Deployment Guide

Document version: 1.0

What's inside:

ORACLE DATABASE READY

Deploying the BIG-IP ASM with Oracle Database Firewall

Welcome to the F5 Deployment Guide for the F5 BIG-IP® Application Security Manager™ (ASM) with Oracle® Database Firewall. This guide provides instructions on configuring the BIG-IP ASM v11.3 and later for unparalleled security for Oracle Database Firewall deployments.

The BIG-IP ASM and Oracle Database Firewall solution links a web application firewall with a database firewall. The two products share common reporting for web-based attempts to gain access to sensitive data, subvert the database, or execute Denial of Service (DoS) attacks against an organization’s databases. Unified reporting for both the web application firewall and database firewall provides more convenient and comprehensive security monitoring.

When threats to data are detected, they are monitored, alerted, or blocked, and the identity of the user is shared between BIG-IP ASM and Oracle Database Firewall. Malicious or compromised users can be isolated, forced to re-authenticate, or prevented from accessing the application, in real time. Subsequent attacks from the same user can be prevented, diverted, or rendered inert.

For more information on Oracle Database Firewall, see *http://www.oracle.com/technetwork/database/database-firewall/overview/index.html*

For more information on the F5 BIG-IP ASM, see *http://www.f5.com/products/big-ip/application-security-manager.html*

Products and versions tested

Product	Version
BIG-IP ASM	11.3
Oracle Database Firewall	5.0 BUNDLED PATCH 2 (Patch 12317493), 5.1

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/oracle-database-firewall-asm-dg.pdf*

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

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- You must be running BIG-IP version 11.3 or later. If you are using versions 10.2 - 11.2, see *http://www.f5.com/pdf/deployment-guides/oracle-database-firewall-dg.pdf*.
- You must have the BIG-IP ASM licensed and provisioned on your BIG-IP system.
- For information on modifying the Oracle Database Firewall configuration for BIG-IP ASM, see *http://download.oracle.com/docs/cd/E20465_01/doc/doc.50/e18695/f5_big_ip.htm#CEGEHHBA*
- The BIG-IP system must be initially configured with the proper VLANs and Self IP addresses. For more information on VLANs and Self IPs, see the online help or the BIG-IP documentation.
- The configuration in this guide assumes you are using the BIG-IP Local Traffic Manager (LTM) and BIG-IP ASM on the same box. If you are using a stand-alone BIG-IP ASM device, you can follow the ASM configuration, but without the LTM, you will lose certain LTM traffic management functionality.
- For information on configuring the BIG-IP LTM for intelligent traffic management for Oracle Database Firewall deployments, including both Database Policy Enforcement (inline) mode and Database Activity Monitoring mode, see *http://www.f5.com/pdf/deployment-guides/oracle-database-firewall-ltm-dg.pdf*.

Configuration example

Web traffic is secured by BIG-IP ASM and database traffic is secured by Oracle Database Firewall. Security events are correlated and available in consolidated reports.

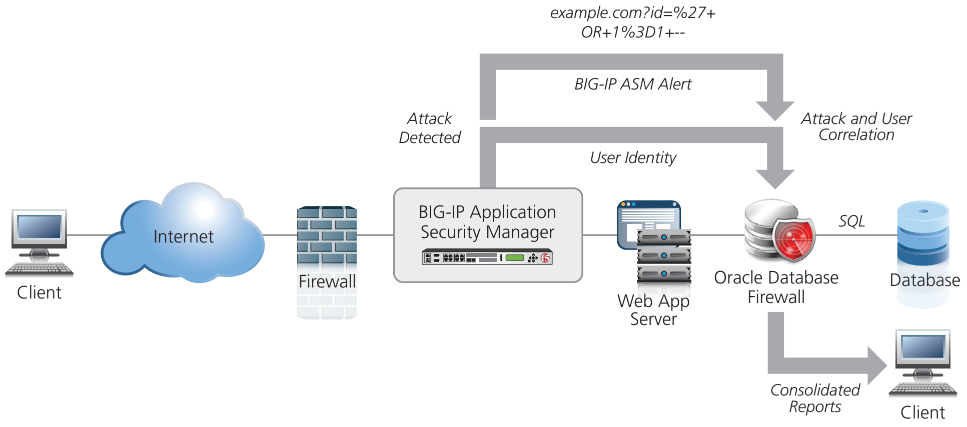

Figure 1: *Configuration example*

Configuring the BIG-IP ASM for Oracle Database Firewall

This section contains procedures for configuring the BIG-IP system for Oracle Database Firewall, as well as a example web application that resides in front of the Oracle Database Firewall and the Oracle database.

Important

Before beginning the BIG-IP ASM configuration, be sure to follow the instructions provided by Oracle for modifying the Oracle Database Firewall configuration for BIG-IP ASM at: http://download.oracle.com/docs/cd/E20465_01/doc/doc.50/e18695/f5_big_ip.htm#CEGEHHBA

Configuring the BIG-IP LTM for your Web application

In this section, we configure the BIG-IP LTM system for your web application. In the following procedures, we use a generic web application running on Oracle WebLogic as an example. You can modify the BIG-IP configuration objects, such as the health monitor and the profiles, to suit your particular application.

If you already have an existing BIG-IP LTM deployment for your applications and want to add the BIG-IP ASM configuration described in this guide, you must make the following changes:

- ***Create a new HTTP Class profile***
  To use the BIG-IP ASM with an existing configuration, you must create a HTTP Class profile with **Application Security** set to **Enabled**. See *Creating the HTTP Class profile on page 6* for instructions. After creating the HTTP Class profile, you must modify the existing virtual server to reference the profile.
- ***Create a new iRule***
  You must create a logging iRule and add it to the virtual server. There are two iRules for logging you can choose between; one monitors the login page and generates a syslog message each time a user logs into the Web application. The other uses the High Speed Logging engine on the BIG-IP system. See *Creating the iRule on page 6* for more details.

If you do not have an existing BIG-IP configuration, use the following procedures.

Creating the HTTP health monitor

The first step is to set up a health monitor for the web application. This procedure is optional, but very strongly recommended. In our example, we create a HTTP health monitor. Choose the monitor that best serves the needs of your application.

To create a health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
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 **http-monitor**.
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. Configure any of the other settings as applicable for your application.
7. Click the **Finished** button. The new monitor is added to the Monitor list.

Creating the Pool

The next step is to define a load balancing pool for the application servers. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. This pool uses the monitor you just created.

To create the pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.
2. Click the **Create** button. The New Pool screen opens.
3. From the **Configuration** list, select **Advanced**.
4. In the **Name** box, type a name for your pool. In our example, we use **weblogic-pool**.
5. In the **Health Monitors** section, select the name of the monitor you created, and click the Add (**<<**) button. In our example, we select **http-monitor**.
6. In the **Slow Ramp Time** box, type **300**. We recommend setting a Slow Ramp Time in conjunction with the Least Connections load balancing method, as to not overwhelm any newly added servers.
7. From the **Load Balancing Method** list, select a load balancing method. We recommend **Least Connections (node)**.
8. In the New Members section, make sure the **New Address** option button is selected.
9. In the **Address** box, type the IP address of one of your application servers.
10. In the **Service Port** box, type the appropriate Port.
11. Click the **Add** button to add the member to the list.
12. Repeat steps 8-10 for each server
13. Click the **Finished** button.

Creating profiles

The BIG-IP system use configuration objects called profiles. A profile is an object that contains user-configurable settings for controlling the behavior of a particular type of network traffic.

In this section, we provide procedures on configuring some common profiles used in our example WebLogic application.

Creating the 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**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **weblogic-http**.
4. From the **Parent Profile** list, select **http**.
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. In our example, we create both WAN and LAN optimized TCP profiles.

To create the TCP profiles

1. On the Main tab, expand Local Traffic, and then click Profiles.
2. On the Menu bar, from the **Protocol** menu, click **TCP**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **weblogic-tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized**.
6. In the **Idle Timeout** row, click the **Custom** box, and then type **1800** in the **Seconds** box.
7. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
8. Click the **Repeat** button.
9. Type a unique name for this profile. We use **weblogic-tcp-wan**.
10. From the **Parent Profile** list, select **tcp-wan-optimized**.
11. In the **Idle Timeout** row, click the **Custom** box, and then type **1800** in the **Seconds** box.
12. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
13. Click the **Finished** button.

Creating the persistence profile

The next profile we create is a Persistence profile. Create this profile if your application requires persistence. In this example, we create a Cookie persistence profile.

To create a new persistence profile

1. On the Main tab, expand Local Traffic, and then click Profiles.
2. On the Menu bar, click **Persistence**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this profile. In our example, we type **weblogic-cookie**.
5. From the **Persistence Type** list, select **Cookie**.
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 a OneConnect profile

The next profile we create is a OneConnect profile. While this profile is optional, with OneConnect enabled, client requests can use existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. For more information on OneConnect, see the BIG-IP LTM documentation.

To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Other** menu, click **OneConnect**.

3. Click the **Create** button.
4. In the Name box, type a name for this profile. In our example, we type **weblogic-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 HTTP Class profile

In this procedure, we create an HTTP Class profile. The HTTP Class only enables the Application Security option in the class, and does not enforce any actual ASM policies.

To create the HTTP class

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Protocol** menu, click **HTTP Class**.
3. Click the **Create** button.
4. In the **Name** box, type a name. In our example, we type **oracle-db-firewall**.
5. From the **Application Security** list, make sure **Enabled** is selected.
6. Configure any of the other settings as applicable for your configuration.
7. Click **Finished**.

Creating the iRule

For this configuration, there are two optional iRules you can use logging. Choose one of the following:

- *syslog iRule,* on this page
  You can use an iRule to monitor the login page and generate a syslog message each time a user logs into the Web application.

- *High Speed Logging iRule on page 7*
  There is a second logging service on the BIG-IP system, called High Speed Logging (HSL). This is a very fast and flexible logging engine that can be used to integrate with various logging systems. This iRule enables high speed logging for the Oracle Database Fireall deployment.

syslog iRule

This iRule monitors the login page, and generates a syslog message every time a user logs in. The syslog message contains the user name of the Web application user, and the cookies associated with that user. The message is routed to the Oracle Database Firewall, which logs the user name against SQL statements generated by the Web application server. This iRule contains the required format of the syslog message, but must be customized to handle the specific login requirements of your Web application.

Because of potential errors with copying and pasting the iRule from this pdf file, it is a downloadable text file. We recommend downloading the text file, making any modifications for your specific login requirements, and then copy and pasting the iRule onto the BIG-IP system.

Use this link to download the iRule:
http://www.f5.com/solution-center/deployment-guides/files/oracle-logging-irule.txt

To create the iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **oracle-logging-irule**.
4. In the **Definition** section, copy and paste the iRule from the text file *http://www.f5.com/solution-center/deployment-guides/files/oracle-logging-irule.txt*.

   Be sure you have made any modifications based on your login requirements.
5. Click the **Finished** button.

High Speed Logging iRule

There is a second logging service on the BIG-IP system, called High Speed Logging (HSL). This is a very fast and flexible logging engine that can be used to integrate with various logging systems. For more information on HSL, please consult the appropriate F5 documentation. The iRule to use HSL has been included here.

To create the iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **oracle-hsl-irule**.
4. In the **Definition** section, copy and paste the iRule from the text file *http://www.f5.com/pdf/deployment-guides/oracle-hsl-irule.txt*.
   Be sure you have made any modifications based on your login requirements.
5. Click the **Finished** button.

Creating the virtual server

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

To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this virtual server. In our example, we type **weblogic-virtual**.
4. In the **Address** box, type the IP address for this virtual server.
5. In the **Service Port** box, type the appropriate port.
6. From the **Configuration** list, select **Advanced**.
7. From the **Protocol Profile (Client)** list, select the WAN optimized TCP profile you created. In our example, we select **weblogic-tcp-wan**.

8. From the **Protocol Profile (Server)** list, select the LAN optimized TCP profile you created. In our example, we select **weblogic-tcp-lan**.
9. From the **OneConnect Profile** list, select the OneConnect profile you created. In our example, we select **weblogic-oneconnect**.
10. From the **HTTP Profile** list, select the HTTP profile you created. In our example, we select **weblogic-http**.
11. *Optional*: From the **SNAT Pool** list, select **Automap**. SNATs can simplify the configuration. For more information on SNAT, see the BIG-IP LTM documentation.
12. In the Resources section, from the **iRules**, **Available** box, select the logging iRule you created, and then click the Add (**<<**) button to move it to the Enabled list. Do not enable both logging iRules.
13. From the **HTTP Class Profiles** list, select the HTTP Class profile you created, and then click the Add (**<<**) button to move it to the Enabled list.
14. From the **Default Pool** list, select the pool you created in Creating the pool, on page 7. In our example, we select **weblogic-pool**.
15. From the **Default Persistence Profile** list, select the persistence profile you created. In our example, we select **weblogic-cookie**.
16. Click the **Finished** button.

This completes the BIG-IP LTM configuration. Continue with configuring the BIG-IP ASM on the following page.

Configuring the BIG-IP ASM

In this section, we configure the Web Application and Policy on the BIG-IP ASM.

Creating the Logging Profile

The first task in the ASM configuration is to create the Logging Profile. The logging profile contains information on where requests to the web application are logged (the Oracle Database Firewall), and which part of requests are logged.

To create the logging profile

1. On the Main tab, expand **Security**, and then click **Event Logs**.
2. On the Menu bar, click **Logging Profiles**.
3. Click the **Create** button.
4. In the **Profile Name** box, type a name. In our example, we type **oracle-logging**.
5. Click the **Application Security** box. The Application Security section appears.
6. Click the **Remote Storage** box.
7. From the **Server Addresses** row, in the **IP Address** box, type the IP address of the Oracle Database Firewall. This should be the same as the Destination IP you defined when configuring the Enforcement Point in your Oracle Database Firewall configuration.

   For information on setting up an Enforcement Point on your Oracle Database Firewall for the BIG-IP ASM, see: *http://download.oracle.com/docs/html/E18695_05/f5_big_ip.htm#CEGFIFEA*
8. In the **Port** box, type **5514**, and then click **Add**. This should be the same as the Destination Port you defined when configuring the Enforcement Point on your Oracle Database Firewall.
9. In the **Storage Format** section, from the **Available Items** box, select each of the following items one at a time, and then click the Add (<<) button after each.

   Important →

   It is critical that these items are in the order below.

   a. violations
   b. unit_hostname
   c. management_ip_address
   d. policy_name
   e. policy_apply_date
   f. x_forwarded_for_header_value
   g. support_id
   h. request_status
   i. response_code
   j. method
   k. protocol
   l. uri
   m. query_string
   n. ip_client
   o. http_class_name
   p. request
10. Click the **Create** button.

Configuring the Security Policy

The next task is to configure the Security policy.

To configure the Security Policy

1. On the Main tab, expand **Security**, and then click **Application Security**.
2. In the **Active Security Policies** list, locate the row that contains the HTTP Class you created in the HTTP Class column, and then click the **Configure Security Policy** link.
3. In the **Deployment Scenarios** section, click **Create a policy manually or use templates (advanced)** and then click the **Next** button.
4. On the Configure Security Policy Properties page, complete the following:
   a. From the **Application Language** list, select an application language.
   b. From the **Application-Ready Security Policy** list, select **Rapid Deployment security policy**.
5. Click **Next**.
6. Make sure the **Signature Staging** box is checked.
7. Click **Next**.
8. Review the settings and then click **Finished**.
9. On the Main tab, expand **Security**, and from the **Application Security** menu, click **Blocking**.
10. Make sure the name of your policy is in the **Current edited policy** list.
11. In the Violations List section, we recommend you leave the **Enforcement mode** set to **Transparent** until you have had a chance to review the configuration and make any necessary changes before switching to Blocking.
12. We recommend you enable the following required events. For each of the following events, click a check in the **Learn** and **Alarm** boxes.

    RFC Violations section

    a. **Evasion technique detected**

    Access Violations section

    a. **Request length exceeds defined buffer size**
    b. **Illegal HTTP status in response**

    Input Violations section

    a. **Illegal dynamic parameter value**
    b. **Illegal meta character in header**
    c. **Illegal meta character in parameter value**
    d. **Illegal parameter data type**
    e. **Illegal parameter numeric value**
    f. **Illegal parameter value length**
    g. **Illegal query string or POST data**
    h. **Illegal static parameter value**
    i. **Parameter value does not comply with regular expression**

13. Click the **Save** button.

Configuring the Security policy to use the Logging profile

The next task is to configure the Security policy to use the logging profile you created.

To configure the policy to use the logging profile

1. On the Main tab, expand **Local Traffic**, and click **Virtual Servers**.
2. Click the name of the virtual server you made in *Creating the virtual server on page 7*.
3. On the Menu bar, from the **Security** menu, select **Policies**.
4. Ensure that the Application Security Policy setting is Enabled and that Policy is set to the security policy you want.
5. From the **Log Profile** list, select **Enabled**.
6. In the **Profile** section, from the **Available** list, select the name of the Logging profile you created in *Creating the Logging Profile on page 9* and then click the Add (**<<**) button.
7. Click the **Update** button.

Creating new custom Attack Signature Sets

By default, the BIG-IP ASM firewall blocks SQL injection attacks on web servers. However, for this integration to work properly, new attack signatures are needed that only monitor and alarm SQL injection attacks. BIG-IP ASM will be configured to allow the SQL injections to pass through to the Oracle Database Firewall, so it can see the attack and take appropriate action based on the Oracle DBFW rules.

To create new SQL Attack Signature sets

1. On the Main tab, expand **Security**, point to **Options**, **Application Security**, **Attack Signatures** and the click **Attack Signature Sets**.
2. Click **Create**.
3. In the **Name** box, type a unique name. In our example we type My_OracleDB.
4. In the **Default Blocking Actions** row, clear the check from the **Block** box.

Important →

*You must ensure the **Block** setting is cleared (not checked).*

5. In the **Assign To Policy By Default** row, clear the check box from **Enabled**.
6. Leave **Attack Type** set to **All**.
7. In the **Systems** section, from the **Available Systems** list, select **General Database**, and also select the type of Database you are using and then click the Add (<<) button.
   In our example, we choose **General Database** and **Oracle**.
8. Click **Create**.

   Next, you create a second Attack Signature for your web server.
9. Click the **Create** button.
10. In the **Name** box, type a unique name. In our example we type My_OracleWebApp.
11. In the **Default Blocking Actions** row, ensure the **Block** box is checked.

Important → *You must ensure the **Block** setting checked.*

12. In the **Systems** section, from the **Available Systems** list, select the type of Operating System you are using and then click the Add (**<<**) button.
13. From the **Available Systems** list, select the type of web server platform you are using. In our example we choose **Apache** and **BEA Systems WebLogic Server**
14. Click **Create**.

Configure the Security Policy

Next we configure the Security Policy to use the new Attack Signature Sets.

To update the Security policy

1. On the Main tab, expand **Security**, point to **Application Security** and then click **Attack Signatures**.
2. From the **Current edited policy** list, ensure that the edited security policy is the one you created for this implementation.
3. In the **Attack Signature Sets Assignment** setting, from the **Available Signature Sets** list, select the attack signature sets that you just created and then click the Add (<<) button.
4. Click the **Save** button.
5. Click the **Apply Policy** button in the upper right.

Change the Security Policy to Blocking (Enforcement) Mode.

After verifying that the Web traffic is flowing properly, and that SQL traffic is flowing through the Database Firewall properly, you will want to place the ASM into Blocking mode, which will stop malicious HTTP and SQL attacks on your web application. Make sure that there are no false positives showing up in the ASM or DBFW logs before placing the ASM in Blocking Mode.

To place the Security Policy in Blocking Mode, use the following procedure. If you do see false positive, you can always change the Policy back to Transparent Mode temporarily.

To enable Blocking mode

1. On the Main tab, expand **Security**, and then click **Application Security**.
2. In the **Active Security Policies** list, click the name of the Security Policy you created.
3. In the **Enforcement Mode** row, click the **Blocking** button.
4. Click the **Save** button.

Set the Oracle Database Signature set to non-Blocking.

After setting the Enforcement Mode to Blocking, all Signature Sets are changed to Blocking. Go back to the Oracle DB Signature Set and clear the Block checkbox.

To Update the Policy

1. On the Main tab, expand **Security**, point to **Application Security** and then click **Attack Signatures**.
2. From the **Current edited policy** list, ensure that the edited security policy is the one you created for this implementation.
3. In the **Attack Signature Sets Assignment** setting, from the **Assigned Signature Sets** list, check the box for Generic Detection Signatures and then click the Remove (**>>**) button.
4. Clear the **Block** check box on the first Signature Set you created. This was **My_OracleDB** in our example.
5. Click the **Save** button.
6. Click the **Apply** Policy button in the upper right.

Configuring syslog-ng.conf

➲ *NOTE: You do not need to follow this procedure if you selected the High Speed Logging iRule earlier.*

To enable the iRule syslog messages to be transmitted to the Oracle Database Firewall, it is necessary to log in to the BIG-IP command line and execute the following BIG-IP ASM command, which modifies **/etc/syslog-ng /syslog-ng.conf** (do not modify the file directly, because changes will not persist after you restart the system):

To configure syslog-ng.conf

1. On the BIG-IP system, start a console session. Log on as **root**.
2. Use the TMSH command line to enable iRule syslog messages to be transmitted to the Oracle Database Firewall. Use the appropriate command syntax (all on one line), replacing the red text as noted below:

   a. To enter TMSH, type **tmsh** and then press Enter.

   b. Use the following command syntax:

   ```
   modify sys syslog remote-servers add {<dbfw_server_name>
   {host <dbfw_IP_address> remote-port <dbfw_port>}}
   ```

   Where ***dbfw_server_name*** is the name of your server, and ***dbfw_IP_address*** and ***dbfw_port*** are the IP address and port number of the Oracle Database Firewall. This should be the same IP address and port of the server you specified in Steps 6 and 7 of *Creating the Logging Profile on page 9.*

   In our example, the command is:

   ```
   modify sys syslog remote-servers add { d_dbfw {host 192.168.0.181 remote-
   port 5514}}
   ```

c. You must also save the change to the system configuration using the following command:

```
save sys config
```

For more information on syslog TMSH commands, please see Support Solution # SOL13083 on support.f5.com.: *http://support.f5.com/kb/en-us/solutions/public/13000/000/sol13083.html?sr=18091813*

This completes the configuration.

Document Revision History

Version	Description
1.0	New deployment guide for BIG-IP v11.3

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com