DEPLOYMENT GUIDE

DEPLOYING F5 WITH ORACLE ACCESS MANAGER

Introducing the F5 and Oracle Access Manager configuration

Welcome to the F5 and Oracle® Access Manager Deployment Guide. This guide provides step-by-step procedures on configuring the BIG-IP LTM and FirePass controller with Oracle Access Manager.

Oracle Access Manager helps enterprises create greater levels of business agility, ensure seamless business partner integration, and enable regulatory compliance. Through an innovative, integrated architecture Oracle Access Manager uniquely combines identity management and access control services to provide centralized authentication, policy-based authorizations, and auditing with rich identity administration functionality such as delegated administration and workflows.

For more information on Oracle Access Manager, see **www.oracle.com/technology/products/id_mgmt/coreid_acc/index.html**.

For more information on F5 products, see **http://www.f5.com/products/**.

This Deployment Guide contains sections for configuring the BIG-IP LTM system, the FirePass controller, and Oracle Access Manager. While we recommend using all of these products together, it is not required. Simply use the sections for the products you have.

- *Configuring the BIG-IP LTM system for deployment with Oracle Access Manager*, on page 3
- *Modifying the Oracle Access Manager configuration*, on page 21
- *Deploying the FirePass controller with Oracle Access Manager*, on page 30

Prerequisites and configuration notes

The following are general prerequisites for this deployment; each section contains specific prerequisites:

- You must have an existing Oracle Access Manager deployment.
- This guide was tested using Oracle Access Manager version 10.1.4.0.1, BIG-IP LTM version 9.4.4, and FirePass controller version 6.0.1.
- This guide contains configuration procedures for both F5 devices and the Oracle devices. You must have administrative access to all devices.
- The Oracle Access Manager configuration in our testing was based off of the ***Oracle Application Server Enterprise Deployment Guide***.
- Although configuring the BIG-IP LTM system for Oracle Internet Directory (OID) devices is not a part of this guide, *Appendix A* contains procedures to perform on the Oracle Access Manager devices if you are using the BIG-IP LTM system in front of your OID devices. See *Appendix A: Modifying the Oracle configuration if a BIG-IP LTM system is in front of Oracle Internet Directory (OID)*, on page 34.

- Appendix B contains information on integrating an Oracle Application Server 10g Portal installation with Oracle Access Manager though the BIG-IP LTM as opposed to Oracle Single Sign On. See *Appendix B: Integrating Oracle Portal with Oracle Access Manager through the BIG-IP LTM*, on page 37. For information on configuring Oracle Application Server 10g Portal with the BIG-IP LTM system, see **http://www.f5.com/pdf/deployment-guides/f5-oracle10g-dg.pdf**

Configuration example

The BIG-IP LTM system provides intelligent traffic management, fail-over, and simple scalability for Oracle Access Manager devices. Through advanced health checking capabilities, the BIG-IP LTM recognizes when resources are unavailable or under-performing and directs traffic to another resource. The FirePass controller is configured to authenticate against the Oracle Access Manager Single Sign On system to simplify access and provide single sign on.

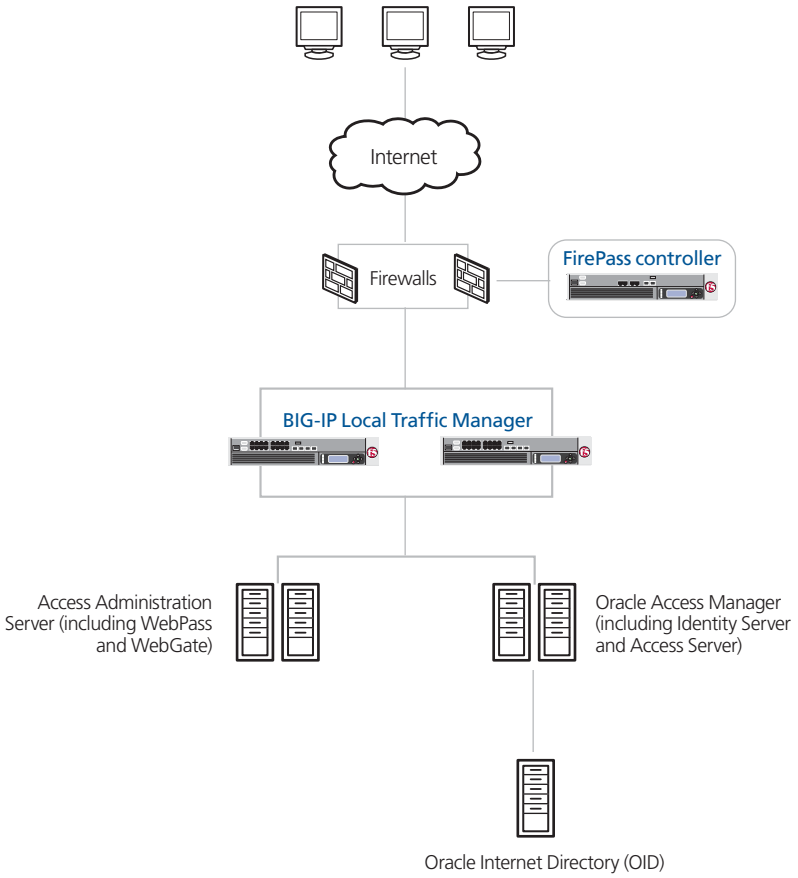

Figure 1 *F5 - Oracle Access Manager logical configuration example*

Configuring the BIG-IP LTM system for deployment with Oracle Access Manager

To configure the BIG-IP LTM system for directing traffic to the Oracle servers, you need to complete the following procedures:

- *Configuring the BIG-IP LTM for Oracle Access Manager Access Administration servers*, on page 4
- *Configuring the BIG-IP LTM for the Identity Server component of Oracle Access Manager*, on page 17
- *Configuring the BIG-IP LTM for the Access Server component of Oracle Access Manager*, on page 19
- *Modifying the Oracle Access Manager configuration*, on page 21

Tip

We recommend you save your existing BIG-IP configuration before you begin the procedures in this Deployment Guide. To save your BIG-IP configuration, see ***Appendix C: Backing up and restoring the BIG-IP LTM configuration****, on page 39.*

The BIG-IP LTM system offers both web-based and command line configuration tools, so that users can work in the environment that they are most comfortable with. This Deployment Guide contains procedures to configure the BIG-IP system using the BIG-IP web-based Configuration utility only. If you are familiar with using the **bigpipe** command line interface you can use the command line to configure the BIG-IP device, however, we recommend using the Configuration utility.

Prerequisites and configuration notes

The following are prerequisites this section of the Deployment Guide.

- This section contains configuration procedures for both F5 devices and the Oracle devices. You must have administrative access to all devices.
- The BIG-IP LTM system should be running version 9.4 or later. If you are using a previous 9.x version, the procedures in this Deployment Guide are valid, however some of the examples in this guide use optimized parent profiles introduced in version 9.4 and later.
  To use these profiles you must either be running LTM version 9.4, or refer to the ***Configuration Guide for BIG-IP Local Traffic Management*** for version 9.4 (available on Ask F5), which shows the differences between the base profiles and the optimized profile types.

Note

This document is written with the assumption that you are familiar with both the BIG-IP LTM system and Oracle Access Manager. For more information on configuring these products, consult the appropriate documentation.

Connecting to the BIG-IP LTM device

Use the following procedure to access the BIG-IP LTM web-based Configuration utility using a web browser.

To connect to the BIG-IP system using the Configuration utility

1. In a browser, type the following URL:
   https://<administrative IP address of the BIG-IP device>
   A Security Alert dialog box appears, click **Yes**.
   The authorization dialog box appears.
2. Type your user name and password, and click **OK**.
   The Welcome screen opens.

Once you are logged onto the BIG-IP system, the Welcome screen of the new Configuration utility opens. From the Configuration utility, you can configure and monitor the BIG-IP system, as well as access online help, download SNMP MIBs and Plug-ins, and even search for specific objects.

Configuring the BIG-IP LTM for Oracle Access Manager Access Administration servers

In this section, we configure the BIG-IP LTM system to direct traffic to the Oracle Access Manager Access Administration devices (also referred to as ADMINHOST in the Oracle documentation; hereafter called the Access Administration servers). The Access Administration servers contain the WebGate and WebPass components of Oracle Access Manager. After completing the BIG-IP LTM configuration, there are additional procedures to perform on the Oracle Access Administration devices.

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

- *Creating a HTTP health monitor*
- *Creating the Access Administration Server pool*
- *Creating the profiles*
- *Creating the Oracle Access Administration virtual server*
- *Optional: Configuring the BIG-IP LTM to offload SSL*
- *Modifying the Oracle Access Manager configuration*

Creating a HTTP health monitor

The first step is to set up a health monitor for the Access Administration devices. This procedure is optional, but very strongly recommended. In our example, 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 **oam-admin-http**.
4. From the **Type** list, select **HTTP**.
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** and **Receive** String sections, you can add an optional Send String and Receive Rule specific to the device being checked.
7. Click the **Finished** button.

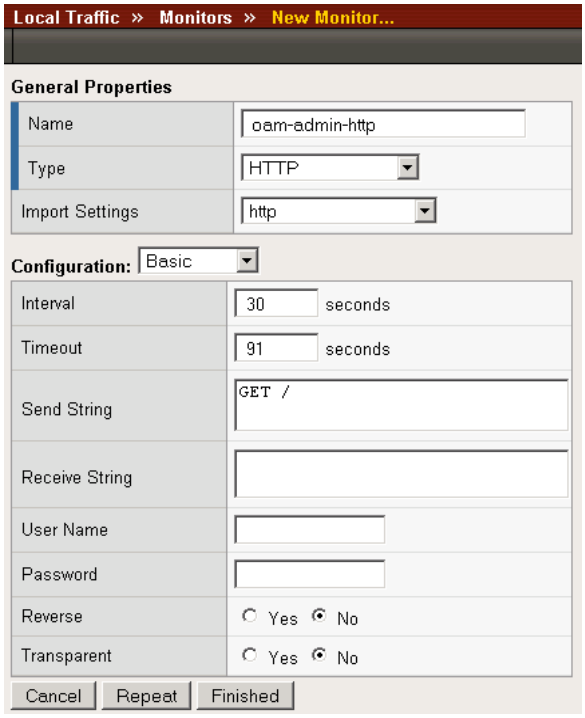

Figure 2 *Creating the HTTP monitor*

Creating the Access Administration Server pool

The next step is to create a pool on the BIG-IP LTM system for the Oracle Access Administration devices. A BIG-IP LTM pool is a set of devices grouped together to receive traffic according to a load balancing method. A BIG-IP LTM pool makes future scaling of your Oracle Access Manager deployment Access Administration devices extremely easy; simply add a new device to the network, then add it to the pool. The BIG-IP LTM immediately begins monitoring and directing traffic to the device.

To create the Oracle Access Administration 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 **oam-admin-pool**.
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 **oam-admin-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 (node)**.
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 device.
   In our example, we type **7777**.
10. Click the **Add** button to add the member to the list.
11. Repeat steps 8-10 for each server you want to add to the pool.
    In our example, we repeat these steps once for **10.133.17.111**.
12. Click the **Finished** button (see Figure 3).

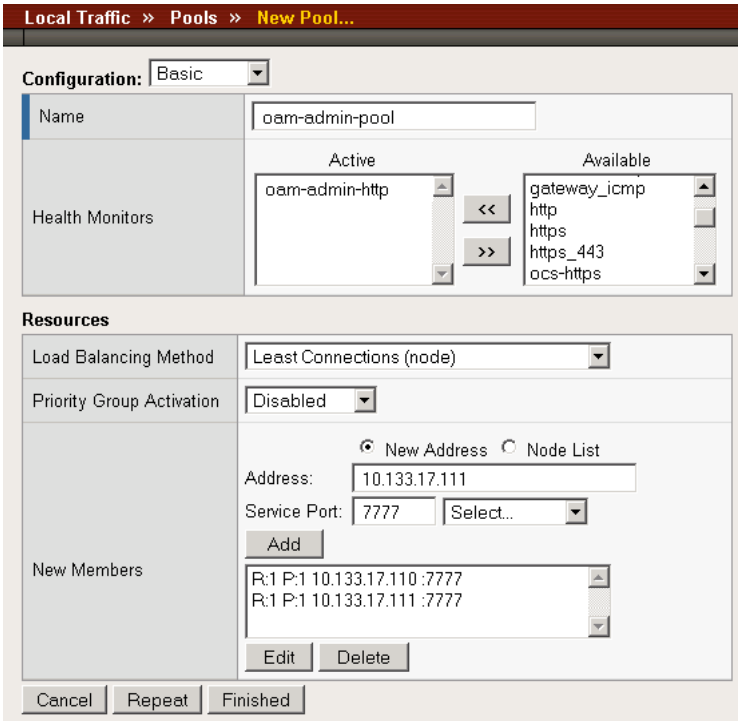

Figure 3 *Creating the BIG-IP LTM pool*

Creating the profiles

BIG-IP LTM 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.

These profiles use new optimized profiles available in BIG-IP LTM version 9.4 and later. If you are using a BIG-IP LTM version prior to 9.4, the ***Configuration Guide for BIG-IP Local Traffic Management*** for version 9.4 (available on **AskF5**) shows the differences between the base profiles and the optimized profile types. Use this guide to manually configure the optimization settings.

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.

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 **oam-admin-http**.
4. From the **Parent Profile** list, select **http**. 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 users are accessing the deployment via a Local Area Network, we recommend using the **tcp-lan-optimized** (for server-side TCP connections) parent profile. If the majority of the 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 are not using version 9.4 or do not want to use this optimized profile, you can choose the default TCP parent profile.

To create a new LAN optimized 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 **oam-admin-tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized** if you are using BIG-IP LTM version 9.4 or later; otherwise select **tcp**.

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 WAN optimized 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 **oam-admin-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 the Stream profile

The next profile we create is a Stream profile. The Stream profile performs a search and replace procedure for all occurrences of a string in a data stream efficiently and with minimal buffering. For more information on the Stream Profile, see *Solution 8115**, Overview of the Stream Profile,** on Ask F5*.
We create a Stream profile to correct instances where the web server inserts its own host name instead of the host name of the virtual servers, or incorrect paths into the content of the web pages.

This procedure uses the host name of the virtual server you will create in *Creating the Oracle Access Administration virtual server*, on page 12. If you do not yet know the host name, you can return to this procedure after creating the virtual server and modify the Target.

To create a new Stream profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, click **Stream**.
The Stream Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button. The New Stream Profile screen opens.

4. In the **Name** box, type a name for this profile. In our example, we type **oam-admin-stream**
5. Click the **Custom** box in the Target row. In the **Target** box, type use the following syntax:

   ```
   @<search>@<replace>@@<search>@<replace>@
   ```

   In our example, we type:

   ```
   @adm0.ora10g.tc.f5net.com:7777@admin.ora10g.tc.f5net.com@
   @identity/oblix"@identity/oblix/"@
   ```

   In this example, we are searching for the host name of the Access Administration Server, and replacing it with the host name of the virtual server you will create in *Creating the Oracle Access Administration virtual server*, on page 12. The second search and replace pattern (following the @@) fixes a potential problem that can cause redirects.
6. Click the **Finished** button.

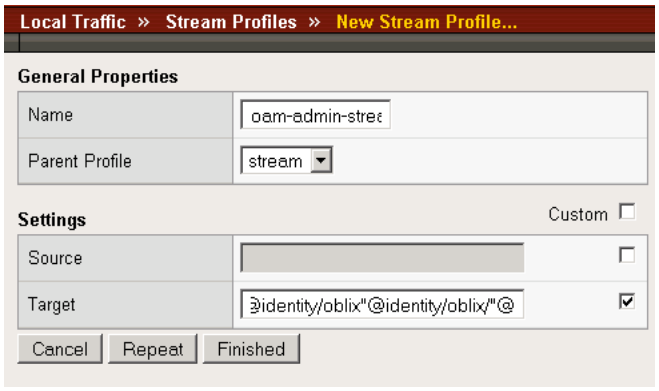

Figure 4 *Creating the Stream profile*

Creating the persistence profile

The final profile we create is a Persistence profile. We recommend using 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 **oam-admin-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.

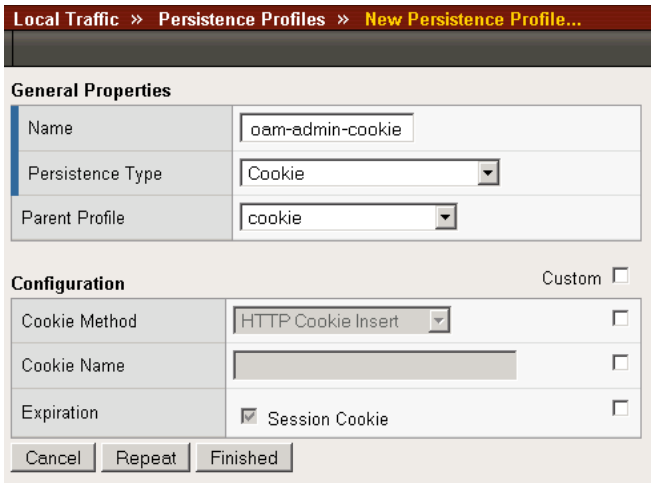

Figure 5 *Creating the cookie persistence profile*

Creating a OneConnect profile

The final 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**.
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 **oam-admin-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 Access Administration 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.
3. In the **Name** box, type a name for this virtual server. In our example, we type **oam-admin-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**.

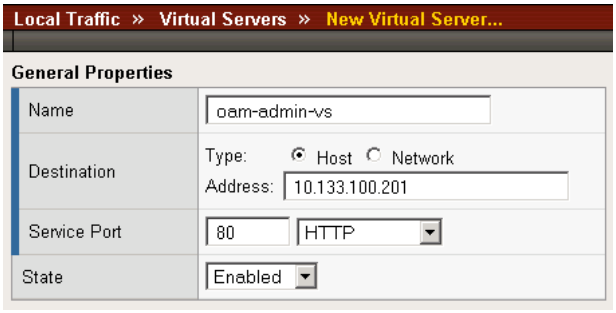

Figure 6 *Creating the Oracle Access Administration virtual server*

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 **oam-admin-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 **oam-admin-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 **oam-admin-oneconnect**.
12. 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 **oam-admin-http** (see Figure 7).

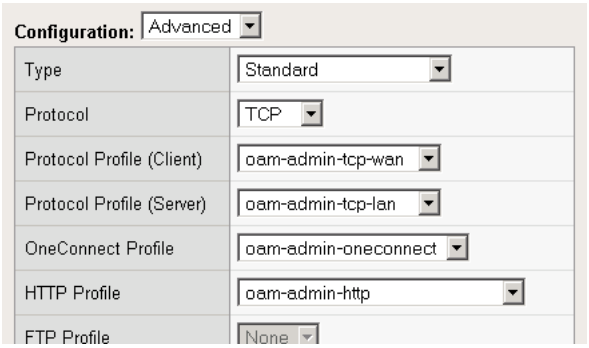

Figure 7 *Selecting the Oracle profiles for the virtual server*

13. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the Access Administration Server pool* section. In our example, we select **oam-admin-http**.
14. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating the persistence profile* section. In our example, we select **oam-admin-cookie**.
15. Click the **Finished** button (see Figure 8).

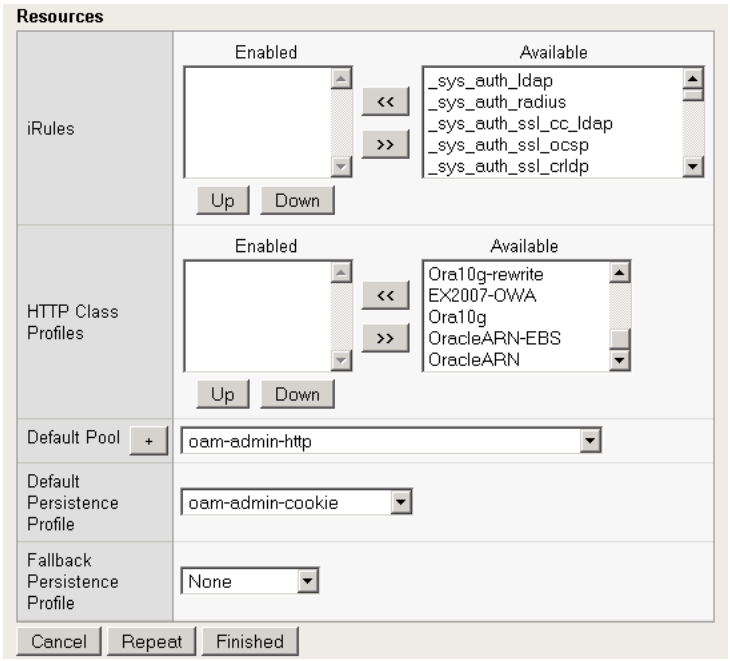

Figure 8 *Adding the Pool and Persistence profile to the virtual server*

If you are using the BIG-IP LTM system to offload SSL, continue with the following section. If not, after completing the BIG-IP LTM configuration, there are changes you need to make on the Oracle Access Manager Access Administration server. 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 Access Manager configuration*, on page 21.

Optional: Configuring the BIG-IP LTM to offload SSL

If you are using the BIG-IP LTM system to offload SSL from the Oracle Access Administration 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 Access Administration 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.

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.

Modifying the HTTP profile

The next step is to modify the HTTP profile you created in *Creating an HTTP profile*, on page 8 to include a Header Insert.

To modify the HTTP profile

1. On the Main tab, expand **Local Traffic**, and the click **Profiles**. The HTTP Profiles screen opens.
2. Click the name of the profile you created in *Creating an HTTP profile*, on page 8. In our example, we click **oam-admin-http**.
3. From the **Request Header Insert** row, click the Custom button.
4. In the **Request Header Insert** box, type **IS_SSL:yes**.
   For more information on this setting, see Section 5.11.6 of the ***Oracle Application Server Enterprise Deployment Guide***.
5. Click the **Update** button.

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

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

Modifying the virtual server

The next task is to modify the Oracle Access Administration virtual server you created to use the SSL profile you just created.

To modify the existing Oracle 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 virtual server you created in *Creating the Oracle Access Administration virtual server*, on page 12. In our example, we click **oam-admin-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 16. In our example, we select **oam-admin-clientssl**
5. Click the **Update** button.

If you are using the BIG-IP LTM system to offload SSL from Oracle Access Manager devices, make sure to follow the notes about SSL offload when performing the Oracle configuration modifications in *Modifying the Oracle Access Manager configuration*, on page 21.

Configuring the BIG-IP LTM for the Identity Server component of Oracle Access Manager

The next group of objects we configure on the BIG-IP LTM system is for the Oracle Identity Server component. These BIG-IP LTM configuration objects are transparent to the end user, but are used on the back-end by the Oracle devices, and provide high availability and simple scalability.

The BIG-IP LTM configuration for the Identity Server is very similar to the preceding configuration, so in the following sections, we reference the procedures from the Access Administration section.

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

- *Creating a TCP health monitor*
- *Creating the pool*
- *Creating the Profile*
- *Creating the Identity Server virtual server*

In many cases, you can use the same BIG-IP LTM objects for both Oracle Access Administration and Identity Server (such as the health monitor and profiles), however, we strongly recommend you create new objects for each Oracle component.

Important

If you have a BIG-IP LTM system in front of your Oracle Internet Directory (OID) installation, be sure to see Modifying the Identity Server to point to the BIG-IP LTM, on page 34.

Creating a TCP health monitor

The first task is to create a health monitor for the Identity Servers. For this monitor, we use a TCP health monitor.

To configure a TCP 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 **oracle-identity-tcp**.
4. From the **Type** list, select **TCP**.
   The TCP 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.

Creating the pool

The next task is to create a pool for the Identity Servers. Follow the procedure *Creating the Access Administration Server pool*, on page 6. Type a unique name for the pool, configure the pool to use the health monitor you just created, and add the appropriate IP address and port (default port is **6022**). All other settings are optional, configure as applicable for your configuration.

Creating the Profile

For the Identity Server virtual server, we only require a TCP profile. In our example, we base our profile off of the **tcp-lan-optimized** parent. Follow the procedure *Creating the LAN optimized TCP profile*, on page 8. Use a unique name for the profile, all other settings are optional.

Creating the Identity Server virtual server

The final step is to create a virtual server for the Oracle Identity Servers. Follow the procedure *Creating the Oracle Access Administration virtual server*, on page 12. Give this virtual server a unique name, and use the appropriate address and port (the default port is **6022**), and configure the virtual server to use the pool and profile you created in the preceding procedures.

Configuring the BIG-IP LTM for the Access Server component of Oracle Access Manager

The next group of objects we configure on the BIG-IP LTM system is for the Oracle Access Server component. The Access Server is a software component that receives requests, responds to the access client, and manages the login session. The Access Server receives requests from WebGate and queries the authentication, authorization, and auditing rules in Oracle Internet Directory.

The BIG-IP LTM configuration for the Access Servers is also very similar to the Access Administration configuration, so in the following sections, we reference the procedures from the Access Administration section.

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

- *Creating a TCP health monitor*
- *Creating the pool*
- *Creating the Profile*
- *Creating the Identity Server virtual server*

Again, we strongly recommend you create new objects for each Oracle component.

Important

If you have a BIG-IP LTM system in front of your Oracle Internet Directory (OID) installation, be sure to see Modifying the Identity Server to point to the BIG-IP LTM, on page 34.

Creating a TCP health monitor

The first task is to create a health monitor for the Access Servers. Follow the procedure *Creating a TCP health monitor*, on page 17. Use a unique name for the monitor, and use the same a 1:3 +1 ratio between the interval and the timeout.

Creating the pool

The next task is to create a pool for the Access Servers. Follow the procedure *Creating the Access Administration Server pool*, on page 6. Type a unique name for the pool, configure the pool to use the health monitor you just created, and add the appropriate IP address and port (default port is **6035**). All other settings are optional, configure as applicable for your configuration.

Creating the Profile

For the Access Server virtual server, we only require a TCP profile. In our example, we base our profile off of the tcp-lan-optimized parent. Follow the procedure *Creating the LAN optimized TCP profile*, on page 8. Use a unique name for the profile, all other settings are optional.

Creating the Access Server virtual server

The final step is to create a virtual server for the Oracle Access Servers. Follow the procedure *Creating the Oracle Access Administration virtual server*, on page 12. Give this virtual server a unique name, and use the appropriate address and port (the default port is **6035**), and configure the virtual server to use the pool and profile you created in the preceding procedures.

Now continue with the following section to modify the Oracle Access Manager configuration.

Modifying the Oracle Access Manager configuration

With the BIG-IP LTM configuration complete, there are now modifications to the Oracle Access Manager configuration that need to be made in order for traffic to resolve and flow properly. For example, we modify the Oracle configuration to use the BIG-IP LTM virtual servers instead of pointing directly to an Oracle device.

This section contains the following procedures:

- *Changing the default port for the Access Administration server*
- *Adding the virtual host entry for the BIG-IP LTM virtual server*
- *Modifying the Identity Server to use the BIG-IP LTM virtual server*
- *Configuring WebPass to use the BIG-IP LTM virtual server*
- *Modifying the Access Server to use the BIG-IP LTM virtual server*
- *Configuring WebGate to use the BIG-IP LTM virtual server*

This section requires you have administrative access to the Oracle devices for both the GUI and the command line.

Changing the default port for the Access Administration server

The first task is to change the default port for the Access Administration server to **80**. We change the default port because the BIG-IP LTM virtual server uses port 80. If you are using an HTTPS virtual server on the BIG-IP LTM system, we change this

To change the default port

1. Log on to your Oracle Access Administration server 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** (**443** if using HTTPS on the BIG-IP LTM).

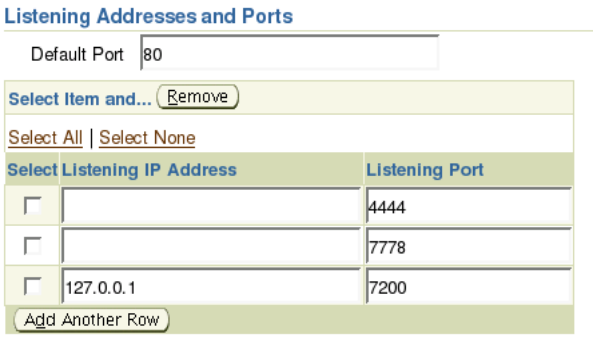

Figure 9 *Changing the default port for the Access Administration server*

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

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.

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 Access Administration 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. Add the following:

   ```
   Port 80
   ```

   The entry should look like this when you are finished:

   ```
   <VirtualHost *:7777>
       ServerName admin.oraclearn.tc.f5net.com
       Port 80
   </VirtualHost>
   ```

   Note that the **ServerName** example above will be different in your deployment.
5. Save and close the **httpd.conf** file.

6. Restart your web server. For simplicity, we recommend you restart the web server through the Oracle Enterprise Manager.

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 Access Administration server 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 Access Administration Server through Enterprise Manager as an administrator.

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 Access Administration virtual server on the BIG-IP LTM system (the virtual server you created in *Creating the Oracle Access Administration virtual server*, on page 12), 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*

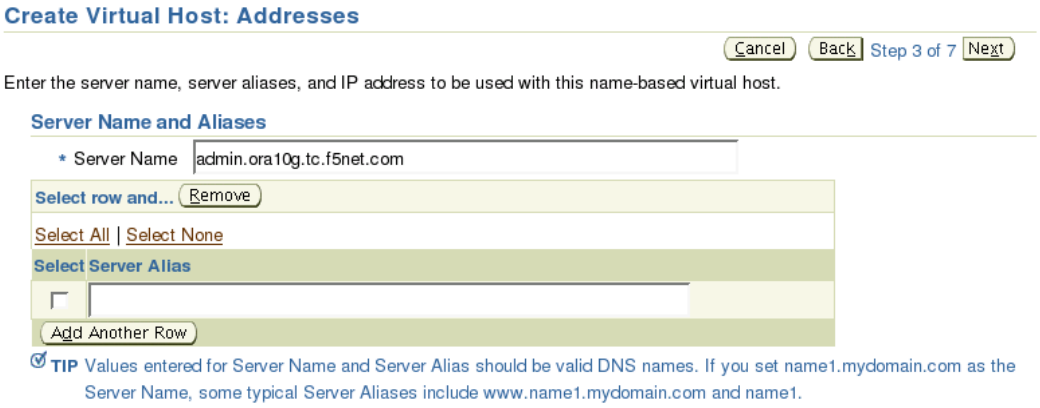

Figure 10 *Adding the BIG-IP LTM virtual server DNS name*

d) In Step 4, make sure that **Listen on a specific port** is selected. From the list, select **7777**. Click the **Next** button.

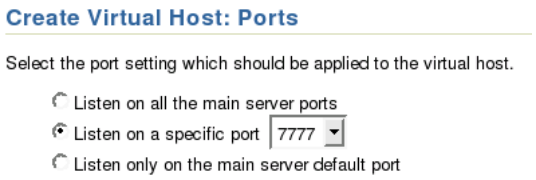

Figure 11 *Selecting the Port*

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.

Modifying the Identity Server to use the BIG-IP LTM virtual server

The first task is to modify the Identity Server configuration to use the Identity server virtual server you created in *Creating the Identity Server virtual server*, on page 18.

To modify the Identity server configuration

1. Log on to the Oracle Access Administration server.
2. Click **Identity System**. The Identity Administration page opens.
3. Click **Identity System Console**. Enter your user name and password if prompted.
4. On the blue menu bar, click **System Configuration**. The System Configuration page opens.
5. In the left navigation pane, click **Identity Servers**. A list of all Identity servers opens.
6. Click the name of your Identity server. The Details page opens.
7. Click the **Modify** button.
8. In the **Hostname** box, type the host name of the Identity server virtual server you created in *Creating the Identity Server virtual server*, on page 18. In our example, we enter **idm.ora10g.tc.f5net.com** (see Figure 12).
9. In the **Port** box, type the port that corresponds with the Identity server virtual server. In our example, we type **6022**.
10. Click the **Save** button.
11. If you are using multiple Identity Servers, repeat this entire procedure for each one.

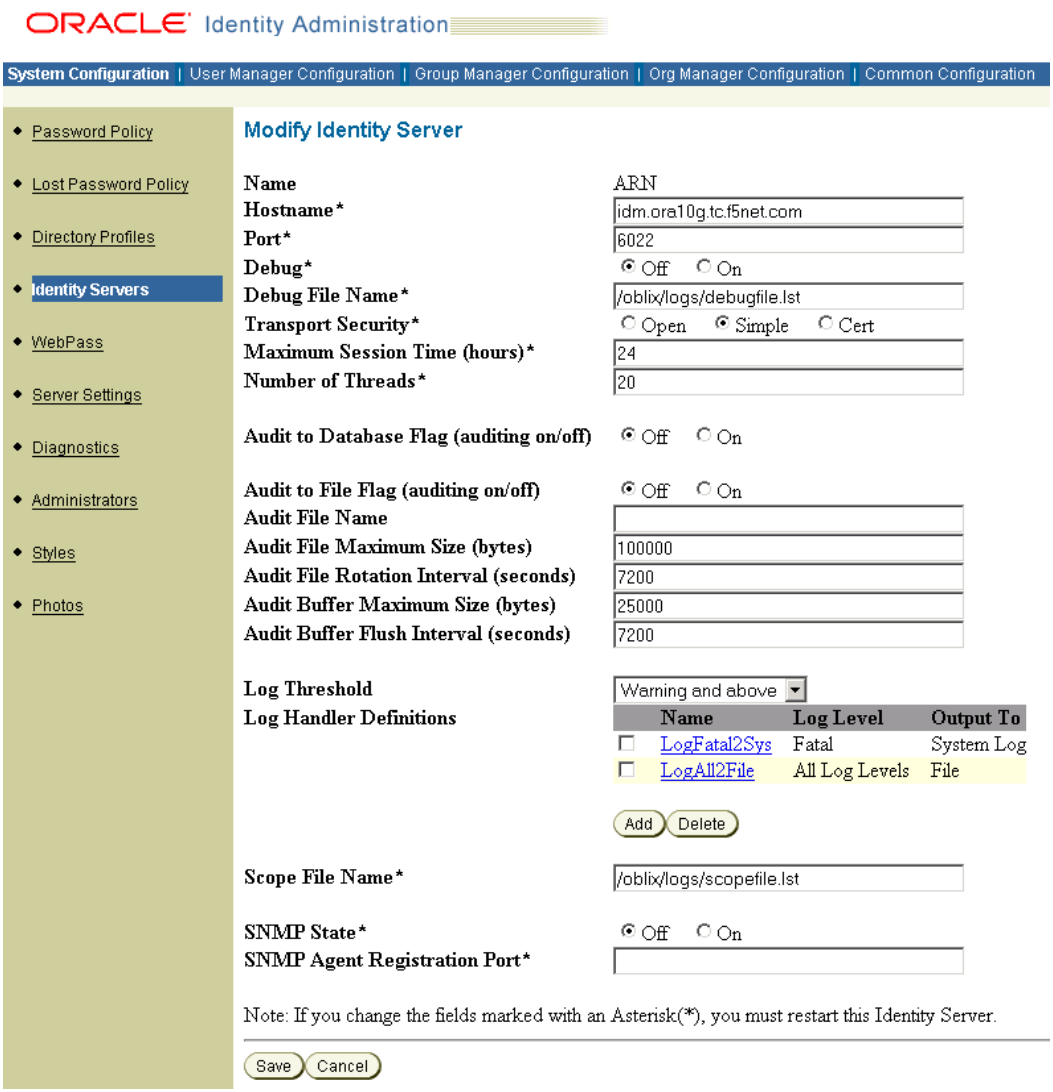

Figure 12 *Modifying the Identity server to use the BIG-IP LTM virtual server*

Configuring WebPass to use the BIG-IP LTM virtual server

The next step is to configure WebPass to use the Access Administration virtual server you created in *Creating the Oracle Access Administration virtual server*, on page 12.

To configure WebPass to use the virtual server

1. Log on to the Access Administration device.
2. Click **Identity System**. The Identity Administration page opens.

3. Click **Identity System Console**. Enter your user name and password if prompted.
4. On the blue menu bar, click **System Configuration**. The System Configuration page opens.
5. In the left navigation pane, click **WebPass**.
6. Click the name of your Access Administration server.
7. Click the **Modify** button at the bottom on the page.
8. In the **Hostname** box, type the host name of the Access Administration virtual server you created in *Creating the Oracle Access Administration virtual server*, on page 12.
9. In the **Port** box, type the port that corresponds with the Access Administration server virtual server. If you are using the BIG-IP LTM to offload SSL, type **443**, if not, use port **80**.

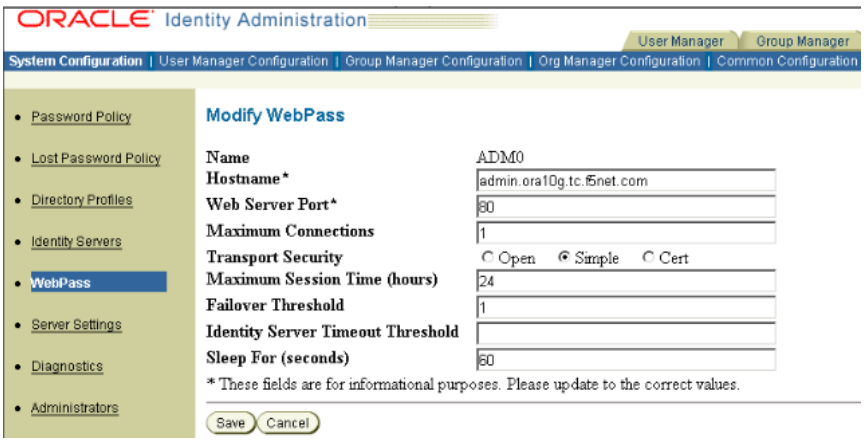

Figure 13 *Modifying WebPass to point to the BIG-IP LTM virtual server*

10. Click the **Save** Button.
11. Restart the Services on the Access Administration server.

Modifying the Access Server to use the BIG-IP LTM virtual server

The next task is to modify the Access Server configuration to use the Access server virtual server you created in *Creating the Access Server virtual server*, on page 20.

To modify the Access server configuration

1. Log on to the Oracle Access Administration server.
2. Click **Access System**. The Access Administration page opens.
3. Click **Access System Console**.

4. Click the **Access System Configuration** tab.
5. In the left navigation pane, click **Access Server Configuration**.
6. Click the name of your Access server, and then click **Modify**.
7. In the **Hostname** box, type the host name of the Access server virtual server you created in *Creating the Access Server virtual server*, on page 20. In our example, we enter **idm.ora10g.tc.f5net.com**
8. In the **Port** box, type the port that corresponds with the Access server virtual server. In our example, we type **6035**.
9. Make sure the **Update Cache** box is checked.
10. Click the **Save** button (see Figure 14).
11. Repeat this entire procedure for any other Access Servers.

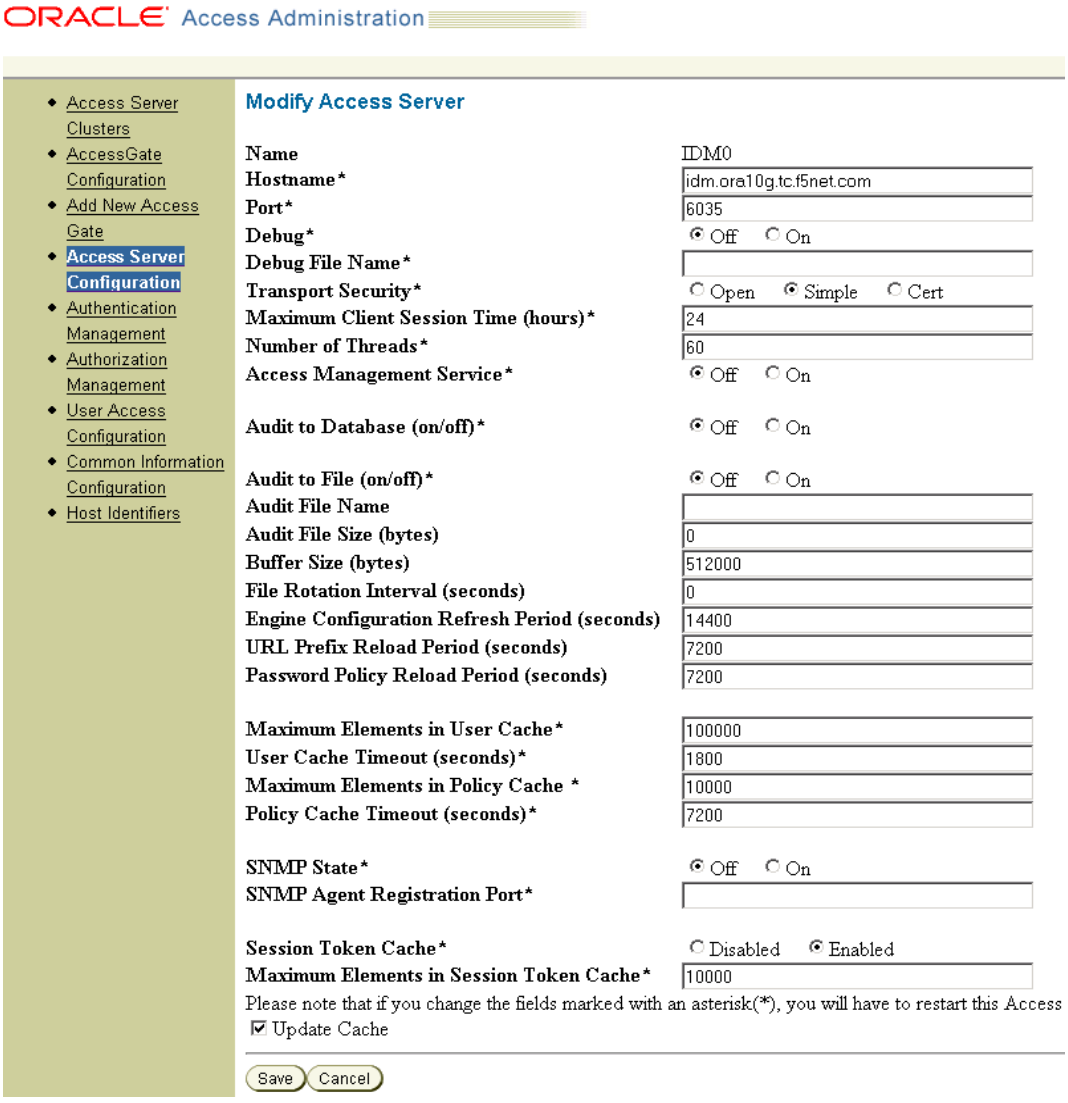

Figure 14 *Modifying the Access Server to use the BIG-IP LTM virtual server*

Configuring WebGate to use the BIG-IP LTM virtual server

The next step is to configure WebGate to use the Access Administration virtual server you created in *Creating the Oracle Access Administration virtual server*, on page 12.

To configure WebGate to use the virtual server

1. Log on to the Oracle Access Administration server.
2. Click **Access System**. The Access Administration page opens.
3. Click **Access System Console**. Enter your user name and password if prompted.
4. Click the **Access System Configuration** tab.
5. In the navigation pane, click **AccessGate Configuration**.
6. In the Search For All Gates section, click **Go** to list the WebGates.
7. In the Search Results, click the name of your Access Gate.
8. Click the **Modify** button at the bottom on the page.
9. In the **Hostname** box, type the host name of the Access Administration virtual server you created in *Creating the Oracle Access Administration virtual server*, on page 12.
10. In the **Port** box, type the port that corresponds with the Access Administration server virtual server (80).
    If you are using the BIG-IP LTM to offload SSL, type **443**, if not, use port **80**.

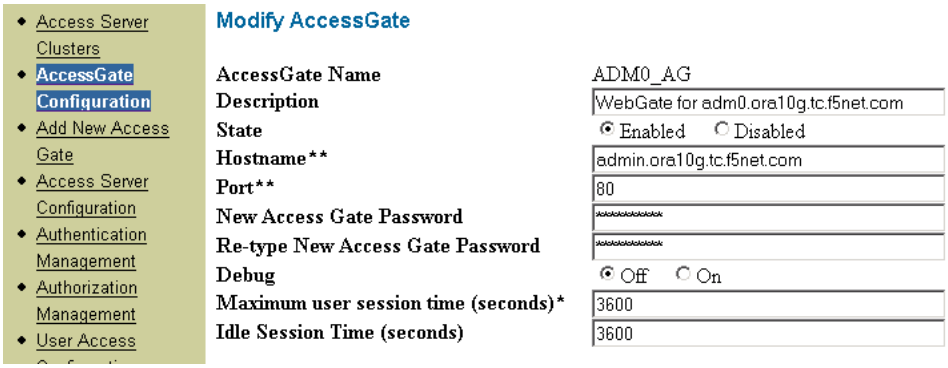

Figure 15 *Modifying AccessGate to point to the BIG-IP LTM virtual server*

11. From the Web Server Client section, in the **Preferred HTTP Host** box, type the host name of the Access Administration virtual server you created in *Creating the Oracle Access Administration virtual server*, on page 12 (see Figure 16).

Figure 16 *Modifying the Preferred HTTP Host*

12. If you are not using the BIG-IP LTM to offload SSL traffic, click the **Save** Button and continue to step 15.
    If you are using the LTM to offload SSL, continue with step 13.
13. From the User Defined Parameters section, in the **Parameters** box, type **ProxySSLHeaderVarVal**.

    In the **Values** box, type **IS_SSL**.
    This corresponds to the Request Header Insert setting on the HTTP profile you created in *Modifying the HTTP profile*, on page 15.

    These variables are taken from Section 5.11 of the ***Oracle Application Server Enterprise Deployment Guide***.

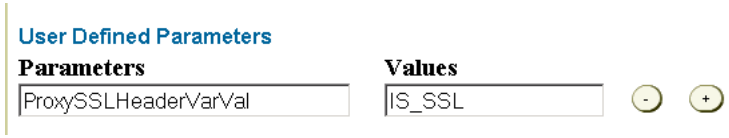

Figure 17 *Setting the User Defined Parameters*

14. Click the **Save** button.
15. Restart the Services on the Access Administration server.
16. Repeat this entire procedure for any additional Access Gates.

Deploying the FirePass controller with Oracle Access Manager

This section of the Deployment Guide shows you how to configure F5's FirePass controller for integration with Oracle Access Manager. In our example configuration, the Oracle Access Manager deployment, along with an OID instance, resides behind a BIG-IP LTM system. This section describes how to configure the FirePass controller to authenticate against the Oracle Access Manager Single Sign On system to provide single sign on.

F5's FirePass® controller is the industry leading SSL VPN solution that enables organizations of any size to provide ubiquitous secure access for employees, partners and customers to applications such as Oracle 10g or E-Business Suite, while significantly lowering support costs associated with legacy client-based VPN solutions.

For more information on the FirePass controller, see **http://www.f5.com/products/FirePass/**.

This section only contains details on how to configure a new Master group on the FirePass controller for user authentication using Oracle Access Manager. For information on how to configure other objects (such as Resource groups and types of access) on the FirePass controller, see the FirePass documentation.

Prerequisites and configuration notes

The following are prerequisites for this deployment:

- The FirePass controller should be running version 6.0 or later.
- This deployment was tested using an Oracle Access Manager installation, load balanced by a BIG-IP LTM system as described in this Deployment Guide.
- All of the configuration procedures in this section are performed on the FirePass device.
- This Deployment Guide is written to the scenario outlined in the following section. It is meant to be a template; modify the configuration as necessary for your deployment.

Configuring the FirePass controller

To configure the FirePass controller for allowing single sign on to the Oracle Access Manager deployment, complete the following procedures.

Connecting to the FirePass controller

To perform the procedures in this Deployment Guide you must have administrative access to the FirePass controller.

To access the Administrative console, in a browser, type the URL of the FirePass controller followed by **/admin/**, and log in with the administrator's user name and password.

Once you are logged on as an administrator, the Device Management screen of the Configuration utility opens. From here, you can configure and monitor the FirePass controller.

Creating the Master group

FirePass controller master groups are composed of users, authentication methods, and security and policy information.

To create a new Master Group

1. From the navigation pane, click **Users**, and expand **Groups**.
   The Master Groups list screen opens.
2. Click the **Create new group** button.
   The Group Management Create New Group screen opens.
3. In the **New group name** box, type the name of your group. In our example we type **OracleAccessManager**.
4. In the **Users in group** box, select **External**.
5. From the Authentication method list, select **HTTP form-based**.
6. In the **Copy settings from** list, make sure **Do not copy** is selected (see Figure 18).
7. Click the **Create** button.
   The General tab of the new Master Group displays.

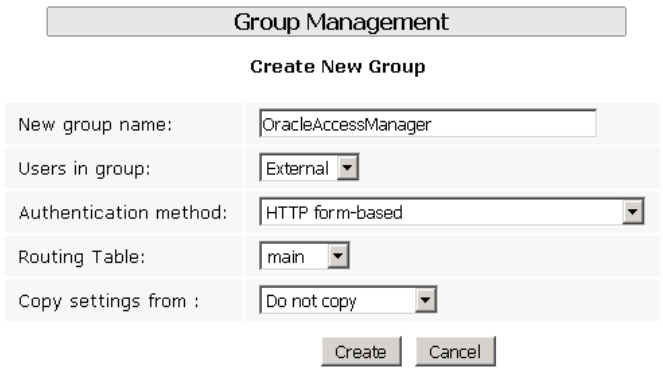

Figure 18 *Creating a new Master Group for employees*

8. Click the Authentication tab.
   The Authentication screen opens.
9. In the **Start URL** box, type **http://** (if the BIG-IP LTM is not offloading SSL) or **https://** (if the BIG-IP LTM is offloading SSL), followed by the host name (or IP address) of the Access Administration virtual server you created in *Creating the Oracle Access Administration virtual server*, on page 12, and then add the following path to complete the URL:

```
/access/oblix/apps/common/bin/common.cgi?program=commonLogin
```

10. In the **Form action** box, type **http://** (if the BIG-IP LTM is not offloading SSL) or **https://** (if the BIG-IP LTM is offloading SSL), followed by the host name (or IP address) of the Access Administration virtual server you created in *Creating the Oracle Access Administration virtual server*, on page 12, and then add the following path to complete the URL:

```
/identity/oblix/apps/userservcenter/bin/userservcenter.cgi?program=commonLogin
```

11. In the Form parameter for user name box, type **login**.
12. In the Form parameter for password box, type **password**.
13. In the Hidden form parameters and values box, specify the following three variables:

    ```
    fromloginpage=true
    comp=
    ObLoginDomain=<LDAP Logon DN>
    ```

    The first two parameters should always be the same. The ObLoginDomain parameter needs to match the domain DN in LDAP for your installation.
14. In the **Number of redirects to follow** box, type **1**.
15. Make sure that **Pass cookies to client browser** is checked.
16. In the Successful logon detection section, click **By presence of specific cookie**.
    In the **Cookie Name** box, type the name of the cookie (**ObTEMC** by default).
17. Click the **Save Settings** button (see Figure 19).

    We recommend you click the **Test Saved Settings** button to verify the procedure. At the bottom of the test results, you should see a line similar to the following:

    ```
    Cookie ObTEMC is set. User orcladmin authenticated
    ```

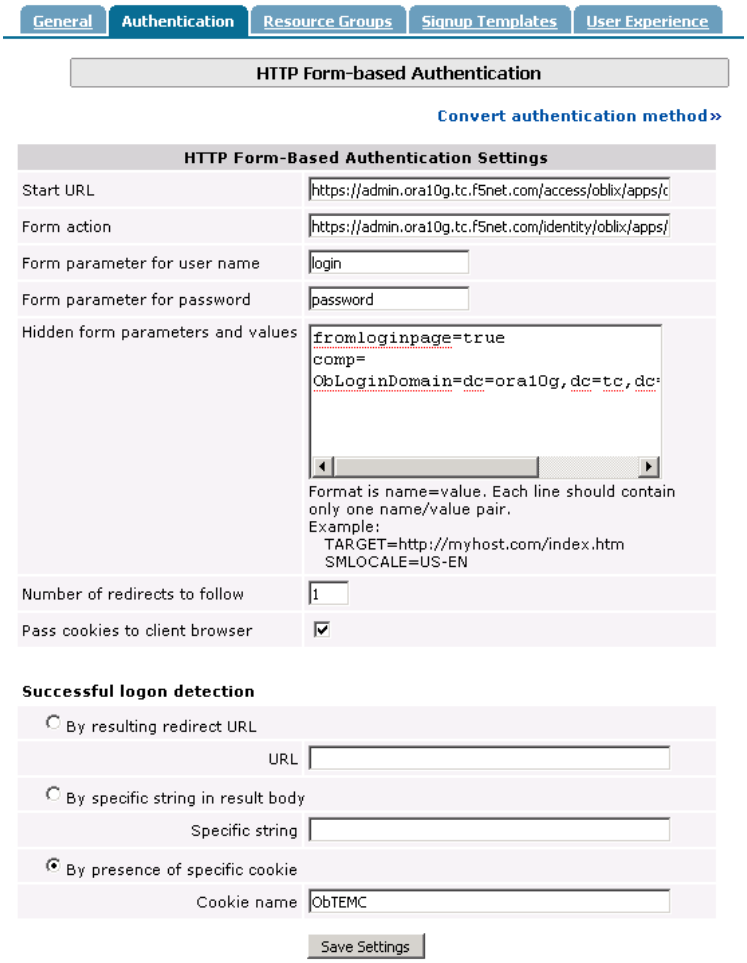

Figure 19 *Configuring the FirePass authentication settings*

Your FirePass controller Master group is now configured to use Oracle Access Manager for authentication. See the FirePass controller documentation for creating Resource groups and other configuration objects.

Appendix A: Modifying the Oracle configuration if a BIG-IP LTM system is in front of Oracle Internet Directory (OID)

This Appendix contains additional procedures for configurations where there is a BIG-IP LTM system in front of the Oracle Internet Directory (OID) devices. This section is not required if you do not have a BIG-IP LTM in front of the OID servers. In the following procedures, we modify the Oracle devices to use the BIG-IP LTM OID virtual server instead of going directly to the OID devices.

There are two procedures in this section, one for the Identity Server component, and one for the Access Server component.

Modifying the Identity Server to point to the BIG-IP LTM

The first procedure in this Appendix is to modify the Oracle Identity server to use the BIG-IP LTM virtual server for the OID devices.

To configure the Identity server

1. Log on to the Oracle Access Administration server.
2. Click **Identity System**. The Identity Administration page opens.
3. Click **Identity System Console**. Enter your user name and password if prompted.
4. On the blue menu bar, click **System Configuration**.
   The System Configuration page opens.
5. In the left navigation pane, click **Directory Profiles**.
6. Click the **Directory Server** link under Configure Profiles.
7. In the **Machine** box, type the host name that corresponds to the BIG-IP LTM virtual server for OID. In our example, we type **inf.ora10g.tc.f5net.com** (see Figure 20).
   You have to re-enter the password for binding to the directory.
8. Click the **Save** button. You will receive the following message: *Database settings have changed. Please go through product setup (refer to Identity System Installation Guide for instructions)*
9. Restart the web server(s) and Identity Server.

Figure 20 *Configuring the Identity Server to use the BIG-IP LTM virtual server*

This completes the modifications for the Identity server when the BIG-IP LTM is in front of the OID installation.

Modifying the Access Server to point to the BIG-IP LTM

The first procedure in this Appendix is to modify the Oracle Access server to use the BIG-IP LTM virtual server for the OID devices.

To configure the Access server

1. Log on to the Oracle Access Administration server.
2. Click **Access System**. The Access Administration page opens.
3. Click **Access System Console**. Enter your user name and password if prompted.
4. Click the **System Configuration** tab.
   The System Configuration page opens.
5. In the left navigation pane, click **Server Settings**.
6. Click the **Directory Server** link.
7. In both **Machine** boxes (Configuration Data Details and Policy Data Details sections), type the host name that corresponds to the BIG-IP LTM virtual server for OID. In our example, we type **inf.ora10g.tc.f5net.com** (see Figure 21).
   You have to re-enter the password for binding to the directory.

8. Click the **Save** button. You will receive the following message: *Database settings have changed. Please go through product setup (refer to Identity System Installation Guide for instructions).*
9. Restart the web server(s) and Access Server.

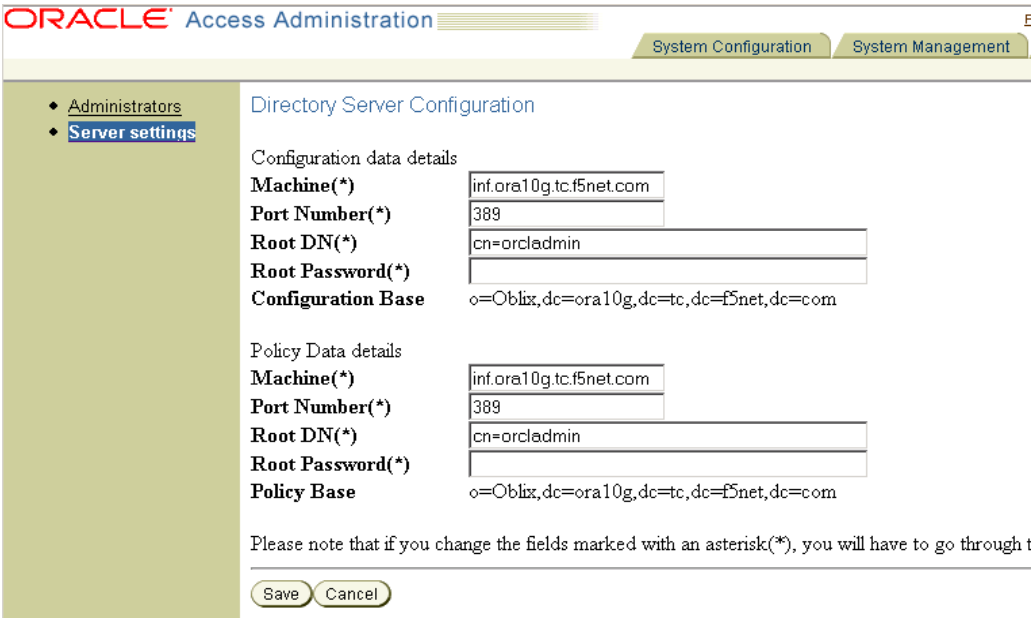

Figure 21 *Configuring the Access Server to use the BIG-IP LTM OID virtual server*

This concludes the modifications to Oracle Access Manager if using a BIG-IP LTM in front of OID devices.

Appendix B: Integrating Oracle Portal with Oracle Access Manager through the BIG-IP LTM

This Appendix contains modifications to Section 11 of the Oracle document titled ***Integrating Oracle Access Manager with Oracle Single Sign On and Oracle Portal***, found on Oracle's website at: **http://www.oracle.com/technology/obe/fusion_middleware/im1014/oam-osso-portal/oam-osso-portal.htm#t11**.

This Appendix is written with the assumption that you have configured the BIG-IP LTM system for use with Oracle Application Server 10g as described in the following Deployment Guide: **http://www.f5.com/pdf/deployment-guides/f5-oracle10g-dg.pdf**. We also assume that you are configuring your Oracle Applications according to the Oracle Integration document described above.

◆ Note

*The following procedure references step numbers found in **Integrating Oracle Access Manager with Oracle Single Sign On and Oracle Portal**. Have this document open and available while performing this procedure.*

Modifying the Oracle configuration

1. Log on to the Access System Console as an administrator, and Add a Host Identifier as described in Steps 1 and 2 of the Oracle document.
2. On the **Add a new host identifier** screen, type name and description in the **Name** and **Description** boxes. The name must match the name of the BIG-IP LTM virtual server you created for Oracle 10g Portal.
   In the **Hostname variations** box, type the fully qualified domain name of your BIG-IP LTM virtual server for Oracle 10g Portal (see ***Creating the Oracle 10g Portal virtual server*** on page **1-11** of the **Oracle Application Server 10g** Deployment Guide.

   Click the **Add** button to add another host name. Type **portal**, and then click the **Save** button (see Figure 22).

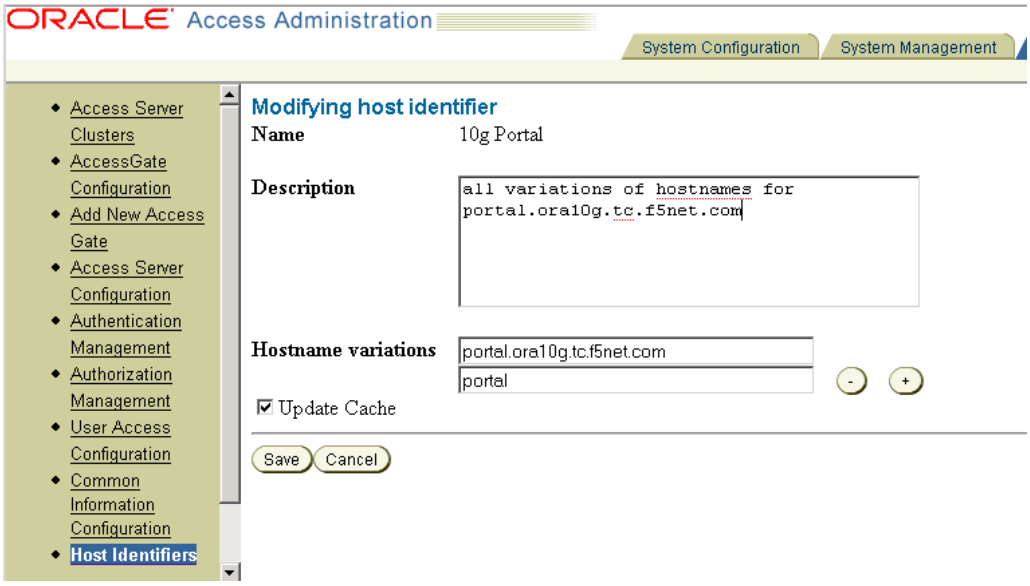

Figure 22 *Modifying the host identifier*

3. In Step 7 of the Oracle document (part of creating resources for the policy domain), from the **Resource Type** list, select **http**. If you are offloading SSL to the BIG-IP LTM for your Portal installation, select **https** instead.
   From the **Host Identifiers** list, select the identifier that you created in Step 2 for your Portal installation.
4. In Step 10 of the Oracle document, (adding a Policy for the OSSO domain), from the **Host Identifiers** list, select the same resource you created in Step 2 and used in Step 7.

That concludes the changes for the BIG-IP LTM. Continue with the rest of the Oracle document.

Appendix C: Backing up and restoring the BIG-IP LTM configuration

We recommend saving your BIG-IP LTM configuration before you begin this configuration. When you save the BIG-IP LTM configuration, it collects the following critical data and compress it into a single User Configuration Set (UCS) file:

- BIG-IP configuration files
- BIG-IP license and passwords
- SSL certificates
- SSH keys

Saving and restoring the BIG-IP configuration

The Configuration Management screen allows you to save and restore all configuration files that you may edit to configure a BIG-IP system. These configuration files are called a User Configuration Set (UCS). The Configuration Management screen contains sections for saving and restoring a configuration. The list boxes in these sections display only files in the **/usr/local/ucs** directory. If you want to save or restore files from another directory, you must type the full path in the box.

To save the BIG-IP configuration using the Configuration utility

1. In the navigation pane, click **System Admin**.
   The User Administration screen displays.
2. Click the Configuration Management tab.
   The Configuration Management screen displays.
3. In the **Save Current Configuration** section, type the path where you want your configuration file saved or choose a path from the list box. If no path is specified, the BIG-IP saves files to **/usr/local/ucs**. The BIG-IP appends the extension.ucs to file names without it.
   In our example, we type **pre_oam_backup.ucs.**
4. Click the **Save** button to save the configuration file.

To restore a BIG-IP configuration

1. In the navigation pane, click **System Admin**.
   The User Administration screen displays.
2. Click the Configuration Management tab.
   The Configuration Management screen displays.

3. In the **Restore a Configuration** section, choose the configuration file you want to restore from the list box, or type the path where your configuration files were saved.
4. Click the **Restore** button.
   To check the status of the restoration, click the **View Log** button. You should wait a few moments for the log file to start generating before you click **View Log**. Repeated clicking of this button will update your screen with the most current log file information until the restoration is complete.