



DEPLOYMENT GUIDE

DEPLOYING THE BIG-IP LTM SYSTEM WITH SAP NETWEAVER AND ENTERPRISE SOA

Introducing the BIG-IP Deployment Guide for SAP NetWeaver and Enterprise SOA

Welcome to the BIG-IP LTM - SAP Deployment Guide. By taking advantage of this Application Ready infrastructure for SAP®, tested and validated at SAP, organizations can achieve a secure, fast and available network infrastructure that reduces the total cost of operation and increases ROI. This guide gives you step-by-step procedures on how to configure the BIG-IP LTM system to optimally direct traffic for SAP deployments.

For more information on the BIG-IP system, see

<http://www.f5.com/products/big-ip/>.

For more information on SAP, see <http://www.sap.com/index.epx>.

Prerequisites and configuration notes

The following are prerequisites for this Deployment Guide:

- ◆ We recommend using the latest version of SAP NetWeaver and mySAP Business Suite applications. Our testing environment included SAP NetWeaver 2004 and mySAP ERP 2005. High availability was configured for Enterprise Portal and Composite Services on the front end along with Exchange Infrastructure (XI), Business Warehouse (BW), and Exchange Core Component (ECC).
- ◆ The BIG-IP LTM system must be running version 9.0 or later, we strongly recommend running version 9.3 or later. Some of the examples in this guide use profiles introduced in version 9.4. To use these profiles you must either be running LTM version 9.4, or refer to the *Configuration Guide for BIG-IP Local Traffic Management* for version 9.4 (available on AskF5), which shows the configuration differences between the base profiles and the optimized profile types.
- ◆ We assume that the BIG-IP LTM device is already installed in the network, and objects like Self IPs and VLANs have already been created. For more information on configuring these objects, see the BIG-IP LTM manuals.
- ◆ This document is written with the assumption that you are familiar with both the BIG-IP LTM system and SAP products. For more information on configuring these devices, consult the appropriate documentation.
- ◆ Make a list of the IP addresses and ports used by each SAP application component in your deployment, as these are used in the BIG-IP LTM system configuration. Consult the SAP documentation and your SAP administrator for this information.
- ◆ If you are using the BIG-IP LTM system to offload SSL traffic from the SAP servers, you must already have obtained an SSL Certificate (but not necessarily installed it on the BIG-IP LTM system). For more

information about offloading SSL traffic, see *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 24.

Configuring the SAP Enterprise Portal for load balancing with the BIG-IP LTM system

This section contains a brief description of how to create a new **System** within SAP EP using the load balancing template that allows the BIG-IP LTM system to load balance the SAP devices.

Important

This is just an overview of some of the SAP configuration details related to load balancing. For more detailed instructions on configuring your SAP solution, see the SAP documentation or contact SAP.

To create a new SAP System

1. Log on to the SAP Enterprise Portal (EP).
2. On the Menu bar, click **System Administration**, and then click **System Configuration**.
3. In the Detailed Navigation pane, click **System Landscape**.
4. Expand **Portal Content**, and then the name of your company/portal.
5. Click **System**. From the System menu, select **New**, and then **System** (see Figure 2). You create a new System for each non EP SAP application type.
The System Wizard opens.

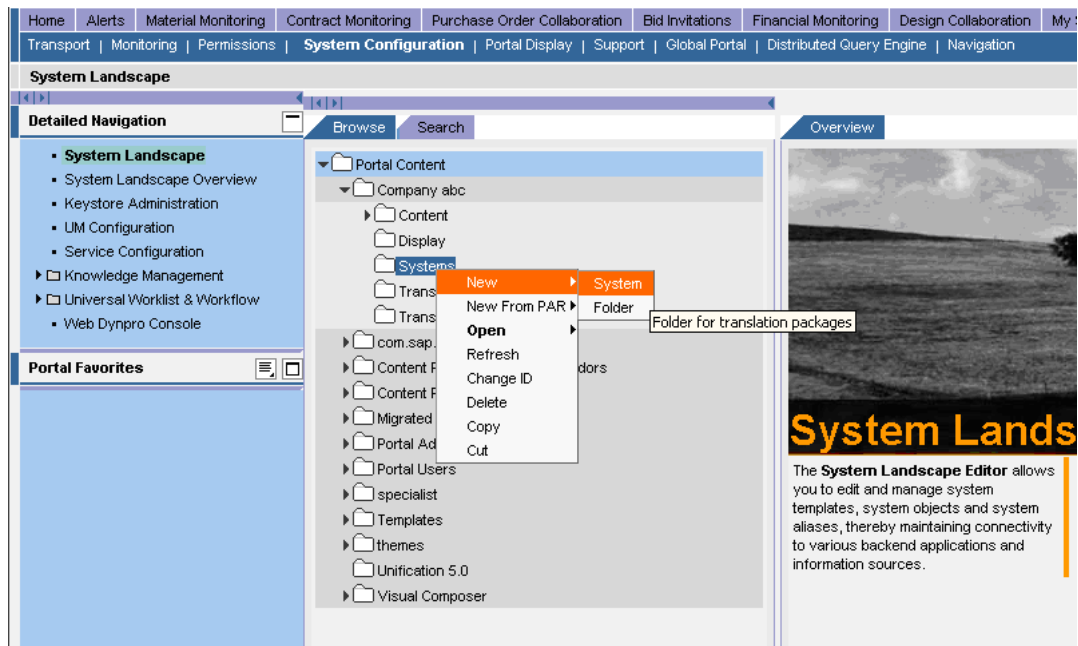


Figure 1 Creating a new System in the SAP Enterprise Portal

- From the System Wizard, Template selection, select **SAP system with load balancing** (see Figure 3), and then click the **Next** button.

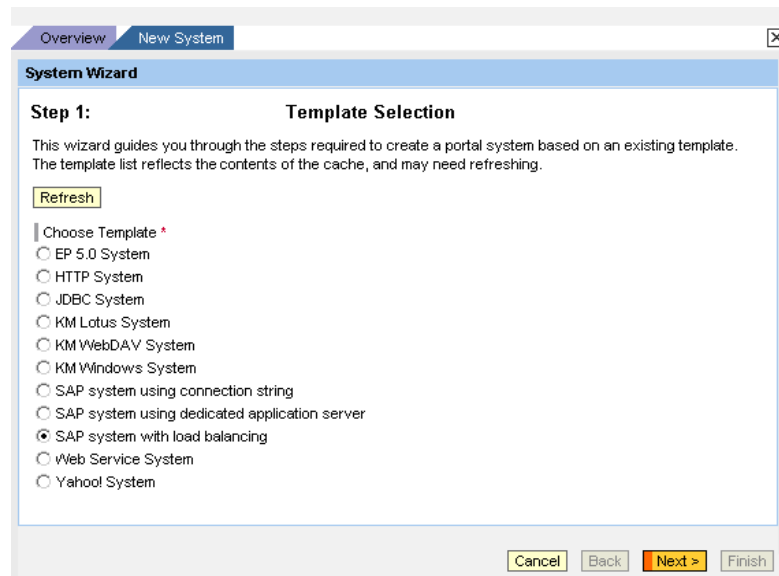


Figure 2 Selecting the load balancing option from the System wizard

7. In the General Properties step, enter the following information (see Figure 4):
 - a) In the **System Name** box, type a name for this system, using the following syntax: **SAP <System Type> <System Name>**
In our example, we type **SAP ECC**.
 - b) In the **System ID** box, type a system ID, using the following syntax: **sap_<system id>**
In our example, we type **sap_ecc**.
 - c) In the **System ID Prefix** box, type a system ID using a prefix from the SAP deployment guidelines (**com.<companyname>.erp.ops.sys**). In our example, we type **com.companyabc.erp.ops.sys**.
 - d) From the **Master Language** list, select a language. In our example, we select **English**.
 - e) In the **Description** box, you can type an optional description of this system.
8. Click the **Next** button.

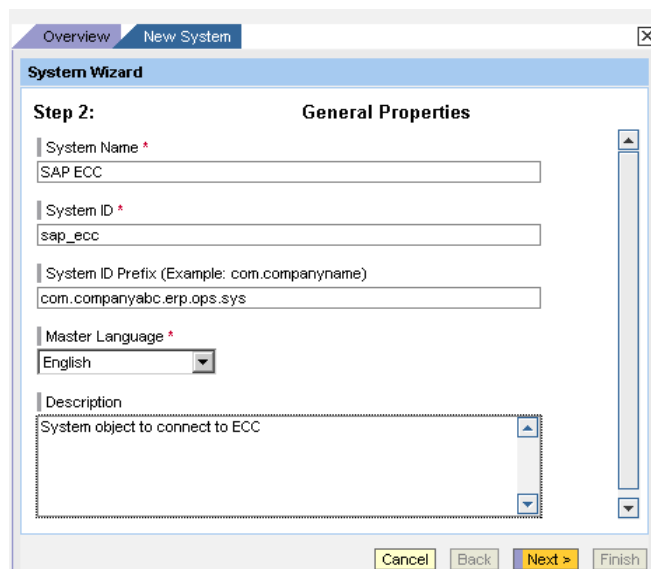


Figure 3 Entering the General properties of the system

9. Complete the Property Editor based on the following table:

Property	Value	Example
Group	<Group ID>	ECC_PRD_01
ITS Host Name	<Load-balanced ITS server host name>: 80 <System #>	Gerp.ecc.site.com:8050 *see warning below
ITS Path	<Path to ITS home>	/sap/bc/gui/sap/its/
ITS Protocol	"http" or "https"	http
Logical System Name	<System ID>CLNT<System #>	RP1CLNT030
Message Server	<System message server>	usri-pdbx-c01.site.com
SAP Client (*)	<SAP Client>	030
SAP System ID	<System ID>	RP1
Server Port	36<System #>	3650
System Type	<Type of system>	SAP_R3
WAS Host Name	<Load-balanced WAS server host name>:5<System #>00	gerp-rp1-ecc.site.com:55000 *see note on the following page
WAS Path	<WAS path>	/webdynpro/dispatcher
WAS Protocol	"http" or "https"	http

Table 1.1 SAP Property table

◆ WARNING

** In the preceding examples, some of the entries include the port numbers. It is critical that if you are using the **BIG-IP LTM** system to terminate SSL traffic, that you do **NOT** use port numbers as shown in the table. If the application ports are hard coded, SSL termination will break the application.*

10. Click the **Next** button. The System Alias Editor opens.
11. In the **Alias** box, type at least one system alias for each object. Every object should have a system alias of the form **SAP_<System Type>_<Environment>** (for example SAP_SRM_QAS).

Note that certain system aliases are required for the portal business packages to work; these aliases are listed in the following table:

System	Alias	For Bus Pack
ECC	SAP_R3_HumanResources	ESS / MSS
Web Dynpro runtime (ECC)	SAP_WebDynpro_XSS	ESS / MSS
SRM	SAP_EBP, SAP_R3_Procurement	SRM / Supplier Collaboration

It is also important to note that system aliases cannot be transported - they must be assigned manually in each EP environment.

- Click the **Save** button.

Configuring the BIG-IP LTM system for deployment with SAP

This Deployment Guide is broken up into three sections:

- ◆ *Configuring the BIG-IP LTM system for the SAP Enterprise Portal, on page 7*
- ◆ *Configuring the BIG-IP LTM system for the SAP ERP Central Component (ECC), on page 18*
- ◆ *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment, on page 24 (optional).*

A SAP deployment can be incredibly large and complex, deployed in infinite variations, with number of different SAP applications and components. In this Deployment Guide, we focus on providing high availability and acceleration for the SAP Enterprise Portal and an example SAP application component: ERP Central Component (ECC). The procedures outlined for the SAP ECC can be repeated for any additional SAP application components you may be running.

◆ Tip

*We recommend you save your existing BIG-IP configuration before you begin the procedures in this Deployment Guide. To save your BIG-IP configuration, see **Appendix A: Backing up and restoring the BIG-IP system configuration**, on page 33.*

The BIG-IP LTM system offers both web-based and command line configuration tools, so that users can work in the environment that they are most comfortable with. This Deployment Guide contains procedures to configure the BIG-IP system using the BIG-IP web-based Configuration utility only.

Connecting to the BIG-IP device

Use the following procedure to access the BIG-IP web-based Configuration utility using a web browser.

To connect to the BIG-IP system using the Configuration utility

1. In a browser, type the following URL:
https://<administrative IP address of the BIG-IP device>
A Security Alert dialog box appears, click **Yes**.
The authorization dialog box appears.
2. Type your user name and password, and click **OK**.
The Welcome screen opens.

Once you are logged onto the BIG-IP system, the Welcome screen of the new Configuration utility opens. From the Configuration utility, you can configure and monitor the BIG-IP system, as well as access online help, download SNMP MIBs and Plug-ins, and search for specific objects.

Configuring the BIG-IP LTM system for the SAP Enterprise Portal

In this section, we configure the BIG-IP LTM system to manage traffic for the SAP Enterprise Portal.

To configure the BIG-IP LTM system for the SAP Enterprise Portal, you must complete the following procedures:

- *Creating the HTTP health monitor*
- *Creating the pool*
- *Creating profiles*
- *Creating the virtual server*

◆ Note

*If you are using the BIG-IP LTM system to offload SSL, there are additional procedures you must follow. After completing this section, go to **Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment**, on page 24.*

Creating the HTTP health monitor

The first step is to set up a health monitor for the SAP Enterprise Portal servers. For this configuration, we create a simple HTTP health monitor. Although the monitor in the following example is quite simple, you can

configure optional settings such as Send and Receive Strings to make the monitor much more specific. You can also use one of the other types of monitors available on the BIG-IP LTM system.

To configure the HTTP health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**. The Monitors screen opens.
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 **sap_http**.
4. From the **Type** list, select **HTTP**. The HTTP Monitor configuration options appear.
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 an **Interval of 30** and a **Timeout of 91**.
6. In the Send String and Receive Rule sections, you can add an optional Send String and Receive Rule specific to the device being checked.

Local Traffic >> Monitors >> New Monitor...	
General Properties	
Name	sap_http
Type	HTTP
Import Settings	http
Configuration: Basic	
Interval	5 seconds
Timeout	16 seconds
Send String	GET /
Receive String	
User Name	
Password	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

Figure 4 Creating the HTTP Monitor

-
7. Click the **Finished** button.

The new monitor is added to the Monitor list.

Remember that if you configure a Send String and Receive String specific to one of the application components, you should create a new monitor for the other components.

Creating the pool

The next step is to create a pool on the BIG-IP LTM system for the SAP Enterprise Portal nodes.

To create a new pool for the Enterprise portal servers

1. On the Main tab, expand **Local Traffic**, and then click **Pools**.
The Pool screen opens.
2. In the upper right portion of the screen, click the **Create** button.
The New Pool screen opens.
*Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.*
3. In the **Name** box, type a name for the pool. We use **sap_portal**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the HTTP health monitor* section, and click the Add (<<) button. In our example, we select **sap_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**.
6. In the New Members section, make sure the **New Address** option button is selected.
7. In the **Address** box, add the first server to the pool. In our example, we type **10.132.81.1**.
8. In the **Service Port** box, type the appropriate port. In our example, we type **80**. Your SAP Portal services might be running on a different TCP port, such as port **50000**. Type the proper port number here, and the BIG-IP LTM system will properly perform the translation.
If you are using the BIG-IP LTM system for offloading SSL, see *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 24 after completing this section.
9. Click the **Add** button to add the member to the list.
10. Repeat steps 9-11 for each SAP Enterprise Portal server. In our example, we repeat these steps for **10.132.81.2** and **10.132.81.3**.

11. Click the **Finished** button.

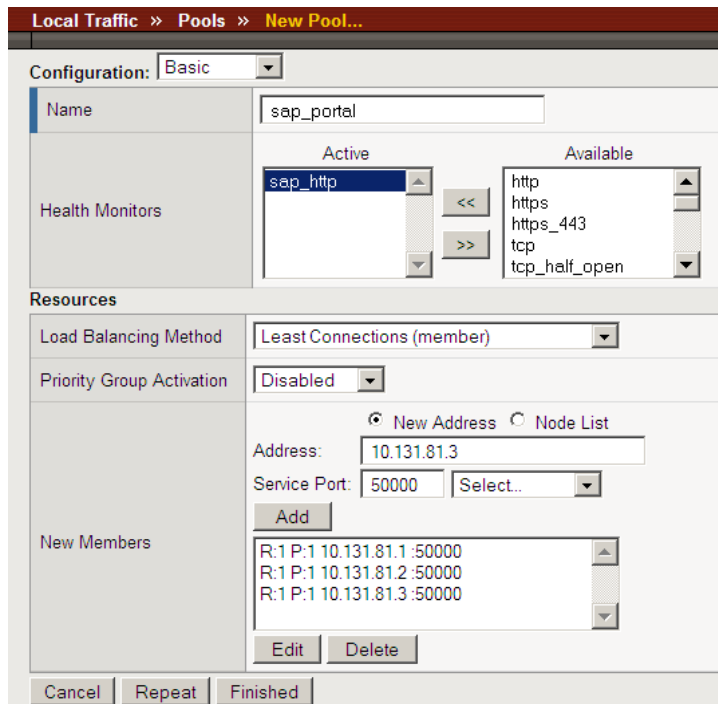


Figure 5 Creating the pool for the Enterprise Portal devices

Creating profiles

BIG-IP version 9.0 and later use profiles. A *profile* is an object that contains user-configurable settings, with default values, for controlling the behavior of a particular type of network traffic, such as HTTP connections. Using profiles enhances your control over managing network traffic, and makes traffic-management tasks easier and more efficient.

Although it is possible to use the default profiles, we strongly recommend you create new profiles based on the default parent profiles, even if you do not change any of the settings initially. Creating new profiles allows you to easily modify the profile settings specific to this deployment, and ensures you do not accidentally overwrite the default profile.

For this configuration, we create the following profiles: an HTTP profile, a TCP profile, a OneConnect profile and two persistence profiles. If you are using the BIG-IP LTM system to terminate SSL traffic, there are additional profiles you need to create. See *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 24.

Creating an HTTP profile

The first new profile we create is an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic. For implementations where the majority of users accessing SAP Enterprise Portal are connecting across a WAN, F5 recommends enabling compression and caching on the BIG-IP LTM by using a profile introduced in BIG-IP version 9.4 called **http-wan-optimized-compression-caching**. This profile uses specific compression and caching (among other) settings to optimize traffic over the WAN. Note that to properly use this profile, you need to have compression and caching licensed on the BIG-IP LTM. For more information on licensing, contact your sales representative.

◆ Tip

*If you are using a version of BIG-IP LTM previous to v9.4, the **Configuration Guide for BIG-IP Local Traffic Management** for version 9.4 (available on AskF5) shows the configuration differences between the base HTTP profile and the optimized profile types. Use the Configuration Guide to manually configure the optimization settings.*

In our example, we also configure the HTTP profile to encrypt the SAP cookie as well as the BIG-IP LTM cookie. This helps prevent cookie tampering attacks by denying malicious users from modifying the otherwise cleartext cookie to gain unauthorized access. Although encrypting cookie is optional, we recommend it. In BIG-IP LTM version 9.4, you simply click a check box for cookie encryption. In versions prior to 9.4, you need to configure an iRule to perform the encryption. See the following post on DevCentral for more information:

<http://devcentral.f5.com/weblogs/Joe/archive/2005/11/09/1541.aspx>

If you are using the BIG-IP LTM system to offload SSL traffic from the SAP deployment, you need to configure an alternate HTTP profile, among other settings. After completing the Enterprise Portal configuration, be sure to see *Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment*, on page 24.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **sap_http-opt**.
4. From the **Parent Profile** list, select **http-wan-optimized-compression-caching**. The profile settings appear.

5. *Optional:* Click a check in the Custom box in the **Encrypt Cookies** row. Type the name of the cookies you want to encrypt, with a space between each cookie. In our example, we type the name of the SAP cookie (**MYSAPSSO2** by default), and the BIG-IP cookie (**BIGipServer<Name_of_Pool>** by default, so in our example, **BIGipServersap_portal**).

You can either modify the Cookie Passphrase or leave it at the default. In our example, we leave it at the default.

6. Check the Custom box for **Content Compression**, and leave **Content List** selected.
7. In the Content List section, add the following items to the existing entries in the **Content Type** box one at a time, each followed by clicking **Include**:
 - **application/pdf**
 - **application/vnd.ms-powerpoint**
 - **application/vnd.ms-excel**
 - **application/msword**
 - **application/vnd.ms-publisher**

We add these MIME types to ensure these highly compressible document types are compressed.

8. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
9. Click the **Finished** button.

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the Enterprise Portal users are accessing the portal via a Local Area Network, we recommend using the base TCP profile as the parent. If the majority of the Enterprise Portal users are accessing the system from remote or home offices, we recommend using two new profiles available in BIG-IP LTM version 9.4, called **tcp-wan-optimized** (for client side TCP connections) and **tcp-lan-optimized** (for server-side TCP connections). In our example, we leave these profiles at their default levels; you can configure any of the options as applicable for your network.

◆ Tip

*If you are using a version of BIG-IP LTM previous to v9.4, the **Configuration Guide for BIG-IP Local Traffic Management** for version 9.4 (available on AskF5) shows the configuration differences between the base TCP profile and the optimized profile types. Use the Configuration Guide to manually configure the optimization settings.*

Creating the WAN optimized TCP profile

First we configure the WAN optimized profile. Remember, if most users are accessing the portal via the LAN, use the base TCP profile instead of this WAN optimized profile.

To create a new TCP WAN optimized profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sap_tcp-wan**.
5. From the **Parent Profile** list, select **tcp-wan-optimized**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the LAN optimized TCP profile

Now we configure the LAN optimized profile. If you have already created a simple TCP profile, based off the default TCP profile (and not the WAN optimized profile above), you do not need to create another TCP profile, continue with the next procedure.

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sap_tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized** if you are using BIG-IP LTM version 9.4 or later; otherwise select **tcp**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

Creating a OneConnect profile

The next profile we create is a OneConnect profile. With OneConnect enabled, client requests can utilize existing, server-side connections, thus reducing the number of server-side connections that a server must open to service those requests. Testing has demonstrated that this can provide significant performance improvements for SAP implementations. For more information on OneConnect, see the BIG-IP LTM documentation.

In our example, we leave all the options at their default settings. You can configure these options as appropriate for your network.

To create a new OneConnect profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Other** menu, click **OneConnect**. The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sap_oneconnect**.
5. From the **Parent Profile** list, ensure that **oneconnect** is selected.
6. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

Creating persistence profiles

The final profiles we create are Persistence profiles. In this case, we create two persistence profiles; a default and a fallback persistence profile. Because we are using HTTP cookie insert persistence as our default mode, we need the fallback mode in case the user's device does not accept cookies.

Creating the Cookie Persistence profile

The first persistence profile we create is the Cookie Persistence profile. In this profile there are some optional settings you can configure, such as the method of cookie persistence and the expiration. In our experience, SAP expects persistence to be maintained for 8 hours. As a result, we set the time out value in this profile to 8 hours and 1 minute.

To create a new cookie persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.

-
2. On the Menu bar, click **Persistence**.
The Persistence Profiles screen opens.
 3. In the upper right portion of the screen, click the **Create** button.
The New Persistence Profile screen opens.
 4. In the **Name** box, type a name for this profile. In our example, we type **sap_cookie**.
 5. From the **Persistence Type** list, select **Cookie**.
The configuration options for cookie persistence appear.
Make sure the Parent Profile is set to **Cookie**.
 6. In the **Expiration** row, click a check in the Custom box. Clear the Session Cookie box, and the Expiration values appear. In the **Hours** box, type **8**, and in the **Minutes** box, type **1**.
 7. Modify any of the other settings as applicable for your network.
 8. Click the **Finished** button.

Creating the Fallback Persistence profile

Now we configure the fallback persistence profile. In our example, we use Source Address Affinity for the fallback persistence type.

To create a new fallback persistence profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
The HTTP Profiles screen opens.
2. On the Menu bar, click **Persistence**.
The Persistence Profiles screen opens.
3. In the upper right portion of the screen, click the **Create** button.
The New Persistence Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **sap_source**.
5. From the **Persistence Type** list, select **Source Address Affinity**.
The configuration options for Source Address Affinity persistence appear.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

Creating the virtual server

Next, we configure a virtual server that uses the profiles and pool you created in the preceding procedures.

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 **sap_portal_vs**.
4. In the **Destination** section, click the **Host** button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.21.15**.
6. In the **Service Port** box, type **80**.

Local Traffic >> Virtual Servers >> New Virtual Server...	
General Properties	
Name	sap_portal_vs
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network
	Address: 10.133.21.15
Service Port	80 HTTP
State	Enabled

Figure 6 Creating the new virtual server

7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. Leave the **Type** and **Protocol** lists at their default settings: **Standard** and **TCP**.
9. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **sap_tcp-wan**.
10. From the **Protocol Profile (Server)** list, select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **sap_tcp-lan**.
11. From the **OneConnect Profile** list, select **sap_oneconnect**.
12. From the HTTP Profile list, select the name of the profile you created in the *Creating an HTTP profile* section. In our example, we select **sap_http-opt** (see Figure 11).

Configuration: Advanced	
Type	Standard
Protocol	TCP
Protocol Profile (Client)	sap_tcp-wan
Protocol Profile (Server)	sap_tcp-lan
OneConnect Profile	sap_oneconnect
HTTP Profile	sap_http-opt
FTP Profile	None
SSL Profile (Client)	None

Figure 7 Selecting the profiles for the virtual server

13. In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **sap_portal**.
14. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating persistence profiles* section. In our example, we select **sap_cookie**.
15. From the **Fallback Persistence Profile** list, select the profile you created for the fallback persistence method in the *Creating persistence profiles* section. In our example, we select **sap_source**.

Resources	
iRules	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid gray; width: 40%; height: 40px;">Enabled</div> <div style="border: 1px solid gray; width: 40%; height: 40px;">Available</div> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> << >> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> Up Down </div>
HTTP Class Profiles	<div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid gray; width: 40%; height: 40px;">Enabled</div> <div style="border: 1px solid gray; width: 40%; height: 40px;">Available</div> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> << >> </div> <div style="display: flex; justify-content: center; margin-top: 5px;"> Up Down </div>
Default Pool	sap_portal
Default Persistence Profile	sap_cookie
Fallback Persistence Profile	sap_source
Cancel Repeat Finished	

Figure 8 Resources section of the add virtual server page

16. Click the **Finished** button. The BIG-IP LTM configuration for SAP Enterprise Portal is now complete.

Configuring the BIG-IP LTM system for the SAP ERP Central Component (ECC)

In this section, we configure the BIG-IP LTM system for directing traffic to one of the SAP application components called SAP ERP Central Component (ECC). As mentioned in the introduction, there are a large number of SAP application components available. This Deployment Guide covers the SAP ECC as an example component application. If you have other component applications, such as SAP Exchange Infrastructure, or Business Warehouse, repeat this entire section for each one, replacing names, IP addresses and ports as applicable. In this Deployment Guide, we are configuring high availability for internal services accessed over the Local Area Network.

Creating the TCP health monitor

For ECC, we create a simple TCP health monitor, based off the default TCP monitor. Although the monitor in the following example is quite simple, you can configure optional settings such as Send and Receive Strings to make the monitor much more specific. You can also use one of the other types of monitors available on the BIG-IP LTM system.

To configure a TCP health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
The Monitors screen opens.
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 **sap_tcp**.
4. From the **Type** list, select **TCP**.
The TCP Monitor configuration options appear.
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 an **Interval** of **30** and a **Timeout** of **91**.
6. In the Send String and Receive Rule sections, you can add an optional Send String and Receive Rule specific to the device being checked.
7. Click the **Finished** button.
The new monitor is added to the Monitor list.

Remember that if you configure a Send String and Receive String specific to one of the application components, you should create a new monitor for the other components.

Creating the pool

The next step is to create a pool on the BIG-IP LTM system for the application components. In our example, we create a pool containing the IP address and Port for the SAP ECC J2EE instances. For more information on these components, see the SAP documentation.

Our example is based on an Instance Number of 50. As a result, our TCP port for the application service is 55000. Other components will have different Instance Numbers, but you should find the required TCP ports to be in the form of 5NN00 for the HTTP application server traffic.

To create the Internet Connection Manager pool

1. On the Main tab, expand **Local Traffic**, and then click **Pools**. The Pool screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New Pool screen opens.
*Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.*
3. In the **Name** box, enter a name for your pool. In our example, we use **sap_ecc_55000**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the TCP health monitor* section, and click the Add (<<) button. In our example, we select **sap_tcp**.
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. In the New Members section, make sure the **New Address** option button is selected.
7. In the **Address** box, add the first server to the pool. In our example, we type **10.133.20.1**.
8. In the **Service Port** box, the appropriate port for this component. In our example, we type **5500**. If you modified this port for ECC in the SAP configuration, you need to use that port.
9. Click the **Add** button to add the member to the list.
10. Repeat steps 9-11 for each server you want to add to the pool. In our example, we repeat these steps once for **10.133.20.2** and **10.133.20.3**.
11. Click the **Finished** button.

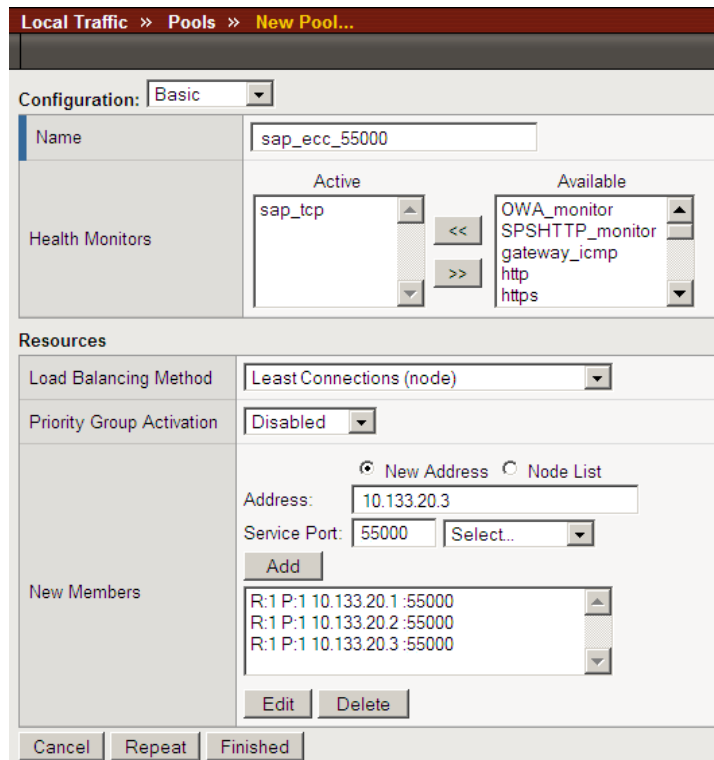


Figure 9 Creating the pool for the ECC devices

Creating the profiles

In our example, we use the same profiles for the ECC that we created for the SAP Portal in *Creating profiles*, on page 10, with the exception of the HTTP profile, and possibly the TCP profile.

If you need to change other BIG-IP profiles you created earlier for individual SAP application components, we recommend creating new profiles using the previous profiles as the parent.

Creating the HTTP profile

In this procedure, we create a new HTTP profile. If you are using the BIG-IP LTM system to offload SSL traffic, there are additional modifications to this profile you need to make. See *Creating the new HTTP profile*, on page 26

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.

-
2. In the upper right portion of the screen, click the **Create** button. The New HTTP Profile screen opens.
 3. In the **Name** box, type a name for this profile. In our example, we type **sap_http-ecc**.
 4. From the **Parent Profile** list, select **http**. The profile settings appear.
 5. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
 6. Click the **Finished** button.

Creating the TCP profile

Next is the TCP profile. In our example, we use the same LAN optimized TCP profile we configured for the Enterprise Portal (see *Creating the LAN optimized TCP profile*, on page 13). If there are specific settings you want to change for the particular component application, we recommend you configure a new TCP profile, based on the **tcp-lan-optimized** profile.

Creating the virtual server

Next, we configure a virtual server that reference the profiles and pool you created in the preceding procedures. In our testing with SAP, we found that persistence was not required for the application server connections. As a result, no persistence is configured for this virtual server. If you find that your implementation requires persistence, refer to the persistence and virtual server configuration for the Enterprise Portal servers discussed earlier in this guide.

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 **sap_ecc_55000**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.21.15**.
6. In the **Service Port** box, type **55000**. Note that this port should match the port number of the pool you created, so if you are using a different port for ECC, use this port here (see Figure 10).

General Properties	
Name	sap_ecc_55000
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.133.21.15
Service Port	55000 Other: [v]
State	Enabled [v]

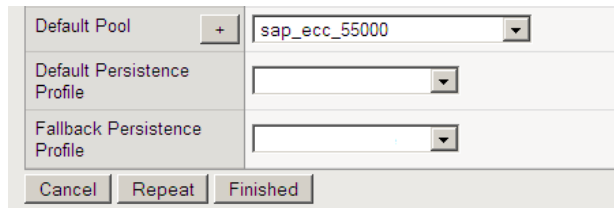
Figure 10 Creating the SAP ECC virtual server

7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. Leave the **Type** list at the default setting: **Standard**.
9. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **sap_tcp-lan**.
10. Leave the **Protocol Profile (Server)** option at the default setting, or you can select **sap_tcp-lan** from the list.
11. From the **OneConnect Profile** list, select **sap_oneconnect**.
12. 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 **sap_http-ecc** (see Figure 11).

Configuration: Advanced [v]	
Type	Standard [v]
Protocol	TCP [v]
Protocol Profile (Client)	sap_tcp-lan [v]
Protocol Profile (Server)	sap_tcp-lan [v]
OneConnect Profile	sap_oneconnect [v]
HTTP Profile	sap_http-ecc [v]
FTP Profile	None [v]
SSL Profile (Client)	None [v]

Figure 11 Selecting the profiles for the virtual server

-
- In the Resources section, from the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **sap_ecc_55000**.



Default Pool	+ sap_ecc_55000
Default Persistence Profile	
Fallback Persistence Profile	
Cancel Repeat Finished	

Figure 12 Resources section of the add virtual server page

- Click the **Finished** button.

Creating a default SNAT

This SNAT is in place to ensure that the inter-application traffic is routed back to the BIG-IP LTM system.

To create a default SNAT

- On the Main tab, expand **Local Traffic**, and then click **SNATs**. The SNATs screen opens.
- In the upper right portion of the screen, click the **Create** button. The New SNAT screen opens.
- In the **Name** box, type a name for this SNAT. In our example, we type **sapSNAT**.
- In the **Translation** list, select **Automap**. With Automap, the BIG-IP LTM system maps one or more client IP addresses using all system self IP addresses as the translation addresses. For more information on SNAT or SNAT Automap, see the BIG-IP LTM manuals.
- Optional:** If you to disable (or enable) the default SNAT for specific VLANs, from the VLAN Traffic list, select either **Enabled on** or **Disabled on** from the list. From the Available list, select the appropriate VLAN and click the Add (<<) button to move it to the Selected list.

- Click the **Finished** button.

Figure 13 Creating a Default SNAT

The configuration for the SAP ECC is now complete. Repeat this section for any additional SAP application components you may be using.

Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment

The BIG-IP LTM device can be configured as an SSL proxy, offloading the SSL duties from the servers. F5's testing, performed in conjunction with SAP, demonstrated significant increases in efficiency for the Enterprise Portal and component application servers when SSL processing was offloaded to the F5 BIG-IP LTM. If you want to use this functionality, you must complete the following procedures.

◆ Important

This section is optional, and only necessary if you are using the BIG-IP LTM system for offloading SSL.

Using SSL certificates and keys

Before you can enable the BIG-IP system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for SAP connections on the BIG-IP device. For this Deployment Guide, we assume that you already have obtained an SSL certificate, but it is not yet installed on the BIG-IP system. For information on generating certificates, or using

the BIG-IP system to generate a request for a new certificate and key from a certificate authority, see the Managing SSL Traffic chapter in the *Configuration Guide for Local Traffic Management*.

Importing keys and certificates

Once you have obtained a certificate, you can import this certificate into the BIG-IP system using the Configuration utility. By importing a certificate or archive into the Configuration utility, you ease the task of managing that certificate or archive. You can use the Import SSL Certificates and Keys screen only when the certificate you are importing is in Privacy Enhanced Mail (PEM) format.

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** list, select the type of import (**Key** or **Certificate**).
5. Select the import method (text or file).
6. Type the name of the key or certificate.
7. Click **Import**.

If you imported the certificate in the preceding procedure, repeat the entire procedure for the key.

Creating additional profiles

When using the BIG-IP LTM system to offload SSL traffic, you need to create two additional profiles. The first is a new Client SSL profile, and the second is a slightly modified HTTP profile that instructs the SAP server to respond with the appropriate content, and directs the BIG-IP LTM system to rewrite the URI in all HTTP redirect responses.

The following profiles can be created whether you are configuring the BIG-IP LTM for the Enterprise Portal or application component servers.

Creating a Client SSL profile

The first profile is the SSL profile. This profile contains the SSL certificate and Key information for offloading the SSL traffic.

To create a new Client SSL profile based on the default profile

1. On the Main tab, expand **Local Traffic**.

2. Click **Profiles**.
The HTTP Profiles screen opens.
3. On the Menu bar, from the **SSL** menu, select **Client**.
The Client SSL Profiles screen opens.
4. In the upper right portion of the screen, click the **Create** button.
The New Client SSL Profile screen opens.
5. In the **Name** box, type a name for this profile. In our example, we type **sap_clientssl**.
6. In the Configuration section, click a check in the **Certificate** and **Key Custom** boxes.
7. From the **Certificate** list, select the name of the Certificate you imported in the *Importing keys and certificates* section.
8. From the **Key** list, select the key you imported in the *Importing keys and certificates* section.
9. Click the **Finished** button.

For more information on creating or modifying profiles, or SSL Certificates, see the BIG-IP documentation.

Creating the new HTTP profile

The next profile is a new HTTP profile that contains the necessary client header, along with the rewrite/redirect setting. You must have an HTTP profile with the settings in the following procedure for each SAP virtual server that will be offloading SSL.

If you have already created an HTTP profile as described earlier in this guide, you can modify that profile with the modifications found in the following procedure.

To create a new HTTP profile for SSL

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
The HTTP Profiles screen opens.
2. In the upper right portion of the screen, click the **Create** button.
The New HTTP Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **sap_ssl**.
4. From the **Parent Profile** list, ensure that **HTTP** is selected.
5. In the **Request Header Insert** row, click a check in the Custom box. In the box, type: **clientprotocol: https**.
6. In the **Redirect Rewrite** row, click a check in the Custom box. From the list, select **Matching**.
7. *Optional for virtual servers requiring Cookie Persistence:* In the **Encrypt Cookies** row, click a check in the Custom box. Type the name of the cookies you want to encrypt, with a space between each

cookie. In our example, we type the name of the SAP cookie (**MYSAPSSO2** by default), and the BIG-IP cookie (**BIGipServer<Name_of_Pool>** by default, so in our example, **BIGipServersap_portal**).

You can either modify the Cookie Passphrase or leave it at the default. In our example, we leave it at the default level.

8. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
9. Click the **Finished** button (see Figure 14).

Figure 14 Creating the HTTP profile for SSL deployments

For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

Creating the Redirect iRule

The next step is to create an iRule that redirects all traffic to same hostname (stripping port if it exists), same URI over HTTPS. This iRule catches the traffic that incorrectly comes in on HTTP and redirects it to HTTPS. This ensures that SSL traffic remains on the virtual server that supports the traffic. The iRule will be applied to an HTTP Virtual Server where required.

To create the redirect iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**.
2. In the upper right portion of the screen, click the **Create** button. The New iRule screen opens.
3. In the **Name** box, enter a name for your iRule. In our example, we use **sap_httptohttps**.
4. In the Definition section, copy and paste the following iRule:

```
when HTTP_REQUEST {
  HTTP::redirect https://[getfield [HTTP::host] ":" 1][HTTP::uri]
}
```

5. Click the **Finished** button.

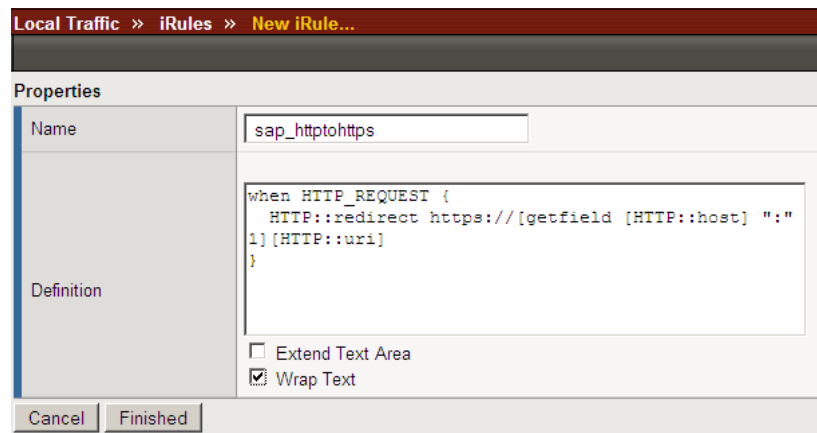


Figure 15 Creating the redirect iRule

The iRule is now complete. You use this iRule when you modify the existing SAP Enterprise Portal virtual server on port 80 in *Modifying the SAP Enterprise Portal virtual server*, on page 31.

Creating an HTTPS virtual server

The next step is to create a virtual server for the SSL offload that will use the Client SSL profile you just created. The example virtual server is for SAP Enterprise Portal. As a result, TCP WAN and LAN optimized profiles are used along with a Cookie Persistence profile. These settings would not necessarily apply if this were a virtual server dedicated to managing traffic between SAP application components.

To create a new HTTPS 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 **sap_erp_ssl**.
4. In the **Destination** section, select the **Host** option button.
5. In the **Address** box, type the IP address of this virtual server. In our example, we use **10.133.21.15**.
6. In the **Service Port** box, type **443**, or select **HTTPS** from the list.

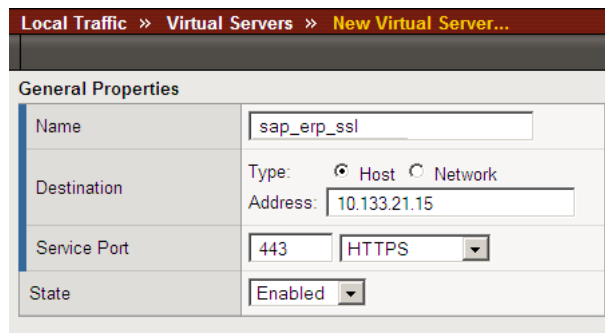


Figure 16 Creating the HTTPS virtual server

7. From the Configuration list, select **Advanced**.
The Advanced configuration options appear.
8. Leave the **Type** list at the default setting: **Standard**.
9. From the **Protocol Profile (Client)** list, select a tcp profile. If you are configuring this virtual server for Enterprise Portal, select the tcp profile you created in *Creating the WAN optimized TCP profile*. If this is for a component application, select the profile you created in *Creating the TCP profile*.
10. From the **Protocol Profile (Server)** select the profile you created in the *Creating the LAN optimized TCP profile* section. In our example, we select **sap_tcp-lan** from the list.
11. From the **OneConnect Profile** list, select **sap_oneconnect**.
12. From the **HTTP Profile** list, select the name of the profile you created in the *Creating the new HTTP profile* section. In our example, we select **sap_ssl**.

- From **SSL Profile (Client)** list, select the name of the profile you created in the *Creating a Client SSL profile* section. In our example we select **sap_clientssl** (see Figure 17).

The screenshot shows the configuration page for an HTTPS virtual server. The configuration mode is set to 'Advanced'. The following table represents the configuration options shown in the interface:

Configuration:	Advanced
Type	Standard
Protocol	TCP
Protocol Profile (Client)	sap_tcp-wan
Protocol Profile (Server)	sap_tcp-lan
OneConnect Profile	sap_oneconnect
HTTP Profile	sap_ssl
FTP Profile	None
SSL Profile (Client)	sap_clientssl
SSL Profile (Server)	None

Figure 17 Selecting the profiles for the HTTPS virtual server

- In the Resources section, from the **Default Pool** list, select the pool you created for your SAP Portal nodes in the *Creating the pool* section. In our example, we select **sap_portal**.
- From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating persistence profiles* section. In our example, we select **sap_cookie**.
- From the **Fallback Persistence Profile** list, select the profile you created for the fallback persistence method in the *Creating persistence profiles* section. In our example, we select **sap_source**.

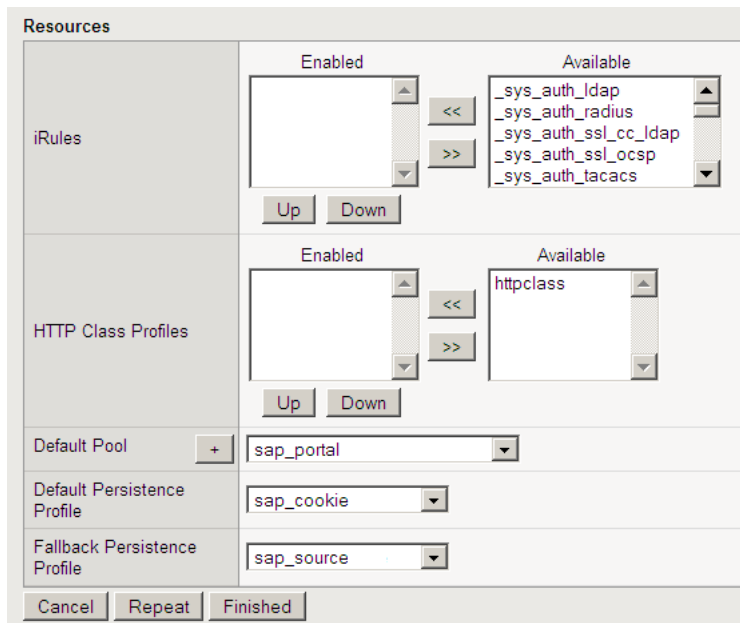


Figure 18 Resources section of the add virtual server page

17. Click the **Finished** button.

Modifying the SAP Enterprise Portal virtual server

In this procedure, we modify the portal virtual server on port 80 that you created to use the iRule instead of the pool. This iRule is in place to ensure that any accidental requests to port 80 are redirected to the SSL virtual server.

To modify the Enterprise Portal virtual server to use the iRule

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the list, click the virtual server you created in *Creating the virtual server*, on page 15. In our example, we click **sap_portal_vs**. The Virtual Server properties page opens.
3. On the Menu bar, click **Resources**.
4. In the iRules section, click the **Manage** button. The iRules Resource Management screen opens.
5. From the **Available** list, select the iRule you created in the *Creating the Redirect iRule* section, and click the Add (<<) button. In our example, we select **sap_httpstohttps**.

6. Click the **Finished** button.
You return to the Resources page.
7. From the Default Pool list, select **None**.
8. Click the **Update** button.

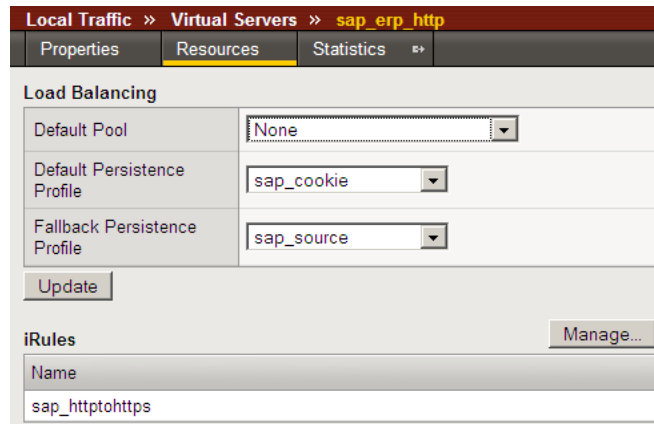


Figure 19 Modifying the virtual server to use the iRule and not the pool.

This concludes the steps necessary to use the BIG-IP LTM system to offload SSL traffic.

Appendix A: Backing up and restoring the BIG-IP system configuration

We recommend saving your BIG-IP configuration before you begin this configuration. When you save the BIG-IP configuration, it collects the following critical data and compress it into a single User Configuration Set (UCS) file:

- BIG-IP configuration files
- BIG-IP license and passwords
- SSL certificates
- SSH keys

Saving and restoring the BIG-IP configuration

The Configuration Management screen allows you to save and restore all configuration files that you may edit to configure a BIG-IP system. These configuration files are called a User Configuration Set (UCS). The Configuration Management screen contains sections for saving and restoring a configuration. The list boxes in these sections display only files in the `/usr/local/ucs` directory. If you want to save or restore files from another directory, you must type the full path in the box.

To save the BIG-IP configuration using the Configuration utility

1. In the navigation pane, click **System Admin**.
The User Administration screen displays.
2. Click the Configuration Management tab.
The Configuration Management screen displays.
3. In the **Save Current Configuration** section, type the path where you want your configuration file saved or choose a path from the list box. If no path is specified, the BIG-IP saves files to `/usr/local/ucs`. The BIG-IP appends the extension `.ucs` to file names without it. In our example, we type **pre_sap_backup.ucs**.
4. Click the **Save** button to save the configuration file.

To restore a BIG-IP configuration

1. In the navigation pane, click **System Admin**.
The User Administration screen displays.
2. Click the Configuration Management tab.
The Configuration Management screen displays.

3. In the **Restore a Configuration** section, choose the configuration file you want to restore from the list box, or type the path where your configuration files were saved.
4. Click the **Restore** button.
To check the status of the restoration, click the **View Log** button. You should wait a few moments for the log file to start generating before you click **View Log**. Repeated clicking of this button will update your screen with the most current log file information until the restoration is complete.