



# Deploying the BIG-IP System v10 with SAP NetWeaver and Enterprise SOA: ERP Central Component (ECC)

**Version 1.1**

# Table of Contents

## Deploying the BIG-IP system v10 with SAP ERP Central Component

Prerequisites and configuration notes .....	1-1
Product versions and revision history .....	1-2
Configuring the BIG-IP LTM system for SAP ECC .....	1-3
Running the SAP ECC application template .....	1-3
Adding an NTLM profile if using NTLM authentication .....	1-8
Creating a new monitor if not using HTTP .....	1-9
SSL Certificates on the BIG-IP system .....	1-11

## Manually configuring the BIG-IP LTM for SAP ECC

Creating the health monitor .....	2-1
Creating the pool .....	2-2
Creating the profiles .....	2-3
Creating the virtual server .....	2-7
Creating a default SNAT .....	2-9
Configuring the BIG-IP system for offloading SSL traffic from SAP ECC .....	2-11
Using SSL certificates and keys .....	2-11
Creating additional profiles .....	2-12
Creating the Redirect iRule .....	2-13
Creating an HTTPS virtual server .....	2-14
Modifying the SAP ECC virtual server .....	2-15

## Manually configuring the WebAccelerator for SAP ECC

Prerequisites and configuration notes .....	3-1
Configuration example .....	3-1
Configuring the WebAccelerator module .....	3-2
Creating an HTTP Class profile .....	3-2
Modifying the Virtual Server to use the Class profile .....	3-3
Creating an Application .....	3-4



I

---

---

## Deploying the BIG-IP System v10 with SAP NetWeaver and Enterprise SOA: ECC

---

---

- Running the SAP ECC application template
- Adding an NTLM profile if using NTLM authentication
- Creating a new monitor if not using HTTP
- SSL Certificates on the BIG-IP system

---

# Deploying the BIG-IP system v10 with SAP ERP Central Component

Welcome to the F5 deployment guide for SAP® NetWeaver and Enterprise SOA, the ERP Central Component (ECC). This guide gives you step-by-step procedures on how to configure the BIG-IP system v10 with SAP ECC deployments. By taking advantage of F5's Application Ready infrastructure for SAP deployments organizations can achieve a secure, fast and available network infrastructure that reduces the total cost of operation and increases ROI.

New in version 10.0 of the BIG-IP system are Application Ready Templates. These application templates ease the process of configuring the BIG-IP system. Instead of having to individually create each object that pertains to the type of application traffic you want the BIG-IP system to manage, you can run an application template. The application template automatically creates BIG-IP system objects that are customized for that application. These objects can be either local traffic objects, TMOS objects, or both.

To provide feedback on this deployment guide or other F5 solution documents, contact us at [solutionsfeedback@f5.com](mailto:solutionsfeedback@f5.com).

## Prerequisites and configuration notes

All of the procedures in this Deployment Guide are performed on the BIG-IP system. The following are prerequisites for this solution:

- ◆ We recommend using the latest version of SAP NetWeaver and mySAP Business Suite applications. Our testing environment included both SAP ERP 6.0 based on NetWeaver 7.0 and 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) now renamed to Process Integration (PI), Business Warehouse (BW), and SAP ERP Central Component (ECC).
- ◆ This document is written with the assumption that you are familiar with both F5 devices 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 F5 configuration. Consult the SAP documentation and your SAP administrator for this information.
- ◆ For this deployment guide, the BIG-IP LTM system must be running version 10.0 or later. If you are using a previous version of the BIG-IP LTM system see the *Deployment Guide* index.
- ◆ If you are using the BIG-IP system to offload SSL, we assume you have already obtained an SSL certificate and key, but it is not yet installed on the BIG-IP LTM system. For more information, see *SSL Certificates on the BIG-IP system*, on page 1-11.

- ◆ While we strongly recommend using the application template, you can also manually configure the BIG-IP system. For more information, see *Manually configuring the BIG-IP LTM for SAP ECC*, on page 2-1.

◆ **Important**

*All local traffic objects that an application template creates reside in administrative partition Common. Consequently, to use the application templates feature, including viewing the Templates list screen, you must have a user role assigned to your user account that allows you to view and manage objects in partition Common.*

## Product versions and revision history

Product and versions tested for this deployment guide:

Product Tested	Version Tested
BIG-IP System (LTM and WebAccelerator)	10.0
SAP ERP	6.0 (based on NetWeaver 7.0)
SAP NetWeaver	7.0 and NetWeaver 2004
mySAP ERP	2007

Revision history:

Document Version	Description
1.0	New deployment guide
1.1	Added a new section covering BIG-IP configuration for SAP deployments that use NTLM authentication. See <i>Adding an NTLM profile if using NTLM authentication</i> , on page 1-8.

---

# Configuring the BIG-IP LTM system for SAP ECC

You can use the new application template feature on the BIG-IP system, to efficiently configure a set of objects corresponding to SAP ECC. The template uses a set of wizard-like screens that query for information and then creates the required objects. At the end of the template configuration process, the system presents a list of the objects created and a description for how each object interacts with the application.

◆ **Note**

---

*Depending on which modules are licensed on your BIG-IP system, some of the options in the template may not appear.*

## Running the SAP ECC application template

Use the following procedure to guide you through the SAP ECC application template.

### To run the SAP ECC application template

1. Verify that your current administrative partition is set to **Common**. The Partition list is in the upper right corner.
2. On the Main tab, expand **Templates and Wizards**, and then click **Templates**. The Templates screen opens, displaying a list of templates.
3. In the Application column, click **SAP ERP Central Component**. The SAP ECC application template opens.
4. In the Template Questions section, you can type a unique prefix for your SAP ECC objects that the template will create. In our example, we leave this setting at the default, **my\_sap\_ecc**.
5. In the ECC - Virtual Server Questions section, complete the following:
  - a) Enter the IP address for this virtual server. The system creates a virtual server named **<prefix from step 4>\_virtual\_server**. In our example, we type **192.168.16.101**.
  - b) If the ECC servers can communicate with the clients using a route through the BIG-IP system to deliver response data to the client, select **Yes** from the list. In this case, the BIG-IP does **not** translate the client's source address.

If the BIG-IP system should translate the client's source address to an address configured on the BIG-IP system, leave the list at the default setting, **No**. Selecting **No** means the BIG-IP system will use SNAT automap. See the Online Help for more information.

In our example, we leave this at the default setting: **No**.

Figure 1.1 Running the SAP ECC application template

6. In the SSL Offload Questions section, complete the following:
  - a) If you are not using the BIG-IP system to offload SSL, leave this setting at the default, **No**. Continue with Step 6.

If you are using the BIG-IP system to offload SSL from the SAP Portal devices, select **Yes** from the list. The SSL options appear.

- b) From the **Certificate** list, select the appropriate certificate you want to use for this deployment. If you plan to use a third party certificate, but have not yet installed it on the BIG-IP system, see *SSL Certificates on the BIG-IP system*, on page 1-11.
- c) From the **Key** list, select the appropriate key for the certificate. If you have not yet installed the key on the BIG-IP system, see *SSL Certificates on the BIG-IP system*, on page 1-11.

For information on generating certificates, or using the BIG-IP LTM 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*.

Figure 1.2 Configuring the BIG-IP system for SSL Offload

- 
7. In the ECC Load Balancing Questions section, complete the following:
- a) From the Load Balancing Method list, select an appropriate load balancing method. In our example, we leave this setting at the default, **Least Connections (member)**.
  - b) Next, add each of the SAP ECC servers that are a part of this deployment.  
In the **Address** box, type the IP address of the first ECC server. In our example, we type **10.132.87.111**.  
In the **Service Port** box, leave the port at **50000**, unless you have modified the configuration on your SAP deployment.  
Click the **Add** button. Repeat this step for each of the SAP ECC devices.
  - c) Next, type a number of seconds that the BIG-IP system issues the health check. In our example, we leave this at the default level, **30**.  
Note that if you are using a ECC instance that does not use HTTP specification, you cannot use the monitor created by the template. See *Creating a new monitor if not using HTTP*, on page 1-9 for instructions on how to create the monitor.
  - d) If you have a specific HTTP request you would like to add to the health check, type it in the box after **GET /**. This is optional.
  - e) From the HTTP Version list, select **Version 1.1**. You should **not** use HTTP version 1.0 for SAP, as it will cause server issues.  
  
A new row appears asking for the fully qualified DNS name (FQDN) that clients use to access the SAP ECC. In the box, type the FQDN for your SAP ECC deployment. Note that this FQDN should resolve to the virtual server on the BIG-IP system. In our example, we type **saperp.siterequest.com**.
  - f) If you entered an HTTP request in step d, and want to enter a response string, type it here. This is optional.

See Figure 1.3.

**ECC - Load Balancing Questions**

Which load balancing method would you like to use?	Least Connections (member) ▼
Please add the servers that will comprise this virtual server (the virtual will not be available until at least one server is added):	Address: <input type="text" value="10.132.87.115"/> Service Port: <input type="text" value="55000"/> <input type="button" value="Select..."/> <input type="button" value="Add"/> <div style="border: 1px solid gray; padding: 2px; min-height: 20px;">                     R:1 P:1 10.132.87.113 :55000                      R:1 P:1 10.132.87.114 :55000                      R:1 P:1 10.132.87.115 :55000                 </div> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
How often should each SAP ERP Enterprise Central Component server's health be checked?	<input type="text" value="30"/> seconds
HTTP request that should be sent to check server health? (HTTP 1.1 headers will be automatically added.)	<input type="text" value="GET /"/>
What HTTP version do your SAP ERP Enterprise Central Component servers expect clients to use?	Version 1.0 ▼
String that should be contained within the health check response for the server to be considered healthy?	<input type="text"/>

*Figure 1.3 Configuring the Load Balancing options*

8. In the Protocol and Security Questions section, complete the following
  - a) If most clients will be connecting to the virtual server from a WAN, select **WAN** from the list. If most clients will be connecting from a LAN, select **LAN** from the list. This option determines the profile settings that control the behavior of a particular type of network traffic, such as HTTP connections.
  - b) If you want to use the WebAccelerator module to accelerate the SAP ECC traffic, select **Yes** from the list. If you do not want to use the WebAccelerator, select **No**. This option does not appear if you do not have the WebAccelerator module licensed. The WebAccelerator module can significantly improve performance for SAP deployments.
  - c) If you want to use the Application Security Manager to secure the SAP ECC traffic, select **Yes** from the list. If you do not want to use the Application Security Manager, select **No**. This option

does not appear if you do not have the Application Security Manager (ASM) licensed. For more information, see the online help or the BIG-IP ASM documentation.

- d) If you are using the Application Security Manager, from the Language Encoding list, select the appropriate language. In our example, we leave this at the default, **Unicode (utf-8)**.
- e) If you are using the WebAccelerator module, in the **Host** box, type the fully qualified DNS name (FQDN) that your users will use to access the SAP ECC deployment (the WebAccelerator application object's Requested Hosts field). Click the **Add** button. If you have additional host names, type each one in the **Host** box, followed by clicking the **Add** button. In our example, we type **saperp.siterequest.com** and click the **Add** button.

**ECC - Protocol Optimization and Security Questions**

Will clients be connecting to this virtual server primarily over a LAN or a WAN?	WAN
Would you like to use the Web Accelerator module to accelerate your SAP ERP Central Component traffic?	Yes
Would you like to use the Application Security Manager module to secure your SAP ERP Central Component traffic?	Yes
About ASM transparent mode:	Application Security Manager's policy enforcement mode will be set to transparent. In this mode, violations will be logged but not blocked. Before changing the mode to blocking, please review the log results and adjust the policy for your deployment if necessary.
What language encoding does your application use?	Unicode (utf-8)
Please enter the fully qualified DNS names your end users will use to access the SAP ERP Central Component Virtual Server (e.g., sap.f5.com).	Host: <input type="text" value="saperp.siterequest.com"/> Add <input type="text" value="saperp.siterequest.com"/> Delete

Cancel Finished

*Figure 1.4 Configuring the Optimization and Security settings*

9. Click the **Finished** button.

After clicking Finished, the BIG-IP system creates the relevant objects. You see a summary screen that contains a list of all the objects that were created.

## Adding an NTLM profile if using NTLM authentication

If you are using NTLM authentication, you need to add a NTLM profile on the BIG-IP system in order for the system to work properly with the OneConnect profile. First you create the NTLM profile, and then associate it with the virtual server created by the template.

### Creating the NTLM profile

Use the following procedure to create the NTLM profile.

#### To create the NTLM 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 **NTLM**. The NTLM Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **sap-NTLM**.
4. Complete any of the other settings as applicable for your configuration.
5. Click the **Finished** button.

### Modifying the virtual server to use the NTLM profile

Use the following procedure to associate the profile you just created with the virtual server(s) created by the template. If the BIG-IP system is offloading SSL, you perform this procedure for both the HTTP and HTTPS virtual servers.

#### To modify the virtual server to use the NTLM profile

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the list, find the (first) virtual server that was created by the template. This virtual server uses the preface you specified in Step 4 on page 1-3. In our example we select **my\_sap\_ecc\_virtual\_server**.
3. In the Configuration section, from the **NTLM Conn Pool** list, select the name of the NTLM profile you created in the preceding procedure. In our example, we select **sap-NTLM** (see Figure 1.5).
4. Click the **Update** button.
5. *Optional:* If you are offloading SSL from the ECC deployment, repeat this procedure for the HTTPS virtual server that was created by the template. In our example, we repeat the procedure for the **my\_sap\_ecc\_https\_virtual\_server**.

Configuration: <span>Advanced</span>	
Type	Standard
Protocol	TCP
Protocol Profile (Client)	my_sap_ecc_wan-optimized_tcp_profile
Protocol Profile (Server)	my_sap_ecc_lan-optimized_tcp_profile
OneConnect Profile	my_sap_ecc_one_connect_profile
NTLM Conn Pool	sap-NTLM

*Figure 1.5 Adding the NTLM profile to the virtual server*

## Creating a new monitor if not using HTTP

If you are using an ECC instance that does not use HTTP specification (such as a SOAP only server instance), you must create a TCP monitor and associate it with the pool. The application template creates an HTTP monitor that will not work in this case.

## Creating the TCP 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.

The next step is to associate the monitor with the pool that was created by the template.

## Modifying the pool to use the TCP monitor

Use the following procedure to associate the monitor you just created with the pool created by the template.

### To modify the pool to use the TCP monitor

1. On the Main tab, expand **Local Traffic**, and then click **Pools**.  
The Pools screen opens.
2. From the list, find the pool that was created by the template. This pool uses the preface you specified in Step 4 above. In our example we select **my\_sap\_ecc\_pool**.
3. In the Configuration section, from the Available list, select the name of the monitor you created in the preceding procedure, and click the Add (<<) button. In our example, we select **sap\_tcp**.
4. From the Active list, select the name of the monitor that was created by the template, and click the Remove (>>) button. In our example, we click **my\_sap\_ecc\_monitor** and click Remove.
5. Click the **Update** button.

This completes the modifications for the new health monitor.

---

## SSL Certificates on the BIG-IP system

Before you can enable the BIG-IP LTM system to act as an SSL proxy, you must install a SSL certificate on the virtual server that you wish to use for SAP ECC connections on the BIG-IP LTM 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 LTM system. For information on generating certificates, or using the BIG-IP LTM 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 LTM 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**. The list of existing certificates displays.
3. In the upper right corner of the screen, click **Import**.
4. From the **Import Type** list, select the type of import (Certificate or Key).
5. In the **Certificate** (or **Key**) **Name** box, type a unique name for the certificate or key.
6. In the **Certificate** (or **Key**) **Source** box, choose to either upload the file or paste the text.
7. Click **Import**.

If you imported the certificate, repeat this procedure for the key.



# 2

---

---

## Manually Configuring the BIG-IP LTM with SAP ECC

---

---

- Creating the health monitor
- Creating the pool
- Creating the profiles
- Creating the virtual server
- Creating a default SNAT
- Configuring the BIG-IP LTM system for offloading SSL traffic from the SAP Deployment

---

# Manually configuring the BIG-IP LTM for SAP ECC

While we recommend using the application template, if you prefer to manually configure the BIG-IP LTM system, perform the following procedures.

## Creating the health monitor

For ECC, we configure a simple health monitor. In our example, we create an HTTP monitor. However, if you are using an ECC instance that does not use HTTP specification, please use the TCP monitor type instead.

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 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.  
As noted above, if you are using an ECC instance that does not use HTTP, choose **tcp** from the list.
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.

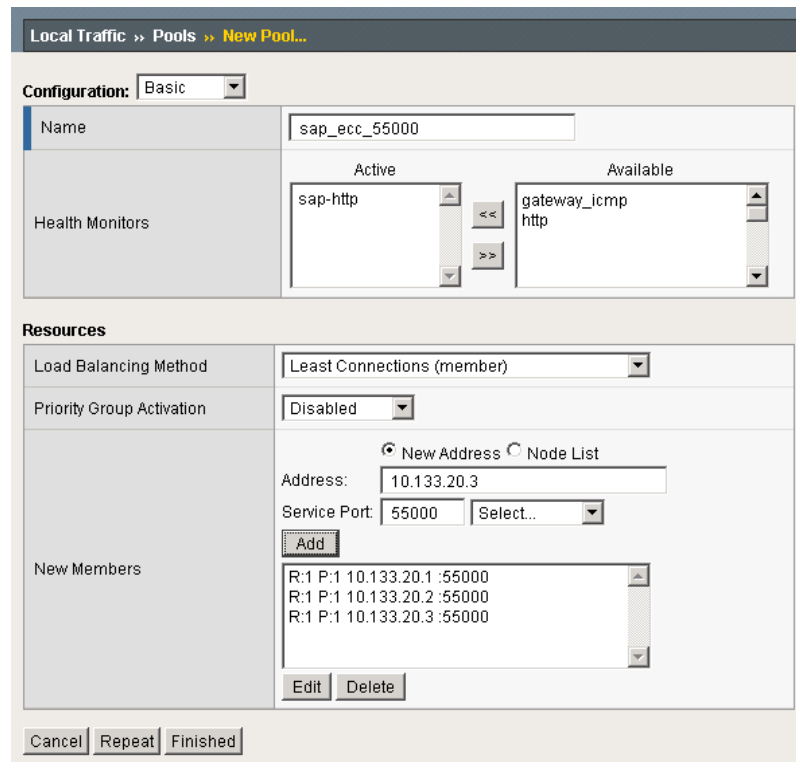
## Creating the pool

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 ECC 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 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 (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 **55000**. 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 2.1* Creating the pool for the ECC devices

## Creating the profiles

The BIG-IP system uses profiles to make configuration easier. 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.

## Creating the HTTP profile

In this procedure, we create an HTTP profile. The HTTP profile contains numerous configuration options for how the BIG-IP LTM system handles HTTP traffic. In the following example, we base our HTTP profile off of the

**http-acceleration** parent profile, as we are using the WebAccelerator. If you are not using the WebAccelerator, we recommend using the **http-wan-optimized-compression-caching** parent.

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 2-12.

### 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.
3. In the **Name** box, type a name for this profile. In our example, we type **ecc\_http-opt**.
4. From the **Parent Profile** list, select **http-acceleration** if you are using the WebAccelerator. If you are not using the WebAccelerator, select **http-wan-optimized-compression-caching**.
5. Check the Custom box for **Content Compression**, and leave **Content List** 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.

## 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 **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.

### 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.

- 
4. In the **Name** box, type a name for this profile. In our example, we type **ecc\_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 **ecc\_tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-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 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 **ecc\_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 an NTLM profile if using NTLM authentication

If you are using NTLM authentication, you need to add a NTLM profile on the BIG-IP system in order for the system to work properly with the OneConnect profile. This is only necessary if you are using NTLM.

### To create the NTLM 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 **NTLM**. The NTLM Profile screen opens.
3. In the **Name** box, type a name for this profile. In our example, we type **sap-NTLM**.
4. Complete any of the other settings as applicable for your configuration.
5. Click the **Finished** button.

## Creating persistence profiles (optional)

The final profiles we create are persistence profiles. Configuring persistence on the BIG-IP system is optional, and depends on the type of ECC instance you are installing. In our example, we create two persistence profiles; a default and a fallback persistence profile (these profiles are also created by the application template). 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**.
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 **ecc\_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 **ecc\_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.

### Creating the virtual server

Next, we configure a virtual server that reference 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\_ecc**.
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 the appropriate port. In our example, we type **80** (see Figure 2.2).

General Properties	
Name	sap-ecc
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network
	Address: 10.133.21.15
Service Port	80 HTTP
State	Enabled

**Figure 2.2** 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 WAN optimized TCP profile* section. In our example, we select **ecc\_tcp-wan**.
10. From the **Protocol Profile (Server)** list, select the profile you created in *Creating the LAN optimized TCP profile*. In our example, we select **ecc\_tcp-lan**.
11. From the **OneConnect Profile** list, select **ecc\_oneconnect**.
12. *Optional:* If you are using NTLM authentication, from the **NTLM Conn Pool** list, select the profile you created in *Creating an NTLM profile if using NTLM authentication*. In our example, we are not using NTLM authentication, so we leave this at the default setting.

- 
- 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 2.3).

The screenshot shows a configuration window titled "Configuration: Advanced". It contains several rows of settings, each with a label and a dropdown menu:

Type	Standard
Protocol	TCP
Protocol Profile (Client)	ecc_tcp-wan
Protocol Profile (Server)	ecc_tcp-lan
OneConnect Profile	ecc-oneconnect
NTLM Conn Pool	None
HTTP Profile	ecc_http-opt
FTP Profile	None

**Figure 2.3** 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**.
- If you created the persistence profiles, from the **Default Persistence Profile** list, select the profile you created in *Creating the Cookie Persistence profile*. In our example, we select **ecc\_cookie**.

From the Fallback Persistence Profile list, select the profile you created in *Creating the Fallback Persistence profile*. In our example, we select **ecc\_source**.

The screenshot shows the "Resources" section of a configuration page. It includes a "Default Pool" dropdown set to "sap\_ecc\_55000", a "Default Persistence Profile" dropdown set to "ecc\_cookie", and a "Fallback Persistence Profile" dropdown set to "ecc\_source". At the top right are "Up" and "Down" buttons. At the bottom are "Cancel", "Repeat", and "Finished" buttons.

**Figure 2.4** 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

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**. The SNATs screen opens.
2. In the upper right portion of the screen, click the **Create** button. The New SNAT screen opens.
3. In the **Name** box, type a name for this SNAT. In our example, we type **sapSNAT**.
4. 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.
5. **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.
6. Click the **Finished** button.

The screenshot shows the 'New SNAT...' configuration window. The breadcrumb navigation at the top reads 'Local Traffic >> SNATs >> New SNAT...'. The window is divided into two main sections: 'General Properties' and 'Configuration'. In the 'General Properties' section, the 'Name' field is populated with 'sapSNAT'. In the 'Configuration' section, there are three dropdown menus: 'Translation' is set to 'Automap', 'Origin' is set to 'All Addresses', and 'VLAN Traffic' is set to 'All VLANs'. At the bottom of the window, there are three buttons: 'Cancel', 'Repeat', and 'Finished'.

*Figure 2.5 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.

### 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.
3. In the **Name** box, type a name for this profile. In our example, we type **sap\_ssl**.
4. From the **Parent Profile** list, select **http-acceleration** if you are using the WebAccelerator. If you are not using the WebAccelerator, select **http-wan-optimized-compression-caching**.
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. Modify any of the other settings as applicable for your network. In our example, we leave the settings at their default levels.
8. Click the **Finished** button.

## 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.

The iRule is now complete. You use this iRule when you modify the existing SAP ERP ECC virtual server on port 80 in *Modifying the SAP ECC virtual server*, on page 2-15.

## 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. 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\_ecc\_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.
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 profile you created in the *Creating the WAN optimized TCP profile* section. In our example, we select **ecc\_tcp-wan** from the list.
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 **ecc\_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**.
13. 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**.
14. 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\_ecc\_55000**.

- 
15. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating persistence profiles (optional)* section. In our example, we select **ecc\_cookie**.
  16. From the **Fallback Persistence Profile** list, select the profile you created for the fallback persistence method in the *Creating persistence profiles (optional)* section. In our example, we select **ecc\_source**.
  17. Click the **Finished** button.

## Modifying the SAP ECC virtual server

In this procedure, we modify the portal virtual server on port 80 that you created in the *Creating the pool*, on page 2, 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 ECC 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 2-7. In our example, we click **sap\_ecc**. 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.

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



# 3

---

---

## Manually Configuring the BIG-IP LTM with SAP ECC

---

---

- Creating an HTTP Class profile
- Modifying the Virtual Server to use the Class profile
- Creating an Application

---

# Manually configuring the WebAccelerator for SAP ECC

In this chapter, we show how to manually configure the WebAccelerator module for the SAP ECC devices to increase performance for end users. The F5 WebAccelerator is an advanced web application delivery solution that provides a series of intelligent technologies designed to overcome problems with browsers, web application platforms and WAN latency issues which impact user performance.

For more information on the F5 WebAccelerator, see <http://www.f5.com/products/WebAccelerator/>.

## Prerequisites and configuration notes

The following are prerequisites for this section:

- ◆ We assume that you have already configured the BIG-IP LTM system for directing traffic to the SAP deployment as described in this Deployment Guide.
- ◆ You must have purchased and licensed the WebAccelerator module on the BIG-IP LTM system.
- ◆ You must have created an HTTP profile on the BIG-IP LTM system that has RAM Cache enabled. In our example (*Creating the HTTP profile*, on page 2-3) we use a parent profile that includes RAM Cache. If you did not create an HTTP profile with RAM Cache enabled, you must create a new HTTP profile, based on the HTTP Acceleration parent and associate it with the virtual server.
- ◆ This document is written with the assumption that you are familiar with the BIG-IP LTM system, WebAccelerator and SAP ECC. Consult the appropriate documentation for detailed information.

## Configuration example

Using the configuration in this section, the BIG-IP LTM system with WebAccelerator module is optimally configured to accelerate traffic to SAP ECC servers. The BIG-IP LTM with WebAccelerator module both increases end user performance as well as offloads the servers from serving repetitive and duplicate content.

In this configuration, a remote client with WAN latency logs onto the SAP ECC via the WebAccelerator. The user's request is accelerated on repeat visits by the WebAccelerator instructing the browser to use the dynamic or static object that is stored in its local cache. Additionally, dynamic and static objects are cached at the WebAccelerator so that they can be served quickly without requiring the server to re-serve the same objects.

## Configuring the WebAccelerator module

Configuring the WebAccelerator module requires creating an HTTP class profile and creating an Application. The WebAccelerator device has a large number of other features and options for fine tuning performance gains, see the *WebAccelerator Administrator Guide* for more information.

### Creating an HTTP Class profile

The first procedure is to create an HTTP class profile. When incoming HTTP traffic matches the criteria you specify in the WebAccelerator class, the system diverts the traffic through this class. In the following example, we create a new HTTP class profile, based on the default profile.

#### To create a new HTTP class profile

1. On the Main tab, expand **WebAccelerator**, and then click **Classes**. The HTTP Class Profiles screen opens.
2. Click the **Create** button.
3. In the **Name** box, type a name for this Class. In our example, we type **SAP\_class**.
4. From the Parent Profile list, make sure **httpclass** is selected.
5. In the Configuration section, from the **WebAccelerator** row, make sure **Enabled** is selected.
6. In the Hosts row, click the Custom box, and then from the list select **Match Only**. The Host List options appear.
  - a) In the **Host** box, type the host name that your end users use to access the SAP Enterprise Portal. In our example, we type **saperp.siterequest.com** (see Figure 3.1).
  - b) Leave the Entry Type at **Pattern String**.
  - c) Click the **Add** button.
  - d) Repeat these sub-steps for any other host names users might use to access the SAP deployment.
7. The rest of the settings are optional, configure them as applicable for your deployment.
8. Click the **Finished** button. The new HTTP class is added to the list.

Local Traffic » Profiles : Protocol : HTTP Class » New HTTP Class Profile...

General Properties	
Name	SAP_class
Parent Profile	httpclass

Configuration		Custom <input type="checkbox"/>
WebAccelerator	Enabled	<input checked="" type="checkbox"/>
Application Security	Disabled	<input type="checkbox"/>
Hosts	Match only...	<input checked="" type="checkbox"/>
Host List	Host: saperp.siterequest.com	
	Entry Type: Pattern String	
	<input type="button" value="Add"/>	
	<input type="button" value="Delete"/>	
URI Paths	Match all	<input type="checkbox"/>
Headers	Match all	<input type="checkbox"/>
Cookies	Match all	<input type="checkbox"/>

Actions		Custom <input type="checkbox"/>
Send To	None	<input type="checkbox"/>
Rewrite URI		<input type="checkbox"/>

Figure 3.1 Creating a new HTTP Class profile

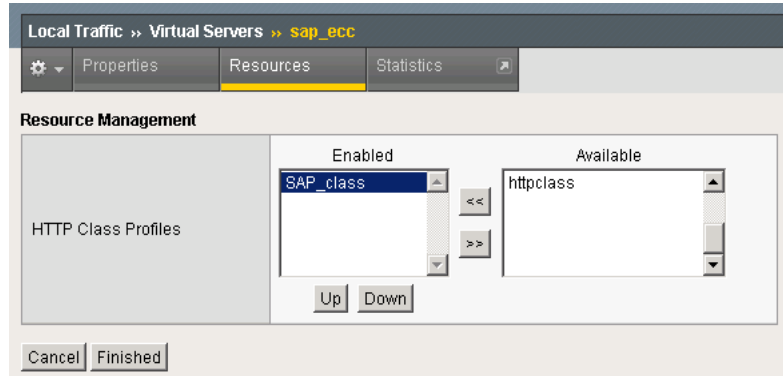
## Modifying the Virtual Server to use the Class profile

The next step is to modify the virtual server for your SAP deployment on the BIG-IP LTM system to use the HTTP Class profile you just created.

### To modify the Virtual Server to use the Class profile

1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. The Virtual Servers screen opens.
2. From the **Virtual Server** list, click the name of the virtual server you created for the SAP ECC in *Creating the virtual server*, on page 2-7. In our example, we click **sap\_ecc**.  
The General Properties screen for the Virtual Server opens.
3. On the Menu bar, click **Resources**.  
The Resources screen for the Virtual Server opens.
4. In the HTTP Class Profiles section, click the **Manage** button.

5. From the **Available** list, select the name of the HTTP Class Profile you created in the preceding procedure, and click the Add (<<) button to move it to the Enabled box. In our example, we select **SAP\_class** (see Figure 3.2).
6. Click the **Finished** button. The HTTP Class Profile is now associated with the Virtual Server.



**Figure 3.2** Adding the HTTP Class Profile to the Virtual Server

#### ◆ Important

*You must have created an HTTP profile on the BIG-IP LTM system that has RAM Cache enabled. In our example (Creating the HTTP profile, on page 2-3) we use a parent profile that includes RAM Cache. If you did not create an HTTP profile with RAM Cache enabled, you must create a new HTTP profile, based on a parent profile that uses RAM Cache (such as HTTP Acceleration), and modify the virtual server to use this new profile.*

*To create the HTTP profile, use Creating the HTTP profile, on page 2-3, selecting the HTTP Acceleration parent profile. You must leave RAM Cache enabled; all other settings are optional. To modify the virtual server, follow Steps 1 and 2 from the preceding procedure to access the virtual server, and then from the HTTP Profile list, select the name of the new profile you just created and click **Update**.*

## Creating an Application

The next procedure is to create a WebAccelerator Application. The Application provides key information to the WebAccelerator so that it can handle requests to your application appropriately.

---

## To create a new Application

1. On the Main tab, expand **WebAccelerator**, and then click **Applications**.  
The Application screen of the WebAccelerator UI opens in a new window.
2. Click the **Create** button.
3. In the Application Name box, type a name for your application.  
In our example, we type **SAP ECC**.
4. In the **Description** box, you can optionally type a description for this application.
5. From the **Central Policies** list, select **SAP Portal** (see Figure 3.3).
6. If you are deploying WebAccelerator in a symmetrical deployment, from the **Remote Policy** list, select **SAP Portal**.  
If you not deploying a remote unit, leave this option unselected.
7. In the **Requested Host** box, type the host name that your end users use to access the SAP deployment. This should be the same host name you used in Step 6a in the preceding procedure. In our example, we type **saperp.siterequest.com**  
If you have additional host names, click the **Add Host** button and enter the host name(s). See Figure 3.3.
8. Click the **Save** button.

The screenshot shows the 'New Application' configuration page in the WebAccelerator UI. The breadcrumb navigation at the top reads 'Configuration >> Applications >> New Application'. The page is divided into three main sections: 'General Options', 'Policies', and 'Hosts'.  
- **General Options:** The 'Application Name' field contains 'SAP ECC'. The 'Description (optional)' field contains 'WebAccelerator class for our SAP ERP Central Component deployment'.  
- **Policies:** The 'Central Policy' dropdown is set to 'SAP Portal'. The 'Remote Policy' dropdown is set to '- Select One -'.  
- **Hosts:** A table with two columns: 'Requested Host' and 'Action'. The 'Requested Host' column contains 'saperp.siterequest.com'. The 'Action' column contains 'Options' and 'Delete' links.  
At the bottom right of the form, there are three buttons: 'Add Host', 'Save' (highlighted in yellow), and 'Cancel'.

*Figure 3.3* Configuring an Application on the WebAccelerator (not a symmetrical deployment)

The rest of the configuration options on the WebAccelerator are optional, configure these as applicable for your network. With this base configuration, your end users will notice an marked improvement in performance after their first visit.