Deployment Guide

Deploying the BIG-IP LTM v11 with Microsoft Lync Server 2010 and 2013

Welcome to the Microsoft® Lync™ Server 2010 and 2013 deployment guide. This document contains guidance on configuring the BIG-IP® Local Traffic Manager™ (LTM) with Microsoft Lync Server 2010 and 2013. BIG-IP version 11.0 introduced iApp™ Application templates, an extremely easy way to configure the BIG-IP system for Microsoft Lync Server.

Why F5?

This deployment guide is the result of collaboration and interoperability testing between Microsoft and F5 Networks using Microsoft Lync Server and the BIG-IP LTM. Microsoft ***requires*** hardware load balancing for Lync Web Services. Organizations using the BIG-IP LTM benefit from mission-critical availability, intelligent traffic management, simple scalability, and enhanced security for Lync Server deployments. This deployment also describes how to use the BIG-IP system as a reverse proxy, eliminating the need for a separate reverse proxy device.

For more information on Microsoft Lync Server see *http://www.microsoft.com/en-us/lync/default.aspx*

For more information on the F5 BIG-IP LTM, see
http://www.f5.com/products/big-ip/product-modules/local-traffic-manager.html

For instructions on configuring BIG-IP Global Traffic Manager (GTM) and BIG-IP LTM modules to support site resiliency for Microsoft Lync Server 2010 and 2013, see *http://www.f5.com/pdf/deployment-guides/lync-2010-site-resiliency-dg.pdf*

Products and versions tested

Product	Version
BIG-IP LTM and Virtual Edition	Manual configuration: v11, 11.0.1, 11.1, 11.2, 11.3, 11.4, 11.5, 11.5.1, 11.6 iApp Template: 11.2 - 11.6
Microsoft Lync Server	2010, 2013
iApp Template Version	f5.microsoft_lync_server_2010_2013.v1.3.0
Deployment Guide version	4.4 (see *Revision History on page 42)*

➲ **Important:** *Make sure you are using the most recent version of this deployment guide:*
http://www.f5.com/pdf/deployment-guides/microsoft-lync-iapp-dg.pdf

Contents

What is F5 iApp? 3

Prerequisites and configuration notes 3

Configuration examples 4

Using this guide 5

Configuring the iApp for Microsoft Lync Server 2010 or 2013 6

Using separate internal and external BIG-IP systems versus a single BIG-IP system 6

Downloading and importing the Lync 2010 and 2013 iApp 7

Advanced options 7

Inline help 7

Tell us about your Lync Server deployment 8

Microsoft Lync Server Front End Virtual Server Questions 8

Front End Server Pools 10

Front End Mediation Server Pools 10

Microsoft Lync Server Director Virtual Server Questions 11

Director Server Pools 11

Microsoft Lync Server Edge Virtual Servers - External Interface 12

Edge Server Pools - External Interface 16

Microsoft Lync Server Edge Virtual Servers - Internal Interface 17

Edge Server Pools - Internal Interface 18

Configuring the iApp for Lync Reverse Proxy 19

Modifying the iApp configuration 27

Troubleshooting 28

Creating a forwarding virtual server for Lync Edge server to Lync client communication 29

Next steps 30

Appendix: Manual Configuration table for BIG-IP objects 31

Revision History 42

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 Lync acts as the single-point interface for building, managing, and monitoring Microsoft Lync Server 2010 and 2013. For more information on iApp, see the *F5 iApp: Moving Application Delivery Beyond the Network* White Paper: *http://www.f5.com/pdf/white-papers/f5-iapp-wp.pdf*.

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- **Critical:** Do not use f5.microsoft_lync_server_2010 version of the iApp template that ships with the BIG-IP system by default.F5 has released an updated and officially supported version of the iApp template for Microsoft Lync Server 2010 and 2013, which must be downloaded from downloads.f5.com as shown in this document. This guide is based the new iApp.

- For users familiar with the BIG-IP system, there is manual configuration guidance at the end of this guide. However, because of the complexity of this configuration, we recommend most users deploy using the iApp template.

- There are a number of advantages for using the F5 Global Traffic Manager (GTM) to support site resiliency for Microsoft Lync Server 2010. For more information, see: *http://www.f5.com/pdf/deployment-guides/lync-2010-site-resiliency-dg.pdf*

  Lync Server 2013 uses the new Microsoft Office Web Apps Server 2013 for sharing Microsoft PowerPoint presentations between computers running the Lync 2013 client. F5 provides detailed configuration steps for deploying, securing, and optimizing Office Web Apps 2013 in the deployment guide available on f5.com:
  http://www.f5.com/pdf/deployment-guides/microsoft-office-web-apps-dg.pdf.

- When used with Lync 2010 or 2013, a BIG-IP appliance and the BIG-IP VE (Virtual Edition) are configured in the same manner and offer the same functionality. Performance for large-scale sites is better met with BIG-IP hardware, particularly for functions such as the Edge Web Conferencing service where SSL/TLS connections are terminated on the BIG-IP LTM.

- Microsoft documentation refers to a hardware load balancer (HLB), this is the equivalent to the industry term *Application Delivery Controller (ADC)*, in this case F5's BIG-IP LTM.

- **Critical:** *If you are using a BIG-IP version prior to 11.2 only:*
  Because this iApp uses an HTTP and SIP monitor, if you disable Strict Updates after completing the iApp configuration, the monitors stop sending requests, and mark the nodes down. At this time, we do not recommend disabling Strict Updates. If you find you need a part of the configuration that is not present in the iApp, use *Appendix: Manual Configuration table for BIG-IP objects on page 31.*

- The BIG-IP LTM can be used in place of "DNS load balancing" in front of an Enterprise Edition pool of Front End servers and a pool of Director servers. Also, BIG-IP LTM is supported between the Front End and Edge servers, and in front of Edge servers.

- You must provision appropriate IP addresses for use in the BIG-IP virtual servers. See the Configuration tables for number of virtual servers and their Lync Server role.

- For an in-depth look at load balancing Lync Edge servers, see *https://devcentral.f5.com/articles/the-hopefully-definitive-guide-to-load-balancing-lync-edge-servers-with-a-hardware-load-balancer*

- Depending on which Lync Services you are deploying for the iApp, you need to know specific information from your Lync Server implementation to include when configuring the BIG-IP system. The following list shows the information you need and where to find it in the Lync Topology Builder. For more information, see the Lync documentation.
  - Define Simple URLs: **Site Properties>Simple URLs**.
  - Front End Web Services FQDNs, Hardware Load Balancer Monitoring Port, Collocated Mediation Server: **Enterprise Edition Front End Pool>Pool Properties**.
  - Director Web Services FQDNs: **Director Pools>Pool Properties**.
  - Edge Internal FQDN, Next Hop Pool, External Edge Services FQDNs and ports: **Edge Pools>Pool Properties**.
  - Specific settings for Edge: **A/V Edge service is NAT enabled**: **Not Checked**
  - Next hop selection: **Select Director pool if deploying Director Servers**

You can run the Lync Topology Builder either before or after performing the BIG-IP configuration; however, because of the complexity of Lync deployment, F5 recommends gathering all information required by **both** the Lync Topology Builder and the iApp template prior to beginning. For more information, see the Microsoft Lync documentation.

- Deploying a third-party external reverse proxy server behind the BIG-IP LTM is not a supported configuration.
- If you have Lync 2013 clients who will be connecting through the Lync Edge external A/V UDP virtual server, be sure to see *Troubleshooting on page 28.*

Configuration examples

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

The following example shows a typical configuration with a BIG-IP LTM system and a Lync Server deployment. With multiple Lync Servers in a pool there is a need for distributing the incoming session requests among the servers. Figure 1 shows a logical configuration diagram.

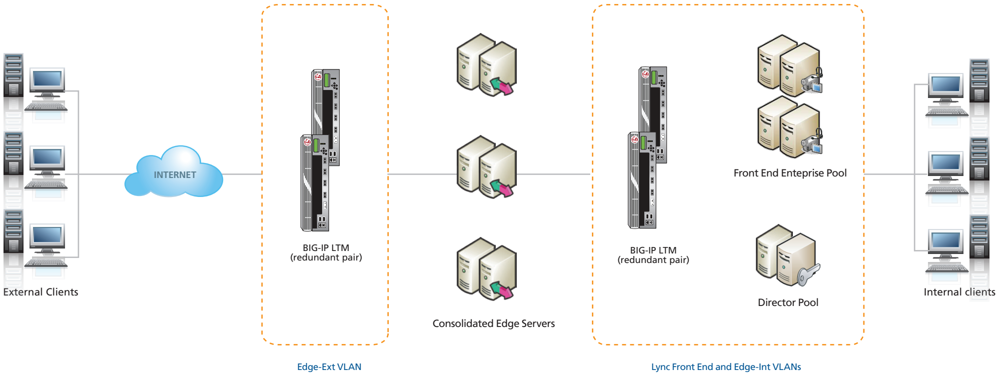


Figure 1: *Logical configuration example*

The following simplified diagram show another possible configuration option using the BIG-IP LTM with Lync Server 2010 and 2013 available in the iApp template.

Figure 2 shows a single BIG-IP LTM (redundant pair) for all internal and external Lync Server services.

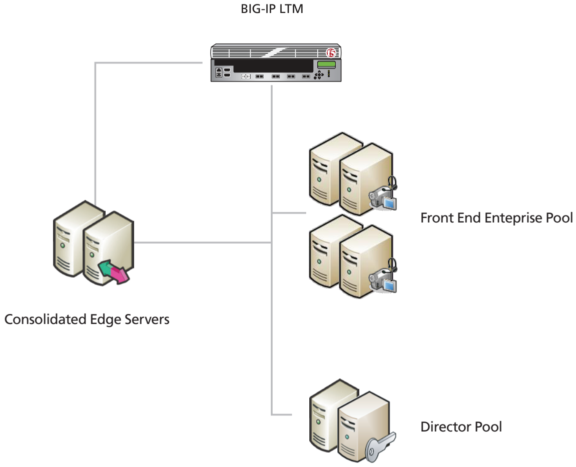


Figure 2: *Alternate logical configuration example*

Using this guide

This deployment guide is intended to help users deploy Microsoft Lync Server 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 document for guidance on configuring the iApp template

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

The iApp template configuration portion of this guide walks you through the entire iApp, giving detailed information not found in the iApp or online 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)*

Manually configuring 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 Lync 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: Manual Configuration table for BIG-IP objects on page 31.*

Configuring the iApp for Microsoft Lync Server 2010 or 2013

Use the following guidance to help you configure Microsoft Lync Server using the BIG-IP iApp template. You must have downloaded and imported the new Lync iApp before beginning. See *Downloading and importing the Lync 2010 and 2013 iApp on page 7.*

Using separate internal and external BIG-IP systems versus a single BIG-IP system

You can use the iApp template to configure BIG-IP devices whether your Lync implementation is using a single BIG-IP system (or redundant pair), or separate internal and external BIG-IP systems. The following sections provide guidance on which sections you need to configure in the iApp on which BIG-IP systems.

Using separate internal and external BIG-IP systems

If you are deploying Lync Server on multiple standalone or redundant BIG-IP systems, as shown in the logical configuration example on page 3, you must complete these sections of the iApp template on each respective BIG-IP system:

- *DMZ/Perimeter Network BIG-IP system* (if deploying Lync Edge services):
  - Microsoft Lync Server Edge Virtual Servers - External Interface
  - Edge Server Pools - External Interface
  - Microsoft Lync Server Reverse Proxy - Reverse Proxy > Forward Reverse Proxy client traffic to another BIG-IP system (if using the BIG-IP system as an external Lync reverse proxy)
- *Internal Network BIG-IP system*
  - Microsoft Lync Server Front End Virtual Servers
  - Front End Server Pools
  - Microsoft Lync Server Director Virtual Servers (if deploying Director servers)
  - Director server Pools (if deploying Director servers)
  - Microsoft Lync Server Edge Virtual Servers - Internal Interface (if deploying Edge services)
  - Edge Server Pools - Internal Interface (if deploying Lync Edge services)
  - Microsoft Lync Server Reverse Proxy - Reverse Proxy > Receive Reverse Proxy traffic from another BIG-IP system (if deploying Edge services and if using BIG-IP to receive Lync reverse proxy traffic from another BIG-IP or 3rd-party reverse proxy server)

Using a single BIG-IP system (or redundant pair)

If you are deploying Lync Server on a single standalone or redundant pair of BIG-IP systems, as shown in the alternate logical configuration example on page 4, you must complete these sections of the iApp template:

- Microsoft Lync Server Edge Virtual Servers - External Interface (if deploying Edge services)
- Edge Server Pools - External Interface (if deploying Lync Edge services)
- Microsoft Lync Server Reverse Proxy - Reverse Proxy > Forward Reverse Proxy traffic to Lync server(s)
- Microsoft Lync Server Front End Virtual Servers
- Front End Server Pools
- Microsoft Lync Server Director Virtual Servers (if deploying Director servers)
- Director server Pools (if deploying Director servers)
- Microsoft Lync Server Edge Virtual Servers - Internal Interface (if deploying Edge services)
- Edge Server Pools - Internal Interface (if deploying Lync Edge services)

Downloading and importing the Lync 2010 and 2013 iApp

The first task is to download the latest iApp for Microsoft Lync 2010 and 2013 and import it onto the BIG-IP system. You can use this iApp for Lync Server 2010 or 2013.

To download and import the iApp

1. Open a web browser and go to *http://support.f5.com/kb/en-us/solutions/public/15000/600/sol15655.html*
2. Follow the instructions to download the **f5.microsoft_lync_server_2010_2013.<latest-version>.zip** file to a location accessible from your BIG-IP system.
3. Extract (unzip) the **f5.microsoft_lync_server_2010_2013.<latest-version>.tmpl** file.
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 Lync Server iApp

To begin the Lync 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 **Lync-2013_.**
5. From the **Template** list, select **f5.microsoft_lync_server_2010_2013.<latest version>**. The new Lync Server template opens.

Advanced options

If you select **Advanced** from the **Template Selection** list at the very top of the template, 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 BIG-IP system 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.

Inline help

At the bottom of the Welcome section, the iApp template asks about inline help text.

1. ***Do you want to see inline help?***
   Select 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 all 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**
  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.

Tell us about your Lync Server deployment

In this section, you select whether you are deploying the iApp for Lync Server 2010 or 2013.

1. ***Which version of Lync Server are you using?***
   The first question in this section asks which version of Microsoft Lync Server you are using, 2010 or 2013. Select the appropriate version from the list.
   - **Lync Server 2010**
     Select this option if you are using Lync Server 2010.
   - **Lync Server 2013**
     Select this option if you are using Lync Server 2013. You must then answer the following question.
     a. *Do you have Lync 2010 servers in your Lync 2013 environment?*
        If you select Lync Server 2013, this row appears asking if your Lync 2013 deployment is using any Lync 2010 servers. The selection you make here determines persistence method and settings. It is important you choose the appropriate setting here, as the implementation might not function properly if you do not.
        - **No, there are no Lync 2010 servers**
          Select this option if your Lync 2013 deployment does not contain any Lync 2010 servers.
        - **Yes, there are Lync 2010 and Lync 2013 servers**
          Select this option if your deployment includes both 2010 and 2013 Lync servers.

Configuring the iApp for Lync Front End Servers

This group of questions gathers information for the virtual servers for the Lync Front End Services.

Microsoft Lync Server Front End Virtual Server Questions

Use this section for configuring the iApp for Front End servers.

1. ***Are you deploying this system for internal Front End services?***
   Select whether you are deploying the BIG-IP system Lync Front End services at this time.
   - **No, do not deploy this BIG-IP system for Front End services**
     Select this option if you are not deploying the BIG-IP system for Front End Servers at this time. You can always re-enter the template at a later time to add Front End Servers to the deployment.
   - **Yes, deploy this BIG-IP system for Front End services**
     Select this option if you are deploying the BIG-IP system for Front End services.
     a. *What IP address do you want to use for the Front End virtual server?*
        This is the address clients use to access Lync (or a FQDN will resolve to this address). The BIG-IP system will create multiple virtual servers using this address on different ports for the different Front End Services.
     b. *How have you configured routing on your Lync Front End servers?*
        Select whether the Front End servers have a route through the BIG-IP system or not. If the Lync Front End Servers do not have a route back for clients through the BIG-IP system, (i.e. if they do not use the BIG-IP system as the default gateway), the BIG-IP system uses Secure Network Address Translation (SNAT) to translate the client's source address to an address configured on the BIG-IP system.

If you indicate that the Lync Front End Servers do have a route back to the clients through the BIG-IP system, the BIG-IP system does not translate the client's source address; in this case, you must make sure that the system is configured as the gateway to the client networks (usually the default gateway) on the Front End servers.

- **Servers do not have a route to clients through the BIG-IP system**
  Select this option if your Lync Front End Servers do not have a route back to Lync clients through this BIG-IP system.

  i). *How many connections do you expect to each Front End server?*
  Select whether you expect more than 64,000 concurrent connections to each Lync Front End server.

  - **Fewer than 64,000 concurrent connections per server**
    Select this option if you expect fewer than 64,000 concurrent connections per Lync Front End server. With this option, the system applies SNAT Auto Map, which does not require any additional IP addresses, as the system uses an existing self IP address for translation.
  - **More than 64,000 concurrent connections per server**
    Select this option if you expect more than 64,000 connections at one time to each server. With this option, the iApp creates a SNAT Pool, for which you need one IP address for each 64,000 concurrent connections you expect.

    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, or fraction thereof. Click **Add** for additional rows.

  ⓘ ***Important***

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

- **Servers have a route to clients through the BIG-IP system**
  Select this option if you have configured a route on the BIG-IP system for traffic coming from the Front End servers back to Lync clients.

c. *On which VLAN(s) should internal Front End traffic be enabled?* New
Specify the VLANs from which the BIG-IP system should accept internal Front End traffic. This optional feature can provide an additional layer of security, as you can allow traffic only from the VLANs you choose. The VLAN objects must already be configured on this BIG-IP system before you can select them.

By default, all VLANs configured on the system appear in the Selected (allowed) box. If you do not move any VLANs, the BIG-IP system accepts traffic from all VLANs. Use the Move buttons (<<) and (>>) to adjust list membership.

d. *Have you enabled a hardware load balancing monitoring port on your Front End Servers?*
Specify whether you have enabled a hardware load balancing monitoring port (the default is 5060) on your Front End Servers.

- **No, a hardware load balancing port is not enabled**
  Select this option if you have not enabled a hardware load balancing port. No further information is needed.
- **Yes, a hardware load balancing port is enabled**
  Select this option if you have enabled a hardware load balancing port. You must answer the following question about which port you are using.

  i). *What port have you enabled?*
  Specify the monitoring port you are using for hardware load balancing. The default is **5060**.

e. *Are you using Microsoft Lync Server Mediation services?*
Choose whether you are deploying Mediation Services at this time. Lync Mediation services are a necessary component for implementing Enterprise Voice and dial-in conferencing.

- **No, this deployment does not use Mediation servers**
  Select this option if you are not deploying the BIG-IP system for Mediation services at this time. You can always re-enter the template at a later time to add this feature.
- **Yes, this deployment uses Mediation services.**
  Select this option if you want the BIG-IP system to support Mediation services.

  i). <u>Are your Mediation Servers separate from the Front End Servers?</u>
  The system needs to know if your Mediation Servers are on different servers than your Front End Servers.

  - **No, both services are on the same server(s)**
    Select this option if your Mediation Servers are on the same servers as your Front End Servers. No further information is required. Continue with the next section.
  - **Yes, each service is on a separate server**
    Select this option if you want to deploy the BIG-IP system for separate Mediation Servers. A new section appears after the Front End Server Pools section asking for information about your Mediation Servers.

Front End Server Pools

This group of questions gathers information about your Front End Servers to create the BIG-IP load balancing pool.

1. ***<u>Which load balancing method do you want to use?</u>***
   Specify the load balancing method you want the BIG-IP system to use for the Front End Servers. While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (node)**.

2. ***<u>Which Front End servers should be in this pool?</u>***
   Type the IP address for each Lync Front End Server. You can optionally add a Connection Limit. Click **Add** to include additional servers. You must add at least one Front End Server here.

Front End Mediation Server Pools

This section only appears if you specified you are deploying Mediation Servers and they are on different servers than the Front End Servers.

This group of questions gathers information about your Front End Servers to create the BIG-IP load balancing pool.

1. ***<u>Which load balancing method do you want to use?</u>***
   Specify the load balancing method you want the BIG-IP system to use for the Mediation Servers. While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (node)**.

2. ***<u>Which Mediation servers should be in this pool?</u>***
   Type the IP address for each Mediation Server. You can optionally add a Connection Limit. Click **Add** to include additional servers. You must add at least one Mediation Server here.

Configuring the iApp for Lync Director Servers

This section of the template asks questions about your Lync Server Director servers

Microsoft Lync Server Director Virtual Server Questions

This group of questions gathers information for the virtual servers for the Lync Director servers. Use this section to deploy Lync 2010/2013 Director servers to refer internal clients to their home pools. If deploying Lync Edge services, Director servers also proxy external connections for meeting and phone conferencing simple URLs.

1. ***Are you deploying this system for internal Director services?***
   Specify whether you are deploying the BIG-IP system for Lync Server Director servers at this time.
   - **No, do not deploy this BIG-IP system for Director services**
     Select this option if you are not deploying the BIG-IP system for Director servers at this time. You can always re-enter the template at a later time to add Director servers to the deployment.
   - **Yes, deploy this BIG-IP system for Director services**
     Select this option if you are deploying the BIG-IP system for Director servers.
     a. *What IP address do you want to use for this server?*
        Type the IP address the BIG-IP system will use for the Lync Director server virtual server.
        - **Servers have a route to clients through the BIG-IP system**
          Select this option if you have configured a route on the BIG-IP system for traffic coming from the Director servers back to Lync clients.

Director Server Pools

This section only appears if you specified you are deploying Director servers.

This group of questions gathers information about your Director servers to create the BIG-IP load balancing pool.

1. ***Which load balancing method do you want to use?***
   Specify the load balancing method you want the BIG-IP system to use for the Director servers. While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (node)**.
2. ***Which Director servers should be in this pool?***
   Type the IP address for each Director server. You can optionally add a Connection Limit. Click **Add** to include additional servers. You must add at least one Director server here.

Configuring the iApp for Lync Edge Servers - External Interface

This section of the template asks questions about your Lync Server Edge Servers - External Interface. This includes the Access, A/V, and Web Conferencing services.

Important

Be sure to see ***Modifying the iApp configuration on page 27*** *for an important change to the virtual server.*

You must provision one unique, publicly routable IP address for each BIG-IP virtual server you create here, plus an additional publicly routable IP address per Edge Server for each Lync Edge service you are deploying. For example, if you are deploying all three services on two Edge Servers, you need to provision nine unique, publicly routable IP addresses.

Microsoft Lync Server Edge Virtual Servers - External Interface

This group of questions gathers information for the virtual servers for the Edge Servers - External Interface.

1. ***Are you deploying this system for Lync external Edge services?***
   The first question in this section asks if you are deploying Edge Servers - External Interface at this time. Select **Yes** from the list if you are deploying Edge Servers - External Interface. The Edge Server External Interface options appear.

   - **No, do not deploy this BIG-IP system for external Edge services**
     Select this option if you are not deploying the BIG-IP system for the Edge Server - External Interface at this time. You can always re-enter the template at a later time to add this option to the deployment.

   - **Yes, deploy this BIG-IP system for external Edge services**
     Select this option if you are deploying the BIG-IP system for the Edge Server - External Interface.

     a. *How have you configured routing on your Lync Edge servers?*
        Select whether the Edge servers have a route through the BIG-IP system or not. If the servers do not have a route back for clients through the BIG-IP system, (i.e. if they do not use the BIG-IP system as the default gateway), the BIG-IP system uses Secure Network Address Translation (SNAT) to translate the client's source address to an address configured on the BIG-IP system.

        If you indicate that the Edge servers do have a route back to the clients through the BIG-IP system, the BIG-IP system does not translate the client's source address; in this case, you must make sure that the system is configured as the gateway to the client networks (usually the default gateway) on the servers.

        - **Servers do not have a route to clients through the BIG-IP system**
          Select this option if your servers do not have a route back to Lync clients through this BIG-IP system.

          i). *How many connections do you expect to each Edge server?*
          Select whether you expect more than 64,000 concurrent connections to each server.

          - **Fewer than 64,000 concurrent connections per server**
            Select this option if you expect fewer than 64,000 concurrent connections per server. With this option, the system applies SNAT Auto Map, which does not require any additional IP addresses, as the system uses an existing self IP address for translation.

          - **More than 64,000 concurrent connections per server**
            Select this option if you expect more than 64,000 connections at one time to each server. With this option, the iApp creates a SNAT Pool, for which you need one IP address for each 64,000 concurrent connections you expect.

            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, or fraction thereof. Click **Add** for additional rows.

          Important

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

- **Servers have a route to clients through the BIG-IP system**
  Select this option if you have configured a route on the BIG-IP system for traffic coming from the Edge servers back to Lync clients.

b. *On which VLAN(s) should external Edge traffic be enabled?* New
Specify the VLANs from which the BIG-IP system should accept external Edge traffic. This optional feature can provide an additional layer of security, as you can allow traffic only from the VLANs you choose. The VLAN objects must already be configured on this BIG-IP system before you can select them.

By default, all VLANs configured on the system appear in the Selected (allowed) box. If you do not move any VLANs, the BIG-IP system accepts traffic from all VLANs. Use the Move buttons (<<) and (>>) to adjust list membership.

c. *How have you configured Lync Edge services in Lync Topology Builder?* New
Choose how you have configured Lync Edge pool services in the Lync Topology Builder. When defining an Edge pool in the Topology Builder, you can specify a single IP address with unique ports for each Edge service, or a unique IP address and FQDN for each service.

- **Lync Edge services use unique FQDNs and IP addresses**
  Select this option if each of your Lync Edge services use a unique FQDN and IP address. The system will create a separate virtual server for each service you select in the following questions.

  i). *What IP address do you want to use for the Access Service virtual server?*
  Type the IP address the BIG-IP system will use for the Edge Servers - External Interface Access Service virtual server. This must be a unique, publicly routable IP address.

  ii). *On which port do Edge servers listen for Access Service traffic?*
  Select the appropriate port on which your Edge Servers listen for Access service traffic. You can select **443** or **5061**.

  iii). *Have you enabled federation on port 5061 in the Lync Server Topology?*
  Choose whether you have enabled federation in the Lync Server Topology (on port 5061).

  - **No, federation on port 5061 is not enabled**
    Select this option if you have not enabled federation on port 5061 in your Lync Server Topology. Continue with the next question.
  - **Yes, federation on port 5061 is enabled.**
    Select this option if you have enabled federation in the Lync Server Topology (on port 5061). The iApp creates an additional virtual server for federation.

  iv). *Have you enabled federation with XMPP providers on port 5269 in the Lync Topology?*
  This question only appears if you chose you are deploying Lync 2013.

  Choose whether you have enabled federation with XMPP providers in the Lync Server Topology (on port 5269).

  - **No, federation with XMPP on port 5269 is not enabled**
    Select this option if you have not enabled federation with XMPP on port 5269 in your Lync Server Topology. Continue with the next question.
  - **Yes, federation with XMPP on port 5269 is enabled**
    Select this option if you have enabled federation with XMPP on port 5269 in your Lync Server Topology. The iApp creates an additional virtual server.

  v). *Should the system monitor the internal SIP virtual servers?*
  Select whether you want to create a second monitor to check the health of the internal SIP virtual server. If this server is marked down, the Access Edge Service virtual server will be marked down. This monitor is useful if configuring Lync with BIG-IP GTM in multiple data centers for site resiliency. This is the same monitor described in *Creating a SIP monitor for the Front End servers on page 39, however in this case, the port is 5061.*

  - **No, do not monitor the internal SIP virtual servers**
    Select this option is you do not want to monitor the health of the internal SIP virtual servers. Continue with the next question.

- **Yes, monitor the internal SIP virtual servers**
  Select this option if you want the BIG-IP system to monitor the health of the internal SIP virtual servers.

  1). *What is the Front End virtual server IP address on the internal BIG-IP LTM?*
  Type the IP address of your internal BIG-IP LTM Front End virtual server. This is the IP address you specified in question 1a *on page 8*.

vi). *Are you deploying this system for Web Conferencing services?*
Select whether you are deploying the Edge Server Web Conferencing Service at this time.

- **No, do not deploy this BIG-IP system for Web Conferencing services**
  Select this option if you are not deploying the Web Conferencing service at this time. You can always re-enter the template at a later time to add the Web Conferencing service to the configuration.
- **Yes, deploy this BIG-IP system for Web Conferencing services**
  Select this option if you want to deploy the BIG-IP system for the Web Conferencing service.

  1). *What IP address do you want to use for the Web Conferencing service virtual server?*
  If you select Yes, a new row appears asking for the publicly routable IP address you want to use for the Web Conferencing virtual server. Type the IP address the BIG-IP system will use for the Edge Servers - External Interface Web Conferencing Service virtual server.

vii). *Are you deploying this system for A/V Edge Services?*
Select whether you are deploying the Edge Server A/V service at this time.

- **No, do not deploy this BIG-IP system for the A/V service.**
  Select this option if you are not deploying the A/V service at this time. You can always re-enter the template at a later time to add the A/V service to the configuration.
- **Yes, deploy this BIG-IP system for the A/V service**
  Select this option if you want to deploy the BIG-IP system for the A/V service.

  1). *What IP address do you want to use for the A/V service virtual server?*
  If you select Yes, a new row appears asking for the publicly routable IP address you want to use for the A/V virtual server. Type the IP address the BIG-IP system will use for the Edge Servers - External Interface A/V virtual server.

  2). *Should the system translate the source address of A/V service connections?*
  Select whether you want the BIG-IP system to use SNAT for the A/V service. For optimal performance, we do not recommend using SNAT for A/V traffic.

Warning

For best performance, F5 recommends against translating the source address (using SNAT) for Lync A/V traffic, as it is optimal if the Lync Edge servers see the IP address of clients for peer-to-peer client communication. If you do select to translate the source address for A/V connections, the system proxies all A/V traffic through the Lync Edge servers.

» No, do not translate the source address of A/V connections
Select this option if you do not want to use SNAT on the BIG-IP system for A/V traffic. We recommend this option for the best performance.

» Yes, translate the source address of A/V connections
Select this option if you want the BIG-IP system to use SNAT for A/V traffic. If you selected **No** in question "*a*" in this section, the system uses the same SNAT setting (Auto Map or a SNAT pool) for the A/V service. Otherwise, if you select to SNAT A/V connections in this question, the system uses SNAT Auto Map.

- **Lync Edge services use a single FQDN and IP address**
  Select this option if all of your Lync Edge services use a single FQDN and IP address.

i). *What IP address do you want to use for the Lync Edge services virtual servers?*
Type the IP address the BIG-IP system will use for Edge Servers - External Interface virtual servers. This must be a unique, publicly routable IP address. The system will use this address for all of the Edge services you choose in this section.

ii). *On which port do Edge servers listen for Access Service traffic?*
Select the appropriate port on which your Edge Servers listen for Access service traffic. You can select **443** or **5061**.

iii). *Have you enabled federation with XMPP providers on port 5269 in the Lync Topology?*
This question only appears if you chose you are deploying Lync 2013.

Choose whether you have enabled federation with XMPP providers in the Lync Server Topology (on port 5269).

- **No, federation with XMPP on port 5269 is not enabled**
  Select this option if you have not enabled federation with XMPP on port 5269 in your Lync Server Topology. Continue with the next question.
- **Yes, federation with XMPP on port 5269 is enabled**
  Select this option if you have enabled federation with XMPP on port 5269 in your Lync Server Topology. The iApp creates an additional virtual server.

iv). *Should the system monitor the internal SIP virtual servers?*
Select whether you want to create a second monitor to check the health of the internal SIP virtual server. If this server is marked down, the Access Edge Service virtual server will be marked down. This monitor is useful if configuring Lync with BIG-IP GTM in multiple data centers for site resiliency. This is the same monitor described in *Creating a SIP monitor for the Front End servers on page 39, however in this case, the port is 5061.*

- **No, do not monitor the internal SIP virtual servers**
  Select this option is you do not want to monitor the health of the internal SIP virtual servers. Continue with the next question.
- **Yes, monitor the internal SIP virtual servers**
  Select this option if you want the BIG-IP system to monitor the health of the internal SIP virtual servers.

  1). *What is the Front End virtual server IP address on the internal BIG-IP LTM?*
  Type the IP address of your internal BIG-IP LTM Front End virtual server. This is the IP address you specified in question 1a *on page 8*.

v). *Are you deploying this system for Web Conferencing services?*
Select whether you are deploying the Edge Server Web Conferencing Service at this time.

- **No, do not deploy this BIG-IP system for Web Conferencing services**
  Select this option if you are not deploying the Web Conferencing service at this time. You can always re-enter the template at a later time to add the Web Conferencing service to the configuration.
- **Yes, deploy this BIG-IP system for Web Conferencing services**
  Select this option if you want to deploy the BIG-IP system for the Web Conferencing service.

  1). *On which port do Edge servers listen for Web Conferencing service traffic?*
  Specify the port the Web Conferencing service uses in your Edge implementation. The default is 444. The BIG-IP system creates a virtual server on this port with the IP address you specified at the beginning of this section.

vi). *Are you deploying this system for A/V Edge Services?*
Select whether you are deploying the Edge Server A/V service at this time.

- **No, do not deploy this BIG-IP system for the A/V service.**
  Select this option if you are not deploying the A/V service at this time. You can always re-enter the template at a later time to add the A/V service to the configuration.
- **Yes, deploy this BIG-IP system for the A/V service**
  Select this option if you want to deploy the BIG-IP system for the A/V service.

  1). *On which port do Edge servers listen for A/V service traffic?*
  Specify the port the A/V service uses in your Edge implementation; the default is 443. The system creates a virtual server on this port with the IP address you specified at the beginning of this section.

  2). *Should the system translate the source address of A/V service connections?*
  Select whether you want the BIG-IP system to use SNAT for the A/V service. For optimal performance, we do not recommend using SNAT for A/V traffic.

⚠ ***Warning***

For best performance, F5 recommends against translating the source address (using SNAT) for Lync A/V traffic, as it is optimal if the Lync Edge servers see the IP address of clients for peer-to-peer client communication. If you do select to translate the source address for A/V connections, the system proxies all A/V traffic through the Lync Edge servers.

- No, do not translate the source address of A/V connections
  Select this option if you do not want to use SNAT on the BIG-IP system for A/V traffic. We recommend this option for the best performance.
- Yes, translate the source address of A/V connections
  Select this option if you want the BIG-IP system to use SNAT for A/V traffic. If you selected **No** in question "*a*" in this section, the system uses the same SNAT setting (Auto Map or a SNAT pool) for the A/V service. Otherwise, if you select to SNAT A/V connections in this question, the system uses SNAT Auto Map.

Edge Server Pools - External Interface

This section only appears if you specified you are deploying Edge Servers - External Interface.

This group of questions gathers information about the load balancing pools for the Edge Servers - External Interface services you are deploying. The number of questions in this section is based on your answers in the previous section.

1. ***Which load balancing method do you want to use for the Access edge service?***
   Specify the load balancing method you want the BIG-IP system to use for the Access Edge service. While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (node)**.

2. ***Which Access Edge servers should be in this pool?***
   Type the IP address for each Access Edge Server. Note these addresses should be publicly routable. You can optionally add a Connection Limit. Click **Add** to include additional servers. You must add at least one server here.

3. ***Which load balancing method do you want to use for the Web Conferencing service?***
   Specify the load balancing method you want the BIG-IP system to use for the Web Conferencing service. While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (node)**.

4. ***Which Web Conferencing servers should be in this pool?***
   Type the IP address for each Web Conferencing Edge Server. Note these addresses should be publicly routable. You can optionally add a Connection Limit. Click **Add** to include additional servers. You must add at least one server here.

5. ***Which load balancing method do you want to use for the A/V Edge service?***
   Specify the load balancing method you want the BIG-IP system to use for the A/V Edge service. While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (node)**.

6. ***Which A/V servers should be in this pool?***
   Type the IP address for each A/V Edge Server. Note these addresses should be publicly routable. You can optionally add a Connection Limit. Click **Add** to include additional servers. You must add at least one server here.

Configuring the iApp for Lync Edge Servers - Internal Interface

This section of the template asks questions about your Lync Server Edge Servers - Internal Interface. Use this section to deploy Lync Internal Edge services for internally-sourced client connections to external resources.

Microsoft Lync Server Edge Virtual Servers - Internal Interface

This group of questions gathers information for the virtual servers for the Edge Servers - Internal Interface.

1. ***Are you deploying this system for internal Edge services?***
   The first question in this section asks if you are deploying Edge Servers - Internal Interface at this time.

   - **No, do not deploy this BIG-IP system for internal Edge services**
     Select this option if you are not deploying the BIG-IP system for the Edge Server - Internal Interface at this time. You can always re-enter the template at a later time to add this option to the deployment.

   - **Yes, deploy this BIG-IP system for internal Edge services**
     Select this option if you are deploying the BIG-IP system for the Edge Server - Internal Interface.

     a. *What IP address do you want to use for this virtual server?*
     Type the IP address the BIG-IP system will use for the Edge Servers - Internal Interface virtual server.

     b. *How have you configured routing on your Lync Edge servers?*
     Select whether the Edge servers - Internal Interface have a route through the BIG-IP system to internal application clients.

     Note

     *Note that for the Edge Internal Interface, the default is **Yes**, as typically the internal interface has a route back to the BIG-IP system.*

     If you indicate that the Lync Edge Servers Internal Interface do have a route back to the clients through the BIG-IP system, the BIG-IP system does not translate the client's source address; in this case, you must make sure that the system is configured as the gateway to the client networks (usually the default gateway) on the Edge servers.

     If you do select Yes from the list, the following question about 64,000 users does not appear.

     - **Servers have a route to internal clients through the BIG-IP system**
       Select this option if the Lync Edge Servers have a route back to internal application clients via this BIG-IP system. No further information is necessary.

     - **Servers do not have a route to clients through the BIG-IP system**
       Select this option if your servers do not have a route back to internal application clients through this BIG-IP system.

       i). *How many connections do you expect to each Edge server?*
       Select whether you expect more than 64,000 concurrent connections to each server.

       - **Fewer than 64,000 concurrent connections per server**
         Select this option if you expect fewer than 64,000 concurrent connections per server. With this option, the system applies SNAT Auto Map, which does not require any additional IP addresses, as the system uses an existing self IP address for translation.

       - **More than 64,000 concurrent connections per server**
         Select this option if you expect more than 64,000 connections at one time to each server. With this option, the iApp creates a SNAT Pool, for which you need one IP address for each 64,000 concurrent connections you expect.

         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, or fraction thereof. Click **Add** for additional rows.

ⓘ ***Important***

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

c. *On which VLAN(s) should internal Edge traffic be enabled?* New
Specify the VLANs from which the BIG-IP system should accept internal Edge traffic. This optional feature can provide an additional layer of security, as you can allow traffic only from the VLANs you choose. The VLAN objects must already be configured on this BIG-IP system before you can select them.

By default, all VLANs configured on the system appear in the Selected (allowed) box. If you do not move any VLANs, the BIG-IP system accepts traffic from all VLANs. Use the Move buttons (<<) and (>>) to adjust list membership.

Edge Server Pools - Internal Interface

This section only appears if you specified you are deploying Edge Servers - Internal Interface.

This group of questions gathers information about the load balancing pools for the Edge Servers - Internal Interface services you are deploying.

1. ***Which load balancing method do you want to use?***
Specify the load balancing method you want the BIG-IP system to use for the Edge Servers - Internal Interface pool. While you can choose any of the load balancing methods from the list, we recommend the default, **Least Connections (node)**.

2. ***Which Edge servers should be in this pool?***
Type the IP address for each Lync internal Edge server. You can optionally add a Connection Limit. Click **Add** to include additional servers. You must add at least one server here.

Configuring the iApp for Lync Reverse Proxy

This section of the template asks questions about whether you are deploying the BIG-IP system for Lync web services (reverse proxy). The configuration described in this section eliminates the need for a separate reverse proxy server in your Lync environment. If you choose to configure the iApp for reverse proxy traffic, you have three options:

- ***Forward reverse proxy client traffic to another BIG-IP system***
  Select this option to use the BIG-IP LTM to act as a reverse proxy and eliminate the need for a separate device. This virtual server uses an iRule to properly send traffic to the correct location.
- ***Forward reverse proxy client traffic to Lync server(s)***
  Select this option if you are using the BIG-IP system to serve as a reverse proxy for Lync Web Services as described in the previous scenario, and are using a single BIG-IP device (or redundant pair). Lync Web Services traffic is forwarded directly to Front End or Director servers.
- ***Receive reverse proxy traffic from another BIG-IP system***
  Select this option to have the BIG-IP system create internal virtual servers to receive Lync Web Services traffic from a reverse proxy server or external BIG-IP LTM and forward it to the Front End servers. If deploying Director services, requests for simple URLs are forwarded to the Director servers. If deploying a reverse proxy server, such as Microsoft Forefront TMG, configure the proxy publishing rules to forward traffic to the IP addresses of the BIG-IP virtual servers created here.

Select the appropriate option (including choosing not deploy the system for reverse proxy services) from question #1.

Note

If you are upgrading this template from a previous version of the Lync iApp, this version of the template (v1.3) does not save the inputs from the previous Reverse Proxy section(s).

1. ***Are you deploying this BIG-IP system for Lync web services (reverse proxy) at this time?***
   The first question in this section asks if you deployed a reverse proxy as part of your Lync Edge topology.

   - **No, do not deploy this BIG-IP system for reverse proxy services**
     Select this option if you are not deploying a reverse proxy at this time. You can always re-enter the template at a later time to add the reverse proxy configuration to the deployment. Continue with the next section.
   - **Forward reverse proxy traffic to another BIG-IP system**
     Select this option to have the iApp create BIG-IP virtual servers to receive external Lync web services traffic and forward it directly to the Lync Front End/Director servers.

     a. *Do you want to forward reverse proxy traffic to Director servers?*
        Choose whether you want to forward reverse proxy traffic to the Lync Director servers.

        - **Yes, forward reverse proxy traffic to Director servers**
          Select this option if you want the system to forward reverse proxy traffic to the Lync Director servers. The system creates an addition virtual server for this traffic.
        - **No, do not forward reverse proxy traffic to Director servers**
          Select this option if you do not want the BIG-IP system to forward reverse proxy traffic to the Director servers.

     b. *Do the pool members (Lync servers or internal BIG-IP) have a route back to application clients via this BIG-IP system?*
        If the Internal BIG-IP system does not have a route back for clients through this BIG-IP system, this BIG-IP system uses Secure Network Address Translation (SNAT) to translate the client's source address to an address configured on the BIG-IP system.

        If you indicate that the internal BIG-IP system does have a route back to the clients through this BIG-IP system, the BIG-IP system does not translate the client's source address; in this case, you must make sure that the BIG-IP system is configured as the gateway to the client networks (usually the default gateway) on the Internal BIG-IP system.

        We recommend choosing **No** from the list because it does not require you to configure routing manually.

- **Pool members do not have a route to clients through the BIG-IP system**
  Select this option if the internal BIG-IP system does not have a route back to the application clients through this BIG-IP system.

  i). *How many connections do you expect to the virtual server?*
  Select whether you expect more than 64,000 concurrent connections to each server.

  - **Fewer than 64,000 concurrent connections to the virtual server**
    Select this option if you expect fewer than 64,000 concurrent connections to the virtual server. With this option, the system applies SNAT Auto Map, which does not require any additional IP addresses, as the system uses an existing self IP address for translation.
  - **More than 64,000 concurrent connections to the virtual server**
    Select this option if you expect more than 64,000 connections at one time to the virtual server. With this option, the iApp creates a SNAT Pool, for which you need one IP address for each 64,000 concurrent connections you expect.

    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, or fraction thereof. Click **Add** for additional rows.

  Important

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

- **Pool members have a route to clients through the BIG-IP system**
  Select this option if you have configured a route on the internal BIG-IP system for traffic to pass from the servers back to the application clients through this BIG-IP system.

c. *On which VLAN(s) should reverse proxy traffic be enabled?* New
Specify the VLANs from which the BIG-IP system should accept reverse proxy traffic. This optional feature can provide an additional layer of security, as you can allow traffic only from the VLANs you choose. The VLAN objects must already be configured on this BIG-IP system before you can select them.

By default, all VLANs configured on the system appear in the Selected (allowed) box. If you do not move any VLANs, the BIG-IP system accepts traffic from all VLANs. Use the Move buttons (<<) and (>>) to adjust list membership.

d. *What IP address do you want to use for the port 443 reverse proxy virtual server?*
Type the unique, publicly routable IP address you want to use for the port 443 reverse proxy virtual server. This virtual server is on port 443.

e. *What is the FQDN of your Lync Front End Web Services pool?*
Type the FQDN you configured in Lync for the External Web Services pool, such as chat.example.com.

f. *What is the FQDN of your Lync Front End Director pool?*
This question only appears if you chose to forward reverse proxy traffic to Director servers in question a.

Type the FQDN you configured in Lync for the Director pool external web services, such as dir.example.com.
When deploying Director Servers, requests for the simple URLs listed in the following questions are forwarded to the Director reverse proxy pool on the internal LTM. If not deploying Director Servers, all requests are forwarded to the internal Front End reverse proxy pool.

g. *What is the simple URL for meetings?*
Type the Meeting Simple URL you specified in your Lync configuration. For example, meet.example.com or www.example.com/meet. Do not use a trailing forward slash in this field.

h. *What is the simple URL for phone access?*
Type the Phone Access Simple URL you specified in your Lync configuration for phone access. For example, dialin.example.com or www.example.com/dialin. Do not use a trailing forward slash in this field.

i. *Do you want to include Lync Mobility services for external clients?*
Select whether you are deploying Lync Mobility services for external clients at this time.

- **No, do not deploy this BIG-IP system for Lync Mobility services**
  Select this option if you do not want to deploy the BIG-IP system for Lync Mobility services for external clients at this time. You can always re-enter the template at a later time to add this functionality to the configuration.
- **Yes, deploy this BIG-IP system for Lync Mobility services**
  Select this option if you want to deploy the BIG-IP system for Lync Mobility services.
  - *i). What is the FQDN for external Lync Mobility access?*
    Type the Lync Mobility external URL, such as: lyncdiscover.example.com

j. *Do you want to create a new client SSL profile for Front End services, or use an existing one?*
Select whether you want the iApp template to create a new client SSL profile for the Front End servers, or if you have already created one on this BIG-IP system for reverse proxy traffic. If you select an existing profile, it must have the appropriate SSL certificate and Key.

> ⓘ ***Important***
>
> *If you selected to forward reverse proxy traffic to the Director servers, and plan to use a different Client SSL profile for the Director server traffic, both the Front End and Director Client SSL profiles must be correctly configured for SNI (see the guidance in manual configuration table on page 34) and your clients must support SNI. Otherwise, we recommend using the same SSL profile for both the Front End and Director servers.*

- *Select an existing Client SSL profile*
  If you created a Client SSL profile for this reverse proxy implementation, select it from the list.
- **Create a new Client SSL profile**
  Select this option for the iApp to create a new Client SSL profile using the SSL certificate and key you imported.
  - *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.

k. *Which client SSL profile do you want to use for Director servers?*
Choose the client SSL profile you want to use for Director server reverse proxy traffic. This question appears because you selected to forward reverse proxy traffic to Director servers. Unless you have a specific need to use a custom client SSL profile or different certificates, we recommend you use the same client SSL profile (which uses the same certificate and key) as the Front End servers.

- *Select an existing Client SSL profile*
  If you created a Client SSL profile for the Director server reverse proxy traffic, select it from the list.

  > ⓘ ***Important***
  >
  > *If the profile you created uses a different certificate than the one you are using for the Front End services, it must be configured for SNI, and your clients must support SNI. Otherwise, we recommend using the same SSL profile for both the Front End and Director servers.*

- **Use the same SSL profile as the Front End Servers (recommended)**
  Select this recommended option to have the Director server reverse proxy virtual server use the same client SSL

profile as the one you used for the Front End servers. We recommend this option unless you have configured separate certificates for Lync Front End and Director services.

- **Create a new Client SSL profile**
  Select this option for the iApp to create a new Client SSL profile using the SSL certificate and key you imported for the Director servers.

  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.

l. What is the port 4443 virtual server IP address that forwards traffic to the Front End servers?
Type the IP address of the internal BIG-IP LTM reverse proxy virtual server for external web services that forwards traffic to the Lync Front End servers.

m. What is the port 4443 virtual server IP address that forwards traffic to the Director Servers?
Type the IP address of the internal BIG-IP LTM reverse proxy virtual server for external web services that forwards traffic to the Lync Director servers.

This completes the configuration for this scenario. Continue with *Finished on page 27.*

- **Forward reverse proxy traffic client traffic to Lync server(s)**
  Select this option to have the iApp create BIG-IP virtual servers to receive external Lync web services traffic and forward it directly to the Lync Front End/Director servers.

a. Do you want to forward reverse proxy traffic to Director servers?
Choose whether you want to forward reverse proxy traffic to the Lync Director servers.

- **Yes, forward reverse proxy traffic to Director servers**
  Select this option if you want the system to forward reverse proxy traffic to the Lync Director servers. The system creates an addition virtual server for this traffic.

- **No, do not forward reverse proxy traffic to Director servers**
  Select this option if you do not want the BIG-IP system to forward reverse proxy traffic to the Director servers.

b. Do the pool members (Lync servers or internal BIG-IP) have a route back to application clients via this BIG-IP system?
If the Lync Servers do not have a route back for clients through this BIG-IP system, this BIG-IP system uses Secure Network Address Translation (SNAT) to translate the source address to an address configured on the BIG-IP system.

If you indicate that the Lync Servers do have a route back to the clients through this BIG-IP system, the BIG-IP system does not translate the source address; in this case, you must make sure that the BIG-IP system is configured as the gateway to the client networks (usually the default gateway) on the Internal BIG-IP system.

We recommend choosing **No** from the list because it does not require you to configure routing manually.

- **Pool members do not have a route to clients through the BIG-IP system**
  Select this option if the Lync Servers do not have a route back to the application clients through this BIG-IP system.

  i). How many connections do you expect to the virtual server?
  Select whether you expect more than 64,000 concurrent connections to each server.

  - **Fewer than 64,000 concurrent connections to the virtual server**
    Select this option if you expect fewer than 64,000 concurrent connections to the virtual server. With this option, the system applies SNAT Auto Map, which does not require any additional IP addresses, as the system uses an existing self IP address for translation.

  - **More than 64,000 concurrent connections to the virtual server**
    Select this option if you expect more than 64,000 connections at one time to the virtual server. With this option, the iApp creates a SNAT Pool, for which you need one IP address for each 64,000 concurrent connections you expect.

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, or fraction thereof. Click **Add** for additional rows.

ⓘ ***Important***

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

- **Pool members have a route to clients through the BIG-IP system**
Select this option if you have configured a route on the BIG-IP system for traffic to pass from the servers back to the application clients through this BIG-IP system.

c. *On which VLAN(s) should reverse proxy traffic be enabled?* **New**
Specify the VLANs from which the BIG-IP system should accept reverse proxy traffic. This optional feature can provide an additional layer of security, as you can allow traffic only from the VLANs you choose. The VLAN objects must already be configured on this BIG-IP system before you can select them.

By default, all VLANs configured on the system appear in the Selected (allowed) box. If you do not move any VLANs, the BIG-IP system accepts traffic from all VLANs. Use the Move buttons (<<) and (>>) to adjust list membership.

d. *What IP address do you want to use for the port 443 reverse proxy virtual server?*
Type the unique, publicly routable IP address you want to use for the port 443 reverse proxy virtual server. This virtual server is on port 443.

e. *What is the FQDN of your Lync Front End Web Services pool?*
Type the FQDN you configured in Lync for the External Web Services pool, such as chat.example.com.

f. *What is the FQDN of your Lync Front End Director pool?*
This question only appears if you chose to forward reverse proxy traffic to Director servers in question a.

Type the FQDN you configured in Lync for the Director pool external web services, such as dir.example.com. When deploying Director Servers, requests for the simple URLs listed in the following questions are forwarded to the Director reverse proxy pool on the internal LTM. If not deploying Director Servers, all requests are forwarded to the internal Front End reverse proxy pool.

g. *What is the simple URL for meetings?*
Type the Meeting Simple URL you specified in your Lync configuration. For example, meet.example.com or www.example.com/meet. Do not use a trailing forward slash in this field.

h. *What is the simple URL for phone access?*
Type the Phone Access Simple URL you specified in your Lync configuration for phone access. For example, dialin.example.com or www.example.com/dialin. Do not use a trailing forward slash in this field.

i. *Do you want to include Lync Mobility services for external clients?*
Select whether you are deploying Lync Mobility services for external clients at this time.

- **No, do not deploy this BIG-IP system for Lync Mobility services**
Select this option if you do not want to deploy the BIG-IP system for Lync Mobility services for external clients at this time. You can always re-enter the template at a later time to add this functionality to the configuration.

- **Yes, deploy this BIG-IP system for Lync Mobility services**
Select this option if you want to deploy the BIG-IP system for Lync Mobility services.

  i). *What is the FQDN for external Lync Mobility access?*
  Type the Lync Mobility external URL, such as: lyncdiscover.example.com

j. *Do you want to create a new client SSL profile for Front End services, or use an existing one?*
Select whether you want the iApp template to create a new client SSL profile for the Front End servers, or if you have

already created one on this BIG-IP system for reverse proxy traffic. If you select an existing profile, it must have the appropriate SSL certificate and Key.

> ⓘ ***Important***
>
> *If you selected to forward reverse proxy traffic to the Director servers, and plan to use a different Client SSL profile for the Director server traffic, both the Front End and Director Client SSL profiles must be correctly configured for SNI (see the guidance in manual configuration table on page 34) and your clients must support SNI. Otherwise, we recommend using the same SSL profile for both the Front End and Director servers.*

- *Select an existing Client SSL profile*
  If you created a Client SSL profile for this reverse proxy implementation, select it from the list.
- **Create a new Client SSL profile**
  Select this option for the iApp to create a new Client SSL profile using the SSL certificate and key you imported.
  - *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.

k. *Which client SSL profile do you want to use for Director servers?*
Choose the client SSL profile you want to use for Director server reverse proxy traffic. This question appears because you selected to forward reverse proxy traffic to Director servers. Unless you have a specific need to use a custom client SSL profile or different certificates, we recommend you use the same client SSL profile (which uses the same certificate and key) as the Front End servers.

- *Select an existing Client SSL profile*
  If you created a Client SSL profile for the Director server reverse proxy traffic, select it from the list.

> ⓘ ***Important***
>
> *If the profile you created uses a different certificate than the one you are using for the Front End services, it must be configured for SNI, and your clients must support SNI. Otherwise, we recommend using the same SSL profile for both the Front End and Director servers.*

- **Use the same SSL profile as the Front End Servers (recommended)**
  Select this recommended option to have the Director server reverse proxy virtual server use the same client SSL profile as the one you used for the Front End servers. We recommend this option unless you have configured separate certificates for Lync Front End and Director services.
- **Create a new Client SSL profile**
  Select this option for the iApp to create a new Client SSL profile using the SSL certificate and key you imported for the Director servers.
  - *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.

l. *Which Front End servers should receive web services traffic?*
Type the IP address(es) of each Front End server that should receive web services traffic. Click **Add** to include additional Front End servers. You can optionally specify a Connection Limit for each server.

m. *Which Director servers should receive web services traffic*
This question only appears if you chose to forward reverse proxy traffic to Director servers in question a.

Type the IP address(es) of each Director server that should receive web services traffic. Click **Add** to include additional Director servers. You can optionally specify a Connection Limit for each server.

This completes the configuration for this scenario. Continue with *Finished on page 27.*

- **Receive reverse proxy traffic from another BIG-IP system**
Select this option if you want to configure this system to receive reverse proxy traffic from another BIG-IP system. The system creates BIG-IP virtual servers to receive Lync web services traffic from a reverse proxy server or external BIG-IP and forward it to the Lync Front End/Director servers.

  If deploying a third-party reverse proxy server, such as Microsoft Forefront TMG, configure the proxy publishing rules to forward traffic to the IP addresses of the BIG-IP virtual servers you create here. If using BIG-IP LTM to receive the external connections, specify these IP addresses in the Reverse Proxy External Interface section.

  a. *Do you want to forward reverse proxy traffic to Director servers?*
  Choose whether you want to forward reverse proxy traffic to the Lync Director servers.

    - **Yes, forward reverse proxy traffic to Director servers**
    Select this option if you want the system to forward reverse proxy traffic to the Lync Director servers. The system creates an addition virtual server for this traffic.

    - **No, do not forward reverse proxy traffic to Director servers**
    Select this option if you do not want the BIG-IP system to forward reverse proxy traffic to the Director servers.

  b. *Do the pool members (Lync servers or internal BIG-IP) have a route back to application clients via this BIG-IP system?*
  If the Internal BIG-IP system does not have a route back for clients through this BIG-IP system, this BIG-IP system uses Secure Network Address Translation (SNAT) to translate the client's source address to an address configured on the BIG-IP system.

  If you indicate that the internal BIG-IP system does have a route back to the clients through this BIG-IP system, the BIG-IP system does not translate the client's source address; in this case, you must make sure that the BIG-IP system is configured as the gateway to the client networks (usually the default gateway) on the Internal BIG-IP system.

  We recommend choosing **No** from the list because it does not require you to configure routing manually.

    - **Pool members do not have a route to clients through the BIG-IP system**
    Select this option if the internal BIG-IP system does not have a route back to the application clients through this BIG-IP system.

      i). *How many connections do you expect to the virtual server?*
      Select whether you expect more than 64,000 concurrent connections to each server.

        - **Fewer than 64,000 concurrent connections to the virtual server**
        Select this option if you expect fewer than 64,000 concurrent connections to the virtual server. With this option, the system applies SNAT Auto Map, which does not require any additional IP addresses, as the system uses an existing self IP address for translation.

        - **More than 64,000 concurrent connections to the virtual server**
        Select this option if you expect more than 64,000 connections at one time to the virtual server. With this option, the iApp creates a SNAT Pool, for which you need one IP address for each 64,000 concurrent connections you expect.

          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, or fraction thereof. Click **Add** for additional rows.

ⓘ ***Important***

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

- **Pool members have a route to clients through the BIG-IP system**
  Select this option if you have configured a route on the internal BIG-IP system for traffic to pass from the servers back to the application clients through this BIG-IP system.

c. *On which VLAN(s) should reverse proxy traffic be enabled?* **New**
Specify the VLANs from which the BIG-IP system should accept reverse proxy traffic. This optional feature can provide an additional layer of security, as you can allow traffic only from the VLANs you choose. The VLAN objects must already be configured on this BIG-IP system before you can select them.

By default, all VLANs configured on the system appear in the Selected (allowed) box. If you do not move any VLANs, the BIG-IP system accepts traffic from all VLANs. Use the Move buttons (<<) and (>>) to adjust list membership.

d. *What IP address do you want to use for the Front End port 4443 reverse proxy virtual server?*
Type the unique IP address you want to use for the port 4443 reverse proxy virtual server. This virtual server is on port 4443.

e. *What IP address do you want to use for the Director port 4443 reverse proxy virtual server?*
This question only appears if you chose to forward reverse proxy traffic to Director servers in question a.

Type the unique IP address you want to use for the port 4443 reverse proxy virtual server. This virtual server is on port 4443.

f. *Do you want to create a new client SSL profile for Front End services, or use an existing one?*
Select whether you want the iApp template to create a new client SSL profile for the Front End servers, or if you have already created one on this BIG-IP system for reverse proxy traffic. If you select an existing profile, it must have the appropriate SSL certificate and Key.

- *Select an existing Client SSL profile*
  If you created a Client SSL profile for this reverse proxy implementation, select it from the list.

- **Create a new Client SSL profile**
  Select this option for the iApp to create a new Client SSL profile using the SSL certificate and key you imported.

  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.

g. *Which client SSL profile do you want to use for Director servers?*
Choose the client SSL profile you want to use for Director server reverse proxy traffic. This question appears because you selected to forward reverse proxy traffic to Director servers. Unless you have a specific need to use a custom client SSL profile or different certificates, we recommend you use the same client SSL profile (which uses the same certificate and key) as the Front End servers.

- *Select an existing Client SSL profile*
  If you created a Client SSL profile for the Director server reverse proxy traffic, select it from the list. Unless you have specific requirements, we recommend using the same certificate and key used for the Front End services.

- **Use the same SSL profile as the Front End Servers (recommended)**
  Select this recommended option to have the Director server reverse proxy virtual server use the same client SSL profile as the one you used for the Front End servers. We recommend this option unless you have configured separate certificates for Lync Front End and Director services.
- **Create a new Client SSL profile**
  Select this option for the iApp to create a new Client SSL profile using the SSL certificate and key you imported for the Director servers.

ⓘ ***Important***

If you are using a different certificate than the one you are using for the Front End services, it must be configured for SNI, and your clients must support SNI. Otherwise, we recommend using the same SSL profile for both the Front End and Director servers.

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.

h. *Which Front End servers should receive web services traffic*
Type the IP address(es) of each Front End server that should receive web services traffic. Click **Add** to include additional Front End servers. You can optionally specify a Connection Limit for each server.

i. *Which Director servers should receive web services traffic*
This question only appears if you chose to forward reverse proxy traffic to Director servers in question a.

Type the IP address(es) of each Director server that should receive web services traffic. Click **Add** to include additional Director servers. You can optionally specify a Connection Limit for each server.

Finished

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

Modifying the iApp configuration

If you configured the iApp for Microsoft Lync Server Edge Servers: External Interface, and specified you were deploying the system for A/V Edge services, you must make a change to the virtual server configuration after completing the iApp template.

First, if you have not yet disabled Strict Updates, click **iApps > Application Services** and then click the name of your Lync application service. On the menu, click Properties, and then from the Application Service list, select **Advanced**. In the **Strict Updates** row, clear the box to disable Strict Updates.

Next, click **Local Traffic > Virtual Servers** and then from the list, click the name of the external UDP virtual server on port 3478. From the **Source Port** list, select **Change**, and then click **Update**.

Troubleshooting

Use this section for common issues and troubleshooting steps.

- **Lync clients cannot connect or receive authentication prompts when accessing Microsoft Exchange Autodiscover and EWS through F5 APM**

  When you have deployed BIG-IP APM in front of Microsoft Exchange 2010 or 2013, Microsoft Lync clients may be unable to successfully query the Autodiscover service or download free/busy information from EWS. Because this is an issue with the BIG-IP system and Exchange, to work around this issue, you must create an iRule to disable APM for these requests in your BIG-IP configuration for Exchange server. For specific instructions, see the Exchange deployment guide, available at *https://f5.com/solutions/deployment-guides/microsoft-exchange-server-2010-and-2013-big-ip-v11*

Creating a forwarding virtual server for Lync Edge server to Lync client communication

When you use F5's recommended configuration for Lync Edge services (includes both manual and iApp template configuration), you must create a forwarding BIG-IP virtual server to accept outbound traffic from the Lync Edge server. Because the Edge server(s) use the BIG-IP self IP address as a default gateway, this BIG-IP virtual server must be configured to allow asymmetric traffic to pass through the BIG-IP LTM when the Edge server is responding to direct Lync client requests.

For this configuration, you must create a Fast L4 Profile and a virtual server. Use the following table for guidance. For information on configuring specific objects, see the online help or BIG-IP documentation.

BIG-IP LTM Object	Non-default settings/Notes	
Fast L4 Profile *(Local Traffic-->Profiles--> Protocol-->Fast L4))*	***Name***	Type a unique name
	Parent Profile	**http**
	Loose Initiation	**Enabled**
	Loose Close	**Enabled**
Virtual Server *(Main tab-->Local Traffic -->Virtual Servers)*	***Name***	Type a unique name
	Type	**Performance Layer 4**
	Destination Address	**0.0.0.0/0**
	Protocol	**All Protocols**
	Protocol Profile (Client)	Select the Fast L4 profile you created
	VLANs and Tunnels	Select appropriate VLAN(s)
	Source Address Translation	**None**
	Address Translation	Clear the **Enabled** box to **disable** Address Translation
	Port Translation	Clear the **Enabled** box to **disable** Port Translation

You must also have configured a network route on the BIG-IP system for forwarding traffic from Lync Edge servers to the client network(s). To configure a BIG-IP route, see **Network > Routes**. For specific information or help, see the BIG-IP documentation or online help.

Next steps

After completing the iApp Template, the BIG-IP Application Services page opens for the Lync Server 2010 service you just created. To see the list of all the configuration objects created to support Lync Server 2010 or 2013, on the Menu bar, click **Components**. The complete list of all Lync server 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 Lync Server 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 Lync Server 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 Lync Server configuration objects.

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.

Appendix: Manual Configuration table for BIG-IP objects

Because of the complexity of this configuration, we strongly recommend using the iApp template to configure the BIG-IP system for Lync Server 2010 and 2013. Advanced users extremely familiar with the BIG-IP can use following tables to configure the BIG-IP manually. This first table shows the non-default settings on BIG-IP objects for the Lync Front End Services. BIG-IP pool members (column 2) are each of the Lync Front End Server pool members (use **Least Connections (Node)** load balancing for all pools). See *Using separate internal and external BIG-IP systems versus a single BIG-IP system on page 6* for guidance on the different BIG-IP system deployment scenarios.

Configuration table for BIG-IP objects: Lync Front End Services

Virtual Server	Pool	Health monitor	Profiles	Persistence profile	SNAT enabled?	Notes
Service Port: **80**	Service Port: **80**[1] **Action on Service down: Reject**	**Lync-http-fe**: Base HTTP parent **Lync-tcp-5061-fe:**[6] Base TCP parent: - **Alias Service Port**: **5061**	***Lync-tcp-fe***: Base TCP Parent profile with **Idle Timeout** set to **1800**	**Lync-source-fe**: Source Address Affinity parent **Timeout** set to **1800**	Yes [2]	HTTP
Service Port: **135**	Service Port: **135**[1] **Action on Service down: Reject**	**lync-tcp-monitor-fe**: Base TCP parent with no required changes	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	RPC
Service Port: **443**	Service Port: **443**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe* **and** *Lync-tcp-5061-fe*	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	HTTPS
Service Port: **444**	Service Port: **444**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	
Service Port: **448**	Service Port: **448**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	
Service Port: **5061**	Service Port: **5061**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe* *Optional monitor* [3]: **Lync-sip-monitor-fe** Base SIP monitor - **Mode** set to **TCP**. - **Additional Accepted** **- Status Code**: add code **401** & **488** - **Alias Service Port**: **5060**		*Default*: SSL [4] **Timeout** set to **1800** *Fallback*: Source Address Affinity.	Yes [2]	SIP over TLS
Service Port: **5067**[5]	Service Port: **5067**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	This service may be collocated on your FE servers or on separate Mediation servers
Service Port: **5068**[5]	Service Port: **5068**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	Same note as above
Service Port: **5070**[5]	Service Port: **5070**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	Same note as above
Service Port: **5071**	Service Port: **5071**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	
Service Port: **5072**	Service Port: **5072**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	
Service Port: **5073**	Service Port: **5073**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	

[1] *Use the Least Connections (node)* load balancing method

[2] ***Required*** (see *Creating a SNAT on page 39*)

[3] For the SIP monitor, additional steps need to be taken on the Microsoft Lync Front-End Servers. See *Creating a SIP monitor for the Front End servers on page 39*

[4] SSL persistence is optional but recommended

[5] These virtual servers are only necessary if deploying Lync Mediation Servers.

[6] This TCP monitor is used to support bringing down pool members when Lync servers are put into Maintenance Mode.

Virtual Server	Pool	Health monitor	Profiles	Persistence profile	SNAT enabled?	Notes
Service Port: **5075**	Service Port: **5075**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	
Service Port: **5076**	Service Port: **5076**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	
Service Port: **5080**	Service Port: **5080**[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-fe*	Use *Lync-tcp-fe*	Use *Lync-source-fe*	Yes [2]	
Service Port: **8080**	Service Port: **8080**[1] **Action on Service down: Reject**	Use *Lync-http-fe* **and** *Lync-tcp-5061-fe*[6]	Use *Lync-tcp-fe* **HTTP**: *Lync-fe-http* Base HTTP parent with no optimizations	**Lync-cookie-fe**: Default profile with Type set to **Cookie** persistence.	Yes [2]	

[1] Select **Advanced** from the **Configuration** list, and use the *Least Connections (node)* load balancing method

[2] ***Required*** (see *Creating a SNAT on page 39*)

[3] For the SIP monitor, additional steps need to be taken on the Microsoft Lync Front-End Servers. See *Creating a SIP monitor for the Front End servers on page 39*

[4] SSL persistence is optional but recommended

[5] These virtual servers are only necessary if deploying Lync Mediation Servers.

[6] This TCP monitor is used to support bringing down pool members when Lync servers are put into Maintenance Mode.

Configuration table for BIG-IP objects: Lync Director Services

The following table shows the non-default settings on BIG-IP LTM objects for the Lync Director services. The BIG-IP pool members (column 2) for the following table are each of the Lync Director servers.

Virtual Server port	Pool	Health monitor	TCP profiles	Persistence profile	SNAT enabled?	Notes
443	Service Port: 443[1] **Action on Service down: Reject**	**lync-tcp-monitor-dir**: Base TCP monitor with no required changes **Lync-tcp-5061-dir**[3]**:** Base TCP parent: **Alias Service Port**: **5061**	Standard TCP	None	Yes [2]	
444	Service Port: 444[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-dir*	Standard TCP	None	Yes [2]	
5061	Service Port: 5061[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-dir*	Standard TCP	None	Yes [2]	SIP over TLS

[1] Select **Advanced** from the **Configuration** list, and use the *Least Connections (node)* load balancing method

[2] ***Required*** (see *Creating a SNAT on page 39*)

[3] This TCP monitor is used to support bringing down pool members when Lync servers are put into Maintenance Mode.

Configuration table for BIG-IP objects: Edge Servers - External Interface

The following table is for external interface of the Microsoft Lync Edge Servers. The BIG-IP pool members (column 2) are the external interface of the Lync Edge Servers

➲ **Note** *When defining an Edge pool in the Lync Topology Builder, you specify a single IP address with unique ports for each Edge service, or a unique IP address and FQDN for each service. If you configured the Topology Builder for separate FQDNs for Web Conferencing and A/V, each Lync Edge server should have a unique publicly routable IP address for each of the three Edge services (Access, A/V, and Web Conferencing) in addition to one unique public IP address for each service's BIG-IP virtual server; if you are deploying two Edge servers, you would need 9 publicly routable IP addresses. If you specified a single IP address and FQDN, you only need one publicly routable IP address on each server in that case.*

Virtual Server port	Pool	Health monitor	Profiles	Persistence profile	SNAT?	Notes
Important: If you configured the Topology Builder for a single FQDN and IP address when defining an Edge pool, use the same IP address for each of the following virtual servers. If you configured unique FQDNs for the web conferencing and A/V services, use a unique IP address for each service.						
Access Service						
Note: For the Access service, you configure either a 443 **or** a 5061 virtual server as described below. However, if you have enabled federation on port 5061 in the Lync Server Topology, and created the Access virtual server on port 443, you must **also** create the virtual server on port 5061. If you are using Lync 2013 and enabled federation with XMPP providers on port 5269 in the Lync Server Topology, you must **also** create the 5269 virtual server.						
443	Service Port: 443[1] **Action on Service down: Reject**	**lync-tcp-monitor-ext**: Base TCP monitor with no required changes	**TCP**: *Lync-edge-tcp-ext*: Base *tcp* parent profile with **Idle Timeout** set to **1800** **Nagle's Algorithm**: **Disabled**	Source Address Affinity	Yes [2]	
5061 (default for single IP address)	Service Port: 5061[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-ext*	Use *Lync-edge-tcp-ext*	*Default*: SSL [3] **Timeout** set to **1800** *Fallback*: Source Address Affinity	Yes [2]	
5269	Service Port: 5269[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-ext*	Use *Lync-edge-tcp-ext*	Source Address Affinity	Yes [2]	
Web Conferencing Service						
443 (444 for single IP address)	Service Port: 443[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-ext*	Use *Lync-edge-tcp-ext*	Source Address Affinity	Yes [2]	
A/V Service [3]						
443 (default for single IP address)	Service Port: 443[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-ext*	Use *Lync-edge-tcp-ext*	Source Address Affinity	Not recommended[4]	The A/V Edge external interfaces must have publicly routable IP addresses
3478 (see troubleshooting on *page 28*)	Service Port: 3478[1] **Action on Service down: Reject**	UDP monitor: Base UDP monitor with no required changes. ICMP monitor: Base Gateway ICMP monitor with no changes	Standard **UDP**	Source Address Affinity	Not recommended[4]	On the virtual server, the **Source Port** list must be set to **Change**. Add both monitors to the pool. The iCMP monitor ensures a pool member is properly marked down

[1] Select **Advanced** from the **Configuration** list, and use the *Least Connections (node)* load balancing method
[2] Optional, but recommended (see *Creating a SNAT on page 39*)
[3] SSL persistence is optional but recommended
[4] For best performance, F5 does not recommend SNAT for Edge A/V services. However, SNAT for these services is supported in deployments where it is required.

Configuration table for BIG-IP objects: Edge Servers - Internal Interface

The following table is for internal interface of the Microsoft Lync Edge Servers.
The BIG-IP pool members (column 2) for the following table are the internal interface of the Lync Edge Servers.

Virtual Server Port	Pool	Health monitor	Profiles	Persistence Profile	SNAT?	Notes
443	Service Port: 443[1] **Action on Service down: Reject**	**lync-tcp-monitor-int**: Base TCP monitor with no required changes	***TCP:*** *Lync-edge-tcp-int*: Base *tcp* Parent profile with **Idle Timeout** set to **1800**	Source Address Affinity	Yes [2]	
3478	Service Port: 3478[1] (UDP) **Action on Service down: Reject**	UDP monitor: Base UDP monitor with no required changes	Standard **UDP**	Source Address Affinity	Yes [2]	STUN/UDP inbound/ outbound
5061	Service Port: 5061[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-int*	Use *Lync-edge-tcp-int*	*Default*: SSL [3] **Timeout** set to **1800** *Fallback*: Source Address Affinity	Yes [2]	
5062	Service Port: 5062[1] **Action on Service down: Reject**	Use *Lync-tcp-monitor-int*	Use *Lync-edge-tcp-int*	*Default*: SSL [3] **Timeout** set to **1800** *Fallback*: Source Address Affinity	Yes [2]	

[1] Select **Advanced** from the **Configuration** list, and use the *Least Connections (node)* load balancing method

[2] ***Required*** (see *Creating a SNAT on page 39*)

[3] SSL persistence is optional but recommended

Configuration table for BIG-IP objects when a reverse proxy is used

When deploying a Scaled Edge topology with a reverse proxy server, you need to create the following virtual servers on the BIG-IP LTM, depending on whether you are using Director servers. Additional details, including a configuration diagram, can be found at *http://technet.microsoft.com/en-us/library/gg398478.aspx*. There are internal and external BIG-IP virtual servers for the reverse proxy configuration. You can optionally create an external reverse proxy virtual server on the BIG-IP LTM that replaces the need for a separate reverse proxy device.

There are three options for configuring the BIG-IP LTM when using a reverse proxy. Follow the guidance applicable to your configuration.

- *Receive Reverse Proxy traffic from another BIG-IP system configuration table on page 35*
- *Forward Reverse Proxy client traffic to another BIG-IP system on page 36*
- *Forward Reverse Proxy traffic to Lync Server(s) on page 37*

Receive Reverse Proxy traffic from another BIG-IP system configuration table

For the internal side, there are additional virtual servers between your reverse proxy and your Front End pool, or optionally your Director pool. In most cases, this is the same BIG-IP LTM you configured with the virtual servers for your Front End or Director pools.

Virtual Server port	Pool	Health monitor	Profiles	Persistence profile	SNAT enabled?	Notes
Front End reverse proxy virtual server						
4443	Front End pool members on port 4443[1] **Action on Service down: Reject**	**Lync-https-4443-fe**: Base HTTPS monitor **Alias Service Port** set to **4443** Other settings optional **Lync-tcp-5061-in-rp**[3]**:** Base TCP parent: **Alias Service Port**: **5061**	Use *Lync-tcp-fe* **Client SSL**: *Lync-fe-client-ssl*: Base client SSL profile. *Important:* Must use same certificate used by Lync Server. **Server SSL**: Lync-fe-server-ssl: Base server SSL profile with proper certs. **HTTP**: *Lync-fe-http* Base HTTP parent profile with no optimizations	**Important:** *This profile is required for Lync 2010 and Lync 2013 implementations using Lync 2010 servers. It is optional for Lync 2013 only deployments.* **Lync-cookie-fe-in-rp**: *Type*: **Cookie** *Cookie Name:* **MS-WSMAN** *Always Send Cookie*: **Enabled** *Expiration:* Clear the check in the Session Cookie box, and then set the Expiration to **3650 Days**	Yes [2]	**Important:** *This virtual server is only required when a reverse proxy server is deployed as part of a Lync Edge server implementation.*

[1] Select **Advanced** from the **Configuration** list, and use the *Least Connections (node)* load balancing method

[2] ***Required*** (see *Creating a SNAT on page 39*)

[3] This TCP monitor is used to support bringing down pool members when Lync servers are put into Maintenance Mode.

This next virtual server is for the reverse proxy if you are using Director servers.

Virtual Server port	Pool	Health monitor	Profiles	Persistence profile	SNAT enabled?	Notes
Front End reverse proxy virtual server						
4443	Director server pool members on port 4443[1] **Action on Service down: Reject**	**Lync-https-4443-fe**: Base HTTPS monitor **Alias Service Port** set to **4443** Other settings optional **Lync-tcp-5061-in-rp**[3]**:** Base TCP parent: **Alias Service Port**: **5061**	Use *Lync-tcp-fe* **Client SSL**: *Lync-fe-client-ssl*: Base client SSL profile. *Important:* Must use same certificate used by Lync Server. **Server SSL**: Lync-fe-server-ssl: Base server SSL profile with proper certs. **HTTP**: *Lync-fe-http* Base HTTP parent profile with no optimizations	Cookie: Cookie Name set to **MS-WSMAN** Always Send Cookie**: Enabled** **(this profile is optional for Lync 2013)**	Yes [2]	**Important:** *This virtual server is only required when a reverse proxy server is deployed as part of a Lync Edge server implementation.*

[1] Select **Advanced** from the **Configuration** list, and use the *Least Connections (node)* load balancing method

[2] ***Required*** (see *Creating a SNAT on page 39*)

[3] This TCP monitor is used to support bringing down pool members when Lync servers are put into Maintenance Mode.

NOTE: When deploying an external reverse proxy for Lync web services, F5 recommends either deploying an LTM virtual server to receive external Lync web services traffic as described in the following section, or locating the reverse proxy server (such as Microsoft Threat Management Gateway) directly on a public network. Deploying a third-party external reverse proxy server behind the BIG-IP LTM is not a supported configuration.

Forward Reverse Proxy client traffic to another BIG-IP system

Create the following virtual server if you want to use the BIG-IP LTM to act as a reverse proxy and eliminate the need for a separate device. This virtual server uses an iRule to properly send traffic to the correct location.

Important: *This virtual server is only required when you want to replace a separate reverse proxy device.*

Virtual Server	Pool	Health monitor	Profiles	Persistence	SNAT?	Other
Service port: **443** **Critical:** Do **NOT** assign a default pool to this virtual server. The pool assignment is handled by the iRule.	*Front End reverse proxy pool*: The only member is the IP address of the internal Front End port 4443 virtual server you created. *Director reverse proxy pool*: If using Director servers, create an additional pool. The only member is the IP address of the internal Director port 4443 virtual server. Both use Service Port **4443**[1] **Action on Service down: Reject**	**Lync-https-4443-fe**: Base HTTPS monitor **Alias Service Port** set to **4443** Other settings optional **Lync-tcp-5061-ex-rp[3]:** Base TCP parent: **Alias Service Port**: **5061**	Use *Lync-tcp-fe* **Server SSL**: Lync-fe-server-ssl: Base server SSL profile with proper certs. **HTTP**: *Lync-fe-http* Base HTTP parent profile with no optimizations **Client SSL**: *Lync-fe-client-ssl*: Base client SSL profile. *Important:* Must use same certificate used by Lync Server. **If using Director servers and a unique certificate**[4]: Set the **Server Name** to the FQDN of your Lync Front End web services pool. You must also create a Director Client SSL profile: *Lync-dir-client-ssl*: Base client SSL profile with **Default SSL profile for SNI** set to **Enabled**.	None	Yes [2]	You must enable Port Translation on this virtual server (enabled by default). **Critical:** You must also attach an iRule to this virtual server. See *Creating the iRules on page 37*

[1] Select **Advanced** from the **Configuration** list, and use the *Least Connections (node)* load balancing method
[2] ***Required*** (see *Creating a SNAT on page 39*)
[3] This TCP monitor is used to support bringing down pool members when Lync servers are put into Maintenance Mode.
[4] If using a unique certificate for the Director servers, the Client SSL profile must be configured for SNI, and your clients must support SNI

Forward Reverse Proxy traffic to Lync Server(s)

Create the following virtual server which will receive external Lync web services traffic and forward it directly to the Lync Front End/Director servers.. This virtual server uses an iRule to properly send traffic to the correct location.

Important: *This virtual server is only required when you want to replace a separate reverse proxy device.*

Virtual Server	Pool	Health monitor	Profiles	Persistence profile	SNAT?	Other
Front End reverse proxy virtual server						
Service port: **443** **Critical:** Do **NOT** assign a default pool to this virtual server. The pool assignment is handled by the iRule.	*Front End reverse proxy pool*: Create a pool with the Front End servers that should receive web services traffic. *Director reverse proxy pool*: If using Director servers, create an additional pool with the Director servers that should receive web services traffic. Both use Service Port **4443**[1] **Action on Service down: Reject**	**Lync-https-4443-fe**: Base HTTPS monitor **Alias Service Port** set to **4443** Other settings optional **Lync-tcp-5061-ex-rp**[3]**:** Base TCP parent: **Alias Service Port**: **5061**	Use *Lync-tcp-fe* **Server SSL**: Lync-fe-server-ssl: Base server SSL profile with proper certs. **HTTP**: *Lync-fe-http* Base HTTP parent profile with no optimizations **Client SSL**: *Lync-fe-client-ssl*: Base client SSL profile. *Important:* Must use same certificate used by Lync Server. **If using Director servers and a unique certificate**[4]: Set the **Server Name** to the FQDN of your Lync Front End web services pool. You must also create a Director Client SSL profile: *Lync-dir-client-ssl*: Base client SSL profile with **Default SSL profile for SNI** set to **Enabled**.	***If using a single BIG-IP LTM only:*** Cookie: Cookie Name set to **MS-WSMAN** Always Send Cookie**: Enabled** Expiration**: 3650 days** **(this profile is optional for Lync 2013**	Yes [2]	You must enable Port Translation on this virtual server (enabled by default). **Critical:** You must also attach an iRule to this virtual server. See *Creating the iRules on page 38*

[1] Select **Advanced** from the **Configuration** list, and use the *Least Connections (node)* load balancing method

[2] ***Required*** (see *Creating a SNAT on page 39*)

[3] This TCP monitor is used to support bringing down pool members when Lync servers are put into Maintenance Mode.

[4] If using a unique certificate for the Director servers, the Client SSL profile must be configured for SNI, and your clients must support SNI

Creating the iRules

For the external reverse proxy virtual server, you must create an iRule that sends traffic to the proper Lync service. The iRule you create depends on whether you are using Director servers or not, and the format of the URLs. We provide four examples in this section.

In the following examples, replace the red text with your URLs and pool names. The code goes in the Definition section when creating the iRule. The line numbers are provided for reference, do not include them in the code.

*iRule for Simple URLs in 'meet.example.com' format when you are **NOT** forwarding reverse proxy traffic to Director servers*

```
when HTTP_REQUEST {
    switch -glob [string tolower [HTTP::host]] {
         chat.example.com* { pool front_end_pool }
         meet.example.com*  { pool front_end_pool }
         dialin.example.com* { pool front_end_pool }
         lyncdiscover.example.com* { pool front_end_pool }
    }
}
```

*iRule for Simple URLs in 'www.example.com/meet' format when you are **NOT** forwarding reverse proxy traffic to Director servers*

```
when HTTP_REQUEST {
   switch -glob [string tolower [HTTP::host]] {
      chat.example.com* { pool front_end_pool }
      example.com {
      switch -glob [string tolower [HTTP::uri]] {
         /meet* { pool front_end_pool }
         /dialin* { pool front_end_pool }
         }
      }
      lyncdiscover.example.com* { pool front_end_pool }
   }
}
```

*iRule for Simple URLs in 'meet.example.com' format when you **ARE** forwarding reverse proxy traffic to Director servers*

```
when HTTP_REQUEST {
    switch -glob [string tolower [HTTP::host]] {
         chat.example.com* { pool front_end_pool }
         dir.example.com* { pool director_pool }
         meet.example.com*  { pool director_pool }
         dialin.example.com* { pool director_pool }
         lyncdiscover.example.com* { pool director_pool }
    }
}
```

*iRule for Simple URLs in 'www.example.com/meet' format when you **ARE** forwarding reverse proxy traffic to Director servers*

```
when HTTP_REQUEST {
    switch -glob [string tolower [HTTP::host]] {
         chat.example.com* { pool front_end_pool }
         dir.example.com* { pool director_pool }
         www.example.com* {
         switch -glob [string tolower [HTTP::uri]] {
              /meet* { pool director_pool }
              /dialin* { pool director_pool }
              }
         }
         lyncdiscover.example.com* { pool director_end_pool }
    }
}
```

Attach the appropriate iRule to the virtual server.

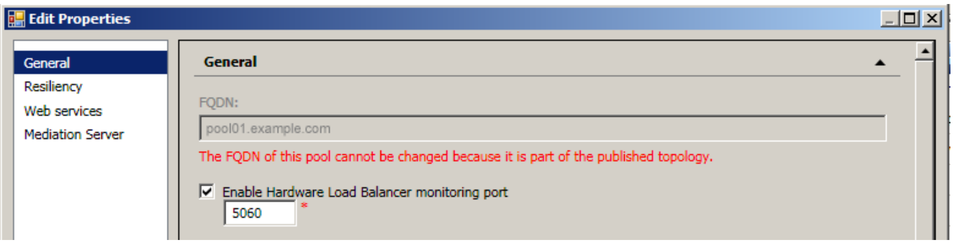
This completes the Reverse Proxy section.

Creating a SIP monitor for the Front End servers

By default, SIP traffic on Front End servers is encrypted on port 5061. You may optionally enable unencrypted port 5060 for the purposes of health monitoring only; normal SIP communication cannot occur on the unencrypted port. A SIP monitor is more accurate than a simple TCP monitor, which only determines whether a port is active and not if the associated service is actually running.

In addition to configuring the SIP monitor on the BIG-IP LTM, you must also modify the Lync Front End Server configuration to enable for 5060.

To enable port 5060, use the Lync Server 2010 Topology Builder to modify the properties for your Enterprise Edition Front End Pool. Select **Enable Hardware Load Balancer monitoring port** as shown in the following figure, and then choose the default port number of **5060** or enter a custom port. Port 5060 is standard for SIP; if you select another port number, it must be one that is not otherwise in use on your Front End servers, you must make sure it is permitted on the local firewalls of those servers, and you must adjust the BIG-IP LTM monitor. Re-run the Lync Server Deployment Wizard on each Front End server to apply the change.



FQDN:
pool01.example.com
The FQDN of this pool cannot be changed because it is part of the published topology.
☑ Enable Hardware Load Balancer monitoring port
5060 *

Figure 3: *Editing the General properties*

To create the BIG-IP LTM SIP monitor

1. On the Main tab, expand **Local Traffic**, and then click **Monitors**.
2. Click the **Create** button. The New Monitor screen opens.
3. In the **Name** box, type a unique name for this monitor. We type **Lync-sip-monitor-fe**.
4. From the **Type** list, select **SIP**.
5. From the **Configuration** list, select **Advanced**.
6. From the **Mode** list, select **TCP**.
7. From the **Additional Accepted Status Codes** list, select **Status Code List**, and then type **488** in the **Status code** box. Click **Add**.
8. In the **Alias Service Port** box, type **5060** (or the custom port you selected in the Topology Builder).
9. Click **Finished**.

➲ ***Additional Information*:**
When a Hardware Load Balancer monitoring port is configured using Topology Builder, Lync Server 2010 will respond to SIP requests on that port with a status code of "488" (and "401" if using NTLM authentication) and the reason "Port is configured for health monitoring only". The BIG-IP LTM health monitor you configured in this step treats that as an expected response from the Front End SIP service and marks the pool member as available to accept traffic.

Creating a SNAT

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

A default SNAT is appropriate for most deployments. If more than 65,000 simultaneous users are connecting to the Lync Server deployment, see *"Configuring a SNAT for large Lync Server deployments"*.

Use the procedure most applicable for your deployment.

As mentioned in the prerequisites, we typically recommend *Auto Map* for SNAT configuration. With SNAT Auto Map configured, BIG-IP LTM translates the source IP address of each connection to that of its own self IP on the local subnet. As an alternative, you might want to SNAT to an address other than the self IP; for instance, you might want to be able to distinguish LTM monitor traffic (which always comes from the self IP) from application traffic. To accomplish this, you can create a *SNAT pool* containing a single, otherwise-unused IP address on the local subnet and use that in place of Automap (see Creating a SNAT pool on the following page). For more information on SNATs, see the BIG-IP LTM documentation, available on Ask F5: *http://support.f5.com/kb/en-us/products/big-ip_ltm.html*.

Creating a default SNAT for less than 64,000 concurrent users
Use this procedure if your Lync Server deployment has fewer than 64,000 simultaneous users.

To create a default SNAT

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**.
2. Click the **Create** button.
3. In the **Name** box, type a name. In our example, we type **lync-default-snat**.
4. From the **Translation** list, select a setting appropriate for your configuration. In our example, we select **Automap**.
5. From the **VLAN Traffic** list, select **Enabled on**.
6. In the **VLAN List** row, from the **Available** list, select the VLANs on which your Lync Servers reside, and then click the Add (**<<**) button.
7. Click the **Finished** button.

Configuring a SNAT for large Lync Server deployments
For large deployments (with 64,000 simultaneous connections), we create a SNAT pool. A SNAT pool is a pool with one unused IP address, on the same subnet as the virtual servers and Lync Servers. You must create a SNAT pool for each 64,000 connections (or fraction thereof).

➲ Important *This procedure is only necessary for large deployments. If your Lync deployment has less than 64,000 simultaneous connections, you do not need to create a SNAT pool. Use the previous procedure.*

To create a SNAT pool for large deployments

1. On the Main tab, expand **Local Traffic**, and then click **SNATs**.
2. On the Menu bar, click **SNAT Pool List**.
3. Click the **Create** button.
4. In the **Name** box, type a name for this SNAT Pool. In our example, we type **lync-snat-pool**.
5. In the **IP Address** box, type in a valid and otherwise-unused address on the subnet containing your Front End servers, and click the **Add** button.
   Repeat this step for each additional address needed. At least one address should be added for each 64,000 anticipated concurrent connections (the number of connection generally corresponds to the number of clients).
6. Click the **Finished** button.

The next part of the SNAT pool configuration is to configure a default SNAT that uses the SNAT pool.

7. On the Main tab, expand **Local Traffic**, and then click **SNATs**.
8. Click the **Create** button.
9. In the **Name** box, type a name for this SNAT. In our example, we type **lync-default-snat**.
10. From the **Translation** list, select **SNAT Pool**.
11. From the **Select** list, select the name of the SNAT pool you created in the preceding procedure. In our example, we select **lync-snat-pool**.
12. From the **VLAN Traffic** list, select **Enabled on**.
13. In the VLAN List row, from the **Available** list, select the VLANs on which your Lync devices reside, and click the Add (<<) button.
14. Click the **Finished** button.

This completes the manual configuration.

Revision History

Version	Description	Date
1.0	New guide for BIG-IP v11	N/A
2.0	Updated the guide for use with the new downloadable iApp. The new iApp contains the following new features: • Tested to work with Lync Server 2010 CU4. • Support added for Lync Mobility service. • Added option to deploy virtual servers for forwarding Lync 2010 topology replication traffic to the Lync Edge Servers. • Made Lync Mediation Server deployment optional. • Added SIP monitor option for checking internal virtual server health from the external BIG-IP LTM. • Added external reverse proxy configuration option. • Added the option to specify which Lync Edge services to deploy. • Added inline documentation and notes. • Expanded Help section. The new iApp contains the following fixes from the previous version: • Added port 443 and 444 virtual servers and pools for Director services. • Corrected configuration issue with Director services; Director virtual server now forwards traffic to correct destination. • Removed HTTP profile, SSL profiles, and cookie persistence for Web Conferencing traffic. Set persistence to source IP address (affinity). • Added a new iRule that limits connections to the internal reverse proxy to URLs specified by the user and separates traffic bound for Director and Front End servers. • Added internal reverse proxy virtual server and pool to forward traffic to the appropriate Lync Servers when Director Servers are deployed. • Clarified SNAT scenarios in simpler terms. • Removed TCP queuing configuration options. • Added guidance for properly configuring Lync Edge services. • Added NTLM challenge response to list of accepted responses for SIP monitor. • Removed serverssl certificate and key questions because those were never used and are unneeded.	02-22-12
2.1	- Added the option to use either port 443 or 5061 for the Edge Access service - Added the option of creating a virtual server if you enabled federation on port 5061 in the Lync Server Topology - Removed the HTTP profile, SSL profiles, and cookie persistence profile for Access service traffic. Set the persistence method to source IP address (affinity).	03-15-2012
2.2	Adding a link and information about the F5 solution for Lync Site Resiliency: *http://www.f5.com/pdf/deployment-guides/lync-2010-site-resiliency-dg.pdf*	05-25-2012
2.3	Added *Adding a virtual server on port 80 on page 16* to the post iApp configuration. You must create this virtual server after completing the iApp.	08-28-2012
2.4	Added guidance on the configuration differences in using a single BIG-IP LTM and separate internal and external BIG-IP LTMs.	09-20-2012
2.5	Added support for Microsoft Lync Server 2013 as well as BIG-IP LTM versions 11.2 and 11.3	12-07-2012
2.6	Added a note in the prerequisites section about the Office Web Apps deployment guide, which includes guidance for configuring Office Web Apps for Lync Server 2013.	01-11-2013

Version	Description	Date
2.7	Updated the deployment guide for a new version of the iApp. The following changes were made: - Added a new section for the new question in the iApp asking if Lync 2010 or 2013 is being deployed. - Removed the section for adding a port 80 virtual server after configuring the iApp. The iApp now correctly configures this virtual server - The iApp now adds a TCP monitor on port 5061 to the HTTP pools (for the virtual servers on ports 80, 8080, 443, and 4443) to support bringing down members when Lync servers are put into Maintenance mode. Added this monitor to the manual configuration tables. - Added a timeout of 1800 to the Source Address persistence profile for the Front End servers in all cases. - Modified the port 80 and 443 Front End HTTP virtual servers to use Source Address and not cookie persistence. - Removed persistence for reverse proxy/external web services when deploying Lync 2013. - Lync 2013 only: added support for XMPP federation. - Removed the port 5060 virtual server for the Director Servers as it was not used - Removed the question asking whether clients are connecting over a WAN or LAN for Edge Servers - External Interface. The iApp now always assigns a WAN optimized profile. - Removed all OneConnect and NTLM profiles from the configuration.	02-13-2013
2.8	- iApp now includes setting *Action on Service Down* to *Reject* for all pools. Manual configuration tables reflect this change. - The iApp now allows an external reverse proxy deployment separate from the Edge Servers. - The iApp now allows a user to select separate certificates and keys for the internal Director and Front End reverse proxy virtual servers. F5 still recommends using the same certificate for these virtual servers. - Removed certificate and key questions from the internal Front End deployment section, as they were not used in the configuration produced by the iApp. - Added a note to the prerequisites and the manual configuration Reverse Proxy section stating that deploying a third-party external reverse proxy server behind the BIG-IP LTM is not supported. - The iApp now adds a timeout value of 3650 days to the cookie persistence profiles for the Edge Internal Reverse Proxy virtual servers if using Lync 2010 only, or in a mixed Lync 2013/2010 environment. The manual configuration tables reflect this change. - The iApp now configures cookie persistence on Director and Front End 4443 virtual servers when running Lync 2010 servers in a Lync 2013 environment. The manual configuration tables reflect this change. - Modified the www.example.com/meet iRules in *Creating the iRules on page 38* to add a wildcard (*) after /meet and /dialin	03-14-2013
2.9	Added a new section for *Troubleshooting on page 42* with information to help solve Lync 2013 call audio issues.	07-10-2013
3.0	Updated the deployment guide for a new version of the iApp (f5.microsoft_lync_server.2013_07_22). The following changes were made in the new iApp template, and in the manual configuration tables in this guide: - Added a ICMP monitor to UDP 3478 Edge A/V pool to ensure the pool member is correctly marked down. - Modified reverse proxy iRules to support host name requests that include the port number - Added a SNAT option for A/V virtual servers. This was necessary because Lync 2013 clients adhere strictly to the STUN protocol by refusing asymmetrical connections. - Removed the Edge Server Internal Interface virtual server on port 8057. According to Microsoft, this port should not be load balanced by a hardware load balancer. - Removed the Edge Server Internal Interface replication 4443 virtual server. Replication takes place directly between the Front End and Edge Internal servers.	08-29-2013
3.1	Updated the deployment guide for a new version of the iApp (f5.microsoft_lync_server.v1.2.0. Note the naming/versioning changed in this version). The following changes were made in the new iApp template and in the manual configuration tables: - Updated the deployment guide to mirror the stylistic and editorial changes in the v1.2.0 iApp template. - Corrected a nesting error in the iRules for the External Edge Reverse Proxy virtual server. - Corrected an error in the iApp that prevented the template from completing if a Ratio load balancing method was selected.	10-02-2013
3.2	In the manual configuration section, corrected the example pool for the optional Lync Mobility service in the iRules when forwarding traffic to Director servers for the External Edge Reverse Proxy virtual server on *page 38*. The iApp configuration for the iRules remains correct and unchanged.	10-03-2013
3.3	Clarified guidance on when to run the Lync Topology Builder in the prerequisites. Removed the section about running the Topology Builder at the end of the manual configuration section.	10-28-2013

Version	Description	Date
3.4	- Updated guide for v1.2.1 of the template, making the following changes to the iApp template and this guide: - Corrected two questions in the Microsoft Lync Server Edge Reverse Proxy: External Interface section that referred to port 443 virtual servers; the correct port is 4443. - Also in that section, modified the question 'What is the URL for external Lync Mobility access' to be 'What is the FQDN for external Lync Mobility access'. - Also in that section, added two Important notes to the iApp template for the Simple URL questions stating not to use HTTPS:// or a trailing slash.	11-14-2013
3.5	Added support for BIG-IP version 11.5	01-31-2014
3.6	Added support for BIG-IP version 11.5.1	03-19-2014
3.7	Fixed an incorrect reference to the name of the Reverse Proxy virtual server created by the iApp.	03-26-2014
3.8	Released Lync iApp v1.3.0 RC-1. This version includes the following updates: - The iApp now includes the ability to select specific VLANs on which to allow traffic. - Combined the two reverse proxy sections in the iApp template to a single section with three choices on how the iApp will configure the system for reverse proxy (see *Configuring the iApp for Lync Reverse Proxy on page 19*) - Added support for using multiple certificates for reverse proxy deployments - The iApp now includes support for using a single IP address and FQDN or multiple IP addresses and FQDNs for Edge external services.	07-03-2014
3.9	Added support for BIG-IP version 11.6	08-25-2014
3.95	In the manual configuration table for the Front End servers, for the port 8080 virtual server, removed the Client SSL profile and Server SSL profile, as they were not necessary. Also changed the persistence profile type from source address affinity to cookie persistence. The iApp template properly configured this virtual server.	09-04-2014
4.0	Updated this guide for the officially supported release of the Lync iApp template (f5.microsoft.lync_server_2010_2013.v.1.3.0), which contained the following changes from v1.3.0 RC-1: - Added the ability to select pre-existing Client SSL profiles, and added the ability to select an intermediate certificate - Removed certificate questions from the Edge Internal Interface section, as they were unused.	10-06-2014
4.1	Moved the Troubleshooting section into a new section immediately following the iApp walkthrough, as it was determined this was more than a troubleshooting step. Made the same change to the manual configuration table for the Edge External A/V virtual server.	11-26-2014
4.2	Created a new troubleshooting section (*Troubleshooting on page 28*) with an issue for Lync clients having issues connecting to the Autodiscover service when also using the BIG-IP system for Microsoft Exchange.	01-16-2015
4.3	Moved the section Modifying the configuration for Lync 2013 clients connecting through the Edge external A/V UDP virtual server to *Troubleshooting on page 28* as changing the virtual server Type to Stateless is not always required.	03-26-2015
4.4	- Removed the section Modifying the configuration for Lync 2013 clients connecting through the Edge external A/V UDP virtual server - Added the section *Creating a forwarding virtual server for Lync Edge server to Lync client communication on page 29*. - Added the section *Modifying the iApp configuration on page 27.*	04-20-2015

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