.

Default: false

Verbose Responses (default.servlet.verbose)

Indicates whether verbose responses include information on the request.

Default: false

GET Allowed (default.servlet.getAllowed)

Indicates whether GET requests are allowed.

Default: false

TRACE Allowed (default.servlet.traceAllowed)

Indicates whether TRACE requests are allowed.

Default: false

Resource Base (default.servlet.resourceBase)

Base path for resources if GET requests are allowed.

informationServletListContexts (jetty.information.servlet.listContexts)

Default: false

Com.soa.uif

Configuration of the user interface framework.

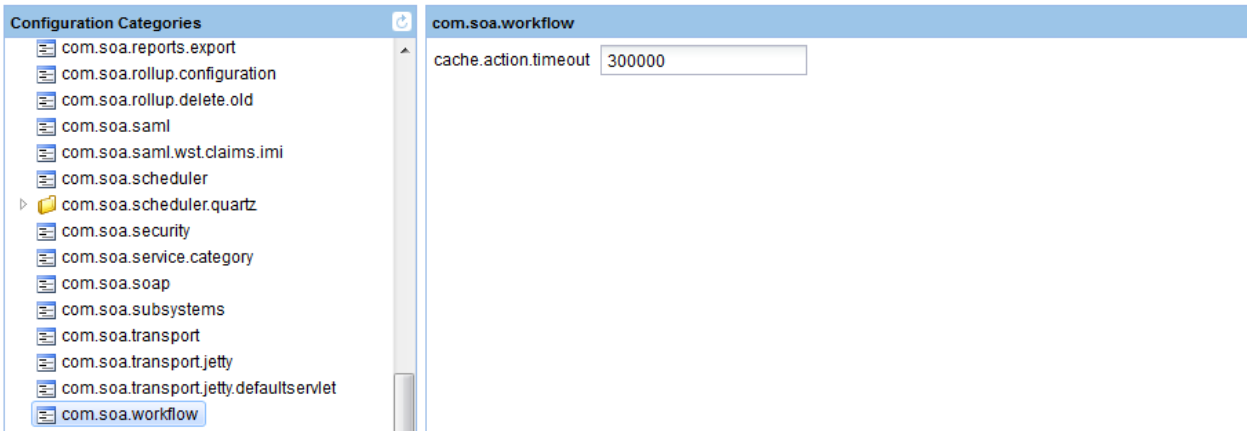
script compilation interval (uif.config.scriptCompilationInterval)

Script compilation interface in seconds. This job compiles all scripts required for a particular application deployed in the container each interval.

Default: 3600

com.soa.workflow

Configuration of workflow properties.



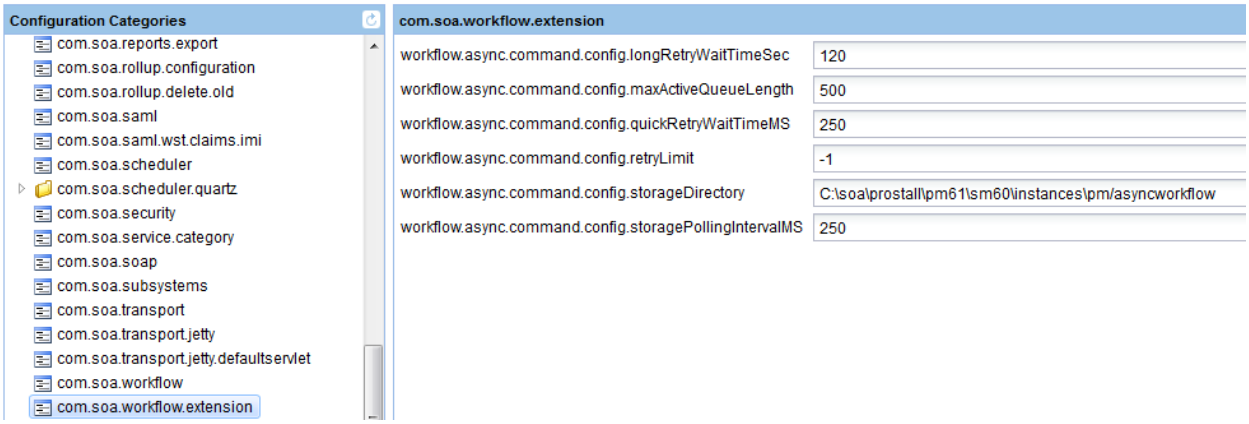
cache.action.timeout

Action Cache Timeout.

Default: 300000

com.soa.workflow.extension

Configuration of workflow settings.



workflow.async.command.config.longRetryWaitTimeSec

The interval, in seconds, between retries for remote asynchronous commands that are failing.

workflow.async.command.config.maxActiveQueueLength

The maximum number of remote asynchronous commands that can be held in the in-memory queue. A value of 0 indicates that there is no limit.

workflow.async.command.config.quickRetryWaitTimeMS

The interval, in milliseconds, before the first retry of a failed remote asynchronous command.

workflow.async.command.config.retryLimit

The maximum number of times to retry a remote asynchronous workflow command that is failing.

workflow.async.command.config.storageDirectory

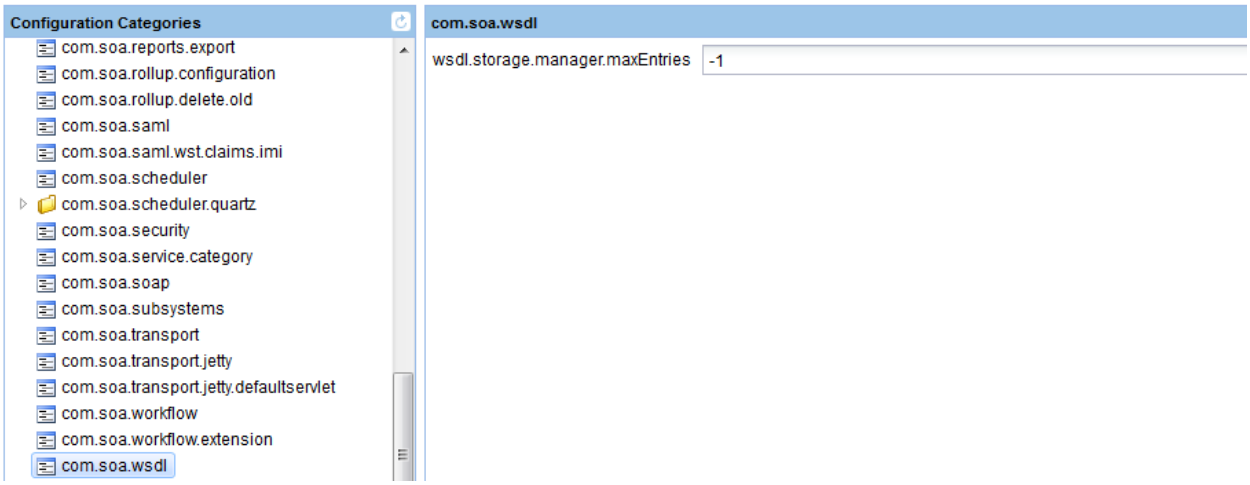
The path to the directory where pending asynchronous remote workflow commands are stored while they are waiting to be executed.

workflow.async.command.config.storagePollingIntervalMS

The polling interval, in milliseconds, for the background thread that checks for persisted asynchronous remote workflow commands.

com.soa.wsdl

SOA Software WSDL Support Utilities: configuration of WSDL-related settings.



wsdl.storage.manager.maxEntries

Defines the maximum number of WSDL documents of hosted or downstream services that can be cached in memory at any given time. A value of -1 indicates all service WSDL documents are cached. All WSDL documents that are not cached are stored locally on disk and are re-read into memory on demand.

WSDL documents can take a large amount of memory in the container. As the number of hosted services grows, cached WSDL files can cause memory scaling issues with the process. Generally, default container capabilities do not require cached WSDL documents, so this number can be quite small. However, option packs and custom extensions may require WSDL document access, and the lack of documents in the cache may cause a loss in performance.

com.soa.wsil

WSIL publishing configuration.

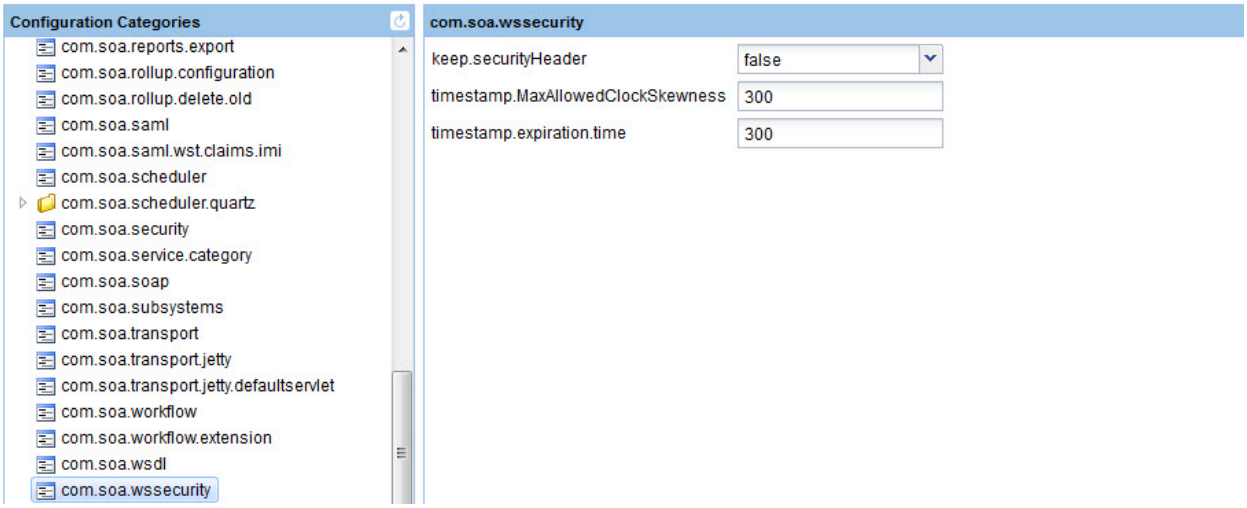
Enable WSIL (wsil.servlet.enable)

Enable/disable the WSIL publishing servlet.

Default: true

com.soa.wssecurity

WS-Security Configuration.



Allowed Maximum Clock Skewness (in seconds). (timestamp.MaxAllowedClockSkewness)

Allowed maximum clock skewness.

Default: 300

Timestamp Expiration time in seconds (timestamp.expiration.time)

Timestamp Expiration time in seconds.

Default: 300

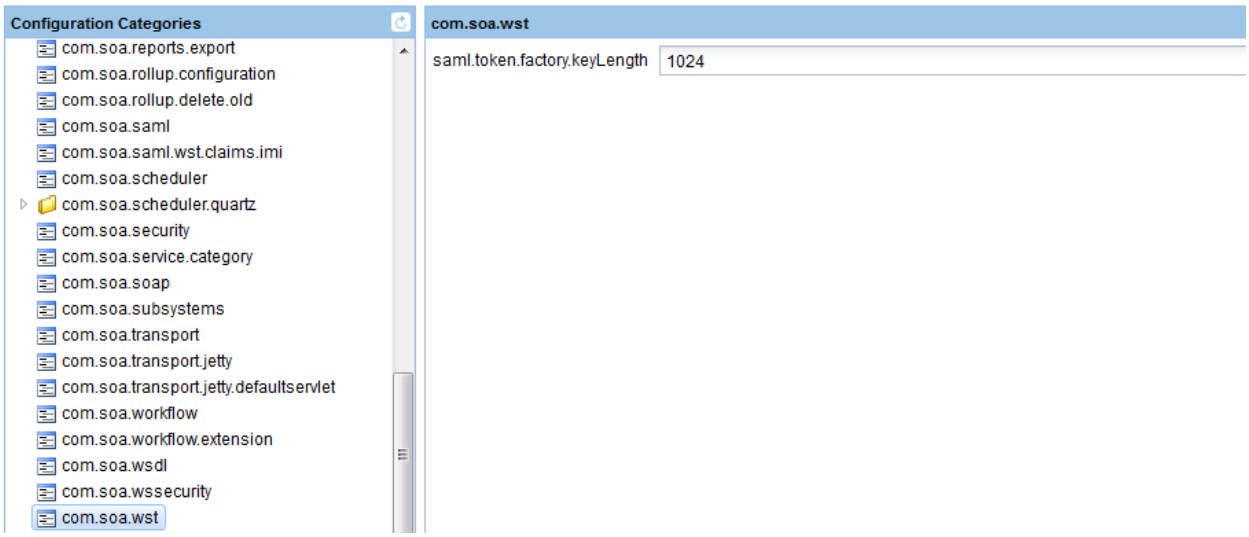
Keep WS Security Header (keep.securityHeader)

Keep WS Security Header after policy enforcement.

Default: false

com.soa.wst

SOA Software WS-Trust and WS-Secure Conversation Common API: configuration of WS-Trust.

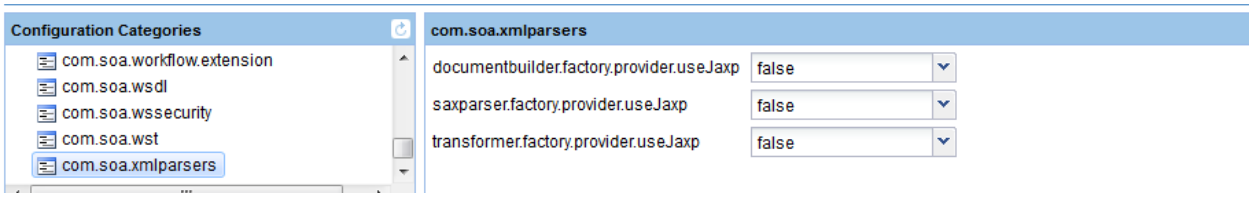


saml.token.factory.keyLength

Length of the key used in the SAML token signature.

com.soa.xmlparsers

SOA Software default XML parser and transformer: JAXP configuration.



Use JAXP for DOM (documentbuilder.factory.provider.useJaxp)

Indicates whether JAXP is used for DOM.

Default: false

Use JAXP for SAX (saxparser.factory.provider.useJaxp)

Indicates whether JAXP is used for SAX.

Default: false

Use JAXP for Transformers (transformer.factory.provider.useJaxp)

Indicates whether JAXP is used for Transformers.

Default: false