

Oracle® Web Services Manager

Quick Start Guide

10g (10.1.3.1.0)

B32126-01

September 2006

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

Preface	v
Audience	v
Documentation Accessibility	v
Related Documents	vi
Conventions	vi
 1 Installing Oracle Web Services Manager	
Before You Begin	1-1
Starting the Oracle Universal Installer	1-1
Starting the Oracle Universal Installer on Windows	1-1
Starting the Oracle Universal Installer on Linux	1-2
Installation Steps	1-2
What Do I Do Next?	1-5
 2 Using Oracle Web Services Manager to Secure Your Web Services	
Before You Begin	2-1
Log In to Web Services Manager Control	2-1
Register Your Gateway	2-4
Register a Web Service to Your Gateway	2-6
Add Policies to the Gateway	2-12
Create the Authentication File	2-18
View Your WSDL	2-20
Test Your WSDL	2-22
Test the File Authentication Policy Step	2-24
Adding the Authorization Policy Step	2-25
Edit the Authorization File	2-27
Execute the Test Page Again	2-28
Test the File Authorization Policy Step	2-29
Summary	2-30
 3 Monitoring Your Oracle Web Services Manager Environment	
Before You Begin	3-1
Generating Oracle Web Services Manager Metrics	3-2
Reusing Your Tests	3-3
Monitoring Oracle Web Services Manager	3-3

View the Overall Statistics	3-4
View the Security Statistics	3-5
Latency Variance	3-6
Traffic Analysis.....	3-7
Service-Level Agreements (SLA)	3-8
Execution Details.....	3-9
Debugging Oracle Web Services Manager	3-10
Congratulations!	3-11

Preface

This preface provides information on the following topics:

- [Audience](#)
- [Documentation Accessibility](#)
- [Related Documents](#)
- [Conventions](#)

Audience

This document is intended for users who are new to Oracle Web Services Manager who want to come up to speed quickly and learn the basic features of the product.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

<http://www.oracle.com/accessibility/>

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, see the following documents in the Oracle Web Services Manager10g (10.1.3.1.0) documentation set:

- *Oracle Web Services Manager Extensibility Guide*
- *Oracle Web Services Manager Administrator's Guide*
- *Oracle Web Services Manager Deployment Guide*
- *Oracle Web Services Manager Installation Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

File Path Locations

When describing the location of files in this book, the UNIX convention of using a forward slash (/) to denote directories, is used. For example:

`ORACLE_HOME/owsm/config/gateway/gateway-config-installer.properties` file

If you are using Oracle Web Services Manager on a Windows operating system, replace the forward slashes with back slashes (\). For example:

`ORACLE_HOME\owsm\config\gateway\gateway-config-installer.properties` file

Installing Oracle Web Services Manager

The *Oracle Web Services Manager Quick Start Guide* can be used with Oracle Web Services Manager either as a standalone installation or as part of a basic installation of Oracle Application Server 10g Release 3 (10.1.3.1.0).

This chapter provides basic installation procedures for installing Oracle Web Services Manager as part of a basic installation of Oracle Application Server 10g Release 3 (10.1.3.1.0). If you are installing Oracle Web Services Manager as a standalone product, refer to *Oracle Web Services Manager Installation Guide* for installation instructions.

Before You Begin

Before you begin installing Oracle Web Services Manager, ensure that you have read both Chapter 2, "Requirements" and Chapter 3, "Things You Should Know Before Starting the Installation" in the installation guide for your platform (*Oracle Application Server Installation Guide for Microsoft Windows* or *Oracle Application Server Installation Guide for Linux x86*). These chapters contain important information with which you must be familiar before you begin the installation so you can avoid potential problems during the installation.

Starting the Oracle Universal Installer

Follow the instructions for starting the Oracle Universal Installer for your platform.

Starting the Oracle Universal Installer on Windows

1. Log in to the computer as a user who is a member of the Windows Administrators group.
2. Insert the disk.
 - CD-ROM users: Insert Oracle Application Server Disk 1 into the CD-ROM drive.
 - DVD-ROM users: Insert Oracle Application Server DVD-ROM into the DVD-ROM drive.
3. If your computer supports the auto-run feature the installer launches automatically.

If your computer does not support the auto run features, you have to start up the installer manually:

- CD-ROM users: Double-click setup.exe.
- DVD-ROM users: Double-click setup.exe in the *application_server* directory.

This launches Oracle Universal Installer, through which you install Oracle Application Server.

Starting the Oracle Universal Installer on Linux

1. If your computer does not mount CD-ROMs or DVDs automatically, you need to set the mount point manually. See "Setting the Mount Point for the CD-ROM or DVD-ROM" in *Oracle Application Server Installation Guide for Linux x86* for details.
2. Log in as the `oracle` user.
3. CD-ROM users: Insert Oracle Application Server Disk 1 into the CD-ROM drive.
DVD-ROM users: Insert the Oracle Application Server DVD-ROM into the DVD-ROM drive.
4. Run the Oracle Universal Installer using the command shown after the notes:

Notes:

- Be sure you are not logged in as the root user when you start the Oracle Universal Installer. The installer gives an error message if you try to run it as the root user.
 - Do not start the installation inside the `mount_point` directory. If you do, then you may not be able to eject the installation disk. The `cd` command below changes your current directory to your home directory.
-
-

CD-ROM:

```
prompt> cd
prompt> mount_point/10.1.3disk1/runInstaller
```

DVD-ROM:

```
prompt> cd
prompt> mount_point/application_server/runInstaller
```

This launches Oracle Universal Installer, through which you install Oracle Application Server.

Installation Steps

To install Oracle Web Services Manager as part of the Oracle Application Server installation, perform the following steps:

1. Start Oracle Universal Installer.
For more information, refer to ["Starting the Oracle Universal Installer"](#) on page 1-1.
2. Oracle Application Server SOA Suite 10.1.3.1.0 Installation Screen ([Figure 1-1.](#))
Installation Directory: Enter the directory where you want install Oracle Application Server.
Select **Basic Installation Mode**.

AS Instance Name: The instance name identifies this Oracle Application Server instance. If you have more than one Oracle Application Server instance on the same host, the instances must have unique names.

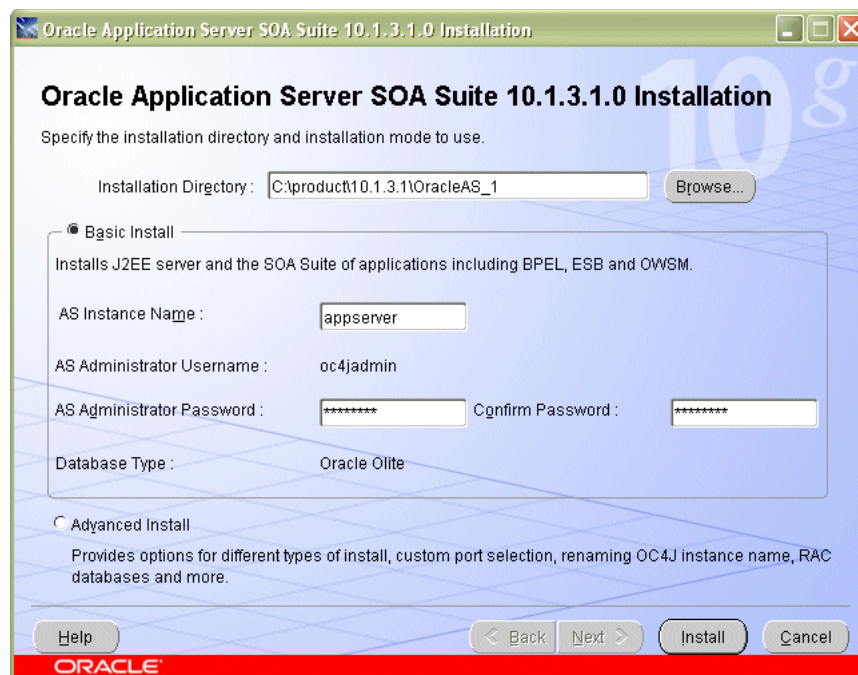
AS Administration Username: The administration username for Oracle Application Server instances is set to `oc4jadmin` and cannot be changed. To manage Oracle Application Server instances using Oracle Enterprise Manager 10g, log in as the `oc4jadmin` user.

AS Administration Password and Confirm Password: Enter the password for the `oc4jadmin` user.

Database Type: An Oracle Olite Database is installed with the basic installation. If you want to use another Oracle database, you must perform an advanced installation.

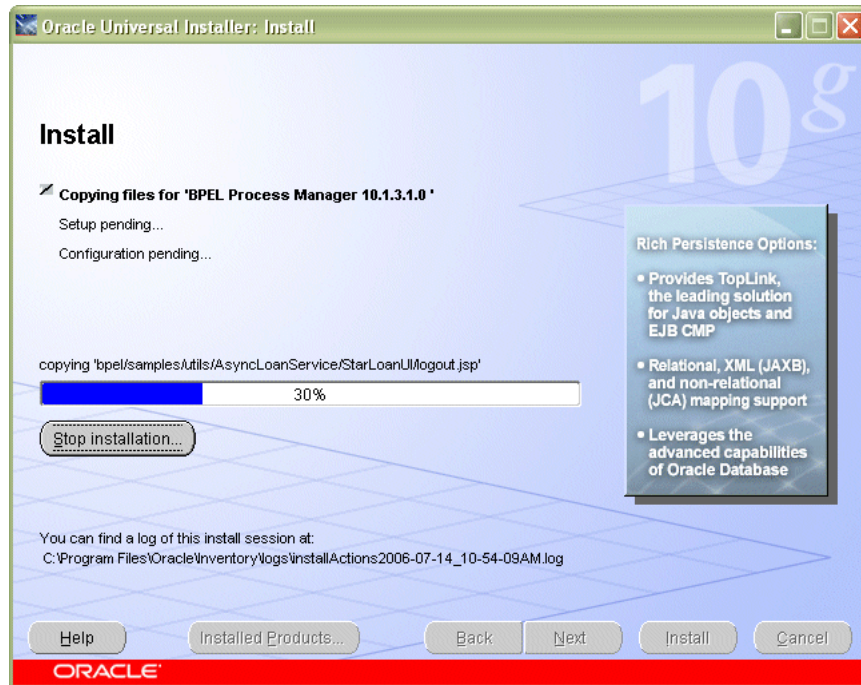
Click **Install**.

Figure 1–1 Oracle Application Server SOA Suite 10.1.3.1.0 Installation Screen



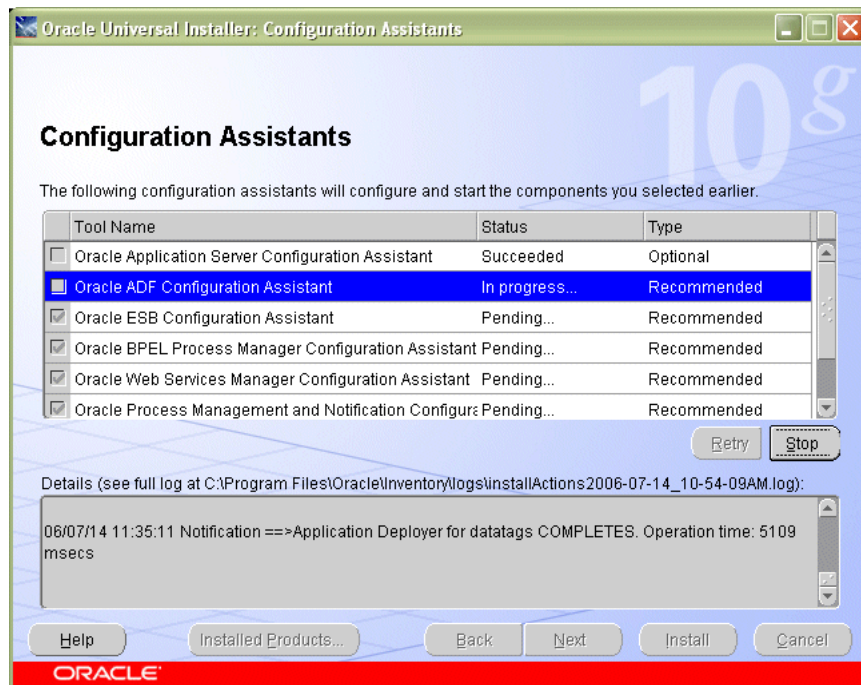
3. Oracle Universal Installer: Install Screen (Figure 1–2).

This screen shows the progress of installation.

Figure 1–2 Oracle Universal Installer: Install Screen

4. Oracle Universal Installer: Configuration Assistants Screen (Figure 1–3).

This screen shows the progress of the configuration assistants.

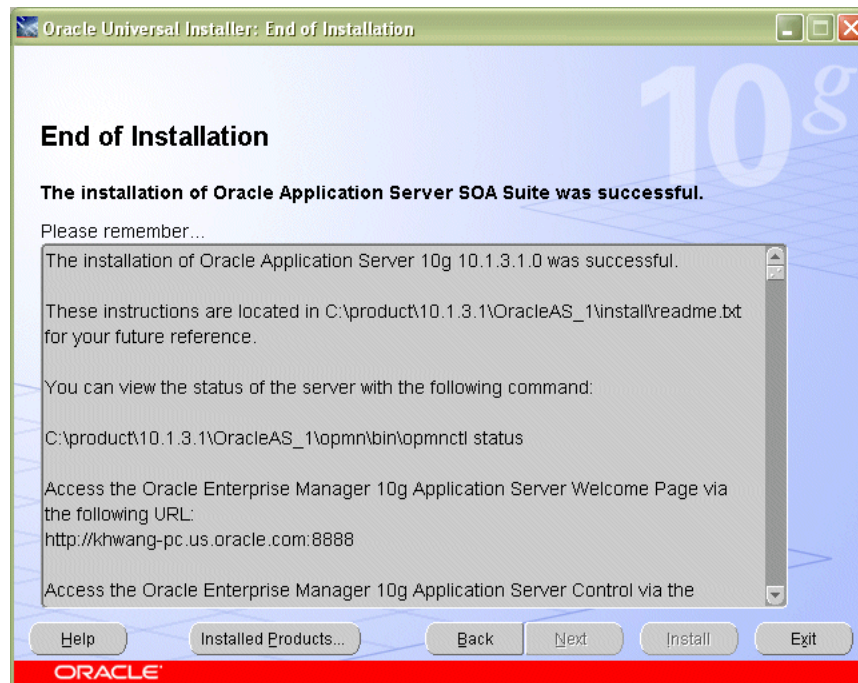
Figure 1–3 Oracle Universal Installer: Configuration Assistants Screen

5. Oracle Universal Installer: End of Installation Screen (Figure 1–4).

This screen tells you whether or not your installation was successful, and provides links to various documentation, such as the product release notes and installation

log, as well as links to various Oracle Application Server pages such as the Welcome Page or Application Server Control Console.

Figure 1–4 Oracle Universal Installer: End of Installation Screen



What Do I Do Next?

Now that you have successfully installed Oracle Web Services Manager, continue with [Chapter 2, "Using Oracle Web Services Manager to Secure Your Web Services"](#).

Using Oracle Web Services Manager to Secure Your Web Services

In this tutorial, you will perform the following tasks:

1. Log in to Web Services Manager Control
2. Register a gateway.
3. Register a Web service to the gateway.
4. Add policies to the gateway that will authenticate users.
5. Create the file used to authenticate users.
6. View the WSDL for the Web service.
7. Test whether the policy step is authenticating users.
8. Add an authorization policy that verifies users' access.
9. Edit the sample authorization file.
10. Test whether the policy step is authorizing users.

Before You Begin

Make a backup copy of the Oracle Web Services Manager Database before you begin this tutorial. The database file (orawsm.odb) is located in the following directory:

`$ORACLE_HOME/10.1.3.1/owsm/Mobile/Sdk/OLDB40`

The instructions in this tutorial assume that you are starting with a new installation of Oracle Web Services Manager. If you run into an error or you want to start the tutorial again, copy the backup copy of the database file into the directory shown above.

Log In to Web Services Manager Control

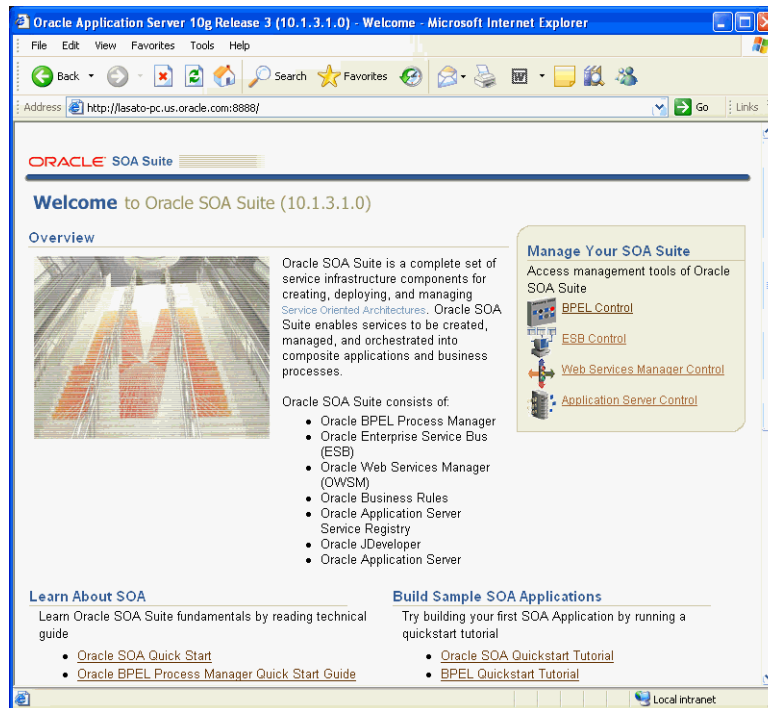
1. Open a Web browser, and enter the following URL:

`http://fully_qualified_host_name:http_port`

Note: If you are logging in to a standalone version of Oracle Web Services Manager, skip to step 3 now.

The Welcome to Oracle SOA Suite (10.1.3.1.0) page appears ([Figure 2-1](#)).

Figure 2–1 Welcome to Oracle SOA Suite (10.1.3.1.0) Page



2. In the Manage Your SOA Suite box, click the **Web Services Manager Control** link.
3. In the Log In page, log in as **oc4jadmin** and use the password you supplied during the installation. Click **Login**. (Figure 2–2)

Note: If you are logging in to a standalone version of Oracle WSM, the log in page looks slightly different. Log in as the Oracle Web Services Manager Administrator. By default the user name is *admin* and the password is *oracle*.

Figure 2–2 Log In Page

The screenshot shows a Microsoft Internet Explorer window titled "Java SSO Login - Microsoft Internet Explorer". The address bar displays the URL: `http://lasato-pc.us.oracle.com:8888/jso/SSOLogin?appurl=http%3A%2F%2Flasato-pc.us.oracle.com%3A8888%2Fccor`. The main content area contains the text "Enter your single sign-on username and password." Below this, there are two input fields: "Username:" with the value "oc4jadmin" and "Password:" with masked characters "*****". At the bottom of the form are two buttons: "Login" and "Cancel".

The next page you see is the Web Services Manager Control page (Figure 2–3).

Figure 2–3 Web Services Manager Control Page

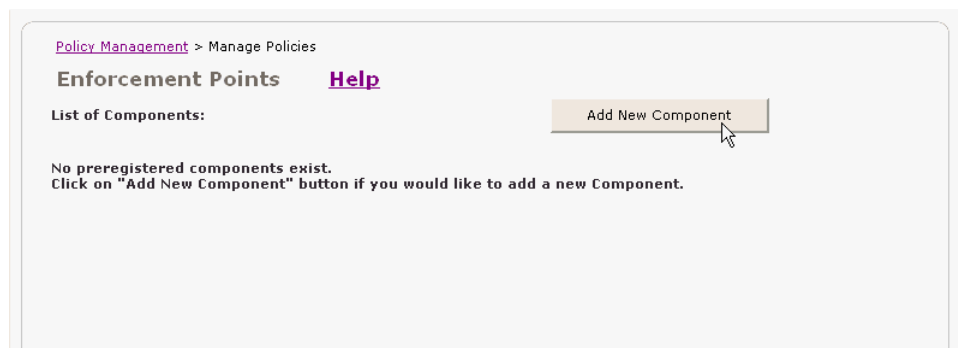
The screenshot shows a Microsoft Internet Explorer window titled "Oracle Web Services Manager - Microsoft Internet Explorer". The address bar displays the URL: `http://lasato-pc.us.oracle.com:8888/core/index.jsp`. The page header includes the Oracle logo and "Enterprise Manager 10g Web Services Manager Control". In the top right corner, there is a "logout oc4jadmin" link. The left sidebar contains a navigation menu with the following items: "Policy Management", "Operational Management", "Tools", and "Administration". The main content area is titled "Policy Management > Manage Policies" and features a section for "Enforcement Points" with a "Help" link. Below this, there is a "List of Components:" section with an "Add New Component" button. A message states: "No preregistered components exist. Click on 'Add New Component' button if you would like to add a new Component." The status bar at the bottom shows "Done" and "Local intranet".

Register Your Gateway

In Oracle Web Services Manager, you can create gateway components, server agent components, and client agent components to protect your Web services. In this quick start tutorial, you will be creating and registering an Oracle WSM Gateway.

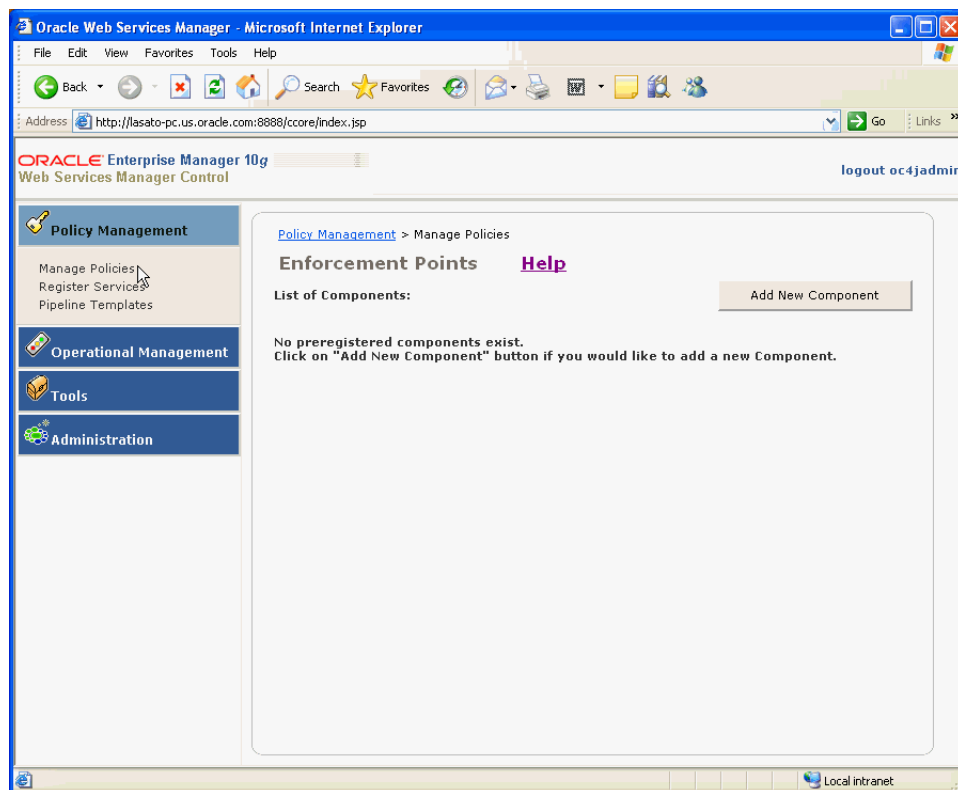
1. Click **Add New Component** (Figure 2–4).

Figure 2–4 Adding a New Component



Note: If you do not see the Add New Component button, click **Policy Management**, then click **Manage Policies** from the navigation pane on the left side to return to the correct page (Figure 2–5).

Figure 2–5 Navigating to the Manage Policies Page



2. In the Add New Component page, enter the following:

- **Component Name** – Enter: MyGateway
- **Component Type** – Accept the default value: Gateway
- **Container Type** – Accept the default value: Oracle Web Services Manager
- **Component URL** – Enter the following: `http://fully_qualified_host_name:http_port/gateway`

where *fully_qualified_host_name* is the URL for Oracle Web Services Manager, and *http_port* is the port on which Oracle Web Services Manager is hosted.

Tip: Check the URL in your browser that you use to access the Web Services Manager Control. Replace "ccore" with "gateway." For example, change the URL:

`http://marcc-pc.us.oracle.com:8888/ccore`

to the following URL:

`http://marcc-pc.us.oracle.com:8888/gateway`

Enter this URL in the **Component URL** field.

- **Component Groups** – Accept the default values for the component groups.

See [Figure 2–6](#) for an example of the Add New Component page.

Figure 2–6 Add New Component Page

Policy Management > Manage Policies > Add New Component

Enforcement Points [Help](#)

Add New Component:

Basic Parameters

Component Name (*): MyGateway

Component Type (*): Gateway

Container Type (*): Oracle Web Services Manager

Component URL (*): http://lasato-pc.us.oracle.com:8888/gateway

Component Groups:

Modify privileges

su1-grp
da1-grp

Add Groups with Modify privileges

ca1-grp
ca2-grp

<< Add

View privileges

Add Groups with View privileges

cs1-grp
cs2-grp

Remove >>

Register Cancel

3. Click **Register**.

The following message confirms that you have successfully registered the gateway ([Figure 2–7](#)).

Figure 2–7 Message Confirming Successful Component Registration

4. Click **Ok**.

The gateway now appears in the List of Components ([Figure 2–8](#)).

Figure 2–8 Gateway Component in the List of Components Page

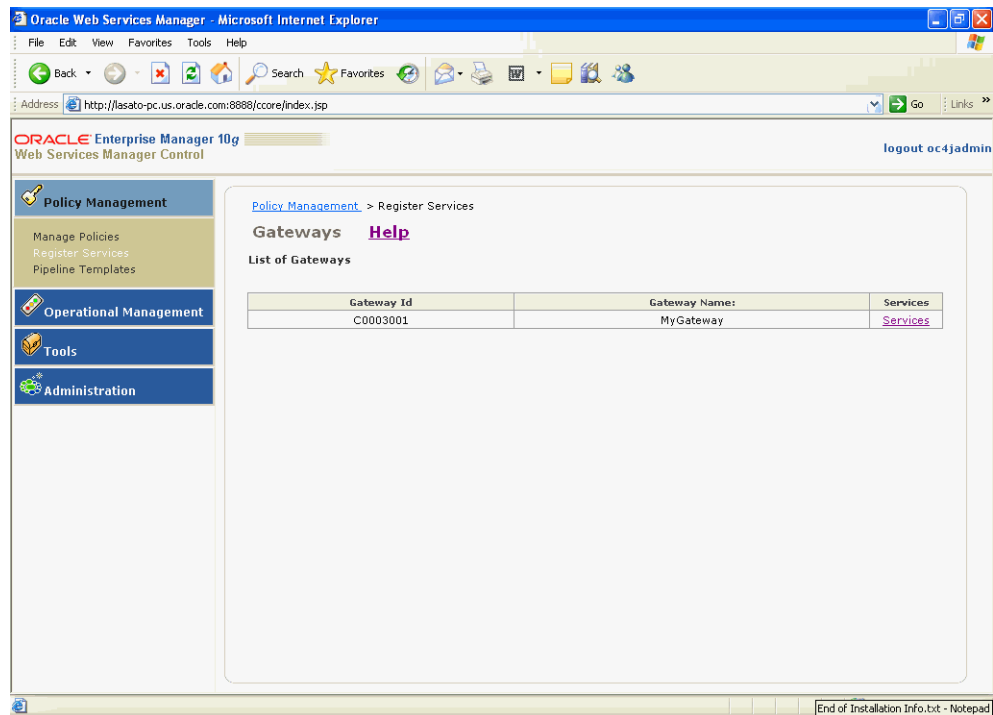
Register a Web Service to Your Gateway

In this tutorial, you will register the Time Service Web service to the gateway that you just created. (There is more information about Time Service at the end of this procedure.) By doing so, you are associating the gateway with the Web service that it will protect.

1. From the navigation pane of Web Services Manager Control, click **Policy Management**, then click **Register Services** ([Figure 2–9](#)).

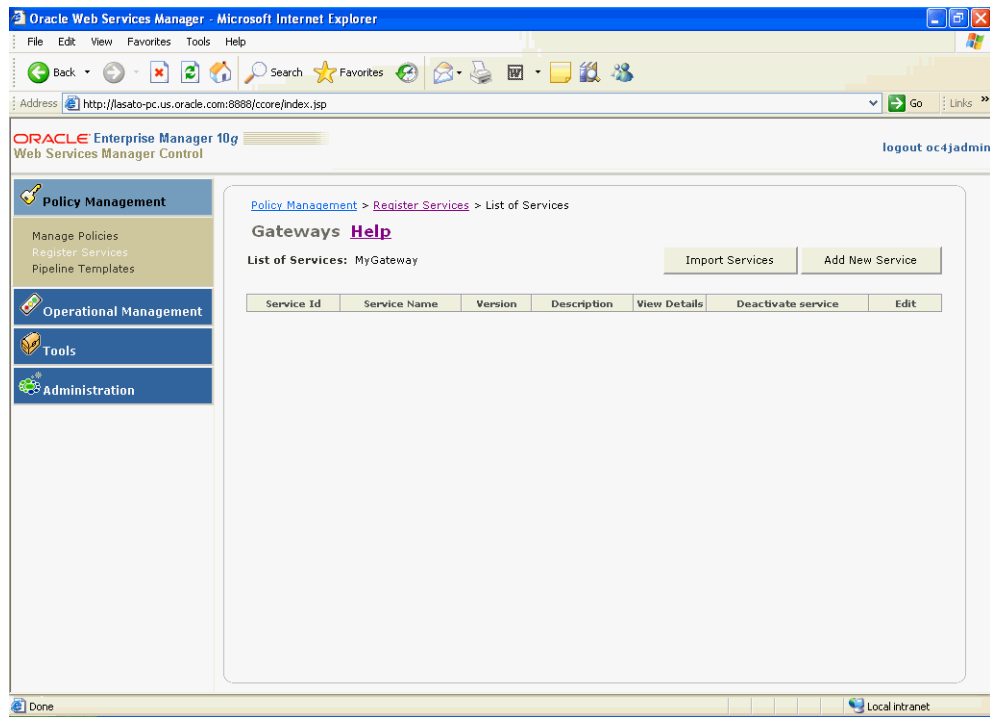
Figure 2–9 Web Service Manager Control Navigation Pane

In the List of Gateways page (Figure 2–10), you see the gateway you just created. The Gateway Name is the name you assigned the gateway when you registered it, and the Gateway Id is the component Id that Oracle Web Services Manager assigned to the gateway.

Figure 2–10 MyGateway in the List of Gateways Page

2. Click the **Services** link.
3. Click **Add New Service**.

Note, in the List of Services page, there are currently no services registered to this gateway (Figure 2–11).

Figure 2–11 List of Services Page for MyGateway

4. Click **Add New Service**.

5. In the Add New Service page, enter the following service details:

- Service Name – TimeService
Note: There is no space between *Time* and *Service*. This will be explained later.
- Service Version – 1.0
- Service Description – Gives the time of day.
- WSDL URL – `http://fully_qualified_host_name:http_port/ccore/TimeService.wsdl`
where *fully_qualified_host_name* is the URL for Oracle Web Services Manager, and *http_port* is the port on which Oracle Web Services Manager is hosted.

Note: It is important that the URL and the port you assign here match the URL and port you specified when you registered your gateway.

- Service Protocol – Accept the default, HTTP(S).
- Service Groups – Accept the defaults.

Figure 2–12 is an example of the Add New Service page with the service details entered.

Figure 2–12 Add New Service Page

> [Register Services](#) > [List of Services](#) > Add New Service

Help

MyGateway Step 1 of 2

Service Details	
Service Name (*):	TimeService
Service Version (*):	1.0
Service Description:	Gives the time of day
WSDL URL:	http://lasato-pc.us.oracle.com:8888/core/TimeSer
Service Protocol(*):	<input checked="" type="radio"/> HTTP(S) <input type="radio"/> JMS(SSL) <input type="radio"/> IBM MQSeries <input type="radio"/> HTTP Post <input type="radio"/> Custom
Custom Protocol Step Template Id:	

Service Groups:

Modify privileges

su1-grp
da1-grp

View privileges

Modify privileges

sa1-grp
sa2-grp

Add Groups with View privileges

ss1-grp
ss2-grp

<< Add
Remove >>

6. Click Next.

The Configure Messenger Step for New Service page is displayed. On the previous page you accepted the default service protocol, HTTP(S). This page (Figure 2–13) displays the parameters for configuring the HTTP(S) protocol.

Figure 2–13 Configure HTTP Messenger Step for New Service Page

[Policy Management](#) > [Register Services](#) > [List of Services](#) > Add New Service

Gateways **Help**

Configure Messenger Step for New Service Step 2 of 2

Service Protocol: HTTP(S)

HTTP Messenger		Environment Properties	
Basic Properties	Type	Default	Value
Enabled	boolean	true	<input checked="" type="radio"/> true <input type="radio"/> false
Messenger Properties			
URL (*)	string		http://lasato-pc.us.oracle.com:8888
ReplyTimeout	int	30000	30000
IsSoapService (*)	boolean	true	<input checked="" type="radio"/> true <input type="radio"/> false
ForwardCredentials (*)	boolean	false	<input type="radio"/> true <input checked="" type="radio"/> false
FailoverURLs	string[]		<div style="border: 1px solid black; height: 20px; width: 100%;"></div>
Attempts	int	5	5
RetryInterval	int	10	10
KeepAlive (*)	boolean	false	<input type="radio"/> true <input checked="" type="radio"/> false

↓

7. In the Configure Messenger Step for New Service page, verify that the URL matches the URL you provided on the previous page. Accept the default values for the remaining fields, and click **Finish.**

The following message appears (Figure 2–14).

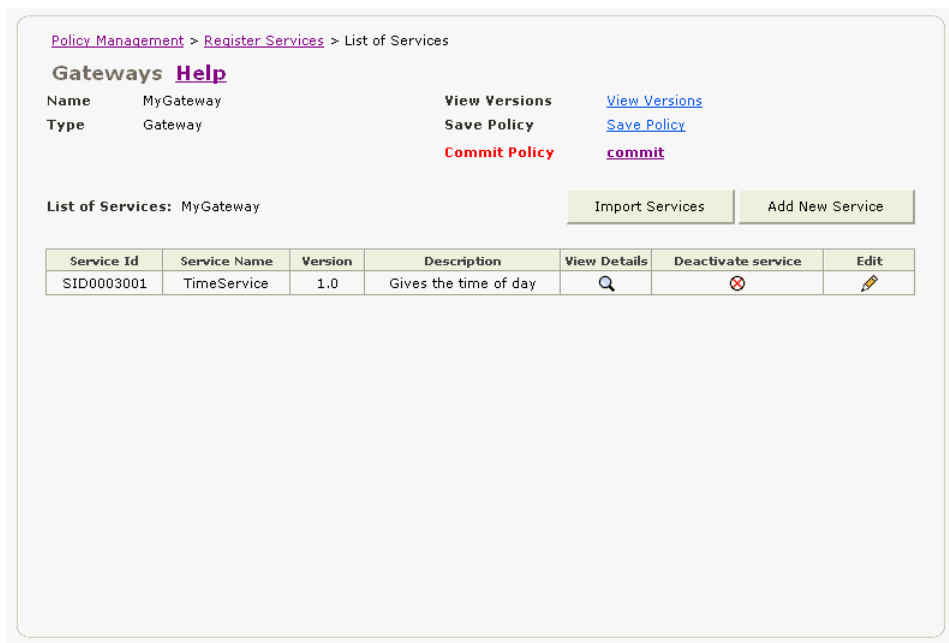
Figure 2–14 Message Confirming Successful Service Registration



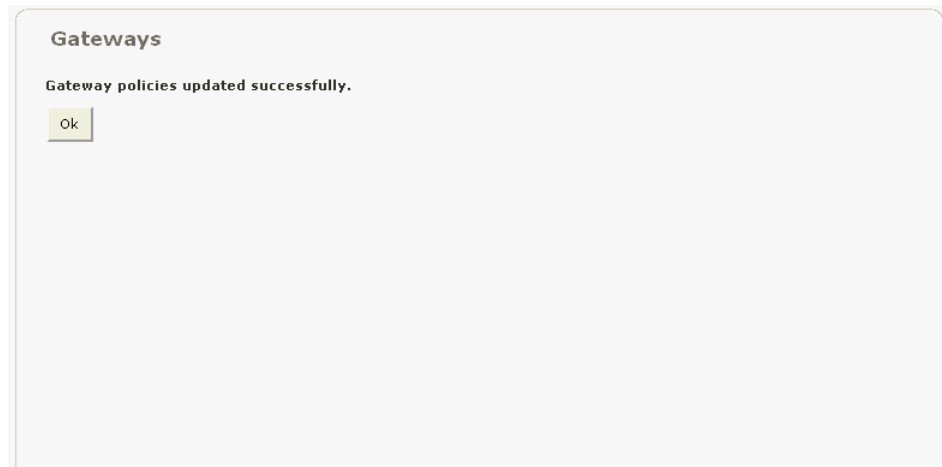
8. Click **Ok**.

Now, the new service appears in the List of Services (Figure 2–15). The Service Name, Version, and Description are what you entered when you registered the service. The Service Id is the Id that Oracle Web Services Manager assigned to the service.

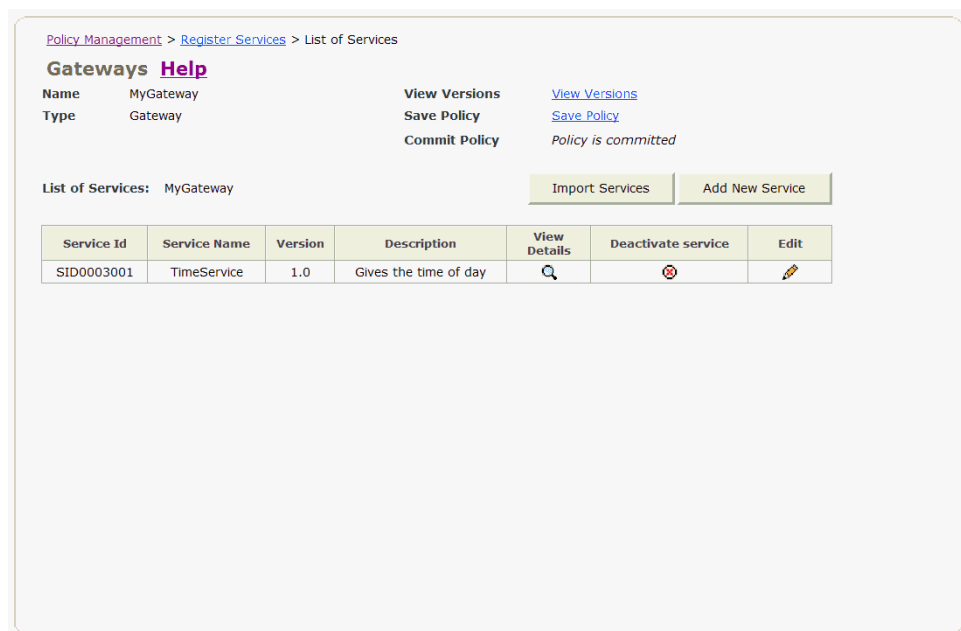
Figure 2–15 List of Services Page with TimeService Added



9. Note the Commit Policy field appears in red. This is to alert you to the fact that you need to click the commit link to commit the change to the Oracle WSM Database. Click **commit**.
10. The following confirmation appears (Figure 2–16). Click **Ok**.

Figure 2–16 Message Confirming Policies Successfully Updated

11. You return to the List of Services page (Figure 2–17). Note, this time, in the Commit Policy field, it says: Policy is committed.

Figure 2–17 List of Services Page Showing the Policy is Committed

About the Time Service Web Service

Oracle WSM ships with a Time Service Web service that returns the current time. Time Service is not an actual Web service in the sense that it is not deployed to the Oracle Application Server. (Time Service is a simple JSP.) Therefore, Time Service can only be used with a gateway and not with an agent. The Time Service WSDL file is located at the following location:

`ORACLE_HOME/j2ee/home/applications/ccore/ccore/TimeService.wsdl`

You can access the Time Service WSDL file in your browser directly, without going through the gateway using the following URL:

`http://fully_qualified_host_name:http_port/ccore/TimeService.wsdl`

Add Policies to the Gateway

Now that you have associated a Web service with your gateway, you will add policies that will be used by the gateway to protect the service. Generally, the Web service client submits a request by sending an XML message that includes user credentials. Because we are using a gateway rather than an agent in this tutorial, the request is made directly to the gateway. In other words, the gateway virtualizes the protected Web service.

In this tutorial, you will be using two policy steps to secure this service. The first policy step, Extract Credentials, will isolate the user name and password credentials from the request. The second step, File Authenticate, will authenticate the user using a file that contains valid users and their passwords.

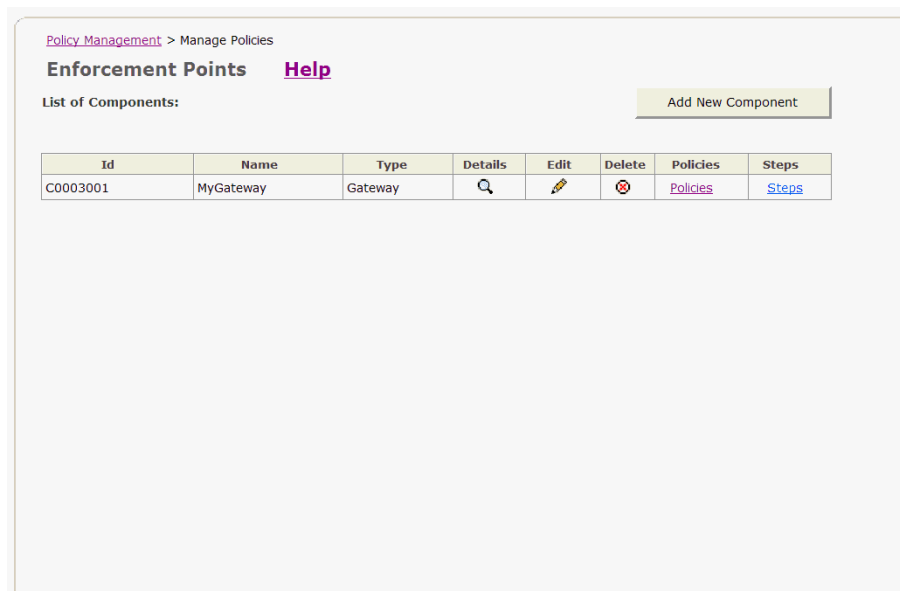
Later in this tutorial, you will add a third policy step, File Authorize, that will authorize the user by checking a file to see if the user belongs to a role that is granted access to the service.

To add the Extract Credentials policy step

This policy step extracts user credentials from the Web service request.

1. From the navigation pane of the Web Services Manager Control, click **Policy Management**, then click **Manage Policies**.
2. In the List of Components, click the **Policies** link for your gateway (Figure 2–18).

Figure 2–18 Gateway Component in the List of Components Page



The policies for the MyGateway component are displayed (Figure 2–19). By default, Oracle WSM creates a policy with same name as the name of the service, in this example, TimeService. Note that the version number is included in parentheses.

Figure 2–19 Policies for the MyGateway Gateway

[Policy Management](#) > [Manage Policies](#) > Policies

Enforcement Points [Help](#)

Name : MyGateway View Versions [Version](#)
 Type : Gateway Save Policy [Save](#)
 Commit Policy *Policy is committed*

Policy Set for Component: "C0003001"

To add a new policy to a Gateway, select Policy Management / Register Service.
 Click on the Services link and press either "Import Services" or "Add new service" button to add a service to Gateway.

Policy Name	View Details	Edit
TimeService(1.0)		

URL Pattern	Policy Name
SID0003001	TimeService(1.0)
TimeService	TimeService(1.0)

3. Click the **Edit** icon.

You see the Policy Definition page for the TimeService(1.0) policy ([Figure 2–20](#)). There are four pipelines or parts to the policy definition:

- ¹PreRequest Pipeline – The policy steps in this pipeline are executed before the Web service request is processed.
- Request Pipeline – The policy steps in this pipeline are executed on the Web service request.
- Response Pipeline – The policy steps in this pipeline are executed on the response from the Web service
- ¹PostResponse Pipeline – The policy steps in this pipeline are executed after the response from the Web service is sent to the client requestor

Note: The screen shot of the page is truncated. You can scroll down the page to see all four pipelines.

For this tutorial, we will be adding policies to the Request pipeline. Note, by default, a Log policy step has been added to the Request and Response pipelines.

¹ The PreRequest and PostRequest Pipelines will not be supported in future releases of Oracle Web Services Manager.

Figure 2–20 Policy Definition Page for the TimeService (1.0) Policy

Policy Management > Manage Policies > Policies > Policy

Enforcement Help
Points

Component: "MyGateway"

Policy Definition: "TimeService(1.0)"

Pipeline: "PreRequest" [Replace Pipeline](#)

Pipeline Steps:

Start Pipeline

↓

End Pipeline

Pipeline: "Request" [Replace Pipeline](#)

Pipeline Steps:

Start Pipeline [Add Step Below](#)

↓

Log [Configure](#) [Add Step Below](#) [Delete](#)

↓

End Pipeline

Pipeline: "Response" [Replace Pipeline](#)

4. We are going to add a policy step below the Log step in the Request pipeline. In the row for the Log step, click the **Add Step Below** link (Figure 2–21).

Figure 2–21 Adding a Policy Step

Policy Management > Manage Policies > Policies > Policy

Enforcement Help
Points

Component: "MyGateway"

Policy Definition: "TimeService(1.0)"

Pipeline: "PreRequest" [Replace Pipeline](#)

Pipeline Steps:

Start Pipeline

↓

End Pipeline

Pipeline: "Request" [Replace Pipeline](#)

Pipeline Steps:

Start Pipeline [Add Step Below](#)

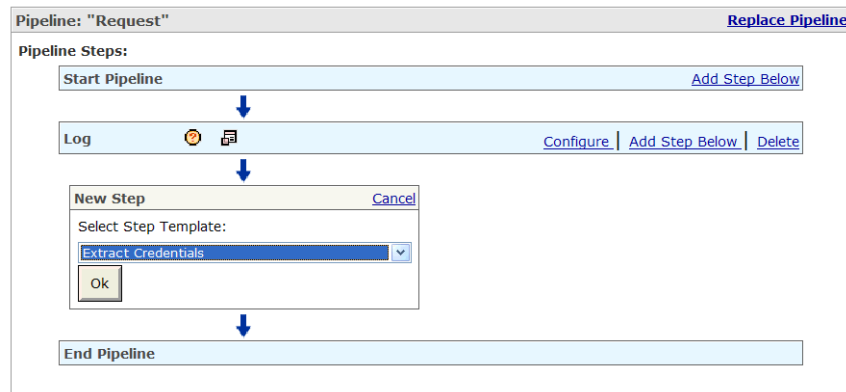
↓

Log [Configure](#) [Add Step Below](#) [Delete](#)

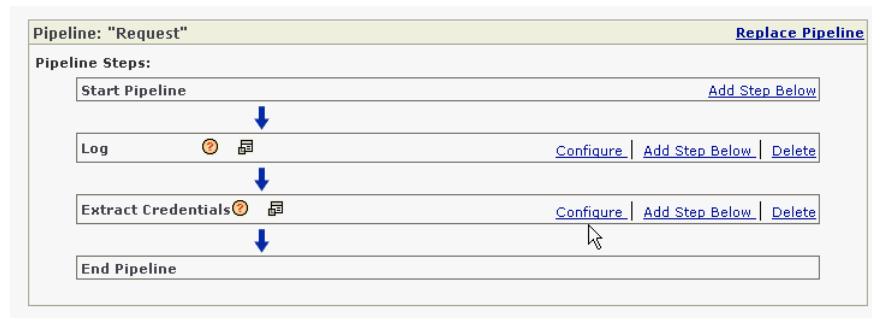
↓

End Pipeline

5. The page refreshes and the New Step box appears. From the Select Step Template list, click the arrow to display a list of policy steps, and select Extract Credentials from the list, and click **Ok** (Figure 2–22).

Figure 2–22 Selecting the Extract Credentials Policy Step

6. The Extract Credentials policy step has been added below the Log step. Now, we are going to configure the Extract Credentials step. In the Extract Credentials row, click the **Configure** link (Figure 2–23).

Figure 2–23 Clicking Configure for the Extract Credentials Policy Step

The properties for the Extract Credentials policy step are displayed.

7. In this tutorial, we will simulate extracting the user's credentials from the standard Username Token as specified in the WS-I Basic Security Profile, and authenticate the user against a file of valid users.

In the Configure pipeline step page, change the default value for the Credentials location to WS-BASIC as shown in Figure 2–24.

Figure 2–24 Extract Credentials Policy Step Properties

Policy Management > Manage Policies > Policies > Policy

Configure Step [Help](#)

Pipeline: "Request"

Configure pipeline step

Pipeline Step Name: Extract Credentials

Extract Credentials ⓘ		Environment Properties	
Basic Properties		Type	Default
Enabled (*)	boolean	true	<input checked="" type="radio"/> true <input type="radio"/> false
Extract Credentials Properties		Type	Default
Credentials location (*)	string	HTTP	WS-BASIC
Namespaces	string		
UserID xpath	string		
Password xpath	string		

8. Scroll down to the bottom of the page, and click **Ok**.

You return to the Policy Definition page.

To add the File Authenticate policy step

The extracted credentials need to be validated against a reference. In this tutorial, the reference is a file of valid user names and passwords. Other references that can be used with Oracle Web Services Manager include LDAP directories, Oracle Access Manager, or eTrust SiteMinder from CA.

1. In the Extract Credentials row, click the **Add Step Below** link.
2. From the Select Step Template list, select File Authenticate, and click **Ok** (Figure 2–25).

Figure 2–25 Selecting the File Authenticate Policy Step

Pipeline: "Request" [Replace Pipeline](#)

Pipeline Steps:

Start Pipeline [Add Step Below](#)

Log ⓘ [Configure](#) [Add Step Below](#) [Delete](#)

Extract Credentials ⓘ [Configure](#) [Add Step Below](#) [Delete](#)

New Step [Cancel](#)

Select Step Template:

File Authenticate

Ok

End Pipeline

3. In the File Authenticate row, click **Configure**.
4. The properties for the File Authenticate policy step are displayed. In the **Passwd file location** box, you will specify the full path location and name of the file used

to authenticate users (Figure 2–26). In our example, we are specifying the following location:

C:\.htpasswd

In a later step, you will be creating a file called .htpasswd at the root directory.

- 5. In the .htpasswd file format field, you specify the format in which passwords are encrypted. Select **md5** from the list (Figure 2–26). MD5 is the message digest algorithm that you will use to encrypt the password later in this tutorial.

Figure 2–26 File Authenticate Policy Step Properties

Policy Management > Manage Policies > Policies > Policy

Configure Step

Help

Pipeline: "Request"

Configure pipeline step

Pipeline Step Name: File Authenticate

File Authenticate

Environment Properties

Basic Properties	Type	Default	Value
Enabled (*)	boolean	true	<input checked="" type="radio"/> true <input type="radio"/> false

Authentication Properties	Type	Default	Value
Passwd file location (*)	string	.htpasswd	c:\.htpasswd
.htpasswd file format (*)	string	mixed	md5

Faults and Fault Handlers

Fault Code:

http://schemas.oblinox.com/ws/2003/08/Faults:AuthenticationFaultAdd Handler

Ok

Cancel

- 6. Click Ok.
- 7. Click Next, then click Save (Figure 2–27).

Figure 2–27 Policy for the MyGateway Component

Policy Management > Manage Policies > Policies > Policy

Enforcement Points

Policy for Component: "C0003001"

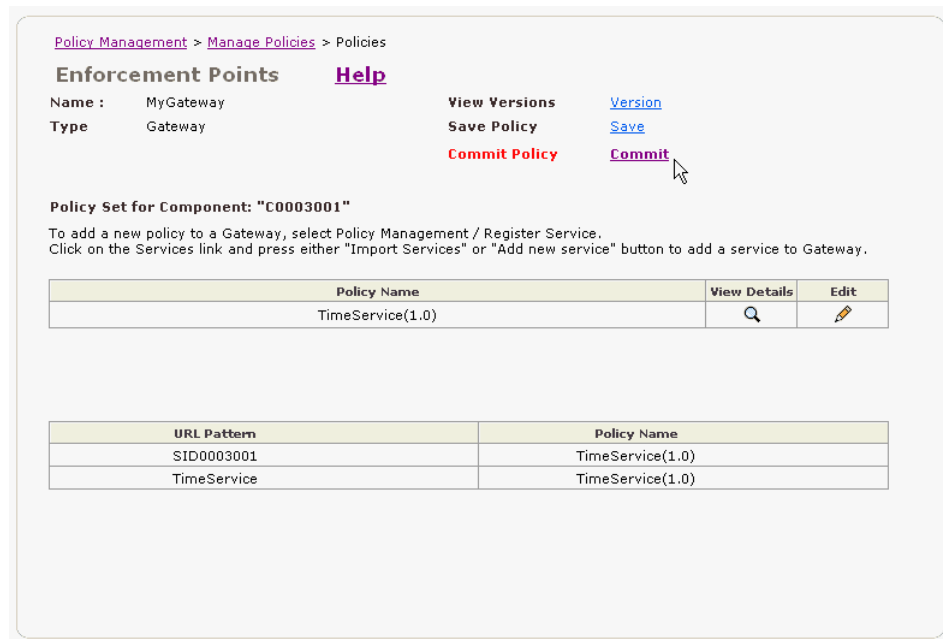
Policy

Policy Name: TimeService(1.0)

Save

- The Commit Policy field appears in red, alerting you that you must commit your changes (Figure 2–31). Click the **Commit** link.

Figure 2–28 Policy Set for MyGateway Gateway with TimeService Policy Added



- The page refreshes and in the Commit Policy field, the message indicates the policy has been committed.

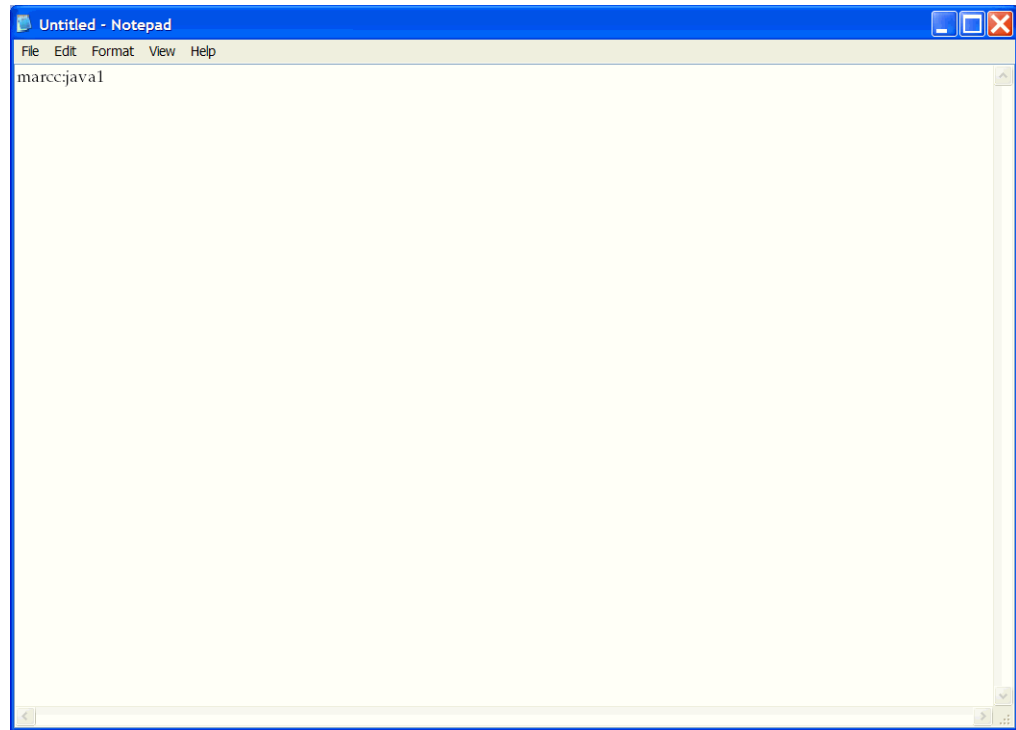
Create the Authentication File

You will be creating a file with your user name and password. This file, which was specified in the File Authenticate step, will be used to authenticate you when you attempt to access the Web service. You will use an Oracle WSM tool to encode the password in the file.

- Create a text file and add a user name and password in the following format:

user_name:password

Figure 2–29 is an example of a text file (.htpasswd) with the user name *marcc* and the password *java1*. Enter this user name and password combination, or add your own user name and password.

Figure 2–29 .htpassword File with User Name and Password

2. Save the file with the name `.htpassword` in the root directory. We are saving the file at the root, but you can save the file anywhere.
3. You will be using an Oracle WSM utility to create a digest or hash of the password. A digest is the result of applying a one-way mathematical function to an input stream in order to compress it. Message-Digest Algorithm 5 (MD5) is one mathematical function commonly used to store passwords.

Open a command window and execute the following command:

On Linux:

```
ORACLE_HOME/owsm/bin/wsmadmin.sh md5encode user_name password
.htpasswd
```

On Windows:

```
ORACLE_HOME\owsm\bin\wsmadmin md5encode user_name password
.htpasswd
```

For example:

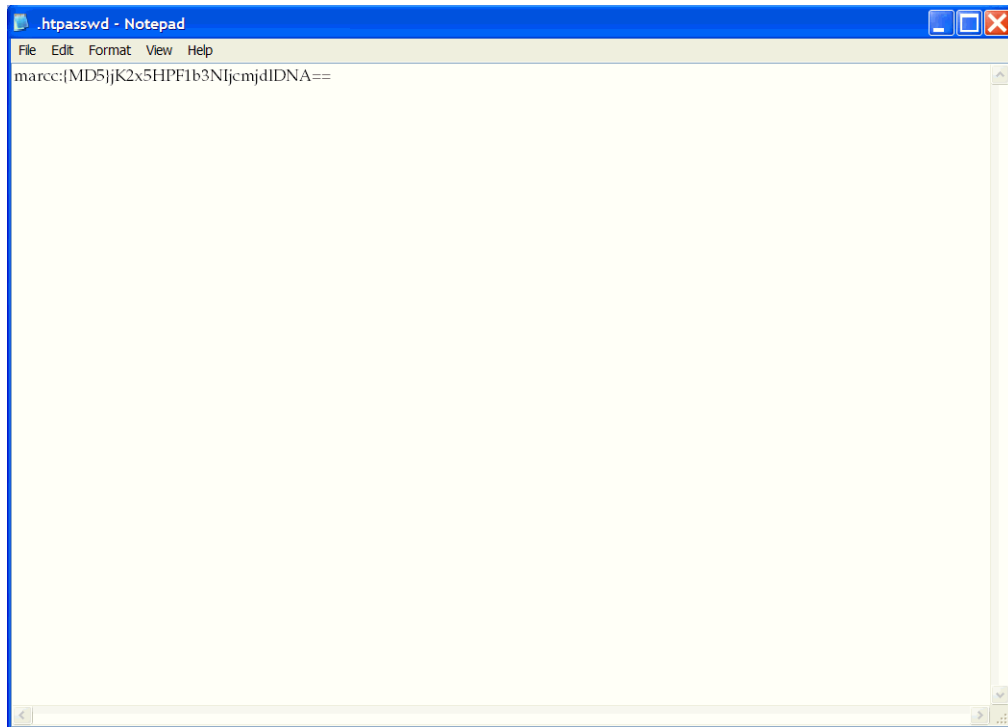
```
ORACLE_HOME\owsm\bin\wsmadmin md5encode marcc java1 .htpasswd
```

Note: Use the user name and password you entered in Step 1 of this procedure.

Be sure to leave a space between the user name (*marcc* in our example) and the password (*java1*).

4. Open the `.htpasswd` file in a text editor. You will see that the password you entered has been replaced by an encrypted version of the password similar to what you see in [Figure 2–30](#).

Figure 2–30 .htpasswd File with Encrypted Password



When the File Authenticate policy step is executed, it uses the .htpasswd file and checks to see if the credentials that are passed matches one of the entries in the file.

View Your WSDL

In order to test your WSDL and see if you can access the Web Service, you need to make a request to the Oracle WSM Gateway to which the WSDL is registered. You need to get the URL to which you make your request.

1. From the navigation pane of Web Services Manager Control, click **Policy Management**, then click **Register Services**.
2. For your gateway, MyGateway, click the **Services** link.
3. In the List of Services, click the **Edit** link for the TimeService service ([Figure 2–31](#)).

Figure 2–31 Editing the TimeService Service

Policy Management > Register Services > List of Services

Gateways [Help](#)

Name MyGateway View Versions [View Versions](#)
 Type Gateway Save Policy [Save Policy](#)
 Commit Policy Policy is committed

List of Services: MyGateway Import Services Add New Service

Service Id	Service Name	Version	Description	View Details	Deactivate service	Edit
SID0003001	TimeService	1.0	Gives the time of day			

- In the Edit Service page, copy the URL in the Service WSDL URL field (Figure 2–32).

You will use this URL in the next task.

Figure 2–32 Copying the Service WSDL URL

> Register Services > List of Services > Edit Details

Gateways [Help](#)

Edit Service: "SID0003001"

Client Access URLs

Service URL: <http://lasato-pc.us.oracle.com:8888/gateway/services/SID0003001>
 Service WSDL URL: <http://lasato-pc.us.oracle.com:8888/gateway/services/SID0003001?wsdl>

Basic Parameters

Service Name: TimeService
 Service Version: 1.0
 Service Description: Gives the time of day
 WSDL URL: <http://lasato-pc.us.oracle.com:3115/ccore/TimeService.wsdl>
 Service Protocol: [--> Modify Protocol Parameters](#)
 Service Policy: [--> Modify Policy](#)
 Compatible Service Versions: [View and Modify version compatibility](#)

Service Groups:
 Modify privileges

sa1-grp
 da1-grp

[Add Groups with Modify privileges](#)

sa1-grp
 sa2-grp

<< Add

Protecting Your Web Services

The Oracle Web Services Manager Gateway is designed to virtualize Web services. Therefore, you could access the Web services directly and circumvent the security provided by the gateway. To correct this potential security breach, Oracle recommends that customers use an Oracle Web Services Manager Agent to ensure that the Web service can only be accessed through the agent. This is sometimes referred to as "last-mile security."

Test Your WSDL

You will simulate a Web service request to test that the Time Service is correctly secured. You will make the request using the user name and password you added to the authentication file.

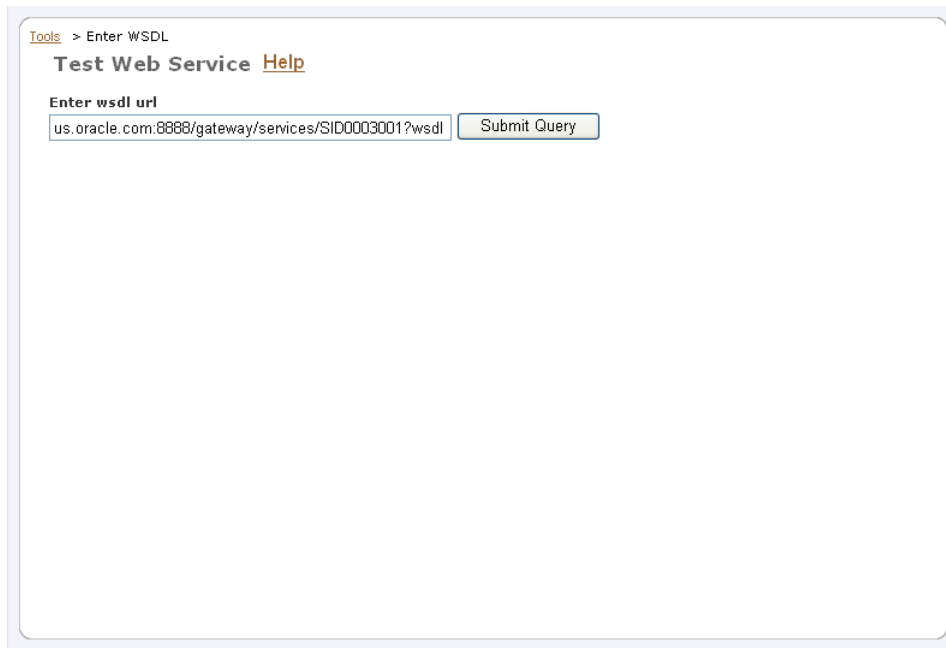
1. From the navigation pane of the Web Services Manager Control, click **Tools**, then click **Test Page** (Figure 2–33).

Figure 2–33 Web Services Manager Navigation Pane



2. Paste the URL you copied into the **Enter wsdl url** text box as shown in (Figure 2–34).

Figure 2–34 Test Web Service Page



3. Click **Submit Query**. The Test Page refreshes and displays a number of parameters (Figure 2–35). Note that the endpoint URL is pointing to the gateway.

Figure 2–35 Test Web Service Page for the Example WSDL

Tools > Enter WSDL > Test Page

Test Web Service [Help](#)

Endpoint URL: Port:

Operation: ☒ HTML Form ☐ XML Source

☒ Reliable Messaging ☐ Include In Header

☒ WS-Security ☐ Include In Header

☒ OWSM Agent ☐ Include In Header

format

☒ Show Transport Info

☒ Save Test ☐

☒ Perform stress test ☐ Enable

4. You will simulate a request from a Web service client by providing credentials. Click the plus sign (+) next to the WS-Security parameter. The User Name and Password parameters are exposed (Figure 2–36).
5. Select the check box **Include in Header** to include the credentials in the WS-Security header (Figure 2–36).

Figure 2–36 Test Web Service Page with WS-Security Parameters Filled In

Tools > Enter WSDL > Test Page

Test Web Service [Help](#)

Endpoint URL: Port:

Operation: ☒ HTML Form ☐ XML Source

☒ Reliable Messaging ☐ Include In Header

☒ WS-Security ☒ Include In Header

User Name xsd:string

Password xsd:string

☒ OWSM Agent ☐ Include In Header

format

6. Enter the user name and password you supplied for the .htpasswd file in the User Name and Password fields. Figure 2–36 shows the user *marcc* and the password for this user obscured.
7. Click **Invoke**.

The Test Result displays the current time. By default, the results are displayed in raw HTML. Click the **Formatted XML** link to see the results in an easier-to-read format (Figure 2–37).

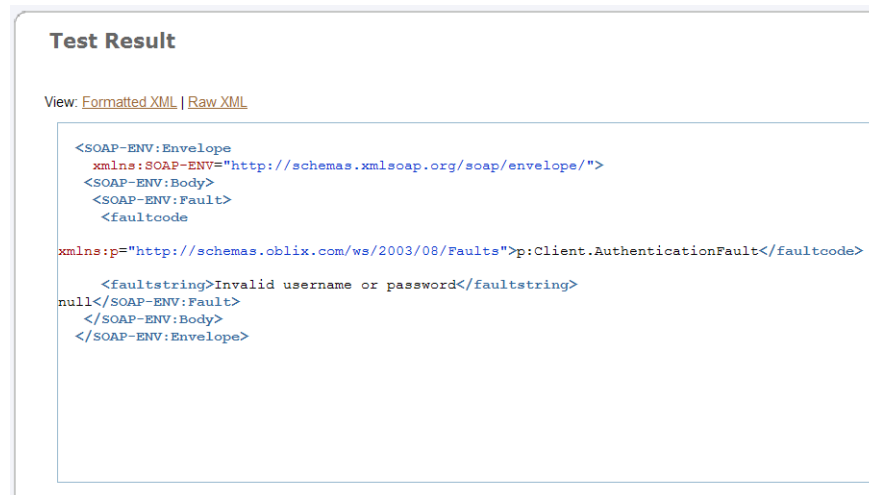
Figure 2–37 Test Result in Formatted XML



Test the File Authentication Policy Step

Now, you will make a request for the Time Service Web service, but this time, you will use an invalid user name and password, to verify that the File Authentication policy step is working.

1. On the Test Result page, click the **Test same WSDL again** link.
2. Click the plus sign (+) next to WS-Security to display the WS-Security parameters.
3. This time, enter a user name that is *not* a valid user, for example, **bugs bunny**, and enter any password.
4. Again, select the check box **Include in Header**.
5. Click **Invoke**.
6. This time, the Test Result shows that a Client Authentication Fault occurred, and the current time is not returned (Figure 2–38).

Figure 2–38 Test Result Page Showing a Client Authentication Fault

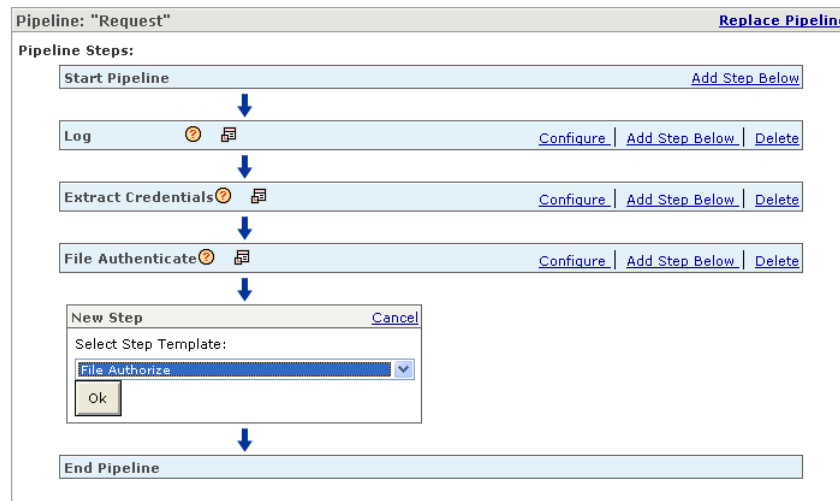
By first providing valid credentials, then providing invalid credentials, you have tested that authentication is working. Authentication verifies your identity based on the credentials you provide. This is, however, only the first step. The second step is to verify whether an authenticated user is authorized to access a resource (in this tutorial, the Time Service Web service) based on attributes assigned to the user's identity.

Adding the Authorization Policy Step

First we need to edit the Request pipeline for the gateway and add an authorization policy step.

To add the File Authorize policy step

1. From the navigation pane of the Web Services Manager Control, click **Policy Management**, then click **Manage Policies**.
2. In the List of Components, click the **Policies** link for your gateway.
3. Click the **Edit** icon.
4. In the File Authenticate row, click **Add Step Below**.
5. From the Select Step Template list, select **File Authorize**, and click **Ok** (Figure 2–39).

Figure 2–39 Selecting the File Authorize Policy Step

6. In the File Authorize row, click **Configure**.
7. The properties for the File Authorize policy are displayed (Figure 2–40).

Figure 2–40 File Authorize Policy Step Properties

The screenshot shows the "Configure Step" dialog for the "File Authorize" policy. The dialog has a "Help" link and a "Pipeline: 'Request'" label. The "Configure pipeline step" section shows the "Pipeline Step Name: File Authorize". Below this, there are three sections: "Basic Properties", "Authorization Properties", and "Environment Properties". The "Basic Properties" section has a table with columns "Type", "Default", and "Value". The "Authorization Properties" section has a table with columns "Type", "Default", and "Value". The "Environment Properties" section has a table with columns "Type", "Default", and "Value". The "User roles file location (*)" field is highlighted. Below the "Authorization Properties" section, there is a "Faults and Fault Handlers" section with a "Fault Code" field and a "Handler" field. The "Ok" and "Cancel" buttons are at the bottom.

Basic Properties	Type	Default	Value
Enabled (*)	boolean	true	<input checked="" type="radio"/> true <input type="radio"/> false

Authorization Properties	Type	Default	Value
User roles file location (*)	string		<input type="text"/>
Allowed roles	string[]		<input type="text"/>

Faults and Fault Handlers

Fault Code: Handler:

8. Specify the file that will be used to authorize users in the **User roles file location** field (Figure 2–40).

Enter: `ORACLE_HOME/owsm/config/gateway/roles.xml`

where `ORACLE_HOME` is the directory where Oracle Web Services Manager is installed.

9. Specify which roles are permitted access to the Web service in the **Allowed roles** field. Enter **guest**, and click **Ok** (Figure 2–41).

Figure 2–41 Configuring the File Authorize Policy Step

Policy Management > Manage Policies > Policies > Policy

Configure Step [Help](#)

Pipeline: "Request"

Configure pipeline step

Pipeline Step Name: File Authorize

File Authorize		Environment Properties	
Basic Properties			
Enabled (*)	boolean	Default	Value
			<input checked="" type="radio"/> true <input type="radio"/> false
Authorization Properties			
User roles file location (*)	string	Default	Value
			eAS_1\owsm\config\gateway\roles.xml
Allowed roles	string[]		guest

↓ ↓

Faults and Fault Handlers

Fault Code: <http://schemas.oblix.com/ws/2003/08/Faults:AuthorizationFault> [Add Handler](#)

Ok Cancel

10. Click **Next**, then click **Save**.
11. The Commit Policy field appears in red, alerting you that you must commit your changes. Click the **Commit** link.

Edit the Authorization File

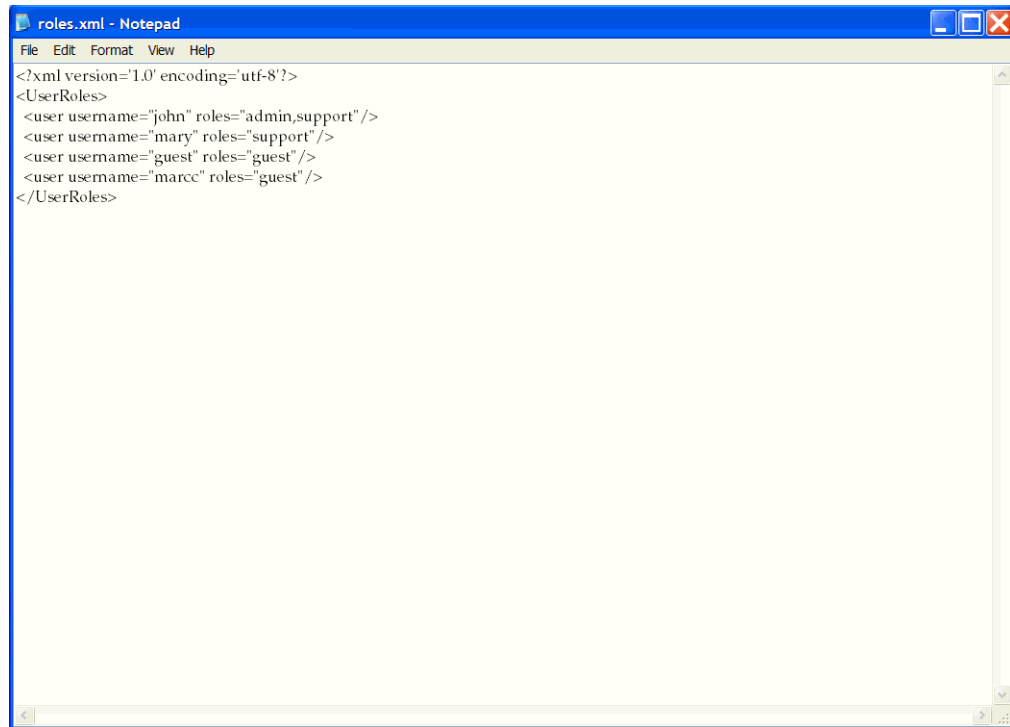
Once the user name and password have been authenticated, then Oracle Web Services Manager checks to see if the user is authorized to access the Web service. In our tutorial, this is done by checking a file to see if the user is assigned to an authorized role.

A sample authorization file can be found in the following location:

`ORACLE_HOME/owsm/config/gateway/roles.xml`

where `ORACLE_HOME` is the directory where Oracle Web Services Manager is installed. You will be adding your user name and the `guest` role to this file.

1. Open the file in a text editor.
2. Add your user name and the role, `guest`. [Figure 2–42](#) shows the user `marcc` assigned to the role `guest`.

Figure 2–42 Roles File with User Name and Role Added

3. Save the file.

If the user name and password are successfully authenticated with the File Authenticate step, then the File Authorize step is executed. Oracle WSM checks the roles.xml file to see if the user has been assigned a role that is authorized to access the Time Service Web service. In this example, users assigned the role of *guest* may access the service.

Execute the Test Page Again

This time, you will be sending valid credentials which will be validated against the file. Then, the user will be checked against a file to see if he is assigned to a role that is authorized to access the Web service.

1. From the navigation pane of the Web Services Manager Control, click **Tools**, then click **Test Page**.
2. Paste the URL you copied into the **Enter wsdl url** text box.
3. Click **Submit Query**.
4. Click the plus sign (+) next to the WS-Security parameter.
5. Select the check box **Include in Header**.
6. Enter the user name and password you supplied for the .htpasswd file, and click **Invoke**.

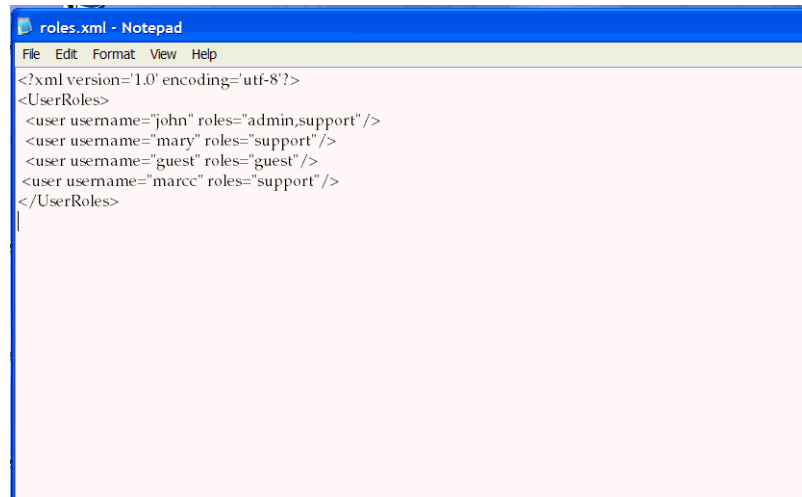
The Test Result displays the current time.

Test the File Authorization Policy Step

Now you will test the File Authorization policy step by editing the file authorization file and assigning a role that is *not* authorized access the Web service to your user.

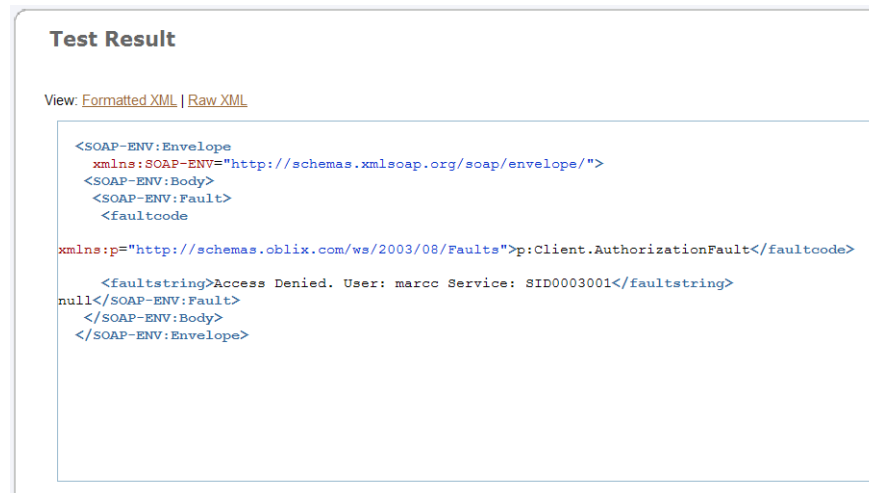
1. Edit the `ORACLE_HOME/owsm/config/gateway/roles.xml` file. Change the role for your user to something other than `guest`, and save the file. In our example, the user `marcc` is now assigned to the role `support` (Figure 2–43).

Figure 2–43 *roles.xml File with User Assigned to Unauthorized Role*



2. From the Test Page, click the **Test same WSDL again** link.
3. Click the plus sign (+) next to WS-Security to display the WS-Security parameters.
4. Enter a valid user name and password, and click **Invoke**.
5. This time, the Test Result page displays a Client Authorization fault, and shows that the user in this example, `marcc`, was denied access to the service whose ID is `SID0003001` (Figure 2–44).

Figure 2–44 *Test Result Page Showing a Client Authorization Fault*



Summary

In this tutorial, you learned about the security features of Oracle Web Services Manager. You created an Oracle WSM Gateway, registered a Web service to the gateway, created policies to protect the Web service, and tested those policies.

Now we will look at the monitoring features of Oracle WSM.

Monitoring Your Oracle Web Services Manager Environment

In this tutorial, we will look at the following monitoring features of Oracle Web Services Manager:

- Overall statistics for your Oracle Web Services Manager environment
- Security Statistics
- Latency Variance
- Traffic Analysis
- Service-Level Agreements (SLA)
- Execution Details
- Message Logs

Before You Begin

You can view Oracle WSM metrics over a period of time. For example, you can get overall statistics for a gateway over the last 2 hours or for the last 30 days. By default, the Oracle WSM Database persists data only for the last 100 minutes. So, if you select the time range **Last 10 minutes** or **Last hour** from the Time Range list, you will see the metrics for the period you selected. If you want to save your metrics over a longer period of time, you will need to configure the Oracle WSM Database to store the data for the desired length of time.

To configure the time period for which metrics data is persisted

1. Edit the following file:

`ORACLE_HOME/owsm/config/coreman/monitor-config-installer.properties`

2. Change the value for the `monitor.aggregator.measurementStore.WindowSize` parameter.

The number specified is the length of time, in minutes, that the Oracle WSM Database retains metric data.

3. Redeploy the application by executing the following command:

On Linux

```
ORACLE_HOME/owsm/bin/wsmadmin.sh deploy passwordmonitor
```

On Windows

```
ORACLE_HOME\owsm\bin\wsmadmin.bat deploy passwordmonitor
```

Use the OC4J Administrator password.

Generating Oracle Web Services Manager Metrics

Use the Test Page to simulate both successful and unsuccessful invocations of the Web service. After you have executed any number of invocations, we will use the Web Services Manager Control to view the generated statistics.

1. From the Oracle Web Services Manager Control, click **Tools**, then click **Test Page**.
2. Enter or paste the URL you copied earlier. If you need to copy the URL again, follow the procedure in the View Your WSDL section of the tutorial.
3. Click **Submit Query**.
4. Click the plus sign (+) next to the WS-Security parameter. The User Name and Password parameters are exposed.
5. Enter the user name and password.
6. Select the check box **Include in Header** to include the WS-Security feature in the test.

Figure 3–1 Test Page with WS-Security Parameters Filled In

Tools > Enter WSDL > Test Page

Test Web Service [Help](#)

Endpoint URL : Port :

Operation : ☒ HTML Form ☐ XML Source

☒ Reliable Messaging ☐ Include In Header

☒ WS-Security ☒ Include In Header

User Name xsd:string

Password xsd:string

☒ OWSM Agent ☐ Include In Header

format xsd:string

7. Select the **Enable** box next to Save Test to enable this feature.
8. Click the plus sign (+) next to **Save Test**, and enter a name for the test and, optionally, a brief description.

For more information on saving tests and how to use saved tests, see "[Reusing Your Tests](#)" on page 3-3.

9. Click **Invoke**.
10. Click Test same WSDL again to return to the Test Page.
11. Repeat steps 4 – 9.

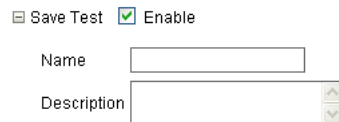
Reusing Your Tests

You can use the Save Test section of the Test Page to save a test so that you can rerun a test without re-entering the test details. This is useful in generating multiple results that can be viewed using the monitoring features of Oracle Web Services Manager.

To create a saved test

1. From the Web Services Manager Control, click **Tools**, then click **Saved Tests**.
2. Click **Create New Test**.
3. Enter the URL of the WSDL in the **Enter wsdl url** field, and click **Submit Query**.
4. Enter any desired values in the Test Page.
5. Select the **Enable** box next to Save Test to enable this feature.
6. Click the plus sign (+) next to **Save Test**, and enter a name for the test and, optionally, a brief description (Figure 3–2).

Figure 3–2 Save Test Parameter on Test Page



Save Test ☒ Enable

Name

Description

7. Click **Invoke**.

To run a saved test

1. From the Web Services Manager Control, click **Tools**, then click **Saved Tests**.
2. In the List of Tests, click the **Run Test** icon for the test you want to execute.

Using Saved Tests to Test Authentication and Authorization

You can create a saved test that results in a successful authentication by entering valid credentials on the Test Page, and saving the test. Similarly, you can create a saved test that results in a *failed* authentication by providing *invalid* credentials on the Test Page. Once the test is saved, you can then run the saved test to get desired result.

The situation is slightly more complicated for testing authorizations. Generating a successful authorization requires that the authorization file contain the correct user name and role, in our example, this role is *guest* for user *marcc*. Therefore, if you want to produce a successful authorization, the file needs to contain a valid user name and role. And, if you want to generate a failed authorization, the file needs to contain an invalid role, an invalid user name, or both. In other words, before running a saved test that produces a particular authorization result (that is, success or fail), you may need to modify the authorization file to get the desired results.

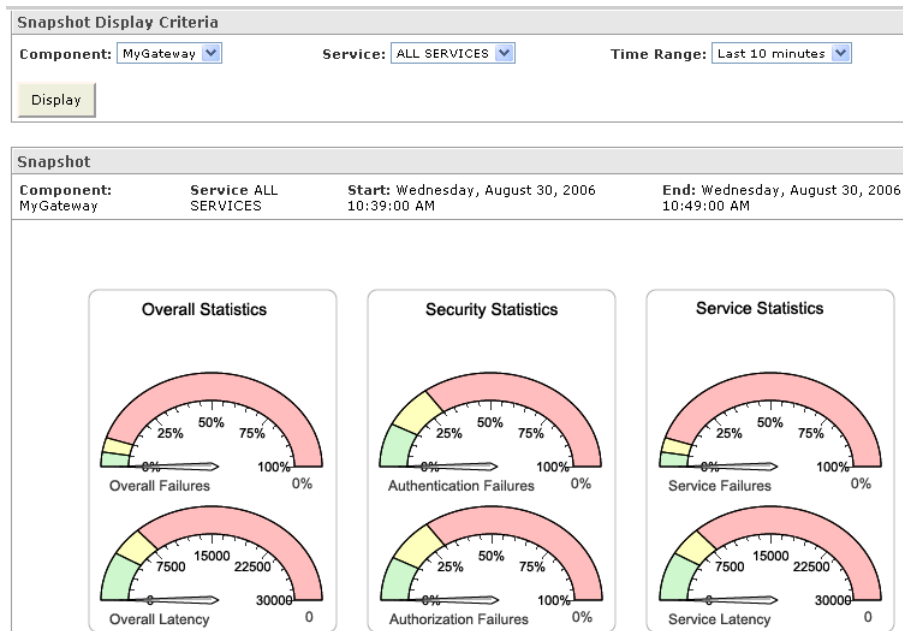
Monitoring Oracle Web Services Manager

View the Overall Statistics

To view the overall statistics

1. From the Web Services Manager Control, click **Operational Management**, then click **Snapshot**.

Figure 3–3 Overall Snapshot with No Data Displayed



2. In the Snapshot Display Criteria, your gateway should appear in the Component list. Select Time Service from the Service List. Select the time range within which you executed the service invocations in the last procedure from the Time Range list.
3. Click **Display**. A graphical display of statistics for Oracle Web Services Manager is displayed ([Figure 3–4](#)).

Figure 3–4 Overall Snapshot View of the Time Service Web Service

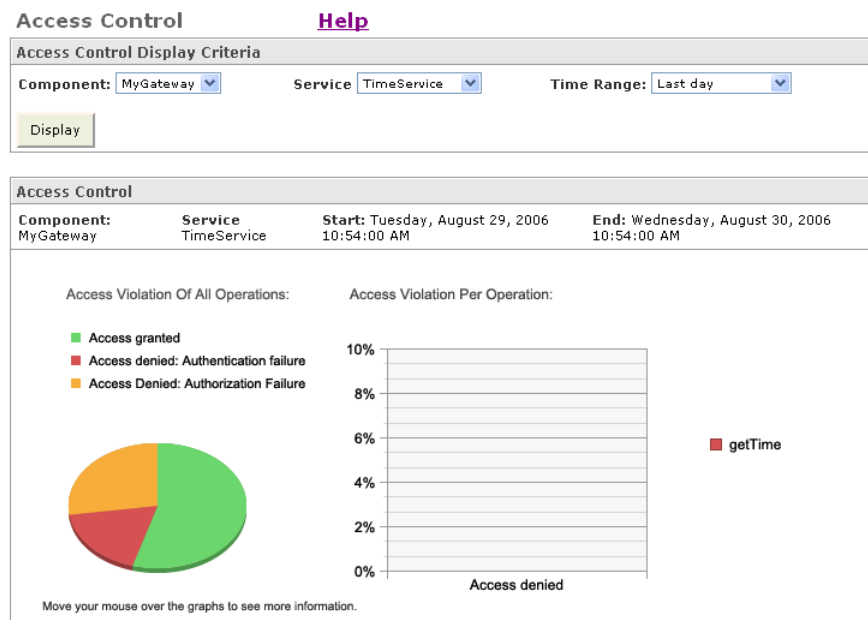
In the Overall Statistics, the Overall Failures show all failures to successfully invoke the service, including security failures and service failures. This is separated out in the Security Statistics and Service Statistics charts. The Security Statistics failures are separated to show the authentication failures and authorization failures.

View the Security Statistics

To view the security statistics

1. From the Web Services Manager Control, click **Operational Management**, click **Security Statistics**, then click **Access Control**. You should see something similar to [Figure 3–5](#).

Note: By default, you will see the statistics for all services. If you have more than one service registered to the gateway, you can see the statistics for each service by selecting the desired service from the Service list.

Figure 3–5 Security Statistics View of Time Service Web Service

- On the Access Control page, you can view and monitor authentication and authorization activity for your Web services. In the Access Control Display Criteria, specify the component (in this example, MyGateway), the service (Time Service), and time range and click **Display**.
- The pie chart is a graphical representation of the proportion of invocations in which the user was authenticated and granted access to the Time Service (indicated in green), the user failed to be authenticated (indicated in red), and the user was authenticated, but was denied access to the Time Service because of an authorization failure (indicated in orange).

Move your cursor over the sections in the pie chart to see additional details such as the number of authentication failures. The number of authentication failures is for the period specified in the Time Range field.

Note: If you are using Internet Explorer, you may be prompted to left-click to see the detailed information.

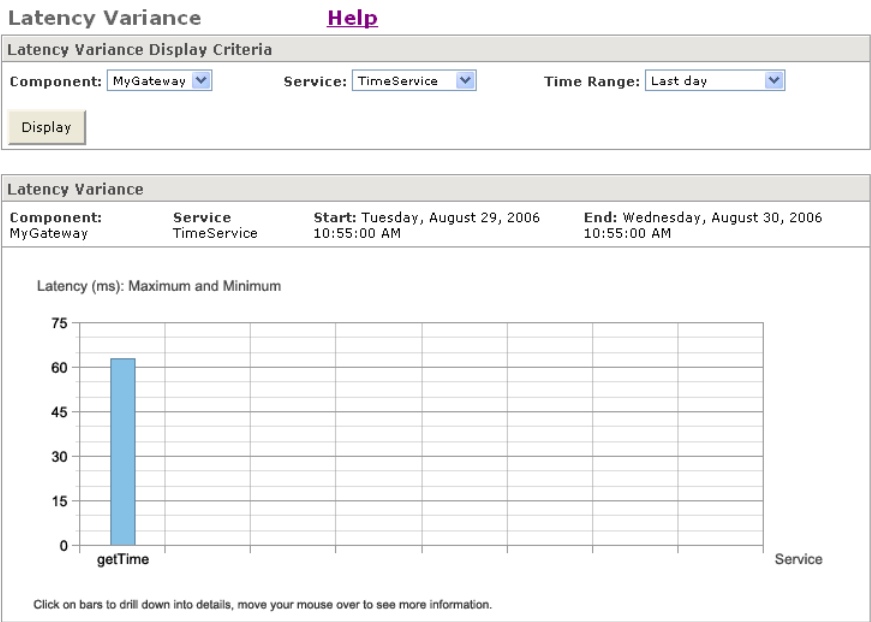
- The bar chart shows the percentage of invocations in which access was denied for each service. In our example, we have only one Web service, TimeService, so there is only one bar.

Latency Variance

To view latency variance for the Web service

From the navigation pane, click **Operational Management**, then click **Service Statistics**, then **Latency Variance**. You should see something similar to [Figure 3–6](#).

Figure 3–6 Latency Variance Page

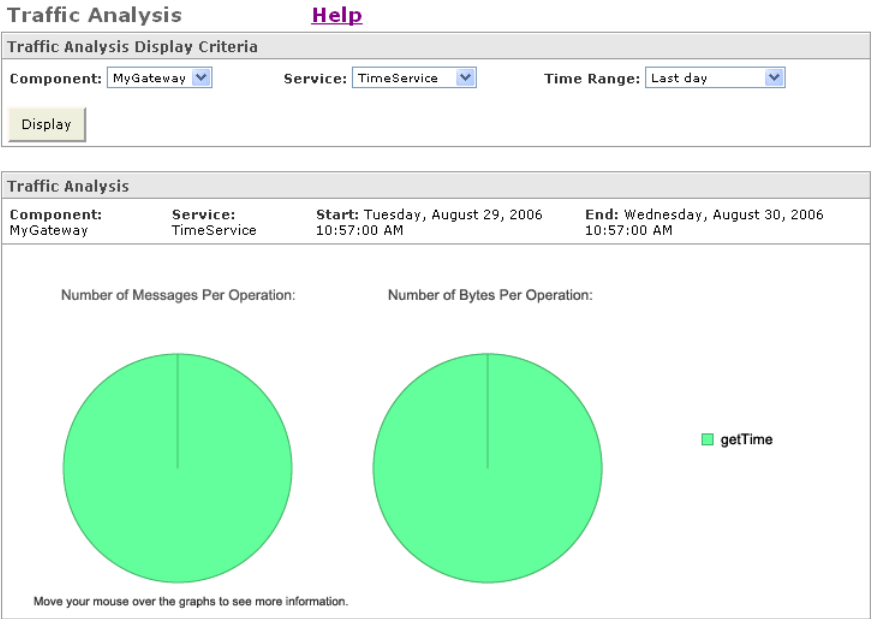


Move your cursor over the bar to see details about the minimum, maximum, and average latency, in milliseconds, for the Web service.

Traffic Analysis

To view traffic analysis
From the navigation pane, click **Operational Management**, then click **Service Statistics**, then **Traffic Analysis**. The page should look similar to [Figure 3–7](#).

Figure 3–7 Traffic Analysis Page



The Traffic Analysis page shows the number of messages for each service or operation and the number of bytes for each service or operation.

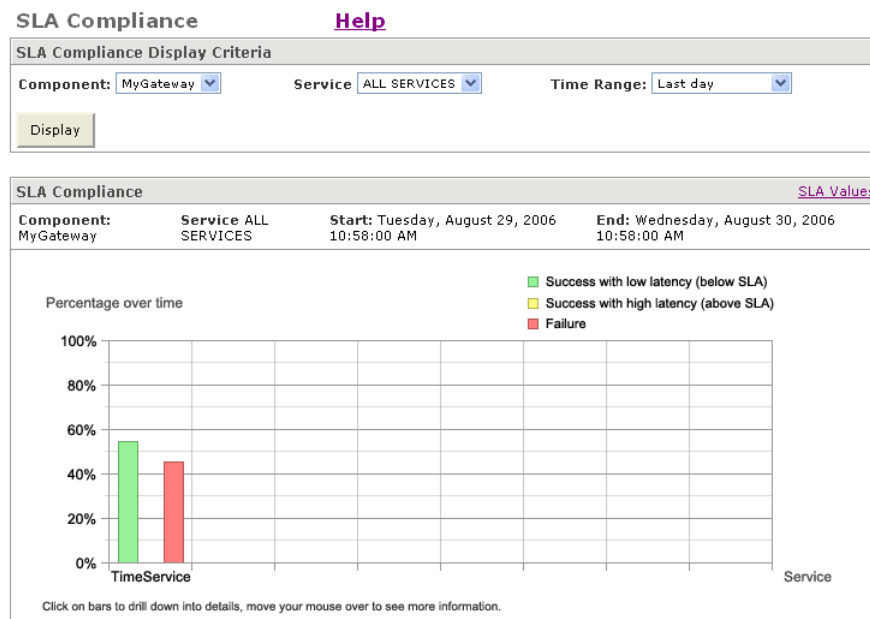
Move your cursor over the charts to see detailed traffic analysis information.

Service-Level Agreements (SLA)

To view the SLA compliance of a Web service

1. From the navigation pane, click **Overall Statistics**, then click **SLA Compliance**. Your page should look similar to [Figure 3–8](#).

Figure 3–8 SLA Compliance Page Showing Invocations Above and Below SLA



The SLA Compliance page shows the percentage of successful Web invocations that fall below the SLA (indicated in green), above the SLA (indicated in yellow), and the percentage of failed invocations (indicated in red). By default, the SLA compliance is shown for all Web services.

2. Click one of the bars (green or red) for a Web service to see the SLA compliance just for that particular service.

To define a Service-Level Agreement

1. Click the **SLA Values** link (in the upper right corner) to define an SLA.
2. From the Service list, select TimeService, and click **Next** ([Figure 3–9](#)).

Figure 3–9 Service Level Agreement Page

[Operation Management](#) > [Overall Statistics](#) > [SLA Compliance](#) > SLA Values

Service Level Agreement

Help

Service Level Agreement	
Component:	MyGateway
Service:	Select Service

Next

Cancel

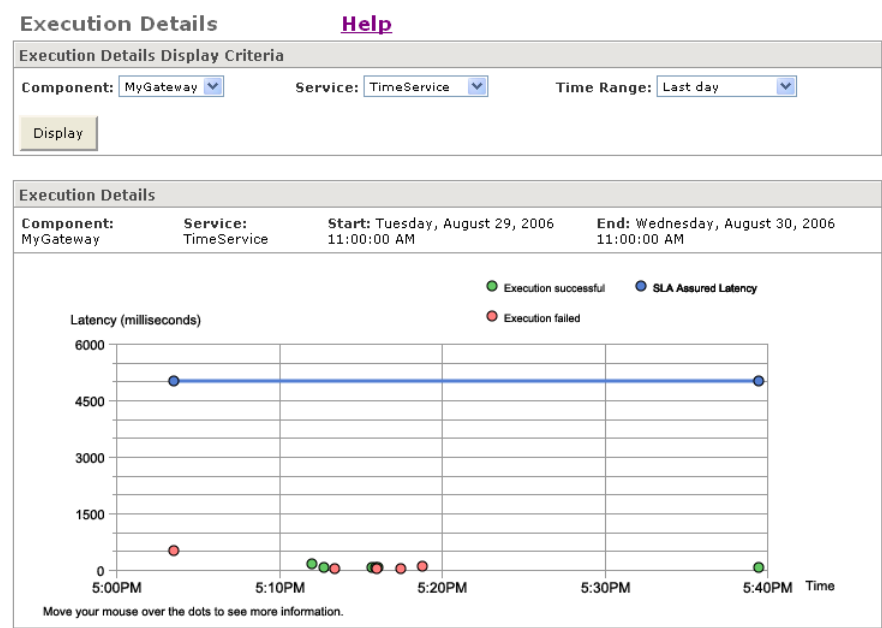
3. Change one or more of the values for your service level agreement, and click **Save**.
The SLA Compliance page displays again. It may look different depending on how the values were changed.

Execution Details

To view the execution details

1. From the navigation pane, click **Operational Management**, then click **Overall Statistics**, then click **Execution Details** (Figure 3–10).

Figure 3–10 Execution Details Page



- Move your cursor over one of the dots and click to see additional details about a particular execution instance.
2. From the navigation pane, click **Operational Management**, then click **Overall Statistics**, then click **Message Logs**.

Figure 3–11 Message Logs Page

Message Logs

[Help](#)

Message Logs Search Criteria

Component: MyGateway

Time Range: Last 2 hours

Search

Index	Service Id	Access Time	Log Type
1	SID0003006	Thursday, August 24, 2006 02:39:54 PM	Request
2	SID0003006	Thursday, August 24, 2006 02:39:54 PM	Response
3	SID0003006	Thursday, August 24, 2006 02:40:01 PM	Request
4	SID0003006	Thursday, August 24, 2006 02:40:01 PM	Response
5	SID0003006	Thursday, August 24, 2006 02:40:03 PM	Request
6	SID0003006	Thursday, August 24, 2006 02:40:03 PM	Response
7	SID0003006	Thursday, August 24, 2006 02:40:05 PM	Request
8	SID0003006	Thursday, August 24, 2006 02:40:05 PM	Response
9	SID0003006	Thursday, August 24, 2006 02:40:07 PM	Request
10	SID0003006	Thursday, August 24, 2006 02:40:07 PM	Response
11	SID0003006	Thursday, August 24, 2006 02:43:27 PM	Request
12	SID0003006	Thursday, August 24, 2006 02:43:30 PM	Request
13	SID0003006	Thursday, August 24, 2006 02:43:31 PM	Request
14	SID0003006	Thursday, August 24, 2006 02:43:33 PM	Request
15	SID0003006	Thursday, August 24, 2006 02:43:42 PM	Request

Component Logs: 1 2 Next

3. Click on the number in the Index column to display one of the logs (Figure 3–12).

Figure 3–12 Example of a Message Log

http://asato-pc.us.oracle.com:3115/ccore/ShowMessageLog?random=E...

<?xml version="1.0" encoding="UTF-8" ?>
- <soap:Envelope
 soap:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
 xmlns:soapenc="http://schemas.xmlsoap.org/soap/encoding/">
 - <soap:Body>
 - <n:getTimeResponse xmlns:n="urn:Test:GetTime">
 <Result xsi:type="xsd:string">02:40 PM</Result>
 </n:getTimeResponse>
 </soap:Body>
</soap:Envelope>

Note: This message log is an example of a successful response to an authentication attempt using an HTTP request. Therefore, you do not see a WS-Security header in the SOAP message.

Debugging Oracle Web Services Manager

The log files for Oracle Web Services Manager are the first source of information when trying to debug problems. The log files can be found in the following directory:

\$ORACLE_HOME/j2ee/instance/log

where *instance* is the name of the OC4J instance into which Oracle WSM is installed.

For more information on log files, see *Oracle Web Services Manager Administrator's Guide*.

Congratulations!

You have successfully completed the Oracle Web Services Manager Quick Start tutorial, and have learned many of the basic features of the product. To learn more about these and other features of Oracle Web Services Manager, refer to the following documentation:

- *Oracle Web Services Manager Deployment Guide*
- *Oracle Web Services Manager Administrator's Guide*
- *Oracle Web Services Manager Extensibility Guide*

Congratulations!
