



Deploying F5 with Oracle E-Business Suite 12

Important: This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support. For a list of current guides, see <https://f5.com/solutions/deployment-guides>.

Table of Contents

Introducing the BIG-IP LTM Oracle E-Business Suite 12 configuration

Prerequisites and configuration notes	1-1
Configuration example	1-2
Configuring the BIG-IP LTM system for deployment with Oracle E-Business Suite	1-3
Prerequisites and configuration notes	1-3
Connecting to the BIG-IP device	1-4
Creating a HTTP health monitor	1-4
Creating the Oracle E-Business Suite pool	1-5
Creating Oracle E-Business Suite profiles	1-7
Creating the Oracle E-Business Suite virtual server	1-12
Configuring the BIG-IP LTM to offload SSL from the E-Business Suite servers	1-14
Appendix A: Backing up and restoring the BIG-IP system configuration	1-17
Saving and restoring the BIG-IP configuration	1-17

Configuring the WebAccelerator module for accelerating Oracle E-Business Suite 12

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

Deploying the FirePass controller with Oracle E-Business Suite 12

Prerequisites and configuration notes	3-1
Configuration scenario	3-1
Configuring the FirePass for deployment with Oracle E-Business Suite	3-2
Connecting to the FirePass controller	3-2
Creating groups on the FirePass controller	3-2
Limiting access for the Partner group	3-7
Configuring Endpoint security	3-8
Conclusion	3-14



I

Deploying F5 with Oracle E-Business Suite 12

- Configuring the BIG-IP LTM system for deployment with Oracle E-Business Suite 12
- Configuring the BIG-IP LTM to offload SSL from the E-Business Suite servers

Introducing the BIG-IP LTM Oracle E-Business Suite 12 configuration

Welcome to the F5 and Oracle® E-Business Suite 12 Deployment Guide. When deployed with Oracle E-Business Suite (EBS), F5 ensures secure, fast and always available access for applications running on Oracle.

Oracle E-Business Suite is a fully integrated, comprehensive suite of business applications for the enterprise. Whether you implement one module at a time, multiple modules, or the complete suite - Oracle E-Business Suite provides better business information for effective decision-making and enables an adaptive enterprise for optimal responsiveness.

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

For more information on Oracle EBS, see <http://www.oracle.com/applications/e-business-suite.html>.

This Deployment Guide contains procedures for configuring the BIG-IP LTM system, the BIG-IP LTM system with SSL, the F5 WebAccelerator module, and the FirePass controller. While we recommend using all of these products together with Oracle EBS, it is not required. Simply use the sections for the products you have. This guide is broken up into the following chapters:

- ◆ *Configuring the BIG-IP LTM system for deployment with Oracle E-Business Suite 12*, on page 1-3
- ◆ *Configuring the BIG-IP WebAccelerator module for accelerating Oracle E-Business Suite 12*, on page 2-1
- ◆ *Deploying the FirePass controller with Oracle E-Business Suite 12*, on page 3-1

Prerequisites and configuration notes

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

- ◆ You must have an existing Oracle E-Business Suite deployment.
- ◆ This Deployment Guide contains configuration procedures for configuring the F5 devices only. For information on how to configure E-Business Suite, see the Oracle documentation.
- ◆ Briefly review the basic configuration tasks and the few pieces of information, such as IP addresses, that you should gather in preparation for completing the F5 device configuration.

Revision history:

Version	Description
1.0	New deployment guide
1.1	Modified the HTTP profile configuration in the SSL offload section to add the OA.jsp page to the Exclude list.
1.2	Moved the Modifying the HTTP profile configuration from the SSL offload section to the main EBS configuration section, as the list of URIs should be excluded whether offloading SSL or not. Added a URI if users are accessing the EBS deploying via Oracle Portal.

Configuration example

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

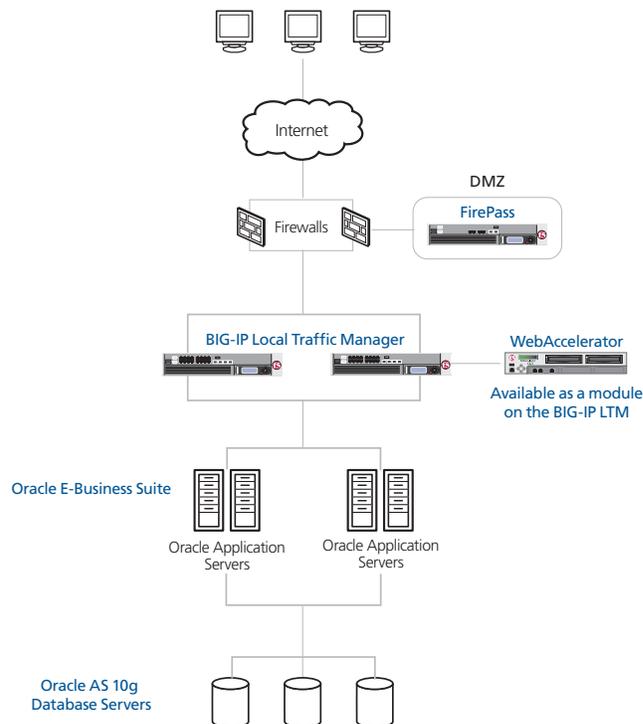


Figure 1.1 BIG-IP Oracle E-Business Suite logical configuration example

Configuring the BIG-IP LTM system for deployment with Oracle E-Business Suite 12

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

- *Creating a HTTP health monitor*
- *Creating the Oracle E-Business Suite pool*
- *Creating Oracle E-Business Suite profiles*
- *Creating the Oracle E-Business Suite virtual server*

This Deployment Guide also contains the following optional procedure:

- *Configuring the BIG-IP LTM to offload SSL from the E-Business Suite servers*

◆ 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 A: Backing up and restoring the BIG-IP system configuration**, on page 1-17.*

The BIG-IP 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 for this section:

- ◆ We strongly recommend you read the Oracle Support white paper *Using Load-Balancers with Oracle E-Business Suite Release 12*. The Doc ID is **Note:380489.1**
- ◆ 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 AskF5), which shows the configuration differences between the base profiles and the optimized profile types.

- ◆ Briefly review the basic configuration tasks and the few pieces of information, such as IP addresses, that you should gather in preparation for completing the BIG-IP LTM system configuration.

◆ **Note**

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

Connecting to the BIG-IP device

Use the following procedure to access the BIG-IP 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.

Creating a HTTP health monitor

The first step is to set up a health monitor for the Oracle E-Business Suite 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 **oracle-ebs-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.

Figure 1.2 Creating the HTTP Monitor

Creating the Oracle E-Business Suite pool

The next step is to create a pool on the BIG-IP LTM system for the Oracle E-Business Suite 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 E-Business Suite pool

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

- 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.*

- In the **Name** box, enter a name for your pool. In our example, we use **oracle-ebs**.
- 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 **oracle-ebs-http**.
- From the **Load Balancing Method** list, select **Predictive (node)**. This is the load balancing method recommended by Oracle.
- For this pool, we leave the Priority Group Activation **Disabled**.
- In the New Members section, make sure the **New Address** option button is selected.
- In the **Address** box, add the first server to the pool. In our example, we type **10.133.17.150**.
- In the **Service Port** box, type the appropriate port for your Oracle E-Business Suite server. In our example, we type **8000**.
- Click the **Add** button to add the member to the list.
- Repeat steps 9-11 for each server you want to add to the pool. In our example, we repeat these steps once for **10.133.17.151**.
- Click the **Finished** button (see Figure 1.3).

Figure 1.3 Creating the pool for the Oracle E-Business Suite

Creating Oracle E-Business Suite 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.

For the Oracle E-Business Suite configuration, we create five new profiles: an HTTP profile, two TCP profiles, a persistence profile, and a OneConnect profile. If you plan on using the BIG-IP LTM system to offload SSL from the Portal devices, make sure to see *Creating a Client SSL 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. For deployments where the majority of users accessing Oracle Portal are connecting across a WAN, F5 recommends enabling compression and caching on the BIG-IP LTM by using a profile introduced in BIG-IP version 9.4 called

http-wan-optimized-compression-caching (if you are using LTM version 9.4.2 or later, we recommend using **http-acceleration**). This profile uses specific compression and caching (among other) settings to optimize traffic over the WAN. Note that to properly use this profile, you need to have compression and caching licensed on the BIG-IP LTM. For more information on licensing, contact your sales representative.

If you are not using version 9.4, or do not have compression or caching licensed, you can choose the default HTTP parent profile, or one of the other optimized HTTP parent profiles.

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 **oracle-eps-http-opt**.

4. From the **Parent Profile** list, select **http-wan-optimized-compression-caching**. The profile settings appear.
5. Check the Custom box for **Content Compression**, and leave **Content List** selected.
6. In the Content List section, add the following items to the existing entries in the **Content Type** box one at a time, each followed by clicking **Include**:
 - **application/pdf**
 - **application/vnd.ms-powerpoint**
 - **application/vnd.ms-excel**
 - **application/msword**
 - **application/vnd.ms-publisher**

We add these MIME types to ensure these highly compressible document types are compressed.
7. In the RAM Cache section, click the Custom box for the **URI Caching** row.
8. From the **URI Caching** list, select **URI List**.
9. In the **URI** box, type the URI of the login, logout and the OA.jsp pages, and then click the **Exclude** button after each entry. In our example, we type **/OA_HTML/AppsLogin**, **/OA_HTML/AppsLogout**, and **/OA_HTML/OA.jsp**.

If your users are accessing the Oracle E-Business Suite implementation through Oracle Portal, you must also exclude: **/pls/portal/!PORTAL.wvpro_app_provider.do_object_signon**
10. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
11. Click the **Finished** button.

Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the Oracle E-Business Suite 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 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 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 **oracle-eps-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 users are accessing the portal via the LAN, 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 **oracle-eps-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. For Oracle E-Business Suite, we use Cookie Persistence in Insert mode, with an Oracle-recommended timeout value of 12 hours.

To create a new cookie persistence profile based on the default 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 **oracle-eps-cookie**.
5. From the **Persistence Type** list, select **Cookie**. The configuration options for cookie persistence appear.
6. In the Expiration row, check the Custom box. Clear the **Session Cookie** box, and the Expiration options appear. In the **Hours** box, type **12**.
7. Click the **Finished** button

Local Traffic >> Persistence Profiles >> New Persistence Profile...

General Properties

Name	oracle-eps-cookie
Persistence Type	Cookie
Parent Profile	cookie

Configuration Custom

Cookie Method	HTTP Cookie Insert	<input type="checkbox"/>			
Cookie Name		<input type="checkbox"/>			
Expiration	Days	Hours	Minutes	Seconds	<input checked="" type="checkbox"/>
	0	12	0	0	
<input type="checkbox"/> Session Cookie					

Cancel Repeat Finished

Figure 1.4 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 **oracle-eps-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 E-Business Suite 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 **oracle-eps-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 **10.133.17.201**
6. In the **Service Port** box, type **80**.

General Properties	
Name	oracle-eps-vs
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.133.17.201
Service Port	80 HTTP
State	Enabled

Figure 1.5 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 **oracle-eps-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 **oracle-eps-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 **oracle-eps-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 **oracle-eps-http-opt** (see Figure 1.6).

Configuration: Advanced	
Type	Standard
Protocol	TCP
Protocol Profile (Client)	tcp-wan-optimized
Protocol Profile (Server)	tcp-lan-optimized
OneConnect Profile	oracle-eps-oneconnect
HTTP Profile	oracle-eps-http-opt

Figure 1.6 Selecting the Oracle profiles for the virtual server

13. From the **SNAT Pool** list, select **Automap**.
14. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the Oracle E-Business Suite pool* section. In our example, we select **oracle-eps**.

-
- From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating persistence profile* section. In our example, we select **oracle-ebs-cookie**.

Resources							
iRules	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td></td><td><ul style="list-style-type: none">_sys_auth_ldap_sys_auth_radius_sys_auth_ssl_cc_ldap_sys_auth_ssl_ocsp_sys_auth_ssl_crlcp</td></tr><tr><td>Up</td><td>Down</td></tr></tbody></table>	Enabled	Available		<ul style="list-style-type: none">_sys_auth_ldap_sys_auth_radius_sys_auth_ssl_cc_ldap_sys_auth_ssl_ocsp_sys_auth_ssl_crlcp	Up	Down
Enabled	Available						
	<ul style="list-style-type: none">_sys_auth_ldap_sys_auth_radius_sys_auth_ssl_cc_ldap_sys_auth_ssl_ocsp_sys_auth_ssl_crlcp						
Up	Down						
HTTP Class Profiles	<table border="1"><thead><tr><th>Enabled</th><th>Available</th></tr></thead><tbody><tr><td></td><td><ul style="list-style-type: none">httpclass</td></tr><tr><td>Up</td><td>Down</td></tr></tbody></table>	Enabled	Available		<ul style="list-style-type: none">httpclass	Up	Down
Enabled	Available						
	<ul style="list-style-type: none">httpclass						
Up	Down						
Default Pool	<input type="button" value="+"/> oracle-ebs						
Default Persistence Profile	oracle-ebs-cookie						
Fallback Persistence Profile	None						
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>							

Figure 1.7 Adding the Pool and Persistence profile to the virtual server

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

Unless you are using the BIG-IP LTM system for offloading SSL, this completes the BIG-IP LTM configuration for Oracle E-Business Suite for a Single Web Entry Point as described in the Oracle MetaLink document. If you are configuring your Oracle E-Business Suite for Multiple Web Entry Points, simply repeat all the procedures in this Deployment Guide for each entry point, using the relevant information from the other Web Entry Point.

Configuring the BIG-IP LTM to offload SSL from the E-Business Suite servers

If you plan on using the BIG-IP LTM system to offload SSL from the Oracle E-Business Suite devices, you must perform the following additional configuration procedures on the BIG-IP LTM system.

◆ Important

*If you are configuring the BIG-IP LTM for SSL offload, you must also make changes to the E-Business Suite devices including running the AutoConfig utility provided by Oracle. For more information, see the Oracle MetaLink white paper **Using Load-Balancers with Oracle E-Business Suite Release 12**. The Doc ID is **Note:380489.1***

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 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 **oracle-eps-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 E-Business Suite virtual server

The next task is to modify the Oracle E-Business Suite 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 Portal virtual server you created in *Creating the Oracle E-Business Suite virtual server*, on page 1-11 section. In our example, we click **oracle-eps-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 1-15. In our example, we select **oracle-eps-clientssl**.
5. Click the **Update** button.

This completes the BIG-IP LTM SSL offload configuration for Oracle E-Business Suite for a Single Web Entry Point as described in the Oracle MetaLink document. Again, if you are configuring your Oracle E-Business Suite for Multiple Web Entry Points, simply repeat all the procedures in this Deployment Guide for each entry point, using the relevant information from the other Web Entry Point.

Appendix A: Backing up and restoring the BIG-IP system configuration

We recommend saving your BIG-IP configuration before you begin this configuration. When you save the BIG-IP 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_EBS_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.



2

Configuring the BIG-IP WebAccelerator module for accelerating Oracle EBS

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

Configuring the BIG-IP WebAccelerator module for accelerating Oracle E-Business Suite 12

◆ Important

The following procedures are optional, and only applicable if you have purchased and licensed the WebAccelerator module on the BIG-IP LTM system.

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 E-Business Suite devices as described in Chapter 1 of this Deployment Guide.
- ◆ You must have purchased and licensed the WebAccelerator module on the BIG-IP LTM system, version 9.4 or later.
- ◆ If you are using the BIG-IP LTM version 9.4.2 or later, 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 1-8) 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 is only required for BIG-IP LTM version 9.4.2 and later.
- ◆ This document is written with the assumption that you are familiar with the BIG-IP LTM system, WebAccelerator and Oracle E-Business Suite. 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 E-Business Suite 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 E-Business Suite 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.

For a visual representation, see Figure 1.1 on page 1-2.

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 **oracle-ebs**.
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 E-Business Suite virtual server. In our example, we type **store.oracle.com** (see Figure 2.1).
Note: This is not the name of the BIG-IP LTM virtual server, but the name that resolves to the virtual server in DNS.
 - b) Leave the Entry Type at **Pattern String**.
 - c) Click the **Add** button.

- d) Repeat these sub-steps to add other host names if applicable.
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.

Figure 2.1 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 E-Business Suite in *Creating the Oracle E-Business Suite virtual server*, on page 1-11. In our example, we click **oracle-ebs-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 **oracle-ebs** (see Figure 2.2).
6. Click the **Finished** button. The HTTP Class Profile is now associated with the Virtual Server.

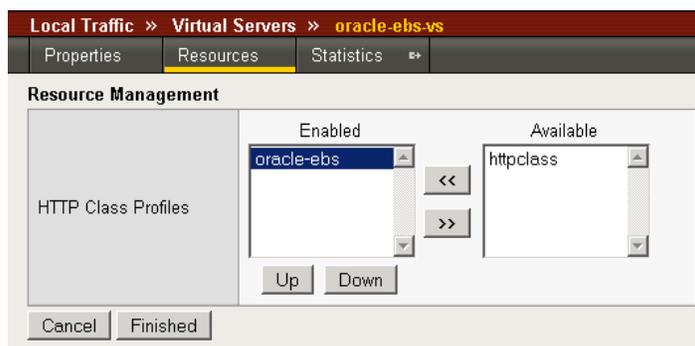


Figure 2.2 Adding the HTTP Class Profile to the Virtual Server

◆ Important

*If you are using the BIG-IP LTM version 9.4.2 or later, 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 1-8) 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. This is only required for BIG-IP LTM version 9.4.2 and later.*

*To create the HTTP profile, use **Creating an HTTP profile**, on page 1-8, 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-ebs**.
4. In the **Description** box, you can optionally type a description for this application.
5. From the **Local Policies** list, select **Oracle 11i**. This is a pre-defined policy created specifically for Oracle E-Business Suite devices.
6. In the **Requested Host** box, type the domain name (FQDN) of your Oracle Portal virtual server. In our example, we type **store.oracle.com**. This should be the same host name you used in Step 6a in the *Creating an HTTP Class profile* procedure.
7. If you have any additional Hosts, click the **Add Host** button and enter the domain name in the Requested Host box.
8. Click the **Save** button.

Configuration >> Applications >> New Application	
General Options	
Application Name:	Oracle EBS
Description: (optional)	WebAccelerator Policy for Oracle E-Business Suite
Policies	
Local Policies:	Oracle 11i
Hosts	
Requested Host	Action
store.oracle.com	Options Delete
Add Host	
Save Cancel	

Figure 2.3 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.



3

Deploying the FirePass controller with Oracle E-Business Suite 12

- Configuring the FirePass controller for deployment with Oracle E-Business Suite
- Creating groups on the FirePass controller
- Limiting access for the Partner group
- Configuring Endpoint security

Deploying the FirePass controller with Oracle E-Business Suite 12

This section of the Deployment Guide shows you how to configure F5's FirePass controller for secure remote access to Oracle® E-Business Suite deployments. The FirePass controller can integrate seamlessly with Oracle Internet Directory (OID) to provide authentication, and simple user maintenance.

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 Portal, 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/>.

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 Oracle E-Business Suite 12, load balanced by a BIG-IP LTM system as described in this Deployment Guide.
- ◆ All of the configuration procedures in this document are performed on the FirePass device.
- ◆ This configuration uses previously defined Oracle Internet Directory (OID) accounts. For information on how to configure OID, consult the Oracle documentation.
- ◆ This Deployment Guide contains procedures for using LDAP (OID) authentication only. There are other authentication methods you can use with the FirePass controller; choose the one most applicable to your configuration.
- ◆ 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.

Configuration scenario

For the scenario used in this Deployment Guide, the Oracle E-Business Suite deployment, along with an OID instance, resides behind a BIG-IP LTM system. There is a requirement to allow employees remote access to

all internal resources using the FirePass device. There is also a requirement for trusted partners to access the Oracle E-Business Suite deployment, although only to a limited subset of the portal, with no other access.

This Deployment Guide describes how to configure the FirePass controller to allow secure remote access to the Oracle E-Business Suite device(s), using OID for authentication, and how to configure the FirePass to give one group of users full access, and restrict users in the partner group to a certain directory. This guide also contains procedures on configuring some endpoint security features, including antivirus checks. For a visual representation of the deployment, see Figure 1.1 on page 1-2.

Configuring the FirePass controller for deployment with Oracle E-Business Suite

To configure the FirePass controller for allowing secure remote access to the Oracle E-Business Suite deployment, you need to complete the following procedures:

- *Connecting to the FirePass controller*
- *Creating groups on the FirePass controller*
- *Limiting access for the Partner group*
- *Configuring Endpoint security*

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 groups on the FirePass controller

In this configuration, we configure two types of groups on the FirePass controller, Resource and Master groups. **Master groups** contain user information, including details about authentication methods. **Resource groups** contain information about applications (resources) that are available to FirePass controller users.

Creating the Resource groups

Resource groups allow you to preconfigure specific applications and access by group, and assign the group to a master group or an individual user. For this configuration, we create two resource groups, one for employees and one for partners, in order to create different access levels to the Oracle E-Business Suite servers.

To configure a resource group

1. From the navigation pane, click **Users**, expand **Groups**, and then click **Resource Groups**.
2. Click the **Create new group** button.
The Group Management - Create New Group screen opens.
3. In the **New group name** box, type a name for your group and click the **Create** button. In our example we type **employees-oracle**. The new group appears on the Resource Groups table.
4. From the Resource Groups table, find the row with the name of the group you just created. In this row, from the Portal access column, click **Edit** (see Figure 3.1). The Web Applications section of the Resource Group page opens.



Group Name	Network access	Application access	Portal access	
Default_resource	Edit	Edit	Edit	Delete
employees-oracle	Edit	Edit	Edit	Delete

Figure 3.1 The Resource groups table

5. Under Web Application Favorites, click **Add New Favorite**. The Favorite options display.
6. Type a name for the Favorite. In our example, we type **Oracle - Employee**. This Favorite link only displays for members of the Employee group.
7. In the **URL** box, type the URL used to access the appropriate Oracle E-Business Suite Server (such as Portal). If you are using a BIG-IP LTM system in front of the Oracle E-Business Suite deployment, this URL should resolve to the Oracle virtual server address in DNS. In our example, we type **http://portal.oraclearn.tc.f5net.com**.
8. Click the **Add to allow list** link to the right of the URL box. This adds the URL to the list of URLs the users are allowed to access.
9. Configure the rest of the settings as applicable to your deployment.

10. Click the **Add New** button.
The new Favorite is added to the list (see Figure 3.2).

Resource Group:

Web Application Favorites [show favorites](#) [allow list](#)

Add New Favorite

Type:

Name:

Web Application Type:

URL:

URL variables:

Use POST for URL variables:

Enforce user-agent:

Open in new window:

Allow list:

Endpoint protection required:

Default:

Figure 3.2 Adding a Web Application Favorite to the Employee group

11. Repeat this entire procedure for the **Partner** resource group, typing appropriate names for the group and the Favorite.
In our example, we type **partners-oracle** for the Resource Group name, and **Oracle Portal - Partners** for the Favorite name.

In Step 7, type the path to the appropriate section of the Oracle E-Business Suite deployment that Partners are entitled to access. For example, the employee Favorite might point to **http://portal.oraclelearn.tc.f5net.com**

while the partner Favorite would point to **http://portal.oraclelearn.tc.f5net.com/partners/**.

Creating the Master groups

FirePass controller master groups are composed of users, authentication methods, and security and policy information. The next task is to create Master groups that will use the resource groups we just created.

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 **Oracle-OID-employee**.
4. In the **Users in group** box, select **External**.
5. From the Authentication method list, select **LDAP**.
6. In the **Copy settings from** list, make sure **Do not copy** is selected (see Figure 3.3).
7. Click the **Create** button.
The General tab of the new Master Group displays.

The screenshot shows a web form titled "Group Management" with a sub-header "Create New Group". The form contains several input fields and buttons:

New group name:	<input type="text" value="Oracle-OID-employee"/>
Users in group:	<input type="text" value="External"/>
Authentication method:	<input type="text" value="LDAP"/>
Routing Table:	<input type="text" value="main"/>
Copy settings from :	<input type="text" value="Do not copy"/>

At the bottom of the form are two buttons: "Create" and "Cancel".

Figure 3.3 *Creating a new Master Group for employees*

8. Click the Resource Groups tab.
The Resource Groups screen opens.
9. From the **Available** box, select the name of the Resource group you created in the *Creating the Resource groups* section. In our example, we select **employees-oracle**.
10. Click the **Add** button to move the group to the **Selected** box, and click the **Update** button. The Resource group is now associated with the Master group.
11. Repeat this procedure to create a new Master group for the Partner resource group. When creating this group, in the **Copy Settings From** list, select the Master group you just created. This way, the authentication settings are automatically created. In our example, we name this group **Oracle-OID-partners**. In Step 9, we select the **partners-oracle** Resource group.

Configuring the Master group for Oracle Internet Directory (LDAP) authentication

The next procedure is configuring the Master group to use OID (LDAP) authentication.

To configure the FirePass Master group to use LDAP authentication

1. From the navigation pane, click **Users**, expand **Groups**, and then click **Master Groups**.
2. Click the name of the Master group you created in the *Creating the Master groups* section. In our example, we select **oracle-OID-employee**.
3. Click the Authentication tab.
The LDAP Authentication tab opens.
4. In the **Host** box, type the host name of your Oracle OID server. In our example, we type **oid.oraclelearn.tc.f5net.com**.
5. In the **Port** box, type the port for the Oracle OID server. In our example we type **636**.
6. Check the **Use SSL connection** box. If you are not using SSL, the port in the preceding Step may be **389**.
7. In the **User DN using template** box, type the user DN template. In our example, we type:
`cn=%logon%,cn=users,dc=oraclelearn,dc=tc,dc=f5net,dc=com`
8. You can optionally click **Test** to test the OID authentication.
9. Click the **Save Settings** button.
10. Repeat this procedure for the **oracle-OID-partners** group.

Master Group:

LDAP Authentication

[Convert authentication method»](#)

Host:

Port: Use SSL connection

Protocol version:

Lookup user's DN using template

User DN template:
 use %logon% in the DN template to insert an user logon. For example "cn=%logon%,ou=it,o=uroam"

Lookup user's DN using query

User DN for query:

Password:

Confirm password:

Search base DN:

Search query template:
 use %logon% in the query template to insert an user logon. For example '&(uid=%logon%)'

Figure 3.4 Configuring the Authentication settings

Limiting access for the Partner group

The FirePass controller allows you to limit access for specific groups on a very granular level. In this scenario, we limit access for the Partner group to only the Favorite we configured earlier, as well as restricting the areas of Oracle E-Business Suite deployment they can access by URL.

To limit access for the Partner group

1. From the navigation pane, click **Portal Access**.
2. Under Web Applications, click **Master Group Settings**.
3. From the **Master Group** list at the top of the page, select the Master Group you created in the *Creating the Master groups* section. In our example, we select **Oracle-OID-partners**.
The configuration settings for the Master group open.
4. In the **Access limitation** section, make sure there is a check in the **Show administrator-defined favorites only** box.

- In the **Access Control Lists** section, configure URL pattern matches to allow and deny based on your deployment. In our example, we type the following (separated by commas) in the **Allow** box to restrict the Partner group to these areas of our Oracle E-Business Suite deployment:

```
http://portal.oraclelearn.tc.f5net.com/partners/*
https://portal.oraclelearn.tc.f5net.com/partners/*
http://login.oraclelearn.tc.f5net.com/*
https://login.oraclelearn.tc.f5net.com/*
```

- We leave the **Deny** box blank, which allows access to all URLs that pass the allow test (see Figure 3.5). The FirePass checks the deny list, then looks for matches in the allow list, then takes the default action.

For more information on configuring the Access Control section, see the online help.

- Click the **Update** button. The new settings take effect after any users currently logged onto the FirePass controller log out.

Master Group:

Access limitation

Show administrator-defined favorites only

Access Control Lists

Restrict using of IP addresses as URL hostnames via Web Applications

Path is case insensitive

Specify a URL pattern in the following format:

 For example: http://*.siterequest.com/abc/*

Deny list:

Allow list:

Default action:

Figure 3.5 Restricting access to the Oracle E-Business Suite deployment

Configuring Endpoint security

One of the strong security features of the FirePass controller is the ability to set endpoint security on an extremely granular level.

In the following procedures, we configure a pre-logout check for anti-virus software on Windows machines. The FirePass controller uses this information to deny Oracle access for members of the Partner Resource group if they do not have the appropriate software. In this configuration example, the FirePass device also denies access to *any* client that is determined to have a virus.

For more information on endpoint security, see the online help.

Creating a pre-logout sequence

The pre-logout sequence allows administrators to create one or more sequences of inspections for items such as installed antivirus programs or OS patch levels.

To configure a pre-logout sequence

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Pre-Logout Sequence**.
2. In the New Sequence section at the bottom of the page, type a name for the sequence in the **Create New Sequence** box. In our example, we type **OracleBasic**.
3. From the **Based on** list, select **template: Collect information with no pre-logout actions**.
4. Click the **Create** button.
The new sequence appears in the Select Sequence to Use table.
5. In the row of the sequence you just created, click the **Edit** button.
Warning - Do not click the radio button next to the sequence yet. If you click the radio button, the **Edit** link will be replaced with the **View** link, and you are not able to edit the sequence.

The Pre-Logout Sequence Editor opens.

6. Move the cursor between **Sequence Start** and the box. A small add **[+]** link appears on the arrow (see the circle marked **1** in Figure 3.6). Click **Add**.
The Change Sequence panel appears on the right.
7. Click the **Check for Antiviruses** option button, and click the **Apply Changes** button.
The Edit Action panel opens.

Note: The Check for Antiviruses is an optional feature on the FirePass controller. If your device does not have this license, you will not see this option.

8. Under **Inspectors**, click **Windows Antivirus Checker**.
The Endpoint Inspector Details page opens in a new window.
9. Configure these options as applicable for your deployment. For more information, click **Help**.
10. Click the **Update** button.

11. In the Sequence pane, find **AV installed**, and click the associated Logon Denied Page link (see the circle marked 2 in Figure 3.6). The End Page Properties pane appears on the right.
12. From the Type box, select **Logon Allowed Page**. This allows a user to logon if they have an antivirus checker installed. You can optionally type a message for failed logons.
13. Repeat steps 11 and 12 for the **Fallback** option.
14. **Optional:** You can click the Logon Allowed Page or Logon Denied Page links for the other options to produce a custom message when a user is denied access. You can also change the actions taken as a result of the virus checker's findings. For example, you might still want to allow a user to login if there is virus checking software installed, but not currently running.

In our example, we click **Logon Denied Page** next to **Virus Detected**, and type a message informing the user there is a virus on their computer.

15. When you are finished, click **Back to Console** in the upper right corner of the screen (see the circle marked 3 in the following figure). You return to the Pre-Logon Sequence main page.

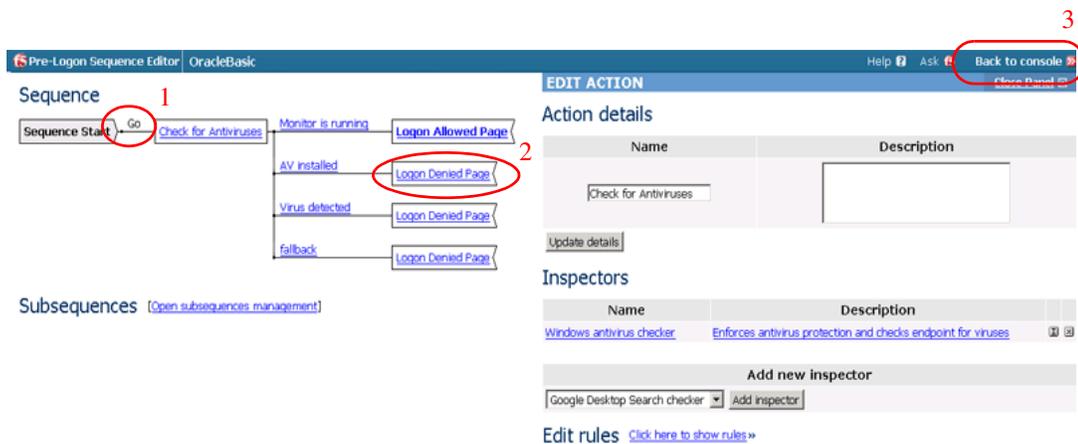


Figure 3.6 The Pre-Logon Sequence Editor

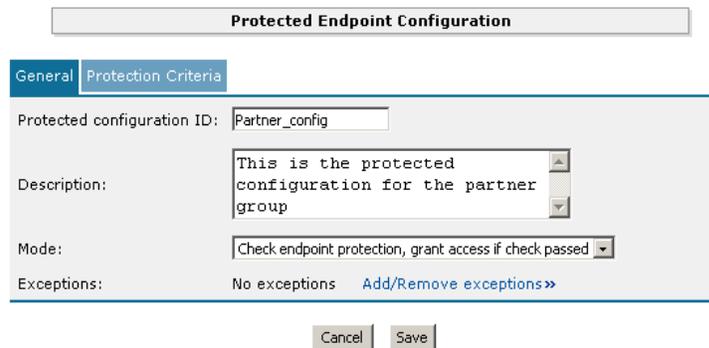
16. From the **Select Sequence to Use** section, click the option button next to the sequence you just created. In our example, we click **OracleBasic**.
17. Click the **Apply** button.

Protected Configurations

Protected Configurations allow administrators to specify the criteria the endpoint systems must meet to enable access to the various resources. In this procedure, we create a protected configuration for the partner group in order make additional security requirements for that group.

To configure Protected Configurations

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Protected Configurations**.
2. Click **New Protection Configuration**.
3. In the Protected configuration ID box, type a name for this configuration. In our example, we type **Partner_config**. You can optionally type a description.
4. Leave the Mode list at the default setting, **Check endpoint protection, grant access if check passed** (see Figure 3.7).



The screenshot shows the 'Protected Endpoint Configuration' dialog box with the 'General' tab selected. The 'Protected configuration ID' field contains 'Partner_config'. The 'Description' field contains 'This is the protected configuration for the partner group'. The 'Mode' dropdown menu is set to 'Check endpoint protection, grant access if check passed'. The 'Exceptions' field shows 'No exceptions' with a link to 'Add/Remove exceptions >>'. At the bottom, there are 'Cancel' and 'Save' buttons.

Figure 3.7 The General tab of the Protected Endpoint Configuration screen

5. Click the Protected Criteria tab.
6. On the menu bar, click **Information Leaks**.

- From the Required safety measures or checks list, select **Cache Cleaner** and click the **Add** button. This will remove content from the cache when a user logs off.

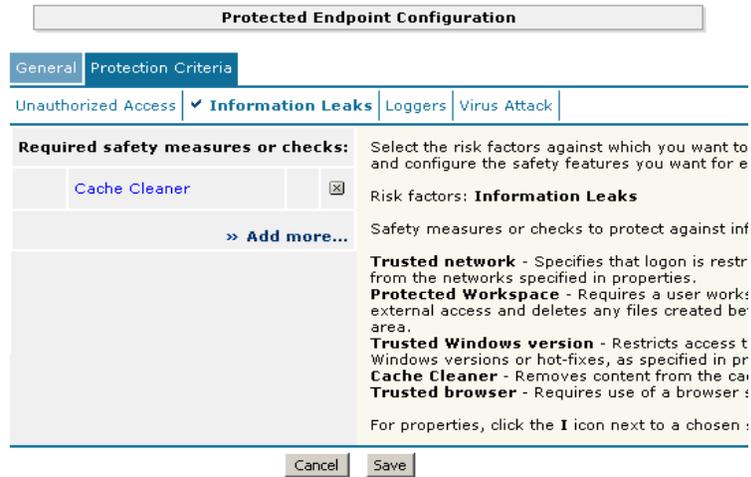


Figure 3.8 The Protection Criteria tab of the Protected Endpoint Configuration screen

Important: The Cache Cleaner feature is currently Windows only. It does not work with Apple Macintosh or Linux systems.

- On the menu bar, click **Virus Attack**
- From the list, select **Antivirus** and click the **Add** button.
- Click the **I** icon next to Antivirus to configure the antivirus properties (see Figure 3.9). The Select trusted anti-viruses screen opens. Configure these properties as applicable for your configuration, and click the **Save** button.

You return to the Protection Criteria tab of the Protected Endpoint Configuration page.

- Click the **Save** button.

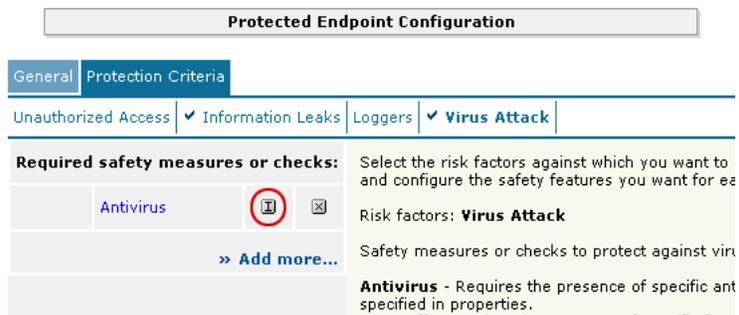


Figure 3.9 The Edit button for Antivirus properties

Protecting the Resources

The next step is to associate the protected configuration you just created with a resource.

To protect the resources

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Protect Resources**.
2. From the Resource Table, expand **Web Applications**.
3. Find the **Partners** resource group (in our example, **partners-oracle**), and click the **Select** link next to the Favorite you configured.
4. From the **Configuration to protect selected resources** list, select the name of the configuration you created in the preceding procedure. In our example, we select **Partner_config**.
5. From the **Protected Configuration** list, select the name of the configuration you created in the preceding procedure. In our example, we type **Partner_config**.
6. Click the **Select** button.
A shield image appears in the row.

Select Protection

Protected configuration Partner_config

Select protected endpoint configuration to protect resource group content (except favorites) against endpoint risk factors

Cancel Select

Figure 3.10 Adding the Protected Configuration to the Resource

Configuring post-logout actions

The final step is to configure a post-logout action in which the FirePass device injects an Active X control or plug-in to clean the client browser's web cache.

To configure the post-logout action

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Post-Logout Actions**.
2. Click a check in the **Inject ActiveX/Plugin to clean-up client browser web cache** box. A list of options displays.
3. Configure these options as applicable for your deployment. In our example, we leave these options at their default settings.

Conclusion

The FirePass controller is now configured to allow secure remote access to the Oracle Application Server E-Business Suite deployments. Remember that the procedures in this Deployment Guide are specific to the scenario described in *Configuration scenario*, on page 3-1. Use this guide as a template, and modify the configuration as applicable to your deployment.