Deploying the BIG-IP APM v11 with Oracle Access Manager

Welcome to the F5 deployment guide for the BIG-IP Access Policy Manager (APM) and Oracle Access Manager. This guide describes how to configure the BIG-IP APM for Oracle Access Manager when you are looking to offload the WebGate functionality. This simplifies the OAM deployment by eliminating WebGate Agents from the application servers and consolidating the proxy layer onto the network infrastructure.

F5 Networks BIG-IP APM is a flexible, high-performance access and security solution that provides unified global access to your business-critical applications and network.

Oracle Access Manager helps enterprises create greater levels of business agility, ensure seamless business partner integration, and enable regulatory compliance.

For more information on Oracle Access Manager, see *www.oracle.com* and then *Products and Services > Oracle Fusion Middleware > Identity Management > Oracle Access Management.*

For more information on BIG-IP APM, see *https://f5.com/products/modules/access-policy-manager*

Products and versions tested

Product	Version
BIG-IP APM	11.1 - 11.6
Oracle Identity Management	11.1.1.0, 11.1.2
Oracle Access Manager	11.1.1.5, 11.1.2
Deployment Guide version	1.5 (see *Document Revision History on page 13)*
Last updated	03-04-2016

➲ **Note:** *Our Oracle Identity Management 11gR1 implementation was deployed according to the Oracle® Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management 11g Release 1 (11.1.1) Part Number E12035-02* and 11g Release 2 (11.1.2) Part number E27301-01.

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/oracle-oam-apm-11-dg.pdf.*

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

Contents

Prerequisites and configuration notes 3

Configuration example 4

Preparation Worksheet 5

Modifying the Oracle configuration to support BIG-IP APM 6

Updating the host identifier for the APM WebGate agent 6

Configuring the BIG-IP APM 7

Creating an AAA server 7

Creating the traffic management objects on the BIG-IP system 8

Modifying name resolution settings 9

Disabling the WebGate on the web server 9

Verifying the configuration 9

Troubleshooting and Verification Tools 10

Eamtest tool on the BIG-IP system 10

Log Messages 10

Appendix: DNS and NTP settings on the BIG-IP system 12

Document Revision History 13

Prerequisites and configuration notes

The following are prerequisites and configuration notes for this implementation:

- This deployment guide provides instructions for configurations with BIG-IP Version 11.1 through 11.6 and OAM 11g R1 and R2 only. For information on other versions, please consult the appropriate documentation.
- For BIG-IP APM, you must have configured NTP and DNS on the BIG-IP system. See *Appendix: DNS and NTP settings on the BIG-IP system on page 12* for configuration information.
- You must have an existing Oracle Access Manager 11g environment running and configured before using the Access Policy Manager integration with OAM. The APM module uses the AccessGate Software Development Kit from Oracle to create a functional Resource WebGate Agent running on the BIG-IP. This Agent is built with the OAM 10g SDK, and is compatible with OAM 11g.
- New If you are installing a new Oracle Access Manager implementation (not protecting any current web server application and no Oracle WebGate agents deployed on any web servers), follow the OAM installation documentation to install the software and verify that the various components are up and functional.

  To connect to the BIG-IP APM, there are two important configuration steps that must take place. Perform the following from the OAM web console. For specific information, see the Oracle documentation.:

  - Create a new Host Identifier, which should be the FQDN of the BIG-IP virtual server that clients are accessing via a web browser.
  - Create WebGate Agent with a unique WebGate name, as typical in an OAM installation. This must be a 10g WebGate. Remember the name you use, as you also enter it in the BIG-IP APM Policy configuration, as described in this document.
- This deployment guide currently supports the following security transport modes: Open, Simple Security and Cert modes.
- The WebGate Agent behind the BIG-IP APM must be disabled on the Application Web Tier servers.
- You must have Administrator privileges to your OAM installation. This is required, as you need to make minor modifications to your policy. For more information, see Modifying the Oracle configuration, on page 18.
- Your OAM policies must be properly configured, such as policies for authentication and authorization failures. The BIG-IP APM relies on the OAM server for defined policies, otherwise the flow/connection will be dropped for an undefined behavior.
- You must have the BIG-IP Access Policy Manager software module (APM) properly licensed and provisioned on your BIG-IP system. For more configuration options on the BIG-IP Access Policy Manager, see the ***Configuration Guide for BIG-IP Access Policy Manager*** for your version, available on Ask F5 (*http://support.f5.com/kb/en-us/products/big-ip_apm.html)* and then select your APM version from the list on the right).
- **Important:** The easiest and simplest way to deploy BIG-IP APM with OAM (as described in this guide) is to use an existing OAM 11g deployment with an existing 10g WebGate on a web server with existing Authentication and Access Policies that have been tried and tested as valid. BIG-IP APM can be easily integrated by simply adding a new Host Identifier to the list of existing WebGate hosts. We strongly recommend this scenario for a successful deployment.
- The configuration in this guide for replacing the WebGate agents is specific to 10g WebGates.
- For additional information, see the BIG-IP APM ***OAM Integration Guide*** for your version, available on Ask F5 (*http://support.f5.com/kb/en-us/products/big-ip_apm.html*) and then select your APM version from the list on the right).

Configuration example

In this guide, we demonstrate an architecture where Oracle Access Manager provides authorization services to an application. Allowing BIG-IP APM to offload the 10g WebGate functionality simplifies the Oracle OAM deployment by eliminating WebGate Agents from the application servers and consolidating the proxy layer onto the network infrastructure.

In this example, the BIG-IP system is first configured to provide access to the application. Once this configuration is completed and tested, the addition of OAM functionality is then added to provide restricted access to the application. The APM module functions as a WebGate which connects to the OAM server and enforces web access policies that have been defined by the OAM administrator.

Figure 1 shows a logical configuration example before the BIG-IP APM has been implemented, and a BIG-IP Local Traffic Manager is directing traffic to the WebGate Proxy. Figure 2 shows the logical configuration example after the BIG-IP APM has been implemented.

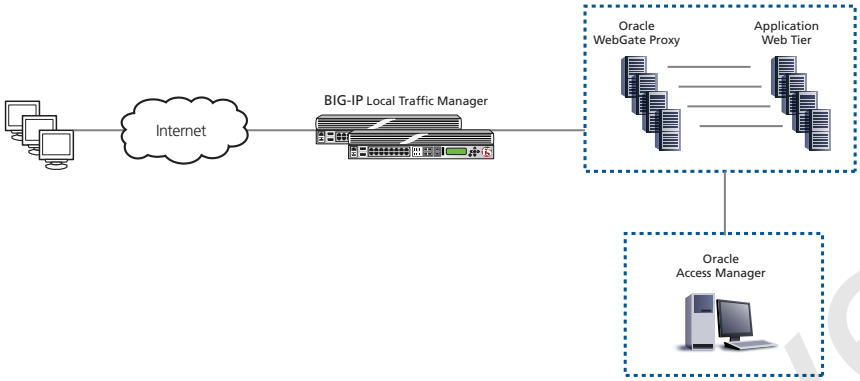


Figure 1: *Logical configuration example before the BIG-IP APM*

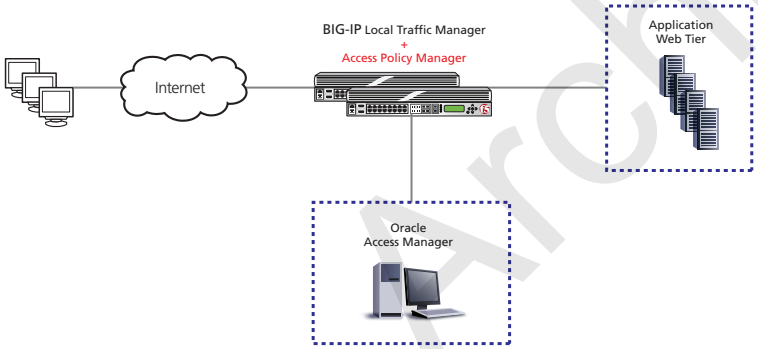


Figure 2: *Logical configuration example including the BIG-IP APM*

Preparation Worksheet

Before beginning this deployment, it is helpful to gather some information from your Oracle OAM deployment in advance to have ready once you begin the BIG-IP configuration. Use the following worksheet to gather the information you will need while configuring the devices. You might find it useful to print this table and then enter the information.

➲ **Note:** *Although we show space for 10 pool members, you may have more or fewer members in each pool.*

Configuration object	Your Value
Oracle Access Manager devices	
Access Server Name	
OAM Server Host name (in FQDN format)	
OAM Server TCP Port (default is 5575)	
OAM Server Transport Security mode:	**Open | Simple | Cert**
- If using Cert mode	
SSL Certificate from OAM server	
SSL Key from OAM server	
You also need to import (and trust) the CA cert:	
key = aaa_key.pem	
webgate certificate = aaa_cert.pem	
CA certificate = aaa_chain.pem	
- If using Simple mode	
Global Access Protocol Passphrase	
OAM user name with administrative permissions	
Associated password	
OAM 10g WebGate agent	
OAM 10g WebGate agent name	
OAM 10g WebGate agent Transport Security mode	
Application information	
IP addresses and TCP port for each of the application servers that are a part of this deployment (for the BIG-IP load balancing pool).	1) 2) 3) 4) 5) 6) 7) 8) 9) 10)
IP Address to be used for the BIG-IP virtual server for the application server deployment	

Modifying the Oracle configuration to support BIG-IP APM

In this section, we modify the Oracle configuration to use the BIG-IP APM.

Important *The following information is provided as general guidance for configuring Oracle Access Manager. For specific instructions on modifying the Oracle configuration, see the Oracle documentation.*

Updating the host identifier for the APM WebGate agent

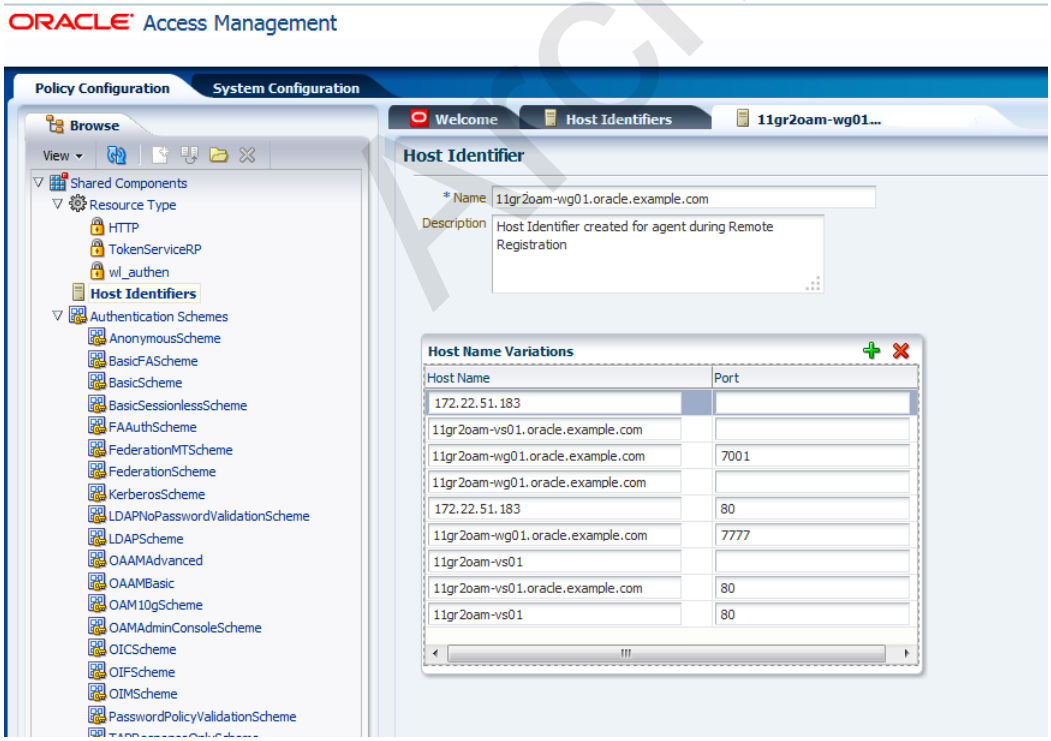
The first task in this section is to update the existing Host Identifier for the existing 10g WebGate to add the BIG-IP APM WebGate agent's FQDN and any alternative host names, virtual servers, or IP addresses with and without all applicable port numbers.

This is an update to the existing 10g WegGate you defined in OAM during remote registration.

In this example, the DNS FQDN name we have configured for the APM agent is **11gr2oam-wg01.oracle.example.com**.

To update an existing host identifier

1. From the Oracle Access Manager web console, on the **Policy Configurations** tab, from the navigation pane, click **Host Identifiers**, and then click the **Edit** icon.
2. In the **Host Name Variations** box, click the Add (**+**) button.
3. In the **Host Name** field, type the FQDN of the BIG-IP virtual server that clients are accessing via a web browser.
4. In the **Port** field, type the appropriate port.
5. Repeat steps 3-5 for all combinations of host, IP address, and port that are used to identify the web server.
   You should have at least **six** entries, one for the FQDN and port, one for the IP address and port, and one for the host name and port, and three without a port.
6. Click the **Apply** button.



Configuring the BIG-IP APM

In this section, we configure the BIG-IP Access Policy Manager. See the Help tab or the APM documentation for specific instructions on configuring individual objects.

Creating an AAA server

The first task is to create the AAA server on the BIG-IP APM. Use the following table for guidance on creating the AAA server.

To begin the AAA Server configuration, from the Main tab of the BIG-IP Configuration utility, expand **Access Policy** and then click **AAA Servers**. On the Menu bar, select **AAA Servers by Type**, and then click **Oracle Access Manager**. Click the **Create** button.

AAA Server Field	Description/Notes
Name	Type a unique name
Access Server Name	Type the name of the Access Server (such as *oam_server1*). This name should match the Access Server name you created in the Oracle configuration.
Access Server Hostname	Type the host name of the Access Server you entered above in FQDN format. ***Important:*** This must be in FQDN format.
Access Server Port	**5575** is the default. If you have changed the port, type it here.
Admin ID	Type the administrative ID that has permissions to log into the Access Server
Admin Password	Type the associated password
Verify Password	Retype the password
Transport Security Mode	**Simple**[1], **Open** or **Cert** (must match your OAM configuration). For **Cert** mode, you must import the AccessGate files. See the APM OAM Integration Guide[2] for instructions.
Global Access Protocol Passphrase[3]	Type the Global Access Protocol Passphrase
Verify Passphrase[3]	Retype the passphrase
AccessGate Configuration	
Name	**<agent_name>** (must match the agent name added to the OAM server; each WebGate agent must be registered with the OAM Server)
Description	You can optionally type a description
Password	**<agent_password>** (the associated password for the WebGate agent)
Enable	Select **Enable** from the list

[1] Simple mode is one of the transport security level between Oracle components, for example, Identity servers, Policy Managers, Access Servers, and associated WebGates . It performs SSLv3/TLSv1.0 secure transport between Oracle components using dynamically generated session keys. For more information about the other available security levels, refer to the Identity and Common Administration Guide provided by Oracle.

[2] See AskF5 for the APM documentation. For example, for 11.2, the procedure can be found at: *https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-oam-integration-11-2-0/2.html*

[2] These fields only appear if you select Simple as the Transport Security Mode.

Creating the traffic management objects on the BIG-IP system

The next task is to configure the monitor, profiles, pool, and virtual server on the BIG-IP system. This is the web application that will be protected by APM and OAM. In our configuration, we are using WebLogic as an example.

The following table contains a list of BIG-IP LTM configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**HTTP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name
	Health Monitor	Select the monitor you created above
	Load Balancing Method	**Least Connections (Member)**
	Address	Type the IP Address of the web server
	Service Port	Type the appropriate port. We use **7001** for our WebLogic example. Repeat Address and Service Port for each server
Profiles (*Main tab-->Local Traffic -->Profiles*)	***HTTP*** (*Profiles-->Services*)	**Name** Type a unique name
		Parent Profile **http**
	TCP WAN (*Profiles-->Protocol*)	**Name** Type a unique name
		Parent Profile **tcp-wan-optimized**
	TCP LAN (*Profiles-->Protocol*)	**Name** Type a unique name
		Parent Profile **tcp-lan-optimized**
Virtual Server (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name
	Address	Type the IP address you want to use for this virtual server. Clients will use this address for access to the deployment
	Port	Type the applicable service port.
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created above
	HTTP Profile	Select the HTTP profile you created above
	OAM Support	Check the **Enabled** box to enable OAM support
	AccessGate	From the AccessGate list that appears, select the appropriate AccessGate
	Default Pool	Select the Pool you created above

[1] You must select **Advanced** from the **Configuration** list for these options to appear

Modifying name resolution settings

Before sending traffic to the BIG-IP system, your DNS administrator may need to modify any DNS entries for the OAM implementation to point to the BIG-IP system's virtual server address. For instructions on modifying name resolution, contact your DNS administrator.

Disabling the WebGate on the web server

You can now disable the WebGate on the web server, as the BIG-IP APM is now acting as the WebGate agent. See Reference "23.8 Verifying httpd.conf Updates for Webgates" in the Oracle Fusion Middleware Administrator's Guide for Oracle Access Management 11g Release 2 (11.1.2) Part Number E27239-03
http://docs.oracle.com/cd/E27559_01/admin.1112/e27239/apch2ihs.htm#AIAAG4921

To disable the WebGate on Oracle HTTP Server (OHS) or other Apache-based servers, open **httpd.conf** and then comment out the entire section starting with:

```
#*** BEGIN Oblix NetPoint Webgate Specific ****
```

Save the file, and then restart the server.

For other server types, such as Microsoft IIS, consult the appropriate documentation.

Verifying the configuration

To verify the configuration is working properly, access the protected resource from a workstation and verify the BIG-IP APM is functioning in the same manner as the WebGate you disabled. Access to the protected resource should follow the configured policy.

When you need to add additional web servers to the configuration, simply add the IP address and port to the BIG-IP Pool. Remember to disable the existing WebGate on those servers before adding them to the Pool.

Troubleshooting and Verification Tools

The BIG-IP APM module includes tools from both F5 and Oracle to use for checking the configuration and functionality of the integration. These two tools are eamtest from F5, and a configuration utility from Oracle called configureAccessGate. Both of these are CLI tools require root level access to the BIG-IP system.

Eamtest tool on the BIG-IP system

The eamtest tool is an Enterprise Access Management client tool that can be used to test/verify the functionality of the OAM agent and the policies on the OAM server. This tool assumes that the BIG-IP WebGate agent has already been configured and started successfully. This tool was introduced with BIG-IP version 11.1.

eamtest tool usage

The following shows the options available when using the eamtest tool.

```
usage: eamtest [options]
-n test number[default: 1]
-c concurrency[default: 1]
-r resources (i.e., http://<host>:<port/<location>
-v virtual IP address (for host header validation)
-d debug level[default: 5, range: 0-7]
```

The following is an example command:

```
eamtest -r "GET https://172.30.55.53/" -v "172.30.55.53" -d 6
```

eamtest tool example

In the following example, the resource is a full URL path to an HTML object on a web server, the user name is “user1”, the password is “abcd1234”, and the debug level is set to “6”.

```
eamtest -r "GET https://oam10gwebgate1.pd1.lab.fp.f5net.com/portal/SDSSO/basic/" -v "172.30.55.53" -d 6
```

Log Messages

There are two log files on the BIG-IP used by the APM-OAM Integration.

- **/var/log/apm** - logs messages from the APM WebGate agent configured on the BIG-IP.
- **/var/log/oblog.log** - logs messages from the Oracle SDK software.

Log Levels

The BIG-IP eam software automatically logs BIG-IP WebGate events at the following levels:

BIG-IP	Oblog
LOG_EMERG	LOGLEVEL_FATAL
LOG_ALERT	LOGLEVEL_FATAL
LOG_CRIT	LOGLEVEL_FATAL
LOG_ERR	LOGLEVEL_ERROR
LOG_WARNING	LOGLEVEL_WARNING
LOG_NOTICE	LOGLEVEL_WARNING
LOG_INFO	LOG_LEVEL_DEBUG1
LOG_DEBUG	LOG_LEVEL_DEBUG1

The **log.sso.level** is the parameter used to control the log level within the oblog.log. The log level can be changed via the CLI using the **db log.sso.level** command.

If other OAM logging is desired, the admin needs to manually edit the **oblog_config.xml** file under the **$ACCESS_GATE_HOME/oblix/config** directory. There are different log levels, from LOGLEVEL_FATAL to LOGLEVEL_ALL. For more detail on logging, see the appropriate Oracle documentation: *http://docs.oracle.com/cd/E15586_01/doc.1111/e15478/log_wg.htm*

Automatic BIG-IP default logging level must be disabled by editing the EAM startup script.

1. Open the **/etc/bigstart/startup/eam** file for edit, and change:
   `export AUTO_OBLOG_CONFIG=true` to `export AUTO_OBLOG_CONFIG=false`
2. Restart the eam plugin by issuing the command: `bigstart restart eam`.

There is also a similar tool, **oamtest**, which can be helpful for troubleshooting. Use the **help** command for information on using oamtest.

This completes the troubleshooting and logging section.

Appendix: DNS and NTP settings on the BIG-IP system

For BIG-IP APM, you must have DNS and NTP settings configured. If you have not already configured DNS and NTP, use the following procedures.

Configuring DNS and NTP settings

If you are configuring the iApp to use BIG-IP APM, you must configure DNS and NTP settings on the BIG-IP system before beginning the iApp.

Configuring the DNS settings

In this section, you configure the DNS settings on the BIG-IP system to point to a DNS server that can resolve your Active Directory server or servers. In many cases, this IP address will be that of your Active Directory servers themselves.

Note: *DNS lookups go out over one of the interfaces configured on the BIG-IP system, not the management interface. The management interface has its own, separate DNS settings.*

Important *The BIG-IP system must have a self IP address in the same local subnet and VLAN as the DNS server, or a route to the DNS server if located on a different subnet. The route configuration is found on the Main tab by expanding **Network** and then clicking **Routes**. For specific instructions on configuring a route on the BIG-IP system, see the online help or the product documentation.*

To configure DNS settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **DNS**.
3. In the **DNS Lookup Server List** row, complete the following:
   a. In the **Address** box, type the IP address of a DNS server that can resolve the Active Directory server.
   b. Click the **Add** button.
4. Click **Update**.

Configuring the NTP settings

The next task is to configure the NTP settings on the BIG-IP system for authentication to work properly.

To configure NTP settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **NTP**.
3. In the **Address** box, type the fully-qualified domain name (or the IP address) of the time server that you want to add to the Address List.
4. Click the **Add** button.
5. Click **Update**.

To verify the NTP setting configuration, you can use the **ntpq** utility. From the command line, run **`ntpq -np`**.

See *http://support.f5.com/kb/en-us/solutions/public/10000/200/sol10240.html* for more information on this command.

Document Revision History

Version	Description	Date
1.0	New document	08-06-2012
1.1	- Added support for BIG-IP APM 11.2 and 11.3 - Added support for OAM 10g R2 (11.1.2) - Added support for Transport Security **Cert** mode - Removed instructions for creating a new 10g WebGate - Modified the section “Adding a new host identifier for the APM WebGate Agent” to be *Updating the host identifier for the APM WebGate agent on page 6.* - Added instructions to *Disabling the WebGate on the web server on page 9*	06-03-2013
1.2	- Added support for BIG-IP APM 11.4 - Modified *Eamtest tool on the BIG-IP system on page 10* to remove the "-i" option, which is not available. Updated the code examples.	10-21-2013
1.3	- Modified *Eamtest tool on the BIG-IP system on page 10* to remove the -u and -w options. These options were not useful in testing/troubleshooting as the tool takes the credentials from the AAA OAM object directly.	09-04-2014
1.4	- Clarified the instructions in *Disabling the WebGate on the web server on page 9* - Added a note in *Prerequisites and configuration notes on page 3* stating the WebGate replacement functionality described in this guide is for version 10g WebGates. - Corrected the location of the startup script at the end of the section *Log Messages on page 10* - Expanded the certificate section for cert mode in the *Preparation Worksheet on page 5*	02-02-2015
1.5	- Added support for BIG-IP APM 11.4.1 - 11.6 - Added a prerequisite concerning steps to take if you are deploying a new Oracle OAM implementation. - Updated the links to F5 and Oracle documentation on pages 1 and 3.	03-04-2016

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