DEPLOYMENT GUIDE
Version 1.1

Deploying the BIG-IP Access Policy Manager with IBM, Oracle, and Microsoft

Important: This guide has been archived. While the content in this guide is still valid for the products and versions listed in the document, it is no longer being updated and may refer to F5 or third party products or versions that have reached end-of-life or end-of-support.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

1

Deploying the BIG-IP APM with IBM, Oracle, and Microsoft

- Introducing the BIG-IP APM deployment guide

Introducing the BIG-IP APM deployment guide

Welcome to the F5 BIG-IP Access Policy Manager (APM) deployment guide. This guide contains guidance on configuring the BIG-IP APM for IBM Tivoli Access Manager for e-business, Oracle Access Manager, and Microsoft Active Directory (for Exchange 2010 OWA and SharePoint).

BIG-IP APM is a flexible, high-performance access and security solution. BIG-IP APM drives identity into your network to provide secure, context-aware user access to web applications while simplifying authentication, authorization, and accounting (AAA) management.

BIG-IP APM provides a simplified, central point of control based on access policies, giving you granular control of users' web access. An optional endpoint security service validates devices with policy to protect your organization from virus or malware infections, accidental data loss, and rogue device access. The advanced Visual Policy Editor makes it easy to create individual and group access policies for many different identities and web authentication environments.

For more information on BIG-IP APM, see ***www.f5.com/products/big-ip/product-modules/access-policy-manager.html***

This guide contains the following chapters:

- *Configuring the BIG-IP APM for Tivoli Access Manager for e-business*, on page 2-1
- *Configuring the BIG-IP APM for Oracle Access Manager*, on page 3-1
- *Configuring the BIG-IP APM for Exchange Server 2010 Access*, on page 4-1

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

Revision history

Revision history:

Document Version	Description
1.0	New deployment guide
1.1	Corrected the Start URI for the SSO configuration on page 4-3 to remove an extraneous login.aspx at the end of the URI.

2

Deploying the BIG-IP APM with IBM Tivoli Access Manager for E-Business

Configuring the BIG-IP APM for Tivoli Access Manager for e-business

The first chapter of this deployment guide shows how to deploy the BIG-IP APM with IBM® Tivoli® Access Manager for e-business. Tivoli Access Manager for e-business provides an integrated security managed platform for authentication services, access control or authorization services. By integrating BIG-IP APM, it is possible to proxy and complete the authentication of users that authenticate against Tivoli directory services.

In this guide, we demonstrate an architecture where Tivoli Access Manager provides authentication services to a series of applications. Instead of authenticating users directly at the application layer BIG-IP APM is used for authentication.

In this example, BIG-IP APM is used to check the client's computer for any viruses, then to authenticate the user and finally to cache the user and provide access only to the resources indicated by the administrator.

Prerequisites and configuration notes

- The BIG-IP system must have DNS and NTP configured. See product documentation on how to configure DNS and NTP, available on ***Ask F5***.

Product versions

Product Tested	Version Tested
BIG-IP APM	10.1
Tivoli Access Manager for e-business	6.1

Configuring the BIG-IP APM

Use the following procedures to configure the BIG-IP APM for IBM Tivoli Access Manager for e-business.

Creating the Rewrite profile

The first task is to configure a Rewrite profile. The Rewrite profile allows APM to act as a reverse proxy.

To create the Rewrite profile

1. On the Main tab, expand **Access Policy**, and then click **Rewrite Profiles**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Tivoli-Rewrite**.
4. Leave the **Client Caching Type** list at the default (**CSS and JavaScript**).
5. Click the **Finished** button.

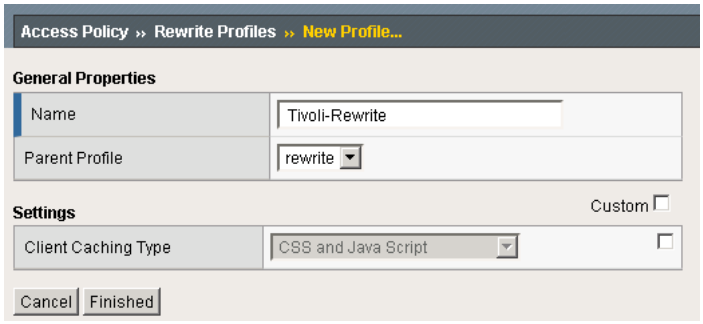

Figure 2.1 *Configuring the Rewrite Profiles*

Creating the SSO configuration

The next task is to create a Single Sign-On Configuration that defines the credentials that will be cached.

To create the SSO configuration

1. On the Main tab, expand **Access Policy**, and then click **SSO Configurations**.
2. Click the **Create** button.
3. In the **Name** box, type a name. In our example, we type **Tivoli-Access-SSO**.

4. From the **SSO Method** list, select the appropriate SSO method. In our example, we select **Form Based**.
5. In the **Username Source** box, type the user name source. In our example, we type **session.sso.token.last.username**.
6. In the **Password Source** box, type the user name source. In our example, we type **session.sso.token.last.password**.
7. In the Start URI box, type the URI. In our example, we type **http://tivoli-am1.tivoli.siterequest.com/**.
8. From the **Form Method** list, select **POST**.
9. In the **Form Action** box, type the destination URL to process the form. In our example, we type **http://tivoli-am1.tivoli.siterequest.com/?/pkmslogin.form**.
10. In the **Form Parameter for User Name** and **Password** boxes, type the elements the SSO form uses during the form submission.
11. In the **Hidden Form Parameters/Values** box, type any applicable parameters or values. We leave this blank.
12. From the **Successful Logon Detection Match Type** list, select **By Presence of Specific Cookie**.
13. In the **Successful Logon Detection Match Value** box, type a value. In our example, we are using a page on an IBM HTTP server that is authentication against Tivoli Access Manager and providing a cookie name **PDWPI-SESSION-COOKIE**.

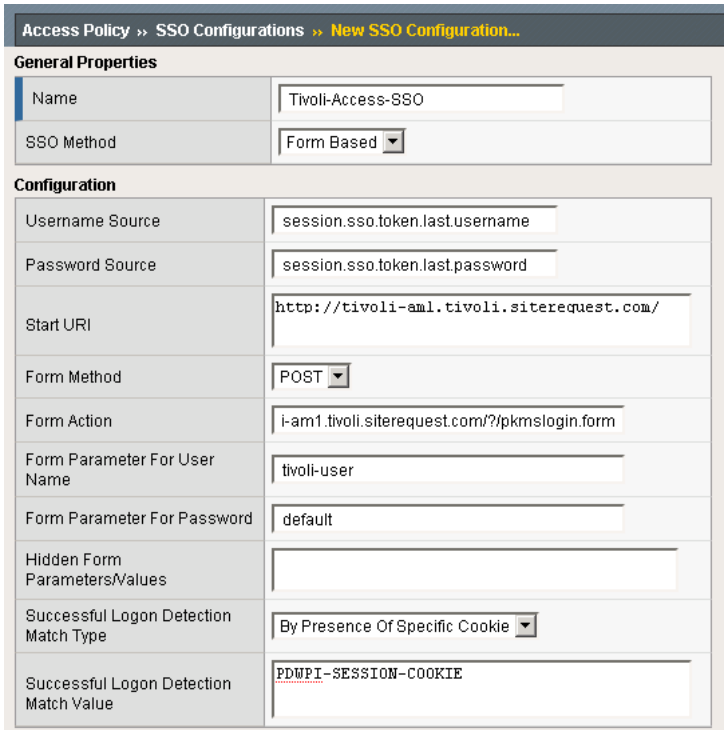

Figure 2.2 *The SSO Configuration*

14. Click **Finished**.

Creating the web application

The next task is to create the web application.

To create the Web Application

1. On the Main tab, expand **Access Policy**, and then click **Web Applications**.
2. Click the **Create** button.
3. In the **Name** box, type a name. In our example, we type **Tivoli-application**. You can optionally type a description.
4. Modify any of the settings as applicable for your configuration. In our example, we leave the settings at their default levels.
5. Click the **Create** button. The web application is saved, and the **Resource Items** section appears at the bottom of the page.
6. In the Resource Items section, click the **Add** button.
7. In the Destination section, click the appropriate option button, and type the applicable value in the box. In our example, we are providing access to a particular host. We click the **Host Name** button, and in the **Host Name** box, type **Tivoli-am1.tivoli.siterequest.com**.
8. In the **Port** box, type the appropriate port. In our example, **Tivoli-am1.tivoli.siterequest.com** is an HTTP application so we type **80**.
9. From the Scheme list, select the appropriate scheme. In our example, we select **HTTP**.
10. Configure the **Paths** and **Headers** section as applicable. We leave these sections blank.
11. From the **Resource Item Properties** list, select **Advanced**.
12. From the Compression list, select **GZIP Compression**. While this is optional, enabling this allows the BIG-IP APM browser component to further compress content when necessary, providing bandwidth and download time savings.
13. From the SSO configuration list, select the SSO object you configured in *Creating the SSO configuration*, on page 2. In our example, we select **Tivoli-Access-SSO**.
14. In the Home Tab row, you can optionally chose to enable the Home Tab. The Home Tab is a browser component that is inserted dynamically through the Access Virtual and allows users to browser pages within the context of BIG-IP APM. The Home Tab also allows users to log out. By clearing the Home Tab box, this feature is hidden.

The following is an example of what the Home Tab looks like for the end users. Note the Home and Logout buttons on the tab in the upper left of the screen.

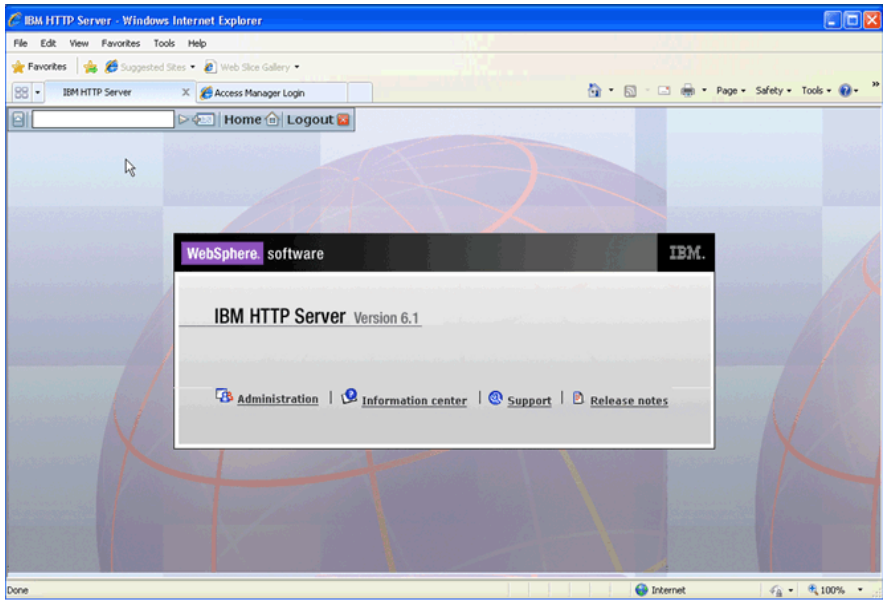

Figure 2.3 *The Home Tab from the end user perspective*

15. Configure the rest of the settings as applicable to your configuration.
16. Click **Finished**.

Creating a Webtop

The next task is to create a Web Top that specifies the end-user destination.

To create a Webtop

1. On the Main tab, expand **Access Policy**, and then click **Webtops**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this webtop. In our example, we type **Tivoli-Webtop**.
4. From the **Type** list, select **Web Applications**.
5. In the **Web Application start URI** box, type the start URI. This is the URI of the destination application that the user hits once they are authenticated and entitled to the resource. In our case we enter another VIP on our BIG-IP named **Tivoli-AM1.tivoli.siterequest.com**

Note: *Configuration of this virtual address can be either on the BIG-IP device running the Access Policy Module, or the virtual address can be on another BIG-IP Local Traffic Manager. For instructions on how to configure an application virtual server, see the product documentation or other F5 Deployment Guides.*

6. Click **Finished**.

Creating an Authentication source

The next task is to create an Authentication Source on the BIG-IP device that specifies a Tivoli Directory Server.

To create an AAA server

1. On the Main tab, expand **Access Policy**, and then click **AAA servers**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Tivoli_AM_aaa_srvr** because we traverse the wide-area-network back to Seattle to perform authentication.
4. From the **Type** list, select the appropriate authentication method. For this example, we select **HTTP**.
   In our example, we are using an HTTP Form Based authentication source. The BIG-IP proxies the authentication against this form. This form is a front-end page for the Tivoli Access Manager for E-Business in our case.
5. In the **Auth Type** row, click **Form Based**.
6. In the Start URI box, type the URI. In our example, we type **http://tivoli-am1.tivoli.siterequest.com/**.
7. From the **Form Method** list, select **POST**.
8. In the **Form Action** box, type the destination URL to process the form. In our example, we type **http://tivoli-am1.tivoli.siterequest.com/?/pkmslogin.form**
9. In the **Form Parameter for User Name** and **Password** boxes, type the appropriate user name and password.
10. In the **Hidden Form Parameters/Values** box, type any applicable parameters or values. We leave this blank.
11. In the Number of Redirects to Follow, type a number of redirects. In our example, we leave this at the default of **0**.
12. From the **Successful Logon Detection Match Type** list, select By **Presence of Specific Cookie**.

13. In the Successful Logon Detection Match Value box, type a value. In our example, we are using a page on an IBM HTTP server that is authentication against Tivoli Access Manager and providing a cookie name **PDWPI-SESSION-COOKIE**.
14. Click **Finished**.

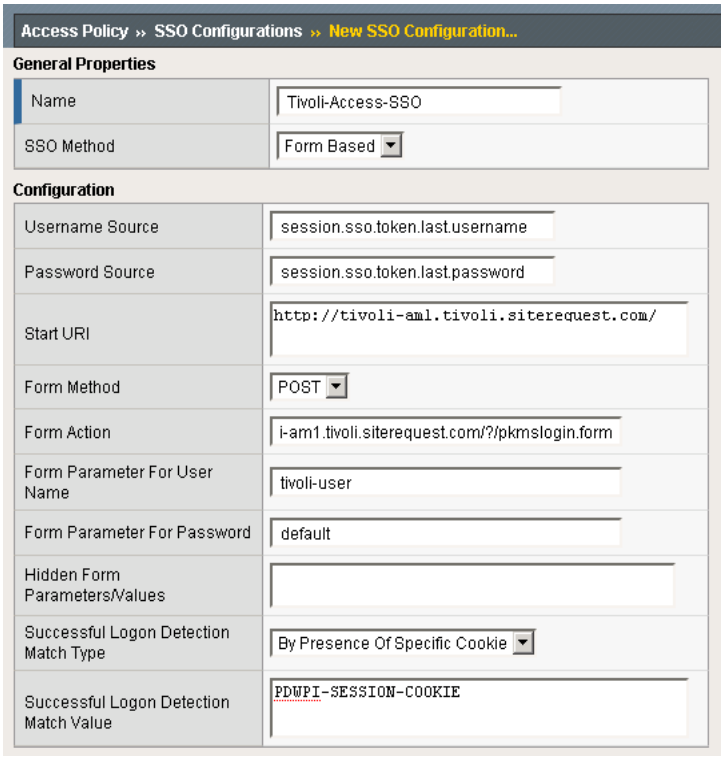

Figure 2.4 *The SSO configuration*

Creating an Access Profile

The next task is to create an Access Profile and a Visual Policy which provides an Antivirus check, a logon page, HTTP Authorization against the AAA source, SSO Credential mapping and a resource assignment.

To create an Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Tivoli_Access_Policy**.

4. In the Settings section, configure the options as applicable for your configuration. In our example, we leave all of the settings at their defaults. Note that depending on licensing, the number of concurrent users may be limited. The other timeouts are administrative choices.
5. In the Configuration section, from the SSO Configurations list, select the name of the SSO Configuration you created in *Creating the SSO configuration*, on page 2. In our example, we type **Tivoli-Access-SSO**.
6. Leave all other options at the default settings.
7. Click **Finished**.

Editing the Access Profile with the Visual Policy Editor

The next task is to edit the Access Policy using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy.

To edit the Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile you just created in the preceding procedure, and in the Access Policy column, click **Edit**.
The Visual Policy Editor opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Antivirus Check** option button, and then click the **Add Item** button at the bottom of the box.
5. Configure the Properties as applicable for your configuration, and then click the **Save** button. You now see two paths, **Successful** and **Fallback**.
6. Click the **+** symbol on the ***Successful*** path between **Antivirus Check** and **Deny**.
7. Click the **Logon Page** option button, and then click the **Add Item** button at the bottom of the box.
8. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults. Click the **Save** button.
9. Click the **+** symbol on the between **Logon Page** and **Deny**.
10. Click the **HTTP Auth** option button, and then click the **Add** button.
11. From the **AAA server** list, select the AAA server you created in *Creating an Authentication source*, on page 6. In our example, we select **Tivoli_AM_aaa_srvr**.

12. Click the **Save** button. You now see two paths, **Successful** and **Fall Back** from the HTTP Auth box.
13. Click the **+** symbol on the ***Successful*** path between **HTTP Auth** and **Deny**.
14. Click the **SSO Credential Mapping** option button, and then click the **Add Item** button.
15. Click the **Save** button.
16. Click the **+** symbol between **SSO Credential Mapping** and **Deny**.
17. Click the **Resource Assign** option button, and then click the **Add Item** button.
18. In the Resource Assign box, perform the following:
    a) Click the **Add new entry** button.
    a) Click the **Add/Delete Web Application Resources** link, and then check the box for the web application you created in *Creating the web application*, on page 2-4. In our example, we select **Tivoli-application**. Click **Update**.
    b) Click the **Set Webtop** link, and then check the box for the Webtop you created in *Creating a Webtop*, on page 2-5. In our example, we select **Tivoli-Webtop**. Click **Update**.
19. Click the **Save** button.
20. Click **Deny** to the left of Resource Assign.
21. Click **Allow** and then click the **Save** button.
22. Click the yellow **Apply Access Policy** link in the upper left part of the window. You always have to apply an access policy before it takes effect.
23. Click the **Close** button on the upper right to close the VPE.
The completed policy should look like the following:

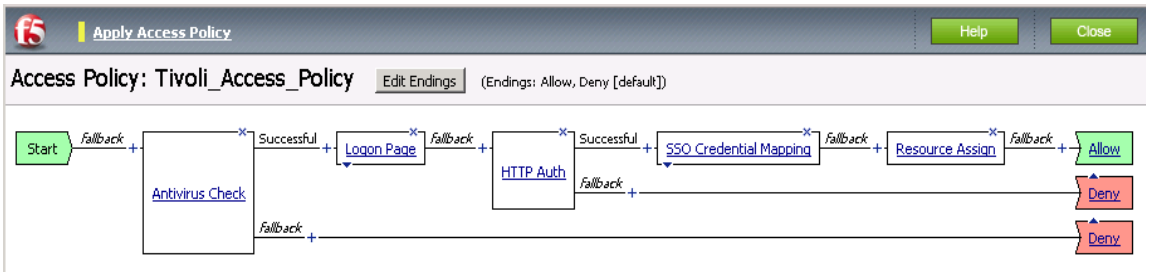

Figure 2.5 *Visual Policy Editor*

Creating the HTTP profile

The next profile to create is the HTTP profile. This profile is required. This should be a simple HTTP profile with no optimization (compression or caching).

To create the HTTP profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then click the **Create** button.
2. In the **Name** box, type a name for this profile. In our example, we type **Tivoli-http**.
3. Modify any of the settings as applicable for your network, but ***do not*** enable compression or RAM Cache. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
4. Click the **Finished** button.

Creating a Client SSL profile

The next step is to create an SSL profile. This profile contains SSL certificate and Key information for offloading SSL traffic. The first task is to import the certificate and key (for this Deployment Guide, we assume that you already have obtained the required SSL certificates, but they are not yet installed on the BIG-IP LTM system. If you do not have a certificate and key, see the BIG-IP documentation).

To import a key or certificate

1. On the Main tab, expand Local Traffic.
2. Click **SSL Certificates**. This displays the list of existing certificates
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**.
8. If you imported the certificate, repeat this procedure for the key.

The next task is to create the SSL profile that uses the certificate and key you just imported.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, select **Client**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Tivoli_https**.
4. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
5. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
6. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
7. Click the **Finished** button.

Creating the virtual servers

The next task is to create the virtual server listening on port 443 to which users connect. This is a virtual server for APM, and should not be confused with other application virtual servers.

We also configure a virtual server on port 80 that simply redirects users to the HTTPS virtual server.

To create the virtual server on port 443

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. 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 **tivoli_am_vs**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address for this Access Virtual on APM.
   Note: This is different than the application VIP. This is the front-end service that users connect to.
   In our example, we type **10.133.56.104**.
6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.
7. From the **HTTP Profile** list, select the name of the profile you created in the *Creating the HTTP profile* section. In our example, we select **Tivoli_http**.
8. From the **SSL Profile (Client)** list, select the SSL profile you created in the *Creating a Client SSL profile* section. In our example, we select **Tivoli_https**.

9. In the Access Policy section, from the **Access Profile** list, select the name of the policy you created in *Creating an Access Profile*, on page 2-7. In our example, we select **Tivoli_Access_Policy**.
10. From the **Rewrite Profile** list, select the profile you created in *Creating the Rewrite profile*, on page 2-2. In our example, we select **Tivoli_Rewrite**.
11. Leave all other settings at the default levels (**Do not** configure any of the options in the WAN Optimization section).
12. Click the **Finished** button (this virtual server does not have any Resources).

Now we create the redirect virtual server.

To create the redirect 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 **tivoli_am_redirect**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address for this Access Virtual on APM.
   Note: This is different than the application VIP. This is the front-end service that users connect to.
   In our example, we type **10.133.56.104**.
6. In the **Service Port** box, type **80**, or select **HTTP** from the list.
7. From the Resources section, in the iRules row, select the **_sys_https_redirect** iRule from the **Available** list, and click the Add (<<) button to move it to the **Enabled** box.
8. Click the **Finished** button.

This completes the BIG-IP APM configuration for Tivoli Access Manager for e-business.

3

Deploying the BIG-IP APM with Oracle Access Manager

Configuring the BIG-IP APM for Oracle Access Manager

This chapter describes how to configure the BIG-IP APM for Oracle® Access Manager.

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

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

In this section. we demonstrate an architecture where Oracle Access Manager provides authentication and authorization services to an application. Instead of authenticating users directly at the application layer, BIG-IP APM is used to proxy the authentication.

In this example, BIG-IP APM is used to check the client's computer for any viruses, authenticates the user to the same backend LDAP directory that Oracle Access Manager uses, and proxies those credentials to any Oracle Access Manager Webgates that request them.

◆ Note

This implementation requires minor changes to the Oracle configuration, so you must have administrative access to the OAM Access System Console

Product versions

Product Tested	Version Tested
BIG-IP APM	10.1
Oracle Identity Management	11gR1

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*.

Configuring the BIG-IP APM

Use the following procedures to configure the BIG-IP APM for Oracle Access Manager.

Creating the SSO configuration

The first task is to create a Single Sign-On Configuration that defines the credentials that are cached.

To create the SSO configuration

1. On the Main tab, expand **Access Policy**, and then click **Web Applications**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Oracle-Access-SSO**.
4. From the **SSO Method** list, select the appropriate SSO method. In our example, we select **Form Based**.
5. In the **Username Source** box, type the user name source. In our example, we type **session.sso.token.last.username**.
6. In the **Password Source** box, type the user name source. In our example, we type **session.sso.token.last.password**.
7. In the **Start URI** box, type the URI of the form on your SSO server. We are bypassing the actual login form, and instead using the destination URL that processes the form. In our example, we type **/access/sso**.
8. From the **Form Method** list, select **POST**.
9. In the **Form Action** box, type the destination URL to process the form. In our example, we type **/access/sso**.
10. In the **Form Parameter for User Name** and **Password** boxes, type the name of the elements the SSO form uses during the form submission. The defaults are **userid** and **password**.
11. In the **Hidden Form Parameters/Values** box, type any applicable parameters or values. We leave this blank.
12. From the **Successful Logon Detection Match Type** list, select **None**. We do not need this check because if the user fails authentication, OAM does not set the proper cookie and redirects the user back to the login form.
13. Click **Finished**.

Creating an Authentication source

The next task is to create an AAA server on the BIG-IP APM device.

To create an AAA server

1. On the Main tab, expand **Access Policy**, and then click **AAA servers**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Oracle-Access-AAA**.
4. From the **Type** list, select the appropriate authentication method. For this example, we select **LDAP**.
5. In the Configuration section, specify the details for connecting to the backend LDAP directory (hosted by Oracle Internet Directory in our installation) that your Oracle Access Manager installation uses. In our example, in the **Host** box, we type the host name for the OID server, in the **Admin DN** we type **cn=orcladmin**, in the **Password** box, we type the password, and leave the **Timeout** at the default.
6. Click **Finished**.

Creating an Access Profile

The next task is to create an Access Profile and a Visual Policy which provides an antivirus check, a logon page, LDAP authentication against the AAA source, and SSO Credential mapping.

To create an Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Oracle-Access-Policy**.
4. In the Settings section, configure the options as applicable for your configuration. In our example, we leave all of the settings at their defaults. Note that depending on licensing, the number of concurrent users may be limited. The other timeouts are administrative choices.
5. In the Configuration section, from the **SSO Configurations** list, select the name of the SSO Configuration you created in *Creating the SSO configuration*, on page 2. In our example, we type **Oracle-Access-SSO**.
6. We recommend checking the **Secure Cookie** box.

7. All other settings are optional, configure as applicable for your configuration. In our example, we leave all settings at the default.
8. Click **Finished**.

Editing the Access Profile with the Visual Policy Editor

The next task is to edit the Access Policy using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy.

To edit the Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile you just created, and in the Access Policy column, click **Edit**.
   The Visual Policy Editor opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Antivirus Check** option button, and then click the **Add Item** button at the bottom of the box.
5. Configure the Properties as applicable for your configuration.
6. Click the **Save** button. You now see two paths, **Successful** and **Fall Back**.
7. Click the **+** symbol on the ***Successful*** path between **Antivirus Check** and **Deny**.
8. Click the **Logon Page** option button, and then click the **Add Item** button at the bottom of the box.
9. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
10. Click the **+** symbol on the between **Logon Page** and **Deny**.
11. Click the **LDAP Auth** option button, and then click the **Add** button.
12. From the **Server** list, select the AAA server you created in *Creating an Authentication source*, on page 3. In our example, we select **Oracle-Access-AAA**.
13. In the **SearchDN** box, type the base DN in your directory from which all of the searches are started. In our example, we type **dc=siterequest, dc=com**.
14. In the **SearchFilter** box, type the LDAP filter you would like to do when performing searches. This should be the same filter that is used in the default form authentication scheme defined in the OAM Policy Manager (OraDefaultFormAuthNScheme). In our example, we type (on one line):

```
(&(&(objectclass=inetorgperson)(uid=%{session.logon.last.username}))(|(!(obuseraccountcont
    rol=*))(obuseraccountcontrol=ACTIVATED)))
```

15. Leave the **UserDN** box blank.
16. From the **Show Extended Error** list, select **Enabled**.
17. From the **Max Logon Attempts Allowed** list, select **3**.
18. Click the **Save** button. You now see two paths, **Successful** and **Fall Back** from the LDAP Auth box.

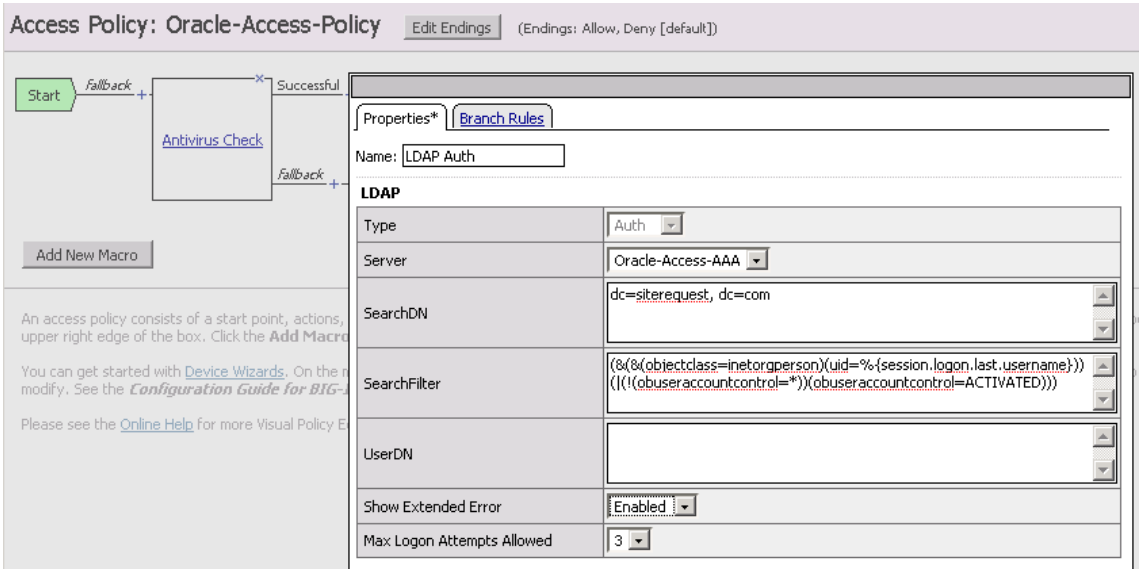

Figure 3.1 *The LSAP Auth section of the VPE*

19. Click the **+** symbol on the ***Successful*** path between **LDAP Auth** and **Deny**.
20. Click the **SSO Credential Mapping** option button, and then click the **Add Item** button at the bottom of the box.
21. Configure the Properties as applicable for your configuration. In our example, we leave the defaults. Click the **Save** button.
22. On the path **SSO Credential Mapping** path, click the **Deny** link box. Click the **Allow** button, and then click **Save**.
23. Click the yellow **Apply Access Policy** link in the upper left part of the window. You must apply an access policy before it takes effect.
24. Click the **Close** button on the upper right to close the VPE.

Creating the health monitor

The next step is to set up a health monitor for the Oracle devices. This procedure is optional, but very strongly recommended. In our example, we create an HTTP health monitor.

To configure a HTTP 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 **Oracle-SSO-monitor-http**.
4. From the **Type** list, select **HTTP**.
5. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout. In our example, we use a **Interval** of **5** and a **Timeout** of **16.**
6. In the **Send String** box, type the following string:

   ```
   GET /\n\n
   ```

7. The rest of the settings are optional, configure as appropriate for your implementation.
8. Click the **Finished** button.

Creating the pool

You must create a pool on the BIG-IP APM system for the Oracle devices. In our example, the pool you define only contains one device, the Oracle Access Manager SSO server. This is the device that hosts the normal OAM login form.

To create the Oracle 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. In the **Name** box, enter a name for your pool. In our example, we use **Oracle-SSO-pool**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the health monitor* section, and click the Add (**<<**) button. In our example, we select **Oracle-SSO-monitor-http**.
5. From the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network). In our example, we select **Least Connections (node)**.
6. For this pool, we leave the Priority Group Activation **Disabled**.

7. In the New Members section, make sure the **New Address** option button is selected.
8. In the **Address** box, add the IP address of your Oracle Access Manager SSO server. In our example, we type **10.133.100.171**.
9. In the **Service Port** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list. In our example, we type **443**, because our Oracle Access Manager SSO server is configured to run over HTTPS.
10. Click the **Add** button to add the member to the list.
11. Click the **Finished** button.

Creating the HTTP profile

The next profile to create is the HTTP profile. This profile is required. This should be a simple HTTP profile with no optimization (compression or caching).

To create the HTTP profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then click the **Create** button.
2. In the **Name** box, type a name for this profile. In our example, we type **Oracle-SSO-http**.
3. Modify any of the settings as applicable for your network, but ***do not*** enable compression or RAM Cache. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
4. Click the **Finished** button.

Creating the SSL profiles

The next step is to create the client and server SSL profiles. These profiles contain SSL certificate and Key information for offloading SSL traffic. The first task is to import the certificate and key (for this Deployment Guide, we assume that you already have obtained the required SSL certificates, but they are not yet installed on the BIG-IP LTM system. If you do not have a certificate and key, see the BIG-IP documentation).

To import a key or certificate

1. On the Main tab, expand Local Traffic.
2. Click **SSL Certificates**. This displays the list of existing certificates
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**.
8. If you imported the certificate, repeat this procedure for the key.

The next task is to create the SSL profiles that uses the certificate and key you just imported.

Creating the Client SSL profile

Use the following procedure to create the Client SSL profile.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, select **Client**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Oracle-SSO-client-ssl**.
4. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
5. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
6. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
7. Click the **Finished** button.

Creating the Server SSL profile

Use the following procedure to create the Server SSL profile.

To create a new Server SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, select **Server**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Oracle-SSO-server-ssl**.
4. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
5. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.

6. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
7. Click the **Finished** button.

Creating the virtual server

The next task is to create the virtual server listening on port 443 to which users connect. This is a virtual server for APM, and should not be confused with other application virtual servers.

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_SSO-apm-vs**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address for this Access Virtual on APM. Note: This is different than the application VIP. This is the front-end service that users connect to. In our example, we type **10.133.15.111**.
6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.
7. From the **HTTP Profile** list, select the name of the profile you created in the *Creating the HTTP profile* section. In our example, we select **Oracle-SSO-http**.
8. From the **SSL Profile (Client)** list, select the SSL profile you created in the *Creating the Client SSL profile* section. In our example, we select **Oracle-SSO-client-ssl**.
9. From the **SSL Profile (Server)** list, select the SSL profile you created in the *Creating the Server SSL profile* section. In our example, we select **Oracle-SSO-server-ssl**.
10. In the Access Policy section, from the **Access Profile** list, select the name of the policy you created in *Creating an Access Profile*, on page 3. In our example, we select **Oracle-Access-Policy**.
11. In the Resources section, from the Default Pool list, select the pool you created in *Creating the pool*, on page 3-6. In our example, we select **Oracle-SSO-pool**.
12. Click the **Finished** button.

This completes the BIG-IP APM configuration for Oracle Access Manager. Be sure to continue to the following section to make changes to the Oracle configuration.

Modifying the Oracle configuration

In this section of the deployment guide, we modify the Oracle Access Manager configuration. There are three changes required in your Oracle Access Manager configuration:

- *Defining a new authentication scheme*, following
- *Modifying the application to use the new Authentication Scheme*, on page 3-13
- *Modifying the Access Gate with a new Preferred HTTP Host*, on page 3-14

Defining a new authentication scheme

The first task is to create a new authentication scheme in Oracle Access Manager.

To define a new authentication scheme

1. Open the OAM Access System Console using a web browser.
2. Click the Access System Configuration tab.
3. In the Navigation pane, click **Authentication Management**.
4. At the bottom of the list of authentication schemes, click the **Add** button.
5. In this step, we configure the options on the General tab. This should essentially be an exact copy of the General tab from OraDefaultFormAuthNScheme with the exception of the 'form' challenge parameter.
   a) In the **Name** box, type a name. In our example, we type **F5 APM Proxied Auth**.
   b) In the **Description** box, type a description. In our example, we type **Proxied authentication via F5 APM to OraDefaultFormAuthNScheme**.
   c) In the **Level** box, type **1**.
   d) In the **Challenge Method** row, click the **Form** button.
   e) In the **Challenge Parameter** boxes, type the following (you may need to click the Add (+) button to add more rows):
      - **form:/access/sso**
      - **creds:userid password**
      - **action:/access/sso**
      - **passthrough:no**
6. In the **SSL Required** row, click **No**.

7. In **Challenge Redirect** box, type the FQDN of the virtual server you created in *Creating the virtual server*, on page 9. In our example, we type **https://sso-apm-11g.siterequest.com**.
8. Click the **Save** button.

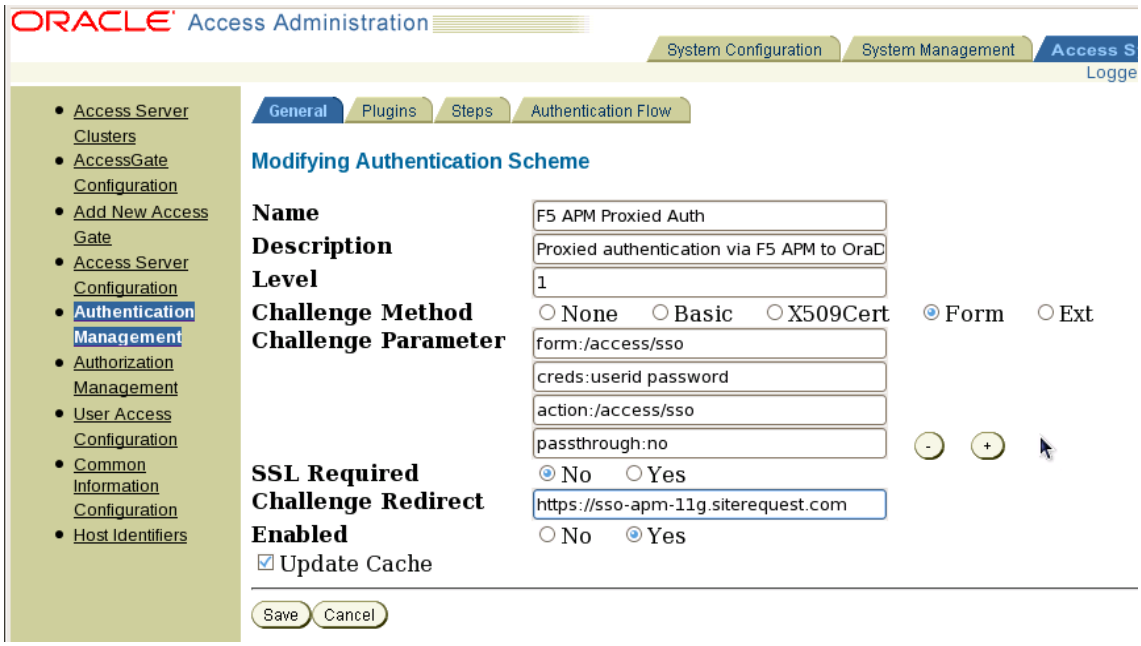

Figure 3.2 *Modifying the Authentication Scheme*

9. Click the Plugins tab, and then configure the following options. This should essentially be an exact copy of the Plugins tab from OraDefaultFormAuthNScheme.
   a) Click the **Modify** button.
   b) Click the **Add** button.
   c) From the list, select **validate_password**.
   d) In the **Plugin Parameters** box, type **ObCredentialPassword="password"**.
   e) Click the **Add** button
   f) From the list, select **credential_mapping**.
   g) In the **Plugin Parameters** box, type the following, all on one line. Note: this should be similar to the string you defined as the Search Filter in Step 14 of *Editing the Access Profile with the Visual Policy Editor*, on page 3-4.

```
obMappingBase="dc=siterequest,dc=com",
    obMappingFilter="(&(&(objectclass=inetOrgPerson)(uid=%userid
    %))(|(!(obuseraccountcontrol=*))(obuseraccountcontrol=ACTIVATED)))"
```

h) Click the **Save** button.

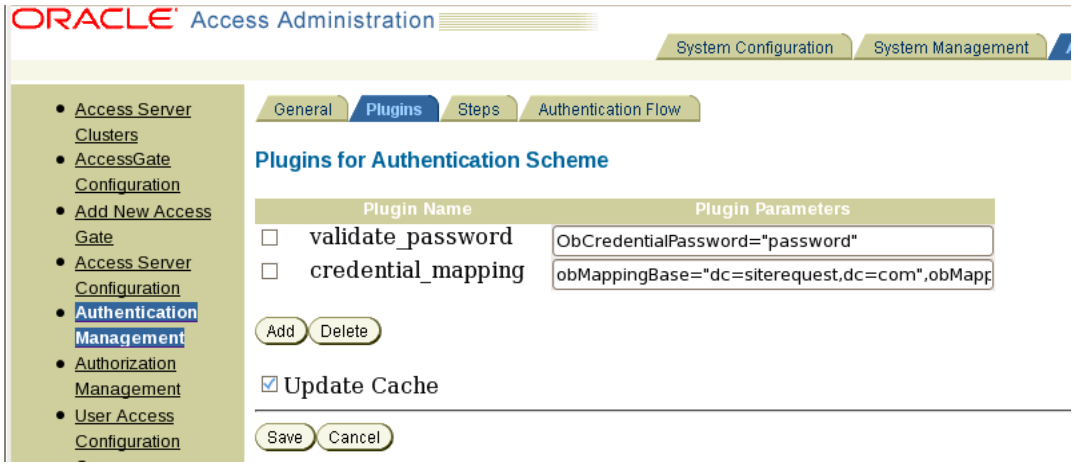

Figure 3.3 *Plugin configuration*

10. Click the General tab.
11. Click the **Modify** button.
12. In the **Enabled** row, click **Yes**.
13. Make sure the **Update Cache** box is checked.
14. Click the **Save** button.

Modifying the application to use the new Authentication Scheme

The next task is to modify your application to use the new authentication scheme.

To modify the application to use the authentication scheme

1. Open the OAM Policy Manager using a web browser.
2. From the navigation pane, click **My Policy Domains**.
3. Click the name of the Policy Domain that will use the new Authentication Scheme.
4. Click the **Default Rules** tab, click **Authentication Rule**, and then click **General**.
5. Click the **Modify** button.
6. From the **Authentication Scheme** list, select the name of the scheme you created in *Defining a new authentication scheme*, on page 11. In our example, we select **F5 APM Proxied Auth**.
7. Make sure the **Update Cache** box is checked.
8. Click the **Save** button.

Modifying the Access Gate with a new Preferred HTTP Host

The final task in this section is to modify your Access Gate with a new preferred HTTP host.

To modify the Access Gate with a new HTTP host

1. Open the OAM Access System Console using a web browser.
2. Click the Access System Configuration tab
3. From the navigation pane, click **AccessGate Configuration**.
4. Using the search form, find the Access Gate configuration that your application uses.
5. In the results list, click the name of your Access Gate configuration.
6. Click the **Modify** button at the bottom of the page.
7. In the **Preferred HTTP Host** box, type the FQDN of the virtual server you created in *Creating the virtual server*, on page 9. In our example, we type **sso-apm-11g.siterequest.com**. This should also be the FQDN you specified in the Challenge Redirect property for your new authentication scheme.
8. Click the **Save** button.

Figure 3.4 *Configuring the Preferred HTTP Host*

You may need to restart their OHS instances that are deploying Webgate in order to reflect these changes.

This completes the Oracle Access Manager configuration for BIG-IP APM.

4

Deploying APM with Microsoft Active Directory for Exchange or SharePoint Access

- Configuring the BIG-IP APM for Exchange Server 2010 Access
- Configuring the BIG-IP APM for SharePoint access

Configuring the BIG-IP APM for Exchange Server 2010 Access

This chapter is broken into two sections, the first for Microsoft® Exchange Server 2010, the second for Microsoft Office SharePoint® (*Configuring the BIG-IP APM for SharePoint access*, on page 4-14).

In this section, we demonstrate using BIG-IP APM for pre-authentication of users in Active Directory before allowing connectivity to an Exchange Server 2010 Outlook Web App pool. If you want to enhance this configuration with additional pre-login checks, such as verification of up-to-date anti-virus software on the client, follow the relevant steps in the Oracle Access Manager section of this document.

Prerequisites and configuration notes

The following are prerequisites and notes about this configuration.

- BIG-IP must have DNS and NTP configured.
- The DNS server(s) that are configured in BIG-IP must be able to resolve all forward and reverse zones associated with the Active Directory domain used by Outlook Web App. Additionally, the BIG-IP must be able to resolve the Host Name used in the Web Application configuration section (see below).
- Active Directory and BIG-IP should ideally share a common time source, but in any case must have times that are closely synchronized. See the BIG-IP documentation on how to configure DNS and NTP.
- End users must be able to resolve the name associated with the IP address for the virtual server that you create in the final step of this process. That name is distinct from the FQDN configured within Outlook Web App as an External URL, which the BIG-IP makes use in the Web Application configuration.

Product versions

Product Tested	Version Tested
BIG-IP APM	10.1
Microsoft Exchange Server	2010*
Microsoft Windows Server‘	2008 R2
Microsoft Office SharePoint	2007

**While Microsoft Exchange Server 2007 was not tested for this guide, but should work with substantially similar configuration.*

Configuring the BIG-IP APM for Exchange Server

The configuration procedures provided in this document result in authenticated access to a resource, which in this case is a BIG-IP virtual server that load-balances a pool of Exchange Server 2010 Client Access Servers running Outlook Web App (OWA). Alternately, you can elect to use a single Outlook Web App as your Resource, in which case you only need to configure the APM virtual server (the final step of this procedure) and do not need to configure a second virtual server for the OWA pool.

Modifying the deployment guide configuration

Configuring the BIG-IP LTM for Microsoft Exchange Server 2010 Outlook Web App is well documented in the deployment guide (***http://www.f5.com/pdf/deployment-guides/f5-exchange-2010-dg.pdf***).

When adding BIG-IP APM to the deployment guide configuration, you need to make the following changes to the BIG-IP LTM virtual server configuration:

- The virtual server you create for Outlook Web App should listen on port 80 (HTTP) rather than 443 (HTTPS).
- Use the **tcp-lan-optimized** TCP profile rather than any of the WAN-optimized options. The BIG-IP APM handles the WAN portion of the connection.
- The HTTP profile should use the basic **http** parent, and not any of the optimized http profiles.
- Do not use a Client SSL profile.
- Do not use WebAccelerator.
- The External URL that you configure for Outlook Web App and the Exchange Control Panel on your Client Access servers must begin with **http**, not **https**.
- The External URL must use a FQDN that the BIG-IP APM device can resolve in DNS (see *Prerequisites and configuration notes*, on page 4-1).

Creating the Rewrite profile

The first task in configuring the APM module is to create a rewrite profile. The Rewrite Profile allows APM to act as a reverse proxy.

To create the Rewrite profile

1. On the Main tab, expand **Access Policy**, and then click **Rewrite Profiles**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Exchange-OWA-Rewrite**.

4. Leave the **Client Caching Type** list at the default (**CSS and JavaScript**).
5. Click the **Finished** button.

Creating the SSO Configuration

The next task is to configure the SSO configuration. A Single Sign-On Configuration that defines the credentials that will be cached.

Note

Outlook Web App defaults to using forms-based authentication. The following instructions permit APM to do credential-caching and proxy login using that default setting. If you have changed your Outlook Web App servers to accept NTLM authentication rather than forms-based, you should use the SSO Configuration method detailed in the SharePoint section of this document.

To create the SSO configuration

1. On the Main tab, expand **Access Policy**, and then click **SSO Configurations**.
2. Click the **Create** button.
3. In the Name box, type a name for this profile. In our example, we type **Exchange-OWA-Access-SSO**.
4. From the **SSO Method** list, select the appropriate SSO method. In our example, we select **Form Based**.
5. In the **Username Source** box, type the user name source. In our example, we leave the default value **session.sso.token.last.username**.
6. In the **Password Source** box, type the user name source. In our example, we leave the default value **session.sso.token.last.password**.
7. In the **Start URI** box, type the URI. For default Exchange 2010 OWA configurations, this takes the form:

```
/owa/auth/logon.aspx?url=https://<hostname>/owa/&reason=0
```

Where **<hostname>** is the fully-qualified name associated with the BIG-IP virtual server for OWA (or standalone OWA server) and that you have configured in the External URL setting of your OWA servers.

In our example, we type

```
/owa/auth/logon.aspx?url=https://owa.siterequest.com/owa/&reason=0
```

Important Note: *Do not include the protocol (http://) or FQDN at the beginning of the string you type in this field, only after the "url=" portion.*

8. From the **Form Method** list, select **POST**.
9. In the **Form Action** box, type the destination URL to process the form. In our example, we type **/owa/auth.owa**. If you have changed the default virtual directory path associated with the OWA service on your servers, you need to alter the first field to match that of your virtual directory.
   Important note: *As with the Start URI field, do not include a protocol or hostname.*
10. In the **Form Parameter for User Name** and **Password** boxes, we type **username** and **password**, respectively.
11. In the **Hidden Form Parameters/Values** box, type any applicable parameters and value pairs, separating each element in a pair by a space and with one pair per line. These correspond to requested values on the original OWA login form, including whether the user is at a public (shared) or private computer and whether or not to use a light version of Outlook Web App, as well as some otherwise-hidden values. In our example, we supply the following parameters and values:

    destination http://owa.siterequest.com/owa/

    flags 4

    forcedownlevel 0

    isUtf8 1

    trusted 4

    The **destination** parameter should be adjusted to match the URI of your OWA server pool.
12. From the **Successful Logon Detection Match Type** list, select **By Presence of Specific Cookie**.
13. In the **Successful Logon Detection Match Value** box, type **sessionid** (see Figure 4.1).
14. Click **Finished**.

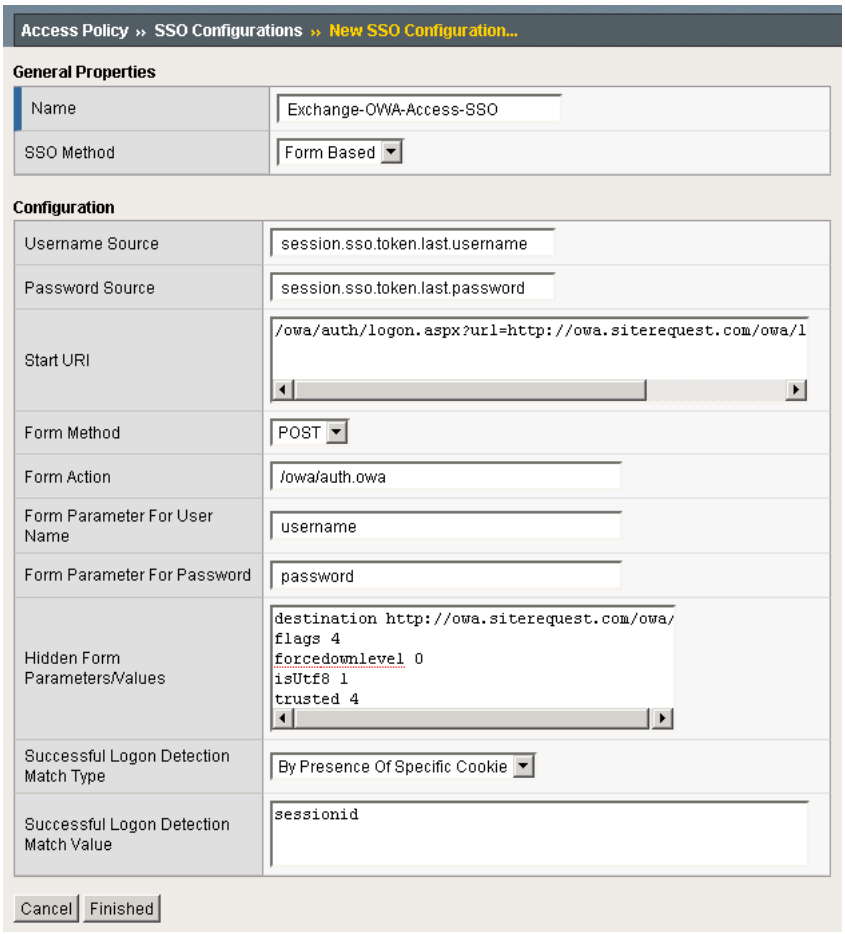

Figure 4.1 *SSO configuration for OWA*

Creating the web application

The next task is to create the Web Application.

To create the Web Application

1. On the Main tab, expand **Access Policy**, and then click **Web Applications**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this web application. In our example, we type **Exchange-OWA-application**. You can optionally type a description.
4. Modify any of the settings as applicable for your configuration. In our example, we leave the settings at their default levels.
5. Click the **Create** button. The web application is saved, and the Resource Items section appears at the bottom of the page.

6. In the Resource Items section, click the **Add** button.
7. In the Destination section, click the appropriate option button, and type the applicable value in the box. In our example, we are providing access to a BIG-IP LTM virtual server that load-balances a pool of OWA servers (see the configuration notes under the Prerequisites heading at the beginning of the OWA section of this document for more details). In our example, we click the **Host Name** button, and in the **Host Name** box, we type the FQDN of our OWA virtual server, **owa.siterequest.com**. (
Reminder: the BIG-IP must be able to resolve this host name to the correct IP address, whether that be an individual server or a BIG-IP virtual).
8. In the **Port** box, type the appropriate port. In our example, OWA is an HTTP application and we are doing all TLS/SSL processing on the BIG-IP, so we type **80**, the standard HTTP port.
9. From the **Scheme** list, select the appropriate scheme. In our example, we select **http**.
10. Configure the Paths and Headers section as applicable. In our example, we type **/owa/*** in the Paths field; this will be correct for most OWA servers unless you have modified your default settings.
11. From the **Resource Item Properties** list, select **Advanced**.
12. From the **Compression** list, select **GZIP Compression**. While this is optional, enabling this allows the BIG-IP APM browser component to further compress content when necessary, providing bandwidth and download time savings.
13. From the **SSO configuration** list, select the SSO object you configured in Creating the SSO configuration. In our example, we select **Exchange-OWA-Access-SSO**.
14. In the Home Tab row, you can optionally chose to enable the **Home Tab**. The Home Tab is a browser component that is inserted dynamically through the Access Virtual and allows users to browser pages within the context of BIG-IP APM. The Home Tab also allows users to log out. By clearing the Home Tab box, this feature is hidden. To see an example of the Home Tab, see Figure 2.3, on page 2-5.
15. Configure the rest of the settings as applicable to your configuration.
16. Click **Finished**.

Creating a Webtop

The next task is to create a Web Top that specifies the end-user destination.

To create a Webtop

1. 1. On the Main tab, expand **Access Policy**, and then click **Webtops**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this webtop. In our example, we type **Exchange-OWA-Webtop**.
4. From the **Type** list, select **Web Applications**.
5. In the **Web Application start URI** box, type the start URI. This is the URI of the destination application that the user hits once they are authenticated and entitled to the resource. In our case we enter the URI that our OWA Server has been configured to use, **http://owa.siterequest.com/owa/logon.aspx**. You must substitute in the correct FQDN for your OWA pool, but otherwise this URI will be correct for most default configurations of OWA.
6. Click **Finished**.

Creating an Authentication Source

The next task is to create an Authentication Source that specifies an Active Directory Server.

To create an AAA server

1. On the Main tab, expand **Access Policy**, and then click **AAA servers**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Exchange-OWA-AAA-AD**.
4. From the **Type** list, select the appropriate authentication method. For this example, we select **Active Directory**.
5. In the **Domain Controller** row, type the IP address or DNS name of the Active Directory server you'll be using. The BIG-IP must have network connectivity to this server.
6. In the **Domain Name** box, type the fully-qualified domain name (FQDN) of your domain. (Note: you must use the FQDN rather than the short NetBIOS domain name). In our example, we type **mydomain.siterequest.com**.
7. You do not need to supply an Admin Name or Admin Password.
8. Click **Finished**.

Creating an Access Profile

The next task is to create an Access Profile and a Visual Policy which provides a logon page, authentication against the Active Directory AAA source, SSO Credential mapping and a resource assignment. If you would optionally like to include a pre-login anti-virus check, follow the example shown in the Tivoli section of this document.

To create an Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Exchange_OWA_Access_Policy**.
4. In the Settings section, configure the options as applicable for your configuration. In our example, we leave all of the settings at their defaults. Note that depending on licensing, the number of concurrent users may be limited. The other timeouts are administrative choices.
5. In the Configuration section, from the **SSO Configurations** list, select the name of the SSO Configuration you created in *Creating the SSO Configuration*, on page 4-3. In our example, we type **Exchange-OWA-Access-SSO**.
6. In our example, and for most Exchange 2010 OWA deployments, leave all other settings at their default values. Consult the BIG-IP documentation if you need details on configuring Language Settings.
7. Click **Finished**.

Editing the Access Profile with the Visual Policy Editor

The next task is to edit the Access Policy using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy.

To edit the Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile you just created, and in the **Access Policy** column, click **Edit**. The Visual Policy Editor opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.

4. Select the **Logon Page** option button, and then click the **Add Item** button at the bottom of the box.
5. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
6. Click the **Save** button.
7. Click the **+** symbol on the between **Logon Page** and **Deny**.
8. Select the **AD Auth** option in the Authentication section, then click **Add Item**.
9. In the **Server** box, select the AAA source you created in *Creating an Authentication Source*, on page 4-7. In our example, we select **Exchange-OWA-AAA-AD**. The other settings are optional.
10. Click the **Save** button. You now see two paths, Successful and Fall Back.
11. At the end of the ***Successful*** path, click **Deny** in the ending box.
12. Select the **Allow** option, and click **Save**. The ending for Successful should now be Allow, and the ending for fallback should be Deny.
13. Click the **+** symbol on the ***Successful*** path between **AD Auth** and **Allow**.
14. Select the **SSO Credential Mapping** item from the General Purpose section, then click **Add Item**. In our configuration example, we leave the settings for **SSO Token Username and SSO Token Password** at their default settings. Click **Save**.
15. Click the **+** symbol between **SSO Credential Mapping** and **Allow**.
16. Select the **Resource Assign** item from the **General Purpose** section, then click **Add Item**.
17. Click **Add New Entry**, then **Add/Delete Web Application Resources**.
18. Select the web application you created in *Creating the web application*, on page 4-5. In our example, we select **Exchange-OWA-application**. The counter on the Web Application Resource tab changes from **0** to **1**.
19. Click the **Webtop** tab. Select the Webtop you created above. In our example, we select **Exchange-OWA-Webtop**. The counter on the Webtop tab changes from **0** to **1**.
20. Click **Update**, and then click **Save**. See Figure 4.2 for an example of what the completed policy looks like.
21. Click the yellow **Apply Access Policy** link in the upper left part of the window. You always have to apply an access policy before it takes effect.

22. Click the **Close** button on the upper right to close the VPE. The items added are a logon page, an AD Auth that will provide to the AAA source created earlier, an SSO Credential Mapping and a Resource Assign.

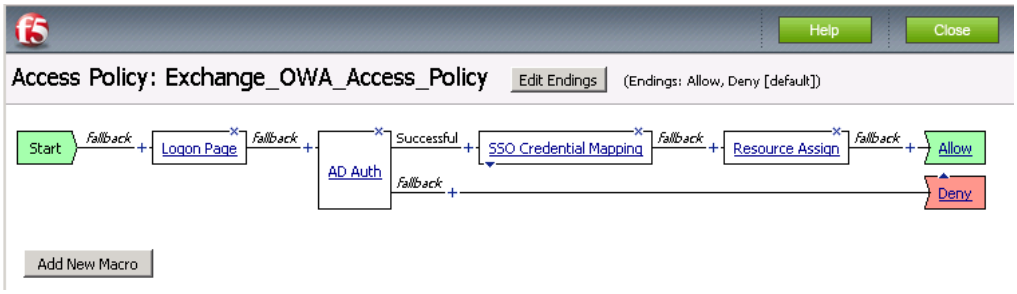

Figure 4.2 *Completed Policy for OWA*

Creating the HTTP profile

The next profile to create is the HTTP profile. This profile is required. This should be a simple HTTP profile with no optimization (compression or caching).

To create the HTTP profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then click the **Create** button.
2. In the **Name** box, type a name for this profile. In our example, we type **Exchange-OWA-http**.
3. Modify any of the settings as applicable for your network, but ***do not*** enable compression or RAM Cache. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
4. Click the **Finished** button.

Creating a Client SSL profile

The next step is to create an SSL profile. This profile contains SSL certificate and Key information for offloading SSL traffic. The first task is to import the certificate and key (for this Deployment Guide, we assume that you already have obtained the required SSL certificates, but they are not yet installed on the BIG-IP LTM system. If you do not have a certificate and key, see the BIG-IP documentation).

To import a key or certificate

1. On the Main tab, expand Local Traffic, and then click **SSL Certificates**. This displays the list of existing certificates

2. In the upper right corner of the screen, click **Import**.
3. From the **Import Type** list, select the type of import (**Certificate** or **Key**).
4. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
5. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
6. Click **Import**.
7. If you imported the certificate, repeat this procedure for the key.

The next task is to create the SSL profile that uses the certificate and key you just imported.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, select **Client**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Exchange-OWA_https**.
4. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
5. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
6. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
7. Click the **Finished** button.

Creating the iRule

In order for APM to successfully login through OWA's forms-based authentication page, we need to create an iRule to pass a required cookie during the login.

If you have reconfigured OWA to use NTLM authentication, and configured BIG-IP APM to also use NTLM in the SSO configuration, skip this step.

To create the iRule

1. On the Main tab, expand **Local Traffic**, click **iRules**, and then click the **Create** button.
2. In the **Name** box, type a name for the iRule. In our example, we type **Exchange_OWA_cookie_add**.

3. In the **Definition** box, type the following (the line numbers on the left are for reference only and should not be included in the Definition box.

```
1   when HTTP_RESPONSE {
2      if { [HTTP::is_redirect] } {
3         set location [HTTP::header location]
4         if { $location contains "owa/auth/logon.aspx" } {
5            HTTP::header insert "Set-Cookie" "PBack=0;"
6         }
7      }
8   }
```

   If you have altered your default virtual directory for OWA, adjust the path as appropriate on line 4.

4. Click the **Finished** button.

Creating the virtual server

The final task is to create the virtual server.

To create the virtual server

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. 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 **Exchange-OWA_vs**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address for this Access Virtual on APM.
   Note: This is different than the application VIP. This is the front-end service that users connect to.
   In our example, we type **10.133.56.114**.
6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.
7. From the **HTTP Profile** list, select the name of the profile you created in the *Creating the HTTP profile* section. In our example, we select **Exchange-OWA-http**.
8. From the **SSL Profile (Client)** list, select the SSL profile you created in the *Creating a Client SSL profile* section. In our example, we select **Exchange-OWA-https**.
9. In the Access Policy section, from the **Access Profile** list, select the name of the policy you created in *Creating an Access Profile*, on page 4-8. In our example, we select **Exchange_OWA_Access_Policy**.

10. From the **Rewrite Profile** list, select the profile you created in *Creating the Rewrite profile*, on page 2. In our example, we select **Exchange-OWA-Rewrite**.
11. In the Resources section, from the iRules **Available** list, select the iRule you created in *Creating the iRule*, on page 4-11, and click the Add (<<) button.
12. Leave all other settings at the default levels (**Do not** configure any of the options in the WAN Optimization section).
13. Click the **Finished** button.

This completes the APM configuration for Microsoft Exchange OWA. The next section contains SharePoint configuration information.

Configuring the BIG-IP APM for SharePoint access

In this section we demonstrate using BIG-IP APM for pre-authentication of users in Active Directory before allowing connectivity to a Microsoft Office SharePoint server pool. If you wish to enhance this configuration with additional pre-login checks, such as verification of up-to-date anti-virus software on the client, follow the relevant steps in the Oracle Access Manager section of this document: see *Editing the Access Profile with the Visual Policy Editor*, on page 3-4.

Prerequisites and configuration notes

- BIG-IP must have DNS and NTP configured.
- The DNS server(s) that are configured in BIG-IP must be able to resolve all forward and reverse zones associated with the Active Directory domain used by SharePoint. Additionally, the BIG-IP must be able to resolve the Host Name used in the Web Application configuration section (see below).
- End users must be able to resolve the name associated with the IP address for the virtual server that you create in the final step of this process. That name is distinct from the FQDN that you have configured your SharePoint application to use and which the BIG-IP makes use in the Web Application configuration.
- Active Directory and BIG-IP should ideally share a common time source, but in any case must have times that are closely synchronized.

  See the BIG-IP product documentation on how to configure DNS and NTP.
- The login form created below only works if users supply their user name without accompanying domain information, for example, just **username** rather than **domain\username** or **username@fully.qualified.domain.name**.

Creating the Rewrite Profile

The first task is to create the rewrite profile.

To create the Rewrite profile

1. On the Main tab, expand **Access Policy**, and then click **Rewrite Profiles**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **SharePoint-Rewrite**.

4. Leave the **Client Caching Type** list at the default (**CSS and JavaScript**).
5. Click the **Finished** button.

SSO Configuration

Next, we create a Single Sign-On Configuration that defines the credentials that will be cached.

To create the SSO configuration

1. On the Main tab, expand **Access Policy**, and then click **SSO Configurations**.
2. Click the **Create** button.
3. In the Name box, type a name for this profile. In our example, we type **SharePoint-Access-SSO**.
4. From the **SSO Method** list, select the appropriate SSO method. In our example, we select **NTLMv1**.

   Note: Unless you altered the default configuration of the Windows Server 2008 servers that run your SharePoint server pool to only accept NTLMv2 authentication, you should select NTLMv1.
5. In the **Username Source** box, type the user name source. In our example, we leave the default setting **session.sso.token.last.username**, which will be correct for most configurations.
6. In the **Password Source** box, type the user name source. In our example, we leave the default setting **session.sso.token.last.password**, which will also be correct for most configurations.
7. In the **NTLM domain** box, type the NetBIOS version of your domain name. In our example, we type **mydomain**. Do ***not*** use the fully qualified domain name (e.g. 'mydomain.example.com').
8. Click **Finished**.

Creating the web application

The next task is to create the Web Application.

To create the Web Application

1. On the Main tab, expand **Access Policy**, and then click **Web Applications**.
2. Click the **Create** button.

3. In the **Name** box, type a name for this web application. In our example, we type **SharePoint-application**. You can optionally type a description.
4. Modify any of the settings as applicable for your configuration. In our example, we leave the settings at their default levels.
5. Click the **Create** button. The web application is saved, and the Resource Items section appears at the bottom of the page.
6. In the **Resource Items** section, click the **Add** button.
7. In the Destination section, click the appropriate option button, and type the applicable value in the box. In our example, we are providing access to a particular host, although the destination could also be a BIG-IP LTM virtual server that load balances a pool of SharePoint servers. We click the **Host Name** button, and in the **Host Name** box, type **sharepoint.mydomain.siterequest.com**. (Note: the BIG-IP must be able to resolve this host name to the correct IP address, whether that be an individual server or a BIG-IP virtual).
8. In the **Port** box, type the appropriate port. In our example, SharePoint is an HTTP application and we are doing all TLS/SSL processing on the BIG-IP, so we type **80**, the standard HTTP port.
9. From the **Scheme** list, select the appropriate scheme. In our example, we select **http**.
10. Configure the Paths and Headers section as applicable. We leave these sections blank.
11. From the **Resource Item Properties** list, select **Advanced**.
12. From the **Compression** list, select **GZIP Compression**. While this is optional, enabling this allows the BIG-IP APM browser component to further compress content when necessary, providing bandwidth and download time savings.
13. From the **SSO configuration** list, select the SSO object you configured in Creating the SSO configuration, above. In our example, we select **SharePoint-Access-SSO**.
14. In the **Home Tab** row, you can optionally chose to enable the Home Tab. The Home Tab is a browser component that is inserted dynamically through the Access Virtual and allows users to browser pages within the context of BIG-IP APM. The Home Tab also allows users to log out. By clearing the Home Tab box, this feature is hidden.
15. Configure the rest of the settings as applicable to your configuration.
16. Click **Finished**.

Creating a Webtop

The next task is to create a Webtop that specifies the end user destination.

To create a Webtop

1. On the Main tab, expand **Access Policy**, and then click **Webtops**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this webtop. In our example, we type **SharePoint-Webtop**.
4. From the **Type** list, select **Web Applications**.
5. In the **Web Application start URI** box, type the start URI. This is the URI of the destination application that the user hits once they are authenticated and entitled to the resource. In our case, we enter the URI that our SharePoint Server has been configured to use, **http://sharepoint.siterequest.com**.
6. Click **Finished**.

Creating an Authentication Source

The next task is to create an Authentication Source that specifies an Active Directory Server.

To create an AAA server

1. On the Main tab, expand **Access Policy**, and then click **AAA servers**.
2. Click the **Create** button.
3. In the Name box, type a name for this profile. In our example, we type **SharePoint-AAA-AD**.
4. From the **Type** list, select the appropriate authentication method. For this example, we select **Active Directory**.
5. In the Domain Controller row, type the IP address or DNS name of the Active Directory server you'll be using. The BIG-IP must have network connectivity to this server.
6. In the **Domain Name** box, type the fully qualified domain name (FQDN) of your domain. (Note: unlike the SSO configuration, you must use the FQDN rather than the short NetBIOS domain name). In our example, we type **mydomain.siterequest.com**.
7. You do not need to supply an Admin Name or Admin Password.
8. Click **Finished**.

Creating an Access Profile

The next task is to create an Access Profile and a Visual Policy which provides a logon page, authentication against the Active Directory AAA source, SSO Credential mapping and a resource assignment. If you would optionally like to include a pre-login anti-virus check, follow the example shown in the Tivoli section of this document.

To create an Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **SharePoint_Access_Policy**.
4. In the Settings section, configure the options as applicable for your configuration. In our example, we leave all of the settings at their defaults. Note that depending on licensing, the number of concurrent users may be limited. The other timeouts are administrative choices.
5. In the Configuration section, from the **SSO Configurations** list, select the name of the SSO Configuration you created in *SSO Configuration*, on page 4-15. In our example, we type **SharePoint-Access-SSO**.
6. In our example and for most SharePoint applications, leave all other settings at their default values. Consult the BIG-IP documentation if you need details on configuring Language Settings.
7. Click **Finished**.

Editing the Access Profile with the Visual Policy Editor

The next task is to edit the Access Policy using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy.

To edit the Access Profile

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile you just created, and in the Access Policy column, click **Edit**. The Visual Policy Editor opens in a new window.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.

4. Select the **Logon Page** option button, and then click the **Add Item** button at the bottom of the box.
5. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults.
6. Click the **Save** button.
7. Click the **+** symbol on the between **Logon Page** and **Deny**.
8. Select the **AD Auth** option in the Authentication section, then click **Add Item**.
9. In the **Server field of the resulting AD Auth Active Directory** properties box, select the AAA source you created in *Creating an Authentication Source*, on page 4-17. In our example, we select **SharePoint-AAA-AD**.
10. Click the **Save** button. You now see two paths, ***Successful*** and ***Fall Back***.
11. At the end of the **Successful** path, click **Deny** in the ending box.
12. Select the **Allow** option, and click **Save**. The ending for Successful should now be **Allow**, and the ending for Fallback should be **Deny**.
13. Click the **+** symbol on the Successful path between **AD Auth** and **Allow**.
14. Select the **SSO Credential Mapping** item from the General Purpose section, then click **Add Item**. In our configuration example, we leave the settings for **SSO Token Username** and **SSO Token Password** at their default settings. Click **Save**.
15. Click the **+** symbol between **SSO Credential Mapping** and **Allow**.
16. Select the **Resource Assign** item from the General Purpose section, then click **Add Item**.
17. Click **Add New Entry**, then **Add/Delete Web Application Resources**.
18. Select the web application you created above. In our example, we select **SharePoint-application**. The counter on the Web Application Resource tab changes from 0 to 1.
19. Click the Webtop tab. Select the Webtop you created above. In our example, we select **SharePoint-Webtop**. The counter on the Webtop tab changes from 0 to 1.
20. Click **Update**, and then click **Save**.
21. Click the yellow **Apply Access Policy** link in the upper left part of the window. You always have to apply an access policy before it takes effect.
22. Click the **Close** button on the upper right to close the VPE.

Creating the HTTP profile

The next profile to create is the HTTP profile. This profile is required for the VPN to function. This should be a simple HTTP profile with no optimization (compression or caching).

To create the HTTP profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then click the **Create** button.
2. In the **Name** box, type a name for this profile. In our example, we type **Exchange-OWA-http**.
3. Modify any of the settings as applicable for your network, but ***do not*** enable compression or RAM Cache. See the online help for more information on the configuration options. In our example, we leave the settings at their default levels.
4. Click the **Finished** button.

Creating a Client SSL profile

The next step is to create an SSL profile. This profile contains SSL certificate and Key information for offloading SSL traffic. The first task is to import the certificate and key (for this Deployment Guide, we assume that you already have obtained the required SSL certificates, but they are not yet installed on the BIG-IP LTM system. If you do not have a certificate and key, see the BIG-IP documentation).

To import a key or certificate

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

The next task is to create the SSL profile that uses the certificate and key you just imported.

To create a new Client SSL profile

1. On the Main tab, expand **Local Traffic**, click **Profiles**, and then, on the Menu bar, from the **SSL** menu, select **Client**.
2. Click the **Create** button.
3. In the **Name** box, type a name for this profile. In our example, we type **Exchange-OWA_https**.
4. In the Configuration section, click a check in the **Certificate** and **Key** Custom boxes.
5. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
6. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
7. Click the **Finished** button.

Creating the virtual server

The final task is to create the virtual server.

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. 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 **SharePoint-OWA_vs**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address for this Access Virtual on APM.
   Note: This is different than the application VIP. This is the front-end service that users connect to.
   In our example, we type **10.133.56.124**.
6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.
7. From the **HTTP Profile** list, select the name of the profile you created in the *Creating the HTTP profile* section. In our example, we select **SharePoint-http**.
8. From the **SSL Profile (Client)** list, select the SSL profile you created in the *Creating a Client SSL profile* section. In our example, we select **SharePoint-https**.
9. In the Access Policy section, from the **Access Profile** list, select the name of the policy you created in *Creating an Access Profile*, on page 4-18. In our example, we select **SharePoint_Access_Policy**.
10. From the **Rewrite Profile** list, select the profile you created in *Creating the Rewrite Profile*, on page 14. In our example, we select **Exchange-OWA-Rewrite**.

11. Leave all other settings at the default levels (**Do not** configure any of the options in the WAN Optimization section).
12. Click the **Finished** button.

This completes the APM configuration for Microsoft Office SharePoint.