



■ **Deployment Guide**

**Microsoft Lync 2013**

**AX Series**

## TABLE OF CONTENTS

1	Introduction .....	3
1.1	Deployment Guide Overview .....	3
1.2	Deployment Guide Assumptions and Prerequisites.....	5
1.3	AX Deployment for Lync Server 2013 Roles .....	5
2	Configuring the AX Series Application Delivery Controller .....	6
2.1	Log into the CLI.....	6
2.2	Log onto the GUI.....	8
3	Services Required for Lync 2013 Deployment .....	9
4	Configuring the Partitions (Optional).....	13
4.1	ADP Configuration .....	14
5	AX Series as a Reverse Proxy .....	15
5.1	Lync Reverse Proxy Requirements.....	16
6	Load Balancer Configuration .....	18
6.1	External Edge Configuration .....	18
6.2	Internal Edge Configuration .....	20
6.3	Front End Configuration .....	24
7	Summary and Conclusion.....	30

## 1 INTRODUCTION

The A10 Networks AX Series Application Delivery Controller (ADC) provides advanced load balancing and enhanced services for Microsoft Lync 2013's new features and applications. The AX Series hardware-based models and Hypervisor-based SoftAX models can be used for Lync 2013 deployments.

A10 Networks is strongly committed to our partnership with Microsoft. For many years, we have completed certifications and provided deployment guides for Microsoft. A10 has shown continued commitment to Microsoft communication products, with deployment guides and certifications for Microsoft Office Communicator 2007 R2 (commonly known as OCS) and Microsoft Lync 2010 already available.

### Summary of Lync 2013 Changes:

Microsoft Lync 2013 brings many feature updates for functional capabilities, but no significant changes within the network topology other than consolidating the monitoring and archiving features towards the Front End servers as an optional feature. The Lync 2010 Director role is no longer recommended but becomes an optional role within the Lync 2013 topology. The Front End servers are able to take the role as Lync Director, which minimizes the number of servers in the deployment. Since Microsoft announced the discontinuation status<sup>1</sup> for Threat Management Gateway (TMG 2010), A10 Networks has provided a solution to handle application traffic before a Lync request hits the back-end servers. The AX Series supplements some of the TMG security features and makes the transition from Microsoft TMG to A10 Networks seamless. Moreover, additional AX Series security features will be available in future releases such as Single Sign-On, LDAP Authentication, NTLM & Basic Authentication, and more.

<sup>1</sup> <http://technet.microsoft.com/en-us/forefront/ee807302.aspx>

## 1.1 DEPLOYMENT GUIDE OVERVIEW

This deployment guide contains step-by-step procedures for configuring AX Series ADCs to support the Microsoft Lync 2013 solution. This deployment guide has been tested specifically for Microsoft Lync 2013 Enterprise Server Edition. This deployment guide does not apply to Microsoft OCS 2007 deployments; however, the deployment guide for Microsoft Lync 2010 can be used as reference to deploy the AX Series within your network for OCS. This guide can be used for Lync 2013 and Lync 2010.

For the other AX Series Microsoft deployment guides, please visit:

[www.a10networks.com/resources/deployment\\_guides.php](http://www.a10networks.com/resources/deployment_guides.php).

The lab topology in Figure 1 is designed to support internal and external users with high availability voice, Instant Messaging (IM), desktop sharing and conferencing communications. The lab topology is deployed with two servers in each application pool and the topology can have additional servers if needed. For a server to be added, it must have the same server role configuration as the other servers in the application pool.

The lab topology for Lync 2013 is very similar to the topology in the Lync 2010 deployment guide, except that instead of requiring 3 physical AX Series load balancers as is the case for Lync 2010 deployment, the Lync 2013 deployment guide adds the configuration instructions for deploying the solution with a single AX Series appliance, using Application Delivery Partitions (ADPs). The ADP feature also can be deployed with either Lync 2013 or Lync 2010. Additional details are available later in the document.

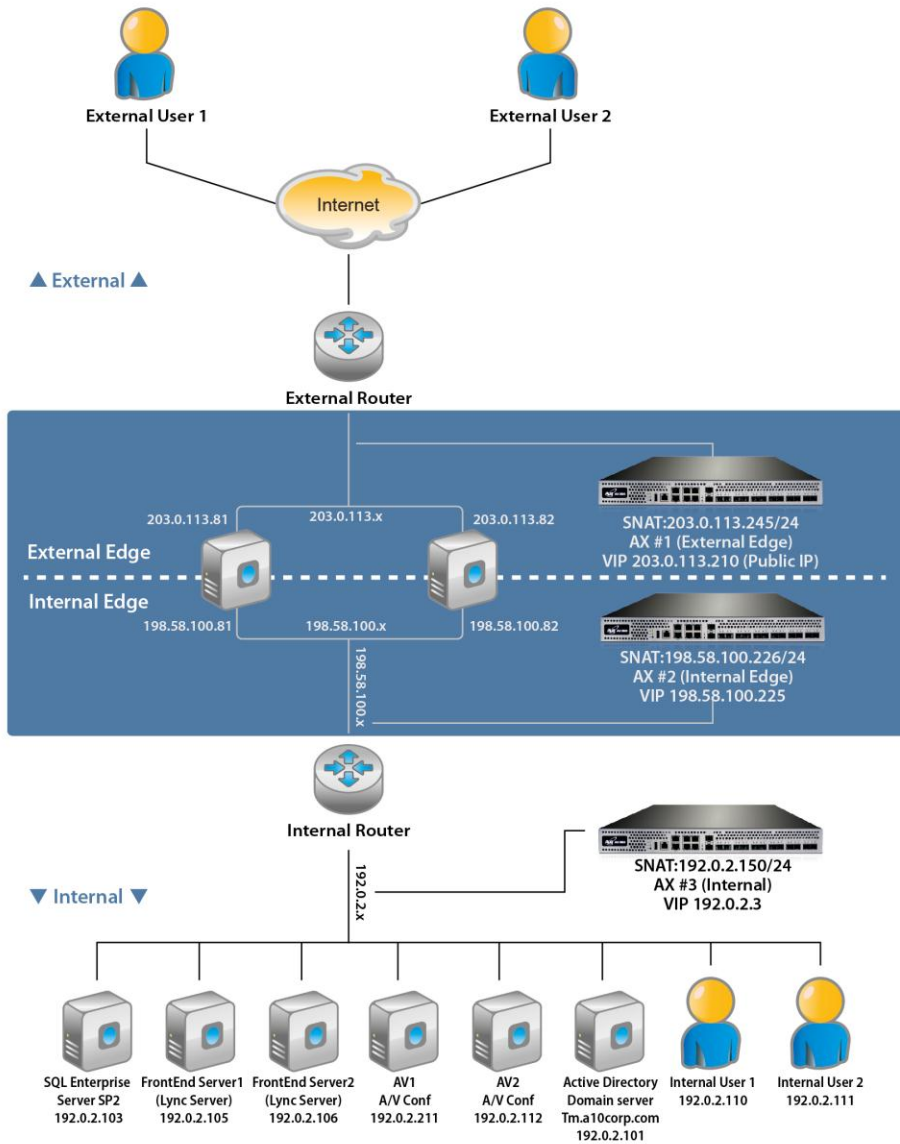


Figure 1: Standard Microsoft Lync 2013 network topology

## 1.2 DEPLOYMENT GUIDE ASSUMPTIONS AND PREREQUISITES

The deployment guide testing was performed using the following configuration:

- A10 Networks AX Series appliances running ACOS version 2.7.0-P1, configured with ADPs enabled for Layer 3 Virtualization (L3V). Previous versions of the AX Series also can be used.
- The Microsoft Lync 2013 Server was tested with Voice, IM, Persistent Chat (Group Chat), Presence, Desktop Collaboration and Audio Visual (AV) conferencing applications. Testing was performed for both internal and external users.
- Testing was performed using Microsoft Lync Server 2013 Enterprise Server with 64-bit Microsoft SQL Server Enterprise Edition Version 10.0.4000.0.
- All Lync 2013 Server components were running on Windows 2008 (64-bit) Standard Edition Server.
- Lync clients were running Windows 7.
- The lab setup was configured using a one-arm deployment model.

## 1.3 LYNC SERVER 2013 ROLES

The Lync server solution uses multiple servers within the solution. The server roles are described below.

- **Front End Servers (Lync Servers)** – The Front End (FE) servers provide the same functionality as in Lync 2010. The main role of the FE servers is to provide user authentication, registration, presence, IM, web conferencing, and application sharing functionality. FE servers also provide an address book service and distribution list expansion. FE servers are provisioned in a front-end pool and are configured identically to provide scalability and failover capability to Lync end-users. In order to load balance the FE servers, it is required that the topology contain two or more FE servers.

In Lync 2013, the Microsoft Lync Director role has been incorporated directly into the FE server instead of having a separate instance of a virtual machine or a server. The FE Servers are used as registrars for all authentication requests.

- **Active Directory Domain Services (AD DS)** – All Lync servers referenced within the topology, with the exception of the Edge Servers, must be joined by a domain and in AD DS. Lync users are managed within the AD Domain and Lync Communication Server Control Panel (CSCP). The AD DS is required in a Lync 2013 topology.

- **Back End (BE) Server** – The BE servers run Microsoft SQL and provide database services for the front-end pool. The information stored in the SQL servers includes user contact lists, presence information, conferencing details, and conferencing schedule information. The SQL server can be configured as a single back-end server; however, a cluster of two or more servers is recommended for failover. The BE server requirement can be implemented with SQL 2008.
- **External Edge Server** – The external edge server enables external users to communicate and collaborate with internal users. Multiple external edge servers can be deployed in a pool for redundancy. The external edge server also enables connectivity to third-party IM services such as Windows Live, AOL and Yahoo.
- **AV Conferencing Server** – Provides AV conferencing functionality for the Lync solution. The AV server can be deployed as a single server or as a pool of servers for redundancy.

## 2 CONFIGURING THE AX SERIES APPLICATION DELIVERY CONTROLLER

AX Series devices provide the following management interfaces:

- **Command-Line Interface (CLI)** – Text-based interface in which commands are entered on a command line. The CLI is directly accessible through the serial console or over the network using either of the following protocols:
  - Secure protocol – Secure Shell (SSH) version 2
  - Unsecure protocol – Telnet (if enabled)
- **Graphical User Interface (GUI)** – Web-based interface in which you click to access configuration or management pages and type or select values to configure or manage the device. You can access the GUI using Hypertext Transfer Protocol over Secure Socket Layer (HTTPS).

**Note:** *HTTP requests are redirected to HTTPS by default on the AX device.*

By default, Telnet access is disabled on all interfaces, including the management interface. SSH, HTTP and HTTPS are enabled by default on the management interface only, and disabled by default on all data interfaces.

### 2.1 LOG INTO THE CLI

The AX Series provides advanced features for securing management access to the device. This section assumes that only the basic security settings are in place.

To log into the CLI using SSH:

1. On a PC connected to a network that can access the AX device's management interface, open an SSH connection to the IP address of the management interface. The default IP address is 172.31.31.31.
2. Generally, if this is the first time the SSH client has accessed the AX device, the SSH client displays a security warning. Read the warning carefully, then acknowledge the warning to complete the connection. (Press "Enter".)
3. At the "login as:" prompt, enter the username "admin".
4. At the Password: prompt, enter the admin password. The default password is "a10". If the admin username and password are valid, the command prompt for the User EXEC level of the CLI appears:

```
AX>
```

The User EXEC level allows you to enter a few basic commands, including some show commands as well as **ping** and **traceroute**.

**Note:** The "AX" in the CLI prompt is the hostname configured on the device, which is "AX" by default. If the hostname has already been changed, the new hostname appears in the prompt instead of "AX".

5. To access the Privileged EXEC level of the CLI and allow access to all configuration levels, enter the **enable** command. At the "Password:" prompt, enter the enable password as blank. (Just press "Enter".)

**Note:** This is not the same as the admin password, although it is possible to configure the same value for both passwords.

If the enable password is correct, the command prompt for the Privileged EXEC level of the CLI appears:

```
AX#
```

6. To access the global configuration level, enter the **config** command. The following command prompt appears:

```
AX(config)#
```

**Note:** See the "AX Series Configuration Guide", or the "AX Series System Configuration and Administration Guide" and "Application Delivery and Server Load Balancing Guide", for additional features and functions of the AX device.

## 2.2 LOG ONTO THE GUI

To log onto the GUI:

In your web browser, navigate to the management IP address of the AX device. A login dialog is displayed. The name and appearance of the dialog depend on the browser you are using.

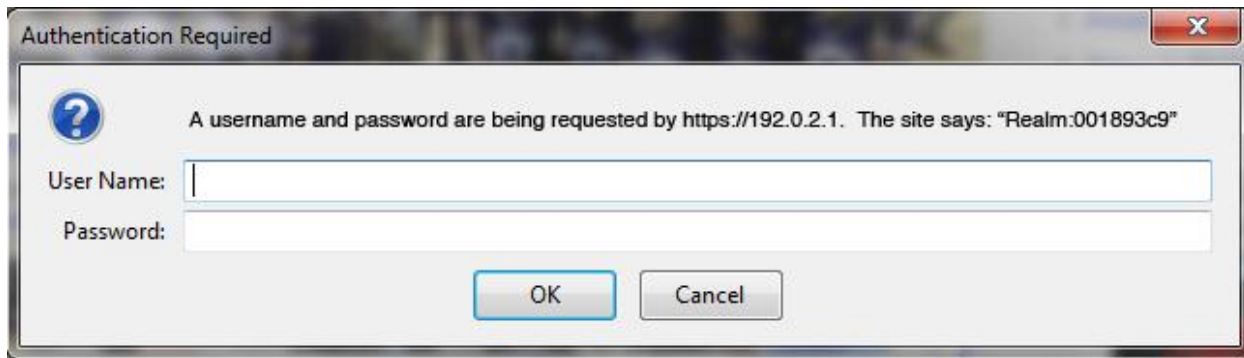


Figure 2: GUI login dialog

**Note:** The default admin credentials are username “admin” and password “a10”.

Enter your admin username and password and click **OK**.

The Summary page appears, showing at-a-glance information for your AX device. You can access this page again at any time while using the GUI, by navigating to **Monitor > Overview > Summary**.



### 3 SERVICES REQUIRED FOR LYNC 2013 DEPLOYMENT

Table 1 lists the services required for a Lync 2013 Enterprise Server deployment.

Table 1: Internal Front End Services					
Server Role	Port	VIP Type	Source NAT	Feature Templates	Usage Notes
Lync Front End Servers	135	TCP	Yes	Persistence: Source-IP TCP Idle Timeout: 1200 Health Monitor: Default	Used for DCOM-based operations such as moving end-users, end-user replicator synchronization, and address book synchronization.
Lync Front End Servers	443	TCP	Yes	Persistence: Source-IP Health Monitor: Default	Used for communication from front-end servers to the web farm FQDNs (the URLs used by IIS web components).
Lync Front End Servers	444	TCP	Yes	Persistence: Source-IP Health Monitor: Default	Used for communication between Lync Server components that manage the conference state and the individual servers.
Lync Front End Servers	5061	TCP	Yes	Persistence: Source-IP TCP Idle Timeout: 1200 Health Monitor: Default	Front-end pools for all internal SIP communications between servers (MTLS), for SIP communication between server and client (TLS), and for SIP communication between front-end servers and Mediation Servers (MTLS).

Table 1: Internal Front End Services

Table 2: Optional Internal Front End Services

Server Role	Port	VIP Type	Source NAT	Feature Templates	Usage Notes
Lync Front End Servers	5060	TCP	Yes	Persistence: Source-IP TCP Idle Timeout: 1200 Health Monitor: Default	Port used for front-end servers for static routes to trusted services.
Lync Front End Servers	5065	TCP	Yes	Persistence: Source-IP TCP Idle Timeout: 1200 Health Monitor: Default	Port for incoming SIP requests for application sharing.
Lync Front End Servers	5071	TCP	Yes	Persistence: Source-IP TCP Idle Timeout: 1200 Health Monitor: Default	Port for incoming SIP requests for the response group application.
Lync Front End Servers	5072	TCP	Yes	Persistence: Source-IP TCP Idle Timeout: 1200 Health Monitor: Default	Port for incoming SIP requests for Microsoft Lync attendant (dial-in conferencing).
Lync Front End Servers	5073	TCP	Yes	Persistence: Source-IP TCP Idle Timeout: 1200 Health Monitor: Default	Port for incoming SIP requests for Lync Server conferencing announcement service.
Lync Front End Servers	5075	TCP	Yes	Persistence: Source-IP TCP Idle Timeout: 1200 Health Monitor: Default	Port for incoming SIP requests for the call park application.

Table 2: Optional Internal Front End Services

Table 3: Services for Internal Edge

Server Role	Port	VIP Type	Source NAT	Feature Templates	Usage Notes
Internal Edge Server	443	TCP	Yes	Persistence: Source-IP Health Monitor: Default	Used for communication between the internal edge server farm FQDN used by Web Components.
Internal Edge Server	3478	UDP	Yes	Health Monitor: Default	Preferred path for media transfer between internal and external users.
Internal Edge Server	5061	TCP/TLS	Yes	Persistence: Source-IP TCP Idle Timeout: 1200 Health Monitor: Default	Used for external ports for SIP/MTLS communication for remote user access or federation.
Internal Edge Server	5062	TCP	Yes	Persistence: Source-IP TCP Idle Timeout: 1200 Health Monitor: Default	Used for authentication of AV users.
Internal Edge Server	8057	TCP	Yes	Persistence: Source-IP Health Monitor: Default	Used for outgoing PSOM traffic sent to the web conferencing server.

Table 3: Services for Internal Edge

Table 4: Services for External Edge

Server Role	Port	VIP Type	Source NAT	Feature Templates	Usage Notes
External Edge Access	443	TCP	Yes	Persistence: Source-IP Health Monitor: Default	Used for external ports for SIP/TLS communication for remote user access, accessing all internal media communications.
External Edge Access	5061	TCP	Yes	Persistence: Source-IP TCP Idle Timeout: 1200 Health Monitor: Default	Port for external SIP/MTLS communication for remote user access and federation.
External Edge WebConf	443	TCP	Yes	Persistence: Source-IP Health Monitor: Default	Used for external ports for SIP/TLS communication for remote user access, accessing all internal media communications.
External Edge AV	443	TCP	Yes	Persistence: Source-IP Health Monitor: Default	Used for external ports for SIP/TLS communication for remote user access, accessing all internal media communications.
External Edge AV	3478	UDP	Yes	Health Monitor: Default	Used for external ports for STUN/UDP inbound and outbound media resources.

Table 4: Services for External Edge

**Note:** During feature selection (Figure 3) of the external edge pool installation, you will be asked to deploy the Lync edge server pool with either single or multiple FQDNs and IP addresses. Deselecting the **use a single FQDN and IP address** option will enable the external edge pool to have multiple IP configurations. The AX device can be deployed in either a single IP configuration or a multiple IP configuration. In a multiple IP configuration, three public “virtual” IP addresses (VIPs) will be required for Access, WebConf and AV. For a single FQDN and IP address configuration, one public VIP will be required.

## 4 CONFIGURING APPLICATION DELIVERY PARTITIONS (OPTIONAL)

In a standard Lync deployment that requires external and internal client access, the deployment must have at least three ADCs to load balance traffic from the External Edge, Internal Edge, and FE Servers within the topology. The AX Series can support Microsoft Lync deployments with Application Delivery Partitions (ADPs), either with Role-based Administration (RBA) or Layer 3 Virtualization (L3V) partitioning. ADPs reduce the ratio of physical-to-virtual ADC device requirements from three hardware load balancers to a single hardware appliance for Microsoft Lync deployments. This significantly simplifies ADC deployment, time to implement, and total cost of ownership (TCO). To get additional information above using ADPs, refer to the *AX Series System Configuration and Administration Guide*.

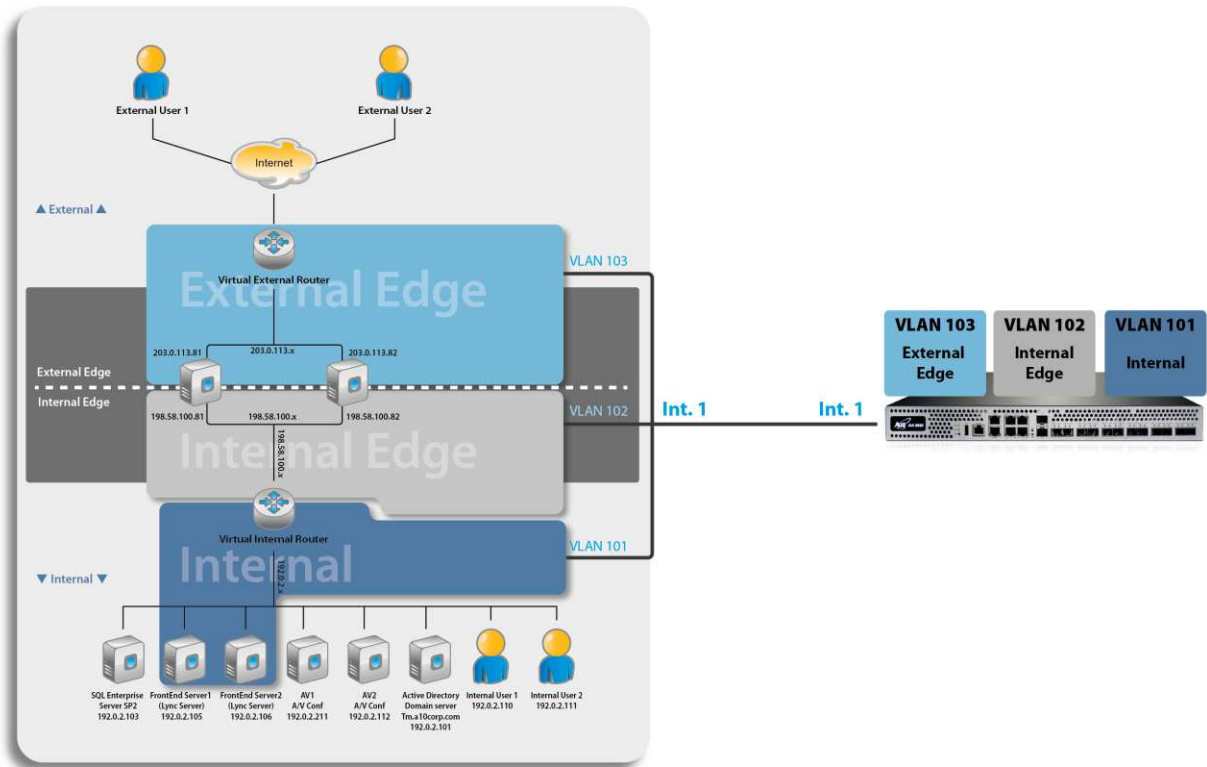


Figure 3: Microsoft Lync 2013 deployment with ADP

## 4.1 ADP CONFIGURATION

ADP support with RBA and L3V was introduced in AX Series Release 2.6.1 for hardware appliances. ADP is easy to configure, requiring only a few ADP commands:

```
active-partition {partition-name | shared}
```

This command enables you to switch the management session among configured partitions.

```
AX#active-partition ExtEdge
Currently active partition: ExtEdge
AX[ExtEdge]#
```

```
partition partition-name
```

This command enables you to create new partitions.

```
AX(config)#partition IntEdge
AX(config)#
```

```
show partition
```

This command enables you to view existing partitions.

```
AX(config)#show partition
Total Number of partitions configured: 3
Partition Name    L3V   Index  Max. aFlex  Admin Count
-----
ExtEdge           No    1      32         0
IntEdge           No    2      32         0
FrontEnd          No    3      32         0
AX(config)#
```

**Note:** For complete syntax information, see the AX Series CLI Reference.

The AX configuration sample shown below contains the following partitions:

- ExtEdge (for the External Edge)
- IntEdge (for the Internal Edge)
- FrontEnd (for the FE Servers).

VLAN tagging (802.1Q) is applied to the frames that travel from the AX device to the Lync VM Servers. Each partition uses a VLAN ID that matches the VLANs within the Lync VM server.

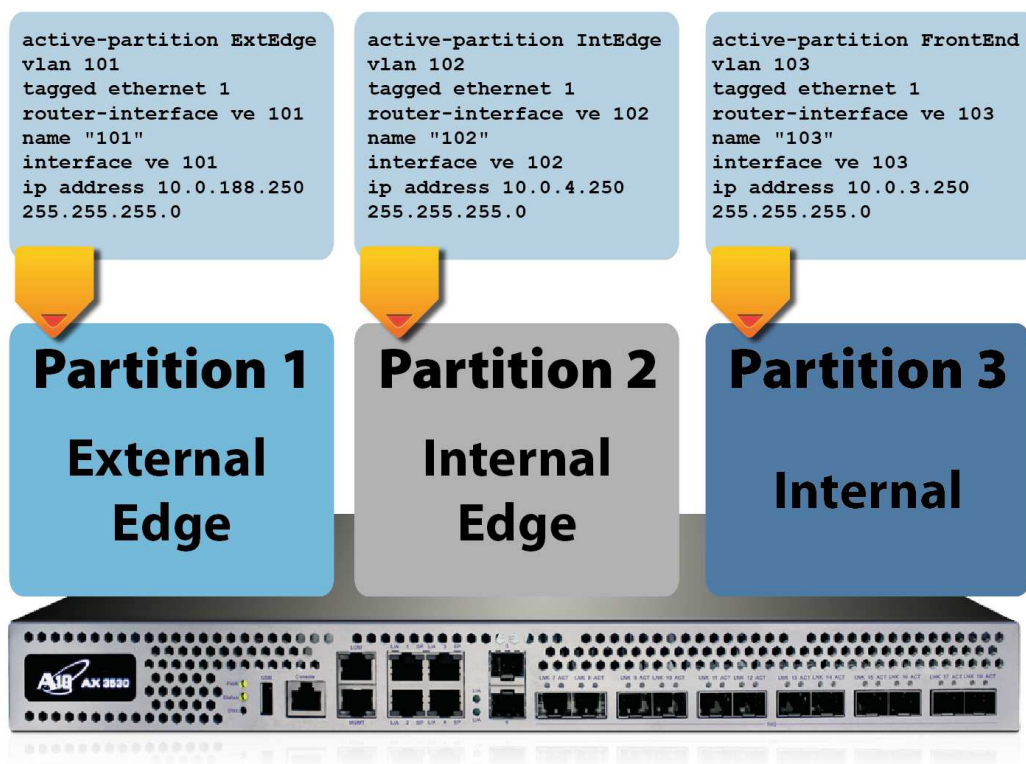


Figure 4: ADP configuration for Lync 2013

## 5 AX SERIES AS A REVERSE PROXY

In order to experience the versatile communication features of Microsoft Lync 2013, there are a few network requirements for communications from the external client to the External Web Services, which is hosted by the Director or the FE server. Deploying a reverse proxy in the Lync 2013 topology allows external Lync clients such as desktop clients, web apps, mobile apps or the Windows Store Lync App to seamlessly log in as external clients to the Lync internal network. The AX Series has been proven and tested to function as a reverse proxy within a Lync 2013 infrastructure.

**Note:** With the Microsoft TMG 2010 End of Life announcement<sup>1</sup>, a load balancer with reverse proxy capabilities such as the AX Series is essential for the Lync 2013 features to work.

## 5.1 LYNC REVERSE PROXY REQUIREMENTS

Lync Server 2013 imposes a few requirements for communication from the external clients to the FE server.

For external clients to be able to communicate with internal Lync services, a secured connection using SSL or TLS certificates is a requirement. Lync 2013 requires the use of SSL and TLS certificates acquired from a public Certificate Authority (CA) to connect to the published External Web Services (EWS) of a front-end server or a director.

As an administrator for the AX Series, you can import and publish the certificates for internal or external web sites. A certificate request must contain the Fully Qualified Domain Name (FQDN) with the matching Simple URLs of the Front End External Pool. The AX Series can support Subject Alternative Name (SAN). When ordering the SAN from a CA, make sure that you list all the FQDN option names from the "Subject Alternative" field.

**Note:** A10 Networks recommends using an SSL or TLS certificate issued from a trusted CA; or, for testing purposes, a self-signed certificate can be generated on the AX Series.

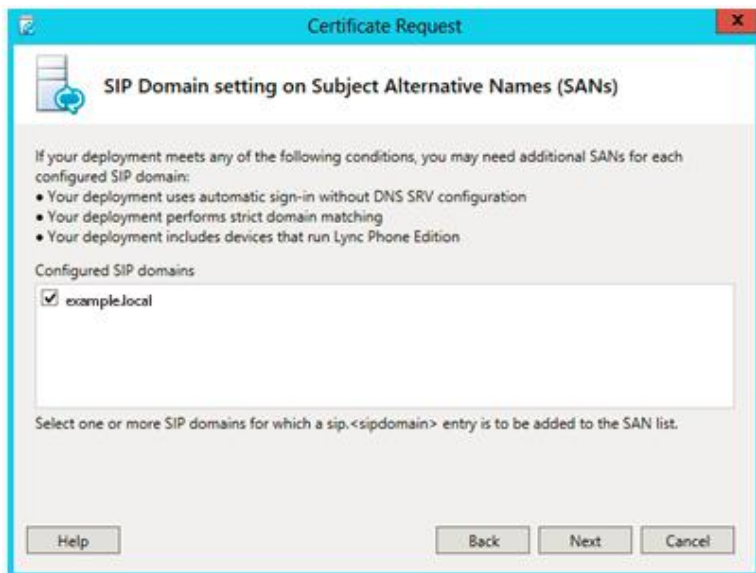


Figure 5: Certificate Request options

<sup>1</sup> <http://technet.microsoft.com/en-us/forefront/ee807302.aspx>

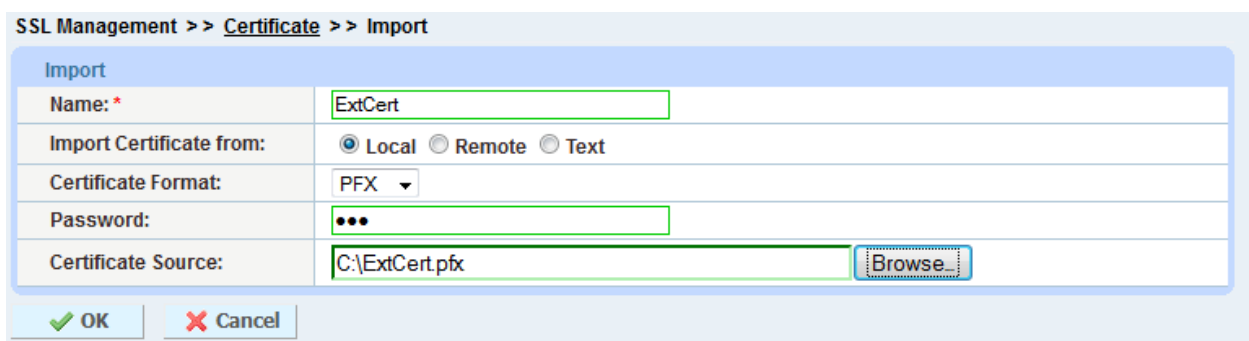


This section of the deployment guide describes how to import a certificate acquired from a CA.

Before starting the procedure, import the certificate and key for Lync 2013:

1. Navigate to **Config Mode > SLB > SSL Management > Certificate**.
2. Click **Import** to add a new SSL certificate.
3. Enter a name for the certificate: "ExtCert".
4. Select **Local** next to Import Certificate from.
5. Enter the certificate **Password** (if applicable).
6. Click **Browse** and navigate to the certificate file.

**Note:** If you are importing a CA-signed certificate for which you used the AX device to generate the CSR, you do not need to import the key. The key is automatically generated on the AX device when you generate the CSR.



SSL Management >> Certificate >> Import

Import	
Name: *	ExtCert
Import Certificate from:	<input checked="" type="radio"/> Local <input type="radio"/> Remote <input type="radio"/> Text
Certificate Format:	PFX
Password:	•••
Certificate Source:	C:\ExtCert.pfx <input type="button" value="Browse"/>

Figure 6: Import a certificate on AX Series

Configure a client-SSL template and add the certificate materials to it. Once completed, apply the client-SSL template to the virtual service, by navigating to **Config Mode > SLB > Service > Virtual Service**. Select the client-SSL certificate template from the drop-down list. Make sure that the server and HTTP templates also are configured and applied to the port 443 virtual service.

Subsequently, the AX Series can bind to a listener or interface through which the FQDN for the EWS will resolve; the AX device allows multiple listeners within a single interface. Typically, the original host header sent by the requesting client is transparently passed on without being modified by the reverse proxy server.

The AX device can redirect or bridge SSL and TLS traffic from one externally defined port to another defined port (for example, from TCP 443 to TCP 4443). The reverse proxy server may decrypt the packet upon receipt and then re-encrypt the packet prior to sending and redirecting unencrypted TCP traffic from one port to another (for example, from TCP 80 to TCP 8080). The AX Series, acting as a reverse proxy for Lync 2013, will seamlessly secure all external clients traversing between external and internal access.

## 6 AX SERIES LOAD BALANCER CONFIGURATION

This section of the deployment guide provides a CLI-based configuration of the AX Series for Lync 2013 deployment. If you prefer to use a GUI-based configuration, please refer to the *AX Series GUI Reference* or you also can use the *Microsoft Lync 2010 Deployment Guide*, as it features the same configuration steps as Lync 2013.

This configuration is segmented into three sections to specifically detail the AX Series configuration requirements for Microsoft Lync 2013 External Edge, Internal Edge and FE Server configuration.

### 6.1 EXTERNAL EDGE CONFIGURATION

This section is for the External Edge configuration. This section of the Lync 2013 topology makes it possible for external end-users to be logged in on the internal network without any remote access or VPN access required. This enables end-users to be authenticated through mobile clients, and users of public IM services to communicate with other users through the same Lync Server.

```
AX2500[ExtEdge]#show run
```

```
active-partition ExtEdge
```

```
vlan 101
```

```
  tagged ethernet 1
```

```
  router-interface ve 101
```

```
  name "101"
```

```
interface ve 101
```

```
  ip address 10.0.188.250 255.255.255.0
```

```
ip nat pool snat 10.0.188.122 10.0.188.122 netmask /24
```

```
health monitor hm
```

```
slb server EE1 10.0.188.4
```

```
  port 443 tcp
```

```
  port 5061 tcp
```

```
  port 3478 udp
```


**External Edge Network configuration**

**Source NAT pool configuration**

**Server health monitor**

**External Edge Server configuration**

```
slb server EE2 10.0.188.5
  port 443 tcp
  port 5061 tcp
  port 3478 udp
slb service-group 443 tcp
  method least-connection
  health-check hm
  member EE1:443
  member EE2:443
slb service-group 5061 tcp
  method least-connection
  member EE1:5061
  member EE2:5061
slb service-group 3478 udp
  method least-connection
  health-check hm
  member EE1:3478
  member EE2:3478
slb template tcp tcp
  idle-timeout 1200
slb template persist source-ip sip
slb virtual-server EEVIP 10.0.188.122
  port 443 tcp
  name _10.0.188.122_TCP_443
  source-nat pool snat
  service-group 443
```



**External Edge service group configuration**



**Persistent template**



**External Edge VIP configuration**

```
    template persist source-ip sip
port 5061 tcp
    name _10.0.188.122_TCP_5061
    source-nat pool snat
    service-group 5061
    template tcp tcp
    template persist source-ip sip
port 3478 udp
    name _10.0.188.122_UDP_3478
    source-nat pool snat
    service-group 3478
    template persist source-ip sip
```

**External Edge VIP configuration  
(continued)**

## 6.2 INTERNAL EDGE CONFIGURATION

This section of the configuration is for the Internal Edge Server for external-to-internal facing communications. The internal and external networks are configured with different subnets; routing between both interfaces is not possible.

```
AX2500[IntEdge]#show run
```

```
active-partition IntEdge
```

```
vlan 102
```

```
    tagged ethernet 1
```

```
    router-interface ve 102
```

```
    name "102"
```

```
interface ve 102
```

```
    ip address 10.0.4.250 255.255.255.0
```

```
ip route 10.0.188.0 /24 10.0.4.1
```

```
ip route 10.0.3.0 /24 10.0.4.1
```

**Internal Edge network configuration**

```
ip nat pool snat 10.0.4.222 10.0.4.222 netmask /24
health monitor hm
slb server IE1 10.0.4.4
    health-check hm
    port 443 tcp
    port 3478 udp
    port 5061 tcp
    port 5062 tcp
    port 8057 tcp
    port 3478 tcp
slb server IE2 10.0.4.5
    health-check hm
    port 443 tcp
    port 3478 tcp
    port 5061 tcp
    port 5062 tcp
    port 8057 tcp
    port 3478 udp
slb service-group 443 tcp
    method least-connection
    health-check hm
    member IE1:443
    member IE2:443
slb service-group 3478 udp
    method least-connection
    health-check hm
```

**Source NAT configuration**

**Server health monitor**

**Internal Edge Server configuration**

```
member IE1:3478
member IE2:3478
slb service-group 5061 tcp
method least-connection
member IE1:5061
member IE2:5061
slb service-group 5062 tcp
method least-connection
member IE1:5062
member IE2:5062
slb service-group 8057 tcp
method least-connection
health-check hm
member IE1:8057
member IE2:8057
slb template tcp tcp
idle-timeout 1200
slb template persist source-ip sip
```



***Internal Edge service group configuration***

***Internal Edge required templates***

```
slb virtual-server IEVIP 10.0.4.122
  port 443 tcp
    name _10.0.4.122_TCP_443
    source-nat pool snat
    template tcp tcp
    template persist source-ip sip
  port 3478 udp
    name _10.0.4.122_TCP_3478
    source-nat pool snat
    template persist source-ip sip
  port 5061 tcp
    name _10.0.4.122_TCP_5061
    source-nat pool snat
    template tcp tcp
    template persist source-ip sip
  port 5062 tcp
    name _10.0.4.122_TCP_5062
    source-nat pool snat
    template tcp tcp
    template persist source-ip sip
  port 8057 tcp
    name _10.0.4.122_TCP_8057
    source-nat pool snat
    template tcp tcp
    template persist source-ip sip
end
```

**Configuration of VIP**

## 6.3 FRONT END CONFIGURATION

This section details the configuration parameters for the Microsoft Lync 2013 FE servers. The FE servers provide user authentication, registration, presence, IM, web conferencing and application sharing functionality. FE servers also provide address book services and distribution list expansion. FE servers are provisioned in a front-end pool and configured identically to provide scalability and failover capability to Lync users.

```
AX2500#active-partition FrontEnd
```

```
Currently active partition: FrontEnd
```

```
AX2500[FrontEnd]#show run
```

```
active-partition FrontEnd
```

```
vlan 103
```

```
  tagged ethernet 1
```

```
  router-interface ve 103
```

```
  name "103"
```

```
interface ve 103
```

```
  ip address 10.0.3.250 255.255.255.0
```

```
ip nat pool snat 10.0.3.222 10.0.3.222 netmask /24
```

```
health monitor hm
```

```
slb server FE1 10.0.3.10
```

```
  health-check hm
```

```
  port 135 tcp
```

```
  port 443 tcp
```

```
  port 444 tcp
```

```
  port 5061 tcp
```

```
  port 5060 tcp
```

```
  port 5065 tcp
```

```
  port 5071 tcp
```


**Front End Server network  
configuration**

**Front End Server health monitor**

**Front End server configuration**




```
port 5072 tcp
port 5073 tcp
port 5075 tcp
slb server FE2 10.0.3.11
health-check hm
port 135 tcp
port 443 tcp
port 444 tcp
port 5061 tcp
port 5060 tcp
port 5065 tcp
port 5071 tcp
port 5072 tcp
port 5073 tcp
port 5075 tcp
slb service-group 135 tcp
method least-connection
member FE1:135
member FE2:135
slb service-group 443 tcp
method least-connection
member FE1:443
member FE2:443
slb service-group 444 tcp
method least-connection
member FE1:444
```



**Front End server configuration  
(continued)**

**Front End service group configuration**

```
    member FE2:444
slb service-group 5061 tcp
    method least-connection
    member FE1:5061
    member FE2:5061
slb service-group 5060 tcp
    method least-connection
    member FE1:5060
    member FE2:5060
slb service-group 5065 tcp
    method least-connection
    member FE1:5065
    member FE2:5065
slb service-group 5071 tcp
    method least-connection
    member FE1:5071
    member FE2:5071
slb service-group 5072 tcp
    method least-connection
    member FE1:5072
    member FE2:5072
slb service-group 5073 tcp
    method least-connection
    member FE1:5073
    member FE2:5073
slb service-group 5075 tcp
```



**Front end service group configuration  
(continued)**

```
method least-connection
member FE1:5075
member FE2:5075
slb template tcp tcp
idle-timeout 1200
slb template persist source-ip sip
slb virtual-server fevip 10.0.3.122
port 135 tcp
name _10.0.3.122_TCP_135
source-nat pool snat
service-group 135
template tcp tcp
template persist source-ip sip
port 443 tcp
name _10.0.3.122_TCP_443
source-nat pool snat
service-group 443
template tcp tcp
template persist source-ip sip
port 444 tcp
name _10.0.3.122_TCP_443
source-nat pool snat
service-group 444
template tcp tcp
template persist source-ip sip
port 5061 tcp
```

**Front End service group configuration  
(continued)**

**Persistence configuration**

**Front End Server VIP configuration**

```
name _10.0.3.122_TCP_5061
source-nat pool snat
service-group 5061
template tcp tcp
template persist source-ip sip
port 5060 tcp
name _10.0.3.122_TCP_5060
source-nat pool snat
service-group 5060
template tcp tcp
template persist source-ip sip
port 5065 tcp
name _10.0.3.122_TCP_5065
source-nat pool snat
service-group 5065
template tcp tcp
template persist source-ip sip
port 5071 tcp
name _10.0.3.122_TCP_5071
source-nat pool snat
service-group 5071
template tcp tcp
template persist source-ip sip
port 5072 tcp
name _10.0.3.122_TCP_5072
source-nat pool snat
```

**Front End Server VIP configuration  
(continued)**

```
service-group 5072
template tcp tcp
template persist source-ip sip
port 5073 tcp
name _10.0.3.122_TCP_5073
source-nat pool snat
service-group 5073
template tcp tcp
template persist source-ip sip
port 5075 tcp
name _10.0.3.122_TCP_5075
source-nat pool snat
service-group 5075
template tcp tcp
template persist source-ip sip
end
```

**Front End Server VIP configuration  
(continued)**

## 7 SUMMARY AND CONCLUSION

The configuration steps described in this document show how to set up the AX Series for Microsoft Lync 2013 Server. By using the AX device to load balance Lync application services, the following key advantages are achieved:

- Transparent application load sharing
- AX Series reverse proxy capabilities for allowing external clients to communicate with the internal FE servers
- Deployment with ADPs to reduce deployment costs, from three physical load balancers required by the Microsoft Lync 2013 topology to 1 physical load balancer using A10 Networks' ADP partitioning technology
- Higher availability when Lync Servers fail, so that there is no direct impact to how end-users access the applications
- Higher utilization, as the AX device transparently load balances to multiple Lync 2013 communication servers
- Higher connection throughput and faster responsiveness experienced by end-users, through offload of security processing to the AX device

For more information about AX Series products, refer to:

<http://a10networks.com/products/axseries.php>

<http://a10networks.com/resources/solutionsheets.php>

<http://a10networks.com/resources/casestudies.php>