SOA Software: Troubleshooting Guide for Agents

SOA | software™

SOA Software

Troubleshooting Guide for Agents
1.1
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 is important to take an orderly approach to installation, deployment, and troubleshooting.

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: Troubleshooting: Agents	General troubleshooting information for all Agents

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

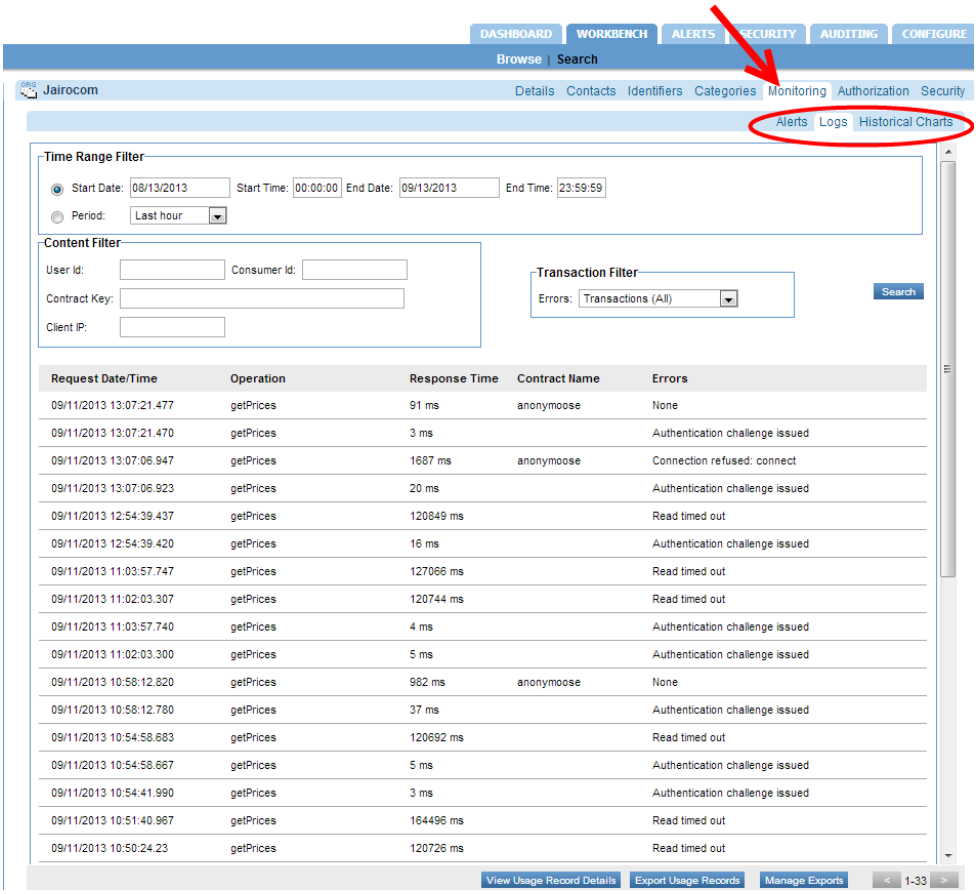
The highest level of monitoring information is available via the monitoring tab for an organization. This lets you view all logs and alerts sent by services and sub-organizations within the organization you are viewing.

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.

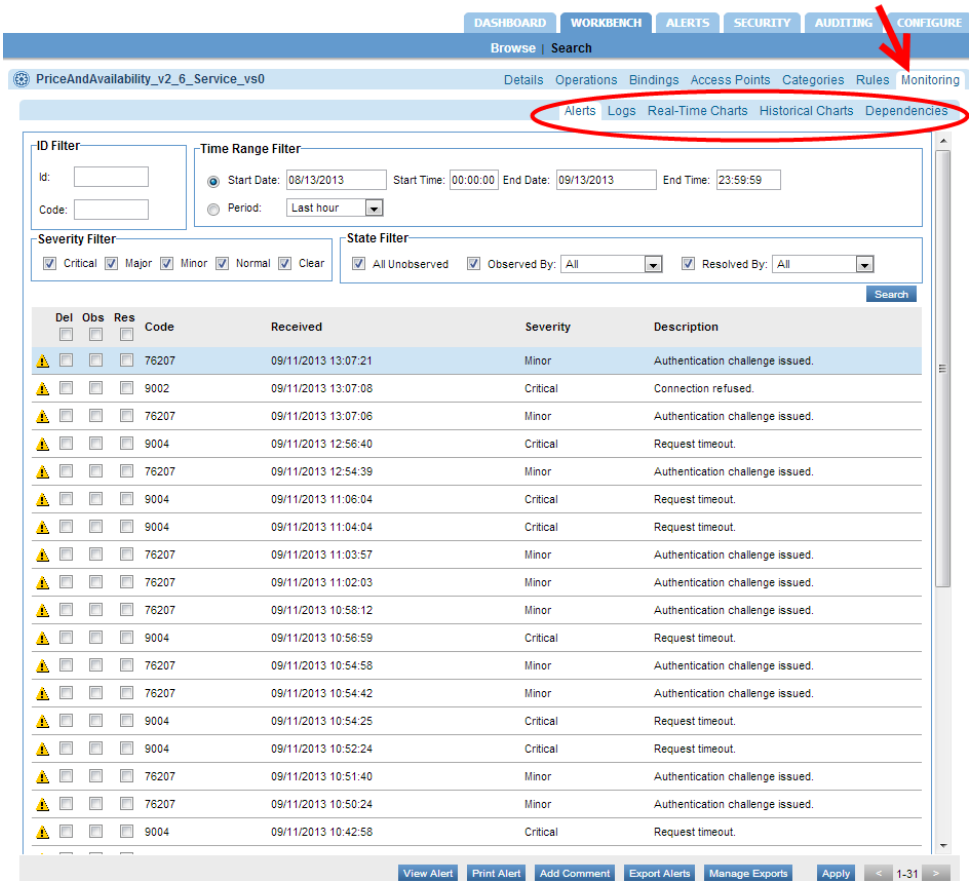
An example of the monitoring tab for an organization is shown below.



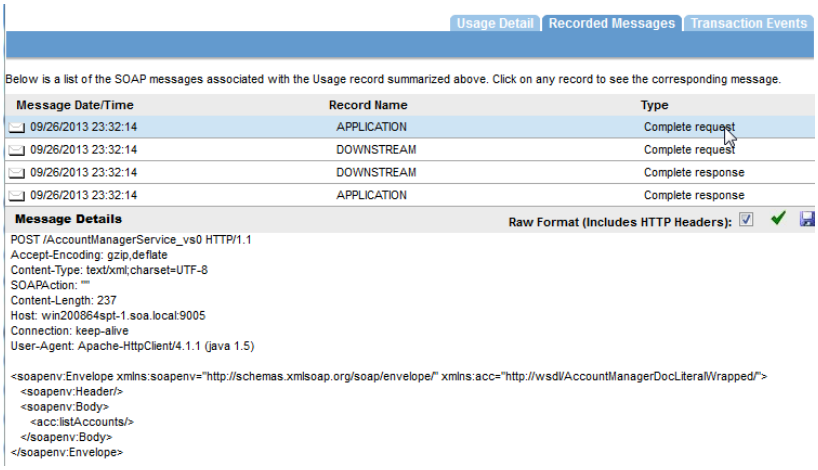
Service-Level Monitoring Tab

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.



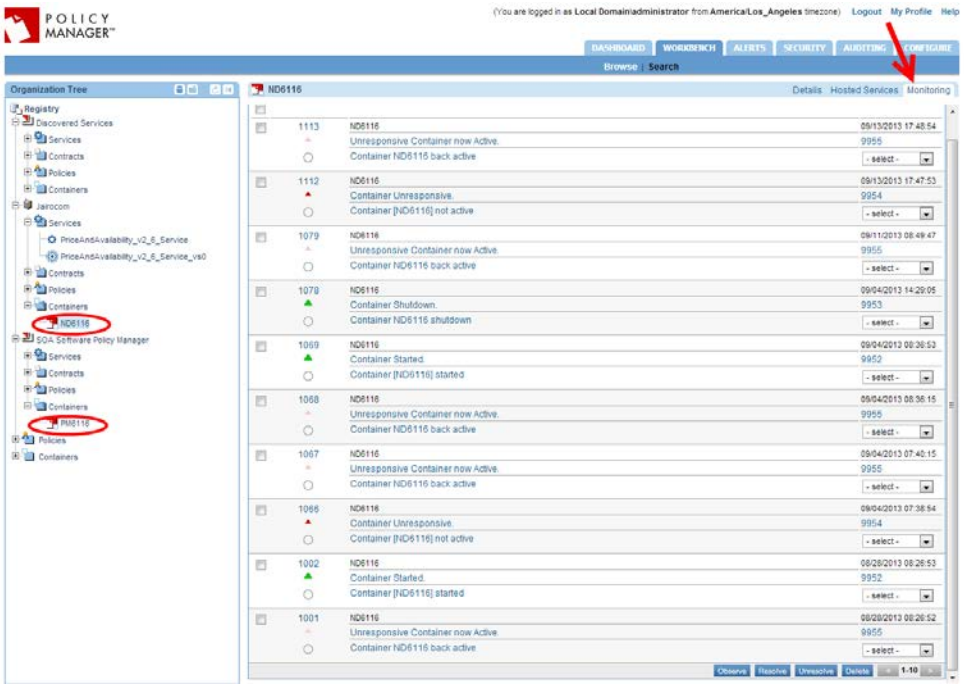
If the detailed auditing policy is being used, you can also view the request and response payload in the Logs tab. Double-click a specific message to see the Usage Data Details overlay. This includes usage detail, recorded messages, and transaction events. In the Recorded Messages tab you can see the 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

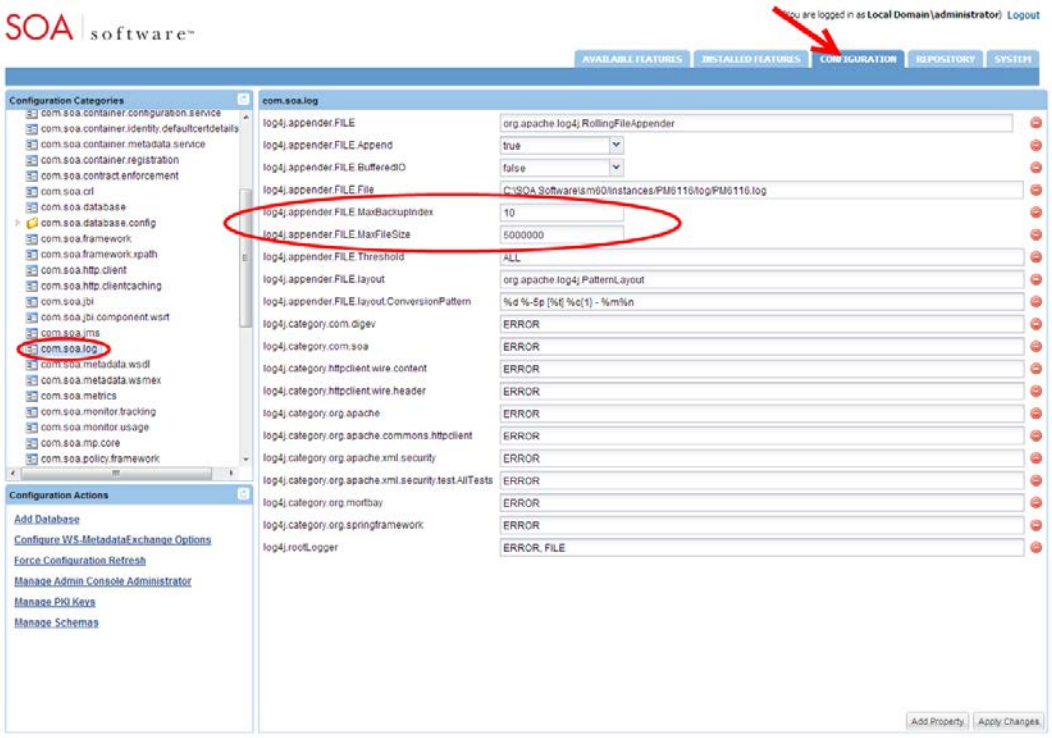
Each instance has its own set of logs at the following default location:

```
<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.

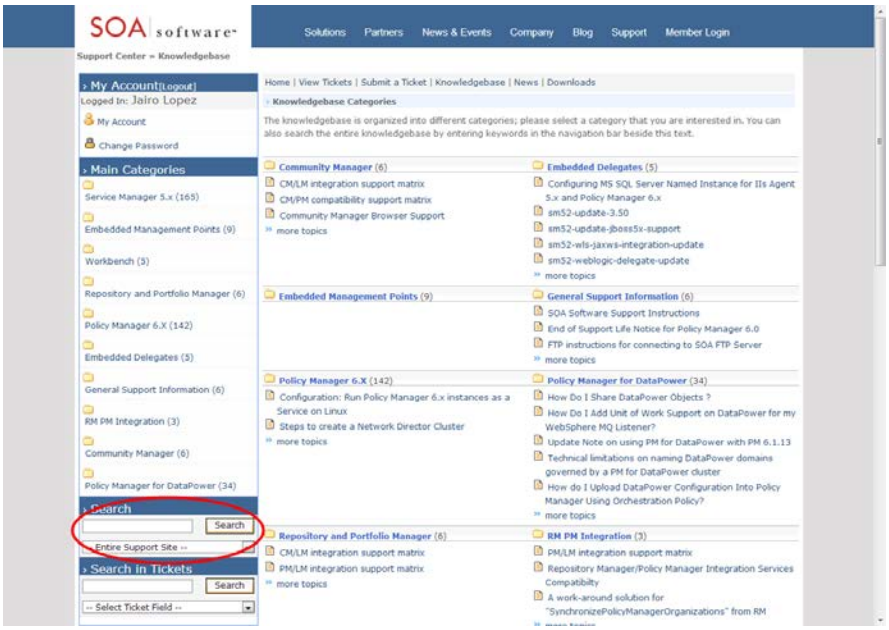
You might find info about these types of errors…	In this location…
Issues with the Policy Manager (for example, usage writer or container configuration), user interface issues, search results, and some database issues.	Policy Manager log files. These types of issues are generally a problem with the Policy 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.

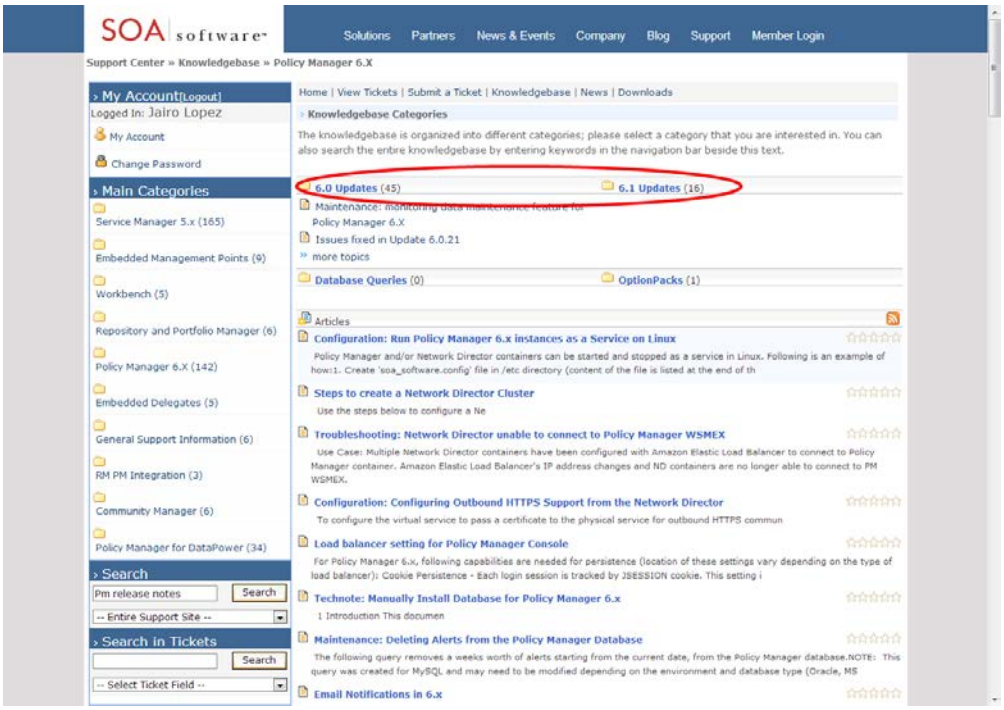


Release Notes

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.

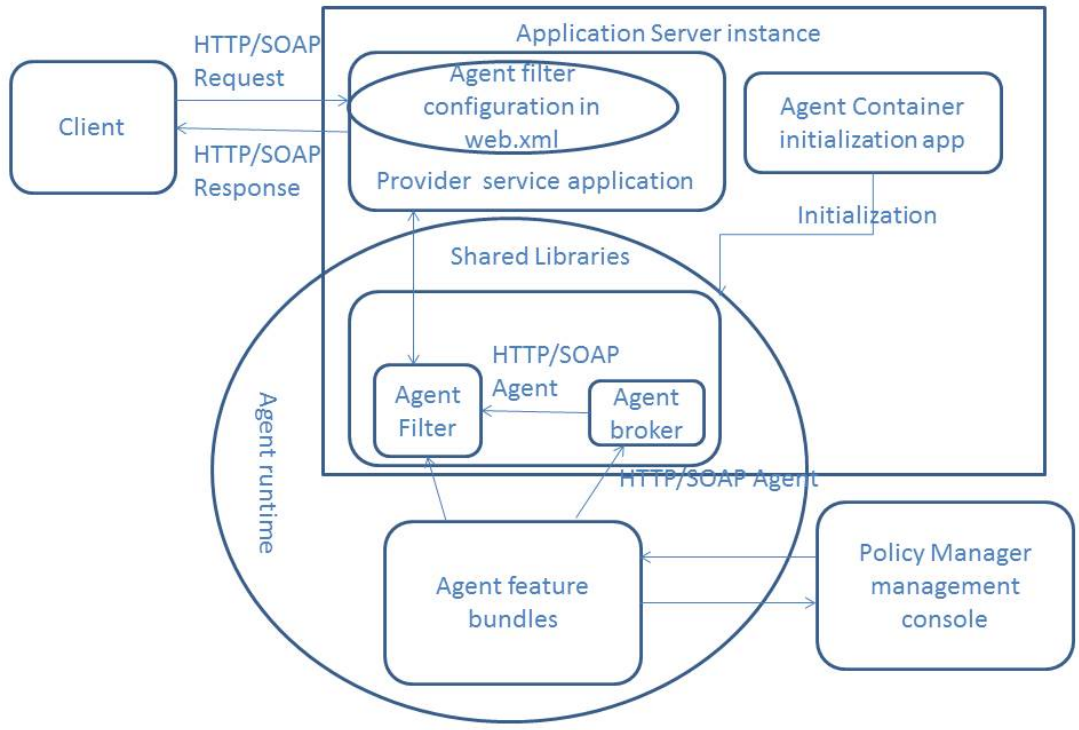
Chapter 2 | Troubleshooting: Agents

This chapter provides information that you can use to help ensure a successful implementation of any SOA Software Server Agent. It includes information general to all Agents, including:

- Process Flow
- Working with Agents
- Troubleshooting Information

Process Flow

The diagram below shows the message flow when an SOA Software Agent is embedded into an application server.



Working with Agents

This section provides information about general actions you might need to perform in relation to Agents. It includes:

- Configuring HTTPS
- Registering the Agent Container with a Metadata File
- Log Files for Agents

Configuring HTTPS

To provide secured access via the HTTPS protocol, you must complete a few setup steps before you can manage/unmanage services via the management console.

Complete, or verify, the steps below, in sequence.

1 Create an application server runtime instance that supports SSL.

2 Register the CA in the Policy Manager Console.

   The application server certificate Authority (CA) is not trusted by Policy Manager until it is registered in the Policy Manager Console. For more information, refer to the Policy Manager user documentation.

3 While registering the Agent container, be sure to provide the correct metadata URL path for HTTPS access with the SSL listening port.

Registering the Agent Container with a Metadata File

If the Agent container is not correctly set up and registered, the Agent will not work.

Registering the Agent container with a metadata file is similar to creating any container with a metadata file in the Policy Manager Admin Console.

For more information, refer to the Policy Manager Install Guide.

Log Files for Agents

Each Agent has log files that you can use to help troubleshoot issues. Default file locations are unique to each application server. For specific file locations, refer to the Agent troubleshooting guide document for the type of application server you are using.

Troubleshooting Information

This section includes problem/resolution information to help you troubleshoot general issues that might come up with any SOA Software Application Server Agent. It includes:

- Cannot Access Agent Admin Console
- Issue with Firewall

- Cannot Register Agent Container in Policy Manager Console
- Request Messages to Services Are Unsuccessful
- Policy Configuration Issues
- Monitoring Logs Not Shown in Policy Manager Management Console
- Service Returns 404 Status Code
- JDBC Connection Issue
- Cannot Create Agent from Configurator Wizard
- Error Message: "Service Is Blocked"
- Cannot Start Agent
- "Authorization Failed" Message when Consuming a Service
- Shared Libraries Not in the Classpath of the Provider Service Application
- Application Server Instance Running Out of Memory

Note: In addition to this general troubleshooting information, there might also be specific information available for each Agent, covering issues that might come up with that specific Agent. If you don't have the correct troubleshooting guide for your Agent, contact SOA Software Technical Support to request available documentation.

Cannot Access Agent Admin Console

If the Agent cannot access the Agent Admin Console, it might be because of one of the following:

- HTTP Port Mismatch with Application Server Access Port
- Context Path Is Incorrect

HTTP Port Mismatch with Application Server Access Port

If you think there is an HTTP port mismatch, check that these two values match:

- The value for org.osgi.service.http.port in the system.properties file in this location:

```
<AGENT_HOME>\sm60\instances\<AGENT_INSTANCE>
```

- The application server port on which it is running. tc Server runs on the following port:
  - For HTTP: 8080
  - For HTTPS: 8443

Context Path Is Incorrect

Verify that the context path set up in the Admin Console matches the context path registered while deploying the SOA container application. For more help, contact your server administrator.

Issue with Firewall

An attempt to access the service returns a 404 HTTP status code because the firewall is blocking access.

Solution:

To test whether there's an issue with the firewall, forward a test request through the firewall.

If needed, resolve issues with the firewall. Contact the system administrator.

Cannot Register Agent Container in Policy Manager Console

If you cannot register an Agent container in the Policy Manager 6.x console, it might be because of an issue with the metadata URL/metadata path.

Solution:

Do the following:

- Verify the metadata URL/path provided for creating the Agent container is valid.
- Verify that the hostname and port for the machine where the application server resides are correct.

Request Messages to Services Are Unsuccessful

The following are possible causes for requests to services not being successful:

- Service is not managed with Agent container
- Invalid value for WS-MEX URL

Solution:

Do the following:

- Verify that the service is managed with an Agent container.
- Verify that the values provided for the metadata URL/metadata path when creating the Agent container are valid.

Policy Configuration Issues

If the consumer can't connect to a service, it could be because of errors in policy configuration.

Solution:

Check policy configuration and correct as needed. Follow the steps below.

To check policy configuration

1 Log in to the Policy Manager console.

2 Under Monitoring > Alerts, check the physical service for errors and correct policy configuration as needed.

Monitoring Logs Not Shown in Policy Manager Management Console

The following are possible causes for this issue:

- Filters have not been set up in the deployment descriptor (web.xml file) of the service application.
- The JDBC driver JAR file is not present in the correct location:

  ```
  <AGENT_HOME>/sm60/instances/<AGENT_INSTANCE>/deploy
  ```

  JDBC writers use this driver to write log file entries relating to the Agent in the OSGI environment of the Agent container.

  Note: The JDBC driver JAR file is not required for SQL Server.

- Check if there is a JDBC connection issue.
- If the Usage Writer service is used instead of direct database access, logs are uploaded to Policy Manager via a web service call, which Policy Manager then writes to the database. There might be errors in communicating to the Usage Writer web service.

Solution:

If filters are missing, you will need to add them manually in the deployment descriptor (web.xml file) of the service application.

For instructions, refer to the Installation Guide.

Add the JDBC driver JAR file in the correct location:

```
<PM_HOME>/sm60/instances/<agent instance>/deploy
```

Service Returns 404 Status Code

If the service is returning a 404 status code, it could be because of one of the following:

- Service is down or not initialized
- Issue with firewall

Solution:

To resolve this issue, try the following steps, in sequence:

- Send a request to the endpoint you listed under the service access point. If you still get an HTTP status code 404, the service is down; contact the service provider administrator.
- Delete the Agent handlers and try sending a request to the service. If the request is unsuccessful with a 404, this indicates that either the service is down or it is not initialized.

- Restart the application server instance.

For issues with the firewall, see *Issue with Firewall* on page *20*.

If the problem still persists, contact the Administrator for the service provider.

JDBC Connection Issue

There are several possible reasons for JDBC connection issues.

Solution:

Check the following and correct as needed:

- Filters must be added manually in the deployment descriptor (web.xml file) of the service application. For details and instructions, refer to the Installation Guide.
- Make sure the JDBC driver is in place. It must be in the following location:

  ```
  <AGENT_HOME>/sm60/instances/<AGENT INSTANCE>/deploy
  ```

  JDBC writers use this driver to write the usage monitoring logs.
- If you are still having JDBC connection issues after following the above steps, and you are sure the JDBC driver JAR file is in the deploy folder, there could be a JDBC connection issue. Verify that with any Java.net.ConnectException in the Agent log file. More information about the logs is provided later in this chapter.

  If necessary, save the log files and contact SOA Software Technical Support.

Cannot Create Agent from Configurator Wizard

If you cannot create an instance of the Agent with the Policy Manager configurator wizard, it might be because the application server is running while you are creating the Agent. If the application server is running, you will not be able to create an Agent instance.

Solution:

Stop the application server while creating the Agent from the configurator.

Error Message: “Service Is Blocked”

In some cases, when a request is sent to a service, this error message is returned:

```
SOA Management is not running, service is blocked.
```

There are several possible causes of this error:

- Agent feature is not installed but filters are configured
- Agent application is not started

Solution:

To resolve:

- Install the Agent feature
- Start the Agent application

Cannot Start Agent

If the Agent does not start, there are several possible reasons.

Solution:

Check the following:

- Verify that the bundles started, and check the message in the OSGI console window to see how many bundles started.
- Check the following log files for errors:
  - Agent container logs
  - Application server logs

After completing the above steps, if the problem still persists, contact SOA Software Technical Support.

403 (Forbidden) Status Code Returned

If the Agent filter is configured but either the service is not registered, or is not managed with a container, a request message sent to the service receives a 403 response.

Solution:

Register the service and manage it with a container.

Note: To unmanage the service via an Agent container, you must manually remove the Agent filter configuration from the deployment descriptor of the provider service application.

"Authorization Failed" Message when Consuming a Service

One possible cause of an "authorization failed" error is that the contract is not configured.

Solution:

To check whether the contract is configured correctly, and correct as needed, follow the steps below.

To configure a contract

1 Log in to the Policy Manager console.

2 From the organization tree, select the virtual service.

3 Verify that the intended consumer is listed under the consumers portlet for the virtual service.
4 Verify that the approval status of the provided contract is Activated.
5 If the contract is listed as Deactivated, activate it:
   a) From the Consumers portlet, select the contract.
   b) From the actions portlet, select Activate Contract.

Shared Libraries Not in the Classpath of the Provider Service Application

When an Agent is configured, Agent shared bundles are kept in a shared library space of an application server instance (the exact location is specific to each application server). The JAR files must be available in the classpath of every application deployed in the application server instance.

For more information on these JAR files for a specific Agent, refer to the applicable Install Guide.

Solution:

Copy the JAR files to the shared location and then restart the application server instance.

Application Server Instance Running Out of Memory

If the application server instance is running out of memory, you might need to add more memory.

Solution:

To resolve the issue:

- Contact the application server administrator for optimal memory settings, and allocate more memory if needed.
- Restart the server. This does not resolve the cause, but could be a short-term solution to resolve an immediate memory issue.