Deployment Guide

Document Version 1.4

What's inside:

Ready for IBM Tivoli software

Deploying F5 with IBM Tivoli Maximo Asset Management

Welcome to the F5 Deployment Guide for IBM® Tivoli® Maximo® Asset Management. This document provides guidance for deploying the BIG-IP Local Traffic Manager (LTM), BIG-IP WebAccelerator, BIG-IP WAN Optimization Manager (WOM) and BIG-IP Access Policy Manager (APM) with the IBM Maximo Asset Management system.

Why F5

This deployment guide is a result of F5 and IBM testing IBM's Maximo Asset Management system with BIG-IP systems. IBM and F5 have collaborated on building and testing Maximo Asset Management in order to bring the benefits of load balancing, traffic optimization, WAN optimization and security to our joint customers. Together, the BIG-IP system and IBM create a highly available, secure and fast Asset Management system.

For more information of IBM Maximo Asset Management system see:
http://www.ibm.com/software/tivoli/products/maximo-asset-mgmt/

For more information on the F5 BIG-IP LTM, WebAccelerator, WOM, APM, see
http://www.f5.com/products/big-ip

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

Products and versions tested

Product	Version
BIG-IP LTM, WebAccelerator, WOM	11.0, 11.0.1, 11.1
BIG-IP APM	11.0
IBM Tivoli Maximo Asset Management	Version 7 Release 1.0

Important: *Make sure you are using the most recent version of this deployment guide, found at http://www.f5.com/pdf/deployment-guides/ibm-tivoli-maximo-dg.pdf.*

Prerequisites and configuration notes

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

- In this guide we describe the offload of authentication with BIG-IP and Maximo using forms based (HTTP) authentication. Your Tivoli Maximo environment can optionally be configured to use Active Directory or another authentication source with which the BIG-IP APM can also communicate.

  For maximum offload of CPU processing, if you are using the BIG-IP APM for single sign-on, the BIG-IP APM must be configured to participate in the same authorization system that Maximo uses. For example, if Tivoli is using LDAP, the BIG-IP APM must be configured to use the same LDAP system.

Important →

- If you are using BIG-IP APM v11.x, you must be on version 11.0.

  Also, if using the BIG-IP APM, you must have NTP and DNS configured on the BIG-IP system. See *Appendix: Configuring DNS and NTP settings on the BIG-IP system on page 15* for specific instructions.

- If the BIG-IP WOM is used for WAN acceleration, routes must be setup between remote sites to allow for network transmission of WAN Accelerated traffic. WOM may be configured either to pass traffic securely over port 443, or insecurely to preserve the applications original ports (in the case of Maximo, port 80 if not SSL).

- In this guide we describe the offload of Authentication with BIG-IP and Maximo using forms based (HTTP) authentication. Your Tivoli Maximo environment can optionally be configured to use Active Directory or another authentication source with which the BIG-IP APM can also communicate.

  Currently supported authentication mechanisms which may be relevant to Maximo include: RADIUS, LDAP, Active Directory, RSA® SecureID, HTTP (described in this document) and Kerberos. Instructions for configuring Tivoli with Active Directory, which is optional for this deployment, are located here: *http://publib.boulder.ibm.com/infocenter/tamit/v7r2m2/index.jsp?topic=%2Fcom.ibm.itam_instWas.doc%2Finstall%2Ft_tamit_manconfigMSAD.html.*

- Be sure to see *Troubleshooting and FAQ on page 13* for common troubleshooting issues.

Configuration example and traffic flows

This deployment guide presents a layered solution for the deployment of BIG-IP systems and Maximo. With the inclusion of each BIG-IP component, another layer of benefit is added to the solution. Each layer and BIG-IP solution can stand independently, however, all are optional except for the BIG-IP LTM.

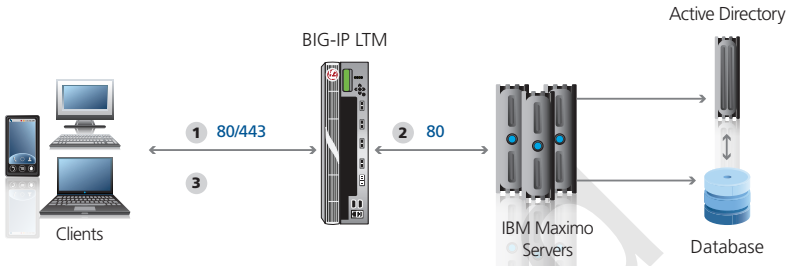
The four deployment scenarios presented in this guide (and described in detail in this section) are:

- BIG-IP LTM for application delivery control, (SSL offload, TCP optimization, caching, compression and high availability)
- BIG-IP WebAccelerator (object caching and intelligent browser referencing)
- BIG-IP APM (single sign-on and remote access)
- BIG-IP WOM (WAN optimization)

As noted, all four deployment scenarios can be combined together.

LTM for load balancing, monitoring, high availability and traffic management

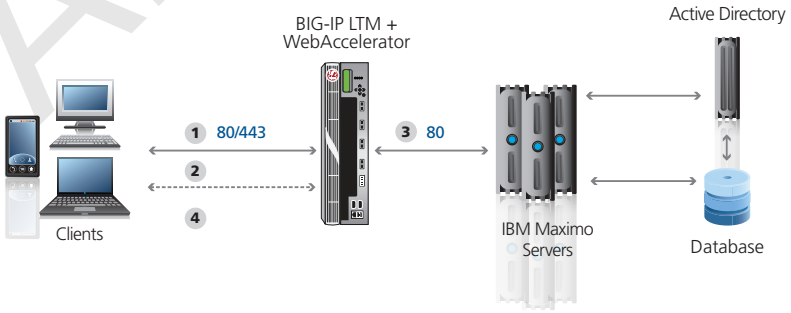
Our LTM scenario provides the core of the solution for the Maximo deployment and should always be used. High availability, monitoring, TCP traffic management and basic acceleration will be achieved with the installation of LTM. With LTM for Maximo, the objects required are a Health Monitor, Pool Members (which contain the Maximo servers themselves), Profiles for Compression, Web Acceleration, TCP, Persistence, OneConnect and SSL offload (if desired). Users will ultimately connect to the Virtual server which will offload SSL (if desired) and deliver traffic to the back-end servers. The connection flow for LTM connections is as follows:



1. User makes a connection to the BIG-IP LTM virtual server
2. The BIG-IP LTM virtual server makes a health check decision and delivers the request to the back-end server
3. The BIG-IP LTM virtual server responds to the client with the payload

WebAccelerator for object caching, acceleration of web content and intelligent browser referencing

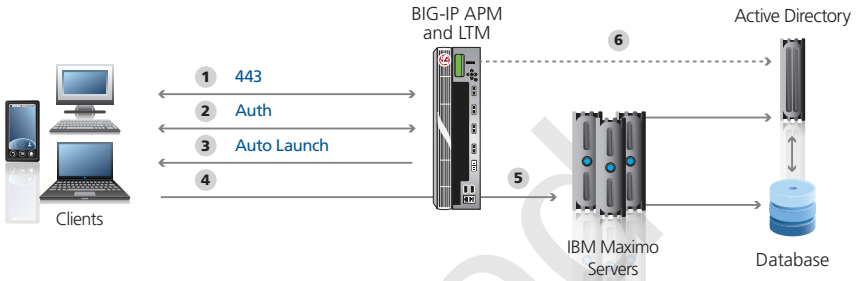
The WAM scenario is an additional component that can be added to the LTM solution. For Maximo installations where speed and acceleration are desired, WAM is recommended. After LTM is installed, WAM is enabled through the Web Acceleration profile. The connection flow with WAM enabled is as follows:



1. The user makes a connection to the BIG-IP LTM virtual server
2. The BIG-IP system consults its local cache to determine if the content is cached, if so, the content is immediately returned to the user
3. If the content is not available, the request is delivered to the back-end server
4. The BIG-IP system virtual server responds to the client with the payload and caches the content for future use if allowable by the policy

APM for single sign-on, security and remote access

The APM scenario solves one of the fundamental issues with any application: single sign-on. While APM is a full-featured product capable of many functions, in this scenario we focus on the benefit it brings to user log-on. The problem solved by APM is when one of the Maximo servers suffers an outage and a user is directed to another Maximo server. Without single sign-on, users will be required to sign-in again, a disruptive and time consuming distraction. With APM, session credentials are securely stored on the APM security device and passed to Maximo when needed. The user is required to sign in only once. The connection flow with APM enabled is as follows:



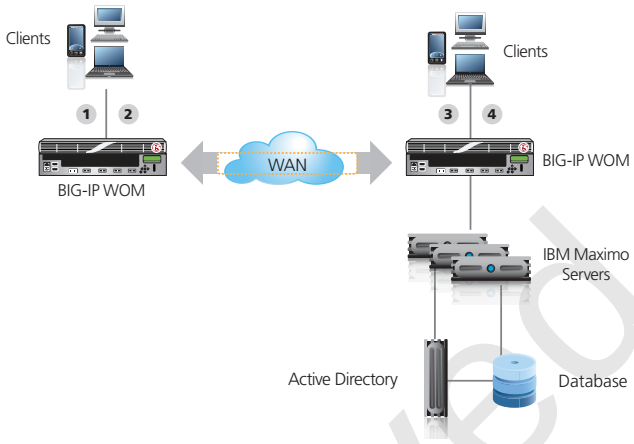
1. The user requests Maximo via a URL in their browser for the first time. This URL resolves to the APM virtual IP address on the BIG-IP system. The request is intercepted and analyzed by BIG-IP APM through the configuration which recognizes the login URI.
2. The BIG-IP APM requests the users credentials through a secure and customizable forms-based login page. After the user enters the credentials, BIG-IP APM securely authenticates against Maximo's authentication system (in this deployment guide through forms-based authentication, but optionally also through Active Directory, LDAP or other authentication system that Maximo is configured to use).
3. After successful authentication, the user is logged in (or the connection is denied and blocked after unsuccessful authentication). The user never directly interacts with the Maximo login screen.
4. Transactions now traverse the BIG-IP APM which is providing security and login services transparently. The user's connection goes to the APM Pool Resource, which in our deployment guide points to a BIG-IP LTM virtual address. The BIG-IP LTM provides all of the benefits of load balancing, SSL offload, optimization, caching, and more.
5. Requests from the LTM virtual server connect directly with the Maximo servers. Because requests are traversing both APM and LTM, if at any time LTM detects an outage with one or more Maximo servers, users are automatically and transparently directed to the remaining available Maximo Servers. At that time, APM detects the login page request by Maximo and securely passes the stored credentials. The user experiences no outage.
6. Optional 6: If Active Directory authentication is configured for Maximo, BIG-IP APM will directly query and authenticate against the Active Directory server. However, in this deployment guide we describe how to authenticate directly against the Maximo Servers through forms-based authentication.

Important →

BIG-IP APM is typically deployed as a layered solution, providing security in front of an application or network. Users connect to the virtual IP address associated with APM first. The APM virtual address contains a pool, which points to the LTM Virtual Server. This virtual server-to-virtual server scenario presents the most scalable and flexible security deployment available.

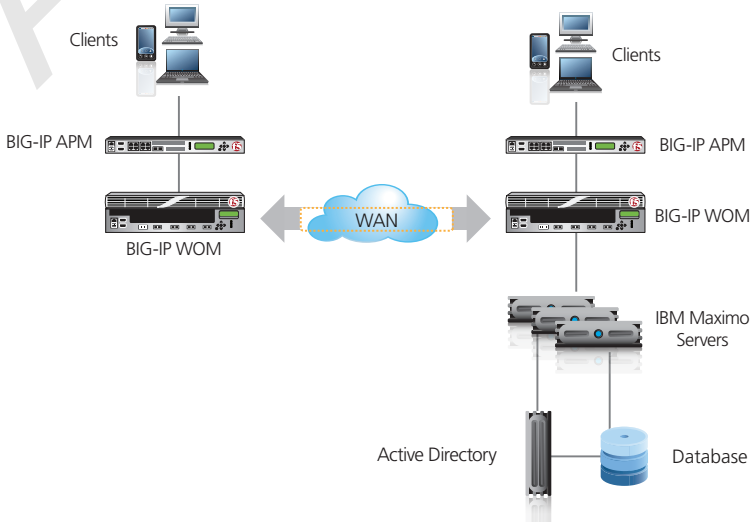
WOM for byte caching, WAN optimization, acceleration of traffic over networks and deduplication of frequently visited content

The WOM scenario extends acceleration by providing a symmetric byte cache for sites and remote data centers and requires BIG-IPs at both location. For Maximo installations over slow links with high latency, WOM is an ideal solution that provides compression, deduplication and encryption. The connection flow with WOM enabled is as follows:



1. The user at a remote site make a connection to the LTM virtual server
2. WOM consults its local byte cache to see if the content is available and serves it locally if it is
3. If the Content is not available, the request is delivered to the back-end server
4. WOM responds to the client with the payload and caches the content for future use

Together, these four solutions present all of the tools necessary to make Maximo Highly available, Accelerated and Secure. The following diagram shows all of the scenarios in this guide working together.



Configuring the BIG-IP LTM for Maximo

Use this section for configuring the BIG-IP LTM for IBM Tivoli Maximo. The following table contains a list of LTM objects along with any non-default settings you should configure as a part of this deployment. Settings not mentioned in the table can be modified as applicable for your configuration. For instructions on configuring individual objects, see the online help or manuals.

BIG-IP 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)
	Send String	**GET / HTTP/1.1\r\nHost: maximo.example.com\r\nConnection: Close\r\n\r\n**[1]
	Receive String	**Maximo**[2]
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name
	Health Monitor	Select the monitor you created above
	Load Balancing Method	Choose **Least Connections (Member)**
	Address	Type the IP Address Maximo nodes
	Service Port	**80** (repeat Address and Service Port for all nodes)
Profiles (*Main tab-->Local Traffic -->Profiles*)	***HTTP*** (*Profiles-->Services*)	Name: Type a unique name Parent Profile: **http** Redirect Rewrite[3]: **All**[3]
	HTTP Compression (*Profiles-->Services*)	Name: Type a unique name Parent Profile: **wan-optimized-compression**
	Web Acceleration (*Profiles-->Services*)	Name: Type a unique name Parent Profile: **webacceleration**
	TCP WAN (*Profiles-->Protocol*)	Name: Type a unique name Parent Profile: **wom-tcp-wan-optimized**
	TCP LAN (*Profiles-->Protocol*)	Name: Type a unique name Parent Profile: **wom-tcp-lan-optimized**
	Persistence (*Profiles-->Persistence*)	Name: Type a unique name Persistence Type: **Cookie**
	OneConnect (*Profiles-->Other*)	Name: Type a unique name Parent Profile: **oneconnect**
	Client SSL[3] (*Profiles-->SSL*)	Name: Type a unique name Parent Profile: **clientssl** Certificate: Select the Maximo Certificate Key: Select the associated Key
Virtual Server (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**443** if offloading SSL, **80** if not offloading SSL
	Protocol Profile (client)[2]	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)[2]	Select the LAN optimized TCP profile you created above

This table continues on the following page

[1] Replace red text with your FQDN. The String should be entered on a single line.
[2] The word "Maximo" appears in the default Maximo installation. If you have a custom page, choose a text string from that page here
[3] Only necessary if you are offloading SSL on the BIG-IP LTM

BIG-IP LTM configuration table continued

BIG-IP Object	Non-default settings/Notes	
Virtual Server (*Main tab-->Local Traffic -->Virtual Servers*)	***OneConnect Profile***	Select the OneConnect profile you created above
	HTTP Profile	Select the HTTP profile you created above
	HTTP Compression profile	Select the HTTP Compression profile you created above
	Web Acceleration profile	Select the Web Acceleration profile you created above
	SSL Profile (client)[1]	Select the Client SSL profile you created above
	SNAT Pool	**Automap**[2]
	Default Pool	Select the pool you created above
	Persistence Profile	Select the cookie persistence profile you created above

[1] Only necessary if you are offloading SSL
[2] Create a SNAT pool if you expect more than 64,000 simultaneous connections.

Configuring the BIG-IP WebAccelerator for Maximo

Use the following table to configure the WebAccelerator Application for Maximo.

Important

To configure the WebAccelerator, you must also configure the BIG-IP LTM as described in the preceding table. If you have not yet configured the BIG-IP LTM, return to the LTM configuration table on the previous page.

After you create the Application, you associate it with the Web Acceleration profile you created when configuring the BIG-IP LTM.

BIG-IP Object	Non-default settings/Notes	
WebAccelerator Application (*Main tab-->WebAccelerator --> Applications*)	***Application Name***	Type a unique name
	Policy	**Generic Policy - Complete**
	Requested Host	Type the Domain name used to access Maximo. Click **Add Host** to add additional hosts.

Adding the WebAccelerator Application to the Web Acceleration profile

The next task is to add the Application to the Web Acceleration profile you created.

To add the Application to the Web Acceleration profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
2. On the Menu bar, from the **Services** menu, select **Web Acceleration**.
3. Click the name of the Web Acceleration profile you created when configuring the BIG-IP LTM.
4. From the **WA Applications** row, click the Custom box.
5. From the **Available** box, select the Application you created, and then click **Enable**.
6. Click the **Update** button.

This completes the WebAccelerator configuration.

Configuring the BIG-IP APM for Maximo

In this section, we configure the BIG-IP Access Policy Manager (APM) for the Maximo devices. This table contains 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 implementation. For instructions on configuring individual objects, see the online help or manuals.

As mentioned in the prerequisites, you must be on APM version 11.0 and not a later version. Before beginning the APM configuration, you should have DNS and NTP configured on the BIG-IP system. See *Appendix: Configuring DNS and NTP settings on the BIG-IP system on page 15.*

BIG-IP Object	Non-default settings/Notes	
Rewrite Profile (*Access Policy-->Portal Access-->Rewrite Profiles*)	***Name***	Type a unique name
	Parent Profile	**Rewrite**
AAA Servers[1] (*Access Policy--> AAA Servers*)	***Name***	Type a unique name
	Type	**HTTP**
	Authentication Type	**Form Based**
	Form Method	**POST**
	Form Action[2]	http://maximo.example.com/maximo/ui/maximo.jsp
	Form Parameter for User Name	**username**
	Form Parameter for Password	**password**
	Hidden Form Parameters/Values	**event loadapp** **value startcntr** **login url**
	Number of Redirects to Follow	**1**
	Successful Logon Detection Match Type	**By Specific String in Response**
	Successful Logon Detection Match Value	**Start Center**
SSO Configurations (*Access Policy--> SSO Configurations*)	***Name***	Type a unique name.
	SSO Method	**Form Based**
	Use SSO Template	**None**
	Start URI	/maximo/webclient/login/login.jsp*
	Form Method	**POST**
	Form Action	/maximo/ui/maximo.jsp
	Form Parameter for User Name	**username**
	Form Parameter for Password	**password**
	Hidden Form Parameters/Values	**event loadapp** **value startcntr** **login url**
Portal Access (*Access Policy--> Portal Access*)	***Name***	Type a unique name
	Application URI	/maximo/webclient/login/login.jsp Click **Create**. Stay on Portal Access page to add Resource item
- Resource Items (*Web Application page-->Resource Items section-->Add)*	***Destination Type***	Click **IP Address** option button.
	Destination IP Address	Type the IP address of the LTM virtual server you created Maximo.
	Scheme	**HTTP**
	Port	Type the appropriate port. We use 80.
	Paths	/maximo/webclient/login/login.jsp
	Compression	**GZIP Compression** (optional)
	SSO Configuration	Select the SSO Configuration you created.

[1] Creating an AAA Server is optional
[2] Replace red text with your FQDN

This table continues on the following page

BIG-IP APM configuration table - continued

BIG-IP Object	Non-default settings/Notes	
Webtop (*Main tab-->Access Policy -->Webtops*)	***Name***	Type a unique name. We use **maximo-webtop**
	Type	**Web Applications**
	Web Application Start URI	Type the IP address or FQDN of the LTM virtual server you created for the Maximo Servers.
Connectivity Profile (*Main tab-->Access Policy -->Secure Connectivity)*	***Name***	Type a unique name
	Parent Profile	**Connectivity**
Access Profile (*Main tab-->Access Policy -->Access Profiles*)	***Name***	Type a unique name
	SSO Configuration	Select the SSO Configuration you created above
Access Policy (*Main tab-->Access Policy -->Access Profiles*)	***Edit***	Edit the Access Profile you created using the Visual Policy Editor. See *"Editing the Access Profile"* below for instructions.
Profiles (*Main tab-->Local Traffic -->Profiles*)	***HTTP*** (*Profiles-->Services*)	Name: Type a unique name Parent Profile: **http** (must ***not*** have compression or caching enabled)
	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-wan-optimized**
	Client SSL (*Profiles-->SSL)*	Name: Type a unique name Parent Profile: **clientssl** Certificate: Select the Certificate you imported Key: Select the associated Key you imported
Virtual Server (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.
	IP Address	Type the IP address for this virtual server. This is the address clients use for access.
	Service Port	**443**
	Protocol Profile (client)	Select the WAN optimized TCP profile you created above
	Protocol Profile (server)	Select the LAN optimized TCP profile you created above
	HTTP Profile	Select the HTTP profile you created above
	SSL Profile (Client)	Select the Client SSL profile you created above
	SNAT Pool	**Auto Map** (if you expect more than 64,000 concurrent connections, create a SNAT Pool)
	Access Profile	Select the Access Profile you created above
	Connectivity Profile	Select the Connectivity profile you created above
	Rewrite Profile	Select the Rewrite profile you created above
	Default Pool	Select the pool you created in the **BIG-IP LTM** section

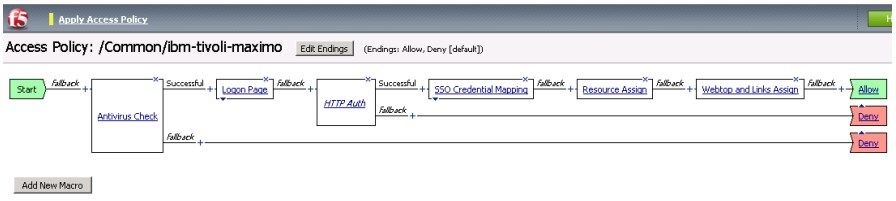
Editing the Access Profile

In the following procedure, we show you how to configure edit the Access Policy on the APM using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy. The Policy shown in the following procedure is just an example, you can use this Access Policy or create one of your own.

To configure the Access Policy

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. *Optional*: Click the **Antivirus Check** option button, and then click the **Add Item** button.
   a. Configure the Properties as applicable for your configuration, and then click the **Save** button. You now see two paths, **Successful** and **Fallback**.
   b. Click the **+** symbol on the Successful path between **Antivirus Check** and **Deny**.
5. Click the **Logon Page** option button, and then click the **Add Item** button.
6. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults. Click the **Save** button.
7. Click the **+** symbol on the between **Logon Page** and **Deny**.
8. *Optional:* If you created an AAA server in the APM table, click the **HTTP Auth** option button, and then click the **Add** button.
   a. From the **AAA Server** list, select the AAA server you created (in the table on page 8).
   b. Click **Save**. You see two paths, **Successful** and **Fallback** from the HTTP Auth box.
   c. Click the **+** symbol on the ***Successful*** path between **HTTP Auth** and **Deny**.
9. Click the **SSO Credential Mapping** option button, and then click the **Add Item** button.
10. Click the **Save** button.
11. Click the **+** symbol between **SSO Credential Mapping** and **Deny**.
12. Click the **Resource Assign** option button, and then click the **Add Item** button.
13. Next to **Portal Access Resources**, click the **Add/Delete** link.
14. Click a check in the box next to the Portal Access object you created (in the table on page 8), and then click **Save**.
15. Click the **+** symbol between **Resource Assign** and **Deny**.
16. Click the **Webtop and Links Assign** option button, and then click the **Add Item** button.
17. Next to **Webtop**, click the **Add/Delete** link.
18. Click the option button for the Webtop object you created (in the table on page 9), and then click **Save**.
19. Click the **Deny** link in the box to the right of **Webtop and Links Assign**.
20. Click **Allow** and then click **Save**. If you configured the optional settings, your Access policy should look like the example below.
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.



This completes the BIG-IP APM configuration.

Configuring the BIG-IP WAN Optimization Manager for Maximo

In this section, we configure the BIG-IP WOM to optimize Maximo traffic over the WAN. The WOM implementation requires you configure both the local and remote WOM device. In our example, we are configuring a BIG-IP WOM in a data center in Seattle (local), and a BIG-IP WOM in New York (remote).

BIG-IP WOM objects	Non-default settings/Notes	
Local BIG-IP WOM Configuration		
Quick Start (*Main tab-->WAN Optimization-->Quick Start*)	***WAN Self IP Address***	Type the WAN Self IP. This will be the Local End Point Self IP.
	Discovery	**Enabled**
	LAN VLANs	From the Available list, move the LAN VLANs to the Selected list. These VLANs should contain the Maximo devices.
	WAN VLANs	From the Available list, move the WAN VLANs to the Selected list. These VLANs should contain the Remote devices .
	Outbound iSession to WAN	**serverssl** (Optional: only necessary if you require encryption)
	Inbound iSession from WAN	**wom-default-clientssl** (or a custom profile you created)
	Create Optimized Applications	Check the **HTTP** box, **Enable** Data Encryption (optional), and then click **Apply**.
Remote Endpoint (*Main tab-->WAN Optimization-->Remote Endpoints*)	***Name***	Type a unique name
	IP Address	Type the IP address of the remote endpoint for WOM communication.
Advertised Routes (*Main tab-->WAN Optimization--> Advertised Routes*)	***Name***	Type a unique name.
	Address	Type the IP address of a subnet in which Maximo resides[1]
	Netmask	Type the corresponding Netmask.
Remote BIG-IP WOM Configuration		
Quick Start (*Main tab-->WAN Optimization-->Quick Start*)	***WAN Self IP Address***	Type the WAN Self IP. This will be the Local End Point Self IP.
	Discovery	**Enabled**
	LAN VLANs	From the Available list, move the LAN VLANs to the Selected list. These VLANs should contain the Maximo devices.
	WAN VLANs	From the Available list, move the WAN VLANs to the Selected list. These VLANs should contain the Remote devices .
	Outbound iSession to WAN	**serverssl** (Optional: only necessary if you require encryption)
	Inbound iSession from WAN	**wom-default-clientssl** (or a custom profile you created)
	Create Optimized Applications	Check the **HTTP** box, **Enable** Data Encryption (optional), and then click **Apply**.
Remote Endpoint (*Main tab-->WAN Optimization-->Remote Endpoints*)	***Name***	Type a unique name
	IP Address	Type the IP address of the remote endpoint for WOM communication.
Advertised Routes (*Main tab-->WAN Optimization--> Advertised Routes*)	***Name***	Type a unique name.
	Address	Type the IP address of a subnet the remote system can reach through this local device
	Netmask	Type the corresponding Netmask.

[1] For example, if your Maximo installation (servers) are in the 10.0.1.x/24 network, you would advertise 10.0.1.x/24 within WOM as a network that should be optimized. The host mask and subnet mask can be adjusted as needed to make the optimization more or less specific.

Next Steps

Now that you've completed the BIG-IP system configuration for IBM Tivoli Maximo Asset Management, here are some examples of what to do next.

Adjust your DNS settings to point to the BIG-IP system

After the configuration is completed, your DNS configuration should be adjusted to point to the BIG-IP virtual server for Maximo.

If you are using the BIG-IP LTM and not BIG-IP APM, you would change the DNS entry for the Maximo URL (http://maximo.example.com in our example), to point to the BIG-IP LTM virtual server IP address you configured in the LTM section.

If you are using BIG-IP APM, you would modify the DNS entry to point to the BIG-IP APM virtual server address you configured in the APM section (which then points to the BIG-IP LTM virtual server IP address).

Check the WOM Dashboard

If you have deployed BIG-IP WOM, the WOM Dashboard is an easy graphical method to examine performance gains and to learn what, if any, adjustments are necessary. You can access the WOM Dashboard from the BIG-IP Configuration utility by expanding **WAN Optimization** and then clicking **Dashboard**.

Check the APM Dashboard

If you have deployed the BIG-IP APM, the APM Dashboard is an easy graphical method of examining APM performance and user sessions. You can access the APM Dashboard from the BIG-IP Configuration utility by expanding **Access Policy** and then clicking **Dashboard**.

Additionally, the APM **Manage Sessions** menu allows for administrative management of user sessions. You can access the APM user session manager from the BIG-IP Configuration utility by expanding **Access Policy** and then clicking **Manage Sessions**.

Apply Analytics for testing, troubleshooting and measuring performance

By creating a custom Analytics profile and applying it to the LTM virtual server, you can gather useful statistics about the performance of the BIG-IP LTM. Learn more about Analytics by reading the LTM Analytics Implementations guide, found on Ask F5:
http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/bigip_analytics_implementations_11_0_0.html

Troubleshooting and FAQ

Q: When one of my Maximo servers is marked down and BIG-IP LTM sends subsequent existing and new requests to my other Maximo servers, users have to sign-in again. How can I prevent this from happening?

A: The IBM Tivoli Maximo Asset Management system does not have built-in session management for user logins. While user state and user transactions are stored in the Maximo database, user session information is independent. A secondary single sign-on solution must be deployed in order to achieve a seamless experience for users. The BIG-IP system provides the Access Policy Manager (APM) to solve this issue. By following the configuration instructions in this guide for APM (*Configuring the BIG-IP APM for Maximo on page 8*) users will experience a single sign-on experience with no changes required to Maximo or the users system. APM functions by authenticating the user's login against the same authentication database that Tivoli is configured to use. Then, by scanning subsequent requests for login requests, APM transparently handles authentication users, creating a seamless user experience.

Q: I am interested in using BIG-IP LTM and APM, however I do not want to use the WAN Optimization Manager, how do I proceed?

A: Each section of this deployment guide stands on its own and can be independently deployed. BIG-IP LTM and APM modules may be deployed without deploying WebAccelerator or WAN Optimization Manager.

Q: I am interested in using BIG-IP WebAccelerator because of its transaction time improvements, but I already have a WAN optimization device in my network. Are these redundant?

A: BIG-IP's WebAccelerator Module (WAM) is an integrated system on the BIG-IP platform and provides an object cache along with browser optimization, PDF linearization (Dynamic Linearization enables users to display PDF pages or jump to specific pages and view them without having to wait for the entire document to download first) and a host of other data offload benefits. WAM optimization provides compression, encryption and data deduplication without application awareness to bring benefits at the network layer. BIG-IP WebAccelerator can be deployed in conjunction with BIG-IP WAN Optimization Manager or other vendor's WAN optimization products. However, only one object cache system should be used. In our testing we have found the following results with Maximo

Maximo Asset Management - Total Transaction Time (average):
Satellite use case (2 Mbps, 300 ms latency, 0.25% packet loss)

Scenario	Baseline	With LTM + WAM	With LTM + WAM + WOM
First Visit (No browser cache)	***108.12 seconds***	***80.98 seconds***	***59.38 seconds***
Repeat Visit (Browser cache)	***85.19 seconds***	***45.80 seconds***	***30.63 seconds***
Maximo 2 MB upload	***54.22 seconds***	***19.35 seconds***	***2.52 seconds****

* WAN deduplication was in place and improved the upload of similar documents over the network to achieve these dramatic reductions.

Q: I would like to deploy BIG-IP WAN Optimization Manager, however I cannot deploy a BIG-IP at the remote site. How can I proceed?

A: WAN optimization typically requires a BIG-IP at both locations in order to achieve a symmetric deployment. Ultimately, a local cache is required at both the remote and local site in order to prevent the retransmission of cached content (known as data deduplication). In the case where symmetric deployments are not possible, the deployment of multiple asymmetric WebAccelerators will provide substantial benefits.

Q: I have deployed the APM module but I would like to modify the Access Policy using the VPE.

A: The Access Policy presented in the APM section of this guide is a suggestion for typical deployments. The APM is fully customizable both for look and feel (to match your company's visual layout) and for functionality. For example, the Antivirus check can be customized to require an Antivirus database that is less than 5 days old (or to your specific requirement). This would ensure the user has the most updated software on their machine before connecting to the environment. Another example is that HTTP Auth may be replaced by Active Directory authentication, or fallback pages may be inserted to present users with options if their machine does not pass the required endpoint inspection checks or authentication. We recommend reviewing the APM product manual for an understanding of all of APM's features: *http://support.f5.com/kb/en-us/products/big-ip_apm/versions.11_0_0.html*

Q: After deploying this solution, why am I having issues related to SSL offload?

A: If you are having issues with SSL Offload, we recommend performing the following tasks on the BIG-IP system and the WebSphere application server as applicable.

On the BIG-IP system
The HTTP profile must have the Request Header Insert enabled. To modify an existing profile to enable this header, use the following procedure.

1. On the Main tab, click **Local Traffic > Profiles**, and then click the name of the HTTP profile you created for the WebSphere application.
2. In the **Request Header Insert** row, click the **Custom** button if necessary, and then use the following syntax in the box: **<value>:**

   For example: **httpsoffload:** Be sure to include the colon. This value must match the value you configure on the WebSphere Application Server in the next section.
3. Click the **Update** button.

On the WebSphere application server
The WebSphere application server needs to be configured to detect the header you configured in the preceding procedure. For more specific instructions, consult the WebSphere documentation.

1. Connect to the administration port for the WebSphere server.
2. Navigate to **Servers** > **Application Servers** and then select the App Server.
3. Navigate to **Web Container Settings** > **Web Container** > **Custom Properties**.
4. Add a property named **httpsIndicatorHeader** and add a value of **httpsoffload**.
   Note that the property value must match the value used in the BIG-IP system, without the trailing colon, and finally, the property and value are case sensitive. Be sure you do not capitalize the "H" in httpsIndicatorHeader for WebSphere versions 7 or greater.
5. Navigate to **Environment** >**Virtual Hosts** and select the host for your application.
6. Select **Host Aliases**.
7. Add a property with the Host Name of ***** and a port of **443**

You must rebuild and redeploy your applications and restart your web and application servers.

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

If you are using the BIG-IP APM, you must have DNS and NTP settings configured on the BIG-IP system. If you do not, use the following procedures.

Configuring the DNS settings

In this section, you configure the DNS settings on the BIG-IP system to point to the Active Directory server.

➲ **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 Route to the Active Directory server. 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 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**.

Document Revision History

Version	Description
1.0	New guide
1.1	Changed the following settings in the BIG-IP APM configuration section: - Made the AAA Server object optional, and modified the settings - In the SSO Configuration section: Modified the Start URI and Form Action Values. Added Hidden Form Parameters/Values. Changed the Successful Logon Detection Match type to None. - In the Portal Access/Resource Items sections, changed the Application URI and Paths value. Added Next Steps section
1.2	- Corrected the example Form Action example when configuring the AAA Server for BIG-IP APM (there was an extraneous /maximo/). - Added the Ready for IBM Tivoli logo - Added support for versions 11.01 and 11.1 for LTM, WAM, and WOM. Added important note that APM must be on v11.0 only for the configuration in this guide.
1.3	Clarified version information
1.4	Added a new troubleshooting entry concerning SSL offload issues.

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