



Deploying the BIG-IP System v10 with Oracle Application Server 10g R2

Version 1.1

Table of Contents

Deploying the BIG-IP system v10 with Oracle's Application Server 10g R2

Prerequisites and configuration notes	1-1
Product versions and revision history	1-2
Configuration example	1-2
Configuring the BIG-IP system for Oracle 10g R2	1-4
Running the Oracle Application Server application template	1-4
Modifying the Oracle 10g R2 configuration	1-10
Modifying the Oracle 10g R2 Portal configuration	1-10
Modifying the Oracle 10g R2 Single Sign-On configuration	1-14
Configuring Oracle 10g R2 Portal to use the new SSO URL	1-18
SSL Certificates on the BIG-IP system	1-20

Manually creating the BIG-IP LTM configuration

Configuring the BIG-IP LTM for Oracle 10g R2 Portal	2-1
Creating a HTTP health monitor	2-1
Creating the Oracle 10g R2 Portal pool	2-2
Creating Oracle 10g R2 Portal profiles	2-4
Creating the Oracle 10g R2 Portal virtual server	2-8
Optional: Configuring the BIG-IP LTM to offload SSL	2-10
Configuring the BIG-IP LTM for Oracle 10g R2 Single Sign-On server	2-12
Creating a HTTP health monitor	2-12
Creating the pool	2-13
Creating the Profiles	2-13
Creating the Single Sign-On virtual server	2-13

Manually Configuring the F5 WebAccelerator module

Prerequisites and configuration notes	3-1
Configuration example	3-1
Configuring the WebAccelerator module	3-2
Creating an HTTP Class profile	3-2
Modifying the Virtual Server to use the Class profile	3-3
Creating an Application	3-4



I

Deploying the BIG-IP System v10 with Oracle 10g R2

- Deploying the BIG-IP system v10 with Oracle's Application Server 10g Release 2
- Configuring the BIG-IP system for Oracle 10g R2
- Modifying the Oracle 10g R2 configuration
- SSL Certificates on the BIG-IP system

Deploying the BIG-IP system v10 with Oracle's Application Server 10g Release 2

Welcome to the F5 and Oracle® Application Server 10g Release 2 (R2) Deployment Guide. When deployed with Oracle 10g R2, the BIG-IP system v10 ensures secure, fast and always available access for applications running on Oracle.

Oracle 10g R2 meets customers' demand for up-to-date business information with reliable, scalable and cost-effective grid computing. With grid computing, organizations can leverage the use of many low-cost, modular servers acting as one computer, making their applications more scalable and less expensive to deploy and manage.

New in version 10.0 of the BIG-IP system are Application Ready Templates. These application templates ease the process of configuring the BIG-IP system. Instead of having to individually create each object that pertains to the type of application traffic you want the BIG-IP system to manage, you can run an application template. The application template automatically creates BIG-IP system objects that are customized for that application. These objects can be either local traffic objects, TMOS objects, or both.

To provide feedback on this deployment guide or other F5 solution documents, contact us at solutionsfeedback@f5.com.

Prerequisites and configuration notes

All of the procedures in this Deployment Guide are performed on the BIG-IP system. The following are prerequisites for this solution:

- ◆ The Oracle installation should be running Oracle 10g Release 2 (10.1.2.0.2).
- ◆ For this deployment guide, the BIG-IP LTM system must be running version 10.0 or later. If you are using a previous version of the BIG-IP LTM system see the *Deployment Guide* index.
- ◆ If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, but it is not yet installed on the BIG-IP LTM system. For more information, see *SSL Certificates on the BIG-IP system*, on page 1-20.
If offloading SSL, it is assumed that the BIG-IP system will perform SSL offload for the Oracle Single Sign On (SSO) servers.
- ◆ While we strongly recommend using the application template, you can also manually configure the BIG-IP system. See *Manually creating the BIG-IP LTM configuration*, on page 2-1.

- ◆ There are important changes for the Oracle configuration, be sure to see *Modifying the Oracle 10g R2 configuration*, on page 1-10.

◆ Important

All local traffic objects that an application template creates reside in administrative partition Common. Consequently, to use the application templates feature, including viewing the Templates list screen, you must have a user role assigned to your user account that allows you to view and manage objects in partition Common.

Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP System (LTM and WebAccelerator)	10.0
Oracle 10g	10g Release 2 (10.1.2.0.2)

Revision history:

Document Version	Description
1.0	New deployment guide
1.1	Added support for BIG-IP v10.1

Configuration example

The BIG-IP system provides intelligent traffic management and fail-over for Oracle 10g R2 Web and Application servers. Through advanced health checking capabilities, the BIG-IP product recognizes when resources are unavailable or under-performing and directs traffic to another resource. The BIG-IP product can also track Oracle Application Server 10g R2 end-user sessions, enabling the application server to maintain client session data. The following diagram shows an example deployment with Oracle 10g R2 and the BIG-IP system.

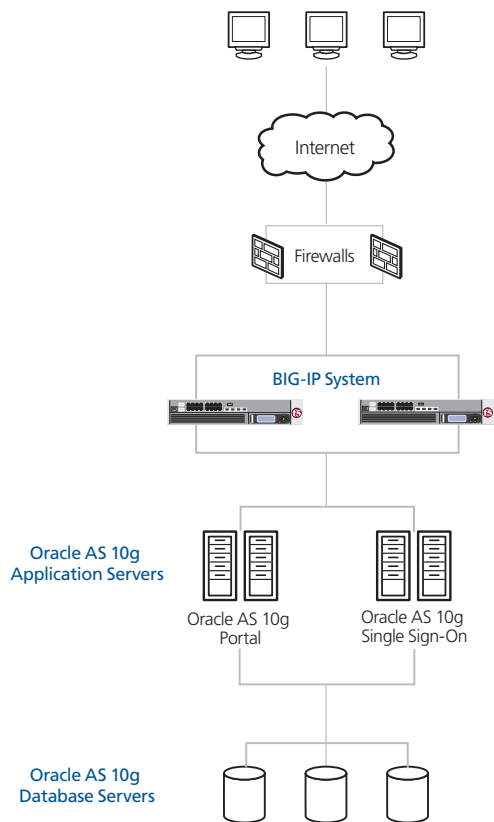


Figure 1.1 BIG-IP Oracle 10g R2 logical configuration example

Configuring the BIG-IP system for Oracle 10g R2

You can use the new Application Template feature on the BIG-IP system, to efficiently configure a set of objects corresponding to Oracle Application Server 10g R2. The template uses a set of wizard-like screens that query for information and then creates the required objects. At the end of the template configuration process, the system presents a list of the objects created and a description for how each object interacts with the application.

◆ Note

Depending on which modules are licensed on your BIG-IP system, some of the options in the template may not appear.

◆ Important

*After completing the application template on the BIG-IP system, you must continue with **Modifying the Oracle 10g R2 configuration**, on page 1-10.*

Running the Oracle Application Server application template

To run the Oracle Application Server 10g R2 application template, use the following procedure. For more information on specific settings, see the online help.

To run the Oracle Application Server application template

1. Verify that your current administrative partition is set to **Common**. The Partition list is in the upper right corner.
2. On the Main tab, expand **Templates and Wizards**, and then click **Templates**. The Templates screen opens, displaying a list of templates.
3. In the Application column, click **Oracle Application Server**. The Oracle Application Server application template opens.
4. In the Template Questions section, complete the following:
 - a) You can type a unique prefix for your Oracle Application Server objects that the template will create. In our example, we leave this setting at the default, **my_oracle_app**.
 - b) If the Portal and SSO servers can communicate with the clients using a route through the BIG-IP system to deliver response data to the client, select **Yes** from the list. In this case, the BIG-IP does **not** translate the client's source address.

If the BIG-IP system should translate the client's source address to an address configured on the BIG-IP system, leave the list at the default setting, **No**. Selecting **No** means the BIG-IP system

will use SNAT automap. See the Online Help for more information.

In our example, we leave this at the default setting: **No**.

The screenshot shows the 'Oracle Application Server Template' wizard. At the top, there is a breadcrumb trail: 'Templates and Wizards » Templates » oracle_as'. Below this, the title 'Oracle Application Server Template' is displayed. A welcome message states: 'Welcome to the Oracle Application Server Template. This wizard will create a complete configuration optimized for managing Oracle Application Server traffic.' The 'Template Questions' section contains two questions. The first question is 'Unique prefix name for all objects that will be created by this template?' with a text input field containing 'my_oracle_app'. The second question is 'Do the Oracle Portal and SSO servers have a route back to application clients via this BIG-IP system?' with a dropdown menu set to 'No'.

Figure 1.2 Running the Oracle Application Server application template

5. In the SSL Offload section, complete the following:
 - a) if you are not using the BIG-IP system to offload SSL, leave this setting at the default, **No**. Continue with Step 6.

If you are using the BIG-IP system to offload SSL from the Oracle devices, select **Yes** from the list. The SSL options appear.

- b) From the **Certificate** list, select the appropriate certificate you want to use for this deployment. If you plan to use a third party certificate, but have not yet installed it on the BIG-IP system, see *SSL Certificates on the BIG-IP system*, on page 1-20.
- c) From the **Key** list, select the appropriate key for the certificate. If you have not yet installed the key on the BIG-IP system, see *SSL Certificates on the BIG-IP system*, on page 1-20.

For information on generating certificates, or using the BIG-IP LTM to generate a request for a new certificate and key from a certificate authority, see the **Managing SSL Traffic** chapter in the *Configuration Guide for Local Traffic Management*.

SSL Offload Questions	
Do you want the BIG-IP system to offload SSL from the Oracle Portal servers?	<input type="button" value="Yes"/>
About SSL Offload:	It is assumed that the BIG-IP will perform SSL Offload for the Oracle Single Sign On servers.
Certificate to authenticate the server? (You may need to import a certificate before deploying this Template.)	<input type="button" value="oracle-ssl"/>
Key used for encryption? (You may need to import a key before deploying this Template.)	<input type="button" value="oracle-ssl"/>

Figure 1.3 Configuring the BIG-IP system for SSL Offload

6. In the Oracle Portal Server Load Balancing Questions section, complete the following:
 - a) Enter the IP address for this virtual server. The system creates a virtual server named **<prefix from step 4a>_virtual_server**. In our example, we type **192.168.12.100**.
 - b) From the Load Balancing Method list, select an appropriate load balancing method. In our example, we leave this setting at the default, **Least Connections (member)**.
 - c) Next, add each of the Oracle Application Servers that are a part of this deployment.

In the **Address** box, type the IP address of the first Oracle 10g R2 server. In our example, we type **10.132.82.100**.

In the **Service Port** box, leave the port at **7778** (the default port for Oracle Portal) unless you have modified the configuration on your Oracle Application Servers.

Click the **Add** button. Repeat this step for each of the Oracle devices.
 - d) Next, type a number of seconds that the BIG-IP system issues the health check. In our example, we leave this at the default level, **30**.
 - e) If you have a specific HTTP request you would like to add to the health check, type it in the box after **GET /**. This is optional.
 - f) Select the HTTP version that the Oracle 10g R2 servers expect clients to use. In our example, we select **Version 1.1**.

If you specify HTTP version 1.1, a new row appears asking for the fully qualified DNS name (FQDN) that clients use to access Oracle Portal. In the box, type the FQDN for your Oracle Portal deployment. Note that this FQDN should resolve to the virtual server on the BIG-IP system. In our example, we type **oracleportal.siterequest.com**.

- g) If you entered an HTTP request in step d, and want to enter a response string, type it here. This is optional.

Oracle Portal Server Load Balancing Questions	
What IP Address do you want to use for this Oracle Portal virtual server?	<input type="text" value="192.168.12.100"/>
Which load balancing method would you like to use?	<input type="text" value="Least Connections (member)"/>
Please add the servers that will comprise this virtual server (the virtual will not be available until at least one server is added):	Address: <input type="text" value="10.132.82.102"/> Service Port: <input type="text" value="7778"/> <input type="text" value="Select..."/> <input type="button" value="Add"/> <div style="border: 1px solid gray; padding: 2px;"> R:1 P:1 10.132.82.100 :7778 R:1 P:1 10.132.82.101 :7778 R:1 P:1 10.132.82.102 :7778 </div> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
How often should each Oracle Portal server's health be checked?	<input type="text" value="30"/> seconds
HTTP request that should be sent to check server health? (HTTP 1.1 headers will be automatically added.)	<input type="text" value="GET /"/>
What HTTP version do your Oracle Portal servers expect clients to use?	<input type="text" value="Version 1.1"/>
Fully qualified DNS name HTTP 1.1 clients are expected to use to access the Oracle Portal?	<input type="text" value="oracleportal.sitere"/>
String that should be contained within the health check response for the server to be considered healthy?	<input type="text"/>

Figure 1.4 *Configuring the Load Balancing options*

7. In the Protocol and Security Questions section, complete the following
 - a) If most clients will be connecting to the virtual server from a WAN, select **WAN** from the list. If most clients will be connecting from a LAN, select **LAN** from the list. This option determines the profile settings that control the behavior of a particular type of network traffic, such as HTTP connections.
 - b) If you want to use the WebAccelerator module to accelerate the Oracle traffic, select **Yes** from the list. If you do not want to use the WebAccelerator, select **No**. This option does not appear if you do not have the WebAccelerator module licensed. The WebAccelerator module can significantly improve performance for Oracle 10g R2 deployments.

- c) If you want to use the Application Security Manager to secure the Oracle traffic, select **Yes** from the list. If you do not want to use the Application Security Manager, select **No**. This option does not appear if you do not have the Application Security Manager (ASM) licensed. For more information, see the online help or the BIG-IP ASM documentation.
- d) If you are using the Application Security Manager, from the Language Encoding list, select the appropriate language. In our example, we leave this at the default, **Unicode (utf-8)**.
- e) If you are using the WebAccelerator module, in the **Host** box, type the fully qualified DNS name (FQDN) that your users will use to access the Oracle 10g R2 deployment (the WebAccelerator application object's Requested Hosts field). Click the **Add** button. If you have additional host names, type each one in the **Host** box, followed by clicking the **Add** button. In our example, we type **oracleportal.siterequest.com** and click the **Add** button.

Protocol Optimization and Security Questions	
Will clients be connecting to this virtual server primarily over a LAN or a WAN?	WAN
Would you like to use the Web Accelerator module to accelerate your Oracle Application Server traffic?	Yes
Would you like to use the Application Security Manager module to secure your Oracle Application Server traffic?	Yes
About ASM transparent mode:	Application Security Manager's policy enforcement mode will be set to transparent. In this mode, violations will be logged but not blocked. Before changing the mode to blocking, please review the log results and adjust the policy for your deployment if necessary.
What language encoding does your application use?	Unicode (utf-8)
Please enter the fully qualified DNS names your end users will use to access the Oracle Application Server Virtual Server (e.g., portal.oracle.f5.com).	Host: oracleportal.siterequest.com <input type="button" value="Add"/> <input type="text" value="oracleportal.siterequest.com"/> <input type="button" value="Delete"/>

Figure 1.5 Configuring the Optimization and Security settings

- 8. In the Oracle Single Sign On Server Load Balancing Questions section, if you want to load balance your Oracle SSO installation, select **Yes** from the list. If you do not want to load balance SSO, leave this option set to **No**, and continue with Step 9.
 - a) Enter the IP address for this virtual server. In our example, we type **192.168.14.110**.

-
- b) From the Certificate list, select the name of the certificate you want to use for the SSO configuration.
 - c) From the Key list, select the name of the key.
 - d) From the Load Balancing Method list, select an appropriate load balancing method. In our example, we leave this setting at the default, **Least Connections (member)**.
 - e) Next, add each of the Oracle Application Servers that are a part of this deployment.
In the **Address** box, type the IP address of the first Oracle 10g R2 server. In our example, we type **10.132.85.100**.
Important: In the **Service Port** box, change the port to **7777**. Click the **Add** button. Repeat this step for each of the Oracle SSO devices.
 - f) Next, type a number of seconds that the BIG-IP system issues the health check. In our example, we leave this at the default level, **30**.
 - g) If you have a specific HTTP request you would like to add to the health check, type it in the box after **GET /**. This is optional.
 - h) Select the HTTP version that the Oracle 10g R2 servers expect clients to use. In our example, we select **Version 1.1**.

If you specify HTTP version 1.1, a new row appears asking for the fully qualified DNS name (FQDN) that clients use to access Oracle Portal. In the box, type the FQDN for your Oracle Portal deployment. Note that this FQDN should resolve to the virtual server on the BIG-IP system. In our example, we type **oraclesso.siterequest.com**.

- i) If you entered an HTTP request in step d, and want to enter a response string, type it here. This is optional.

9. Click the **Finished** button.

After clicking Finished, the BIG-IP system creates the relevant objects. You see a summary screen that contains a list of all the objects that were created. Note that at least one OneConnect profile is created by template, but does not currently appear in the summary screen.

Be sure to continue with the following section for important changes to make on the Oracle devices.

Modifying the Oracle 10g R2 configuration

With the BIG-IP LTM configuration complete, there are now modifications to the Oracle 10g R2 configuration that need to be made in order for traffic to resolve and flow properly.

Modifying the Oracle 10g R2 Portal configuration

The first task is to modify the Oracle 10g R2 Portal configuration. To modify the 10g R2 Portal configuration, you need to perform the following procedures:

- *Disabling Web Cache*
- *Changing the default port*
- *Adding the virtual host entry for the BIG-IP LTM virtual server*
- *Making sure the server responds on port 80*

You must perform these procedures on each Oracle AS 10g R2 Portal server.

Disabling Web Cache

Because the caching duties in this configuration are handled by the BIG-IP LTM system, we disable the Oracle 10g R2 Web Cache. This frees the servers you would normally use for the Web Cache devices to run other Oracle applications.

To disable the Oracle Web Cache

1. Log on to your Oracle Application Server Portal GUI as an administrator.
2. Click the **Administer** tab.
3. Under the **Services** portlet, click **Global Settings**.
4. Click the **Cache** tab.
5. Clear the **Enable Web Cache For Caching Portal Content** box to disable the Web Cache.

6. Click the **Apply** button.

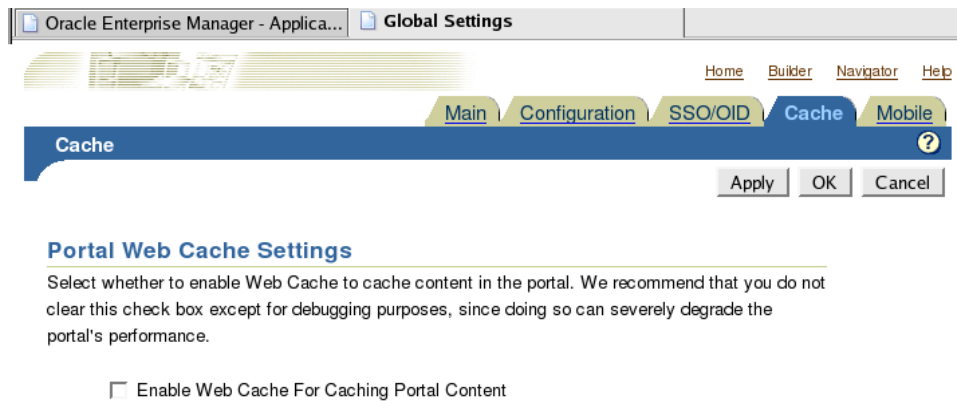


Figure 1.6 Disabling the Portal Web Cache

Changing the default port

The next step is to change the default port for the Oracle 10g R2 Portal server to **80**.

If you are using the BIG-IP LTM to offload SSL traffic, change the default port to **443**.

To change the default port

1. Log on to your Oracle Application Server Portal GUI through Enterprise Manager as an administrator.
2. Under System Components, click **HTTP Server**.
3. Click the Administration Tab.
4. Click the **Server Properties** link.
5. In the **Listening Addresses and Ports** section, change the default port to **80**. If you are using the BIG-IP LTM for SSL offload, change the port to **443**.

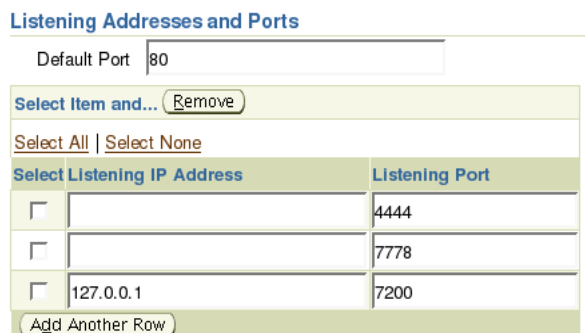


Figure 1.7 Changing the default port for Oracle 10g R2 Portal

6. Click the **Apply** button
7. At the prompt, click to restart the service.

Adding the virtual host entry for the BIG-IP LTM virtual server

The next step is to add a virtual host entry on the Oracle device for the BIG-IP LTM virtual server. This ensures that traffic is properly routed to the BIG-IP LTM system.

To add a virtual host entry

1. Log on to your Oracle Application Server Portal GUI through Enterprise Manager as an administrator.
(If you are already logged in, return to the **HTTP Server** page).
1. Under System Components, click **HTTP Server**.
2. Click the Virtual Hosts tab.
3. Click the **Create** button. The Create Virtual Host wizard opens.
 - a) In Step One of the virtual Host wizard, click **Next**.
 - b) In Step 2, make sure that the Virtual Host is set to **Name-based** (this is the default setting).
 - c) In Step 3, in the **Server Name** box, type the DNS name that resolves to the Oracle 10g R2 Portal virtual server on the BIG-IP LTM system, and then click the **Next** button.

Important: *This is not the name of the virtual server itself, it is the name that resolves to the virtual server in DNS; check with your DNS administrator*

Create Virtual Host: Addresses

[Cancel](#) [Back](#) [Step 3 of 7](#) [Next](#)

Enter the server name, server aliases, and IP address to be used with this name-based virtual host.

Server Name and Aliases

* Server Name

Select row and... [Remove](#)

Select All | Select None

Select Server Alias

[Add Another Row](#)

TIP Values entered for Server Name and Server Alias should be valid DNS names. If you set name1.mydomain.com as the Server Name, some typical Server Aliases include www.name1.mydomain.com and name1.

Figure 1.8 Adding the BIG-IP virtual server DNS name

-
- d) In Step 4, make sure that **Listen on a specific port** is selected. From the list, select **7778**. Click the **Next** button.

Create Virtual Host: Ports

Select the port setting which should be applied to the virtual host.

- Listen on all the main server ports
- Listen on a specific port
- Listen only on the main server default port

Figure 1.9 Selecting the Port

- e) In Step 6 (Step 5 does not appear), click **Next**.
- f) In Step 7, click **Finish**.
4. Restart the service by clicking **Yes** at the prompt.

Making sure the server responds on port 80

The next step is to configure the Oracle HTTP Server (OHS) so that it returns the correct URLs to the user on port 80. If you are using the BIG-IP LTM for SSL offload of the Portal servers, this is port 443.

This procedure must be performed from the command line.

To configure the Oracle service to respond on port 80

1. Log on to the Oracle 10g R2 Portal Server from the command line as the Oracle user.
2. Open the **httpd.conf** file (**\$ORACLE_HOME/Apache/Apache/conf/httpd.conf**) in a text editor, such as VI or PICO.
3. Find the **Virtual Host** entry at the bottom of the file.
4. Create a Port Directive for the virtual host by adding Port 80 to the entry (port 443 if the BIG-IP LTM system is offloading SSL from the Portal devices). Add the following:

Port 80

The entry should look like this when you are finished:

```
<VirtualHost *:7778>
    ServerName portal.oraclelearn.tc.f5net.com
    Port 80
</VirtualHost>
```

Note that the **ServerName** example above will be different in your deployment.

5. **Optional:** If you are using the BIG-IP LTM system to offload SSL from the Oracle 10g R2 Portal device, you need to add another line immediately following the line you just entered:

```
SimulateHttps on
```

So the final result of the Virtual Host entry for offloading SSL should look like:

```
<VirtualHost *:7778>  
  ServerName portal.oraclelearn.tc.f5net.com  
  Port 443  
  SimulateHttps on  
</VirtualHost>
```

You must also add the following LoadModule line at the end of the LoadModule entries in the **httpd.conf** file:

```
LoadModule certheaders_module libexec/mod_certheaders.so
```

6. Save and close the **httpd.conf** file.
7. Restart your web server. For simplicity, we recommend you restart the web server through the Oracle Enterprise Manager.

You must repeat all of these procedures for each Oracle 10g R2 Portal server in your configuration. Return to *Modifying the Oracle 10g R2 Portal configuration*, on page 10 to start again.

There is an additional procedure necessary if you are using the BIG-IP LTM for offloading SSL from the Oracle 10g R2 Portal devices, after completing the following section for Oracle Single Sign-On.

Modifying the Oracle 10g R2 Single Sign-On configuration

In the following procedures, we configure the Oracle 10g R2 SSO service to use the BIG-IP LTM system.

Deleting the SSO Partner Application

The first procedure in this configuration is to delete the SSO Partner Application, before adding it back. It is necessary to delete the SSO Partner application because the Site ID field is not editable, and the login URL will change.

To delete the SSO Partner Application

8. Log on to the Oracle 10g R2 Single Sign-On Server as an administrator.
9. Click the **Single Sign-On Server Administration** link.
10. Click the **Administer Partner Applications** link.
11. In the **Edit/Delete Partner Application** section, click the Delete button for the SSO Partner Application (**SSO Server (orasso)**).
12. On the Delete Partner Application confirmation page, click **OK**.

Configuring a new Single Sign-On URL for partner applications

The next step is to configure a new Single Sign-On URL for partner applications. This procedure requires a manual command line entry on Single Sign-On server.

◆ Tip

The following procedure is also a manual command line entry, so you can remain logged on to the command line after you complete this procedure.

To configure a new Single Sign-On URL

1. Log on to the Oracle Single Sign-On device from the command line as the Oracle user.
2. Type the following command to change directories:

```
cd $ORACLE_HOME/sso/bin
```

3. Use the following syntax to create the new URL:

```
./ssocfg.sh https <DNS name of LTM SSO virtual server> 443
```

For example:

```
./ssocfg.sh https login.oraclelearn.tc.f5net.com 443
```

Registering the SSO server as a Partner Application

The next step is to register the Single Sign-On server as a Partner Application. This procedure also requires a manual command line entry on Single Sign-On server. If you are already logged on from the previous procedure, you can skip to Step 3.

For more information on this command, see Oracle MetaLink article ID#315053.1

To register the SSO server as a partner application

1. Log on to the Oracle Single Sign-On device from the command line as the Oracle user.
2. Type the following command to change directories:

```
cd $ORACLE_HOME/sso/bin
```

3. Use the following syntax to create the new URL:

```
./ssoreg.sh -site_name 'SSO Server orasso' -mod_osso_url <DNS name of LTM SSO virtual server> -config_mod_osso TRUE -oracle_home_path $ORACLE_HOME -config_file $ORACLE_HOME/Apache/Apache/conf/osso/osso.conf -admin_info 'cn=orcladmin' -virtualhost
```

For example:

```
./ssoreg.sh -site_name 'SSO Server orasso' -mod_osso_url https://login.oraclelearn.tc.f5net.com -config_mod_osso TRUE -oracle_home_path $ORACLE_HOME -config_file $ORACLE_HOME/Apache/Apache/conf/osso/osso.conf -admin_info 'cn=orcladmin' -virtualhost
```

Changing the default port to port 443

The next procedure is to change the default port of the Single Sign-On Server to port 443. For more information on this procedure, see Oracle MetaLink ID #315200.1.

To change the default port

1. Log on to your Oracle Application Server SSO Infrastructure GUI through Enterprise Manager as an administrator.
2. Under System Components, click **HTTP Server**.
3. Click the Administration Tab.
4. Click the **Server Properties** link.
5. In the Listening Addresses and Ports section, change the default port to **443**.
6. Click the **Apply** button
7. At the prompt, click to restart the service.

Adding the virtual host entry for the BIG-IP LTM virtual server

The next step is to add a virtual host entry on the Oracle device for the BIG-IP LTM virtual server.

To add a virtual host entry

1. Log on to your Oracle SSO GUI through Enterprise Manager as an administrator.
If you are already logged in, return to the HTTP Server page.
1. Under System Components, click **HTTP Server**.
2. Click the Virtual Hosts tab.
3. Click the **Create** button. The Create Virtual Host wizard opens.
 - a) In Step One of the virtual Host wizard, click **Next**.
 - b) In Step 2, make sure that the Virtual Host is set to **name-based** (this is the default setting).
 - c) In Step 3, in the Server Name box, type the DNS name that resolves to the virtual server on the BIG-IP LTM system for Single Sign On.
 - d) In Step 4, make sure that **Listen on specific port** is selected. From the list, select **7777**.
 - e) In Step 6 (Step 5 does not appear), click **Next**.
 - f) In Step 7, click **Finish**.
4. Restart the service by clicking **Yes** at the prompt.

Making sure the server responds on port 443

The next step is to configure the Oracle 10g R2 SSO device to respond on port 443. If you do not make this change, the URLs will retain the original port (such as 7777).

This procedure must be performed from the command line.

To configure the Oracle service to respond on port 443

1. Log on to the Oracle device from the command line as an administrator.
2. Open the **httpd.conf** file (**\$ORACLE_HOME/Apache/Apache/conf/httpd.conf**) in a text editor, such as VI or PICO.
3. Find the end of the **LoadModule** entries, and add the following line:

```
LoadModule certheaders_module libexec/mod_certheaders.so
```

We load this file in order for the **SimulateHttps on** directive to work in the **VirtualHost** directive in the following step.

4. Find the **Virtual Host** entry at the bottom of the file, and add the following lines to the **Virtual Host** entry:

```
Port 443
SimulateHttps on
```

So the final result if you are offloading SSL should look like:

```
<VirtualHost *:7777>
    ServerName login.oraclearn.tc.f5net.com
    Port 443
    SimulateHttps on
</VirtualHost>
```

5. Save and close the **httpd.conf** file.
6. Restart your web server. We recommend you restart the web server through the Oracle Enterprise Manager

Configuring the SSO URL for Oracle DAS

In this section, we configure the new SSO url for Oracle Directory Administration Server (DAS). You can find more information on this procedure in Oracle Metalink Article ID#302634.1

To configure the SSL URL for Oracle DAS

1. Login to Oracle Directory Manager (OID console).
2. Navigate to the following directory:

```
Oracle Internet Directory Servers
cn=orcladmin@OID_hostname:OID_port
Entry Management
cn=OracleContext
```

cn=Products
cn=DAS
cn=OperationalURLs

3. Under the property **orclidasurlbase**, replace the URL with the name that resolves to the SSO virtual server on the BIG-LTM in DNS (see Figure 1.10).
4. Click **Apply**.
5. Restart the Single Sign-On server.

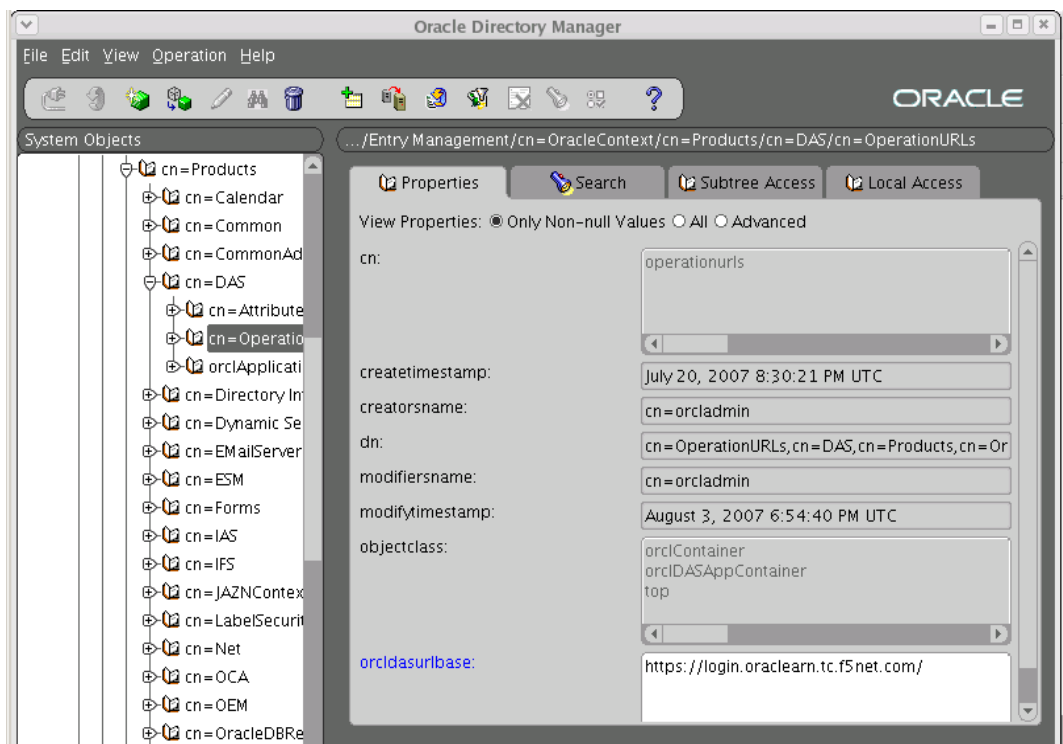


Figure 1.10 Adding the DNS name of the SSO virtual server to Oracle DAS

Configuring Oracle 10g R2 Portal to use the new SSO URL

Now that we have successfully configured Oracle 10g R2 Portal and Single Sign-On with URLs that are direct traffic through the BIG-IP LTM system, we need to configure the Oracle 10g R2 Portal servers to use the new SSL-enabled SSO URL (the name that resolves to the SSO virtual server on the BIG-LTM in DNS).

To add the SSO URL to the 10g R2 Portal configuration

1. Log on to your Oracle Single Sign-On server, using the new Single Sign-On URL (the URL that resolves to the SSO virtual server on the BIG-IP LTM).
2. Click the **Single Sign-On Server Administration** link.
3. Click the **Administer Partner Applications** link.
4. In the **Edit/Delete Partner Application** section, click the Delete button for the Portal Partner Application (**Oracle Portal (portal)**).
5. On the Delete Partner Application confirmation page, click **OK**.

Registering the Portal server as a Partner Application

The final procedure is to (re)register the Portal server as a Partner Application. This procedure also requires a manual command line entry on Single Sign-On server. If you are already logged on from the previous procedure, you can skip to Step 3.

To register the Portal server as a Partner Application

1. Log on to the Oracle Single Sign-On device from the command line as an administrator.
2. Type the following command to change directories:
`cd $ORACLE_HOME/portal/conf`
3. Use the following syntax to create the new URL:

```
./ptlconfig -dad portal -sso -host <DNS name of BIG-IP LTM Portal virtual server> -port 80
```

For example:

```
./ptlconfig -dad portal -sso -host portal.oraclelearn.tc.f5net.com -port 80
```

4. Optional: If you configured the BIG-IP LTM system to offload SSL from the Portal devices, the port in the preceding command would be 443. For example:

```
./ptlconfig -dad portal -sso -host portal.oraclelearn.tc.f5net.com -port 443
```

After completing the Oracle 10g R2 modifications, log on to Enterprise Manager for the Oracle 10g R2 Portal and restart all services. You must restart each Portal server, however you only need to run this command on one server.

SSL Certificates on the BIG-IP system

Before you can enable the BIG-IP LTM system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for Oracle 10g R2 connections on the BIG-IP LTM device. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP LTM system. For information on generating certificates, or using the BIG-IP LTM to generate a request for a new certificate and key from a certificate authority, see the **Managing SSL Traffic** chapter in the *Configuration Guide for Local Traffic Management*.

Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP LTM system using the Configuration utility. By importing a certificate or archive into the Configuration utility, you ease the task of managing that certificate or archive. You can use the Import SSL Certificates and Keys screen only when the certificate you are importing is in Privacy Enhanced Mail (PEM) format.

To import a key or certificate

1. On the Main tab, expand **Local Traffic**.
2. Click **SSL Certificates**. The list of existing certificates displays.
3. In the upper right corner of the screen, click **Import**.
4. From the **Import Type** list, select the type of import (Certificate or Key).
5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
7. Click **Import**.

If you imported the certificate, repeat this procedure for the key.

This completes the configuration.



2

Manually Configuring the BIG-IP LTM System with Oracle 10g R2

- Configuring the BIG-IP LTM for Oracle 10g R2 Portal
- Configuring the BIG-IP LTM for Oracle 10g R2 Single Sign-On server

Manually creating the BIG-IP LTM configuration

While we recommend using the application template, if you prefer to manually configure the BIG-IP LTM system rather than use the application template, use the following procedures.

Be sure to follow the procedures in *Modifying the Oracle 10g R2 configuration*, on page 1-9 after completing the BIG-IP configuration.

Configuring the BIG-IP LTM for Oracle 10g R2 Portal

In this section, we configure the BIG-IP LTM system to direct traffic to the Oracle 10g R2 Portal devices. After completing the BIG-IP LTM configuration, there are additional procedures to perform on the Oracle 10g R2 portal devices.

To configure the BIG-IP LTM system for the Oracle Portal, you must complete the following procedures:

- *Creating a HTTP health monitor*
- *Creating the Oracle 10g R2 Portal pool*
- *Creating Oracle 10g R2 Portal profiles*
- *Creating the Oracle 10g R2 Portal virtual server*
- *Optional: Configuring the BIG-IP LTM to offload SSL*

Creating a HTTP health monitor

The first step is to set up a health monitor for the Oracle Portal devices. This procedure is optional, but very strongly recommended. For this configuration, we create a simple HTTP health monitor. Although the monitor in the following example is quite simple, you can configure optional settings such as Send and Receive Strings to make the monitor much more specific.

To configure a HTTP health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
The Monitors screen opens.
2. Click the **Create** button.
The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor.
In our example, we type **oracle10g-portal-http**.
4. From the **Type** list, select **HTTP**.
The HTTP Monitor configuration options appear.

5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91**.
6. In the Send String and Receive Rule sections, you can add an optional Send String and Receive Rule specific to the device being checked.
7. Click the **Finished** button.
The new monitor is added to the Monitor list.

The screenshot shows the 'New Monitor...' configuration page. The breadcrumb trail is 'Local Traffic » Monitors » New Monitor...'. The 'General Properties' section includes:

- Name: oracle10g-portal-http
- Type: HTTP
- Import Settings: http

 The 'Configuration' section is set to 'Basic' and includes:

- Interval: 30 seconds
- Timeout: 91 seconds
- Send String: GET /
- Receive String: (empty)
- User Name: (empty)
- Password: (empty)
- Reverse: Yes No
- Transparent: Yes No

 At the bottom, there are buttons for 'Cancel', 'Repeat', and 'Finished'.

Figure 2.1 Creating the HTTP Monitor

Creating the Oracle I0g R2 Portal pool

The next step is to create a pool on the BIG-IP LTM system for the Oracle 10g R2 Portal devices. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method.

To create the Oracle I0g R2 Portal pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**.
The Pool screen opens.

-
2. In the upper right portion of the screen, click the **Create** button. The New Pool screen opens.

*Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.*

3. In the **Name** box, enter a name for your pool.
In our example, we use **oracle10g-portal**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating a HTTP health monitor* section, and click the Add (<<) button. In our example, we select **oracle10g-portal-http**.
5. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
In our example, we select **Least Connections (member)**.
6. For this pool, we leave the Priority Group Activation **Disabled**.
7. In the New Members section, make sure the **New Address** option button is selected.
8. In the **Address** box, add the first server to the pool. In our example, we type **10.133.17.110**.
9. In the **Service Port** box, type the appropriate port for your Portal server.
In our example, we type **7778**, the default port for Oracle 10g R2 Portal.
10. Click the **Add** button to add the member to the list.
11. Repeat steps 9-11 for each server you want to add to the pool.
12. Click the **Finished** button (see Figure 2.2).

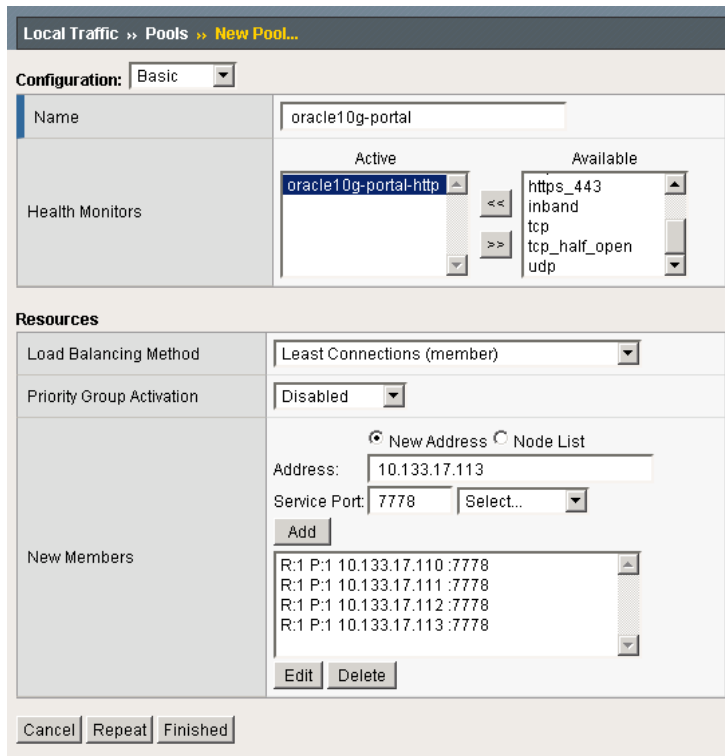


Figure 2.2 Creating the pool for the Oracle 10g R2 Portal

Creating Oracle 10g R2 Portal profiles

BIG-IP version 9.0 and later use profiles. A *profile* is an object that contains user-configurable settings for controlling the behavior of a particular type of network traffic, such as HTTP connections. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Although it is possible to use the default profiles, we strongly recommend you create new profiles based on the default parent profiles, even if you do not change any of the settings initially. Creating new profiles allows you to easily modify the profile settings specific to this deployment, and ensures you do not accidentally overwrite the default profile.

Creating an HTTP profile

The first new profile we create is an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic. In the following example, we base our HTTP profile off of the **http-acceleration** parent profile, as we are using the WebAccelerator. If you are not using the WebAccelerator, we recommend using the **http-wan-optimized-compression-caching** parent.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **oracle10g-http-opt**.
4. From the **Parent Profile** list, select **http-acceleration** if you are using the WebAccelerator. If you are not using the WebAccelerator, select **http-wan-optimized-compression-caching**. The profile settings appear.
5. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
6. Click the **Finished** button.

Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the Oracle 10g R2 Portal users are accessing the portal via a Local Area Network, we recommend using the **tcp-lan-optimized** (for server-side TCP connections) parent profile. If the majority of the Portal users are accessing the system from remote or home offices, we recommend using an additional TCP profile, called **tcp-wan-optimized** (for client side TCP connections). In our example, we leave these profiles at their default levels; you can configure any of the options as applicable for your network.

Creating the LAN optimized TCP profile

First we configure the LAN optimized profile. If you do not want to use this optimized profile, you can choose the default TCP parent profile.

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **oracle10g-tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the WAN optimized TCP profile

Now we configure the WAN optimized profile. Remember, if most of the users are accessing the system over the LAN or other low latency links, you do not need to create this profile.

To create a new TCP WAN optimized profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **oracle10g-tcp-wan**.
5. From the **Parent Profile** list, select **tcp-wan-optimized**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating persistence profile

The final profile we create is a Persistence profile. We recommend using persistence for the Oracle Web Tier, although the type of persistence depends on your configuration. In our example, use cookie persistence (HTTP cookie insert).

To create a new cookie persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, click **Persistence**. The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button. The New Persistence Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **oracle10g-cookie**.
5. From the **Persistence Type** list, select **Cookie**. The configuration options for cookie persistence appear.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.

7. Click the **Finished** button.

General Properties	
Name	oracle10g-cookie
Persistence Type	Cookie
Parent Profile	cookie

Configuration		Custom <input type="checkbox"/>
Cookie Method	HTTP Cookie Insert	<input type="checkbox"/>
Cookie Name		<input type="checkbox"/>
Expiration	<input checked="" type="checkbox"/> Session Cookie	<input type="checkbox"/>
Override Connection Limit	<input type="checkbox"/>	<input type="checkbox"/>

Cancel Repeat Finished

Figure 2.3 Creating the cookie persistence profile

Creating a OneConnect profile

The next profile we create is a OneConnect profile. With OneConnect enabled, client requests can utilize existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. This can provide significant performance improvements for Oracle implementations. For more information on OneConnect, see the BIG-IP LTM documentation.

In our example, we leave all the options at their default settings. You can configure these options as appropriate for your network.

To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Other** menu, click **OneConnect**. The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **oracle10g-oneconnect**.
5. From the **Parent Profile** list, ensure that **oneconnect** is selected.
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the Oracle I0g R2 Portal virtual server

Next, we configure a virtual server that references the profiles and pool you created in the preceding procedures.

To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
The Virtual Servers screen opens.
2. In the upper right portion of the screen, click the **Create** button.
The New Virtual Server screen opens.
3. In the **Name** box, type a name for this virtual server. In our example, we type **oracle10g-portal-vs**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.100.201**.
6. In the **Service Port** box, type **80**.

General Properties	
Name	oracle10g-portal-vs
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.133.100.201
Service Port	80 HTTP
State	Enabled

Figure 2.4 Creating the Oracle Portal virtual server

7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. Leave the **Type** list at the default setting: **Standard**.
9. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. If you did not create a WAN optimized profile, select the LAN optimized profile as in the following Step. In our example, we select **oracle10g-tcp-wan**.
10. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **oracle10g-tcp-lan**.
11. From the **OneConnect Profile** list, select the name of the profile you created in *Creating a OneConnect profile*. In our example, we select **oracle10g-oneconnect**.

- From the HTTP Profile list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **oracle10g-http-opt** (see Figure 2.5).

The screenshot shows a configuration window with a 'Configuration:' dropdown set to 'Advanced'. Below it is a table of settings:

Type	Standard
Protocol	TCP
Protocol Profile (Client)	oracle10g-tcp-wan
Protocol Profile (Server)	oracle10g-tcp-lan
OneConnect Profile	oracle10g-oneconnect
HTTP Profile	oracle10g-http-opt
FTP Profile	None

Figure 2.5 Selecting the Oracle 10g R2 profiles for the virtual server

- In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the Oracle 10g R2 Portal pool* section. In our example, we select **oracle10g-portal-http**.
- From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating persistence profile* section. In our example, we select **oracle10g-cookie**.

The screenshot shows a dialog box with three rows of settings:

Default Pool	+	oracle10g-portal
Default Persistence Profile		oracle10g-cookie
Fallback Persistence Profile		None

At the bottom, there are three buttons: Cancel, Repeat, and Finished.

Figure 2.6 Adding the Pool and Persistence profile to the virtual server

- Click the **Finished** button.
The BIG-IP LTM configuration for the Oracle Portal configuration is now complete.

◆ Important

*After completing the BIG-IP LTM configuration, there are changes you need to make for Oracle 10g R2 Portal in Oracle configuration. We recommend completely configuring the BIG-IP LTM system before making changes to the Oracle configuration. When you have completed the BIG-IP LTM configuration, see **Modifying the Oracle 10g R2 configuration**, on page 1-9.*

Optional: Configuring the BIG-IP LTM to offload SSL

If you are using the BIG-IP LTM system to offload SSL from the Oracle 10g R2 Portal devices, there are additional configuration procedures you must perform on the BIG-IP LTM system.

Using SSL certificates and keys

Before you can enable the BIG-IP LTM system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for Oracle 10g R2 connections on the BIG-IP LTM device. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP LTM system. For information on generating certificates, or using the BIG-IP LTM to generate a request for a new certificate and key from a certificate authority, see the **Managing SSL Traffic** chapter in the *Configuration Guide for Local Traffic Management*.

Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP LTM system using the Configuration utility. By importing a certificate or archive into the Configuration utility, you ease the task of managing that certificate or archive. You can use the Import SSL Certificates and Keys screen only when the certificate you are importing is in Privacy Enhanced Mail (PEM) format.

To import a key or certificate

1. On the Main tab, expand **Local Traffic**.
2. Click **SSL Certificates**. The list of existing certificates displays.
3. In the upper right corner of the screen, click **Import**.
4. From the **Import Type** list, select the type of import (Certificate or Key).
5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
7. Click **Import**.

If you imported the certificate, repeat this procedure for the key.

Creating a Client SSL profile

The next step in this configuration is to create a Client SSL profile. This profile contains the SSL certificate and Key information for offloading the SSL traffic.

To create a new Client SSL profile based on the default profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.
The HTTP Profiles screen opens.
3. On the Menu bar, from the SSL menu, select **Client**.
The Client SSL Profiles screen opens.
4. In the upper right portion of the screen, click the **Create** button.
The New Client SSL Profile screen opens.
5. In the **Name** box, type a name for this profile. In our example, we type **oracle10g-clientssl**.
6. In the Configuration section, check the **Certificate** and **Key Custom** boxes.
7. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
8. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
9. Click the **Finished** button.

Modifying the Oracle 10g R2 Portal virtual server

The next task is to modify the Oracle 10g R2 Portal virtual server you created to use the SSL profile you just created.

To modify the existing Oracle 10g R2 Portal virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the Virtual Server list, click the Oracle Portal virtual server you created in *Creating the Oracle 10g R2 Portal virtual server*, on page 2-8. In our example, we click **oracle10g-portal-vs**.
3. In the **Service Port** box, type **443**, or select HTTPS from the list.
4. From the **SSL Profile (Client)** list, select the name of the profile you created in *Creating a Client SSL profile*, on page 2-10. In our example, we select **oracle10g-clientssl**.
5. Click the **Update** button.

If you are using the BIG-IP LTM system to offload SSL from Oracle 10g R2 Portal devices, make sure to follow the notes about SSL offload when performing the Oracle configuration modifications in *Modifying the Oracle 10g R2 configuration*, on page 1-9

Configuring the BIG-IP LTM for Oracle 10g R2 Single Sign-On server

The next group of objects we configure on the BIG-IP LTM system is for the Oracle 10g R2 Single Sign-On (SSO) devices. The BIG-IP LTM configuration for SSO is very similar to the configuration for portal, so in the following sections, we reference the procedures from the Portal section.

You must configure the following objects on the BIG-IP LTM system:

- *Creating a HTTP health monitor*
- *Creating the pool*
- *Creating the Profiles*
- *Creating the Single Sign-On virtual server*

In many cases, you can use the same objects for both Oracle Portal and Oracle SSO (such as the health monitor and profiles), however, we strongly recommend you create new objects for each Oracle component.

Creating a HTTP health monitor

The first task is to create a health monitor for the SSO devices. Follow the procedure *Creating a HTTP health monitor*, on page 2-1. Use a unique name for the monitor, and use the same a 1:3 +1 ratio between the interval and the timeout. All other settings are optional, configure as applicable for your configuration.

Creating the pool

The next task is to create a pool for the SSO devices. Follow the procedure *Creating the Oracle 10g R2 Portal pool*, on page 2-2. Type a unique name for the pool, configure the pool to use the health monitor you just created, and add the appropriate SSO address and port. All other settings are optional, configure as applicable for your configuration.

Creating the Profiles

As with the Portal configuration, you create the five profiles for Oracle Single Sign-On: HTTP, two TCP profiles, OneConnect, and Persistence. However, because Single Sign-On should be over SSL, you need to create a Client SSL profile as well.

You can use the same profiles you created for the Portal configuration, but we strongly recommend you create new profiles. By creating new profiles for each Oracle component, it makes it much easier to fine tune optimization and other settings for specific applications.

Create all five profiles in *Creating Oracle 10g R2 Portal profiles*, on page 2-4, giving each a unique name. You can change any of the options as applicable for your network.

Additionally, follow the procedure *Creating a Client SSL profile*, on page 2-10. If you are importing a new certificate and key, follow *Importing keys and certificates*, on page 2-10.

Creating the Single Sign-On virtual server

The final step is to create a virtual server for the Oracle SSO devices. Follow the procedure *Creating the Oracle 10g R2 Portal virtual server*, on page 2-8. Give this virtual server a unique name, and use the appropriate address and port (**443**), and configure the virtual server to use all of the objects you created in the preceding procedures.

This completes the manual configuration for the BIG-IP LTM.



3

Manually Configuring the BIG-IP LTM System with Oracle 10g R2

- Creating an HTTP Class profile
- Modifying the Virtual Server to use the Class profile
- Creating an Application

Manually Configuring the F5 WebAccelerator module

F5 WebAccelerator module is an advanced web application delivery solution that provides a series of intelligent technologies designed to overcome problems with browsers, web application platforms and WAN latency issues which impact user performance.

To configure the WebAccelerator module, you must create an HTTP Class profile, modify the virtual server to use this profile, and create an Application on the WebAccelerator module.

Prerequisites and configuration notes

The following are prerequisites for this section:

- ◆ We assume that you have already configured the BIG-IP LTM system for directing traffic to the Oracle 10g R2 devices as described in this Deployment Guide.
- ◆ You must have purchased and licensed the WebAccelerator module on the BIG-IP LTM system.
- ◆ You must have created an HTTP profile on the BIG-IP LTM system that has RAM Cache enabled. In our example (*Creating an HTTP profile*, on page 2-4) we use a parent profile that includes RAM Cache. If you did not create an HTTP profile with RAM Cache enabled, you must create a new HTTP profile, based on a parent profile that uses RAM Cache (we recommend HTTP Acceleration) and associate it with the virtual server.
- ◆ This document is written with the assumption that you are familiar with the BIG-IP LTM system, WebAccelerator and Oracle 10g R2. Consult the appropriate documentation for detailed information.

Configuration example

Using the configuration in this section, the BIG-IP LTM system with WebAccelerator module is optimally configured to accelerate traffic to Oracle Application Server 10g R2 devices. The BIG-IP LTM with WebAccelerator module both increases end user performance as well as offloads the servers from serving repetitive and duplicate content.

In this configuration, a remote client with WAN latency accesses Oracle 10g R2 via the WebAccelerator. The user's request is accelerated on repeat visits by the WebAccelerator instructing the browser to use the dynamic or static object that is stored in its local cache. Additionally, dynamic and static objects are cached at the WebAccelerator so that they can be served quickly without requiring the server to re-serve the same objects.

Configuring the WebAccelerator module

Configuring the WebAccelerator module requires creating an HTTP class profile, creating an Application, and modifying the BIG-IP LTM virtual server to use the HTTP class. The WebAccelerator device has a large number of other features and options for fine tuning performance gains, see the *WebAccelerator Administrator Guide* for more information.

Creating an HTTP Class profile

The first procedure is to create an HTTP class profile. When incoming HTTP traffic matches the criteria you specify in the WebAccelerator class, the system diverts the traffic through this class. In the following example, we create a new HTTP class profile, based on the default profile.

To create a new HTTP class profile

1. On the Main tab, expand **WebAccelerator**, and then click **Classes**. The HTTP Class Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New HTTP Class Profile screen opens.
3. In the **Name** box, type a name for this Class. In our example, we type **oracle10g**.
4. From the Parent Profile list, make sure **httpclass** is selected.
5. In the Configuration section, from the **WebAccelerator** row, make sure **Enabled** is selected.
6. In the Hosts row, from the list select **Match Only**. The Host List options appear.
 - a) In the **Host** box, type the domain name (FQDN) of your Oracle 10g R2 Portal virtual server. In our example, we type **oracleportal.siterequest.com** (see Figure 3.1).
 - b) Leave the Entry Type at **Pattern String**.
 - c) Click the **Add** button.
 - d) Repeat these sub-steps for any other hosts.
7. The rest of the settings are optional, configure them as applicable for your deployment.
8. Click the **Finished** button. The new HTTP class is added to the list.

Local Traffic » Profiles : Protocol : HTTP Class » **New HTTP Class Profile...**

General Properties

Name	oracle10g
Parent Profile	httpclass

Configuration Custom

WebAccelerator	Enabled	<input checked="" type="checkbox"/>
Application Security	Disabled	<input type="checkbox"/>
Hosts	Match only...	<input checked="" type="checkbox"/>
Host List	Host: oracleportal.siterequest.com Entry Type: Pattern String <input type="button" value="Add"/> <div style="border: 1px solid gray; padding: 2px;">oracleportal.siterequest.com</div> <input type="button" value="Delete"/>	
URI Paths	Match all	<input type="checkbox"/>
Headers	Match all	<input type="checkbox"/>
Cookies	Match all	<input type="checkbox"/>

Actions Custom

Send To	None	<input type="checkbox"/>
Rewrite URI		<input type="checkbox"/>

Figure 3.1 Creating a new HTTP Class profile

Modifying the Virtual Server to use the Class profile

The next step is to modify the virtual server on the BIG-IP LTM system to use the HTTP Class profile you just created.

To modify the Virtual Server to use the Class profile

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the **Virtual Server** list, click the name of the virtual server you created for the Oracle 10g R2 Portal in *Creating the Oracle 10g R2 Portal virtual server*, on page 2-8. In our example, we click **oracle10g-portal-vs**.
The General Properties screen for the Virtual Server opens.

3. On the Menu bar, click **Resources**.
The Resources screen for the Virtual Server opens.
4. In the HTTP Class Profiles section, click the **Manage** button.
5. From the **Available** list, select the name of the HTTP Class Profile you created in the preceding procedure, and click the Add (<<) button to move it to the Enabled box. In our example, we select **oracle10g** (see Figure 3.2).
6. Click the **Finished** button. The HTTP Class Profile is now associated with the Virtual Server.

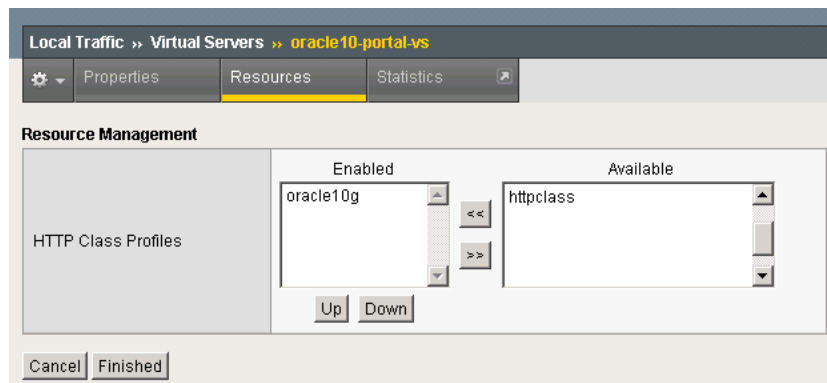


Figure 3.2 Adding the HTTP Class Profile to the Virtual Server

◆ Important

You must have created an HTTP profile on the BIG-IP LTM system that has RAM Cache enabled. In our example (**Creating an HTTP profile**, on page 2-4) we use a parent profile that includes RAM Cache. If you did not create an HTTP profile with RAM Cache enabled, you must create a new HTTP profile, based on a parent profile that uses RAM Cache (such as HTTP Acceleration), and modify the virtual server to use this new profile.

To create the HTTP profile, use **Creating an HTTP profile**, on page 2-4, selecting the HTTP Acceleration parent profile. You must leave RAM Cache enabled; all other settings are optional. To modify the virtual server, follow Steps 1 and 2 from the preceding procedure to access the virtual server, and then from the HTTP Profile list, select the name of the new profile you just created and click **Update**.

Creating an Application

The next procedure is to create a WebAccelerator Application. The Application provides key information to the WebAccelerator so that it can handle requests to your application appropriately.

To create a new Application

1. On the Main tab, expand **WebAccelerator**, and then click **Applications**.
The Application screen of the WebAccelerator UI opens in a new window.
2. Click the **New Application** button.
3. In the Application Name box, type a name for your application.
In our example, we type **oracle-10g**.
4. In the **Description** box, you can optionally type a description for this application.
5. From the **Local Policies** list, select **Oracle AS 10g Portal**. This is a pre-defined policy created specifically for Oracle devices.
6. In the **Requested Host** box, type the domain name (FQDN) of your Oracle Portal virtual server. In our example, we type **oracleportal.siterequest.com**. This should be the same host name you used in Step 6a in the *Creating an HTTP Class profile* procedure. If you have any other hosts, click the Add Host button, and type the name. Repeat as necessary.
7. Click the **Save** button.

The screenshot displays the 'New Application' configuration interface. At the top, the breadcrumb navigation reads 'Configuration >> Applications >> New Application'. The form is organized into several sections:

- General Options:** Contains 'Application Name' (text input: oracle-10g) and 'Description (optional)' (text area: WebAccelerator application for Oracle 10g).
- Policies:** Contains 'Central Policy' (dropdown menu: Oracle AS 10g Portal) and 'Remote Policy' (dropdown menu: - Select One -).
- Hosts:** A table with two columns: 'Requested Host' and 'Action'. One row is present with 'Requested Host' as 'oracleportal.siterequest.com' and 'Action' as 'Options | Delete'.

At the bottom right, there are three buttons: 'Add Host', 'Save' (highlighted in yellow), and 'Cancel'.

Figure 3.3 Configuring an Application on the WebAccelerator

The rest of the configuration options on the WebAccelerator are optional, configure these as applicable for your network. With this base configuration, your end users will notice a marked improvement in performance after their first visit.