SOA™

software

SOA Software API Gateway Appliance 6.2 Administration Guide

Trademarks

SOA Software and the SOA Software logo are either trademarks or registered trademarks of SOA Software, Inc. Other product names, logos, designs, titles, words or phrases mentioned within this guide may be trademarks, service marks or trade names of SOA Software, Inc. or other third parties and may be registered in the U.S. or other jurisdictions.

Copyright

Table of Contents

Chapter 1: Using the API Gateway Appliance Administration Console

OVERVIEW

The *API Gateway Appliance Administration Console* provides tools that allow you to manage your API Gateway Appliance installation. This guide provides a functional overview of the console.

> **Note:** If at any time you need help determining a console password, refer to *Appendix A: Console Default Passwords*.

LAUNCHING API GATEWAY APPLIANCE ADMINISTRATION CONSOLE

The *API Gateway Appliance Administration Console* is accessed using the following URL construction:

https://<ipaddress>:5480/

- IP Address - Represents the address assigned to the API Gateway installation.
- Port Number - 5480 is the required default port used to access the *API Gateway Appliance Administration Console*.

HEADER

The "API Gateway Header" displays the following items:

- **About API Gateway** - Launches a functional overview of the API Gateway Appliance product.
- **Help** - Launches the online help for the *API Gateway Appliance Administration Console*.
- **Logout user admin** – Logs you out of the *API Gateway Appliance Administration Console*.

CONFIGURING THE SYSTEM

The *System* tab allows you to accomplish the following:

- Obtain a summary of system information for the API Gateway Appliance.
- Reboot the API Gateway Appliance.

- Shutdown the API Gateway Appliance.
- Set the Time Zone of the API Gateway Appliance.

CONFIGURING THE NETWORK

The *Network* tab allows you to accomplish the following:

- Obtain the most current network status information for the API Gateway Appliance.
- Specify static IP information or retrieve IP settings from a DHCP server.
- Specify a proxy server and port for accessing external networks

CONFIGURING NETWORK ADDRESS SETTINGS

The *Network Address Settings* section allows you to specify static IP information or to retrieve IP settings from a DHCP server. DHCP is generally used for local laptops, and Static IP is used for enterprise installations.

To Configure Static IP Network Address Settings

Step	Procedure
1.	Navigate to the *Network > Address.*
2.	From the IPv4 Address Type drop-down menu select **Static**. Update the following fields: ● IP Address—IP address of the API Gateway virtual appliance. ● Netmask—Network mask for the virtual appliance. ● IPv4 Default Gateway—IP address of the gateway (network router) ● Preferred DNS Server—IP address of the primary DNS server. ● Alternate DNS Server—IP address of the secondary DNS server.

CONFIGURING PROXY SETTINGS

The *Proxy > Settings* section allows you to specify a proxy server and port for accessing external networks.

To Configure a Proxy Server

Step	Procedure
1.	Navigate to the *Network > Proxy.*
2.	Click the **Use a Proxy Server** checkbox, and specify the following information: ● HTTP Proxy Server—Host name or IP address for the proxy server.

To Configure a Proxy Server

	● Proxy Port—Proxy server communications port. ● Proxy Username (Optional)—Username to access the proxy server. ● Proxy Password (Optional)—Password to access the proxy server.
3.	Save your configuration.

UPDATING THE API GATEWAY APPLIANCE

SOA Software periodically issues updates to the API Gateway appliance for the VMware application, API Gateway Appliance, or Policy Manager. Updates can be applied after the API Gateway Appliance is deployed via the *Update* tab on the *API Gateway Appliance Administration Console*.

Note: You must back up your VMware image before performing an update because the automatic update option will stop the Policy Manager and Network Director instances.

The *Update* tab allows you to accomplish the following:

- View summary information about your virtual appliance and details (i.e., release notes) about the most recent update.
- Configure automatic update method and default repository.
- Check for available updates to the API Gateway Appliance.
- Install updates to your API Gateway Appliance.

BACKING UP YOUR VMWARE IMAGE

The SOA Software API Gateway Appliance update process permanently removes feature files from the installation directory. Therefore, as a standard practice we recommend that you have a complete backup copy of the VMware image where your SOA Software API Gateway Appliance is installed. The backup should include Installation Files and Database.

VIEWING UPDATE STATUS

To view information about your virtual appliance, click the *Update* > *Status*. Here you can:

- View information about the API Gateway Appliance displays including Vendor, Appliance Name, Appliance Version, Last Check, and Last Install.
- Select the *Details* link to view release notes about the most recent update.

Configure Automatic Update Repository and Update Method

Before you use the **Check Updates** and **Install Updates** options on the *Update > Status* page, you must first configure the Update Method and Update Repository on the *Update > Settings* page.

Configure Update Repository

The *Update Repository* section of the *Update Status* screen includes the following Update Repository options:

Update Repository Option Name	Description
Use Default Repository	This option represents the API Gateway Appliance default update repository. During the API Gateway Appliance installation, the *Update* tab was linked to the SOA Software Customer Support site (based on your software license) and the following default repository was assigned: https://support.soa.com/support/appliance/update-gateway.
Use CD-ROM Updates	This option is designed for users who would like to download a CD-ROM ISO image directly from the SOA Software Customer Support website (via the *Downloads > API Gateway* directory) and apply the API Gateway update via the CD-ROM. When you use the **Check Update** function with this option, the system polls the CD-ROM drive to find the API Gateway update files. You can then install it using the **Install Update** function.
Use Specified Repository	This option is designed for users who would like to download API Gateway Appliance updates to their own repository from the SOA Software Customer Support website (via the *Downloads > API Gateway* directory) and apply the update via their repository. When you use the **Check Update** function with this option, the system polls the specified repository location to find and install the API Gateway update.

To Configure Update Repository

Step	Procedure
1.	Navigate to the *Update > Settings.*
2.	Click the radio button of the *Automatic Update* option you would like to use for delivering API Gateway Appliance updates.
3.	If you selected one of the "Automatic" update options, select a day and time from the "Schedule a frequency for the updates" drop-down menus.

To Configure Update Repository

4.	Save your changes.

Check For and Install Updates

When new updates are uploaded to the API Gateway Appliance repository, they can be installed to your API Gateway Appliance using one of the available options (described below).

> **Note:** SOA Software recommends that you use ONLY the "No automatic updates" option to ensure optimum reliability of the update process because the automatic update will stop the Policy Manager instance and Network Director instance.

Automatic Update Option Name	Description
No automatic updates	If you do not want the API Gateway Appliance to automatically check for updates.
Automatic check for updates	If you want the API Gateway Appliance to automatically check for updates.
Automatic check and install updates	If you want your API Gateway appliance to automatically check for and install updates.

To Configure Automatic Update Option

Step	Procedure
1.	Navigate to the *Update > Settings.*
2.	Select the radio button of the update option you would like to use for obtaining API Gateway Appliance updates.
3.	If you selected the "Use Specified Repository" option, specify the Repository URL in the text box.
4.	Save your configuration.

MANAGING THE API GATEWAY APPLIANCE

After the installation of the SOA Software API Gateway Appliance and feature installation are complete, you can then begin managing various aspects of your installation via the *Management* tab.

The *Management* tab allows you to accomplish the following:

- Launch the *Policy Manager Management Console* or *SOA Software Administration Console*.
- Start / Stop Policy Manager, Network Director, and MySQL Database instances.
- Create a tenant and launch the tenant console in the Tenant Management section.
- Manage resource usage on your deployment to ensure optimum performance.
- Change the password of the *API Gateway Appliance Administration Console*.
- Execute site maintenance scripts provided by SOA Software.

LAUNCHING CONSOLES

The *Management / Administration Consoles* section includes links to both the *Policy Manager Management Console* and *SOA Software Administration Console* (for Policy Manager and Network Director instances).

Launch Policy Manager Management Console

- The default login for the *Policy Manager Management Console* is **administrator/password**.
- If you would like to change the administrator password, log into the *Policy Manager Management Console*, and use the **Modify User** function in the *Security* section.

Launch SOA Software Administration Console

- The default login for the *SOA Software Administration Console* is **administrator/password**.
- If you would like to change the Administrator credentials, log into the *SOA Software Administration Console*, and use the **Manage Admin Console Administrator** function in the *Configuration > Configuration Actions* section.

STARTING / STOPPING API GATEWAY INSTANCES

The *Instance Status* section allows you to manage the current state of Policy Manager, Network Director, and MySQL database instances that comprise your API Gateway Appliance deployment. These instances are automatically started as part of the automated installation and configuration process.

- Use the **Start** or **Stop** links to manage the state of each instance.
- A started instance shows a status of *Running*.
- A stopped instance shows a status of *Stopped*.
- The **Start** process takes approximately two minutes.

CREATING A TENANT AND LAUNCHING COMMUNITY MANAGER

If you chose *Option 2: API Gateway Master-Community Manager* for your VMWare instance, a *Tenant Management* section will display in the *Management* tab. Here you can:

- Define a tenant by specifying a series of field parameters and launch the *Community Manager Console*.

To Create a Tenant

<table>
<tr><th>Step</th><th>Procedure</th></tr>
<tr><td>1.</td><td>In the <i>Management</i> > <i>Tenant Management</i> section click <b>Create Tenant</b>. The <b>Create Tenant</b> page displays.</td></tr>
<tr><td>2.</td><td>Enter the following values:
<table>
<tr><td>URL</td><td>This is the base URL of the Platform API. The URL is normally structured similar to the following: http://[hostname/ip address]:9980. This is the hostname or IP Address on which the SOA container is running. There is normally no context unless the product is running in an application server.</td></tr>
<tr><td>Tenant Name</td><td>This is a friendly name for the tenant that may be used in emails, etc.</td></tr>
<tr><td>Tenant Id</td><td>This is the internal id of the tenant. It cannot have spaces or special characters. It should be lower case. It is normally the lower case (without spaces) version of the tenant name above. This will appear in all object ids and the URLs in the system.</td></tr>
<tr><td>Address</td><td>This is the base URL of the tenant. The hostname must be unique. This hostname is what will be used in the browser when accessing the UI and the product will use it to identify the tenant. Do not use any additional context paths in the Address field, as it should be root only. For example, use http://[hostname]:9980, not http://[hostname]:9980/abc/.</td></tr>
<tr><td>Console Address</td><td>This is the same as Address: it is the full URL where Community Manager is running. Console Address is used in the browser when accessing the UI.</td></tr>
<tr><td>Theme</td><td>This is the UI theme identifier. It is typically set to "default" unless a custom theme has been developed.</td></tr>
<tr><td>Email Address</td><td>This is the email address you want to be used as the default tenant administrator.</td></tr>
<tr><td>Password</td><td>This is the password you want to configure for the default tenant administrator.</td></tr>
<tr><td>Contract Email Address</td><td>Used in email templates.</td></tr>
</table></td></tr>
</table>

To Create a Tenant

<table>
<tr><td></td><td><table><tr><td>From Email Address</td><td>Account used by the system to send email.</td></tr><tr><td>Virtual Hosts</td><td>A comma-separated list of host names that the product will accept (e.g., "open.soa.com").</td></tr></table></td></tr>
<tr><td>3.</td><td>After specifying the values click <b>Create Tenant</b>. Do not close the page until you receive a successful pop-up message. Creating a tenant takes approximately three minutes and displays the following message upon completion:
<i>Creating tenant, please do not close this window and wait about three minutes…</i>
If you close the window before receiving confirmation that the tenant was successfully created, you cannot use the tenant as it will only be created on the backend.</td></tr>
<tr><td>4.</td><td>After you create a tenant, verify that it works by clicking the link for the tenant you created.
Note: Verify that the tenant name is accessible from your network. If you would like to access the <i>Community Manager Console</i> on a local system, you must add a hostname in the following hosts file:
• Windows: C:\Windows\System32\drivers\etc
• LINUX: /etc/hosts.</td></tr>
</table>

CHECKING RESOURCE USAGE

The *Management > Resources* section allows you to view a current a listing of processes running on Linux using the **Top Processes** link. You can use this listing to check resources allocated to your virtual machine (e.g., VMware usage) and then take the necessary steps on your own to optimize performance.

CHANGING THE ADMINISTRATOR PASSWORD

The *Management > Actions* section includes a **Change Password** function that allows you to change the administrator password used to log onto the *API Gateway Appliance Administration Console*.

Note: If you forget your password contact SOA Software Customer Support for assistance.

EXECUTING A SCRIPT

The *Management > Actions* section includes an **Execute Script** function that allows you to run scripts that are distributed by SOA Software for the purpose of maintenance or troubleshooting. Each script is signed by SOA Software with a private key.

Note: Only scripts distributed by SOA Software can be run using the **Execute Script** function.

The following example illustrates how to execute a script on the appliance. It is signed in the package apln_script.zip. To run this test substitute the <appliance_ip> with the IP address of your API Gateway deployment.

```
#!/bin/bash
mkdir -p /opt/vmware/share/htdocs/service/management/output
ls / > /opt/vmware/share/htdocs/service/management/output/ls.txt
echo "Please visit
https://appliance_ip:5480/service/management/output/ls.txt"
```

To Execute a Script

Step	Procedure
5.	In the *Management* > *Actions* section click **Execute Script**.
6.	Click **Browse** to select the package to be executed, and then **Upload**.
7.	You will receive a confirmation message indicating that the script has been successfully uploaded, plus a question asking whether you would like to execute the script. To execute the script, click **Yes**. Do not close the window until a confirmation message displays showing the result URL.
8.	Obtain the output of the script by launching the URL specified in the confirmation message.

USING LOGS

The *Logs* tab provides a listing of application log files that contain events logged by Policy Manager, Network Director, and the System (i.e., database/operating system). These logs can be used to troubleshoot issues associated with your API Gateway Appliance or Policy Manager or Network Director instances.

The following logs are provided:

- Gateway - This log holds the messages after the classes are loaded and the Policy Manager and Network Director container starts running.
- Stdout - This log prints the output stream of events to the command line.
- Startup - This log holds log messages while the classes are being loaded.
- System - This log captures a history of actions executed by the database management system and operating system.

Appendix A: Console Default Credentials

The following table provides default username / password credentials that are used during API Gateway Appliance installation tasks and for logging into consoles that are accessed via the API Gateway Appliance Administration Console.

Console Name	Default Username / Password
Root Login Credentials *(for initial API Gateway Appliance Installation)*	• If this is your first login, enter the root login credentials **admin/password** and choose a new password. **Note:** When performing the change password process, remember to enter your existing password first, followed by the new password and confirmation. • Your new password will also be your login credentials for the *API Gateway Appliance Administration Console*. • If you forget your root login credentials contact *SOA Software Customer Support*. *Password Rules:* • Password must be 6 to 8 characters in length and cannot contain a space. • Password cannot include Linux reserved words. • Password cannot be the reverse, same with a change of case, similar, or rotated version of the previous password.
Policy Manager Management Console	• The default login for the *Policy Manager Management Console* is **administrator/password**. • If you would like to change the administrator password, log into the *Policy Manager Management Console*, and use the **Modify User** function in the *Security* section.
SOA Software Administration Console	• The default login for the *SOA Software Administration Console* is **administrator/password**. • If you would like to change the Administrator credentials, log into the *SOA Software Administration Console*, and use the **Manage Admin Console Administrator** function in the

Console Name	Default Username / Password
	Configuration > Configuration Actions section.
SOA Software Network Director Slave *(for initial installation)*	If you change the *Policy Manager Management Console* username/password to something other than the administrator/password default, the console installation process will prompt you for the new password.