



What's inside:

- 2 Prerequisites and configuration notes
- 2 Configuration example
- 3 Configuring the BIG-IP LTM for the SiteMinder Administrative User Interface servers
- 5 Configuring the BIG-IP LTM for the SiteMinder Policy Servers
- 7 Next Steps
- 7 Optional: Configuring your directory servers for high availability with BIG-IP
- 8 Document Revision History

Deploying the BIG-IP System with CA SiteMinder

Welcome to the F5 deployment guide for CA SiteMinder®. This guide describes how to achieve high availability by deploying the BIG-IP Local Traffic Manager (LTM) with CA SiteMinder, load balancing the Administrative User Interface, the Policy Server and the User Directory Servers.

SiteMinder enables better control access to Web applications and portals for employees, customers and business partners — securely and efficiently — with powerful Web access management.

For more information on CA SiteMinder, see: <http://www.ca.com/us/web-access-management.aspx>

For more information on the BIG-IP LTM system, see <http://www.f5.com/products/bigip/ltm/>.

Why F5

CA SiteMinder is mission critical to the uptime and availability of entire websites . If SiteMinder is unavailable, so are the web servers that SiteMinder serves. Therefore, high availability and proactive health monitoring is critical to the success of all SiteMinder deployments.

Organizations using SiteMinder receive the benefits immediately after deploying the BIG-IP LTM:

- High availability of CA SiteMinder Policy Servers at the network layer. Instead of configuring IP Addresses manually in the SiteMinder Configuration files and relying on manual intervention, the BIG-IP system automatically directs users to the most available CA SiteMinder server.
- High availability of CA Administrative UI servers. Equally as important as the Policy Servers, if an Administrative server goes down, users are no longer able to maintain, manage or troubleshoot policy servers. Load balancing the Administrative UI is often overlooked, but is extremely important.
- With the BIG-IP system, organizations can configure an architecture that solves the many different pieces of a CA Architecture entirely on one platform, the BIG-IP LTM. Specifically, the BIG-IP LTM addresses the high availability needs of Policy Servers, Directory Servers, Administrative Servers, and the content servers themselves.

Products and versions tested

Product	Version
BIG-IP LTM	11.2 HF-1
CA SiteMinder	12.0 SP 3

Important: Make sure you are using the most recent version of this deployment guide, available at www.f5.com/pdf/deployment-guides/ca-siteminder-dg.pdf

Prerequisites and configuration notes

- The BIG-IP LTM system must be running version 11.2 HF 1 or later.
- Each SiteMinder Administrative UI server must be registered directly with a SiteMinder Policy server before it is configured for load balancing. Register your Administrative UI servers directly with a policy server instead of using the BIG-IP Virtual IP Address (VIP). After initial registration you may point to the BIG-IP system's virtual server address. See *Configuring the SiteMinder devices on page 3*.

Configuration example

SiteMinder is a critical component of any infrastructure in which it is deployed, so being able to achieve high availability is critical. The BIG-IP system can bring high availability through monitoring to CA SiteMinder environments.

The CA SiteMinder environment has several locations where scaling and high availability are critical:

- The BIG-IP system is deployed in front of multiple redundant Administrative User Interfaces
- The BIG-IP system is deployed in front of multiple redundant Policy Servers
- The BIG-IP system is deployed in front of the entitlement and user stores (LDAP)

After the deployment of BIG-IP these are the traffic scenarios:

1. Administrators use the Administrative UI virtual server on the BIG-IP system to manage and administer CA SiteMinder. This virtual server is typically *not* externally accessible.
2. Agents, configured on web servers and application servers, communicate through a virtual server on the BIG-IP system to the Policy Server. This virtual server is also not typically externally accessible.
3. The Policy Server communicates to a virtual server on the BIG-IP system to reach the LDAP servers.

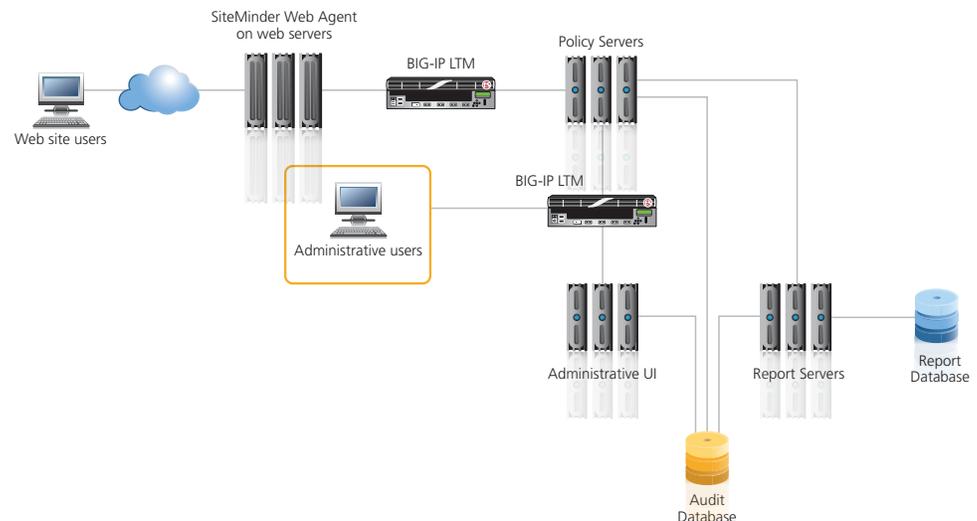


Figure 1: Logical configuration example

Configuring the BIG-IP LTM for the SiteMinder Administrative User Interface servers

The SiteMinder Administrative User Interface must be used to manage and configure the CA SiteMinder environment. If anything happens to the machine running the Administrative User Interface, management of the CA environment becomes difficult and it could lead to a complete site-wide outage. CA recommends the deployment of multiple redundant Administrative User Interface servers.

Each Administrative User Interface device must be registered with a Policy server. In the case of multiple identical policy servers, it is important that each Administrative User Interface machine is registered before configuring the BIG-IP system for load balancing.

Configuring the SiteMinder devices

Use the following guidance for configuring SiteMinder devices. Refer to the CA documentation for specific instructions.

1. Setup two identical servers and install the CA Administrative User Interface servers
2. Initiate the setup scripts according to CA's instructions and register the Administrative User Interface with the Policy server's direct IP address.
3. Repeat step 2 to register the Policy Server with the other Policy servers in your environments.
4. Configure the BIG-IP LTM system for the Administrative UI servers.
5. Configure the BIG-IP LTM for the Policy Servers.
6. Adjust the IP address on the Administrative User Interface to point to the BIG-IP LTM virtual server IP address for the Policy Servers.

Following these steps ensures that each Administrative UI device is properly registered with each Policy Server. If your Administrative UI devices are already registered, these steps can be skipped.

Configuration table for the Administrative User Interface

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

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (Main tab-->Local Traffic -->Monitors)	Name	Type a unique name
	Type	HTTP
	Interval	30 (recommended)
	Timeout	91 (recommended)
	Send String	GET /iam/siteminder/console HTTP/1.0\r\n\r\n
	Receive String	SiteMinder

BIG-IP LTM Object	Non-default settings/Notes	
Pool (Main tab-->Local Traffic -->Pools)	Name	Type a unique name
	Health Monitor	Select the monitor you created above
	Load Balancing Method	Choose a load balancing method. We recommend Least Connections (Member)
	Address	Type the IP Address of an Administrative User Interface server
	Service Port	Type the service port, typically 8080 . Click Add , and repeat Address and Port for all servers.
Profiles (Main tab-->Local Traffic -->Profiles)	TCP (Profiles-->Protocol)	Name Parent Profile Type a unique name tcp-lan-optimized¹
	HTTP (Profiles-->Services)	Name Parent Profile Redirect Rewrite Type a unique name HTTP All
	Client SSL (Profiles-->SSL)	Name Parent Profile Certificate Key Type a unique name clientssl Select the certificate you imported Select the associated key
	Server SSL² (Profiles-->SSL)	Name Parent Profile Type a unique name serverssl
	Persistence (Profiles-->Persistence)	Name Persistence Type Type a unique name Cookie
	Persistence (Profiles-->Persistence)	Name Persistence Type Type a unique name for this fallback persistence profile Source Address Affinity
	Virtual Server (Main tab-->Local Traffic -->Virtual Servers)	Name Address Service Port Protocol Profile (client)² HTTP Profile SSL Profile (Client) SSL Profile (Server)³ SNAT Pool⁴ Default Pool Default Persistence Profile Fallback Persistence Profile

¹ If you have users connecting to the administrative interface primarily over a WAN connection, use the tcp-wan-optimized parent profile.

² You must select **Advanced** from the **Configuration** list for this option to appear

³ Only create a Server SSL profile if you are configuring the BIG-IP LTM for SSL Bridging.

⁴ If want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.

Configuring the BIG-IP LTM for the SiteMinder Policy Servers

In this section, you configure the BIG-IP LTM for the SiteMinder Policy Servers.

Configuration table for the Policy Servers

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

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (Main tab-->Local Traffic -->Monitors)	Name	Type a unique name
	Type	TCP
	Interval	30 (recommended)
	Timeout	91 (recommended)
Pool (Main tab-->Local Traffic -->Pools)	44441 Policy server pool	
	Name	Type a unique name
	Health Monitor	Select the monitor you created above
	Load Balancing Method	Choose a load balancing method. We recommend Least Connections (Member)
	Address	Type the IP Address of a Policy Server
	Service Port	44441 Click Add , and repeat Address and Port for all servers.
	44442 Policy server pool	
	Name	Type a unique name
	Health Monitor	Select the monitor you created above
	Load Balancing Method	Choose a load balancing method. We recommend Least Connections (Member)
	Address	Type the IP Address of a Policy Server
	Service Port	44442 Click Add , and repeat Address and Port for all servers.
44443 Policy server pool		
Name	Type a unique name	
Health Monitor	Select the monitor you created above	
Load Balancing Method	Choose a load balancing method. We recommend Least Connections (Member)	
Address	Type the IP Address of a Policy Server	
Service Port	44443 Click Add , and repeat Address and Port for all servers.	
Profiles: Persistence (Main tab-->Local Traffic -->Profiles-->Persistence)	Name	Type a unique name
	Persistence Type	Source Address Affinity
	Match Across Virtual Servers	Enabled (Click a check in the box)

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Server (Main tab-->Local Traffic -->Virtual Servers)	44441 virtual server	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server. <i>All Policy Server virtual servers must have the same IP address.</i>
	Service Port	44441
	SNAT Pool ¹	Automap (optional; see footnote ¹)
	Default Pool	Select the pool you created using port 44441
	Default Persistence Profile	Select the Persistence profile you created.
	44442 virtual server	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server. <i>All Policy Server virtual servers must have the same IP address.</i>
	Service Port	44442
	SNAT Pool ¹	Automap (optional; see footnote ¹)
	Default Pool	Select the pool you created using port 44442
	Default Persistence Profile	Select the Persistence profile you created.
	44443 virtual server	
Name	Type a unique name.	
Address	Type the IP Address for the virtual server. <i>All Policy Server virtual servers must have the same IP address.</i>	
Service Port	44443	
SNAT Pool ¹	Automap (optional; see footnote ¹)	
Default Pool	Select the pool you created using port 44443	
Default Persistence Profile	Select the Persistence profile you created.	

¹ If want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation on configuring SNAT Pools.

Next Steps

After completing the BIG-IP LTM configuration, perform the following tasks on your SiteMinder servers. See the SiteMinder documentation for specific instructions.

1. Adjust your **SmHosts.conf** files on every webAgent to point to the BIG-IP virtual server address for Policy Server.
2. Adjust your Administrative User Interface to point to the appropriate BIG-IP virtual server for Policy Server
3. Advertise the BIG-IP virtual server address for the Administrative User Interface so that users can administer CA using this implementation.
4. Adjust the User Directory settings with the CA SiteMinder Configuration to point to the BIG-IP virtual server IP address for the LDAP servers.

Optional: Configuring your directory servers for high availability with BIG-IP

We strongly recommend configuring BIG-IP LTM for your directory servers. You can find deployment guides for configuring directory servers on f5.com (<http://www.f5.com/products/documentation/deployment-guides/>).

In this section, we show you how to use the BIG-IP LTM iApp template for LDAP servers. For more information on iApps, see <http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf>

To configure the iApp for LDAP

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **SiteMinder_LDAP_**.
5. From the **Template** list, select **f5.Idap**.
The LDAP template opens.
6. Complete the template as appropriate for your LDAP configuration.
7. Click the **Finished** button.
8. Adjust your policy server to point to the BIG-IP virtual server for your directory servers.

For more information on configuring the BIG-IP LTM for LDAP servers, including manual configuration procedures, see <http://www.f5.com/pdf/deployment-guides/ldap-iapp-dg.pdf>

Document Revision History

Version	Description	Date
1.0	New Version	09-11-2012

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

