



Deploying the BIG-IP LTM v9.x with
Microsoft Office Communications
Server 2007



Microsoft[®] Partner

Introducing the BIG-IP and Office Communications Server 2007 configuration

Microsoft® and F5 have collaborated on a highly effective way to intelligently direct traffic for Microsoft Office Communications Server 2007 with the F5 BIG-IP® application traffic management device. Microsoft and F5 Networks have conducted interoperability testing between the BIG-IP LTM system and Office Communications Server 2007. Organizations using the BIG-IP LTM system benefit from mission-critical availability, intelligent traffic management, simple scalability, and enhanced security for Office Communications Server deployments.

Office Communications Server 2007 manages all real-time (synchronous) communications including: instant messaging, VoIP, audio and video conferencing. It works with existing tele-communications systems, so business can deploy advanced VoIP and conferencing without tearing out their legacy phone networks.

Microsoft Office Communications Server 2007 also powers presence, a key benefit of Microsoft unified communications that unites all the contact information stored in Active Directory with the ways people communicate. With presence, you can see at-a-glance if someone is available and contact them with a click using instant messaging, a phone call or a video conference.

For more information on Microsoft Office Communications Server, see <http://www.microsoft.com/uc/products/ocs2007.mspx>.

For more information on the BIG-IP LTM system, see <http://www.f5.com/products/big-ip/product-modules/local-traffic-manager.html>

Prerequisites and configuration notes

The following are prerequisites for this deployment:

- ◆ The BIG-IP LTM system must be running version v9.0 or later. We highly recommend using version 9.4 or later.
- ◆ You must be running Microsoft Office Communications Server 2007. For deployment guidance for Microsoft Live Communications Server 2005 Enterprise Edition for BIG-IP versions 4.5 and 9.0, see the **F5 Solution Center**.

◆ Note

This document is written with the assumption that you are familiar with both the BIG-IP LTM system and the Office Communications Server 2007. For more information on configuring these products, consult the appropriate documentation.

Configuration example

The BIG-IP LTM system can be used to add high availability and traffic direction to an Office Communication Server 2007 Enterprise Pool. Additionally, the BIG-IP LTM system provides required SNAT functionality to enable inter-server communication within the pool.

The following example shows a typical configuration with a BIG-IP LTM system and an Office Communications Server deployment. With multiple Office Communications Servers in a pool there is a need for distributing the incoming session requests among the servers. Figure 1 shows how a BIG-IP device is located in front of a pool of Office Communications Servers.

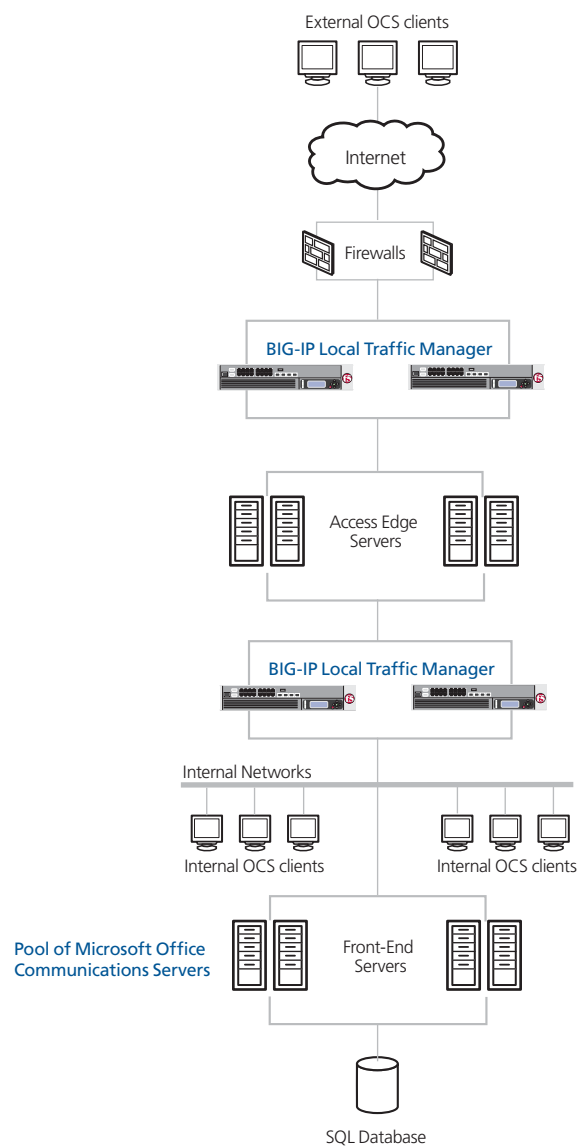


Figure 1 BIG-IP LTM - Microsoft Office Communications Server logical configuration

Configuring the BIG-IP LTM for Microsoft Office Communications Server 2007

This deployment guide is broken up into the following sections:

- *Performing the initial configuration tasks*, on page 3
- *Configuring the BIG-IP LTM for OCS Front-end servers*, on page 6
- *Configuring the BIG-IP LTM for OCS Edge servers*, on page 22

◆ 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 32.*

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 LTM system using the BIG-IP Configuration utility only. Unless you are familiar with using the **bigpipe** command line interface, we recommend using the Configuration utility.

Performing the initial configuration tasks

The following configuration includes creating VLANs and a Self IP on the BIG-IP LTM system. If you already have these objects configured on the BIG-IP LTM, you do not need to repeat these procedures. Continue with *Configuring the BIG-IP LTM for OCS Front-end servers*, on page 6.

Connecting to the BIG-IP device

The first step in this configuration is to connect to the BIG-IP LTM system. You can connect to the BIG-IP LTM system using the Configuration utility. You can also connect to the BIG-IP LTM system using the command line, however this Deployment Guide only contains configuration procedures from the Configuration utility.

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

To connect to the BIG-IP LTM 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 LTM system, the Welcome screen of the new Configuration utility opens. From the Configuration utility, you can configure and monitor the BIG-IP LTM system, as well as access online help, download SNMP MIBs and Plug-ins, and even search for specific objects.

Creating a VLAN

The first procedure in this deployment is to create a VLAN on the BIG-IP LTM system. The next step in this configuration is to create a VLAN on the BIG-IP LTM system. Depending on the desired network architecture, you may have one or multiple VLANs associated with the BIG-IP LTM configuration:

◆ One armed configuration

When the Communicator 2007 clients reside on the same network as the Office Communications Server Front End servers, you will only need one VLAN. This is also known as a one armed configuration.

Note: In deployments with more than 65,000 simultaneous connections, you need to configure more than one SNAT address on the BIG-IP LTM. See *Creating a SNAT*, on page 13.

◆ Routed configuration

A more common example is when the Communicator 2007 clients reside on a different network than the Office Communications Server Front Ends. In this case, you will need an external VLAN for the incoming clients, and an internal VLAN for the Office Communications Server Front End servers. This is known as a routed configuration.

To create a VLAN

1. On the Main tab, expand **Network**, and then click **VLANs**.
The VLANs screen opens.
2. Click the **Create** button.
The new VLAN screen opens.
3. In the **Name** box, type a unique name for the VLAN. In our example we use **ocs-vlan**.

4. In the **Resources** section, from the available list, select the interface that will have access to tagged traffic, and add it to the **Untagged** box by clicking the Add (<<) button. In our example, we select **1.14**. See Figure 2.
5. Click the **Finished** button.

The screenshot shows the 'Network > VLANs' configuration page. Under 'General Properties', the 'Name' field contains 'ocs-vlan' and the 'Tag' field is empty. The 'Resources' section is divided into three columns: 'Untagged', 'Available', and 'Tagged'. The 'Untagged' column contains '1.4'. The 'Available' column contains '1.1', '1.2', '1.3', '2.1', and '2.2'. There are '<<' and '>>' buttons between the columns. The 'Configuration' section has a dropdown set to 'Basic', a 'Source Check' checkbox that is unchecked, and an 'MTU' field with '1500'. At the bottom are 'Cancel', 'Repeat', and 'Finished' buttons.

Figure 2 Adding a VLAN in the BIG-IP LTM Configuration utility

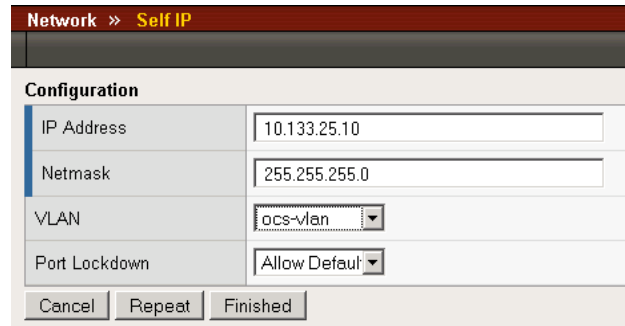
Creating a self IP

Self IP addresses are the IP addresses owned by the BIG-IP LTM system that you use to access the internal and external VLANs. The next step in this configuration is to create a self IP address for the VLAN we created in the preceding procedure.

To create a self IP address using the Configuration utility

1. On the Main tab, expand **Network**, and then click **Self IPs**. The Self IP screen opens.
2. Click the **Create** button. The new Self IP screen opens.
3. In the **IP Address** box, type a static IP address in the VLAN you created in the preceding procedure. Note that this needs to be on the same network as the Office Communications Server devices. In our example, we use **10.133.35.10**.
4. In the **Netmask** box, type the corresponding subnet mask. In our example, we use **255.255.255.0**.
5. From the **VLAN** list, select the VLAN you created in the *Creating a VLAN* procedure. In our example, we select **ocs-vlan**.

6. Click the **Finished** button.
The new self IP address appears in the list.



Configuration	
IP Address	10.133.25.10
Netmask	255.255.255.0
VLAN	ocs-vlan
Port Lockdown	Allow Default

Cancel Repeat Finished

Figure 3 Adding a self IP address in the BIG-IP Configuration utility

Configuring the BIG-IP LTM for OCS Front-end servers

In the following procedures, we configure the BIG-IP LTM for the Office Communications Server Front-End servers. A Front-End server is an Office Communications Server 2007 server in the internal network that hosts the IM Conferencing Service, Address Book Service, and Telephony Conferencing Service to support registration, presence, IM, and conferencing.

For the OCS Front-end servers, you must complete the following sections:

- *Configuring the BIG-IP LTM for HTTPS/SSL (444) traffic on the OCS Front-End servers*
- *Configuring the BIG-IP LTM for SIP traffic on the OCS Front-end servers*
- *Creating a wildcard virtual server*
- *Synchronizing the BIG-IP configuration if using a redundant system*

Configuring the BIG-IP LTM for HTTPS/SSL (444) traffic on the OCS Front-End servers

Microsoft OCS clients require HTTPS communication with Front-End servers on custom port 444. Using the BIG-IP LTM to direct traffic to a pool of Front-End servers provides load distribution, high availability, and increased scalability.

Creating a health monitor

The first step in configuring the BIG-IP LTM for the Front-end servers is to configure a health monitor on the BIG-IP LTM system. We use the **HTTPS** parent monitor to create this monitor. We configure this monitor to specifically check port **444**.

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 **ocs-fe-https**.
4. From the **Type** list, select **HTTPS**.
The HTTPS Monitor configuration options appear.
5. From the Configuration list, select **Advanced**.
The advanced configuration options appear.
6. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout. In our example, we use a **Interval of 30** and a **Timeout of 91**.
7. In the **Alias Service Port** box, type **444**.
8. All other configuration settings are optional, configure as applicable for your deployment.
9. Click the **Finished** button (see Figure 4).

Local Traffic >> Monitors >> New Monitor...

General Properties

Name: ocs-fe-https

Type: HTTPS

Import Settings: https

Configuration: Advanced

Interval: 30 seconds

Timeout: 91 seconds

Manual Resume: Yes No

Send String: GET /

Receive String:

Cipher List: DEFAULT:+SHA:+3DES:+kEDH

User Name:

Password:

Compatibility: Enabled

Client Certificate:

Reverse: Yes No

Alias Address: * All Addresses

Alias Service Port: 444 * All Ports

Cancel Repeat Finished

Figure 4 Configuring the Front-end health monitor

Creating the Front-End SSL pool

The next step is to create a pool on the BIG-IP LTM system for the Office Communications Server Front-End servers. A BIG-IP LTM pool is a set of devices grouped together to receive traffic according to a load balancing method.

Creating the Front-end SSL 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.
3. From the **Configuration** list, select **Advanced**. The advanced configuration options appear.

-
4. In the **Name** box, enter a name for your pool.
In our example, we use **ocs-frontend-ssl**.
 5. In the **Health Monitors** section, select the name of the monitor you created in the *Creating a health monitor* section, and click the Add (<<) button. In our example, we select **ocs-fe-https**.
 6. Complete the rest of the Configuration section as applicable for your deployment.
 7. In the Resources section, from the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
For this configuration, we recommend selecting **Least Connections (node)**. In Least Connections mode, the BIG-IP LTM system passes a new connection to the node that has the least number of current connections. Least Connections mode works best in environments where the servers or other equipment you are load balancing have similar capabilities. With Office Communications Server, traffic from servers to clients is roughly the same on each connection.
 8. In the **New Members** section, you add the Office Communications Front-End servers to the pool.
 - a) In the **Address** box, type the IP address of the Office Communications Server. In our example, we type **10.133.35.21**.
 - b) In the **Service Port** box, type the service number you want to use for this device. In our example, we type **444**.
 - c) Click the **Add** button to add the member to the list.
 - d) Repeat steps a-c for each Office Communications Server you want to add to the pool. In our example, we repeat these steps for the other two Front-End servers (**10.133.35.22** and **10.133.35.23**).
 9. Click the **Finished** button (see Figure 5).

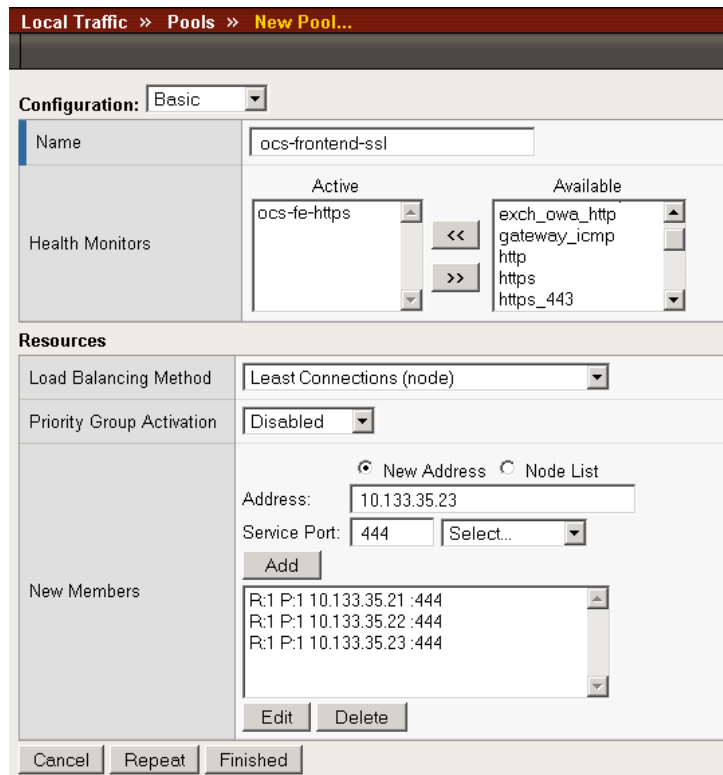


Figure 5 Creating the OCS Front-end pool

Creating the TCP profile

The next step is to create a TCP profile. For this TCP profile, we set the Idle Timeout value to 1200 seconds (20 minutes). If a connection is completely idle for this period, the BIG-IP LTM system will reset the connection. We set the Idle Timeout value higher than the default setting because it is important to allow connections to remain open and idle for longer time periods, as this is normal behavior of OCS clients.

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.
The HTTP Profiles screen opens.
3. On the Menu bar, from the **Protocol** menu, select **TCP**.
4. In the upper right portion of the screen, click the **Create** button.
The New TCP Profile screen opens.
5. In the **Name** box, type a name. In our example, we type **ocs-fe-ssl**.

6. In the **Idle Timeout** row, check the **Custom** box. In the seconds box, type **1200**.
7. Modify the rest of the settings as applicable for your network. The default settings should suffice for most networks.
8. Click the **Finished** button.

Figure 6 Creating a new TCP profile

Creating the virtual server

A virtual server with its virtual address is the visible, routable entity through which the Office Communications Servers in a load balancing pool are made available to the client (the IP address to give clients or add to DNS).

The next step in this configuration is to define a virtual server that references the profile and pool you created.

To create the Front-end SSL 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 **ocs-frontend-ssl-vs**.
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 **10.133.35.50**.
6. In the **Service Port** box, type **444**.

The screenshot shows the 'New Virtual Server...' configuration window. The breadcrumb path is 'Local Traffic > Virtual Servers > New Virtual Server...'. The 'General Properties' section includes the following fields:

Name	ocs-frontend-ssl-vs
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 10.133.35.50
Service Port	444 Other: [dropdown]
State	Enabled [dropdown]

Figure 7 The General Properties of the Front-End SSL virtual server

7. From the **Configuration** list, select **Advanced**.
8. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the TCP profile* section. In our example, we select **ocs-fe-ssl**.
9. In the Resources section, from the Default Pool list, select the pool you created in the *Creating the Front-End SSL pool* section. In our example, we select **ocs-frontend-ssl**.
10. Click the **Finished** button.

The screenshot shows the 'Resources' section of the configuration window. It features two list boxes for moving items between 'Enabled' and 'Available' states, along with 'Up' and 'Down' buttons for each. The 'Default Pool' is set to 'ocs-frontend-ssl'. Other persistence profiles are set to 'None'.

iRules	Enabled	Available
	[empty]	_sys_auth_ldap _sys_auth_radius _sys_auth_ssl_cc_ldap _sys_auth_ssl_ocsp _sys_auth_ssl_crdp
HTTP Class Profiles	Enabled	Available
	[empty]	SiebelHttpClass exch07_class httpclass Sharepoint2007Forum WebSphereWA
Default Pool	+ ocs-frontend-ssl [dropdown]	
Default Persistence Profile	None [dropdown]	
Fallback Persistence Profile	None [dropdown]	

Buttons: Cancel Repeat Finished

Figure 8 The Resources section of the Front-End SSL virtual server

Creating a SNAT

A source network address translation (SNAT) allows for inter-server communication and provides the ability to perform certain Office Communications Server pool-level management operations from the servers in a pool. Additionally, in a one-armed configuration, a SNAT allows virtual servers to exist on the same IP subnet as the Office Communication Server hosts.

A default SNAT will be appropriate for most deployments. If more than 65,000 simultaneous users will be connecting to the Office Communications Server deployment, see *Configuring a SNAT for large Office Communications Server deployments*, on page 14.

Use the procedure most applicable for your deployment.

To create a default SNAT for less than 65,000 concurrent users

Use this procedure if your Office Communications Server deployment has fewer than 65,000 simultaneous users.

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 **ocs-default-snat**.
4. From the **Translation** list, select a setting appropriate for your configuration. In our example, we select **Automap**.
5. From the **VLAN Traffic** list, select **Enabled on**.
6. In the VLAN List row, from the Available list, select the VLANs on which your OCS devices reside, and click the Add (<<) button.
7. Click the **Finished** button (see Figure 9).

Figure 9 Configuring a default SNAT

Configuring a SNAT for large Office Communications Server deployments

For large deployments (with 65,000 simultaneous users), we create a SNAT pool. A SNAT pool is a pool with one otherwise-unused address, on the same subnet as the virtual servers and Office Communications Servers. You must create a SNAT pool for each 65,000 clients (or fraction thereof).

◆ Important

*This procedure is **only** necessary for large deployments. If your Office Communications Server deployment has less than 65,000 simultaneous users, you **do not** need to create a SNAT pool. Use the procedure **To create a default SNAT for less than 65,000 concurrent users**, on page 13.*

To create a SNAT pool for large OCS deployments

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**. The SNATs screen opens.
2. On the Menu bar, click **SNAT Pool List**.
3. In the upper right portion of the screen, click the **Create** button. The New SNAT Pool screen opens.
4. In the Name box, type a name for this SNAT Pool. In our example, we type **ocs-snat-pool**.

5. In the **IP Address** box, type in a valid and otherwise-unused address on the subnet containing your OCS 2007 Front End servers, and click the **Add** button. In our example, we type **10.133.35.110**.
6. Repeat Step 5 for each additional address needed. At least one address should be added for each 65,000 anticipated concurrent connections (the number of connection generally corresponds to the number of OCS clients). In our example, we add **10.133.35.111**.
7. Click the **Finished** button.

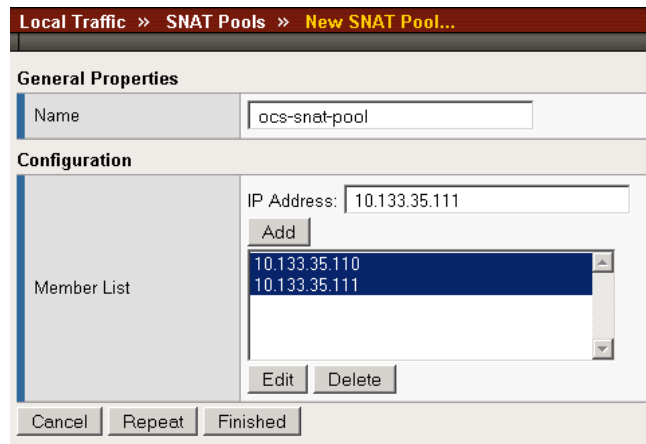


Figure 10 Creating the SNAT pool for large OCS deployments

The next step in the SNAT pool configuration is to configure a default SNAT that uses the SNAT pool.

To create a default SNAT that uses the SNAT pool

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 **ocs-default-snat**.
4. From the **Translation** list, select **SNAT Pool**.
5. From the **Select** list, select the name of the SNAT pool you created in the preceding procedure. In our example, we select **ocs-snat-pool**.
6. From the **VLAN Traffic** list, select **Enabled on**.
7. In the VLAN List row, from the Available list, select the VLANs on which your OCS devices reside, and click the Add (<<) button.
8. Click the **Finished** button (see Figure 11).

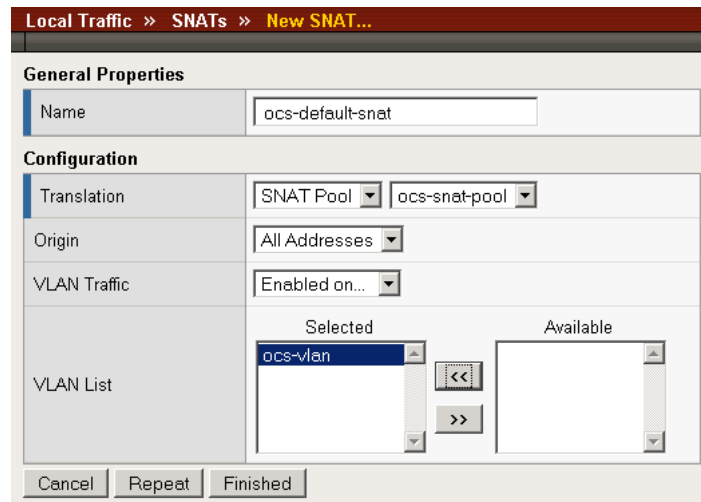


Figure 11 Creating a default SNAT for large OCS deployments

Configuring the BIG-IP LTM for SIP traffic on the OCS Front-end servers

The next task is to configure the BIG-IP LTM for directing SIP traffic to the Office Communications Server Front-End servers.

Creating a health monitor

The first step in configuring the BIG-IP LTM for SIP traffic on the Front-end servers is to configure a health monitor on the BIG-IP LTM system. We use the TCP parent monitor to create this monitor. We configure this monitor to specifically check port **5061**.

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 **ocs-fe-sip**.
4. From the **Type** list, select **TCP**. The TCP Monitor configuration options appear.

-
5. From the Configuration list, select **Advanced**.
The advanced configuration options appear.
 6. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout. In our example, we use a **Interval of 30** and a **Timeout of 91**.
 7. In the **Alias Service Port** box, type **5061**.
 8. All other configuration settings are optional, configure as applicable for your deployment.
 9. Click the **Finished** button.

Creating the pool

The next step is to create a pool on the BIG-IP LTM system.

Creating the Front-end SIP 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.
3. From the **Configuration** list, select **Advanced**.
The advanced configuration options appear.
4. In the **Name** box, enter a name for your pool.
In our example, we use **ocs-frontend-sip**.
5. In the **Health Monitors** section, select the name of the monitor you created in the *Creating a health monitor* section, and click the Add (<<) button. In our example, we select **ocs-fe-sip**.
6. Complete the rest of the Configuration section as applicable for your deployment.
7. In the Resources section, from the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
For this configuration, we recommend selecting **Least Connections (node)**. In Least Connections mode, the BIG-IP LTM system passes a new connection to the node that has the least number of current connections. Least Connections mode works best in environments where the servers or other equipment you are load balancing have similar capabilities. With Office Communications Server, traffic from servers to clients is roughly the same on each connection.

8. In the **New Members** section, you add the Office Communications Servers to the pool.
 - a) In the **Address** box, type the IP address of the Office Communications Server. In our example, we type **10.133.35.21**.
 - b) In the **Service Port** box, type the service number you want to use for this device. In our example, we type **5061**.
 - c) Click the **Add** button to add the member to the list.
 - d) Repeat steps a-c for each Office Communications Server you want to add to the pool. In our example, we repeat these steps for the other two Front-end servers (**10.133.35.22** and **10.133.35.23**).
9. Click the **Finished** button.

Creating the TCP profile

The next step is to create a TCP profile. Although this TCP profile is identical to the TCP profile we created earlier, we strongly recommend you create a new TCP profile for this virtual server. This allows you to fine tune this TCP profile for this virtual server in the future without affecting other virtual servers.

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.
The HTTP Profiles screen opens.
3. On the Menu bar, from the **Protocol** menu, select **TCP**.
4. In the upper right portion of the screen, click the **Create** button.
The New TCP Profile screen opens.
5. In the **Name** box, type a name. In our example, we type **ocs-fe-sip**.
6. In the **Idle Timeout** row, check the **Custom** box. In the seconds box, type **1200**.
7. Modify the rest of the settings as applicable for your network. The default settings should suffice for most networks.
8. Click the **Finished** button.

Creating the virtual server

The next step in this configuration is to define a virtual server that references the profile and pool you created.

To create the Front-end SIP 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 **ocs-frontend-sip-vs**.
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 **10.133.35.50**.
6. In the **Service Port** box, type **5061**.
7. From the **Configuration** list, select **Advanced**.
8. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the TCP profile* section. In our example, we select **ocs-fe-sip**.
9. In the Resources section, from the Default Pool list, select the pool you created in the *Creating the Front-End SSL pool* section. In our example, we select **ocs-frontend-ssl**.
10. Click the **Finished** button.

Creating a wildcard virtual server

The final task in the Office Communications Server Front-End configuration is to create a wildcard virtual server. This virtual server is for non-OCS specific traffic, such as domain authentication, and WINS traffic.

◆ Important

This procedure allows the Office Communications Servers behind the BIG-IP LTM device to communicate out. If this is not necessary in your environment, you can skip this procedure.

To create the wildcard 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 **ocs-wildcard-virtual**.
4. In the **Destination** section, select the **Network** option button.

5. In the **Address** box, type **0.0.0.0** to specify a wildcard virtual server.
6. In the **Mask** box, type **0.0.0.0**.
7. From the **Service Port** list, select ***All Ports**.
8. In the Configuration section, from the **Type** list, select **Forwarding (IP)**.
9. From the Protocol list, select **All Protocols**.
10. From the **VLAN Traffic** list, make sure that **All VLANs** is selected.
11. Click the **Finished** button.

Local Traffic » Virtual Servers » New Virtual Server...

General Properties

Name	ocs-wildcard-virtual
Destination	Type: <input type="radio"/> Host <input checked="" type="radio"/> Network Address: 0.0.0.0 Mask: 0.0.0.0
Service Port	* <input type="text"/> * All Ports
State	Enabled

Configuration:

Type	Forwarding (IP)
Protocol	TCP
Protocol Profile (Client)	fastL4
Statistics Profile	None
VLAN Traffic	All VLANs
Rate Class	None
Connection Limit	0
SNAT Pool	None
Clone Pool (Client)	None
Clone Pool (Server)	None
Last Hop Pool	None

Figure 12 Creating the Wildcard virtual server

Synchronizing the BIG-IP configuration if using a redundant system

If you are using a redundant BIG-IP configuration, the final step is to synchronize the configuration to the peer BIG-IP device.

To synchronize the configuration

1. On the Main tab, expand **System**.
2. Click **High Availability**.
The Redundancy screen opens.
3. On the Menu bar, click **ConfigSync**.
4. Click the **Self --> Peer** button.
The configuration synchronizes with its peer.

◆ Important

If you have a redundant BIG-IP configuration (active-active or active-standby), you must also perform the first two procedures (Creating a VLAN and Creating a self IP) on both devices. The rest of the procedures only need to be performed on one BIG-IP device. The first two procedures are not included in the items that are synchronized between the BIG-IP devices.

*In a redundant configuration, you also need to configure a Floating Self IP address for the VLAN on both devices. To create this Floating Self IP address, follow the procedure **Creating a self IP**, on page 5, but check the **Floating IP** box. On the redundant device, create a Floating Self IP address using the same IP address as the original device, and check the Floating IP box.*

Configuring the BIG-IP LTM for OCS Edge servers

The next task in this deployment is to configure the OCS Edge servers. An Edge server is an Office Communications Server 2007 server in the perimeter network that provides connectivity for external users and public IM connections. Employees traveling, or working from home or in remote offices, use the Edge servers to remotely access the service.

◆ Important

It is possible to deploy Office Communications Server 2007 without using the Edge Servers or services (for example, in an internal only deployment). If your configuration does not include Edge servers, you do not need to complete this section.

For the OCS Front-end servers, you must complete the following sections:

- *Configuring the BIG-IP LTM for HTTPS/SSL (444) traffic on the OCS Edge servers*
- *Configuring the BIG-IP LTM for SIP traffic on the OCS Edge servers*

The OCS Edge servers can be running multiple services or in different configurations. The examples below show how to configure the BIG-IP LTM for SIP and HTTPS OCS Edge Server traffic.

Configuring the BIG-IP LTM for HTTPS/SSL (444) traffic on the OCS Edge servers

The first task in this configuration is to configure the BIG-IP LTM for Edge server HTTPS traffic. As previously noted, Microsoft Office Communications Server clients require HTTPS communication with servers on custom port 444.

Creating a health monitor

The first step in configuring the BIG-IP LTM for the Edge servers is to configure a health monitor on the BIG-IP LTM system. We use the **HTTPS** parent monitor to create this monitor.

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 **ocs-edge-https**.
4. From the **Type** list, select **HTTPS**.
The HTTPS Monitor configuration options appear.
5. From the Configuration list, select **Advanced**.
The advanced configuration options appear.
6. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout. In our example, we use a **Interval of 30** and a **Timeout of 91**.
7. In the **Alias Service Port** box, type **444**.
8. Click the **Finished** button.

Local Traffic > Monitors > New Monitor...	
General Properties	
Name	ocs-edge-https
Type	HTTPS
Import Settings	https
Configuration: Advanced	
Interval	30 seconds
Timeout	91 seconds
Manual Resume	<input type="radio"/> Yes <input checked="" type="radio"/> No
Send String	GET /
Receive String	
Cipher List	DEFAULT:+SHA:+3DES:+kEDH
User Name	
Password	
Compatibility	Enabled
Client Certificate	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alias Address	* All Addresses
Alias Service Port	444 * All Ports
<input type="button" value="Cancel"/> <input type="button" value="Repeat"/> <input type="button" value="Finished"/>	

Figure 13 Configuring the health monitor

Creating the Edge server SSL pool

The next step is to create an Edge server pool on the BIG-IP LTM system.

Creating the Edge SSL 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.
3. From the **Configuration** list, select **Advanced**. The advanced configuration options appear.
4. In the **Name** box, enter a name for your pool. In our example, we use **ocs-edge-ssl**.
5. In the **Health Monitors** section, select the name of the monitor you created in the *Creating a health monitor* section, and click the Add (<<) button. In our example, we select **ocs-edge-https**.
6. Complete the rest of the Configuration section as applicable for your deployment.

Figure 14 Configuration options for the TLS pool

7. In the Resources section, from the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network). For this configuration, we recommend selecting **Least Connections (node)**. In Least Connections mode, the BIG-IP LTM system passes a new connection to the node that has the least number of current connections. Least Connections mode works best in environments

- where the servers or other equipment you are load balancing have similar capabilities. Using Office Communications Server, traffic from servers to clients is roughly the same on each connection.
8. In the **New Members** section, you add the Office Communications Servers to the pool.
 - a) In the **Address** box, type the IP address of the Office Communications Server.
In our example, we type **10.133.36.22**.
 - b) In the **Service Port** box, type **444**.
 - c) Click the **Add** button to add the member to the list.
 - d) Repeat steps a-c for each Office Communications Server you want to add to the pool. In our example, we repeat these steps twice for the other two Office Communications Servers (**10.133.36.23** and **10.133.36.24**). See Figure 15.
 9. Click the **Finished** button.

Figure 15 Configuring the resources for the pool

Repeat this procedure for any other OCS Edge services. Be sure to create a unique name for each pool, and use the appropriate IP addresses and Service Port.

Creating the TCP profile

The next step is to create a TCP profile. Although this TCP profile is identical to the TCP profile we created earlier, we strongly recommend you create a new TCP profile for this virtual server. This allows you to fine tune this TCP profile for this virtual server in the future without affecting other virtual servers.

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**. The HTTP Profiles screen opens.
3. On the Menu bar, from the **Protocol** menu, select **TCP**.
4. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
5. In the **Name** box, type a name. In our example, we type **ocs-edge-ssl**.
6. In the **Idle Timeout** row, check the **Custom** box. In the seconds box, type **1200**.
7. Modify the rest of the settings as applicable for your network. The default settings should suffice for most networks.
8. Click the **Finished** button.

Creating the virtual server

The next step in this configuration is to define a virtual server that references the profile and pool you created.

To create the Edge SSL 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 **ocs-edge-ssl-vs**.
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 **10.133.36.51**.
6. In the **Service Port** box, type **444**.

The screenshot shows the 'New Virtual Server...' configuration window. The breadcrumb path is 'Local Traffic >> Virtual Servers >> New Virtual Server...'. The 'General Properties' section contains the following fields:

Name	ocs-edge-ssl-vs	
Destination	Type:	<input checked="" type="radio"/> Host <input type="radio"/> Network
	Address:	10.133.36.51
Service Port	444	Other: <input type="text"/>
State	Enabled <input type="text"/>	

Figure 16 The General Properties of the TLS virtual server

7. From the **Configuration** list, select **Advanced**.
8. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the TCP profile* section. In our example, we select **ocs-edge-ssl**.
9. In the Resources section, from the Default Pool list, select the name of the pool you created in the *Creating the Edge SSL pool* section. In our example, we select **ocs-edge-ssl**.

The screenshot shows the 'Resources' configuration window. It has a title bar 'Resources' and a light beige background. The window is divided into several sections:

- iRules:** Contains two lists: 'Enabled' (empty) and 'Available' (containing _sys_auth_ldap, _sys_auth_radius, _sys_auth_ssl_cc_ldap, _sys_auth_ssl_ocsp, _sys_auth_ssl_crdp). There are '<<' and '>>' buttons between the lists, and 'Up' and 'Down' buttons below the 'Enabled' list.
- HTTP Class Profiles:** Contains two lists: 'Enabled' (empty) and 'Available' (containing exch07_class, httpclass, Sharepoint2007Forum, WebSphereWA, Sharepoint). There are '<<' and '>>' buttons between the lists, and 'Up' and 'Down' buttons below the 'Enabled' list.
- Default Pool:** A dropdown menu with a '+' icon on the left and 'ocs-edge-ssl' selected.
- Default Persistence Profile:** A dropdown menu with 'None' selected.
- Fallback Persistence Profile:** A dropdown menu with 'None' selected.

At the bottom of the window, there are three buttons: 'Cancel', 'Repeat', and 'Finished'.

Figure 17 Selecting the pool while creating the virtual server

10. Click the **Finished** button.

Configuring the BIG-IP LTM for SIP traffic on the OCS Edge servers

The next task is to configure the BIG-IP LTM for SIP traffic to the Office Communications Server Edge servers.

Creating a health monitor

The first step in configuring the BIG-IP LTM for SIP traffic on the Front-end servers is to configure a health monitor on the BIG-IP LTM system. We use the TCP parent monitor to create this monitor.

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 **ocs-edge-sip**.
4. From the **Type** list, select **TCP**.
The TCP Monitor configuration options appear.
5. From the Configuration list, select **Advanced**.
The advanced configuration options appear.
6. In the Configuration section, in the **Interval** and **Timeout** boxes, type an Interval and Timeout. We recommend at least a 1:3 +1 ratio between the interval and the timeout. In our example, we use a **Interval of 30** and a **Timeout of 91**.
7. In the **Alias Service Port** box, type **5061**.
8. All other configuration settings are optional, configure as applicable for your deployment.
9. Click the **Finished** button.

Creating the Edge SIP pool

The next step is to create a pool on the BIG-IP LTM system.

Creating the Edge SIP 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.

-
3. From the **Configuration** list, select **Advanced**.
The advanced configuration options appear.
 4. In the **Name** box, enter a name for your pool.
In our example, we use **ocs-edge-sip**.
 5. In the **Health Monitors** section, select the name of the monitor you created in the *Creating a health monitor* section, and click the Add (<<) button. In our example, we select **ocs-edge-sip**.
 6. Complete the rest of the Configuration section as applicable for your deployment.
 7. In the Resources section, from the **Load Balancing Method** list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
For this configuration, we recommend selecting **Least Connections (node)**. In Least Connections mode, the BIG-IP LTM system passes a new connection to the node that has the least number of current connections. Least Connections mode works best in environments where the servers or other equipment you are load balancing have similar capabilities. With Office Communications Server, traffic from servers to clients is roughly the same on each connection.
 8. In the **New Members** section, you add the Office Communications Servers to the pool.
 - a) In the **Address** box, type the IP address of the Office Communications Server. In our example, we type **10.133.32.21**.
 - b) In the **Service Port** box, type the service number you want to use for this device. In our example, we type **5061**.
 - c) Click the **Add** button to add the member to the list.
 - d) Repeat steps a-c for each Office Communications Server you want to add to the pool. In our example, we repeat these steps for the other two Front-end servers (**10.133.32.22** and **10.133.32.23**).
 9. Click the **Finished** button.

Creating the TCP profile

The next step is to create a TCP profile. Although this TCP profile is identical to the TCP profile we created earlier, we strongly recommend you create a new TCP profile for this virtual server. This allows you to fine tune this TCP profile for this virtual server in the future without affecting other virtual servers.

To create a new TCP profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.
The HTTP Profiles screen opens.

3. On the Menu bar, from the **Protocol** menu, select **TCP**.
4. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
5. In the **Name** box, type a name. In our example, we type **ocs-edge-sip**.
6. In the **Idle Timeout** row, check the **Custom** box. In the seconds box, type **1200**.
7. Modify the rest of the settings as applicable for your network. The default settings should suffice for most networks.
8. Click the **Finished** button.

Creating the virtual server

The next step in this configuration is to define a virtual server that references the profile and pool you created.

To create the Edge SIP 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 **ocs-edge-sip-vs**.
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 **10.133.36.51**.
6. In the **Service Port** box, type **5061**.
7. From the **Configuration** list, select **Advanced**.
8. From the **Protocol Profile (Client)** list, select the name of the profile you created in the *Creating the TCP profile* section. In our example, we select **ocs-edge-sip**.
9. In the Resources section, from the Default Pool list, select the pool you created in the *Creating the Edge SIP pool* section. In our example, we select **ocs-edge-sip**.
10. Click the **Finished** button.

Synchronizing the BIG-IP configuration if using a redundant system

If you are using a redundant BIG-IP configuration, the final step is to synchronize the configuration to the peer BIG-IP device.

To synchronize the configuration

1. On the Main tab, expand **System**.
2. Click **High Availability**.
The Redundancy screen opens.
3. On the Menu bar, click **ConfigSync**.
4. Click the **Self --> Peer** button.
The configuration synchronizes with its peer.

◆ Important

If you have a redundant BIG-IP configuration (active-active or active-standby), you must also perform the first two procedures (Creating a VLAN and Creating a self IP) on both devices. The rest of the procedures only need to be performed on one BIG-IP device. The first two procedures are not included in the items that are synchronized between the BIG-IP devices.

*In a redundant configuration, you also need to configure a Floating Self IP address for the VLAN on both devices. To create this Floating Self IP address, follow the procedure **Creating a self IP**, on page 5, but check the **Floating IP** box. On the redundant device, create a Floating Self IP address using the same IP address as the original device, and check the Floating IP box.*

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_ocs_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.