



Deploying F5 for High Availability and Scalability of Microsoft Dynamics 4.0



Microsoft[®] Partner

Introducing the F5 and Microsoft Dynamics CRM configuration

Microsoft® Dynamics CRM is a full customer relationship management (CRM) suite with marketing, sales, and service capabilities that are fast, familiar, and flexible, helping businesses of all sizes to find, win, and grow profitable customer relationships. Customers interested in deploying Dynamics CRM in the enterprise are going to need to provide a system that is always available, can scale to meet increased demand, and ensure the best end user performance.

Dynamics CRM 4.0 provides the ability to segment and cluster the specific server roles in order to facilitate the introduction of traffic management devices that deliver the networking support needed to provide mission critical CRM application delivery.

Leveraging BIG-IP Local Traffic Manager (LTM) provides:

- ◆ **High Availability**

BIG-IP LTM is designed to be CRM system aware, sending users to CRM front end servers that are currently serving valid content. When a CRM front end is down, or otherwise unable to deliver the appropriate content, the BIG-IP LTM sends all users to the other front ends which are currently available. This ensures that users will always be sent to the most available CRM resources.

- ◆ **Scalability**

By providing the necessary Traffic Management, BIG-IP LTM facilitates deploying Dynamics CRM in a distributed fashion, further allowing customers to meet the requirements of enterprise class deployments.

- ◆ **Performance**

Built into every BIG-IP LTM is TMOS™, F5's proprietary network operating system. TMOS provides unparalleled network traffic optimization, making sure network performance works for you, and not against you. HTTP based acceleration, such as intelligent caching, compression, and SSL termination further accelerate performance for the end user.

For more information on Microsoft Dynamics CRM, see <http://www.microsoft.com/dynamics/crm/default.aspx>

You can also find helpful resources in *Appendix B: Microsoft Dynamics CRM Resources*, on page 21.

This Deployment Guide contains procedures for configuring the BIG-IP LTM system & the BIG-IP LTM system with SSL. Further information on configuring F5 FirePass, WebAccelerator, & Application Security Module can be found at <http://www.f5.com/products/>.

You can also visit the Microsoft page of F5's online developer community, DevCentral, for Microsoft forums, solutions, blogs and more: <http://devcentral.f5.com/Default.aspx?tabid=89>.

Prerequisites and configuration notes

The following are general prerequisites for this deployment; each section contains specific prerequisites:

- ◆ All of the configuration procedures in this document are performed on F5 devices. For information on how to deploy or configure Microsoft Dynamics CRM 4.0, consult the appropriate Microsoft documentation.
- ◆ We recommend running Microsoft Dynamics CRM Server 4.0 edition. While the BIG-IP LTM procedures in this guide will work for version 3.0, this document was written for Dynamics CRM 4.0.
- ◆ We recommend the use of BIG-IP v9.4 or later. Although earlier versions can be used, the testing done to support this document was done using the v9.4 branch.
- ◆ The configuration in this document was performed on a local (that is, not a hosted or Live offering) deployment of Microsoft Dynamics CRM 4.0, and was configured according to the preferred practices guidelines as documented in the CRM implementation guide(s). For more information, see the Microsoft documentation.
- ◆ This document is written with the assumption that you are familiar with both the F5 devices and Microsoft Dynamics CRM 4.0. For more information on configuring these products, consult the appropriate documentation.
- ◆ This Deployment Guide assumes that you have already installed the F5 devices in your network. It also assumes that you have performed basic configuration tasks such as creating Self IP addresses and VLANs. For more information on how to install F5 devices and configure the basic settings, refer to the appropriate F5 manual, available on AskF5.
- ◆ For certain optional optimization features, the appropriate module on the BIG-IP LTM system must be licensed (such as RAM Cache).

Configuration example

The BIG-IP LTM system provides intelligent traffic management and high availability for Microsoft Dynamics CRM 4.0 deployments.

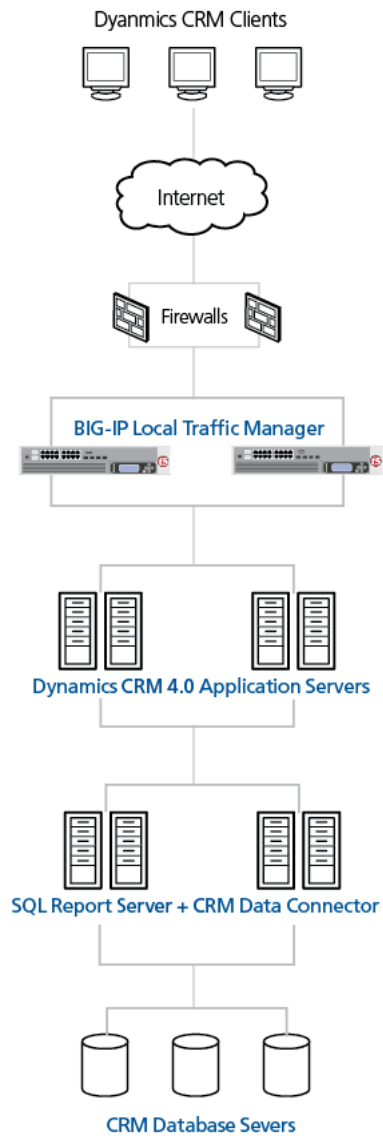


Figure 1 BIG-IP LTM - Dynamics CRM 4.0 logical configuration diagram

Configuration Tasks

To configure the BIG-IP and Dynamics CRM 4.0 devices for integration, you need to complete the following procedures:

- *Connecting to the BIG-IP LTM device*
- *Creating the HTTP health monitor*
- *Creating the pool*
- *Creating profiles*
- *Creating the HTTP virtual server*
- *Synchronizing the BIG-IP configuration if using a redundant system*

If you are using the BIG-IP LTM system as an SSL proxy for your Microsoft Dynamics CRM deployment, be sure to see *Configuring the BIG-IP LTM system for Microsoft Dynamics using SSL termination*, on page 14 after you complete the procedures in this section.

◆ 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 19.*

Connecting to the BIG-IP LTM device

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

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

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

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

Creating the HTTP health monitor

The next step is to set up health monitors for the Dynamics CRM Front End Servers. This procedure is optional, but very strongly recommended. For this configuration, we use an HTTP monitor, which checks nodes (IP address and port combinations), and can be configured to use Send and Receive statements in an attempt to retrieve explicit content from nodes.

To configure a HTTP health monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**. The Monitors screen opens.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a name for the Monitor. In our example, we type **Dynamics-monitor**.
4. From the **Type** list, select **http**.
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 (for example, the default setting has an interval of **5** and an timeout of **16**). In our example, we use a **Interval** of **30** and a **Timeout** of **91**.
6. In the **Send String** and **Receive String** sections, you can add specific Send and Receive Strings to the device being checked.

Local Traffic >> Monitors >> New Monitor...	
General Properties	
Name	Dynamics-monitor
Type	HTTP
Import Settings	http
Configuration: Basic	
Interval	30 seconds
Timeout	91 seconds
Send String	GET /
Receive String	
User Name	
Password	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
Cancel Repeat Finished	

Figure 2 Creating the HTTP Monitor

7. Click the **Finished** button.
The new monitor is added to the Monitor list.

Creating the pool

The next step in this configuration is to create a pool on the BIG-IP system. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this configuration, we create one pool for the Dynamics CRM Front ends.

To create the Dynamics 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 **Dynamics-servers**.
4. In the **Health Monitors** section, select the name of the monitor you created in the *Creating the HTTP health monitor* section, and click the Add (<<) button. In our example, we select **Dynamics-monitor**.
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. For this pool, we leave the Priority Group Activation **Disabled**.
7. In the New Members section, make sure the **New Address** option button is selected.
8. In the **Address** box, add the first server to the pool. In our example, we type **10.10.100.151**
9. In the **Service Port** box, type the service number you want to use for this device, or specify a service by choosing a service name from the list.
In our example, we type **80**.
10. Click the **Add** button to add the member to the list.
11. Repeat steps 9-11 for each server you want to add to the pool.
In our example, we repeat these steps once for the remaining server, **10.10.100.152**.
12. Click the **Finished** button (see Figure 3).

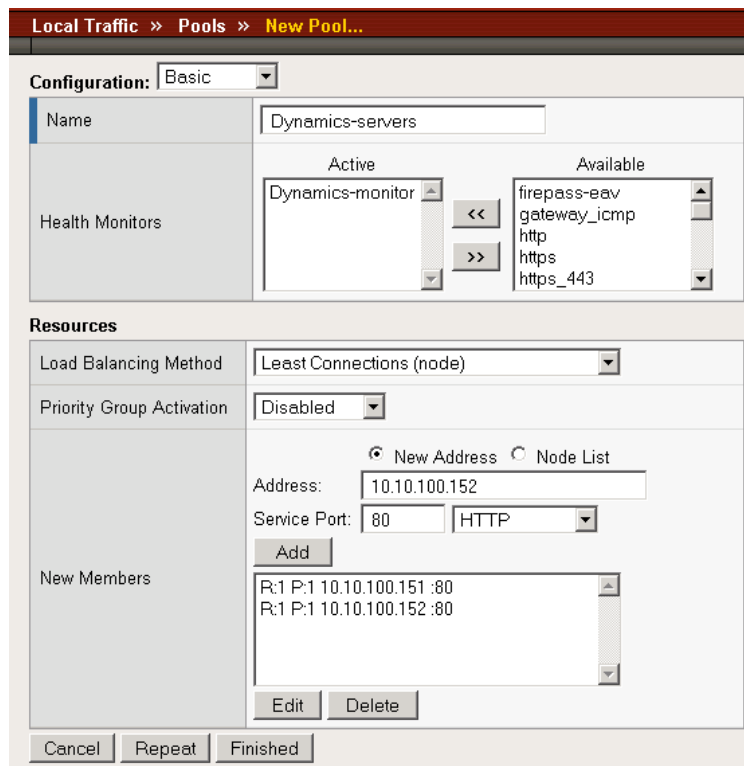


Figure 3 Creating the BIG-IP LTM pool for the Dynamics servers

Creating profiles

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

Although it is possible to use the default profiles, we strongly recommend you create new profiles based on the default parent profiles. 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 an HTTP profile

The first new profile we create is an HTTP profile. In the following example, we base our HTTP profile off of a new profile included with BIG-IP LTM version 9.4, called **http-wan-optimized-compression-caching**, with a few additional modifications. This profile includes some default optimization settings that increase the performance of Dynamics CRM 4.0 over the WAN.

The following procedure shows one way to optimize the Microsoft Dynamics CRM 4.0 configuration and shown to give the greatest improvement. These procedures and the specific values given in some steps should be used as guidelines, modify them as applicable to your configuration.

To create a new HTTP profile

1. On the Main tab, expand **Local Traffic**.
2. Click **Profiles**.
The HTTP 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 **dynamics-http-opt**.
5. From the **Parent Profile** list, select **http-wan-optimized-compression-caching**.
6. In the Settings section, check the Custom box for **Redirect Rewrite**, and from the **Redirect Rewrite** list, select **Match**.
7. In the Compression section, check the Custom box for **Compression**, and from the **Compression** list, select **Enabled**.
8. Check the Custom box for **Content Compression**, and leave **Content List** selected.
9. In the Content List section, add the following entries to the **Content Type** box one at a time, each followed by clicking **Include**:
 - application/pdf
 - application/vnd.ms-powerpoint
 - application/vnd.ms-excel
 - application/msword
 - application/vnd.ms-publisher
10. Check the Custom box for **Keep Accept Encoding**, and check the box to enable Keep Accept Encoding.
11. Modify any of the other settings as applicable for your network.
12. Click the **Finished** button.

Creating the TCP profiles

The next profiles we create are the TCP profiles. If most of the Dynamic CRM 4.0 users are connecting via a Local Area Network, we recommend using the **tcp-lan-optimized** (for server-side TCP connections) parent profile. If the majority of the users are accessing the system from remote or home offices, we recommend using an additional TCP profile, called

tcp-wan-optimized (for client side TCP connections). In our example, we use both profiles, and leave the settings at their default levels; you can configure any of the options as applicable for your network.

Creating the LAN optimized TCP profile

First we configure the LAN optimized profile. If you are not using version 9.4 or do not want to use this optimized profile, you can choose the default TCP parent profile.

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 **dynamics-tcp-lan**.
5. From the **Parent Profile** list, select **tcp-lan-optimized** if you are using BIG-IP LTM version 9.4 or later; otherwise select **tcp**.
6. Modify any of the settings as applicable for your network. In our example, we leave the settings at their default levels.
7. Click the **Finished** button.

Creating the WAN optimized TCP profile

Now we configure the WAN optimized profile. Remember, if most users are accessing the portal via the LAN, you do not need to create this profile.

To create a new TCP WAN optimized profile

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**. The HTTP Profiles screen opens.
2. On the Menu bar, from the **Protocol** menu, click **tcp**.
3. In the upper right portion of the screen, click the **Create** button. The New TCP Profile screen opens.
4. In the **Name** box, type a name for this profile. In our example, we type **dynamics-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 a cookie persistence profile

The final profile we create is a Cookie Persistence profile. We recommend using the default cookie method for this profile (HTTP cookie insert), but you can change other settings, such as specifying a cookie expiration.

To create a new cookie persistence profile based on the default 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 **Dynamics-cookie**.
5. From the **Persistence Type** list, select **Cookie**. The configuration options for cookie persistence appear.
6. Modify any of the settings as applicable for your network.
7. Click the **Finished** button.

General Properties	
Name	dynamics-cookie
Persistence Type	Cookie
Parent Profile	cookie

Configuration		Custom <input type="checkbox"/>
Cookie Method	HTTP Cookie Insert	<input type="checkbox"/>
Cookie Name		<input type="checkbox"/>
Expiration	<input checked="" type="checkbox"/> Session Cookie	<input type="checkbox"/>

Cancel Repeat Finished

Figure 4 Creating the cookie persistence profile

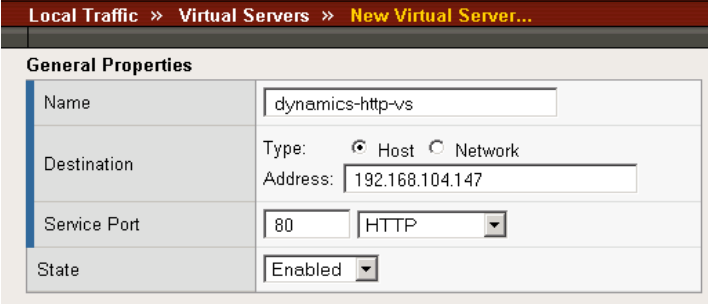
For more information on creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.

Creating the HTTP virtual server

Next, we configure a HTTP virtual server that references 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 **dynamics-http-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 **192.168.104.147**.
6. In the **Service Port** box, type **80** or select **HTTP** from the list.



The screenshot shows the 'New Virtual Server...' configuration window. The breadcrumb trail at the top reads 'Local Traffic > Virtual Servers > New Virtual Server...'. The 'General Properties' section is expanded, showing the following fields:

Name	dynamics-http-vs
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 192.168.104.147
Service Port	80 HTTP
State	Enabled

Figure 5 Configuring the virtual server General Properties

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 *Creating the WAN optimized TCP profile*. In our example, we select **dynamics-tcp-wan**.
10. From the **Protocol Profile (Server)** list, select the name of the profile you created in *Creating the LAN optimized TCP profile*. In our example, we select **dynamics-tcp-lan**.
11. From the HTTP Profile list, select the name of the profile you created in *Creating an HTTP profile*. In our example, we select **dynamics-http-opt** (see Figure 6).

The screenshot shows the Configuration tab with the following settings:

Configuration:	Advanced
Type	Standard
Protocol	TCP
Protocol Profile (Client)	dynamics-tcp-wan
Protocol Profile (Server)	dynamics-tcp-lan
OneConnect Profile	None
HTTP Profile	dynamics-http-opt
FTP Profile	None

Figure 6 Selecting the TCP and HTTP profiles for the virtual server

12. 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.
13. From the **Default Persistence Profile** list, select the persistence profile you created in the *Creating a cookie persistence profile* section. In our example, we select **SPSCookie**.

The screenshot shows the Resources section with the following configurations:

Resources							
iRules	<table border="1"> <tr> <th>Enabled</th> <th>Available</th> </tr> <tr> <td></td> <td> _sys_auth_ssl_ocsp _sys_auth_ssl_crdp _sys_auth_tacacs OutlookAnywherePersistRule firepass-sslload </td> </tr> <tr> <td>Up</td> <td>Down</td> </tr> </table>	Enabled	Available		_sys_auth_ssl_ocsp _sys_auth_ssl_crdp _sys_auth_tacacs OutlookAnywherePersistRule firepass-sslload	Up	Down
Enabled	Available						
	_sys_auth_ssl_ocsp _sys_auth_ssl_crdp _sys_auth_tacacs OutlookAnywherePersistRule firepass-sslload						
Up	Down						
HTTP Class Profiles	<table border="1"> <tr> <th>Enabled</th> <th>Available</th> </tr> <tr> <td></td> <td> redirect-class httpclass oracle-ebs </td> </tr> <tr> <td>Up</td> <td>Down</td> </tr> </table>	Enabled	Available		redirect-class httpclass oracle-ebs	Up	Down
Enabled	Available						
	redirect-class httpclass oracle-ebs						
Up	Down						
Default Pool	Dynamics-servers						
Default Persistence Profile	dynamics-cookie						
Fallback Persistence Profile	None						
<table border="1"> <tr> <td>Cancel</td> <td>Repeat</td> <td>Finished</td> </tr> </table>		Cancel	Repeat	Finished			
Cancel	Repeat	Finished					

Figure 7 Adding the pool and persistence profile to the virtual server

14. 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 using the Configuration utility

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.

The BIG-IP LTM system is now configured to direct traffic to the Microsoft Dynamics CRM 4.0 deployment. If you are using the BIG-IP LTM system to offload SSL traffic from your Dynamics CRM 4.0 deployment, continue to the following section.

Configuring the BIG-IP LTM system for Microsoft Dynamics using SSL termination

This section describes how to configure the BIG-IP LTM system as an SSL proxy for a Microsoft Dynamics CRM 4.0 deployment. If you are not using the BIG-IP LTM system to offload SSL traffic, you do not need to perform these procedures.

◆ **Note**

This section is written with the assumption that you have already configured your BIG-IP LTM system for a Dynamics CRM 4.0 deployment as described in this Deployment Guide.

Prerequisites and configuration notes

The following are additional prerequisites for this section:

- ◆ You need an SSL certificate for your site that is compatible with the BIG-IP LTM system. For more information, consult the BIG-IP documentation.
- ◆ You have already configured the BIG-IP LTM system as described in this Deployment Guide. If you have not, start with *Configuration example*, on page 3.

This section contains following procedures for configuring the BIG-IP LTM system:

- *Using SSL certificates and keys*
- *Create a Client SSL profile*
- *Creating the Redirect iRule*
- *Modifying the HTTP virtual server*
- *Creating the HTTPS virtual server*

Using SSL certificates and keys

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 Dynamics CRM 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 LTM 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 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**.
This displays the list of existing certificates.
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.

Create a Client SSL profile

The next step in this configuration is to create an 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 **dynamics_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 Redirect iRule

The Redirect iRule takes incoming HTTP requests (non-secure) and redirects them to the correct HTTPS (secure) virtual server, without user interaction

To create the Redirect iRule

1. On the Main tab, expand **Local Traffic**, and then click **iRules**. The iRule screen opens.
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 **dynamics-http-to-https**.
4. In the Definition section, copy and paste the following iRule:

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

5. Click the **Finished** button.

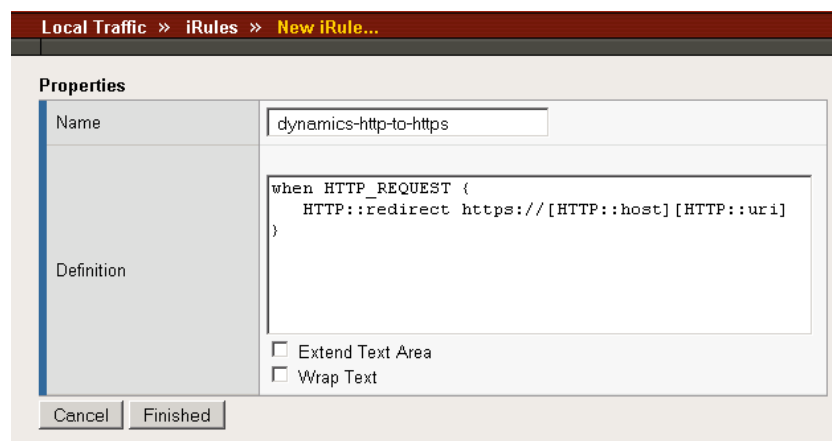


Figure 8 Creating the iRule

Modifying the HTTP virtual server

The next task is to modify the HTTP virtual server you created in *Creating the HTTP virtual server*, on page 10 to use the iRule you just created.

To modify the existing HTTP virtual server

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 Dynamics HTTP virtual server you created in the *Creating the HTTP virtual server* section. In our example, we click **dynamics-http-vs**.
3. On the menu bar, click **Resources**. The Resources page for the virtual server opens.
4. In the iRules section, click the **Manage** button. The 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 **dynamics-http-to-https**.
6. Click the **Finished** button.

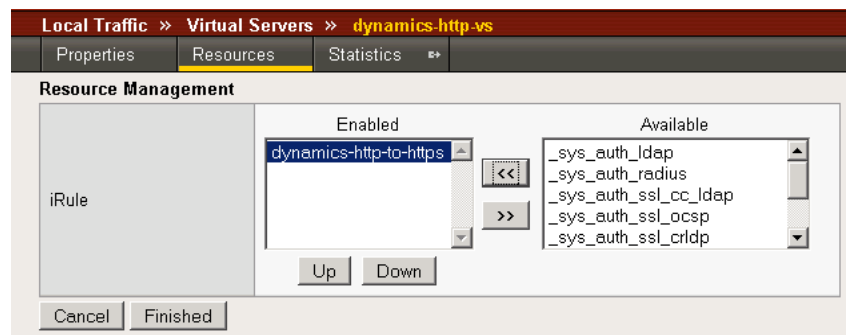


Figure 9 Adding the iRule to the virtual server

7. From the **Default Pool** list, select **None**. This virtual server no longer requires the load balancing pool, as traffic is redirected to the HTTPS virtual server we create in the following procedure.
8. Click the **Update** button.

Creating the HTTPS virtual server

The final task in this section is to create a HTTPS virtual server.

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 **dynamics-https-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 **192.168.104.146**.
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 name of the profile you created in *Creating the WAN optimized TCP profile*. In our example, we select **dynamics-tcp-wan**.
10. From the **Protocol Profile (Server)** list, select the name of the profile you created in *Creating the LAN optimized TCP profile*. In our example, we select **dynamics-tcp-lan**.
11. From the HTTP Profile list, select the name of the profile you created in *Creating an HTTP profile*. In our example, we select **dynamics-http-opt**.
12. From the **SSL Profile (Client)** list, select the name of the SSL profile you created in *Create a Client SSL profile*. In our example, we select **dynamics-clientssl**.
13. From the **Default Pool** list, select the pool you created in the *Creating the pool* section. In our example, we select **Dynamics-servers**.
14. From the **Default Persistence Profile** list, select the persistence profile you created in *Creating a cookie persistence profile*. In our example, we select **dynamics-cookie**.
15. Click the **Finished** button.

This concludes the BIG-IP LTM configuration. If you are using a redundant BIG-IP LTM system, see *Synchronizing the BIG-IP configuration if using a redundant system*, on page 13.

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.
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.

Appendix B: Microsoft Dynamics CRM Resources

The following is a list of helpful resources for Microsoft Dynamics CRM.

Web Resources

- ◆ The Microsoft CRM Web page is a great place to start learning about the features and benefits of Microsoft CRM:
<http://www.microsoft.com/dynamics/crm/default.aspx>
- ◆ Microsoft Dynamics CRM 4.0 Overview:
<http://www.microsoft.com/dynamics/crm/product/overview.aspx>
- ◆ Microsoft CRM Community
The official Microsoft CRM Community Web page contains links to thriving newsgroups, blogs, and other communities that focus on Microsoft CRM:
<http://www.microsoft.com/dynamics/crm/community/default.aspx>
- ◆ Microsoft CRM on MSDN
<http://msdn2.microsoft.com/en-us/dynamics/crm/default.aspx>

Documentation Resources

- ◆ The Microsoft CRM 4.0 documentation is updated on a regular basis and posted to the Microsoft Download Center:
<http://www.microsoft.com/downloads/results.aspx?poId=&freetext=Microsoft%20CRM%204.0&DisplayLang=en>
- ◆ Microsoft CRM 4.0 Implementation Guide
The Implementation Guide provides the information you need to successfully implement Microsoft CRM in your business. This guide addresses the planning, installing (both hardware and software), pre-deployment, testing, and operating tasks for the maintenance of the Microsoft CRM system:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=1ceb5e01-de9f-48c0-8ce2-51633ebf4714&DisplayLang=en>