Deployment Guide

Deploying F5 with Microsoft Dynamics CRM 2011 and 2013

Welcome to the F5 deployment guide for configuring the BIG-IP Local Traffic Manager (LTM), Access Policy Manager (APM), and Advanced Firewall Manager (AFM) with Microsoft® Dynamics CRM. This document provides guidance on configuring the BIG-IP system for Dynamics CRM 2011 or 2013 deployments. Dynamics CRM is a full customer relationship management 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. This guide shows how to quickly and easily configure the BIG-IP system using the new Dynamics iApp Application template. There is also an appendix with manual configuration tables for users who prefer to create each individual object.

Why F5?

F5 offers a complete suite of application delivery technologies designed to provide a highly scalable, secure, and responsive Dynamics CRM deployment.

- Terminating HTTPS connections at the BIG-IP LTM reduces CPU and memory load on CRM front end servers, and simplifies TLS/SSL certificate management.
- The BIG-IP LTM can balance load and ensure high-availability across multiple CRM servers using a variety of load balancing methods and priority rules.
- The BIG-IP LTM TCP Express feature set ensures optimal network performance for all clients and servers, regardless of operating system and version.
- The LTM provides content compression features which improve client performance.
- The BIG-IP Access Policy Manager (APM), F5's high-performance access and security solution, can provide pre-authentication and secure remote access to your Dynamics CRM environment.

Products and versions

Product	Version
BIG-IP LTM, APM, AFM	11.3, 11.4, 11.4.1, 11.5, 11.5.1, 11.6
Microsoft Dynamics CRM	2011 (Update Rollup 15), 2013, 2013 SP1
iApp version	f5.microsoft_dynamics_crm_2011_2013.v1.0.0
Deployment guide version	2.9 (*Document Revision History on page 48)*

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/dynamics-crm-2011-2013-dg.pdf*

Microsoft Partner Network

Contents

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/Microsoft/*

To provide feedback on this deployment guide or other F5 solution documents, contact us at *solutionsfeedback@f5.com*.

What is F5 iApp?

New to BIG-IP version 11, F5 iApp is a powerful new set of features in the BIG-IP system that provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. The iApp template for Microsoft Dynamics acts as the single-point interface for building, managing, and monitoring these servers.

For more information on iApp, see the White Paper *F5 iApp: Moving Application Delivery Beyond the Network:* *http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf*.

Prerequisites and configuration notes

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

- This document provides guidance on using the **downloadable iApp** for Microsoft Dynamics CRM 2011 and 2013 available from *downloads.f5.com*.
- All of the configuration procedures in this document are performed on F5 devices. For information on how to deploy or configure Microsoft Dynamics CRM, consult the appropriate Microsoft documentation.
- If using Dynamics 2011, we recommend running Microsoft Dynamics CRM Server 2011 edition, with Update Rollup 15 (*http://support.microsoft.com/kb/2555051*) or later. While the BIG-IP LTM procedures in this guide may work for previous versions of Dynamics CRM, this document was written for Dynamics CRM 2011 and updated for 2013.
- You must be on BIG-IP LTM version 11.3 or later.
- The configuration in this document was performed on an on-premises deployment of Microsoft Dynamics CRM, and was configured according to the preferred practices guidelines as documented in the CRM implementation guide(s). For more information, see the Microsoft documentation.
- The BIG-IP system supports deploying Dynamics CRM in both Internet-facing (IFD) and non-Internet-facing configurations. With IFD deployments, clients accessing the CRM site are redirected to Microsoft AD FS (or AD FS Proxy) for authentication. The AD FS deployment guide (*http://www.f5.com/pdf/deployment-guides/microsoft-adfs-dg.pdf)* describes how to configure the BIG-IP system to load balance these AD FS requests. For non-IFD deployments, you may secure CRM using F5's APM by following the guidance in *Configuring BIG-IP Access Policy Manager for Dynamics CRM 2011 and 2013 on page 33*.
- You must have already installed the F5 device(s) in your network and performed the initial configuration tasks, such as creating Self IP addresses and VLANs. For more information, refer to the appropriate BIG-IP LTM manual, available at *http://support.f5.com/kb/en-us.html*.
- ***SSL Offloading and Microsoft Dynamics CRM for Microsoft Outlook***
  Currently, SSL offloading is not supported for the Microsoft Dynamics CRM for the Outlook client. If you are deploying CRM for Microsoft Outlook, you **must** configure the BIG-IP system for either unencrypted HTTP client/server traffic, or SSL decryption/re-encryption (SSL bridging). Also note that SSL offload is not supported for IFD deployments. SSL bridging is mandatory for IFD.

Configuration example

The BIG-IP LTM system provides intelligent traffic management and high availability for Microsoft Dynamics CRM deployments. You can also use the BIG-IP APM module to provide secure remote access and proxy authentication to your Dynamics CRM implementation. The following diagram shows a simple, logical configuration.

Figure 1: *Logical configuration diagram*

Optional Modules

This Microsoft Dynamics CRM iApp allows you to use four modules on the BIG-IP system. To take advantage of these modules, they must be licensed and provisioned before starting the iApp template. For information on licensing modules, contact your sales representative.

- **BIG-IP AAM** (formerly BIG-IP WAN Optimization Manager and WebAccelerator)
  BIG-IP AAM provides application, network, and front-end optimizations to ensure consistently fast performance for today's dynamic web applications, mobile devices, and wide area networks. With sophisticated execution of caching, compression, and image optimization, BIG-IP AAM decreases page download times. You also have the option of using BIG-IP AAM for symmetric optimization between two BIG-IP systems. For more information on BIG-IP Application Acceleration Manager, see *http://www.f5.com/products/big-ip/big-ip-application-acceleration-manager/overview/*.
- **BIG-IP AFM**
  BIG-IP Advanced Firewall Manager (AFM) is a high-performance, stateful, full-proxy network firewall designed to guard data centers against incoming threats that enter the network on the most widely deployed protocols—including HTTP/S, SMTP, DNS, and FTP. By aligning firewall policies with the applications they protect, BIG-IP AFM streamlines application deployment, security, and monitoring. For more information on BIG-IP AFM, see *https://f5.com/products/modules/advanced-firewall-manager*.
- **BIG-IP APM**
  BIG-IP Access Policy Manager (APM) is a flexible, high-performance access and security solution that provides unified global access to your business-critical applications and networks. By consolidating remote access, web access management, VDI, and other resources in a single policy control point—and providing easy-to-manage access policies—BIG-IP APM helps you free up valuable IT resources and scale cost-effectively. See *http://www.f5.com/products/big-ip/big-ip-access-policy-manager/overview/*.
- **Application Visibility and Reporting**
  F5 Analytics (also known as Application Visibility and Reporting or AVR) is a module on the BIG-IP system that lets customers view and analyze metrics gathered about the network and servers as well as the applications themselves. Making this information available from a dashboard-type display, F5 Analytics provides customized diagnostics and reports that can be used to optimize application performance and to avert potential issues. The tool provides tailored feedback and recommendations for resolving problems. Note that AVR is licensed on all systems, but must be provisioned before beginning the iApp template.

Guidance for configuring email with server-side synchronization for Dynamics 2013

If you are using Dynamics CRM 2013 for email routing, we recommend using server-side synchronization, Microsoft's recommended method for Dynamics 2013. Server-side synchronization has been validated while protecting both CRM 2013 and Exchange 2010/2013 with BIG-IP APM. We recommend using server-side synchronization (and not the CRM plug-in for Outlook) for CRM 2013 because SSL offload and using the BIG-IP APM are both supported for server-side synchronization, but are not supported when using the plug-in.
For specific instructions on configuring the BIG-IP system for Microsoft Exchange Server, see *http://www.f5.com/pdf/deployment-guides/microsoft-exchange-2010-2013-iapp-dg.pdf*.
For information on setting up email through server-side synchronization in Dynamics CRM 2013, see *http://www.microsoft.com/en-us/dynamics/crm-customer-center/set-up-email-through-server-side-synchronization.aspx*.

Using this guide

This deployment guide is intended to help users deploy web-based applications using the BIG-IP system. This document contains guidance configuring the BIG-IP system using the iApp template, as well as manually configuring the BIG-IP system.

Using this guide to configure the iApp template

We recommend using the iApp template to configure the BIG-IP system for your Microsoft Dynamics implementation. The majority of this guide describes the iApp template and the different options the template provides for configuring the system for Microsoft Dynamics.

The iApp template configuration portion of this guide walks you through the entire iApp, giving detailed information not found in the iApp or inline help. The questions in the UI for the iApp template itself are all displayed in a table and at the same level. In this guide, we have grouped related questions and answers in a series of lists. Questions are part of an ordered list and are underlined and in italics or bold italics. Options or answers are part of a bulleted list, and in bold. Questions with dependencies on other questions are shown nested under the top level question, as shown in the following example:

1. ***Top-level question found in the iApp template***
   - *Select an object you already created from the list* (such as a profile or pool; not present on all questions. Shown in bold italic)
   - **Choice #1** (in a drop-down list)
   - **Choice #2** (in the list)
     a. *Second level question dependent on selecting choice #2*
        - **Sub choice #1**
        - **Sub choice #2**
          i). *Third level question dependent on sub choice #2*
              - **Sub-sub choice**
              - **Sub-sub #2**
                1). *Fourth level question (rare)*

Advanced options/questions in the template are marked with the Advanced icon: Advanced . These questions only appear if you select the Advanced configuration mode.

Using this guide to manually configure the BIG-IP system

Users already familiar with the BIG-IP system can use the manual configuration tables to configure the BIG-IP system for the Dynamics implementation. These configuration tables only show the configuration objects and any non-default settings recommended by F5, and do not contain procedures on specifically how to configure those options in the Configuration utility. See *Appendix A: Manual Configuration Tables on page 30.*

Preparing to use the iApp

In order to use the iApp for Microsoft Dynamics, it is helpful to have some information, such as server IP addresses and domain information before you begin. Use the following table for information you may need to complete the template. The table includes the information that is helpful to have in advance. More information on specific template questions can be found on the individual pages.

<table>
<tr><th colspan="3">BIG-IP system Preparation Table</th></tr>
<tr><td>Basic/Advanced mode</td><td colspan="2">In the iApp, you can configure the system for Microsoft Dynamics with F5 recommended settings (Basic mode) which are a result of extensive testing and tuning with Microsoft Dynamics. Advanced mode allows configuring the BIG-IP system on a much more granular level, configuring specific options, or using your own pre-built profiles or iRules. Basic/Advanced "configuration mode" is independent from the Basic/Advanced list at the very top of the template which only toggles the Device and Traffic Group options</td></tr>
<tr><td rowspan="5">Network</td><td>Type of network between <u>clients</u> and BIG-IP</td><td>Type of network between <u>servers</u> and BIG-IP</td></tr>
<tr><td>LAN | WAN | WAN through another BIG-IP system</td><td>LAN | WAN | WAN through another BIG-IP system</td></tr>
<tr><td colspan="2">If WAN through another BIG-IP system, you must have BIG-IP AAM pre-configured for Symmetric Optimization.</td></tr>
<tr><td>Where are BIG-IP virtual servers in relation to the servers</td><td>Expected number of concurrent connections per server</td></tr>
<tr><td>Same subnet | Different subnet
If they are on different subnets, you need to know if the Dynamics servers have a route through the BIG-IP system. If there is not a route, you need to know the number of concurrent connections.</td><td>More than 64k concurrent | Fewer than 64k concurrent
If more than 64k per server, you need an available IP address for each 64k connections you expect for the SNAT Pool</td></tr>
<tr><td>SSL Encryption</td><td>SSL Offload or SSL Bridging</td><td>Re-encryption (Bridging and server-side encryption)</td></tr>
<tr><td>If configuring the system for SSL Offload or SSL Bridging, you must have imported a valid SSL certificate and key onto the BIG-IP system. You have the option of also using an Intermediate (chain) certificate as well if required in your implementation.
Certificate:
Key:
Intermediate Certificate (optional):</td><td>When the BIG-IP system encrypts traffic to the servers, it is acting as an SSL client and by default we assume the servers do not expect the system to present its client certificate on behalf of clients traversing the virtual server. If your servers expect the BIG-IP system to present a client certificate, you must create a custom Server SSL profile outside of the template with the appropriate certificate and key.</td></tr>
<tr><td rowspan="2">Virtual Server and Pools</td><td>Virtual Server</td><td>Dynamics server pool</td></tr>
<tr><td>The virtual server is the address clients use to access the servers.
IP address for the virtual server:
Associated service port:
FQDN clients will use to access the Microsoft Dynamics servers:</td><td>The load balancing pool is the LTM object that contains the servers.
IP addresses of the servers: 1: 3:
2: 5:
4: 7:
6: 9:
8:</td></tr>
<tr><td>Profiles</td><td colspan="2">For each of the following profiles, the iApp will create a profile using the F5 recommended settings (or you can choose ‘do not use’ many of these profiles). While <u>we recommend using the profiles created by the iApp</u>, you have the option of creating your own custom profile outside the iApp and selecting it from the list. The iApp gives the option of selecting our the following profiles (some only in Advanced mode). Any profiles must be present on the system before you can select them in the iApp
HTTP | Persistence | HTTP Compression | TCP LAN | TCP WAN | OneConnect | Web Acceleration | NTLM | iSession</td></tr>
<tr><td rowspan="2">Health monitor</td><td>HTTP Request</td><td>User Account</td></tr>
<tr><td>In Advanced mode, you have the option of selecting the type of HTTP request the health monitor uses: GET or POST.
You can also specify Send and Receive strings to more accurately determine server health.
Send string (the URI sent to the servers):
Receive string (what the system expects in return):
POST Body (only if using POST):</td><td>Also in advanced mode, the monitor can attempt to authenticate to the Dynamics servers as a part of the health check. If you want the monitor to require credentials, create a user account specifically for this monitor that has no additional permissions and is set to never expire. Account maintenance becomes a part of the health monitor, as if the account is deleted or otherwise changed, the monitor will fail and the servers will be marked down.</td></tr>
<tr><td>BIG-IP Application Acceleration Manager</td><td colspan="2">You can optionally use the BIG-IP Application Acceleration Manager (AAM) module to help accelerate your Dynamics traffic. To use BIG-IP AAM, it must be fully licensed and provisioned on your BIG-IP system. Consult your F5 sales representative for details.
If you are using BIG-IP AAM, and want to use a custom Web Acceleration policy, it must have an Acceleration policy attached.</td></tr>
<tr><td>BIG-IP Application Security Manager</td><td colspan="2">You can optionally use the BIG-IP Application Security Manager (ASM) module to help protect and secure your Dynamics deployment. To use BIG-IP ASM, it must be fully licensed and provisioned on your BIG-IP system. Consult your F5 sales representative for details.</td></tr>
<tr><td>iRules</td><td colspan="2">In Advanced mode, you have the option of attaching iRules you create to the virtual server created by the iApp. For more information on iRules, see https://devcentral.f5.com/irules. Any iRules you want to attach must be present on the system at the time you are running the iApp.</td></tr>
</table>

Configuring the BIG-IP iApp for Microsoft Dynamics CRM 2011 and 2013

Use the following guidance to help configure the BIG-IP system for Microsoft Dynamics using the BIG-IP iApp template.

Downloading and importing the new iApp

The first task is to download and import the new Dynamics 2011 and 2013 iApp template.

To download and import the iApp

1. Open a browser and go to: *https://support.f5.com/kb/en-us/solutions/public/15000/800/sol15895.html*.
2. Follow the instructions to download the Dynamics iApp to a location accessible from your BIG-IP system.
3. Extract (unzip) the **f5.microsoft_dynamics_crm_2011_2013v1.0.0.tmpl** file (or newer, if applicable).
4. Log on to the BIG-IP system web-based Configuration utility.
5. On the Main tab, expand **iApp**, and then click **Templates**.
6. Click the **Import** button on the right side of the screen.
7. Click a check in the **Overwrite Existing Templates** box.
8. Click the **Browse** button, and then browse to the location you saved the iApp file.
9. Click the **Upload** button. The iApp is now available for use.

Getting Started with the iApp for Microsoft Dynamics

To begin the Dynamics iApp Template, use the following procedure.

1. Log on to the BIG-IP system.
2. On the Main tab, expand **iApp**, and then click **Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **Dynamics-iapp_.**
5. From the **Template** list, select **f5.microsoft_dynamics_crm_2011_2013.v1.0.0**. The Microsoft Dynamics CRM template opens.

Advanced options

If you select **Advanced** from the **Template Selection** list at the top of the page, you see Device and Traffic Group options for the application. This feature, new to v11, is a part of the Device Management configuration. This functionality extends the existing High Availability infrastructure and allows for clustering, granular control of configuration synchronization and granular control of failover. To use the Device and Traffic Group features, you must have already configured Device and Traffic Groups before running the iApp. For more information on Device Management, see the product documentation.

1. ***Device Group***
   To select a specific Device Group, clear the **Device Group** check box and then select the appropriate Device Group from the list.

2. ***Traffic Group***
   To select a specific Traffic Group, clear the **Traffic Group** check box and then select the appropriate Traffic Group from the list.

Template Options

This section contains general questions about the way you configure the iApp template.

1. ***Do you want to see inline help?***
   Choose whether you want to see informational and help messages inline throughout the template, or if you would rather hide this inline help. If you are unsure, we recommend having the iApp display the inline help.
   Important and critical notes are always shown, no matter which selection you make.

   - **Yes, show inline help text**
     Select this option to see all available inline help text.
   - **No, do not show inline help text**
     If you are familiar with this iApp template, or with the BIG-IP system in general, select this option to hide the inline help text.

2. ***Which configuration mode do you want to use?***
   Select whether you want to use F5 recommended settings, or have more granular, advanced options presented.

   - **Basic - Use F5's recommended settings**
     In basic configuration mode, options like load balancing method and parent profiles are all set automatically. The F5 recommended settings come as a result of extensive testing with web applications, so if you are unsure, choose Basic.
   - **Advanced - Configure advanced options**
     In advanced configuration mode, you have more control over individual settings and objects, such as server-side optimizations and advanced options like Slow Ramp Time and Priority Group Activation. You can also choose to attach iRules you have previously created to the Application Service. The Advanced option provides more flexibility for experienced users.

     As mentioned, advanced options in the template are marked with the Advanced icon: Advanced. If you are using Basic/F5 recommended settings, you can skip the questions with the Advanced icon.

Network

This section contains questions about your networking configuration.

1. ***What type of network connects clients to the BIG-IP system?***
   Choose the type of network that connects your clients to the BIG-IP system. If you choose WAN or LAN, the BIG-IP system uses this information to determine the appropriate TCP optimizations. If you choose WAN through another BIG-IP system, the system uses a secure an optimized tunnel (called an iSession tunnel) for traffic between BIG-IP systems on opposite sides of the WAN.
   Only choose this option if you have another BIG-IP system across the WAN that will be a part of this implementation.

   - **Local area network (LAN)**
     Select this option if most clients are connecting to the BIG-IP system on a LAN. This field is used to determine the appropriate TCP profile which is optimized for LAN clients. In this case, the iApp creates a TCP profile using the *tcp-lan-optimized* parent with no additional modifications.

- **Wide area network (WAN)**
  Select this option if most clients are connecting to the BIG-IP system over a WAN. This field is used to determine the appropriate TCP profile which is optimized for WAN clients. In this case, the iApp creates a TCP profile using the *tcp-wan-optimized* parent with no additional modifications.
- **WAN through another BIG-IP system**
  Select this option if client traffic is coming to this BIG-IP system from a remote BIG-IP system across a WAN. As mentioned in the introduction to this question, the iApp creates an iSession tunnel between this BIG-IP system and the BIG-IP system you will configure (or already have configured) on the other side of the WAN.

  If you select this option, you must have already initially configured the BIG-IP AAM for Symmetric Optimization. See the BIG-IP AAM documentation available on Ask F5 for specific instructions on configuring BIG-IP AAM for Symmetric Optimization.

2. ***Do you want to restrict client traffic to specific VLANs?*** Advanced
   The BIG-IP system allows you to restrict client traffic to specific VLANs that are present on the system. This can provide an additional layer of security, as you can allow or deny traffic from the VLANs you choose. By default, all VLANs configured on the system are enabled. If you select to enable or disable traffic on specific VLANs, you must specify the VLANs in the next question. The VLAN objects must already be configured on this BIG-IP system before you can select them.

   - **Enable traffic on all VLANs and Tunnels**
     Choose this option to allow traffic from all VLANs and Tunnels. If you select this option, the question asking about VLANs disappears. Continue with #3.
   - **Yes, enable traffic only on the VLANs I specify**
     Choose this option to restrict client traffic to specific VLANs that you specify in the following question. The system will accept Dynamics client traffic from these VLANs, and deny traffic from all other VLANs on the system.

     a. *On which VLANs should traffic be enabled or disabled?*
     Use this section to specify the VLANs that will accept client traffic. By default, all VLANs on the BIG-IP system appear in the Selected box, so click the VLANs and then use the Move buttons (<<) and (>>) to adjust list membership.

     Note

     If you choose to allow traffic from certain VLANs, when additional VLANs are added to the BIG-IP system at a later time, this iApp configuration will deny traffic from these VLANs by default. To accept traffic from these VLANs, you must re-enter the template and add the VLAN(s).

   - **Yes, disable traffic only on the VLANs I specify**
     Choose this option to deny client traffic from the specific VLANs that you specify in the following question. The system will refuse Dynamics client traffic from these VLANs, and accept traffic from all other VLANs on the system.

     a. *On which VLANs should traffic be enabled or disabled?*
     Use this section to specify the VLANs that should not accept client traffic. By default, all VLANs on the BIG-IP system appear in the Selected box, so it is critical in this case that you click the VLANs and then use the Move button (>>) to adjust list membership.

     Warning

     If you choose to disable certain VLANs, you must move at least one VLAN to the Options list. Otherwise, the system will deny traffic from all VLANs on the box, and the configuration, although valid, will not pass any traffic.

3. ***What type of network connects servers to the BIG-IP system?***
   Choose the type of network that connects your servers to the BIG-IP system. Similar to the question about clients connecting to the BIG-IP system, if you choose WAN or LAN, the system uses this information to determine the appropriate TCP optimizations. If you choose WAN through another BIG-IP system, the system uses a secure an optimized tunnel (called an iSession tunnel) for traffic between BIG-IP systems on opposite sides of the WAN. Only choose this option if you have another BIG-IP system across the WAN that will be a part of this Microsoft Dynamics implementation.

- **Local area network (LAN)**
  Select this option if the servers connect to the BIG-IP system on a LAN. This field is used to determine the appropriate TCP profile. In this case, the iApp creates a TCP profile using the *tcp-lan-optimized* parent with no additional modifications.
- **Wide area network**
  Select this option if the servers connect to the BIG-IP system over a WAN. This field is used to determine the appropriate TCP profile. In this case, the iApp creates a TCP profile using the *tcp-wan-optimized* parent with no additional modifications.
- **WAN through another BIG-IP system**
  Select this option if servers are across a WAN behind another BIG-IP system. As mentioned in the introduction to this question, the iApp creates an iSession tunnel between this BIG-IP system and the BIG-IP system you will configure (or already have configured) on the other side of the WAN.

  If you select this option, you must have already initially configured the BIG-IP AAM for Symmetric Optimization. See the BIG-IP AAM documentation available on Ask F5 for specific instructions on configuring BIG-IP AAM for Symmetric Optimization.

4. ***Where will the virtual servers be in relation to the Dynamics CRM servers?***
   Select whether your BIG-IP virtual servers are on the same subnet as your Dynamics servers, or on different subnets. This setting is used to determine the SNAT (secure NAT) and routing configuration.

   - **BIG-IP virtual server IP and Dynamics CRM servers are on the same subnet**
     If the BIG-IP virtual servers and Dynamics servers are on the same subnet, SNAT is configured on the BIG-IP virtual server and you must specify the number of concurrent connections.

     a. *How many connections to you expect to each Dynamics CRM server?*
        Select whether you expect more or fewer than 64,000 concurrent connections to each server. This answer is used to determine what type of SNAT that system uses. A SNAT is an object that maps the source client IP address in a request to a translation address defined on the BIG-IP device. The system configures SNAT Auto Map (fewer than 64,000) or a SNAT pool (more than 64,000).

        - **Fewer than 64,000 concurrent connections**
          Select this option if you expect fewer than 64,000 concurrent connections per Dynamics CRM server. With this option, the system applies SNAT Auto Map, doesn't require any additional IP addresses, as an existing self IP address is used for translation. Continue with *Virtual Server and Pools on page 16.*
        - **More than 64,000 concurrent connections**
          Select this option if you have a very large deployment and expect more than 64,000 connections at one time. The iApp creates a SNAT Pool, for which you need one IP address for each 64,000 connections you expect.

          i). Create a new SNAT pool or use an existing one?
          If you have already created a SNAT pool on the BIG-IP system, you can select it from the list. Otherwise, the system creates a new SNAT pool with the addresses you specify.

          - **Create a new SNAT pool**
            Select this option (the default) to enable the system to create a new SNAT pool. You must specify the appropriate number of IP addresses in the next question.

            1). What are the IP addresses you want to use for the SNAT pool?
            Specify one otherwise unused IP address for every 64,000 concurrent connections you expect, or fraction thereof. Click **Add** for additional rows. Do not use any self IP addresses on the BIG-IP system.

          - **Select a SNAT pool**
            Select the SNAT pool you created for this deployment from the list.

            Important

            If you choose more than 64,000 connections, but do not specify enough SNAT pool address(es), after the maximum connection limit of 64,000 concurrent connections per Dynamics CRM server is reached, new requests fail.

- **BIG-IP virtual servers and Dynamics CRM servers are on different subnets**
  If the BIG-IP virtual servers and servers are on different subnets, the following question appears.

  a. *How have you configured routing on your Dynamics CRM servers?*
  If you chose different subnets, this question appears asking whether the Dynamics CRM servers use this BIG-IP system's self IP address as their default gateway. Select the appropriate answer.

  - **Servers have a route to clients through the BIG-IP system**
    Choose this option if the servers use the BIG-IP system as their default gateway. In this case, no configuration is needed to support your environment to ensure correct server response handling. Continue with the next section.
  - **Servers do not have a route to clients through the BIG-IP system**
    If the Dynamics servers do not use the BIG-IP system as their default gateway, SNAT is configured on the BIG-IP virtual server and you must select the expected number of concurrent connections in the next question.

    i). *How many connections to you expect to each Dynamics CRM server?*
    Select whether you expect more or fewer than 64,000 concurrent connections to each server. This answer is used to determine what type of SNAT that system uses. A SNAT is an object that maps the source client IP address in a request to a translation address defined on the BIG-IP device. The system configures SNAT Auto Map (fewer than 64,000) or a SNAT pool (more than 64,000).

    - **Fewer than 64,000 concurrent connections**
      Select this option if you expect fewer than 64,000 concurrent connections per Dynamics CRM server. With this option, the system applies SNAT Auto Map, doesn't require any additional IP addresses, as an existing self IP address is used for translation. Continue with the *SSL Encryption* section.
    - **More than 64,000 concurrent connections**
      Select this option if you have a very large deployment and expect more than 64,000 connections at one time. The iApp creates a SNAT Pool, for which you need one IP address for each 64,000 connections you expect.

      1). *Create a new SNAT pool or use an existing one?*
      If you have already created a SNAT pool on the BIG-IP system, you can select it from the list. Otherwise, the system creates a new SNAT pool with the addresses you specify.

      * **Create a new SNAT pool**
        Select this option (the default) to enable the system to create a new SNAT pool. You must specify the appropriate number of IP addresses in the next question.

        a). *Which IP addresses do you want to use for the SNAT pool?*
        Specify one otherwise unused IP address for every 64,000 concurrent connections you expect, or fraction thereof. Click **Add** for additional rows. Do not use any self IP addresses on the BIG-IP system.

      * **Select a SNAT pool**
        Select the SNAT pool you created for this deployment from the list.

      Important

      If you choose more than 64,000 connections, but do not specify enough SNAT pool address(es), after the maximum connection limit of 64,000 concurrent connections per Dynamics CRM server is reached, new requests fail.

Access Policy Manager (BIG-IP APM)

The section in this scenario asks about the BIG-IP APM. You must have APM fully licensed and provisioned to use APM. If you are not deploying APM, continue with the next section. As mentioned in the prerequisites, if you are deploying APM, you must have configured the BIG-IP system for DNS and NTP. See *Appendix E: Configuring DNS and NTP on the BIG-IP system on page 47* for instructions.

1. ***Provide secure authentication with BIG-IP Access Policy Manager?***
   Specify whether you want to deploy BIG-IP APM to provide proxy authentication and secure remote access for Microsoft Dynamics CRM.

- **No, do not provide secure authentication using BIG-IP APM**
  Select this option if you do not want to use the BIG-IP APM at this time. You can always reconfigure the iApp template at a later date should you decide to add BIG-IP APM functionality.
- **Yes, provide secure authentication using BIG-IP APM**
  Select this option if you want to use the BIG-IP APM to provide proxy authentication and secure remote access for your Dynamics deployment.

  a. *Should APM create a pool of Active Directory servers for authentication requests?*
  Select whether you want the BIG-IP APM to create a pool of multiple Active Directory servers, or to use a single Active Directory server to service authentication requests.

  We recommend using a pool of servers, which enables high availability and redundancy.

  - **No, use a single Active Directory server**
    Select this option if you want APM to use a single Active Directory server for authentication requests.

    i). *Which Active Directory server IP address in your domain can this BIG-IP system contact?*
    Specify the IP address of the Active Directory server you want the BIG-IP APM to use for servicing authentication requests.

  - **Yes, create a pool of Active Directory servers**
    Select this option have multiple Active Directory servers you want to use for implementation. The iApp creates a load balancing pool for the Active Directory servers you specify.

    i). *Which Active Directory servers in your domain can this BIG-IP system contact?*
    Specify both the FQDN and IP address of each Active Directory server you want the BIG-IP APM to use for servicing authentication requests. Click **Add** to include additional servers.

  b. *What is the FQDN of your Active Directory domain for your Dynamics CRM users?*
  Specify the FQDN of the Active Directory deployment for your Dynamics users. This is the FQDN for your domain, such as example.com, rather than the FQDN for any specific host.

  c. *Does your Active Directory domain allow anonymous binding?*
  Select whether anonymous binding is allowed in your Active Directory environment.

  - **Yes, anonymous binding is allowed**
    Select this option if anonymous binding is allowed. No further information is required.
  - **No, credentials are required for binding**
    If credentials are required for binding, you must specify an Active Directory user name and password for use in the AAA Server.

    i). *Which Active Directory user with administrative permissions do you want to use?*
    Type a user name with administrative permissions.

    ii). *What is the password associated with that account?*
    Type the associated password.

  d. *How do you want to handle health monitoring for this pool?*
  Specify whether you want the template to create a new LDAP monitor or a new ICMP monitor, or if you select an existing monitor. For more accurate monitoring, we recommend using an LDAP monitor.

  - **Select an existing monitor for the Active Directory pool**
    Select this option if you have already created a health monitor (only monitors with a **Type** of LDAP or External can be used) for the Active Directory pool that will be created by the template. If you want to create a health monitor, but have not already done so, you must exit the template and create the object before it becomes available from the list.

    The iApp allows you to select monitors that are a part of another iApp Application Service. If you select a monitor that is a part of another Application Service, be aware that any changes you make to the monitor in the other Application Service will apply to this Application Service as well.

i). Which monitor do you want to use?
From the list, select the LDAP or External monitor you created to perform health checks for the Active Directory pool created by the template. Only monitors that have a Type value of LDAP or External appear in this list. Continue with the next section.

- **Use a simple ICMP monitor for the Active Directory pool**
Select this option if you only want a simple ICMP monitor for the Active Directory pool. This monitor sends a ping to the servers and marks the server UP if the ping is successful.
Continue with the next section.

- **Create a new LDAP monitor for the Active Directory pool**
Select this option if you want the template to create a new LDAP monitor for the Active Directory pool. You must answer the following questions:

i). Which Active Directory user name should the monitor use?
Specify an Active Directory user name for the monitor to use when attempting to log on as a part of the health check. This should be a user account created specifically for this health monitor, and *must* be set to never expire.

ii). What is the associated password?
Specify the password associated with the Active Directory user name.

iii). What is the LDAP tree for this user account?
Specify the LDAP tree for the user account. As noted in the inline help, ADSI editor, an tool for Active Directory LDAP administration, is useful for determining the correct LDAP tree value. For example, if the user name is 'user1' which is in the organizational unit 'F5 Users' and is in the domain 'f5.example.com', the LDAP tree would be: ou=F5 Users, dc=f5, dc=example, dc=com.

iv). Does your Active Directory domain require a secure protocol for communication?
Specify whether your Active Directory implementation requires SSL or TLS for communication, or does not require a secure protocol. This determines the port the health monitor uses.

- **No, a secure protocol is not required**
Select this option if your Active Directory domain does not require a secure protocol.
- **Yes, SSL communication is required**
Select this option if your Active Directory domain requires SSL communication. The health check uses port 636 as the Alias Service Port.
- **Yes, TLS communication is required**
Select this option if your Active Directory domain requires TLS communication. The health check uses port 389 as the Alias Service Port.

v). How many seconds between Active Directory health checks?
Specify how many seconds the system should use as the health check Interval for the Active Directory servers. We recommend the default of 10 seconds.

vi). Which port is used for Active Directory communication?
Specify the port being used by your Active Directory deployment. The default port displayed here is determined by your answer to the secure protocol question. When using the TLS security protocol, or no security, the default port 389. The default port used when using the SSL security protocol is 636.

SSL Encryption

Before running the template you should have already imported a certificate and key onto the BIG-IP system. While the BIG-IP system does include a self-signed SSL certificate that can be used internally or for testing, we strongly recommend importing a certificate and key issued from a trusted Certificate Authority for processing client-side SSL.

For information on SSL certificates on the BIG-IP system, see the online help or the *Managing SSL Certificates for Local Traffic* chapter in the ***Configuration Guide for BIG-IP Local Traffic Manager*** *available at http://support.f5.com/kb/en-us.html.*

1. ***How should the BIG-IP system handle SSL traffic?***
There are four options for configuring the BIG-IP system for SSL traffic (only two are available if you deployed BIG-IP APM in the previous section. Select the appropriate mode for your configuration.

- **Encrypt to clients, plaintext to servers (SSL Offload)**
  Choose this method if you want the BIG-IP system to offload SSL processing from the servers. You need a valid SSL certificate and key for this method.

  a. *Which Client SSL profile do you want to use?* **Advanced**
  Select whether you want the iApp to create a new Client SSL profile, or if you have already created a Client SSL profile which contains the appropriate SSL certificate and key.

  Unless you have requirements for configuring specific Client SSL settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **SSL** : **Client** to create a Client SSL profile. To select any new profiles you create, you need to restart or reconfigure this template.

  - *Select an existing Client SSL profile*
    If you created a Client SSL profile for this implementation, select it from the list. If you select an existing Client SSL profile, the rest of the questions in this section disappear. Continue with the next section.
  - **Create a new Client SSL profile**
    Select this option for the iApp to create a new Client SSL profile

    i). *Which SSL certificate do you want to use?*
    Select the SSL certificate you imported for this implementation.

    ii). *Which SSL private key do you want to use?*
    Select the associated SSL private key.

    iii). *Which intermediate certificate do you want to use?* **Advanced**
    If your deployment requires an intermediate or chain certificate, select the appropriate certificate from the list. Immediate certificates are intended to create a chain of trust between the CA that signed the certificate and the CA that is already trusted by the recipient of the certificate. This allows the recipient to verify the validity of the certificates presented, even when the signing CA is unknown.

- **Terminate SSL from clients, re-encrypt to servers (SSL Bridging)**
  Choose this method if you want the BIG-IP system to terminate SSL to process it, and then re-encrypt the traffic to the servers (SSL Bridging). You need a valid SSL certificate and key for the client-side, and optionally for the server-side (see #b).

  a. *Which Client SSL profile do you want to use?* **Advanced**
  Select whether you want the iApp to create a new Client SSL profile, or if you have already created a Client SSL profile which contains the appropriate SSL certificate and key.

  Unless you have requirements for configuring specific Client SSL settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **SSL** : **Client** to create a Client SSL profile. To select any new profiles you create, you need to restart or reconfigure this template.

  - *Select an existing Client SSL profile*
    If you created a Client SSL profile for this implementation select it from the list. If you select an existing Client SSL profile, the rest of the questions in this section disappear. Continue with the next section.
  - **Create a new Client SSL profile**
    Select this option for the iApp to create a new Client SSL profile

    i). *Which SSL certificate do you want to use?*
    Select the SSL certificate you imported for this implementation.

    ii). *Which SSL private key do you want to use?*
    Select the associated SSL private key.

    iii). *Which intermediate certificate do you want to use?* **Advanced**
    If your deployment requires an intermediate or chain certificate, select the appropriate certificate from the list.

    Immediate certificates are intended to create a chain of trust between the CA that signed the certificate and the CA that is already trusted by the recipient of the certificate. This allows the recipient to verify the validity of the certificates presented, even when the signing CA is unknown.

b. *Which Server SSL profile do you want to use?*
Select whether you want the iApp to create the F5 recommended Server SSL profile, or if you want to choose a Server SSL profile you already created. In this scenario, the BIG-IP system is acting as an SSL client and by default, we assume the servers do not expect the BIG-IP system to present its client certificate on behalf of clients traversing the virtual server. If your servers expect the BIG-IP system to present a client certificate, you must create a custom Server SSL profile with the appropriate certificate and key.

The default, F5 recommended Server SSL profile uses the serverssl parent profile. For information about the ciphers used in the Server SSL profile, see http://support.f5.com/kb/en-us/solutions/public/8000/800/sol8802.html.

- **Encrypted traffic is forwarded without decryption (SSL pass-through)**
Choose this method if you do not want the BIG-IP system to do anything with encrypted traffic and simply send it to the Dynamics CRM servers. This is similar to SSL bridging, although in this case the system does not decrypt then re-encrypt the traffic, it only sends it on to the servers without modification.
- **Plaintext to clients, encrypt to servers**
Choose this method if you want the BIG-IP system to accept plain text from the clients and then encrypt it before sending it to the servers.

  Unless you have requirements for configuring specific Server SSL settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **SSL** : **Server** to create a Server SSL profile. To select any new profiles you create, you need to restart or reconfigure this template.

  The default, F5 recommended Server SSL profile uses the *serverssl* parent profile. For information about the ciphers used in the Server SSL profile, see http://support.f5.com/kb/en-us/solutions/public/8000/800/sol8802.html.

- **Plaintext to both clients and servers**
Choose this method if the BIG-IP system is not sending or receiving any SSL traffic in this implementation.

Application Firewall Manager (BIG-IP AFM)

This section gathers information about BIG-IP Advanced Firewall Manager if you want to use it to protect the Dynamics deployment. For more information on configuring BIG-IP AFM, see http://support.f5.com/kb/en-us/products/big-ip-afm.html, and then select your version.

1. ***Do you want to use BIG-IP AFM to protect your application?***
Choose whether you want to use BIG-IP AFM, F5's network firewall, to secure this Dynamics deployment. If you choose to use BIG-IP AFM, you can restrict access to the Dynamics virtual server to a specific network or IP address. See the BIG-IP AFM documentation for specific details on configuring AFM.

   - **No, do not use Application Firewall Manager**
Select this option if you do not want to enable BIG-IP AFM at this time. You can always re-enter the template at a later date to enable BIG-IP AFM. Continue with the next section.
   - *Select an existing AFM policy from the list*
If you already created a BIG-IP AFM policy for this implementation, select it from the list. Continue with ***c***.
   - **Yes, use F5's recommended AFM configuration**
Select this option if you want to enable BIG-IP AFM using F5's recommended configuration.

     a. *Do you want to restrict access to your application by network or IP address?*
Choose whether you want to restrict access to the Dynamics implementation via the BIG-IP virtual server.

        - **No, do not restrict source addresses (allow all sources)**
By default, the iApp configures the Advanced Firewall module to accept traffic destined for the Dynamics virtual server from all sources. If you do not have a need to restrict access to the virtual server, leave this option selected and then continue with ***b***.
        - **Restrict source addresses**
Select this option if you want to restrict access to the Dynamics virtual server by IP address or network address.

i). *What IP or network addresses should be allowed to access your application?*
Specify the IP address or network access that should be allowed access to the Dynamics virtual server. You can specify a single IP address, a list of IP addresses separated by spaces (not commas or other punctuation), a range of IP addresses separated by a dash (for example **192.0.2.10-192.0.2.100**), or a single network address, such as **192.0.2.200/24**.

b. *How do you want to control access to your application from sources with a low reputation score?*
The BIG-IP AFM uses an IP intelligence database to categorize IP addresses coming into the system. Choose what you want the system to do for sources that are attempting to access the Dynamics virtual server with a low reputation score. For more information, see the BIG-IP AFM documentation.

Important: You must have an active IP Intelligence license for this feature to function. See *https://f5.com/products/modules/ip-intelligence-services* for information.

- **Allow all sources regardless of reputation**
  Select this option to allow all sources, without taking into consideration the reputation score.
- **Reject access from sources with a low reputation**
  Select this option to reject access to the Dynamics virtual server from any source with a low reputation score.
- **Allow but log access from sources with a low reputation**
  Select this option to allow access to the Dynamics virtual server from sources with a low reputation score, but add an entry for it in the logs.

c. *Would you like to stage a policy for testing purposes?*
Choose whether you want to stage a firewall policy for testing purposes. A staged policy allows you to evaluate the effect a policy has on traffic by analyzing the system logs, without actually modifying traffic based on the firewall rules. You must already have a policy on the system in order to select it.

- **Do not apply a staging policy**
  Select this option if you do not want to apply a logging profile at this time. You can always re-enter the template at a later date to add a logging profile. Continue with the next question.
- *Select an existing policy from the list*
  If you have already created a firewall policy for this implementation, select it from the list. Only policies that already exist on the system appear in the list. To create a new policy, on the Main tab, click **Security > Network Firewall > Policies**. Specific instructions for creating a firewall policy is outside the scope of this iApp and deployment guide.

d. *Which logging profile would you like to use?*
Choose whether you or not you want to use a logging profile for this AFM implementation. You can configure the BIG-IP system to log detailed information about BIG-IP system Network Firewall events and store those logs on the BIG-IP system or a remote logging server (supports syslog and Splunk). If you want to use a logging profile, we recommend creating one outside this template. The list only contains profiles with Network Firewall enabled.

- **Do not apply a logging profile**
  Select this option if you do not want to apply a logging profile at this time. You can always re-enter the template at a later date to add a logging profile. Continue with the next question.
- *Select an existing logging profile from the list*
  If you have already created a logging profile for this implementation, select it from the list. You must create a profile before it is available in the list. To create a logging profile, on the Main tab, click **Security > Event Logs > Logging Profiles**. Specific instructions for creating a logging profile is outside the scope of this iApp and deployment guide. See the online help or the *About Local Logging with the Network Firewall* chapter of the ***BIG-IP Network Firewall: Policies and Implementations*** guide for more information.

Virtual Server and Pools

This section gathers information about your Dynamics CRM deployment that is used in the BIG-IP virtual server and load balancing pool.

1. ***What IP address do you want to use for the virtual server?***
   Type the IP address you want to use for the BIG-IP virtual server. This is the address clients use (or a DNS entry resolves to this address) to access the Dynamics CRM deployment via the BIG-IP system.

If necessary for your configuration, this can be a network address to create a network virtual server (you must specify an IP mask in the following question for a network virtual server). A network virtual server is a virtual server whose IP address has no bits set in the host portion of the IP address (that is, the host portion of its IP address is 0), allowing the BIG-IP system to direct client connections that are destined for an entire range of IP addresses, rather than for a single destination IP address. Thus, when any client connection targets a destination IP address that is in the network specified by the virtual server IP address, the system can direct that connection the pool of Dynamics CRM servers.

2. ***If using a network virtual address, what is the IP mask?*** Advanced
   If you specified a network address for the virtual server (allowing the virtual server to handle multiple IP addresses), you must enter the full network mask representing the address range. If you specified a single address for the virtual server, you may leave this field blank.

3. ***What port do you want to use for the virtual server?***
   Type the port number you want to use for the BIG-IP virtual server. For Dynamics deployments, this is typically 80 (HTTP) or 443 (HTTPS). The default port in the box is based on your answer to the How should the system handle SSL traffic question.

4. ***Which FQDNs will clients use to access the servers?***
   Type each fully qualified domain name clients will use to access the Dynamics CRM deployment. Click the **Add** button to insert additional rows. If you only have one FQDN, do not click Add.

5. ***Do you want to redirect inbound HTTP traffic to HTTPS?*** Advanced
   This question only appears if you selected SSL Offload or SSL Bridging in the SSL question.

   Select whether you want the BIG-IP system to automatically redirect HTTP traffic to the HTTPS virtual server. This is useful when users forget to use HTTPS when attempting to connect to the Microsoft Dynamics CRM deployment.

   - **Redirect HTTP to HTTPS**
     Select this option to redirect HTTP traffic to HTTPS. If you select this option (the default), the BIG-IP system attaches a very small redirect iRule to the virtual server.

     a. *From which port should traffic be redirected?*
        Type the port number for the traffic that you want to redirect to HTTPS. The most common is port 80 (the default).

   - **Do not redirect HTTP to HTTPS**
     Select this option if you do not want to enable the automatic redirect.

6. ***Which HTTP profile do you want to use?*** Advanced
   The HTTP profile contains settings for instructing the BIG-IP system how to handle HTTP traffic. Choose whether you want the iApp to create a new HTTP profile or if you have previously created an HTTP profile for this deployment.

   Unless you have requirements for configuring specific HTTP settings, we recommend allowing the iApp to create a new profile. To select a profile from the list, it must already be present on the BIG-IP system. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Services : HTTP** to create a HTTP profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - *Select an existing HTTP profile from the list*
     If you already created an HTTP profile for this implementation, select it from the list.

   - **Create a new HTTP profile (recommended)**
     Select this option for the iApp to create a new HTTP profile.

     a. *Should the BIG-IP system insert the X-Forwarded-For header?* Advanced
        Select whether you want the BIG-IP system to insert the X-Forwarded-For header in the HTTP header for logging purposes.

        - **Insert the X-Forwarded-For header**
          Select this option if you want the system to include the X-Forwarded-For header. You may have to perform additional configuration on your Dynamics servers to log the value of this header. For more information on configuring logging see *Appendix C: Using X-Forwarded-For to log the client IP address in IIS 7.0, 7.5, and 8 (optional) on page 43*.

        - **Do not insert the X-Forwarded-For header**
          Select this option if you do not want the system to include X-Forwarded-For in the HTTP header.

7. ***Which persistence profile do you want to use?*** Advanced
   By using persistence, the BIG-IP system tracks and stores session data, such as the specific pool member that serviced a client request, ensuring client requests are directed to the same pool member throughout the life of a session or during subsequent sessions.

   Unless you have requirements for configuring specific persistence settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Persistence** to create a persistence profile. To select any new profiles you create, you need to restart or reconfigure this template. Select one of the following persistence options:

   - **Use Cookie Persistence (recommended)**
     This is the recommended option for Dynamics CRM. Leave this option to have the BIG-IP system create a new cookie persistence profile (cookie insert mode). With Cookie persistence, the BIG-IP system uses an HTTP cookie stored on the client's computer to allow the client to reconnect to the same server previously visited.
   - **Use Source IP Address persistence**
     Select this option if you want to use the Source IP address (also known as simple) persistence. With this mode, the BIG-IP system assigns the built-in Source Address Affinity persistence type, and directs session requests to the same server based only on the source IP address.
   - **Do not use persistence**
     If your implementation does not require persistent connections, select this option.
   - *Select an existing persistence profile*
     If you have previously created a persistence profile, you have the option of selecting it instead of allowing the iApp to create a new one. From the list, select an existing persistence profile. We recommend using a persistence profile that uses Cookie persistence, Insert mode.

8. ***Do you want to create a new pool or use an existing one?***
   A load balancing pool is a logical set of servers, grouped together to receive and process traffic. When clients attempt to access the application via the BIG-IP virtual server, the BIG-IP system distributes requests to any of the servers that are members of that pool.

   - *Select an existing pool*
     If you have already created a pool for your Dynamics CRM servers, you can select it from the list.
     If you do select an existing pool, all of the rest of the questions in this section disappear.
   - **Do not use a pool**
     If you are deploying this iApp in such a way that you do not need a pool of Dynamics CRM servers, select this option. If you specified the servers are connected to the BIG-IP system over the WAN through another BIG-IP system, this is the default option, as the system sends the traffic across the iSession tunnel to the other BIG-IP system to be distributed to the servers.
   - **Create a new pool**
     Leave this default option to create a new load balancing pool and configure specific options.

     a. *Which load balancing method do you want to use?* Advanced
        Specify the load balancing method you want to use for this Dynamics CRM server pool. We recommend the default, **Least Connections (member)**.

     b. *Do you want to give priority to specific groups of servers?* Advanced
        Select whether you want to use Priority Group Activation. Priority Group Activation allows you to segment your servers into priority groups. With Priority Group Activation, the BIG-IP system load balances traffic according to the priority number you assign to the pool members. A higher number indicates higher priority. Traffic is only sent to the servers with the highest priority, unless the number of available servers in that priority group falls below the value you specify as the minimum. The BIG-IP then sends traffic to the group of servers with the next highest priority, and so on. See the BIG-IP documentation for more details.

        - **Do not use Priority Group Activation (recommended)**
          Select this option if you do not want to enable Priority Group Activation.
        - **Use Priority Group Activation**
          Select this option if you want to enable Priority Group Activation.

You must add a priority to each server in the Priority box described in #c.

i). What is the minimum number of active members for each priority group?
Specify the minimum number of servers that must be active to continue sending traffic to the priority group. If the number of active servers falls below this minimum, traffic will be sent to the group of servers with the next highest priority group number.

c. *Which Dynamics CRM servers should be included in this pool?*
Specify the IP address(es) of your Dynamics CRM servers. If you have existing nodes on this BIG-IP system, you can select them from the list, otherwise type the addresses. You can optionally add a Connection Limit. If you enabled Priority Group Activation, you must also specify a Priority for each device. Click **Add** to include additional servers.

Delivery Optimization

In this section, you answer questions about how you want the BIG-IP system to optimize the delivery of your Dynamics traffic.

1. ***Use the BIG-IP Application Acceleration Manager?***
Choose whether you want to use the BIG-IP Application Acceleration Manager (formerly known as WebAccelerator). BIG-IP Application Acceleration Manager helps accelerate your Dynamics CRM traffic.

   - **Yes, use BIG-IP AAM (recommended)**
   Select this option to enable BIG-IP AAM.
   - **No, do not use BIG-IP AAM**
   Select this option if you do not want to enable BIG-IP AAM at this time.

2. ***Which Web Acceleration profile do you want to use for caching?*** Advanced
Select whether you want the system to create a new Web Acceleration profile, or if you have already created a Web Acceleration profile for use in this deployment. The Web Acceleration profile contains the caching settings for this implementation.

   Unless you have requirements for configuring specific acceleration settings (such as specific allowing/denying specific URIs), we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Services : Web Acceleration** to create an acceleration profile. To select any new profiles you create, you need to restart or reconfigure this template.

   Note if using BIG-IP AAM:
   If you are using BIG-IP AAM, and want to select a custom Web Acceleration profile for caching you have already created, it must have an AAM application enabled, otherwise it does not appear in the list of caching profiles. If you want access to all Web Acceleration profiles on the box, then you must choose No to the use BIG-IP AAM question. Use a custom Web Acceleration profile only if you need to define specific URIs that should or should not be cached.

   Note if not using BIG-IP AAM:
   If you are not using BIG-IP AAM, we recommend you only use a custom Web Acceleration profile if you need to define specific URIs which should or should not be cached.

   - **Create a profile based on optimized-caching (recommended)**
   Leave this default option to create a new Web Acceleration profile for caching.
   - **Do not use caching**
   This question does not appear if you chose to enable BIG-IP AAM
   Select this option if you do not want to enable caching on the BIG-IP system for this implementation.
   - *Select an existing Web Acceleration profile*
   If you have already created a Web Acceleration profile for your Dynamics CRM servers, you can select it from the list.

3. ***Do you want to insert the X-WA-Info header?*** Advanced
This question only appears if you chose to enable BIG-IP AAM

The BIG-IP system can optionally insert an X-WA-Info response header that includes specific codes describing the properties and history of the object. The X-WA-Info response header is for informational and debugging purposes only and provides a way for you to assess the effectiveness of your acceleration policy rules.

By default, the AAM X-WA-info header is not included in the response from the BIG-IP system. If you choose to enable this header, you have two options, Standard and Debug. In Standard mode, the BIG-IP system inserts an HTTP header that includes numeric codes which indicate if and how each object was cached. In Debug mode, the BIG-IP system includes additional information which may help for extended troubleshooting.

- **Do not insert the header (recommended)**
  Select this option if you do not want to insert the X-WA-Info header. Typically F5 recommends not inserting the header unless instructed to do so by an F5 Technical Support Engineer.
- **Insert the Standard header**
  Select this option if you want to insert the Standard header. For detailed information on the numeric codes used by the header, see *http://support.f5.com/kb/en-us/solutions/public/13000/700/sol13798.html*
- **Insert the Debug header**
  Select this option if you want to insert the Debug header for extended troubleshooting.

4. ***Do you want to use the legacy AAM performance monitor?*** **Advanced**
   This question only appears if you chose to enable BIG-IP AAM

   Enabling the legacy AAM performance monitor can adversely affect system performance. This monitor is primarily used for legacy AAM performance monitoring and debugging purposes, and can adversely affect system performance. The BIG-IP Dashboard provides performance graphs and statistics related to AAM.

   - **Do not enable the legacy performance monitor (recommended)**
     Select this option if you do not want to enable the legacy monitor.
   - **Enable the legacy performance monitor**
     Select this option if you want to enable the legacy performance monitor. Remember enabling this legacy monitor can impact overall system performance.

     a. *For how many days should the BIG-IP system retain the data?*
        Specify the number of days the BIG-IP system should retain the legacy performance data.

5. ***Which acceleration policy do you want to use?*** **Advanced**
   This question only appears if you chose to enable BIG-IP AAM

   Unless you have created a custom BIG-IP AAM policy for this deployment, we recommend you select the default policy (**Generic Policy - Enhanced**).

6. ***Which compression profile do you want to use?***
   Compression improves performance and end user experience for Web applications that suffer from WAN latency and throughput bottlenecks. Compression reduces the amount of traffic sent to the client to complete a transaction.

   Unless you have requirements for configuring specific compression settings, we recommend allowing the iApp to create a new profile. F5 recommends the default profile which is optimized for Dynamics CRM servers. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Services : HTTP Compression** to create a compression profile. To select any new profiles you create, you need to restart or reconfigure this template.

7. ***How do you want to optimize client-side connections?*** **Advanced**
   The client-side TCP profile optimizes the communication between the BIG-IP system and the client by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   Unless you have requirements for configuring specific TCP optimization settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Protocol : TCP** to create a TCP profile. To select any new profiles you create, you need to restart or reconfigure this template.

- **Create the appropriate tcp-optimized profile (recommended)**
  Select this option to have the system create the recommended TCP profile. The parent profile (either WAN or LAN optimized) is determined by your selection to the "What type of network connects clients to the BIG-IP system" question.

- *Select the TCP profile you created from the list*
  If you created a custom TCP profile for the Dynamics CRM servers, select it from the list.

Server offload

In this section, you configure the options for offloading tasks from the Dynamics CRM servers. This entire section only appears if you selected Advanced mode.

1. ***Which OneConnect profile do you want to use?*** Advanced
   OneConnect (connection pooling or multiplexing) improves server scalability by reducing load associated with concurrent connections and connection rate to Dynamics CRM servers. When enabled, the BIG-IP system maintains one connection to each Dynamics CRM server which is used to send requests from multiple clients.

   Unless you have requirements for configuring specific settings, we recommend allowing the iApp to create a new profile. F5 recommends the default profile which is optimized for Dynamics CRM servers. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Other : OneConnect** to create a OneConnect profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - **Create a profile based on the oneconnect parent (recommended)**
     Select this option to have the system create the recommended OneConnect profile. The system uses the oneconnect parent profile with a Source Mask setting of 255.255.255.255.
   - **Do not use a OneConnect profile**
     Select this option if you do not require the BIG-IP system to perform connection pooling using a OneConnect profile.
   - *Select the OneConnect profile you created from the list*
     If you created a custom OneConnect profile for the Dynamics CRM servers, select it from the list.

2. ***Which NTLM profile do you want to use?*** Advanced
   The NTLM profile optimizes network performance when the system is processing NTLM traffic. When both an NTLM profile and a OneConnect profile are enabled, the system can take advantage of server-side connection pooling for NTLM connections.

   If you are creating this template in a BIG-IP partition other than /Common, you must create a custom NTLM profile and select it from this list. See *Troubleshooting on page 28* for detailed information.

   If your environment uses NTLM, we recommend allowing the iApp to create a new profile unless you have requirements for configuring specific settings. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Other : NTLM** to create a NTLM profile. To select any new profiles you create, you need to restart or reconfigure this template.

   - **Use F5's recommended NTLM profile**
     Select this option to have the system create the recommended NTLM profile. The system uses the ntlm parent profile.
   - **Do not use NTLM (recommended)**
     Select this option if you do not use NTLM authentication in your Dynamics CRM implementation.
   - *Select the NTLM profile you created from the list*
     If you created a custom NTLM profile for the Dynamics CRM servers, select it from the list.

3. ***How do you want to optimize server-side connections?*** Advanced
   The server-side TCP profile optimizes the communication between the BIG-IP system and the server by controlling the behavior of the traffic which results in higher transfer rates, improved connection reliability and increased bandwidth efficiency.

   Unless you have requirements for configuring specific TCP optimization settings, we recommend allowing the iApp to create a new profile. Creating a custom profile is not a part of this template; see **Local Traffic** >> **Profiles** : **Protocol : TCP** to create a TCP profile. To select any new profiles you create, you need to restart or reconfigure this template.

- **Create the appropriate tcp-optimized profile (recommended)**
  Select this option to have the system create the recommended TCP profile. The parent profile (either WAN or LAN optimized) is determined by your selection to the "What type of network connects servers to the BIG-IP system" question.
- *Select the TCP profile you created from the list*
  If you created a custom TCP profile for the Dynamics CRM servers, select it from the list.

4. ***Do you want the BIG-IP system to queue TCP requests?***
   Select whether you want the BIG-IP system to queue TCP requests. TCP request queuing provides the ability to queue connection requests that exceed the capacity of connections for a pool, as determined by the connection limit. Consequently, instead of dropping connection requests that exceed the capacity of a pool, TCP request queuing enables those connection requests to reside within a queue according to defined conditions until capacity becomes available. For more information on TCP Request Queuing, see the *Preventing TCP Connection Requests From Being Dropped* chapter in the ***BIG-IP Local Traffic Manager: Implementations*** guide, available on AskF5.

   Important

   TCP Request Queuing is an advanced feature and should be used only if you understand how it will affect your deployment, including application behavior and BIG-IP performance.
   If you enable TCP Request Queuing, you must have a Connection Limit set on at least one of the nodes when configuring the Address/Port for the nodes.

   - **No, do not enable TCP request queuing (recommended)**
     Select this option if you do not want the BIG-IP system to queue TCP requests.
   - **Yes, enable TCP request queuing**
     Select this option if you want to enable TCP request queuing on the BIG-IP system.

     a. *What is the maximum number of TCP requests for the queue?*
        Type the maximum number of requests you want to queue. We do ***not*** recommend using 0, which means unlimited and is only constrained by available memory.

     b. *How many milliseconds should requests remain in the queue?*
        Type a number of milliseconds for the TCP request timeout value.

5. ***Use a Slow Ramp time for newly added servers?*** Advanced
   With Slow Ramp, the BIG-IP system gradually adds connections to a newly-enabled or newly-added Dynamics CRM server over a time period you specify, rather than sending a full proportion of the traffic immediately. Slow Ramp is essential when using the Least Connections load balancing method (our recommended method for Dynamics CRM servers), as the BIG-IP system would otherwise send all new connections to a new server immediately, potentially overwhelming that server.

   Select whether you want to use a Slow Ramp time.

   - **Use Slow Ramp**
     Select this option for the system to implement Slow Ramp time for this pool.

     a. *How many seconds should Slow Ramp time last?*
        Specify a duration in seconds, for Slow Ramp. The time period you select for Slow Ramp is highly dependent on the speed of your server hardware and the behavior of your web services. The default setting of 300 seconds (5 minutes) is very conservative in most cases.

   - **Do not use Slow Ramp**
     Select this option if you do not want to use Slow Ramp. If you select this option, we recommend you do not use the Least Connections load balancing method.

Application Health

In this section, you answer questions about how you want to implement application health monitoring on the BIG-IP system.

1. ***Create a new health monitor or use an existing one?***
   Application health monitors are used to verify the content that is returned by an HTTP request. The system uses these monitors to ensure traffic is only sent to available Dynamics CRM servers.

   Unless you have requirements for configuring other options not in the following list of questions, we recommend allowing the iApp to create a new monitor. Creating a custom health monitor is not a part of this template; see **Local Traffic** >> **Monitors**. To select any new monitors you create, you need to restart or reconfigure this template.

   - *Select the monitor you created from the list*
     If you manually created the health monitor, select it from the list.
     Continue with *iRules on page 24.*
   - **Create a new health monitor**
     If you want the iApp to create a new monitor, continue with the following.

     a. *How many seconds should pass between health checks?*
     Specify how long the system should wait between each health check. This is used as the Interval setting for the monitor. We recommend the default of 30 seconds.

     b. *What type of HTTP request should be sent to the servers?*
     Select whether you want the system to send an HTTP GET or POST request. The GET method requests data from the server, the POST submits data to be processed by the server.

     - **GET**
       Select this option if you want the system to use a GET request. The system uses the URI you specify in the next question to request content from the Dynamics CRM server.
     - **POST**
       Select this option if you want the system to use a POST request. The system uses the URI you specify in the next question, along with the HTTP POST body you will specify to form the request.

     c. *What HTTP URI should be sent to the servers?*
     The HTTP URI is used to specify the resource on the Dynamics CRM server for a given request. This parameter can be customized to request a specific part of your application, which can indicate the application-health on a granular level.

     d. *What HTTP version do your servers expect clients to use?*
     Choose the HTTP version which you expect most of your clients to be using. This allows the system to detect failures more accurately.

     - **HTTP/1.0**
       Choose this option if you expect your clients to use HTTP/1.0.
     - **HTTP/1.1**
       Choose this option if you expect your clients to use HTTP/1.1.

     e. *What HTTP POST body do you want to use for this monitor?*
     This question only appears if you selected a POST request.

     If you selected a POST request, you must specify the message body for the POST.

     f. *What is the expected response to the HTTP request?*
     Specify the response you expect returned from the request. The system checks the response from the server against the response you enter here to determine server health.

     g. *Should the health monitor require credentials?*
     Choose whether you want the system to attempt to authenticate to the Dynamics CRM server deployment as a part of the health check.

     - **No, allow anonymous access**
       Select this option if you do not want the monitor to attempt authentication.

- **Yes, require credentials for Basic authentication**
  Select this option if you want to attempt Basic authentication as a part of the health monitor. To require credentials, you should have a user account specifically for this health monitor which has no other privileges, and has a password set to never expire.

  i). What user name should the monitor use?
  Type the domain and user name for the account you created for the health monitor. You must include the domain in front of the user, such as EXAMPLE\USER.

  ii). What is the associated password?
  Type the password for the account.

- **Yes, require credentials for NTLM authentication**
  Select this option if you want to attempt NTLM authentication as a part of the health monitor. To require credentials, you should have a user account specifically for this health monitor which has no other privileges, and has a password set to never expire.

  i). What user name should the monitor use?
  Type the user name for the account you created for the health monitor.

  Warning

  Do not include DOMAIN\ for the NTLM monitor user name.

  ii). What is the associated password?
  Type the password for the account.

iRules

In this section, you can add custom iRules to the Dynamics CRM deployment. This section is available only if you selected Advanced mode.

iRules are a scripting language that allows an administrator to instruct the system to intercept, inspect, transform, direct and track inbound or outbound application traffic. An iRule contains the set of instructions the system uses to process data flowing through it, either in the header or payload of a packet.

1. ***Do you want to add any custom iRules to the configuration?*** Advanced
   Select if have preexisting iRules you want to add to your Dynamics CRM implementation.

   Warning

   While iRules can provide additional functionality not present in the iApp, iRules are an advanced feature and should be used only if you understand how each iRule will affect your deployment, including application behavior and BIG-IP system performance.

   If you do not want to add any iRules to the configuration, continue with the following section.

   If you have iRules you want to attach to the virtual server the iApp creates for your Dynamics CRM servers, from the **Options** box, click the name of the applicable iRule(s) and then click the Add (**<<**) button to move them to the **Selected** box.

Statistics and Logging

In this section, you answer questions about logging and statistics settings. This section is available only if you selected Advanced mode.

1. ***Do you want to enable Analytics for application statistics?***
   The Application Visibility Reporting (AVR) module for analytics allows you to view statistics specific to your application implementation. AVR is included and available on all BIG-IP systems v11 and later, however you must have the AVR provisioned for this option to appear. This provisioning requirement is only for AVR, you can view object-level statistics from the BIG-IP without provisioning AVR.

   Important

   Enabling Analytics may adversely affect overall system performance. If you choose to enable Analytics, we recommend gathering statistics for a set time period, such as one week, and then re-entering this template and disabling Analytics while you process the data.

If you plan on using AVR for analytics, we recommend creating a custom Analytics profile. To create a new profile, from the Main tab, select **Profiles** and then click **Analytics**. Click **New** and then configure the profile as applicable for your configuration. See the online help or product documentation for specific instructions. To select the new profile, you need to restart or reconfigure the iApp template.

- **Do not enable Application Visibility Reporting**
  If you do not want to enable Analytics, leave this list set to **No**, and continue with the next section.
- *Select the Analytics profile you created from the list*
  If you choose to enable Analytics, select the Analytics profile you want to use for this implementation from the list.

2. ***Which HTTP request logging profile do you want to use?***
   HTTP request logging enables customizable log messages to be sent to a syslog server for each HTTP request processed by your application. You can choose to enable HTTP request logging by selecting a logging profile you already created from the list.
   We strongly recommend you thoroughly test the performance impact of using this feature in a staging environment prior to enabling on a production deployment

   Creating a request logging profile is not a part of this template. See Local Traffic>>Profiles: Other: Request Logging. To select any new profiles you create, you need to restart or reconfigure this template.

   - **Do not enable HTTP request logging**
     If you do not want to enable HTTP request logging, leave this list set to **No**, and continue with the next section.
   - *Select the HTTP request logging profile you created from the list*
     If you choose to enable HTTP request logging, select the profile you want to use for this implementation from the list.

Finished

Review the answers to your questions. When you are satisfied, click the **Finished** button. The BIG-IP system creates the relevant objects for the Dynamics CRM application.

Optional: Configuring BIG-IP LTM/APM to support NTLMv2-only deployments

If you have configured your Microsoft Windows domain to support only NTLMv2 authentication and refuse LM/NTLM requests, you must either modify the configuration produced by the template by disabling the Strict Updates feature and add/modify the required objects for NTLMv2 authentication.

Disabling the strict updates feature on the iApp deployment

First you must disable the strict updates feature.

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your Dynamics Application Service from the list.
3. From the **Application Service** menu, select **Advanced**.
4. In the **Strict Updates** row, clear the checkbox to disable Strict Updates.
5. Click **Update**.

Creating a new NTLM SSO Configuration object

Next, you create a new NTLM SSO Configuration object on the BIG-IP APM.

1. On the Main tab, click **Access Policy > Access Profiles > SSO Configurations > NTLMv2**.
2. Click **Create**.
3. In the **Name** box, type a unique name.
4. In the NTLM Domain field, type the fully qualified name of the domain where users authenticate.
5. Click Finished.

Modifying the Access Profile

The final task is to update the Access Profile created by the iApp template to use the NTLM SSO Configuration object you just created.

1. On the Main tab, click **Access Policy > Access Profiles**.
2. Click the name of the Access Profile created by the template. This profile starts with the name you gave your Dynamics iApp, followed by **_apm_access**.
3. On the Menu bar, click **SSO/Auth Domains**.
4. From the **SSO Configuration** list, select the NTLMv2 SSO Configuration you created.
5. Click **Update**.
6. You can optionally re-enable Strict Updates. Keep in mind, if you re-enter the iApp template and make changes to the configuration, you must perform this procedure again.

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the Microsoft Dynamics service you just created. To see the list of all the configuration objects created to support the Dynamics application, on the Menu bar, click **Components**. The complete list of all related objects opens. You can click individual objects to see the settings.

Once the objects have been created, you are ready to use the new deployment.

Modifying DNS settings to use the BIG-IP virtual server address

Before sending traffic to the BIG-IP system, your DNS administrator may need to modify any DNS entries for the Dynamics implementation to point to the BIG-IP system's virtual server address.

Modifying the iApp configuration

The iApp Application Service you just created can be quickly and easily modified if you find it necessary to make changes to the configuration. The Strict Updates feature of the iApp prevents users from manually modifying the iApp configuration (Strict Updates can be turned off, but use extreme caution). iApp allows you to re-enter the template, make changes, and then update the template. The modifications are automatically made to any of the associated objects.

To modify the configuration

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your Dynamics CRM Application Service from the list.
3. On the Menu bar, click **Reconfigure**.
4. Make the necessary modifications to the template.
5. Click the **Finished** button.

Viewing statistics

You can easily view a number of different statistics on the BIG-IP system related to the configuration objects created by the iApp template. You can get statistics specific to the Application Service if you have provisioned AVR. Otherwise, you can always get object-level statistics.

AVR statistics

If you have provisioned AVR, you can get application-level statistics for your Dynamics Application Service.

To view AVR statistics

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. From the Application Service List, click the Dynamics service you just created.
3. On the Menu bar, click **Analytics**.
4. Use the tabs and the Menu bar to view different statistics for your iApp.

Object-level statistics

If you haven't provisioned AVR, or want to view object-level statistics, use the following procedure.

To view object-level statics

1. On the Main tab, expand **Overview**, and then click **Statistics**.
2. From the **Statistics Type** menu, you can select **Virtual Servers** to see statistics related to the virtual servers.
3. You can also choose **Pools** or **Nodes** to get a closer look at the traffic.
4. To see Networking statistics in a graphical format, click **Dashboard**.

For more information on viewing statistics on the BIG-IP system, see the online help or product documentation.

Troubleshooting

Q: *Why isn't the Dynamics UI displaying page objects from the* ***/help*** *directory?*

A: Upgrading to Dynamics CRM 2011 Update Rollup 15 solves this issue.
If you cannot upgrade to Rollup 15, use the following guidance.

If your Dynamics CRM user interface is not correctly displaying page objects located in the **/help** directory, you may need to configure a Stream profile on the BIG-IP system to ensure the correct FQDN for your Dynamics deployment is returned to the client browser.

The stream profile **Target** field should be comprised of one or more pairs of values, separated by the **@** symbol. The first value corresponds to the NetBIOS name of a server in your deployment, and the second value is the fully qualified domain name (FQDN) that clients use to access Dynamics CRM. For example, if you have two servers in your Dynamics 2011 CRM deployment named *server01* and *server02*, and the FQDN of the deployment is *dynamics.mycompany.com*, the Stream profile Target field would be:
@server01@dynamics.mycompany.com@server02@dynamics.mycompany.com@

Use the following procedure to create the Stream profile and attach it to the virtual server.

To create the Stream profile

1. On the Main tab, expand **Local Traffic** and then click **Profiles**.
2. On the Menu bar, from the **Other** menu, click **Stream**.
3. In the **Name** box, type a unique name.
4. In the **Target** box, type the appropriate value, using the guidance in the paragraph above.
5. Click **Finished**.
6. If you used the iApp to configure Dynamics CRM, you must first disable Strict Updates:
   a. On the Main tab, expand **iApp** and then click **Application Services**.
   b. Click the name of your Dynamics Application Service from the list.
   c. From the **Application Service** menu, select **Advanced**.
   d. In the **Strict Updates** row, clear the checkbox to disable Strict Updates.
   e. Click **Update**.
7. On the Main tab, click **Virtual Servers**.
8. Click the name of the external HTTPS virtual server you created. The properties page opens.
9. If necessary, from the **Configuration** list, select **Advanced**.
10. From the **Stream Profile** list, select the profile you just created.
11. Click **Update**.

Q: *Why are users getting a "Generic Error" when browsing pages after deploying the BIG-IP system?*

A: If your users are seeing a "Generic Error", check the BIG-IP HTTP profile. If you are not using the BIG-IP system to offload SSL, you should ***NOT*** have the **Request Header Insert** field set to **FRONT-END-HTTPS:on**. This field should be left at the default (no value) if not using the BIG-IP system to offload SSL. If you are offloading SSL and have the correct header in the HTTP profile, and you are seeing this error, confirm that you have a matching header value configured under NLB and SSL Header Information in the Dynamics CRM deployment properties.

Q: *Why are client connections unresponsive or seem to hang when using the OneConnect feature?*

A: If you have configured the BIG-IP LTM to use OneConnect (part of F5's recommended configuration), and users are experiencing slow performance or the need to refresh pages, Microsoft IIS may be failing to reset the TCP connection after the default timeout period of 120 seconds.

To work around this issue, modify the server-side TCP profile you created to set the **Idle Timeout** value to less that 120 seconds. To modify the Idle Timeout setting, open the TCP profile you created, check the Custom box for **Idle Timeout**, and then in the **Seconds** box, type a number less than 120, such as **110**. Click **Update**.

Q: I configured the iApp template to use AFM to Reject or Log access connections from sources with low reputation scores, why isn't the system rejecting or logging those connections?

A: This issue was fixed in the v1.0.0 release of the iApp template. If you are still using v1.0.0rc1, we recommend you upgrade to the v1.0.0 release. If you cannot upgrade, use the following guidance to work around the issue.

If you are using BIG-IP AFM and IP Intelligence, and configured the iApp template v1.0.0rc1 to log or reject connection attempts from sources with a low reputation scores, you must configure the Blacklist categories manually before connections are logged or rejected. Use the following guidance.

1. Disable Strict Updates if you have not already. See Step 6 of the Stream Profile procedure on the previous page for instructions.
2. Click **Security > Network Firewall > IP Intelligence > Policies >** *(name-you-gave-the-iApp)*_**ip_intelligence**.
3. In the Blacklist Matching Policy area, from the **Blacklist Category** list, select a category that you want to log or reject, and then click **Add**.
4. Repeat step 3 to add all applicable blacklist categories.
5. Click **Update**.
6. You can optionally re-enable Strict Updates. Keep in mind, if you re-enter the iApp template and make changes to the configuration, you must perform this procedure again.

Appendix A: Manual Configuration Tables

Use the following tables for guidance on manually configuring the BIG-IP system for Dynamics CRM.

Manually configuring the BIG-IP LTM for Dynamics CRM 2011 and 2013

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

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitor (*Main tab-->Local Traffic -->Monitors*)	**Standard monitor if you are not using Claims-based authentication or IFD**	
	Name	Type a unique name
	Type	**HTTP** (or **HTTPS** if using SSL Bridging)
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Send String[1,2]	**GET /F5Dynamics/main.aspx HTTP/1.1\r\nUser-Agent: Mozilla/4.0\r\nHost: dynamics.example.local**
	Receive String[1]	**200 OK**
	User Name[1]	Type a user name with access to Dynamics CRM. We recommend creating an account for use in this monitor.
	Password[1]	Type the associated password
	Monitor if using Claims-based authentication or IFD *(see page 33 for configuration details)*	
	Name	Type a unique name
	Type	**HTTPS**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Send String	**GET /adfs/fs/federationserverservice.asmx HTTP/1.1\r\nHost: \r\nConnection: Close\r\n**
	Receive String	**200 OK**
Pool (*Main tab-->Local Traffic -->Pools*)	***Name***	Type a unique name
	Health Monitor	Select the appropriate monitor you created
	Slow Ramp Time	**300**
	Load Balancing Method	Choose a load balancing method. We recommend **Least Connections (Member)**
	Address	Type the IP Address of a Dynamics CRM node.
	Service Port	Type the port. In our example, we use **80**. Click **Add**, and then repeat Address and Port for all nodes

[1] IMPORTANT: If using BIG-IP LTM version 11.0.x or earlier, Basic authentication must be enabled on the Dynamics website in IIS to use Send and Receive Strings, and a user name and password. If you do not have Basic authentication enabled, do not configure these objects.
If using BIG-IP version 11.1 or later, the monitor tries Basic authentication first, then falls back to NTLM authentication.

[2] Replace red text with the URI for your deployment in the first instance, and with the FQDN in the second.

BIG-IP LTM Object	Non-default settings/Notes		
Profiles (*Main tab-->Local Traffic -->Profiles*)	***TCP WAN*** (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	Use **tcp-wan-optimized**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	Use **tcp-lan-optimized**
	HTTP (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**http**
		Redirect Rewrite[3]	**All**
		Insert X-Forwarded-For	**Enabled** (see *page 41* for adding the X-Forwarded-For log field to IIS)
		Request Header Insert[3]	**FRONT-END-HTTPS:on** [3] (Do ***not*** configure this option if not offloading SSL) This must match the header value configured in the Dynamics CRM deployment properties
	HTTP Compression (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**wan-optimized-compression**
		Keep Accept Encoding	**Enabled**
	Web Acceleration (*Profiles-->Services*)	Name	Type a unique name
		Parent Profile	**webacceleration**
	Persistence (*Profiles-->Persistence)*	Name	Type a unique name
		Persistence Type	**Cookie**
	OneConnect (*Profiles-->Other*)	Name	Type a unique name
		Parent Profile	**oneconnect**
		Source Mask	**255.255.255.255**
	NTLM (*Profiles-->Other)*	Name	Type a unique name
		Parent Profile	**NTLM**
	Client SSL[3] (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select the Certificate and Key you imported from the associated list
	Server SSL[4] (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**serverssl**
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**HTTP**		
	Name	Type a unique name.	
	Address	Type the IP Address for the virtual server	
	Service Port	**80**	
	Protocol Profile (Client)[1,2]	Select the WAN optimized TCP profile you created	
	Protocol Profile (Server)[1,2]	Select the LAN optimized TCP profile you created	
	HTTP Profile[2]	Select the HTTP profile you created	
	Web Acceleration profile[2]	Select the Web Acceleration profile you created	
	HTTP Compression profile[2]	Select the HTTP Compression profile you created	
	OneConnect profile[2]	Select the OneConnect profile you created	
	SNAT Pool [3]	**Auto Map** (optional; see footnote [3])	
	Default Pool[2]	Select the pool you created	
	Persistence Profile[2]	Select the Persistence profile you created	
	iRule[4]	If configuring SSL offload or SSL bridging: Enable the built-in **_sys_https_redirect** irule	

[1] You must select **Advanced** from the **Configuration** list for these options to appear

[2] *Do not enable these objects on the HTTP virtual server if offloading SSL. The HTTP virtual server is only used for redirecting users to the HTTPS virtual server, and only requires a name, IP address, Port, and the redirect iRule.*

[3] *In version 11.3 and later, this field is* ***Source Address Translation****. If you want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation specific information.*

[4] *Only enable this iRule if offloading SSL*

[5] *Only create this virtual server if offloading SSL or SSL Bridging*

[6] *Only necessary if configuring SSL Bridging*

BIG-IP LTM Object	Non-default settings/Notes	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	**HTTPS**[5]	
	Name	Type a unique name.
	Address	Type the IP Address for the virtual server
	Service Port	**443**
	Protocol Profile (client)[1]	Select the WAN optimized TCP profile you created
	Protocol Profile (server)[1]	Select the LAN optimized TCP profile you created
	HTTP Profile	Select the HTTP profile you created
	Web Acceleration profile	Select the Web Acceleration profile you created
	HTTP Compression profile	Select the HTTP Compression profile you created
	SSL Profile (Client)	Select the Client SSL profile you created
	SSL Profile (Server)[6]	Select the Server SSL profile you created
	OneConnect profile	Select the OneConnect profile you created
	SNAT Pool [3]	**Automap** (optional; see footnote [3])
	Default Pool	Select the pool you created
	Persistence Profile	Select the Persistence profile you created

[1] You must select **Advanced** from the **Configuration** list for these options to appear
[2] *Do not enable these objects on the HTTP virtual server if offloading SSL. The HTTP virtual server is only used for redirecting users to the HTTPS virtual server, and only requires a name, IP address, Port, and the redirect iRule.*
[3] *In version 11.3 and later, this field is **Source Address Translation**. If you want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation specific information.*
[4] *Only enable this iRule if offloading SSL*
[5] *Only create this virtual server if offloading SSL or SSL Bridging*
[6] *Only necessary if configuring SSL Bridging*

Configuring BIG-IP Access Policy Manager for Dynamics CRM 2011 and 2013

In this section, we provide guidance on configuring the BIG-IP Access Policy Manager (APM) for use with Dynamics CRM. The BIG-IP APM, F5's high-performance access and security solution, can provide proxy authentication and secure remote access to Dynamics deployments.

Important

When using the BIG-IP APM with Microsoft Dynamics CRM, be sure to add the FQDN used to access Dynamics to Trusted Sites in Internet Explorer. Otherwise, you may experience prompts for authentication.

Using the configuration table

Use the following table to manually configure the BIG-IP APM for Dynamics CRM. This table contains a list of BIG-IP configuration objects along with any non-default settings you should configure as a part of this deployment. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or product manuals.

BIG-IP APM Object	Non-default settings/Notes	
DNS and NTP	See *Appendix E: Configuring DNS and NTP on the BIG-IP system on page 47* for instructions.	
AAA Servers (*Access Policy -->AAA Servers*)	**Name**	Type a unique name
	Type	**Active Directory**
	Domain Name	Type the Windows Domain FQDN
	Server Connection*	**Direct** (v11.2 and later only. If you want to create a pool of Domain Controllers, see *Using a pool of AAA Servers in BIG-IP version 11.2 and later (optional) on page 35)*
	Domain Controller	Type the IP address of the Domain controller
	Admin Name/Password	If required, type the Admin name and Password
SSO Configurations (*Access Policy--> SSO Configurations*)	**Name**	Type a unique name
	SSO Method	**NTLMV1**
	NTLM Domain	Type the NTLM Domain name
iRules (*Main tab-->Local Traffic-->iRules*)	**Important:** *The Outlook CRM plug-in is incompatible with BIG-IP APM at this time. You must include this iRule to disable BIG-IP APM for CRM requests from Microsoft Outlook.*	
	Name	Type a unique name
	Definition	See "iRule to disable BIG-IP APM for CRM requests from Microsoft Outlook" following this table for the iRule definition.
Access Profile (*Access Policy --> Access Profiles*)	**Name**	Type a unique name.
	Languages	Move the appropriate language(s) to the **Accepted** box.
Access Policy	**Edit**	Edit the Access Profile you created using the Visual Policy Editor. See the procedure on this page.

***** BIG-IP v11.2 and later only. See *Using a pool of AAA Servers in BIG-IP version 11.2 and later (optional) on page 35 to create a health monitor to go with the Use Pool option.*

iRule to disable BIG-IP APM for CRM requests from Microsoft Outlook

Use the following code for the Definition section of the iRule, omitting the line numbers.

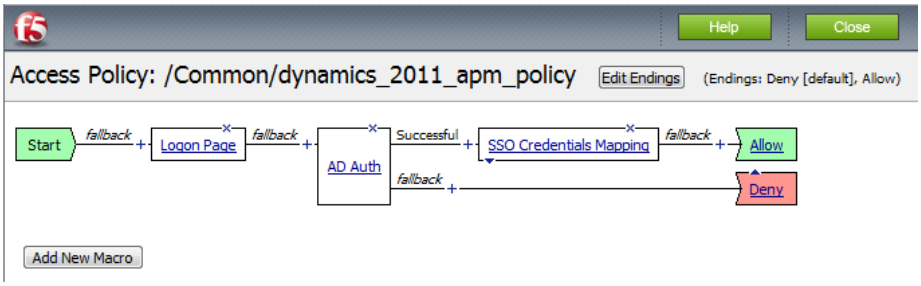
```
1  when HTTP_REQUEST {
2    if { [ string tolower [HTTP::uri] ] contains "xrmservices" || [ string tolower [HTTP::uri] ] contains "outlookworkstationclient" || [HTTP::cookie exists "FullClient"] } {
3          ACCESS::disable
4      }
5  }
```

Editing the Access Policy

In the following procedure, we show you how to edit the Access Policy on the APM using the Visual Policy Editor (VPE). The VPE is a powerful visual scripting language that offers virtually unlimited options in configuring an Access Policy. The Policy shown in the following procedure is just an example, you can use this Access Policy or create one of your own.

To edit the Access Policy

1. On the Main tab, expand **Access Policy**, and then click **Access Profiles**.
2. Locate the Access Profile you created in the table above, and then, in the Access Policy column, click **Edit**. The VPE opens.
3. Click the **+** symbol between **Start** and **Deny**. A box opens with options for different actions.
4. Click the **Logon Page** option button, and then click the **Add Item** button.
5. Configure the Properties as applicable for your configuration. In our example, we leave the settings at the defaults. Click **Save**.
6. Click the **+** symbol on the between **Logon Page** and **Deny**.
7. Click **AD Auth** option button, and then click the **Add Item** button.
   a. From the **Server** list, select the AAA server you configured in the table above. All other settings are optional.
   b. Click **Save**. You now see a Successful and Fallback path from AD Auth.
8. On the Successful path between **AD Auth** and **Deny**, click the **+** symbol.
9. Click the **SSO Credential Mapping** option button, and then click the **Add Item** button.
10. Click the **Save** button.
11. Click the **Deny** link in the box to the right of **SSO Credential Mapping**.
12. Click **Allow** and then click **Save**. Your Access policy should look like the example below.
13. Click the yellow **Apply Access Policy** link on the upper left. You have to apply an access policy before it takes effect.
14. Click the **Close** button on the upper right to close the VPE.



Add the Access policy and iRule to the virtual server

The final task is to add the Access Policy to the HTTPS virtual server you created.

To modify the virtual server

1. On the Main tab, under **Local Traffic**, click **Virtual Servers**.
2. From the list, click the HTTPS virtual server you created.
3. In the Access Policy section, from the **Access Profile** list, select the name of the Access Profile you created using the table.
4. In the iRule section, from the Available list, select the name of the iRule you created to disable BIG-IP APM for CRM requests from Outlook, and then click the Add (**<<**) button to enable it.
5. Click **Update**.

Using a pool of AAA Servers in BIG-IP version 11.2 and later (optional)

A new feature in BIG-IP APM version 11.2 is the ability to use High Availability between pool members. This option enables Access Policy Manager to send AAA requests for the associated policy item to the virtual server, and standard pool behavior is used to implement High Availability for AAA domain controllers. While you configure the pool during the AAA Server creation process, we very strongly recommend creating a health monitor before creating the AAA server if using the pool option.

You have two options when configuring a monitor for the Active Directory servers; a lighter-weight TCP monitor on port 636 or 389, or a more specific LDAP monitor. Choose the monitor that is most suitable for your configuration.

Creating the TCP monitor

Use the following table for creating the TCP monitor.

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitors (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**TCP**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	Alias Service Port	**636** for LDAP over SSL, or **389** if not using SSL.

Creating the LDAP monitor

Use the following table for creating the more specific LDAP monitor. We recommend creating a unique user account for use in this monitor. For additional guidance on monitoring LDAP, see *http://support.f5.com/kb/en-us/solutions/public/9000/300/sol9311.html.*

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitors (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**LDAP**
	Interval	**10** (recommended)
	Timeout	**91** (recommended)
	User Name	Type the LDAP common name of the user account you created for use in monitoring.
	Password	Type the associated password
	Base	Type the LDAP distinguishedName of the base group in Active Directory to search, such as *dc=bigip-test,dc=net*.
	Filter	Type the LDAP distinguishedName of the key to search for in Active Directory, such as *cn=user01*.
	Alias Service Port	**636** for LDAP over SSL, or **389** if not using SSL.

Creating the AAA server with the Use Pool option and the health monitor you created

Use the following table to create the AAA server with the Use Pool option.

BIG-IP APM Object	Non-default settings/Notes	
AAA Servers (*Access Policy -->AAA Servers*)	***Name***	Type a unique name
	Type	**Active Directory**
	Domain Name	Type the Windows Domain FQDN
	Server Connection	**Use Pool**
	Domain Controller Pool Name	Type a name for this pool of Active Directory servers
	Domain Controllers	Type the IP address and the FQDN for each Domain Controller you want to add and then click Add.
	Server Pool Monitor	Select the TCP or LDAP monitor you created.
	Admin Name/Password	If required, type the Admin name and Password

Manually configuring the BIG-IP Advanced Firewall Module to secure your Dynamics CRM deployment

This section describes how to manually configure BIG-IP AFM, F5's Network Firewall module, to secure your Dynamics CRM deployment. BIG-IP AFM is particularly useful if you want to only allow access from specific clients or networks. Because this configuration can be complex, we recommend using the iApp template in version 11.6 and later to configure BIG-IP AFM.

Network Firewall settings

When configuring the BIG-IP Advanced Firewall Manager, you may want to configure your BIG-IP system to drop all traffic that you have not specifically allowed with firewall rules. This in known as ***firewall mode***. By default, your BIG-IP system is set to default-accept, or ***ADC mode***. Instructions for configuring your BIG-IP system, and the implications to consider, can be found on AskF5. For example, for BIG-IP v11.5: *http://support.f5.com/kb/en-us/products/big-ip-afm/manuals/product/network-firewall-policies-implementations-11-5-0/1.html*

If you have licensed IP Intelligence on the BIG-IP system, you can prohibit connections from sources with low reputation scores.

The following instructions cover a basic firewall configuration that is effective for the most common scenario of wanting to allow connections from a single trusted network. If you have complex requirements, such as the need to schedule different policies for different times of the day, or you want to create complicated rule or address lists, consult the BIG-IP AFM documentation. The basic steps for Policy and Rule creation apply to all scenarios.

To configure the BIG-IP AFM to allow connections from a single trusted network

1. Create a Network Firewall Policy:
   a. From the Configuration utility, click **Security > Network Firewall > Policies**, and then click **Create**.
   b. In the **Name** field, type a unique name for the policy, such as **Dynamics-Policy**.
   c. Click **Finished**.
2. Create a rule to allow authorized hosts or networks to connect:
   a. Click **Security > Network Firewall > Policies**.
   b. Click the name of the policy you just created.
   c. In the Rule section (below the General Properties section), click the **Add** button.
   d. Leave the **Type** list set to Rule.
   e. From the **Order** list, select **First**. The Order list only appears in version 11.5 and later. In 11.4.x, you must reorder the rules from the Policy General Properties page.
   f. In the **Name** field, type a unique name, for instance **Dynamics-traffic-Allowed**.
   g. Ensure the **State** list is set to **Enabled**.
   h. From the **Protocol** list, select **TCP**. Leave the box to the right of TCP set to **6**.
   i. In the **Source** section, from the **Address/Region** list, select **Specify**.
   You are now able to list the trusted source addresses for your connection.
   In the following example, we will configure a single subnet as trusted.
      - Select **Address**.
      - In the box, type the network address you want to allow, including netmask if more than a single host. Specify a network using CIDR notation, such as **10.0.0.0/24**.
      - Do not configure a source port.
      - Optional: If you want to limit inbound connections to a specific VLAN or Tunnel, from the **VLAN / Tunnel** list, select **Specify**, and then move the VLANs or tunnels that are allowed access to the Selected box.
      - Click **Add**.
      - Repeat these steps for additional hosts or networks. Use **Address List** or **Address Range** when appropriate.
   j. In the **Destination** section, leave the **Address/Region** and **Port** set to **Any**. Because you will be applying your policy to a virtual server that listens only on a single desired address and port, do not specify that information here.

k. If necessary, from the **Action** list, select **Accept**.

l. *Optional:* If you have configured a logging profile and want to log connections, from the **Logging** list, select **Enabled**. Typically, allowed connections do not need to be logged.

m. Click **Finished**.

3. Creating a firewall rule to block all other traffic
The next task is to create a firewall rule to block all other traffic that you have not allowed. Although this is not a required step if your BIG-IP system is set to default deny (**Firewall mode**), it is required in default-accept (**ADC mode**), and is a good practice to always configure such a rule.

a. Click **Security > Network Firewall > Policies**.

b. Click the name of the policy you created in step 1.

c. In the Rule section (below the General Properties section), click the **Add** button.

d. Leave the **Type** list set to **Rule**.

e. Leave the **Order** list, select **Last**.

f. In the **Name** field, type a unique name, for example **Dynamics-traffic-Prohibited**.

g. Ensure the **State** list is set to **Enabled**.

h. From the **Protocol** list, select **TCP**. Leave the box to the right of TCP set to **6**.

i. In the **Source** section, leave all the lists set to **Any**

j. From the **Action** list, select either **Drop** (to silently discard incoming connections) or **Reject** (to send a Destination Unreachable message to the sender).

k. If you configured a logging profile as described in *Optional: Configuring the BIG-IP system to log network firewall events on page 38*, from the **Logging** list, select **Enabled**.

l. Click **Finished**. You return to the Policy Properties page.

m. On the Policy Properties page, in the Rules section, ensure the rule with the Action of Accept comes before the Drop or Reject rule you just created. If it does not, use the **Reorder** button and drag the rules into the correct order.

4. Apply Your Firewall Policy to your Virtual Server

a. Click **Security > Network Firewall > Active Rules**.

b. In the Rule section (below the General Properties section), click the **Add** button.

c. From the **Context** list, select **Virtual Server**, and then select the virtual server you created for your Dynamics traffic.

d. From the **Type** list, select **Policy**, and then select the firewall policy you created.

e. From the **Policy Type** list, select **Enforced**.

f. Click **Finished**.

Optional: Assigning an IP Intelligence Policy to your Dynamics virtual server

If you want to restrict access to your Dynamics virtual server based on the reputation of the remote sender, you can enable and assign an IP Intelligence policy. This requires an IP intelligence license; contact your F5 Sales representative for more information.

It is outside the scope of this document to provide instructions on configuring an IP Intelligence Policy. Full documentation on enabling and configuring the IP Intelligence feature can be found on AskF5. For example, the manual for BIG-IP AFM v11.5 is:
https://support.f5.com/kb/en-us/products/big-ip-afm/manuals/product/network-firewall-policies-implementations-11-5-0/5.html

After you have enabled and configured an IP Intelligence policy, use the following steps to assign the policy to your Dynamics virtual server:

To assign the IP intelligence policy to the Dynamics virtual server

1. On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.
2. Click the name of your Dynamics virtual server.
3. From the **Security** menu, choose **Policies**.
4. Next to **IP Intelligence**, select **Enabled**, then select the IP intelligence policy to apply to traffic on the virtual server.
5. Click **Update**. The list screen and the updated item are displayed. The IP Intelligence policy is applied to traffic on the virtual server.

Optional: Configuring the BIG-IP system to log network firewall events

If you are using BIG-IP AFM, you have the option of logging network firewall events to one or more remote syslog servers (recommended) or to log events locally. You can either use an iApp template to create the logging profile, or create the logging profile manually. In this guide, we only provide instructions for creating the logging profile with the iApp template.

For specific information on logging on the BIG-IP system, see the appropriate guide for your version. For example, for 11.5.0:

- Remote High-Speed Logging: *https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-11-5-0/22.html*
- Local logging: *https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-concepts-11-5-0/11.html*

Creating the logging profile using the iApp template

Use this section to create the logging profile using the logging profile iApp template. If you have not already downloaded the iApp template, see *https://devcentral.f5.com/wiki/iApp.F5-Remote-Logging-iApp.ashx*.

To configure the logging profile iApp

1. Log on to the BIG-IP system.
2. On the Main tab, click **iApp > Application Services**.
3. Click **Create**. The Template Selection page opens.
4. In the **Name** box, type a name. In our example, we use **logging-iapp_.**
5. From the **Template** list, select **f5.remote_logging.v*<latest-version>***. The template opens
6. Use the following table for guidance on configuring the iApp template. Questions not mentioned in the table can be configured as applicable for your implementation.

Question	Your selection
Do you want to create a new pool of remote logging servers, or use an existing one?	Unless you have already created a pool on the BIG-IP system for your remote logging servers, select **Create a new pool**.
Which servers should be included in this pool?	Specify the IP addresses of your logging servers. Click **Add** to include more servers.
What port do the pool members use?	Specify the port used by your logging servers, typically **514**.
Do the pool members expect UDP or TCP connections?	**TCP**
Do you want to create a new monitor for this pool, or use an existing one?	Unless you have already created a health monitor for your pool of logging servers, select **Use a simple ICMP (ping) monitor**.
Do your log pool members require a specific log format?	If your logging servers require a specific format, select the appropriate format from the list.

7. Click **Finished**.
8. On the Main tab, click **Local Traffic > Virtual Servers**. The Virtual Server List screen opens.
9. Click the name of your Dynamics virtual server.

10. From the **Security** menu, choose **Policies**.
11. Next to **Log Profile**, select **Enabled**, then select the Logging profile you created.
12. Click **Update**. The list screen and the updated item are displayed.

> ***Note***
>
> *The iApp template creates a log publisher and attaches it to the logging profile. If the publisher does not appear in the BIG-IP Configuration utility (GUI), you can verify the configuration by running the following command from the Traffic Management shell (tmsh):* **`list security log profile`** ***`<your profile name>`***.

Assigning the logging profile to the virtual server

The final task is to assign the logging profile to the virtual server.

To assign the logging profile to the Dynamics virtual server

1. On the Main tab, expand **iApp** and then click **Application Services**.
2. Click the name of your Dynamics Application service from the list.
3. On the Menu bar, click **Reconfigure**.
4. In the Advanced Firewall Manager (BIG-IP AFM) section, from the **Which logging profile would you like to use?** question, select the profile you just created.
5. Click the **Finished** button.

Appendix B: Configuring the BIG-IP for server-to-server traffic if there is a NATing device between the BIG-IP and the servers

If you have a NATing device between the servers and the BIG-IP device, so that the BIG-IP system is unable to recognize the true server IP address, you must use the following guidance for configuring a virtual server for server-to-server traffic.

In this case, you need to configure a virtual server on the same local VLAN as the Dynamics servers that includes an iRule. The iRule ensures each request is directed to the same server that made it. You must also add a host entry to the Dynamics servers directing all requests for the Dynamics URL to the IP address of the internal BIG-IP LTM virtual server. See Microsoft documentation for guidance on adding host entries.

Use the following table to create the objects on the BIG-IP LTM. Unless otherwise specified, settings not mentioned in the table can be configured as applicable for your configuration. For specific instructions on configuring individual objects, see the online help or manuals.

Important *This virtual server must match the SSL configuration of the virtual server you created for Dynamics client-server traffic. If that virtual server uses SSL offload you must also configure this virtual server for SSL offload. Likewise, if you configured SSL bridging, you must configure SSL bridging here.*

BIG-IP LTM Object	Non-default settings/Notes		
Health Monitors (*Main tab-->Local Traffic -->Monitors*)	**Name**	Type a unique name	
	Type	**HTTP**	
	Interval	**30** (recommended)	
	Timeout	**91** (recommended)	
Pools (*Main tab-->Local Traffic -->Pools*)	**Name**	Type a unique name	
	Health Monitor	Select the HTTP monitor you created above	
	Load Balancing Method	**Round Robin**	
	Address	Type the IP Address of your Dynamics CRM server	
	Service Port	**80** Click **Add** to repeat Address and Port for all nodes	
Profiles (*Main tab-->Local Traffic -->Profiles*)	***Persistence*** (*Profiles-->Persistence*	Name	Type a unique name
		Persistence Type	**Source Address Affinity**
	TCP LAN (*Profiles-->Protocol*)	Name	Type a unique name
		Parent Profile	**tcp-lan-optimized**
	Client SSL[1] (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**clientssl**
		Certificate and Key	Select the Certificate and Key you imported from the associated list
	Server SSL[1] (*Profiles-->SSL*)	Name	Type a unique name
		Parent Profile	**serverssl**
iRules (*Main tab-->Local Traffic-->iRules*)	***Name***	Type a unique name	
	Definition	See "Creating the iRule definition" following this table for the iRule definition.	
Virtual Servers (*Main tab-->Local Traffic -->Virtual Servers*)	***Name***	Type a unique name.	
	Destination Address	Type the IP address for this virtual server	
	Service Port	**80**	
	Profiles	Select the applicable profiles you created	
	SNAT Pool[2]	**Auto Map**[2]	
	iRule	Enable the iRule you created above	
	Default Pool	Select the pool you created above	
	Default Persistence Profile	Select the persistence profile you created above	

[1] *Create a Client SSL profile if you are configuring SSL offload or SSL bridging. Only create the Server SSL profile if you are configuring SSL Bridging.*

[2] *In version 11.3 and later, this field is **Source Address Translation**. If you want to use SNAT, and you have a large deployment expecting more than 64,000 simultaneous connections, you must configure a SNAT Pool with an IP address for each 64,000 simultaneous connections you expect. See the BIG-IP documentation specific information.*

Creating the iRule definition

Use the following code for the Definition section of the iRule, omitting the line numbers.

Critical *Be sure to change the red text below to the name of the pool you created in the table.*

```
when CLIENT_ACCEPTED {
     set pm_selected 0
     foreach { pm } [members -list internal-dynamics-pool-name] {
     if { $pm equals “[IP::remote_addr] 80” } {
          set pm_selected 1
          pool internal-dynamics-pool-name member [IP::remote_addr]
     }
}
if { $pm_selected equals 0 } {
     pool internal-dynamics-pool-name
     }
}
```

Configuring the BIG-IP system for Dynamics CRM server-to-server traffic

If you are not using split DNS, and requests from the Dynamics servers to the Dynamics URL are routed through the external Dynamics virtual server on the BIG-IP LTM you may see problems when a request from the Dynamics server is load balanced to another server rather than to itself.

There are two ways to configure this functionality, depending on whether you have a device performing NAT between the servers and the BIG-IP system.

Configuring the BIG-IP system for server-to-server traffic if the BIG-IP system can see server IP addresses

If you do not have a device (such as a NATing device) between the servers and the BIG-IP system that prevents the BIG-IP system from seeing the real server IP addresses, you must attach an iRule to the virtual server you just created. There are multiple versions of the iRule in this section; choose the one applicable to your configuration.

iRule if you do not plan on deploying BIG-IP APM

Use the following iRule definition if you do not plan on using the BIG-IP Access Policy Manager as a part of this deployment.

Critical *Be sure to change the red text below to the name of the pool (and the port the pool members are using) you created in the table.*

```
when CLIENT_ACCEPTED {
    foreach { pm } [members -list example_dynamics_pool] {
        if { $pm equals "[IP::remote_addr] <443 or 80>" } {
            pool example_dynamics_pool member [IP::remote_addr]
        }
    }
}
```

Rule if you plan on deploying BIG-IP APM

Use the following iRule definition if you plan on using the BIG-IP Access Policy Manager as a part of this deployment. If you are using the CRM plug-in for Microsoft Outlook, do not use this iRule, but use the next one.

Critical *Be sure to change the red text below to the name of the pool you created in the table.*

```
when CLIENT_ACCEPTED {
    set is_crm 0
    foreach { pm } [members -list example_dynamics_pool] {
        if { $pm equals "[IP::remote_addr] <443 or 80>" } {
            set is_crm 1
            pool example_dynamics_pool member [IP::remote_addr]
        }
    }
}

when HTTP_REQUEST {
    if { $is_crm == 1 }  {
        ACCESS::disable
    }
}
```

Rule if you plan on deploying BIG-IP APM and are deploying the CRM plug-in for Microsoft Outlook

Use the following iRule definition if you plan on using the BIG-IP Access Policy Manager as a part of this deployment, and are using the CRM plug-in for Microsoft Outlook.

Critical *Be sure to change the red text below to the name of the pool you created in the table. Enter line 12 on a single line.*

```
when CLIENT_ACCEPTED {
    set is_crm 0
    foreach { pm } [members -list example_dynamics_pool] {
        if { $pm equals "[IP::remote_addr] 443" } {
            set is_crm 1
            pool example_dynamics_pool member [IP::remote_addr]
        }
    }
}

when HTTP_REQUEST {
    if { $is_crm == 1 || [string tolower [HTTP::uri]] contains "xrmservices" || [string tolower [HTTP::uri]] contains
    "outlookworkstationclient" || [HTTP::cookie exists "FullClient"]}  {
        ACCESS::disable
    }
}
```

After creating the appropriate iRule, attach it to the virtual server you created using the table on the previous page.

Appendix C: Using X-Forwarded-For to log the client IP address in IIS 7.0, 7.5, and 8 (optional)

When you configure BIG-IP LTM to use SNAT, the BIG-IP system replaces the source IP address of an incoming connection with its local self IP address (in the case of SNAT Automap), or an address you have configured in a SNAT pool. As a result, Microsoft IIS logs each connection with its assigned SNAT address, rather than the address of the client. The iApp produces an HTTP profile on the BIG-IP system which inserts an X-Forwarded-For header, so the original client IP address is sent as well; however, in default IIS configuration, this information is not logged.

Beginning with IIS 7, Microsoft provides an optional Advanced Logging Feature for IIS that allows you to define custom log definitions that can capture additional information such as the client IP address included in the X-Forwarded-For header.

Deploying the Custom Logging role service

The first task is to deploy the Custom Logging role service. If you do not deploy this role service, you may receive a "Feature not supported" error when trying to edit the log definition in the next section. If you receive this error, ensure that you are editing the log definition at the server level in IIS Manager.

The configuration is slightly different depending on which version of IIS you are running. Use the procedure applicable to your version of IIS.

To deploy the Custom Logging role service for IIS 7.0 and 7.5 (Windows Server 2008)

1. From your Windows Server 2008 or Windows Server 2008 R2 device, open Server Manager.
2. In the Navigation pane, expand **Roles**.
3. Right-click **Web Server**, and then click **Add Role Services**.
4. Under Health and Diagnostics, check the box for **Custom Logging**, and then click **Next**.
5. On the Confirmation page, click **Install**.
6. After the service has successfully installed, click the **Close** button.

To deploy the Custom Logging role service for IIS 8.0 (Windows Server 2012)

1. From your Windows Server 2012 device, open Server Manager.
2. Click **Manage** and then **Add Roles and Features**.
3. Select Role-based or feature-based installation.
4. On the Roles screen, expand **Web Server (IIS)** and **Health and Diagnostics** and then check the box for **Custom Logging**.
5. Click **Next** and then on the Features screen, click **Next** again.
6. Click **Install**.
7. After the service has successfully installed, click the **Close** button.

Adding the X-Forwarded-For log field to IIS

Before beginning the following procedure, you must have installed IIS Advanced Logging. For installation instructions, see *http://www.iis.net/community/files/media/advancedlogging_readme.htm*

If you are using IIS version 6, F5 has a downloadable ISAPI filter that performs a similar function to the Advanced Logging Feature discussed here. For information on that solution, see the DevCentral post at *http://devcentral.f5.com/weblogs/Joe/archive/2009/08/19/x_forwarded_for_log_filter_for_windows_servers.aspx*

The following procedure is the same for IIS versions 7.0, 7.5, and 8.0.

To add the X-Forwarded-For log field to IIS

1. From your Windows Server device, open the Internet Information Services (IIS) Manager.
2. From the Connections navigation pane, click the appropriate server on which you are configuring Advanced Logging. The Home page appears in the main panel.
3. From the Home page, under IIS, double-click **Advanced Logging**.
4. From the Actions pane on the right, click **Edit Logging Fields**.
5. From the Edit Logging Fields dialog box, click the **Add Field** button, and then complete the following:
    a. In the **Field ID** box, type **X-Forwarded-For**.
    b. From the **Category** list, select **Default**.
    c. From the **Source Type** list, select **Request Header**.
    d. In the **Source Name** box, type **X-Forwarded-For**.
    e. Click the **OK** button.
6. Click a Log Definition to select it. By default, there is only one: %COMPUTERNAME%-Server. The log definition you select must have a status of Enabled.
7. From the Actions pane on the right, click **Edit Log Definition**.
8. Click **Select Fields**, and then check the box for the X-Forwarded-For logging field.
9. Click the **OK** button.
10. From the Actions pane, click **Apply**.
11. Click **Return To Advanced Logging**.
12. In the Actions pane, click **Enable Advanced Logging**.
    Now, when you look at the Advanced Logging logs, the client IP address is included.

Appendix D: Configuring WMI monitoring for IIS Servers (optional)

If you find your IIS servers are under high performance load, you can dynamically load balance between them using F5's Windows Management Interface (WMI) monitor. This monitor checks the CPU, memory, and disk usage of the nodes and, in conjunction with Dynamic Ratio load balancing mode, sends the connection to the server most capable of processing it.

For an overview of the WMI performance monitor, see *http://support.f5.com/kb/en-us/solutions/public/6000/900/sol6914.html*.

Installing the F5 WMI handler

The first task is to copy the F5 WMI handler to the Windows Server and configure IIS to use the F5 Data Gathering Agent.

To install the Data Gathering Agent F5.IsHandler.dll on an IIS 7.0, 7.5, or 8.0 server

1. Create a **scripts** directory under the directory **C:\Inetpub**. (**C:\Inetpub\scripts**).
2. Create a **\bin** directory under the scripts directory (**C:\Inetpub\scripts\bin**).
3. Copy the file **F5.IsHandler.dll** to the directory **C:\Inetpub\scripts\bin**.
4. In the **C:\Inetpub\scripts** directory, create the file **web.config**. The following shows an example of this file.

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
<system.webServer>
<handlers>
<clear />
<add name="F5IsHandler" path="F5Isapi.dll" verb="*" type="F5.IsHandler" modules="ManagedPipelineHandler"
scriptProcessor="" resourceType="Unspecified" requireAccess="Script" preCondition="" />
</handlers>
<security>
<authentication>
<anonymousAuthentication enabled="false" />
</authentication>
</security>
</system.webServer>
</configuration>
```

5. Allow anonymous authentication to be overridden by using the **appcmd** command to set the override mode in the machine-level **applicationHost.config** file. **appcmd.exe** is located in %systemroot%\system32\inetsrv\.
   For example:

```
appcmd set config "Default Web Site/scripts" /section:anonymousAuthentication /overrideMode:Allow /commit:APPHOST
```

6. Set up a new application pool for the file **F5.IsHandler.dll**:
   a. From the **Start** menu, choose Control Panel.
   b. Choose Administrative Tools
   c. Choose Internet Information Services (IIS) Manager.
   d. From **Connections**, expand **<MachineName>** (**MachineName\UserName**).
   e. Right click the Application Pools menu and choose Add Application Pool.
   f. In the **Name** box, type **F5 Application Pool**.
   g. Click **OK**.
7. Create a new application named **scripts**:
   a. Expand **<MachineName> and Sites**.

b. Right click **"Default Web Site"** (or the applicable web site), and choose **Add Application**.
c. In the **Alias** box, type **scripts**.
d. To change the application pool, click **Select**.
e. For the physical path, type the directory you created in step 1 (**C:\Inetpub\scripts**).
f. Click **OK**.

8. Change the **Authentication** setting to **Basic Authentication**:
   a. Select **scripts**.
   b. In the center pane, double click **Authentication**.
   c. Verify that the status of all items under **Authentication** is **Disabled**, except for the Basic Authentication item. To enable or disable an authentication item, right click the name and choose Enable or Disable.

Creating the WMI Monitor on the BIG-IP LTM

The next task is to create the WMI monitor on the applicable BIG-IP LTM systems. Use the following table:

BIG-IP LTM Object	Non-default settings/Notes	
Health Monitors (*Main tab-->Local Traffic -->Monitors*)	***Name***	Type a unique name
	Type	**WMI**
	Interval	**30** (recommended)
	Timeout	**91** (recommended)
	User Name	Type the appropriate user name
	Password	Type the associated password
	URL:	**/scripts/F5lsapi.dll** (for IIS 6, 7, and 7.5)

Create this monitor on all applicable BIG-IP LTM systems.

Apply the monitor on the BIG-IP LTM devices

Next, we apply the monitor to the IIS nodes on the BIG-IP LTM system.

To apply the monitor to the nodes

1. On the Main tab, expand **Local Traffic** and then click **Nodes**.
2. From the list of nodes, click the IP address of one of your IIS server.
3. In the Configuration section, from the **Health Monitor** list, select **Node Specific**.
4. From the Available list, select the WMI monitor you created, and then click the Add (<<) button.
5. Click **Update**.
6. Repeat for all appropriate nodes.

Modifying the pool to use the Dynamic Ratio load balancing method

The next task is to modify the BIG-IP LTM pool to use the Dynamic Ratio load balancing method.

To modify the load balancing method on the pool

1. On the Main tab, expand **Local Traffic** and then click **Pools**.
2. Click the name of the applicable pool.
3. On the Menu bar, click **Members**.
4. From the **Load Balancing Method** list, select **Dynamic Ratio (Node)**.
5. Click the **Update** button.

Appendix E: Configuring DNS and NTP on the BIG-IP system

If you are using the BIG-IP APM, you must have DNS and NTP settings configured on the BIG-IP system. If you do not, use the following procedures.

Configuring the DNS settings

In this section, you configure the DNS settings on the BIG-IP system to point to the Active Directory server.

➲ **Note**: *DNS lookups go out over one of the interfaces configured on the BIG-IP system, not the management interface. The management interface has its own, separate DNS settings.*

➲ **Important:** *The BIG-IP system must have a Route to the Active Directory server. The Route configuration is found on the Main tab by expanding **Network** and then clicking **Routes**. For specific instructions on configuring a Route on the BIG-IP system, see the online help or the product documentation.*

To configure DNS settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **DNS**.
3. In the **DNS Lookup Server List** row, complete the following:
   a. In the **Address** box, type the IP address of a DNS server that can resolve the Active Directory server.
   b. Click the **Add** button.
4. Click **Update**.

Configuring the NTP settings

The next task is to configure the NTP settings on the BIG-IP system for authentication to work properly.

To configure NTP settings

1. On the Main tab, expand **System**, and then click **Configuration**.
2. On the Menu bar, from the **Device** menu, click **NTP**.
3. In the **Address** box, type the fully-qualified domain name (or the IP address) of the time server that you want to add to the Address List.
4. Click the **Add** button.
5. Click **Update**.

To verify the NTP setting configuration, you can use the **ntpq** utility. From the BIG-IP command line, run **`ntpq -np`**.

See *http://support.f5.com/kb/en-us/solutions/public/10000/200/sol10240.html* for more information on this command.

Document Revision History

Version	Description	Date
1.0	New Version	08-15-2012
1.1	Added a Source Mask value to the OneConnect profile in the configuration table on *page 30.* This Source Mask is necessary when also using an NTLM profile.	02-04-2013
1.2	Removed the double backslashes from the health monitor send string and highlighted the FQDN as an item the user must change in *Configuration table for Dynamics CRM client-server traffic on page 30*	04-17-2013
1.3	Added a Request Header Insert value of FRONT-END-HTTPS:on to the HTTP profile in the *Configuration table for Dynamics CRM client-server traffic on page 30.*	05-17-2013
1.4	Added an iRule to disable BIG-IP APM when CRM requests come from Microsoft Outlook. The Outlook CRM plug-in is incompatible with BIG-IP APM at this time.	08-15-2013
1.5	- Added Dynamics CRM Update Rollup 15 to the list of recommended versions. - Added support for BIG-IP versions up to 11.4.1. - Expanded *Configuring the BIG-IP system for Dynamics CRM server-to-server traffic on page 41* which now includes two options, one if there is a device performing address translation between the system and the servers, and one if there is not.	11-08-2013
2.0	- Added support for Dynamics 2013 - Added support for BIG-IP version 11.5 - Added the section *Configuring the BIG-IP system for ADFS 2.0 to support Claims-based authentication/IFD on page 33* - Moved the server-to-server configuration tables to a new Appendix	02-14-2014
2.1	Updated and expanded the section *Why F5? on page 1.*	03-20-2014
2.2	- Added an entry to *Troubleshooting on page 28* for client connections that are unresponsive or seem to hang when using the OneConnect feature. - Added support for BIG-IP version 11.5.1.	06-20-2014
2.3	- Added a note to *Configuring BIG-IP Access Policy Manager for Dynamics CRM 2011 and 2013 on page 33* that if using BIG-IP APM, you must add the FQDN for the Dynamics deployment to Trusted Sites in Internet Explorer. - Added the requirement that **Keep Accept Encoding** must be enabled on the HTTP Compression profile.	08-04-2014
2.4	Added support for BIG-IP version 11.6	08-25-2014
2.5	Added support for Dynamics CRM 2013 SP1	09-04-2014
2.6	- Updated this guide to reference the Dynamics CRM 2011 and 2013 iApp template available on downloads.f5.com in the RELEASE-CANDIDATE folder. - Added the iApp walkthrough section, as well as manual configuration guidance for BIG-IP AFM. - Removed the section Configuring the BIG-IP system for AD FS 2.0 to support Claims-based authentication/IFD, as there is now a full F5 with AD FS deployment guide. Added the link to the AD FS guide to Prerequisites and configuration notes.	10-06-2014
2.7	- Added a new entry to the troubleshooting section page 29 with a required modification to the configuration produced by the iApp template if using BIG-IP AFM and the IP Intelligence database to log or restrict traffic with low reputation scores.	10-30-2014
2.8	- Updated this guide to reference the fully supported Dynamics CRM 2011 and 2013 iApp template available on downloads.f5.com. - Resolved the issue with BIG-IP AFM and the IP intelligence where connections where not being logged or rejected. The iApp now properly creates the Blacklist categories. Made a note in the troubleshooting entry.	12-16-2014
2.9	Added the section *Optional: Configuring BIG-IP LTM/APM to support NTLMv2-only deployments on page 26.*	04-23-2015

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com