SOA Software API Gateway Appliance 6.2 Installation Guide for VMware®

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

PREFACE

OVERVIEW

The SOA Software API Gateway virtual appliance is a virtual machine that provides an automated installation and configuration approach for SOA Software's Community Manager, Policy Manager, and Network Director. Product installations are packaged in the following feature sets:

- Option 1: SOA Software API Gateway Master

    Installs a virtual machine with Policy Manager, Network Director, and MySQL Server.

- Option 2: SOA Software API Gateway Master—Community Manager

    Installs a virtual machine with Community Manager, Policy Manager, and Network Director with options for installing an internal MySQL database or using an external database (e.g., Oracle, Microsoft SQL Server, or MySQL Server).

- Option 3: SOA Software API Gateway Slave

    Installs a virtual machine with Network Director. The Network Director instance will be a node of the Network Director Cluster created on the master appliance.

DEPLOYMENT DIAGRAMS

You can choose an option from one of the deployment scenarios described in the diagrams below to decide which feature to install.

> **Note:** Option 3: SOA Software API Gateway Slave is used *only* if you plan to deploy the Network Director Cluster scenario.
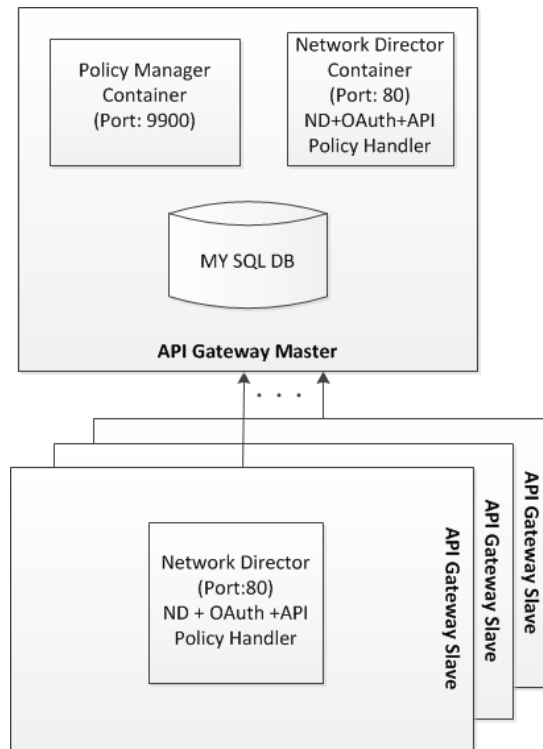
Figure 1: Deployment Diagram for Feature Option 1 (SOA Software API Gateway Master) and Multiple Instances of Feature Option 3 (SOA Software API Gateway Slave)
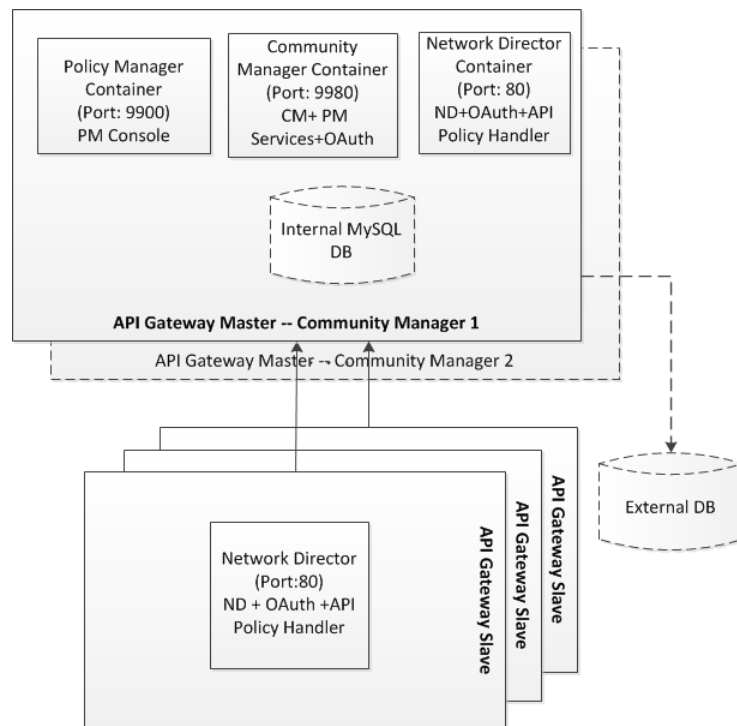
Figure 2: Deployment Diagram for Feature Option 2 (SOA Software API Gateway Master - Community Manager) and Multiple Instances of Feature Option 3 (SOA Software API Gateway Slave)

IN THIS GUIDE

This guide includes the following:

- Deploying and Installing the API Gateway Appliance

    o Step 1 – Download API Gateway Appliance

    o Step 2 – Deploy API Gateway Appliance

    o Step 3 – Select API Gateway Appliance Features

    o Step 4 – Use It

- Appendix A – System Requirements

- Appendix B – Console Default Credentials

- Appendix C – Setting Up a Community Manager Tenant

- Appendix D – Documentation

- Appendix E – Customer Support

DEPLOYING AND INSTALLING THE API GATEWAY APPLIANCE

OVERVIEW

The following instructions tell you how to deploy and install the SOA Software API Gateway Appliance on supported VMware® environments.

Note: If you need help determining a console password, refer to *Appendix B: Console Default Passwords*.

STEP 1: DOWNLOAD API GATEWAY APPLIANCE

Download the SOA Software API Gateway Appliance ZIP or OVF files to your local machine via the SOA Software Customer Support website (support.soa.com) from the following location:

Downloads -> API Gateway

Select the format that is supported by the VMware version you are using (see *Appendix A: System Requirements*).

VMware Version	Setup File Type
VMware vCenter Server 5.1 > VMware ESX 5.1	OVF
VMware Workstation 9.0	ZIP

STEP 2: DEPLOY API GATEWAY APPLIANCE

- Before you start VMware, verify that your Memory and Network Adaptor settings comply with those specified in *Appendix A: System Requirements*.

- The deployment process automatically assigns a default host name of **soagw**.

To Deploy the API Gateway Appliance

Step	Procedure
1.	For VMware ESX 5.1: • Use the vCenter *Deploy OVF Template* wizard to deploy the OVF file. • Select **Power on after deployment**. For VMware Workstation 9.0:

To Deploy the API Gateway Appliance

	• Extract the downloaded `ZIP` file to a local folder. • Use VMware Workstation 9.0 to **Open** the `vmxf` file. • Select **Power on this virtual machine**.
2.	During the installation process: • You can use the space bar to scroll down to the end of the agreement. • Accept the license agreement.
3.	The deployment process takes approximately three minutes.
4.	After the initial deployment, you are presented with Login and Set Timezone (Current: <timezone>) options. **Set Time Zone:** • We recommend setting your system time zone before starting the installation. Policy Manager will be automatically installed according to the system time zone. You can also change the time zone in the *Policy Manager Management Console* after you complete the installation. **Login:** • If this is your first login, enter the root login credentials **admin/password** and provide a new password. Refer to *Appendix B: Console Default Credentials* for information on default passwords and password rules. **Note:** When performing the change password process, remember to enter the default password first, followed by the new password and confirmation. • Please make sure you remember the password. Your new password will also be your login credentials for the *API Gateway Appliance Administration Console*.
5.	After the deployment is complete, continue to *Step 3: Select API Gateway Appliance Features*.

STEP 3: SELECT API GATEWAY APPLIANCE FEATURES

After you complete the initial login process and upload the MySQL Connector, you configure the API Gateway Appliance for selected feature sets. There are three configuration options, each with different configuration requirements.

Option	Feature Set Name	Description
1	SOA Software API Gateway Master	• Includes Policy Manager and Network Director features, and internal MySQL Server.

Option	Feature Set Name	Description

2	SOA Software API Gateway Master — Community Manager	• Includes Community Manager, Policy Manager and Network Director features. This feature set offers two Database support options:
		
		    o Create a database on an internal MySQL Server.
		
		    o Use an external database. The appliance supports Oracle, Microsoft SQL Server, and MySQL Server).
		
		Note: If you are using Microsoft SQL Server, uploading the database driver file is not required as it's included as part of the feature set installation.

3	SOA Software API Gateway Slave	• Includes Network Director feature. • You must specify the IP address of the API Gateway Master. This enables the API Gateway Slave to connect to the database on the API Gateway Master. • The API Gateway Master must be running when the *SOA Software API Gateway Slave* feature is being installed.

Note: Refer to the *Deployment Diagrams* section in the *Preface* to decide which feature set to install. Each virtual appliance can only support a single feature set.

To Install the API Gateway Appliance Features

1.	Choose a feature set to install from the displayed list. • During the installation, you will see a list of tasks being performed (i.e., installation, configuration, startup, and an expected time of completion). • The startup process takes approximately three minutes. Note that the Linux interface may show a notification that describes the status as well as the expected wait time.
2.	If you choose to install *Option 2: SOA Software API Gateway Master—Community Manager* (with an external database) or *Option 3: SOA Software API Gateway Slave*, you will be prompted to "Enter Gateway ID." This Gateway ID must be a string without a space and can contain letters, numbers or a dash "-" character.
3.	**Upload Database Driver File** • First download your database driver from the MySQL or Oracle website (MySQL: com.springsource.com.mysql.jdbc-5.1.6.jar, Oracle: ojdbc6.jar). • Then launch https://ip:5480/dbdrive.html in your browser and upload the MySQL Server or Oracle database driver.
4.	**SOA Software Slave Feature**

To Install the API Gateway Appliance Features

	If you choose the *SOA Software API Gateway Slave* feature, you will be prompted for more information: • At the **Enter the hostname of the primary gateway prompt**, specify the IP address of the Master API Gateway and password of the admin user. • The API Gateway Master must be running. This will exchange the admin user account SSH public keys of the primary and slave gateways to enable communication after the installation is complete.

To Verify API Gateway Appliance Installation

1.	After the appliance installation is complete, the system displays the *API Gateway Appliance Administration Console* URL that you will launch to complete the remaining installation tasks. The default URL is https://<ip address>:5480/.
2.	To illustrate what you've accomplished: • Log into the *API Gateway Appliance Administration Console* for the API Gateway Master (https://<ip address>:5480/). • On the *Management* tab, you will see the container instances that you installed. If you installed *Option 1: SOA Software API Gateway Master*, use *the Policy Manager Management Console* URL and log in using the default credentials (administrator/password) at http://<ip address>:9900/. • From the *Policy Manager Management Console*, select the *Containers* folder in the root level Organization to verify that the Network Director container is running (State = Started). • If you have multiple Network Director Slaves, you can also verify that these Network Director containers are running.
3.	**Option 2: SOA Software API Gateway Master—Community Manager** If you chose *Option 2: SOA Software API Gateway Master - Community Manager*, you must create a tenant. On the *Management* tab of the A*PI Gateway Administration Console*, click the **Create Tenant...** under the *Tenant Management* section. This opens the *Create Tenant* page. ● Enter values in all of the fields on the *Create Tenant* page. Refer to *Appendix C: Setting up a Community Manager Tenant* for more information about each field on the *Create Tenant* page. ● 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/. ● After specifying the values click **Create Tenant**. 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: *Creating tenant, please do not close this window and wait about three minutes…* 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.

To Verify API Gateway Appliance Installation

	• After you create a tenant, verify that it works by clicking the link for the tenant you created. *Note: If you are using an external database, the tenant URL will not be displayed.* **Note:** Verify that the tenant name is accessible from your network. If you would like to access the *Community Manager Console* on a local system, you must add a hostname in the following hosts file: • Windows: C:\Windows\System32\drivers\etc • LINUX: /etc/hosts.
4.	Refer to the *SOA Software API Gateway Appliance Administration Guide* where you will use the *API Gateway Appliance Administration Console* to complete a series of general configuration tasks that apply to all feature sets including: • Configuring Network Address and Proxy Settings • Updating the API Gateway Appliance .

STEP 4: USE IT

Now that you've completed the installation of one or more API Gateway feature sets, it's time to start using the system to publish services, monitor services, define policies, and so on. Refer to the *Policy Manager Getting Started Guide* for details.

APPENDIX A: SYSTEM REQUIREMENTS

The following table provides hardware requirements, a list of VMware versions that the SOA Software API Gateway Appliance product has been certified on, and a list of minimum system requirements for running the SOA Software API Gateway Appliance.

Item	Requirement
VMware Environment to Host the API Gateway Virtual Appliance	• VMware vCenter > ESX 5.1 (Requires OVF setup file) • VMware Workstation 9.0 (Requires ZIP setup file)
Resources required by API Gateway Virtual Appliances	• 64-bit Processor ONLY. • Memory: The default and recommended memory size is 6GB with 3GB minimum. • CPU: 2 cores • Hard Drive: 60GB • Network Adapter: One Ethernet Network Adapter • IP Address: DHCP server is required to provide an IP address. One static IP address is required to be configured on the primary virtual appliance if slave virtual appliances 4neet to be set up. IPV4 is supported. • DNS Setting: One host name for each tenant must be configured in the DNS server if the virtual appliance needs to host tenants. • Communication Port: TCP 22, 80, 3306, 5480, 9900
Web Browser	• Internet Explorer 8 • Mozilla Firefox 23

APPENDIX B: 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 provide 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**. • After you log into Policy Manager, you can change the administrator password via the *Security* tab.
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.

APPENDIX C: SETTING UP A COMMUNITY MANAGER TENANT

Community Manager requires at least one tenant. Each tenant is logically separate from every other tenant and is keyed off the hostname used to access the console. The following table provides a brief description of each field that you see on the *Create Tenant* page:

Field	Description
URL	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.
Tenant Name	This is a friendly name for the tenant that may be used in emails, etc.
Tenant Id	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.
Address	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/.
Console Address	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.
Theme	This is the UI theme identifier. It is typically set to "default" unless a custom theme has been developed.
Email Address	This is the email address you want to be used as the default tenant administrator.
Password	This is the password you want to configure for the default tenant administrator.
Contact Email Address	Used in email templates.
From Email Address	Account used by the system to send email.
Virtual Hosts	A comma-separated list of host names that the product will accept (e.g., "open.soa.com")

APPENDIX D: DOCUMENTATION

After the base product installation is complete, refer to the following product documentation for Policy Manager administration and usage information.

- API Gateway Appliance Administration Guide

- Policy Manager Getting Started Guide

- Policy Manager Online Help

- Policy Manager Administration Guide

APPENDIX E: CUSTOMER SUPPORT

SOA Software offers a variety of support services to our customers. The following options are available:

Support Options:	
Email (direct)	support@soa.com
Phone	1-866 SOA-9876 (1-866-762-9876)
Email (Web)	The "Support" section of the SOA Software website (www.soa.com) provides an option for emailing product related inquiries to our support team.
Support Site	SOA Software Customer Support website (`https://support.soa.com/support`)