SOA Software:
Policy Manager
Configuration Categories
and Settings

SOA | software™

SOA Software Policy Manager

Policy Manager Configuration Categories (6.x, 7.x)
December, 2014

Copyright

Copyright © 2014 SOA Software, Inc. All rights reserved.

Trademarks

SOA Software, Policy Manager, Portfolio Manager, Repository Manager, Service Manager, Community Manager, SOA Intermediary for Microsoft and SOLA are trademarks of SOA Software, Inc. All other product and company names herein may be trademarks and/or registered trademarks of their registered owners.

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

The information provided in this document is provided "AS IS" WITHOUT ANY WARRANTIES OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT OF INTELLECTUAL PROPERTY. SOA Software may make changes to this document at any time without notice. All comparisons, functionalities and measures as related to similar products and services offered by other vendors are based on SOA Software's internal assessment and/or publicly available information of SOA Software and other vendor product features, unless otherwise specifically stated. Reliance by you on these assessments / comparative assessments is to be made solely on your own discretion and at your own risk. The content of this document may be out of date, and SOA Software makes no commitment to update this content. This document may refer to products, programs or services that are not available in your country. Consult your local SOA Software business contact for information regarding the products, programs and services that may be available to you. Applicable law may not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Contents

Chapter 1 | 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 categories

1   Log in to the *SOA Software Administration Console*.

2   Click the **Configuration** tab.

The *Configuration Categories* are in the left panel.

com.soa.admin.console.login

Used to enable / disable the Policy Manager Admin User account. If you initially defined this account as part of the Policy Manager installation process via the *Create Policy Manager Admin User* function, this configuration category will be set to **True**.

If the admin user account does not get created (e.g., the wizard is bypassed during the Policy Manager installation, you are installing the database manually, etc.), the configuration category setting will be set to **False**. You can also set it to **False** manually if you would like create a new admin user account and overwrite the existing one.

When the configuration category is set to **False**, the *Create Policy Manager Admin User* task displays in the *Installed Features* section. Select **Complete Configuration** to define a new admin user account.

```
┌─ Pending Installation Tasks ─────────────────┐
│ There are 1 installation task(s) pending completion.
│
│ Create Policy Manager Admin User
│
│ ┌──────────────────────┐
│ │ Complete Configuration │
│ └──────────────────────┘
└───────────────────────────────────────────────┘
```
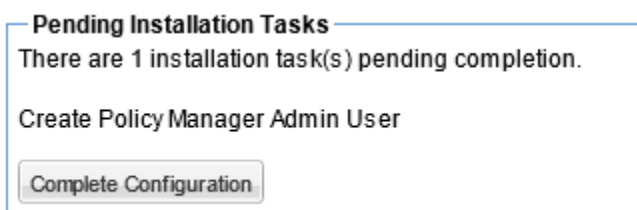
Running Admin Console and Policy Manager on Two Separate Interfaces on the Same Machine

To run the *SOA Software Administration Console* and Policy Manager or hosted services on multiple network interfaces with optional restriction to just the specified ports make the following configuration changes:

Change the ports for the *SOA Software Administration Console* using the following options in:

```
/<release directory>/instances/<Container>/system.properties:
```

```
org.osgi.service.http.port=9903
```

Add the following values if not already present:

```
org.osgi.service.http.port.secure=9446
com.soa.http.bind.all=true
com.soa.http.bind.all.secure=true
```

You can then restrict the *SOA Software Administration Console* to **JUST** the ports specified above by specifying the following in the *Configuration > Configuration Categories*:

```
com.soa.admin.console -> admin.console.access.restricted=true
```

com.soa.admin.container

admin.container.basicauth.enabled

This property is used for our REST API's on the SOA Software Administration Console. If true, you will have to provide HTTP basic auth credentials on our API calls, such as /admin/container/configjob. Note that this property is not associated with disabling the login to the SOA Software Administration Console.

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.
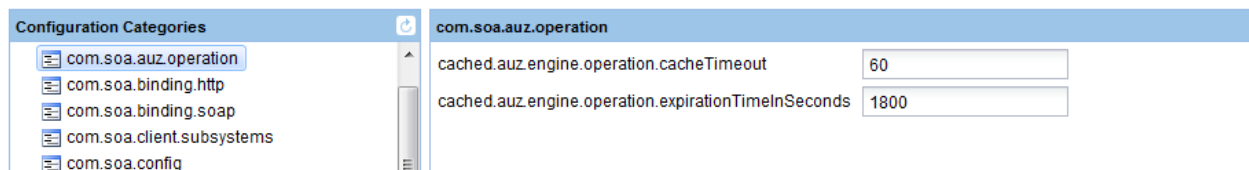
Default: 60

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.

Configuration Categories	com.soa.auz.operation	
com.soa.auz.operation	cached.auz.engine.operation.cacheTimeout	60
com.soa.binding.http	cached.auz.engine.operation.expirationTimeInSeconds	1800
com.soa.binding.soap		
com.soa.client.subsystems		
com.soa.config		

cached.auz.engine.operation.cacheTimeout

Cache Timeout: The time, in seconds, after which authorization decisions will timeout.
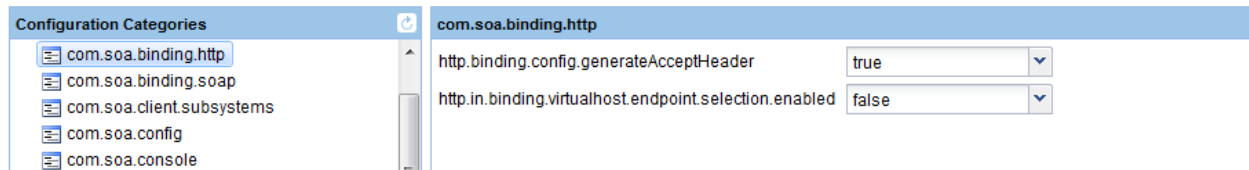
Default: 60

---

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.
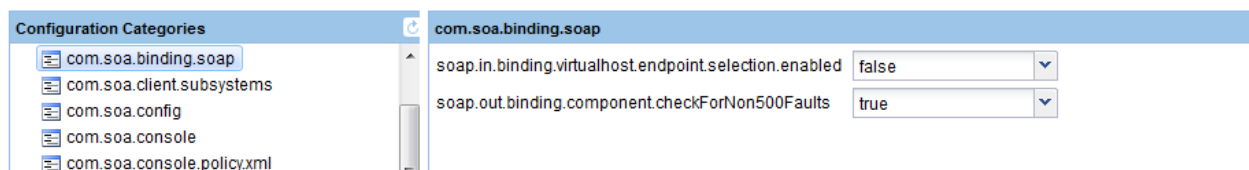
Default: true

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.

Configuration Categories	
com.soa.console	
com.soa.console.policy.xml	
com.soa.console.xss	
com.soa.container.configuration.service	
com.soa.container.identity.defaultcertdetails	
com.soa.container.metadata.service	
com.soa.container.registration	
com.soa.contract.enforcement	
com.soa.crl	
com.soa.database	
com.soa.database.config	
com.soa.framework	
com.soa.framework.xpath	
com.soa.http.client	
com.soa.http.clientcaching	
com.soa.jbi	
com.soa.jbi.component.wsrt	
com.soa.jms	
com.soa.log	
com.soa.metadata.wcdl	

Configuration Actions

Add Database

Configure WS-MetadataExchange Options

Force Configuration Refresh

Manage Admin Console Administrator

Manage PKI Keys

Manage Schemas

com.soa.console	
CHARTS.AVGPERFTIMEBYOP.TYPE	line
CHARTS.AVGPERFTIMEBYOP.XAXISTITLE	Time
CHARTS.AVGPERFTIMEBYOP.YAXISTITLE	Avg Response Time (ms)
CHARTS.AVGPERFTIMEBYSRV.TYPE	line
CHARTS.AVGPERFTIMEBYSRV.XAXISTITLE	Time
CHARTS.AVGPERFTIMEBYSRV.YAXISTITLE	Avg Response Time (ms)
CHARTS.USAGEBYOP.TYPE	bar
CHARTS.USAGEBYOP.XAXISTITLE	Time
CHARTS.USAGEBYOP.YAXISTITLE	Hits
CHARTS.USAGEBYOPS.COMPONENT	Usage
CHARTS.USAGEBYOPS.LEVEL	Service
CHARTS.USAGEBYOPS.TYPE	pie
CHARTS.USAGEBYSRV.TYPE	bar
CHARTS.USAGEBYSRV.XAXISTITLE	Time
CHARTS.USAGEBYSRV.YAXISTITLE	Hits
CHARTS.USAGEBYUSER.LEVEL	Operation
CHARTS.USAGEBYUSER.TYPE	data
CHARTS.USAGEBYUSER.XAXISTITLE	Time
QuickSearch.enabled	false
USER.PERSPECTIVE.DEFAULT	organization
schemas.dir	C:\soa\prostall\pm61\sm60/schemas
workbench.search.performAutoSearch	true

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.
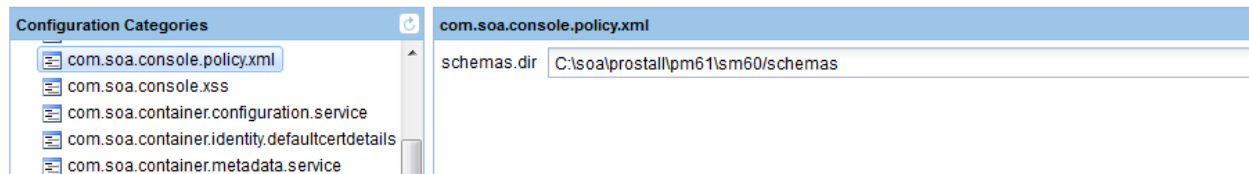
Default: /admin/cluster/publish/state

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

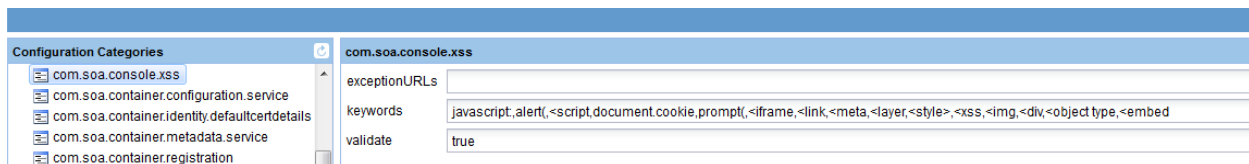Configuration of the XML policy handler.

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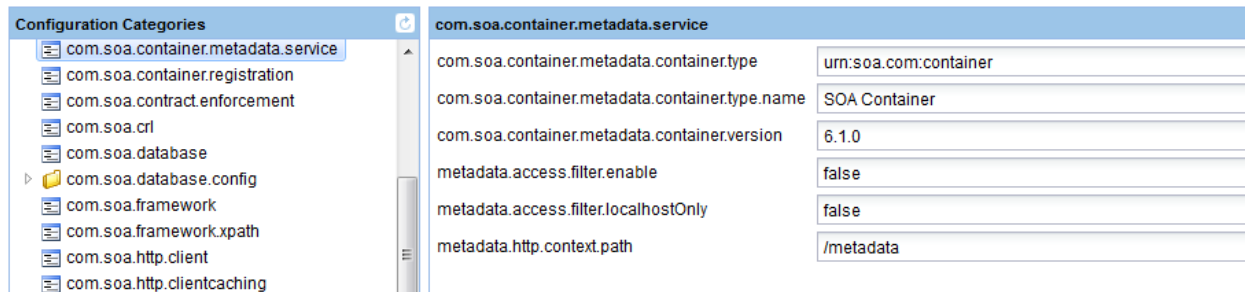
Container Type (com.soa.container.metadata.container.type)

> 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.
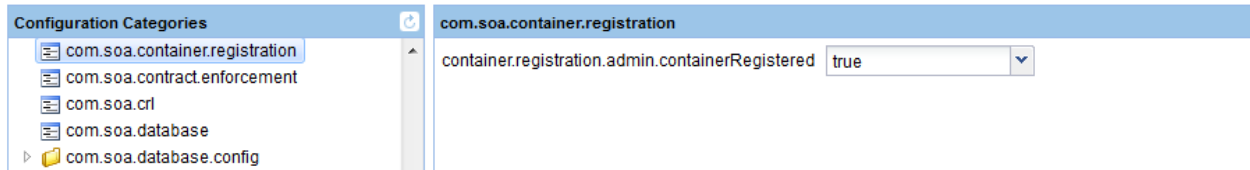
container.registration.admin.containerRegistered

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.

Configuration Categories		com.soa.contract.enforcement	
com.soa.contract.enforcement		contract.handler.framework.idleExpiration	300
com.soa.crl		contract.handler.framework.maxRefreshInterval	120
com.soa.database		contract.refresh.trigger.repeatInterval	15000
com.soa.database.config		contract.refresh.trigger.startDelay	15000
com.soa.framework			
com.soa.framework.xpath			
com.soa.http.client			

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.

Configuration Categories		com.soa.crl	
com.soa.crl		com.soa.crl.cacheRefreshInterval	600
com.soa.database		com.soa.crl.enabled	true
com.soa.database.config		com.soa.crl.failOnError	false
com.soa.framework			
com.soa.framework.xpath			

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.
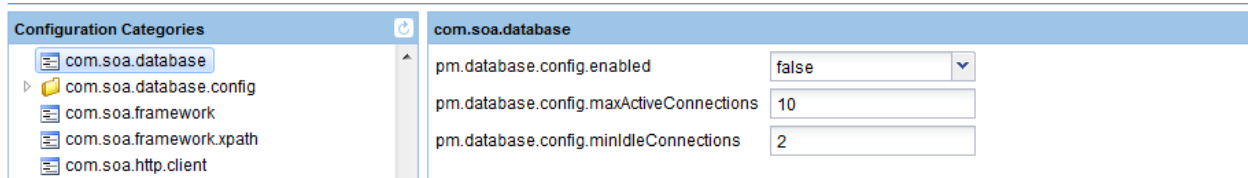
Default: true

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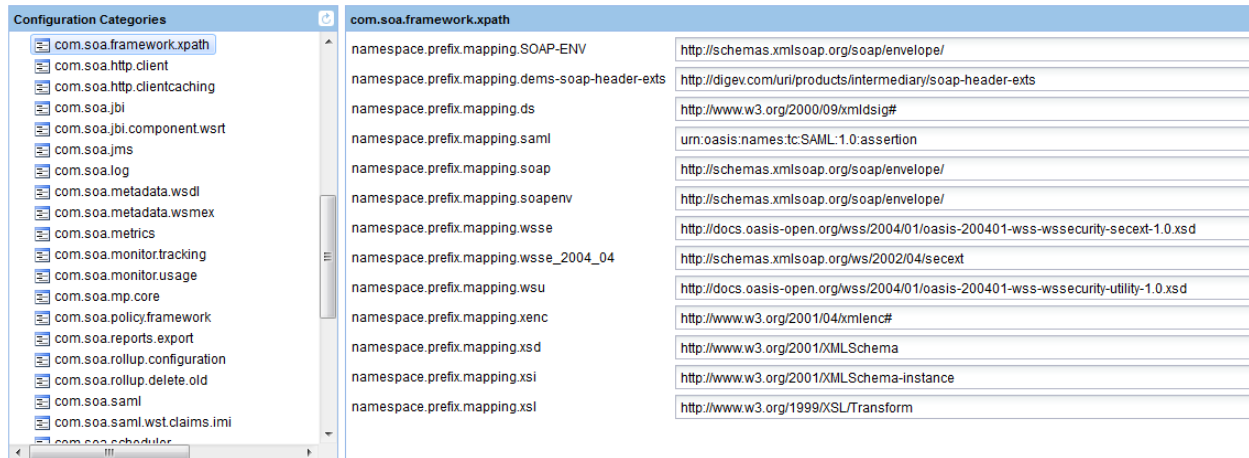
Using this setting can help you find performance issues. Note that some processes might legitimately take a longer time, and might be logged even though there is no issue. This setting is only relevant when failure.data.capture.enabled is set to true.

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.

Configuration Categories	com.soa.framework.xpath	
com.soa.framework.xpath	namespace.prefix.mapping.SOAP-ENV	http://schemas.xmlsoap.org/soap/envelope/
com.soa.http.client	namespace.prefix.mapping.dems-soap-header-exts	http://digev.com/uri/products/intermediary/soap-header-exts
com.soa.http.clientcaching	namespace.prefix.mapping.ds	http://www.w3.org/2000/09/xmldsig#
com.soa.jbi	namespace.prefix.mapping.saml	urn:oasis:names:tc:SAML:1.0:assertion
com.soa.jbi.component.wsrt	namespace.prefix.mapping.soap	http://schemas.xmlsoap.org/soap/envelope/
com.soa.jms	namespace.prefix.mapping.soapenv	http://schemas.xmlsoap.org/soap/envelope/
com.soa.log	namespace.prefix.mapping.wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
com.soa.metadata.wsdl	namespace.prefix.mapping.wsse_2004_04	http://schemas.xmlsoap.org/ws/2002/04/secext
com.soa.metadata.wsmex	namespace.prefix.mapping.wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
com.soa.metrics	namespace.prefix.mapping.xenc	http://www.w3.org/2001/04/xmlenc#
com.soa.monitor.tracking	namespace.prefix.mapping.xsd	http://www.w3.org/2001/XMLSchema
com.soa.monitor.usage	namespace.prefix.mapping.xsi	http://www.w3.org/2001/XMLSchema-instance
com.soa.mp.core	namespace.prefix.mapping.xsl	http://www.w3.org/1999/XSL/Transform
com.soa.policy.framework		
com.soa.reports.export		
com.soa.rollup.configuration		
com.soa.rollup.delete.old		
com.soa.saml		
com.soa.saml.wst.claims.imi		
com.soa.scheduler		

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.grid

Used to create a clusterable cache. This feature is supported in Policy Manager 7.2 only.

Grid.network.config.enableMulticast

Set to **false**. Note that the Multicast option is currently not supported.

Grid.network.config.enableenableTcp

Set to **true**.

Grid.network.config.peerAddresses

Specify the peer address of each Network Director instance in your deployment. Omit the peer address of the current Network Director instance in the list.

See the "Using a Clusterable Cache" document on the SOA Software Documentation Repository for detailed instructions:

http://docs.soa.com/ag/performance/using_clusterable_cache.htm

com.soa.http.client

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

Configuration Categories	com.soa.http.client	
com.soa.http.client	blocking.header.formatter.blocked	content-type,content-length,content-range,content-md5,host,expect,keep-alive,connection,transfer-encoding
com.soa.http.clientcaching	http.client.config.connectionManagerTimeout	10000
com.soa.jbi	http.client.transport.config.connectionTimeout	10000
com.soa.jbi.component.wsrt	http.client.transport.config.defaultMaxConnectionsPerHost	300
com.soa.jms	http.client.transport.config.maxTotalConnections	500
com.soa.log	http.client.transport.config.soTimeout	120000
com.soa.metadata.wsdl	http.client.transport.config.staleCheckingEnabled	true
com.soa.metadata.wsmex	http.client.transport.factory.bufferContent	false
com.soa.metrics	http.client.transport.factory.cipherSuites	
com.soa.monitor.tracking	http.client.transport.factory.followRedirect	true
com.soa.monitor.usage	http.client.transport.factory.idleCheckInterval	30000
com.soa.mp.core	http.client.transport.factory.idleTimeout	300000
com.soa.policy.framework	http.client.transport.factory.retryOnNoResponse	true
com.soa.reports.export	http.client.transport.factory.useExpectContinue	false
com.soa.rollup.configuration	template.header.formatter.templates	
com.soa.rollup.delete.old	user.agent.header.formatter.defaultUserAgent	SOA Software HTTP Client Transport
com.soa.saml		
com.soa.saml.wst.claims.imi		
com.soa.scheduler		
com.soa.scheduler.quartz		

Configuration Actions

Add Database

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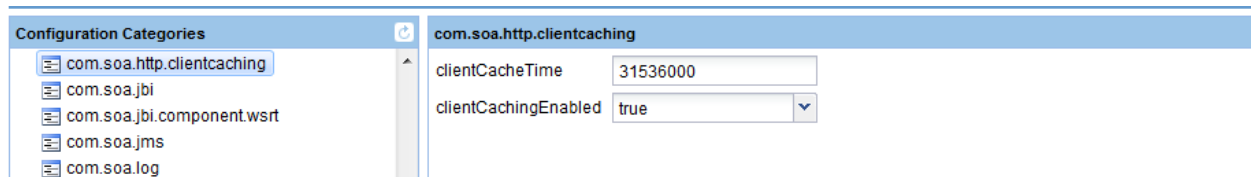
User Agent (user.agent.header.formatter.defaultUserAgent)

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.
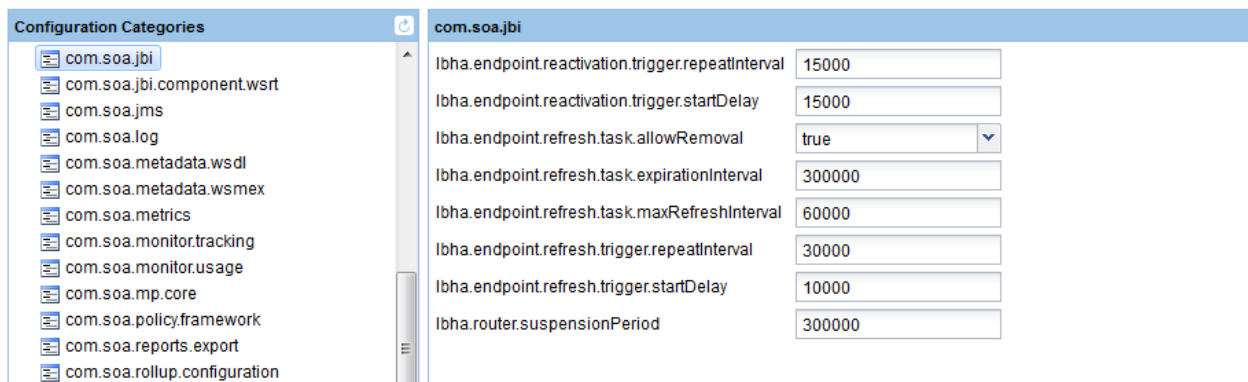
Target URL Pattern (url)

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.
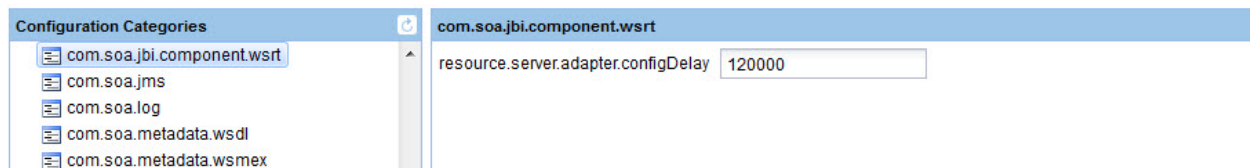
Configuration Delay (resource.server.adapter.configDelay)

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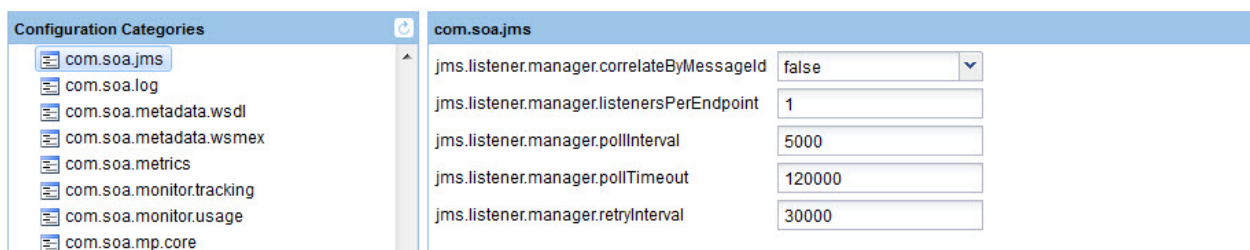
Correlate by Message ID (jms.listener.manager.correlateByMessageId)

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.

Configuration Categories		com.soa.log	
com.soa.log		log4j.appender.FILE	org.apache.log4j.RollingFileAppender
com.soa.metadata.wsdl		log4j.appender.FILE.Append	true
com.soa.metadata.wsmex		log4j.appender.FILE.BufferedIO	false
com.soa.metrics		log4j.appender.FILE.File	C:\soa\prostall\pm61\sm60/instances/pm/log/pm.log
com.soa.monitor.tracking		log4j.appender.FILE.MaxBackupIndex	10
com.soa.monitor.usage		log4j.appender.FILE.MaxFileSize	5000000
com.soa.mp.core		log4j.appender.FILE.Threshold	ALL
com.soa.policy.framework		log4j.appender.FILE.layout	org.apache.log4j.PatternLayout
com.soa.reports.export		log4j.appender.FILE.layout.ConversionPattern	%d %-5p [%t] %c{1} - %m%n
com.soa.rollup.configuration		log4j.category.com.digev	ERROR
com.soa.rollup.delete.old		log4j.category.com.soa	ERROR
com.soa.saml		log4j.category.httpclient.wire.content	ERROR
com.soa.saml.wst.claims.imi		log4j.category.httpclient.wire.header	ERROR
com.soa.scheduler		log4j.category.org.apache	ERROR
com.soa.scheduler.quartz		log4j.category.org.apache.commons.httpclient	ERROR
com.soa.security		log4j.category.org.apache.xml.security	ERROR
com.soa.service.category		log4j.category.org.apache.xml.security.test.AllTests	ERROR
com.soa.soap		log4j.category.org.mortbay	ERROR
com.soa.subsystems		log4j.category.org.springframework	ERROR
com.soa.transport		log4j.rootLogger	ERROR, FILE

Configuration Actions

Add Database

Configure WS-MetadataExchange Options

Force Configuration Refresh

Manage Admin Console Administrator

Manage PKI Keys

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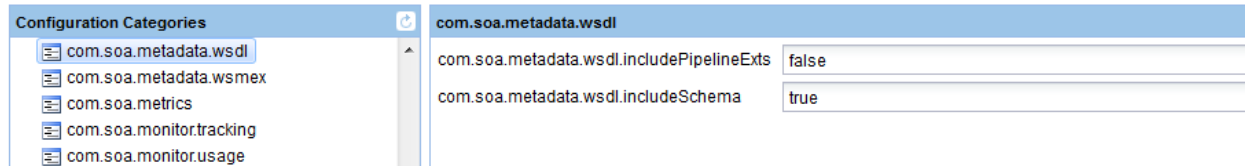
Include Schema in WSDL (com.soa.metadata.wsdl.includeSchema)

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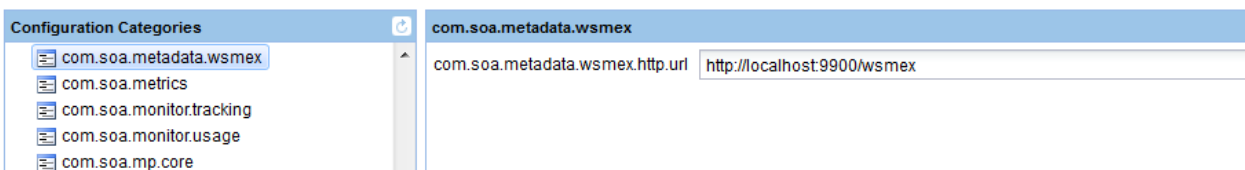
WS-Mex Service URL (com.soa.metadata.wsmex.http.url)

> 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.policyhandle.quota.throughput

Allows you to use a clusterable cache in a Throughput Quota Policy. This feature is supported in Policy Manager 7.2 only.

Use.clustered.cache

Set to **true**.

See the "Using a Clusterable Cache" document on the SOA Software Documentation Repository for detailed instructions:

http://docs.soa.com/ag/performance/using_clusterable_cache.htm

com.soa.policy.handle.quota.bandwidth

Allows you to use a clusterable cache in a Bandwidth Quota Policy. This feature is supported in Policy Manager 7.2 only.

Use.clustered.cache

Set to **true**.

See the "Using a Clusterable Cache" document on the SOA Software Documentation Repository for detailed instructions:

http://docs.soa.com/ag/performance/using_clusterable_cache.htm

com.soa.policy.handle.wssp.noncecache

Using a clusterable cache, you can share nonces to prevent getting duplicate messages across all ND's in a cluster. Supported WS-Security policies include WS-Security Message, WS-Security Assymmetric Binding, and WS-Security Transport policies. This feature is supported in Policy Manager 7.2 only.

See the "Using a Clusterable Cache" document on the SOA Software Documentation Repository for detailed instructions:

http://docs.soa.com/ag/performance/using_clusterable_cache.htm

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.

SOA Software, Inc.

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

SOA Software Policy Manager: Configuration Categories and Settings   39

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.jobs

Used to enable/ disable scheduled jobs for process rollups, alerts, etc.

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.

Configuration Categories	com.soa.scheduler.quartz.b92dcaef-8354-45a2-ac4a-75f1c8d59dc2	
com.soa.reports.export	org.quartz.jobStore.clusterCheckinInterval	20000
com.soa.rollup.configuration	org.quartz.jobStore.isClustered	true
com.soa.rollup.delete.old	org.quartz.jobStore.misfireThreshold	60000
com.soa.saml	org.quartz.jobStore.tablePrefix	SOA_QRTZ_
com.soa.saml.wst.claims.imi	org.quartz.jobStore.useProperties	false
com.soa.scheduler		
com.soa.scheduler.quartz	org.quartz.scheduler.enabled	true
com.soa.scheduler.quartz.b92dcaef-835	org.quartz.scheduler.instanceId	AUTO
com.soa.security	org.quartz.scheduler.instanceName	SOAScheduler
com.soa.service.category	org.quartz.thread.pool.threadCount	3
com.soa.soap	org.quartz.thread.pool.threadNamePrefix	QuartzSchedulerThread
com.soa.subsystems	org.quartz.thread.pool.threadPriority	5
com.soa.transport	org.quartz.thread.pool.threadsInheritContextClassLoaderOfInitializingThread	true
com.soa.transport.jetty	org.quartz.thread.pool.threadsInheritGroupOfInitializingThread	true
com.soa.transport.jetty.defaultservlet	service.factoryPid	com.soa.scheduler.quartz
com.soa.workflow		
com.soa.workflow.extension		
com.soa.wsdl		
com.soa.wssecurity		
com.soa.wst		

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.
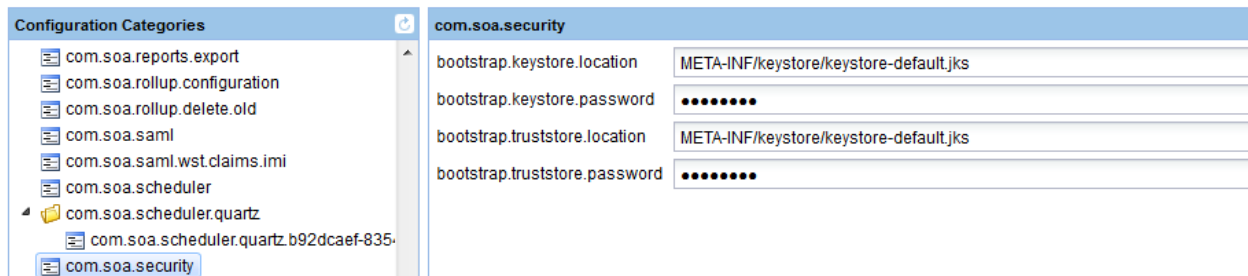
Key Store location (bootstrap.keystore.location)

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.
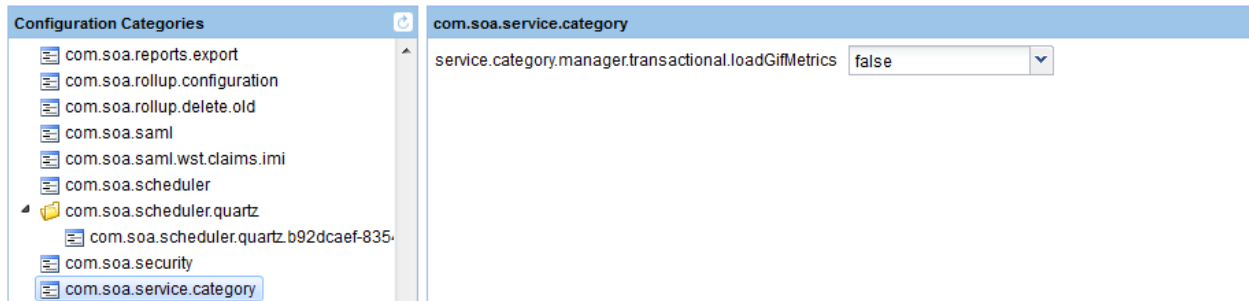
service.category.manager.transactional.loadGifMetrics

Category Manager GIF metrics calculation.

Default: false

com.soa.soap

Configuration of SOAP settings.
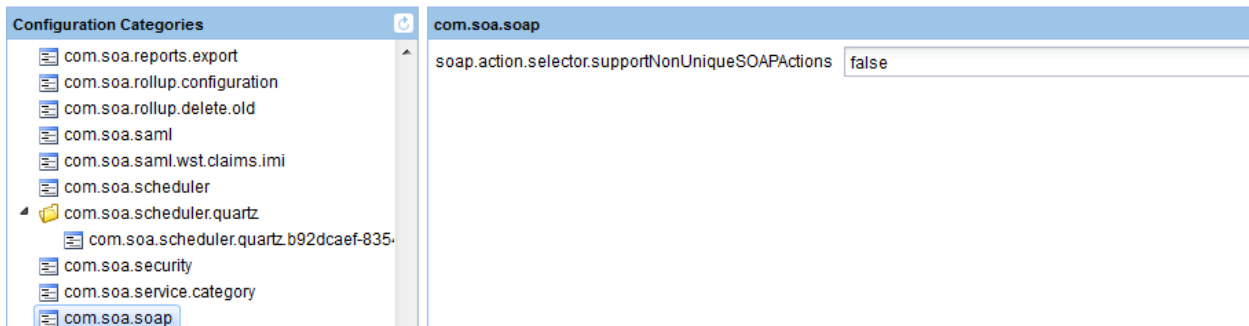
soap.action.selector.supportNonUniqueSOAPActions

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.subsystems.provisioning

uddi.provision.enabled
Subsystem provisioning is a process that creates system services and hosts them on Policy Manager. It also creates system policies and associates them with system services, and adds default workflows and a default contract. This feature is supported in Policy Manager 7.2 only.

> To enable auto provisioning on start up set this property to **true** (default).

> When performing database schema updates set this property to **false**.

com.soa.transport

Configuration of transport properties.
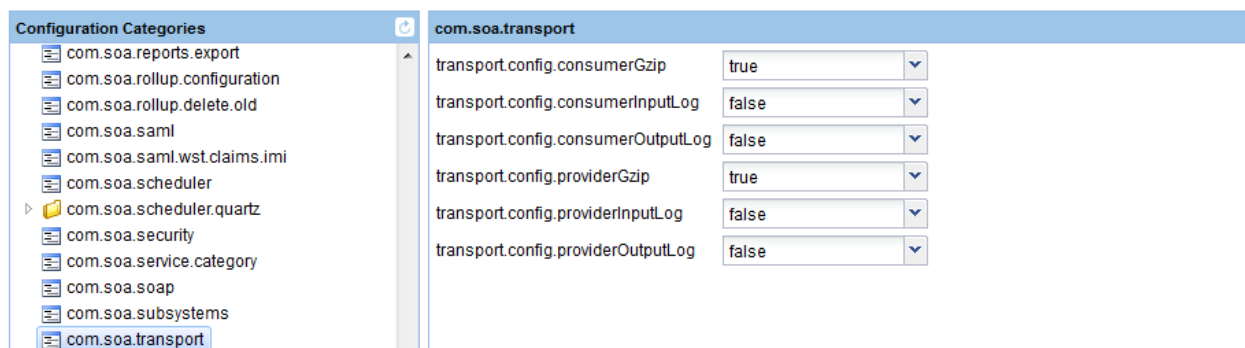
Consumer gzip Support (transport.config.consumerGzip)
> Enable or disable client-side gzip encoding/decoding support.

> 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.
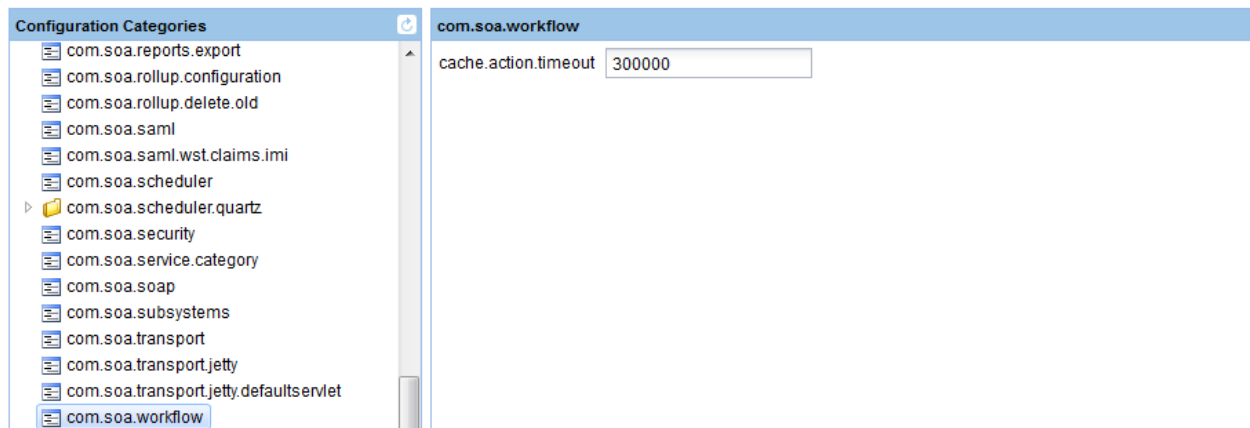
cache.action.timeout

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.
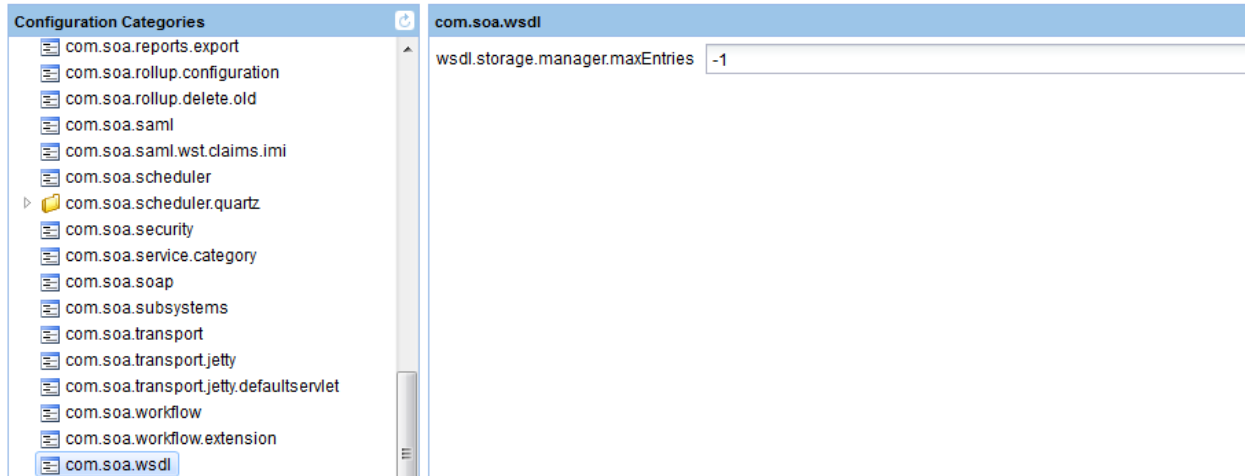
wsdl.storage.manager.maxEntries

> 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)

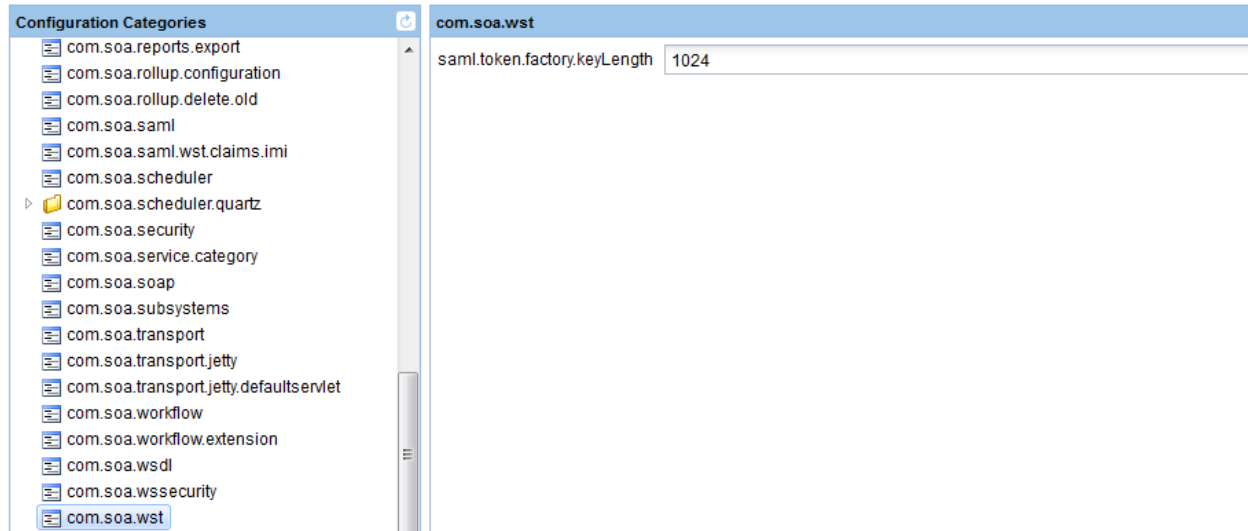Timestamp Expiration time in seconds.

Default: 300

Keep WS Security Header (keep.securityHeader)

Keep WS Security Header after policy enforcement.

Default: false

com.soa.wst

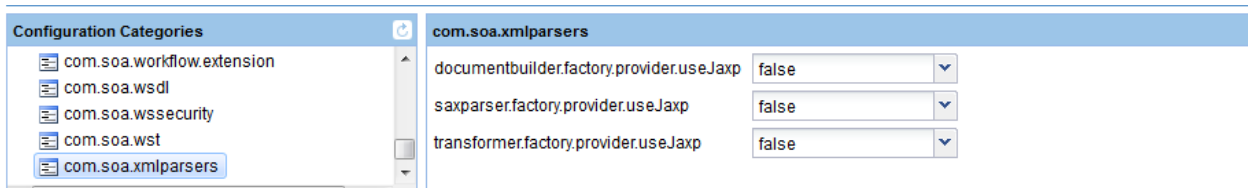SOA Software WS-Trust and WS-Secure Conversation Common API: configuration of WS-Trust.

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