Oracle® Communications Services Gatekeeper

Getting Started Guide

Release 6.1

E64620-02

November 2016

ORACLE®

Oracle Communications Services Gatekeeper Getting Started Guide, Release 6.1

E64620-02

Contents

Preface

This book explains how to quickly get a Services Gatekeeper implementation up and running.

Audience

This document is intended for IT personnel who will install Services Gatekeeper, especially for the purpose of API management.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Communications Services Gatekeeper Release 6.0 documentation set:

- *Oracle Communications Services Gatekeeper Concepts*
- *Oracle Communications Services Gatekeeper System Administrator's Guide*

1

Getting Started with Services Gatekeeper

This document explains how to install and start the default (single-tier) version of Services Gatekeeper, and add additional clustered servers as needed.

About Installing Services Gatekeeper

This chapter explains how to install a default (single-tier) Services Gatekeeper implementation that you use to manage APIs, partners, and interfaces.

See *Services Gatekeeper Concepts* for information on the difference between Services Gatekeeper and multi-tier Services Gatekeeper. See “Installing Services Gatekeeper” in *Services Gatekeeper Multi-tier Installation Guide* for information on how to install a multi-tier Services Gatekeeper implementation.

The default Services Gatekeeper implementation includes everything you need to start, run, and test a Services Gatekeeper implementation for API management.

Services Gatekeeper is built on top of Oracle WebLogic Server and can use all WebLogic Server components. A knowledge of WebLogic Server is not required for installing the default Services Gatekeeper implementation, but it would be helpful for administering larger implementations. The WebLogic Server documents are referenced from this documentation set where appropriate.

Services Gatekeeper requires a database, and it ships with a version of Java DB for you to use. You also have the option to use your own Oracle RAC Database, or MySQL Cluster Carrier Grade Edition (CGE) database which you must install before Services Gatekeeper. The "(Optional) Installing a Different Database" section explains how.

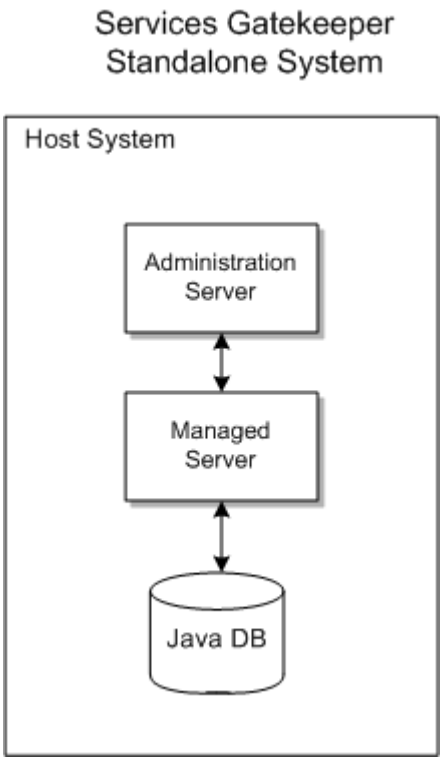
You also have the option of creating a clustered system to take advantage of the high availability protection, and using the WebLogic Server Node Manager utility to control the clustered system. See "Adding a Managed Server to Create a Clustered Services Gatekeeper Implementation" and "Controlling Clustered Managed Servers with WebLogic Node Manager" for details.

Before installing Services Gatekeeper, you need to download and install the Java SDK on your host system. After that, installing a standalone Services Gatekeeper implementation using the default Java DB database should take less than 10 minutes. The "Installing the Java JDK and JCE" section explains how to obtain the JDK.

Figure 1–1 shows the default Services Gatekeeper single-tier standalone implementation installed on a single host system. This figure shows the default Java DB being used as the database. You can also use your own Oracle RAC Database, or a MySQL CGE database. You can run any of these databases on their own separate, dedicated system.

You can also easily scale your Services Gatekeeper implementation by dynamically adding more managed servers to create a clustered system for high availability. See "About Using a Clustered Services Gatekeeper Implementation" and "Adding a Managed Server to Create a Clustered Services Gatekeeper Implementation" for information.

Figure 1–1 Services Gatekeeper Standalone System



After it is installed, see "Starting and Stopping Services Gatekeeper" for information on how to start the Services Gatekeeper servers. See "Start the Tools to Manage Your APIs" for information on how to get the Services Gatekeeper API and Partner Manager GUI up and running.

Finally, if you need to remove Services Gatekeeper from the host system, see "Uninstalling Services Gatekeeper" for instructions.

Understanding the Services Gatekeeper Administrative Accounts

Services Gatekeeper and the underlying WebLogic Server software rely on different levels of administrative users to maintain and administer the implementation. During installation, you are prompted for the user names and passwords of these users:

- A domain user name. This is the default WebLogic administrative account that you use to control and configure the Services Gatekeeper Administration Server. The default user name is **weblogic**, but for security reasons Oracle encourages you to use a different user name for production implementations. You are prompted for a password for this user.
- A Partner Manager Portal user. This is a user required to access the Partner and API Management Portal GUI tool that you use to administer your API Management accounts. The default user name is **op**, but for security reasons,

Oracle encourages you to use a different user name for production implementations. You are prompted for a password for this user.

This user is also important because this user creates or approves the partner and network service supplier (NSS) accounts that partners and NSSs create using the Partner Portal and Network Service Supplier Portal GUI tools.

See these sections for more information on the administrative users that Services Gatekeeper and the API management GUI tools use:

- "Managing Users and User Groups" in *Services Gatekeeper System Administrator's Guide*
- "Managing Partner and Partner Groups" in *Services Gatekeeper API Management Guide*

Hardware, Software, and Database Requirements

You can install Services Gatekeeper on the Windows (test-only), Solaris, and Linux systems. See "Software Requirements" and "Hardware Requirements" for a list of the supported hardware and software required for the host system.

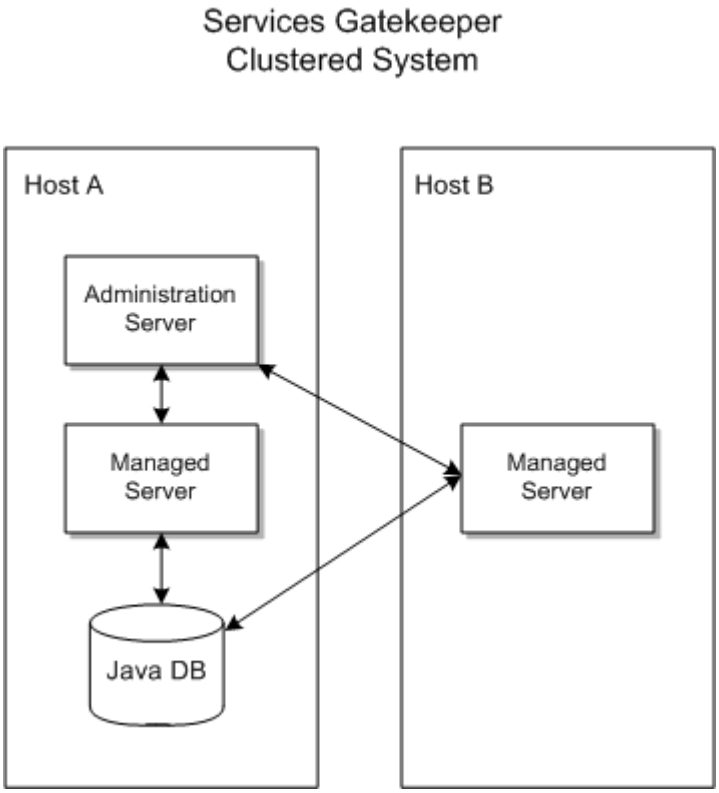
The single-tier Services Gatekeeper implementation requires a database and comes with a built-in Java DB database you can use. Java DB is appropriate for test and evaluation implementations, and small to medium size production implementations. If you have a larger production system, you will probably use one of the other supported databases. See "Supported Databases" for a list of the supported databases.

About Using a Clustered Services Gatekeeper Implementation

You can create a clustered Services Gatekeeper environment, which allows your implementation to continue working if one system become unavailable for any reason. In a clustered environment, you install a complete Services Gatekeeper (Administration Server, managed server, and database) on one system, and then install just a managed server and database on another system. You can add additional managed servers at any time. If one of the systems becomes unavailable, the other(s) have managed serves to continue processing traffic.

Figure 1–2 shows a simple clustered system using the default Java DB on the same system as the Services Gatekeeper servers.

Figure 1–2 Services Gatekeeper Clustered System



You also have the option of installing the database on its own host system. This is not required, but it is a likely choice for larger production systems, because databases are more efficient on a dedicated system.

What You Need to Know Before Installation

You need the following information before you begin the Services Gatekeeper installation:

- The directory where you will install Services Gatekeeper. Or use the default **/home/***username***/oraInventory** directory. Make sure you have write permission for the installation directory.
- (Optional) If you are not using the default database, you need this information for the database you are using:
  - The database service name
  - The database user name and password
  - The database host name
  - The database instance name
  - The database port number
- If you are going to offer your partners or subscribers any of the Services Gatekeeper communication service capabilities, choose them before you start the installation. You can install them afterward, but it is easier to do it during installation. See *Communication Service Reference Guide* for a list of the communication services and details on their capabilities. Also see "Adding Communication Services to Services Gatekeeper" for more information.

Note: Services Gatekeeper requires administrator access if you are installing it on a Windows-based host system.

Placeholders Used in this Guide

Table 1–1 lists the placeholders used in this guide.

Table 1–1 Placeholders Used in this Documentation

Placeholder	Description
Middleware_home	The directory that serves as the repository for common files that are used by Oracle Communications products installed on the same machine, such as Services Gatekeeper and WebLogic Server. The files in the *Middleware_home* directory are essential to ensuring that software operates correctly on your system. They: ■ Facilitate checking of cross-product dependencies during installation ■ Facilitate Service Pack installation
Services_Gatekeeper_home	The directory in which the Services Gatekeeper software is installed. By default, this is a subdirectory of *Middleware_home*; for example, *Middleware_home***/ocsg**.
domain_home	The directory in which the Services Gatekeeper domain resides, located in *Middleware_home***/user_projects/domains**.
installer_file	The product installation file that you download and run to install the software.

Installing the Java JDK and JCE

The Oracle Java Development Kit (JDK) is required to run the Services Gatekeeper installation program, and the JDK must be installed on your system before you install Services Gatekeeper. Oracle also recommends that you download the Java Cryptography Extension (JCE) to protect applications with 24- and 32-bit application passwords.

Installing the JDK

You must download and install a supported JDK on the target machine before installing Services Gatekeeper. If you are installing on a 64-bit system, you must install a 64-bit JDK or a hybrid 32/64-bit JDK. See "Software Requirements" for information about the required JDK version.

Download the JDK from the Java page on the Oracle Technology Network website at:

`http://www.oracle.com/technetwork/java/index.html`

Setting the Java Path

You must set the Java path on the target machine.

To ensure that the appropriate JDK is installed and that the Java path is set:

1. Log in to the target system.

2. Run the `java -version` command, or the `java -d64 -version` command on platforms using a 32/64-bit hybrid JDK, to ensure that the **JAVA_HOME** variable is set to a 64-bit JDK.

   If JAVA_HOME is not correctly set, set it to point to the correct JDK.

3. Add the **bin** directory of the JDK that you installed to the beginning of the **PATH** variable definition. For example:

   ```
   PATH=$JAVA_HOME/bin:$PATH
   export PATH
   ```

   Where JAVA_HOME represents the full path to the JDK directory.

Installing the JCE

This section explains how to install the Java Cryptography Extension to the JDK that Services Gatekeeper uses.

1. Open a browser on the system running Services Gatekeeper, and navigate to the Oracle Integrated Cloud Applications and Platform Services web site:

   `http://www.oracle.com/index.html`

2. Search for "Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files."

3. Download the .zip file for the JCE version that matches the JDK you installed with Services Gatekeeper. Use this UNIX command in a shell if you do not remember:

   which java

   Record the *Java_installation_home* location. You need to replace files ther.

4. Extract the .zip file.

5. Copy the l**ocal_policy.jar** and **US_export_policy.jar** files.

6. Navigate to your *Java_installation_home***/jr/lib/security** directory and replace the old versions by pasting the l**ocal_policy.jar** and **US_export_policy.jar** files here.

7. Restart all Services Gatekeeper servers.

Your Services Gatekeeper implementation now accepts 24- and 32-bit encryption passwords. When you are securing your Services Gatekeeper implementation, you will enter such a key to encrypt application passwords.

(Optional) Installing a Different Database

Services Gatekeeper can be used with its own Java DB database, or you can use one of the supported Oracle RAC or MySQL databases. See "Hardware, Software, and Database Requirements" for more information. If you are using Oracle RAC or MySQL database, you need to install and start it before you install Services Gatekeeper. See your database installation documentation for instructions on how to install it. Do this before you install Services Gatekeeper. The database can be used on the same system as Services Gatekeeper, or another host system.

Installing Services Gatekeeper

The installation program is a GUI tool that prompts you for the information required to complete the installation and configure the domain. This section explains how to install a standalone implementation of Services Gatekeeper with the servers and

database on a single system. To create a clustered implementation, follow the instructions in this section and then the instructions in "Adding a Managed Server to Create a Clustered Services Gatekeeper Implementation".

To get a test and evaluation version of Services Gatekeeper up and running quickly, just accept the default settings and enter two passwords. The passwords are for a domain user, and an API and Partner Manager GUI user.

> **WARNING: Single-tier Services Gatekeeper is preconfigured to use the services-gatekeeper-domain domain name. Do not change this name.**

For a production environment, you probably need to change some of the default settings. The installation screens include help messages to guide you.

To install Services Gatekeeper:

1. Log into the target system.
2. Confirm that you followed the steps in "Installing the Java JDK and JCE" and installed the Java JDK in your *Services_Gatekeeper_home* (you see the **java_sdk_home** subdirectory in *Services_Gatekeeper_home*).
3. Download the Oracle Communications Services Gatekeeper 6.0 Media Pack software file from:

   `https://edelivery.oracle.com`

   and put it in your *Services_Gatekeeper_home*. A login for the edelivery web site is required.
4. Change the directory to the *Services_Gatekeeper_home* directory.
5. In a command window, run this command in *Services_Gatekeeper_home* to start the installation:

   ```
   java -jar ocsg_generic.jar
   ```

   The Installation Inventory Setup screen appears.
6. If required, change the Inventory Directory and Operating System Group options.
7. Click **Ok**.

   The Welcome screen appears.
8. Click **Next**.

   The Installation Location pane appears.
9. If required, enter an alternate location and click **Next**.

   The Installation Type pane appears.
10. Select between the **Default Installation** and **Custom Installation** options.
    - If you selected **Default Installation**, the Prerequisite Checks screen appears. Skip to Step 12.
    - If you selected **Custom Installation**, the Features to Install screen appears.
11. Select the Services Gatekeeper communication services to install.

    The Prerequisite Checks screen appears and starts checking the host system.
12. Wait for the green checkmarks to appear, and then click **Next**.

The Domain Information screen appears.

13. Edit these fields as necessary for your implementation, and enter passwords for the domain and partner manager portal users. If you only run one test implementation, you can simply accept the defaults and enter the two passwords.

    Oracle recommends that you always change default port numbers for security reasons. Changing port numbers also helps prevent unexpected behavior if you test more than one Services Gatekeeper implementation at a time.

    You will use the user names and passwords to start the API management tools, and the coherence cluster port to set up other clustered systems, so be sure to record your choices.

    The individual fields have help messages at the bottom of the window to guide you.

14. Click **Next**.

    The Database Information screen appears.

15. Select a database to use:

    The help messages will guide you through the choices. If you choose:

    - **Java DB**, skip to step 17. Java DB is the default database supplied with Services Gatekeeper.
    - **Oracle DB RAC**, go to Step 16.
    - **MySQL Carrier Grade Edition**, go to step 16.
    - **Ignore Database Setting**, skip to Step 17.

16. Enter this information for your database:

    - Service Name
    - A database user name
    - The password for the database user
    - The database host name
    - The Instance name
    - The port number the database uses

17. Click **Next**.

    The Installation Summary screen appears.

18. Click **Install**.

19. The Installation Progress screen appears and the installation begins.

    Wait for the green checkmarks to appear. There are **View Messages** and **View Logs** buttons that you can use to view status during or after the installation.

20. Click **Finish**.

Go to "Starting and Stopping Services Gatekeeper" for instructions on how to start the process and GUI tools you use to run Services Gatekeeper.

Installing Single-tier Services Gatekeeper in Silent Mode

Using silent mode, you can configure installation options once, and then using those settings to duplicate the installation on many machines. The installation program

reads your settings from the configuration file that you create prior to beginning the installation. The installation program does not display any options during the installation process. Silent-mode installation works on all supported systems.

Adding a Managed Server to Create a Clustered Services Gatekeeper Implementation

This section explains how to create a clustered Services Gatekeeper implementation. Figure 1–2 shows an example of a clustered system. To create a clustered system, you install a standalone Services Gatekeeper implementation on one system, and then install just the Services Gatekeeper managed server on a separate system. You then run a script to connect the systems.

You can add more managed servers to your cluster later as your implementation requires them.

To add a managed server to a clustered implementation:

1. (If you use a standalone database) Log on to the system with the standalone database.
2. Start the database.

   See your database documentation for instructions.
3. Ensure that you have followed the instructions in "Installing Services Gatekeeper" and "Starting a Standalone Services Gatekeeper Implementation" and have installed and started Services Gatekeeper on a standalone system.
4. Log on to the system to receive the new managed server.
5. Follow the instructions in "Installing Services Gatekeeper" again to install the managed server. The steps are the same with these exceptions:
   - In Step 13, be sure to use the same coherence port number as the system with the Administration Server.
   - In Step 15, select **Ignore Database Setting** on the **Database Information** window.
6. Log on to the system running the Administration Server.
7. Change the directory to *Middleware_home*/**Oracle_home/extend_wizard**.
8. Run this script:
   - Solaris/Linux:

     ```
     extendDomain.sh IP_addr_new_system server_name_new_system
     ```
   - Windows:

     ```
     extendDomain.cmd IP_addr_new_system server_name_new_system
     ```

   For example:

   ```
   ./extendDomain.sh 155.155.10.105 ManagedServer2
   ```
9. Copy this file from the system with the administration server:

   domain_home/**services-gatekeeper-domain/security/SerializedSystemIni.dat**

   To this directory on the system with the new managed server:

   domain_home/**services-gatekeeper-domain/security**

10. On the system with the new managed server, change the directory to *domain_home*/**services-gatekeeper-domain/bin**.
11. Run this script. It starts the managed server and identifies the system with the Administration Server:
    - Solaris/Linux:

      ```
      startGatekeeper.sh IP_addr_admin_server_system
      ```

    - Windows:

      ```
      startGatekeeper.cmd IP_addr_admin_server_system
      ```

The two systems now function as a clustered Services Gatekeeper implementation. See "Starting a Clustered Services Gatekeeper Implementation" for information on how to start the Services Gatekeeper serves and database.

Starting and Stopping Services Gatekeeper

You use the **startWeblogic.sh** script to start the Services Gatekeeper managed server and Java DB, and the **StartGatekeeper.sh** script to start the Services Gatekeeper Administration Server. If you use a different database, see your database documentation for instructions on how to start it. These sections explain how to start Services Gatekeeper implementations using Java DB:

- Starting a Standalone Services Gatekeeper Implementation
- Starting a Clustered Services Gatekeeper Implementation

Starting a Standalone Services Gatekeeper Implementation

You use the **startWeblogic.sh** and **StartGatekeeper.sh** scripts to start the Services Gatekeeper servers and the JavaDB database.

You are prompted for the domain user name that you entered during installation when running the **startWeblogic** script. The default user name is **weblogic**. You can avoid entering the user name and password manually by creating a **boot.properties** file in your *domain_home*/**services-gatekeeper-domain/security** directory. For details, see *Oracle WebLogic Server 12c: Creating a Boot Identity File for Easier Server Startup* on the Oracle Technology Network website at:

`http://www.oracle.com/webfolder/technetwork/tutorials/obe/fmw/wls/12c/15-BootProp--4471/bootproperties.htm`

To start a standalone Services Gatekeeper implementation:

1. (If you use a standalone database) Log on to the system with the standalone database, and start the database.

   See your database documentation for instructions.
2. Log on to the Services Gatekeeper system.
3. Change the directory to *domain_home*/**services-gatekeeper-domain**.

   services-gatekeeper-domain is the default domain name. if you created a different domain then navigate to that directory.
4. Run the **startWeblogic** script to start the Administration Server with this syntax:
   - Solaris/Linux:

     ```
     ./startWeblogic.sh
     ```

- Windows:

```
./startWeblogic.cmd
```

5. Change the directory to *domain_home*/**services-gatekeeper-domain/bin**.
6. Run the **startGatekeeper** script to start the managed server and Java DB with this syntax:
   - Solaris/Linux:

```
./startGatekeeper.sh
```

   - Windows:

```
./startGatekeeper.cmd
```

   You are prompted for the database user password you entered in step 13 of "Installing Services Gatekeeper".

After you have started your Services Gatekeeper servers, you can start the API and Partner Manager GUI and start administering APIs. See "Start the Tools to Manage Your APIs" for instructions.

Starting a Clustered Services Gatekeeper Implementation

In a clustered Services Gatekeeper implementation, the first step is to start your database if you use one on an external system. Then you need to start the Services Gatekeeper Administration Server with the **startWeblogic** script. Finally, start the Services Gatekeeper managed server with the **StartGatekeeper** script.

You are prompted for the domain user name that you entered during installation when running the **startWeblogic** script. The default user name is **weblogic**. You can avoid entering the user name and password manually by creating a **boot.properties** file in your *domain_home*/**services-gatekeeper-domain/security** directory. For details, see *Oracle WebLogic Server 12c: Creating a Boot Identity File for Easier Server Startup* on the Oracle Technology Network website at:

http://www.oracle.com/webfolder/technetwork/tutorials/obe/fmw/wls/12c/15-BootProp--4471/bootproperties.htm

To start a clustered Services Gatekeeper implementation:

1. (If you use a standalone database) Log on to the system with the standalone database and start the database.

   See your database documentation for instructions.
2. Log on to the system with the Services Gatekeeper Administration Server.
3. Change the directory to *domain_home*/**services-gatekeeper-domain**.
4. Run the **startWeblogic** script to start the Administration Server with this syntax:
   - Solaris/Linux:

```
./startWeblogic.sh
```

   - Windows:

```
./startWeblogic.cmd &
```

5. Log on to a system running just the managed server.

6. Change the directory to *domain_home*/**services-gatekeeper-domain/bin**.
7. Run this script to start the managed server and identify the system with the Administration Server:
   - Solaris/Linux:

     ```
     ./StartGatekeeper.sh IP_addr_administration_server
     ```

   - Windows:

     ```
     ./StartGatekeeper.cmd IP_addr_administration_server
     ```

   You are prompted for the database user password you entered in step 13 of "Installing Services Gatekeeper".
8. Repeat Steps 5 through 7 on all of the systems running a managed server.

After your database and the Services Gatekeeper servers are running, you can start the API and Partner Manager GUI and start administering APIs. See "Start the Tools to Manage Your APIs" for instructions.

Starting a Standalone System Using Node Manger

If you use the WebLogic 12c Node Manager program, you have the option of using it to start and control your domain. You do this by running the *domain_home*/**bin/startNodeManager** script. This script starts the Administration Server and gives you control over the managed server.

Stopping Services Gatekeeper

You stop Services Gatekeeper by stopping the Administration Server, the managed server, and the database.

To stop Services Gatekeeper:

1. Log on to the Services Gatekeeper system.
2. Stop the Administration Server with this command:
   - Solaris/Linux:

     ```
     ./stopWeblogic.sh
     ```

   - Windows:

     ```
     ./stopWeblogic.cmd
     ```

3. Stop the managed server on all systems by logging on to each system and running this command:
   - Solaris/Linux:

     ```
     ./stopManagedWeblogic.sh
     ```

   - Windows:

     ```
     ./stopManagedWeblogic.cmd
     ```

4. If you do not use the Java DB database, see your database documentation for instructions on how to stop it.
5. If you use the Java DB database, stop the it with this command:
   - Solaris/Linux:

```
dbcontrollerstop.sh
```

- Windows:

```
dbcontroller.cmd
```

Controlling Clustered Managed Servers with WebLogic Node Manager

You can use the WebLogic Server Node Manager utility to control the Administration Server and managed servers in a clustered Services Gatekeeper implementation.

See *Fusion Middleware Node Manager Administrator's Guide for Oracle WebLogic Server* for information on the Node Manager utility. Start with the "Introduction and Roadmap" section in that guide.

To install a clustered Services Gatekeeper implementation under Node Manager control:

1. Follow the instructions in "Starting a Standalone Services Gatekeeper Implementation" to install a standalone Services Gatekeeper implementation with an Administration Server.
2. Log on to the system with the Administration Server.
3. Change the directory to *domain_home***/services-gatekeeper-domain/bin**.
4. Execute the **startNodeManager** script with this syntax:
   - Solaris/Linux:

     ```
     startNodeManager.sh
     ```

   - Windows:

     ```
     startNodeManager.cmd
     ```

5. Follow the instructions in "Adding a Managed Server to Create a Clustered Services Gatekeeper Implementation" to add a second system with a managed server.
6. Log on to the system with just the managed server.
7. Change the directory to *domain_home***/bin**.
8. Run this script to start Node Manager:
   - Solaris/Linux:

     ```
     startNodeManager.sh
     ```

   - Windows:

     ```
     startNodeManager.cmd
     ```

9. Log on to the system running the Administration Server.

Both systems in your cluster are now configured to run Node Manager, and the Node Manager processes have started.

Start the Tools to Manage Your APIs

Now that Services Gatekeeper is installed and started, you can start using the PRM portals to administer your APIs, partners, and network services. Open a web browser

on your running Services Gatekeeper system and use this URI to start the default API and Partner Portal GUI:

```
http://IP_addr:8001/portal/partner-manager/index/login.html
```

Where *IP_addr* is the IP address of the system you installed Services Gatekeeper on.

You are prompted for the administrative user name (domain user name) and password that you entered during installation.

See these documents for details and instructions on API management:

- *Services Gatekeeper API Management Guide*
- Services Gatekeeper API and Partner Manager Portal Online Help
- Services Gatekeeper Partner Portal Online Help
- Services Gatekeeper Network Service Supplier Portal Online Help

Integrating Services Gatekeeper With Network Services

Your Services Gatekeeper implementation may require a connection to network nodes that your applications require, such as Diameter servers for payment, or SMSCs for managing short messages. For details on making these connections, see *Services Gatekeeper Integration Guide*.

You can also use any of the default Services Gatekeeper prepackaged communication services in your APIs and applications. See "Adding Communication Services to Services Gatekeeper" for details on how make a communication service available to use.

Administering and Securing Services Gatekeeper

Your Services Gatekeeper implementation requires security, maintenance, and tuning to work correctly. For details on these tasks, see *Services Gatekeeper System Administrator's Guide*.

Also, you may have noticed this message when you started Services Gatekeeper:

```
Demo trusted CA certificate is being used in production mode
The system is vulnerable to security attacks since it trusts certificates signed
by the demo trusted CA
```

You can safely ignore this message for test and evaluation implementations. However, if you are creating a production implementation, you should read through these sections and books for information on securing your implementation, including replacing the key and truststores that secure your resources:

- "Securing Network-facing Servers with Keystores" in *Services Gatekeeper System Administrator's Guide*
- *Services Gatekeeper Security Guide*
- "Securing Services Gatekeeper" in the *Services Gatekeeper System Administrator's Guide*

Adding Support for Reporting

Both the Services Gatekeeper single-tier and multi-tier products support reporting through the Oracle Business Intelligence (OBI) product. See "Installing Oracle Business

Intelligence" in *Services Gatekeeper Multi-tier Installation Guide* for information on installing OBI, and "Managing Application and API Usage with Report Statistics" in *Services Gatekeeper API Management Guide* for information on running reports.

Uninstalling Services Gatekeeper

This section explains how to remove a Services Gatekeeper implementation by using the **deinstall.sh** script.

To remove Services Gatekeeper:

1. If your Services Gatekeeper servers are running, stop them.
2. In a command-line tool, change the directory to the *Middleware_home***/Oracle_home/oui/bin** directory
3. Run the deinstallation script with this syntax:

   ```
   ./deinstall.sh
   ```

   The Oracle Fusion Middleware 12c Deinstall GUI appears.
4. Click **Next**.

   The Deinstallation Summary screen appears.
5. Confirm that it is deinstalling the correct software and click **Deinstall**.

   The Deinstallation Progress screen appears.
6. Wait for the green checkmarks to appear.

   There are **View Messages** and **View Logs** buttons that you can use to view status during or after the installation
7. Click **Finish**.
8. Repeat steps 1 through 7 on each system with Services Gatekeeper components you want to remove.

2

Adding Communication Services to Services Gatekeeper

This chapter explains how to add a Oracle Communications Services Gatekeeper communication service to a single-tier Services Gatekeeper implementation.

About Adding a Communication Service to a Single-Tier Services Gatekeeper

Services Gatekeeper includes a rich set of communication services that you, your partners, or network service suppliers can use when creating APIs. See *Communication Service Reference Guide* for the complete list of communication services. You can add communication services to Services Gatekeeper before or after installation. After it is installed, you then need to make the communication services available to Services Gatekeeper, and configure their attributes as needed.

Adding a Communication Service to a Single-Tier Services Gatekeeper

The process of adding a communication service to a single-tier Services Gatekeeper implementation includes these steps:

- Adding Communication Services During Installation, or Adding Communication Services After Installation
- Configuring a Communication Service for Use with Services Gatekeeper

Adding Communication Services During Installation

The easiest way to make a communication service available to use with your APIs is to perform a custom installation of Services Gatekeeper. The **Installation Type** screen of the installation GUI (step 10 of "Installing Services Gatekeeper") asks if you want to perform a default or custom installation. If you select **Custom Installation**, you are then offered a list of the communication services to install. You can choose to select all of them.

If, however, you have already installed Services Gatekeeper, you can do another custom installation on the same system, selecting the communication services to add.

Adding Communication Services After Installation

You can add a communication service to an existing Services Gatekeeper implementation by installing the Services Gatekeeper again using a custom installation, and selecting the communication services you need. In step 10 of

"Installing Services Gatekeeper" select **Custom Installation**. In the next step, you are then offered a list of the communication services to install. In step 15, ensure that you do not install another database.

Configuring a Communication Service for Use with Services Gatekeeper

After it is installed, you need to make the communication services available to Services Gatekeeper and then configure them. You use the WebLogic Administration Console for both of these tasks. See "Starting and Using the Administration Console" in *Services Gatekeeper System Administrator's Guide* for details on using the Administration Console.

This section explains the general steps you need to take to make communication services available and to configure them. The relevant documents are listed that have more complete information.

You first need some information about the communication services. Individual communication services are documented in *Communication Service Reference Guide*, including the names of the two EAR files. Each communication service chapter lists the attributes you need to configure, and operations that are available to you for a communication service.

To make a communication service available, you need to "install" it by referencing the EAR files in the Administration Console. In the Administration Console, go to **Deployments**, and then select **lib**. The Install Applications Assistant window appears. You need to enter the communication service EAR file in the **Path** field, and then select **Next**. The Assistant walks you through the process of installing the communication service.

After a communication service is available to Services Gatekeeper, you can navigate to its configuration settings and make any changes your implementation requires. See "Starting and Using the Administration Console" in *Services Gatekeeper System Administrator's Guide* for details on using the Administration Console. Your changes automatically take effect.

See these documents for more detailed information:

- "Deploying and Administering Communication Services" in *Services Gatekeeper System Administrator's Guide*.
- "About Communication Services" in *Services Gatekeeper Communication Service Reference Guide*.
- "Understanding Communication Services" in *Services Gatekeeper Extension Developer's Guide*.