DEPLOYMENT GUIDE

# A10 THUNDER ADC WITH MICROSOFT EXCHANGE 2016

## EMPOWERING EMPLOYEES TO COMMUNICATE AND COLLABORATE WITH MICROSOFT EXCHANGE 2016

# OVERVIEW

Microsoft® Exchange® is the leading global unified communication solution for the enterprise.

The purpose of this guide is to provide a step-by-step process for deploying A10 Thunder® ADC as a load balancer in a Microsoft Exchange 2016 server deployment using AppCentric Templates (ACT). Refer to Appendix A for the equivalent CLI-based configuration.

Adding Thunder ADC to your Microsoft Exchange Server deployments provides the following benefits:

- High Scalability – Thunder ADC allows enterprises to scale their Exchange services for a very large number of employees by load balancing traffic among multiple Exchange Servers.
- High Availability – Exchange services are guaranteed even if an Exchange Server goes offline.
- High Performance – Thunder ADC can improve Exchange Server performance by terminating SSL connections in its hardware.
- Better Security – Thunder ADC can mitigate Distributed Denial of Service (DDoS) attacks. In addition, it can provide an authentication proxy service and provide pre-authentication.
- Simplified Deployment – A10 Networks AppCentric Templates allow enterprises to configure and deploy one single public virtual IP (VIP) address to be used for all Exchange services effortlessly. They also provide visibility into Exchange services and login activities.

For additional Microsoft deployment guides such as Skype for Business Server 2015, Lync, SharePoint and IIS, please refer to: a10networks.com/resources/deployment-guides.


TALK
WITH A10

CONTACT US
a10networks.com/contact

# TABLE OF CONTENTS


OVERVIEW ..... 2
EXCHANGE 2016 ARCHITECTURE ..... 4
DEPLOYMENT PREREQUISITES ..... 4
ACCESSING THUNDER ADC ..... 4
ARCHITECTURE OVERVIEW ..... 5
VALIDATING EXCHANGE 2016 CONFIGURATION ..... 5
- Virtual Directories ..... 6
- Database Availability Group ..... 7
- SSL Offload ..... 8
- POP3 and IMAP4 Services ..... 9
- OWA/ECP Authentication ..... 10

THUNDER ADC CONFIGURATION SUMMARY ..... 12
- Session Persistence in Exchange 2016 ..... 13
- SSL Certificate Configuration ..... 13

THUNDER ADC EXCHANGE CONFIGURATION USING APPCENTRIC TEMPLATES ..... 14
- AppCentric Templates (ACT) Overview ..... 14
- Configuration Using ACT ..... 14
- Wizard – Topology ..... 16
- Wizard – Virtual Server ..... 16
- Wizard – HTTPS ..... 17
- Wizard – IMAP4/POP3 ..... 19
- Wizard – SMTP ..... 20
- Wizard – Review ..... 21
- Exchange Dashboard ..... 23

ADDITIONAL SECURITY FEATURE – DDOS MITIGATION (OPTIONAL) ..... 24
- DDoS Mitigation ..... 24

SUMMARY ..... 25
APPENDIX A – THUNDER ADC TEST CONFIGURATION ..... 26
APPENDIX B – APPCENTRIC TEMPLATES UPGRADE ..... 31
- Upgrading ACT using Cloud-based Update ..... 31
- Upgrading ACT using Manual Update ..... 32
- ABOUT A10 NETWORKS ..... 33



***DISCLAIMER***

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and noninfringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

# EXCHANGE 2016 ARCHITECTURE

Microsoft Exchange is the leading global unified communication solution for the enterprise. With Exchange 2016, Microsoft reduced the number of server roles to two: the Mailbox and Edge Transport server roles.

The Mailbox server in Exchange 2016 includes all of the server components from the Exchange 2013 Mailbox and Client Access server roles[1]:

- Client Access services provide authentication, limited redirection and proxy services. Client Access services don't do any data rendering and offer all the usual client access protocols: HTTP, POP, IMAP and SMTP.
- Mailbox services include all traditional server components found in the Exchange 2013 Mailbox server role: the backend client access protocols, Transport service, Mailbox databases, and Unified Messaging. The Mailbox server handles all activity for the active mailboxes on that server.

The Edge Transport role is typically deployed in the perimeter network, outside the internal Active Directory forest, and is designed to minimize the attack surface of your Exchange deployment. By handling all Internet-facing mail flows, it also adds additional layers of message protection and security against viruses and spam, and can apply mail flow rules (also known as transport rules) to control message flow.

For more information about the Exchange 2016 architecture, see:

https://technet.microsoft.com/en-us/library/jj150491(v=exchg.160).aspx

A10 Networks Thunder ADC (Application Delivery Controller) provides intelligent load balancing, security, acceleration and optimization for Microsoft Exchange 2016.

[1] https://technet.microsoft.com/EN-US/library/jj150540(v=exchg.160).aspx

# DEPLOYMENT PREREQUISITES

This Microsoft Exchange 2016 deployment with Thunder ADC has the following prerequisites (based on tested configuration, Appendix A):

- A10 Thunder ADC must be running A10 Networks Advanced Core Operating System (ACOS®) version 4.1.1-P1 or higher.
- The AppCentric Templates (ACT) version is: act-0706-17 (see Appendix B for details).
- Microsoft Exchange 2016 has been tested with A10 physical and virtual appliances.
- Thunder ADC can be deployed in routed mode, one-arm mode and transparent mode.
- Both IPv4 and IPv6 are supported. The examples in this deployment guide use IPv4.

For technical requirements to deploy Exchange 2016 servers, see Exchange 2016 system requirements:

https://technet.microsoft.com/en-us/library aa996719(v=exchg.160).aspx

# ACCESSING THUNDER ADC

This section describes how to access Thunder ADC from a Command Line Interface (CLI) or Graphical User Interface (GUI):

- CLI – The CLI is a text-based interface in which you type commands on a command line. You can access the CLI directly 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)
- GUI – This is a web-based interface in which you click buttons, menus and other graphical icons to access the configuration or management pages. From these pages, you can type or select values to configure or manage the device. You can access the GUI using the following protocol:
  - Secure protocol – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

***NOTE**: HTTP requests are redirected to HTTPS by default on Thunder ADC.*

**Default Access Information:**

- Default Username: "admin"
- Default password: "a10"
- Default IP address of the device: "172.31.31.31"

***NOTE**: For detailed information on how to access the Thunder ADC device, refer to the System Configuration and Administration Guide.*

# ARCHITECTURE OVERVIEW

The diagram below provides an architectural overview of how Exchange 2016 can be optimized with A10 Thunder ADC.

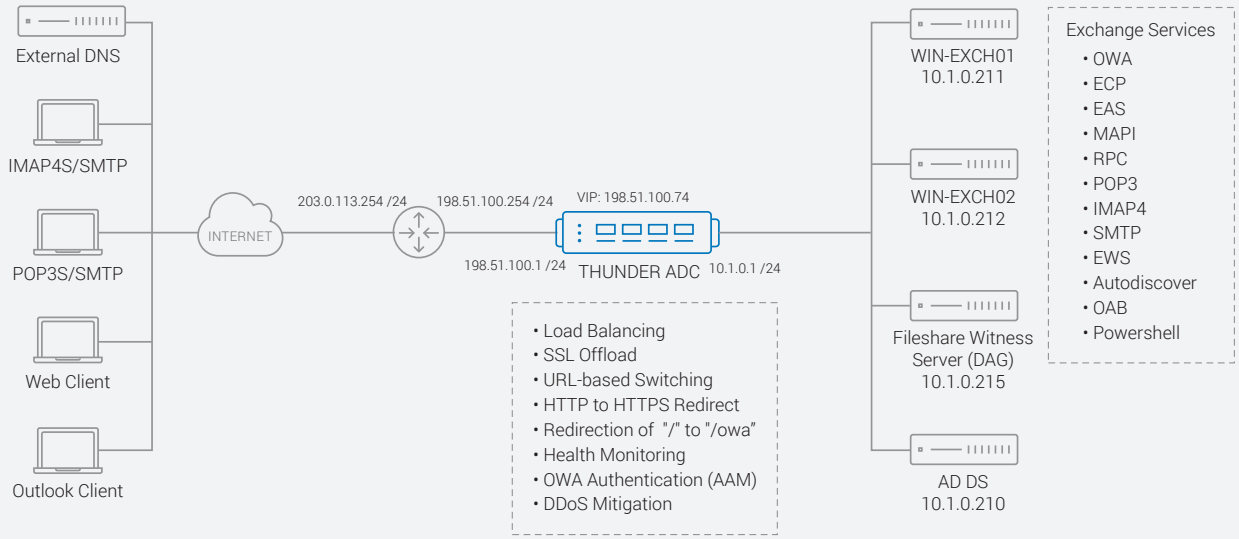



**Figure 1**: Lab topology

# VALIDATING EXCHANGE 2016 CONFIGURATION

Before you start making configuration changes from Thunder ADC, use this section to validate the Exchange 2016 server configuration.

1. Open a web browser and navigate to one of the Exchange Mailbox servers.
2. Navigate to https://<Exchange Server IP Address>/ecp.
3. Log in with domain administrator credentials.
4. On the left menu panel, click Servers and on the top panel select Servers again. The menu provides a list of Mailbox servers deployed within Exchange 2016. These servers will be configured as real servers on Thunder ADC and referenced by a virtual IP (VIP) address.

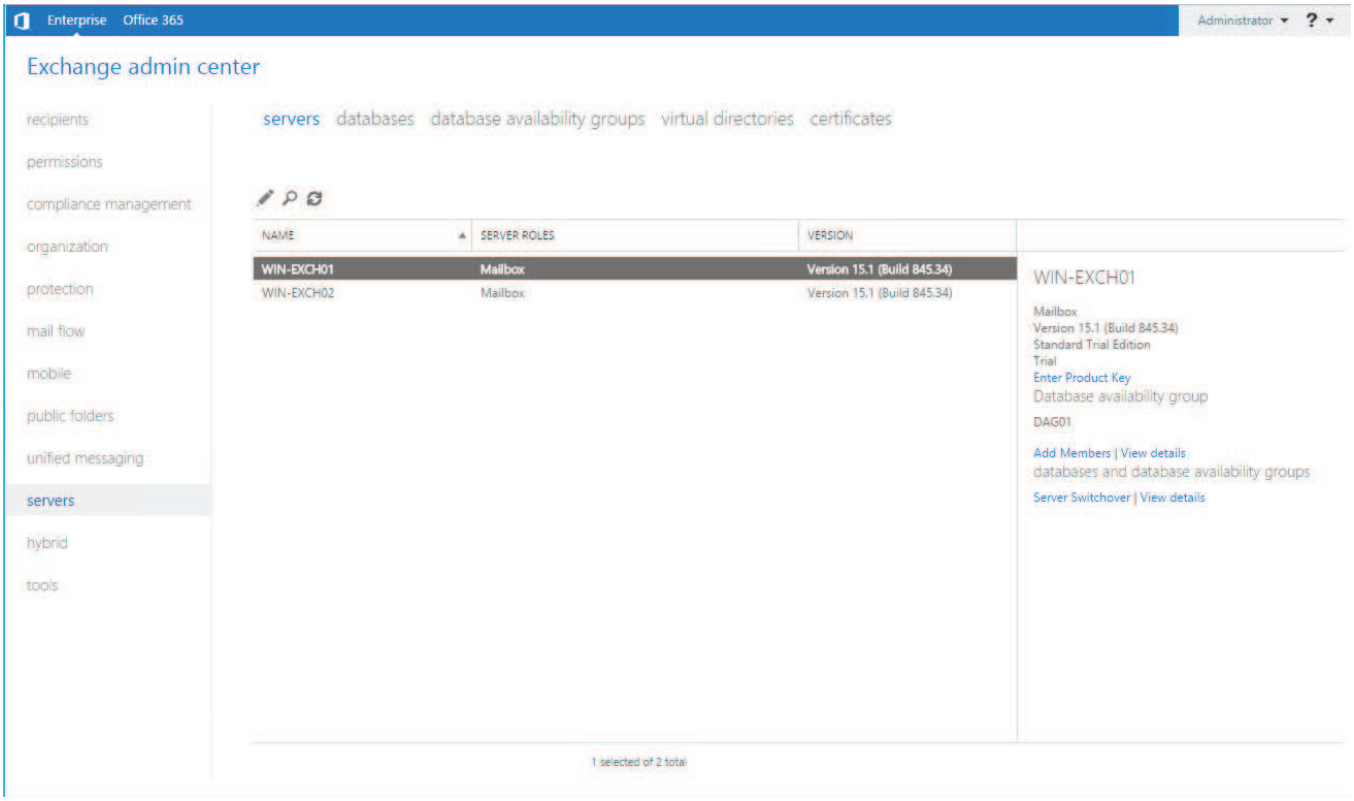



Figure 2: List of Exchange 2016 servers

## *VIRTUAL DIRECTORIES*

In this setup, a single namespace has been deployed on the Exchange Servers. Additionally, the internal and external URLs have been configured to be the same.

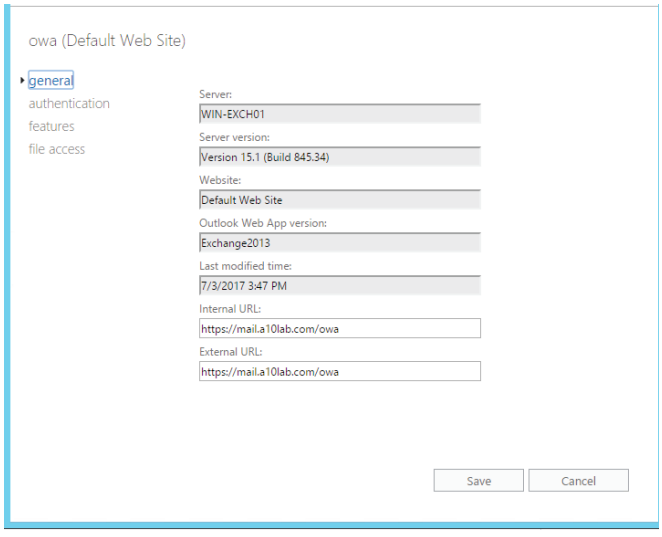



**Figure 3**: OWA virtual directory

## *DATABASE AVAILABILITY GROUP*

A database availability group (DAG) is a set of up to 16 Microsoft Exchange Server 2016 Mailbox servers that provide automatic database-level recovery from a database, server or network failure. When a Mailbox server is added to a DAG, it works with the other servers in the DAG to provide automatic, database-level recovery from database, server and network failures.

On the left menu panel, click Servers, and in the top menu, select Databases. A menu appears, listing the databases configured in your solution. The databases must be configured within DAGs for redundancy purposes.

To understand how to configure DAGs in Exchange 2016, refer to the following URL: https://technet.microsoft.com/en-us/library/dd351172(v=exchg.160).aspx

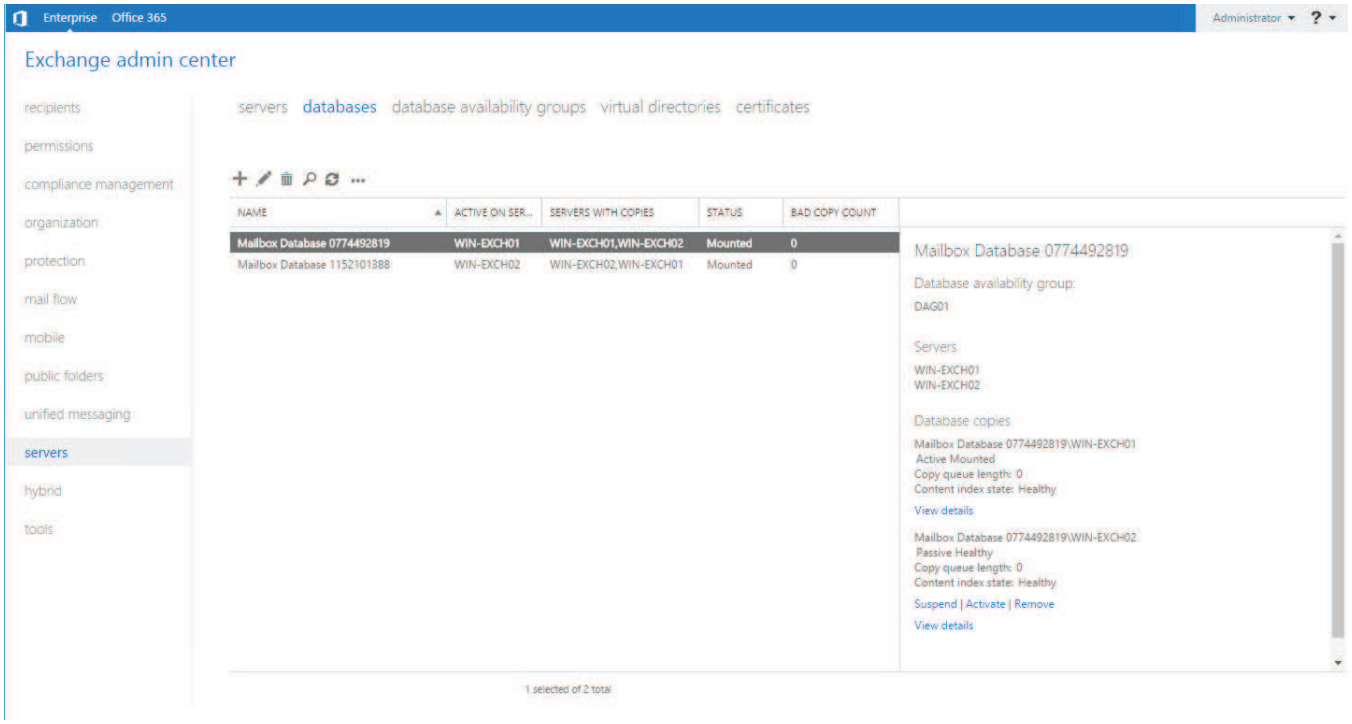



**Figure 4:** Mailbox databases

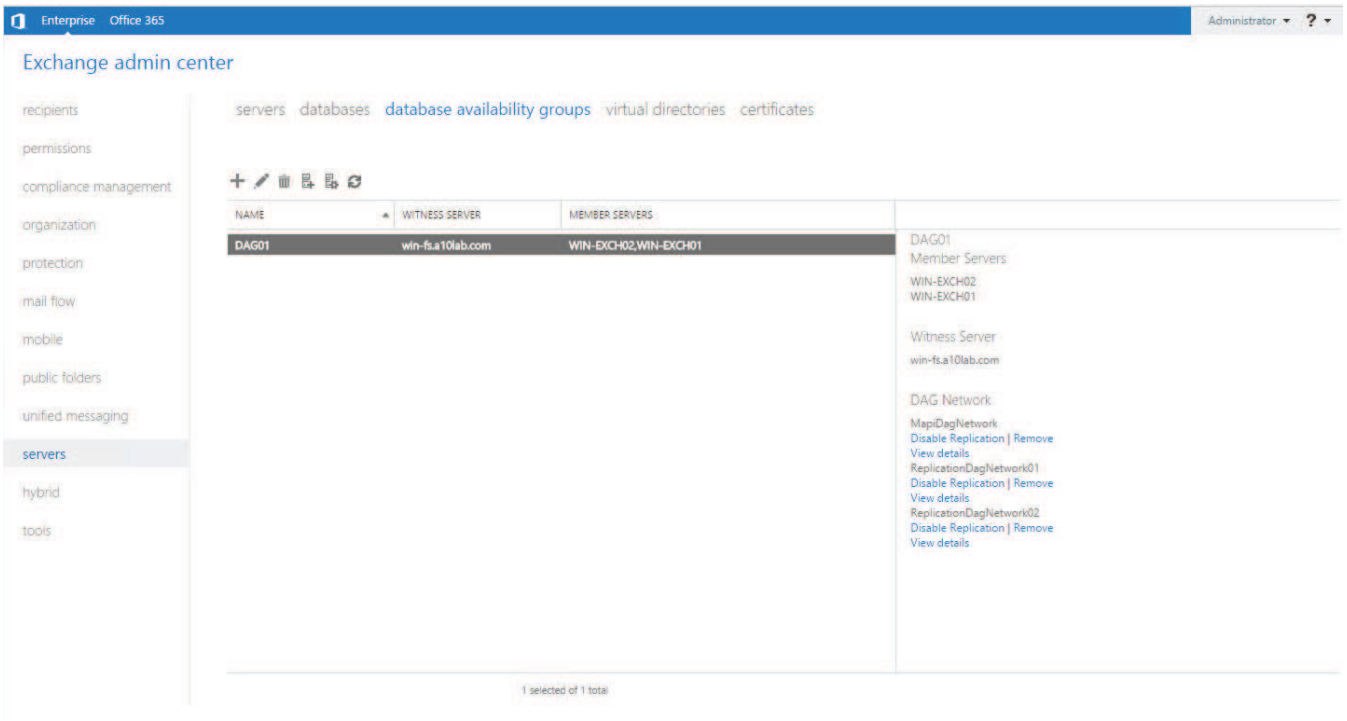



**Figure 5:** Database availability groups

## *SSL OFFLOAD*

To enable SSL Offloading for the various servers running on the Exchange Servers, follow the steps outlined at: https://technet.microsoft.com/en-us/library/dn635115(v=exchg.150).aspx

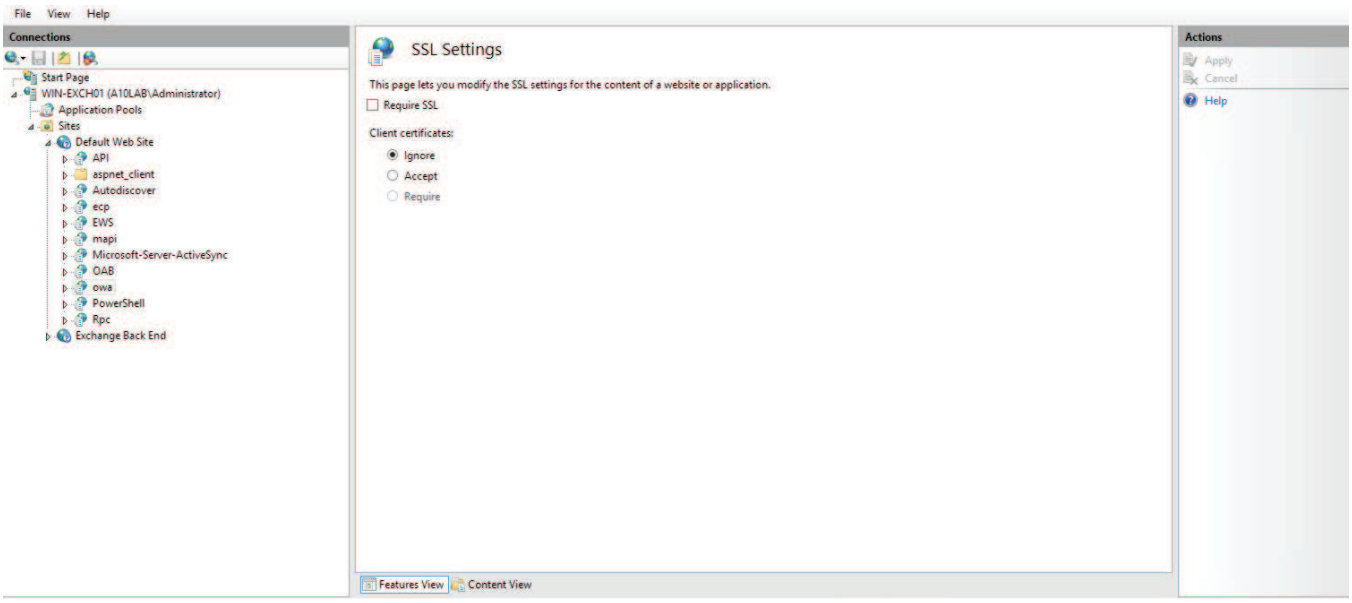



**Figure 6:** IIS Server: Disable the option "Require SSL"

## *POP3 AND IMAP4 SERVICES*

By default, POP3 and IMAP4 client connectivity isn't enabled in Exchange. To enable POP3 and/or IMAP4 client connectivity, you need to perform the following steps:

1. Start the POP3 and/or IMAP4 services, and configure the services to start automatically
2. Configure the POP3 and/or IMAP4 settings for external clients
3. Configure authenticated SMTP settings for POP3 and IMAP4 clients in Exchange 2016

See the Microsoft TechNet webpage for details:

https://technet.microsoft.com/en-us/library/dd298114(v=exchg.160).aspx

In addition, if you plan to use SSL Offload on Thunder ADC, set the logon method for POP3 and IMAP4 services to plain text as shown below.

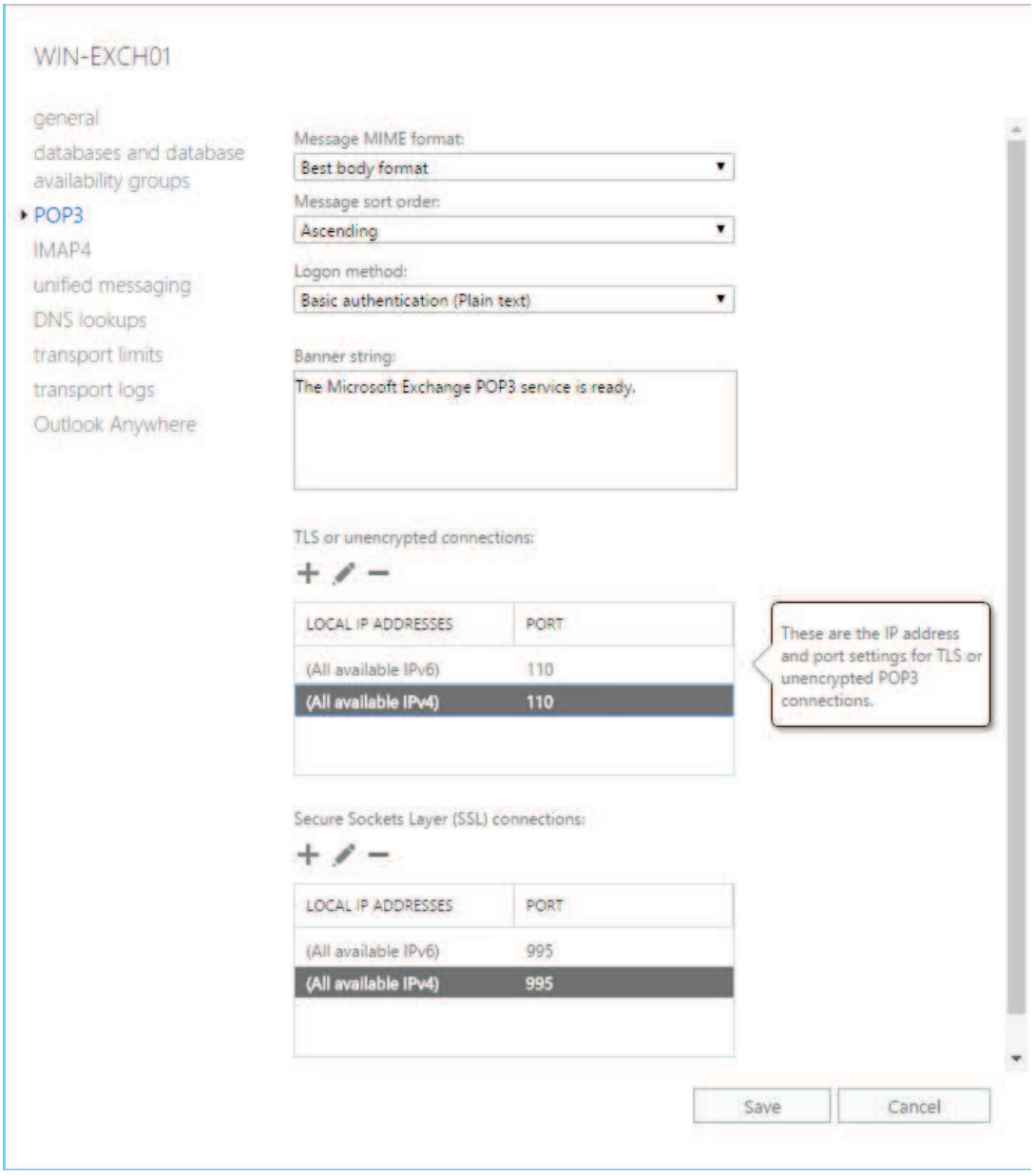



**Figure 7:** POP3 settings

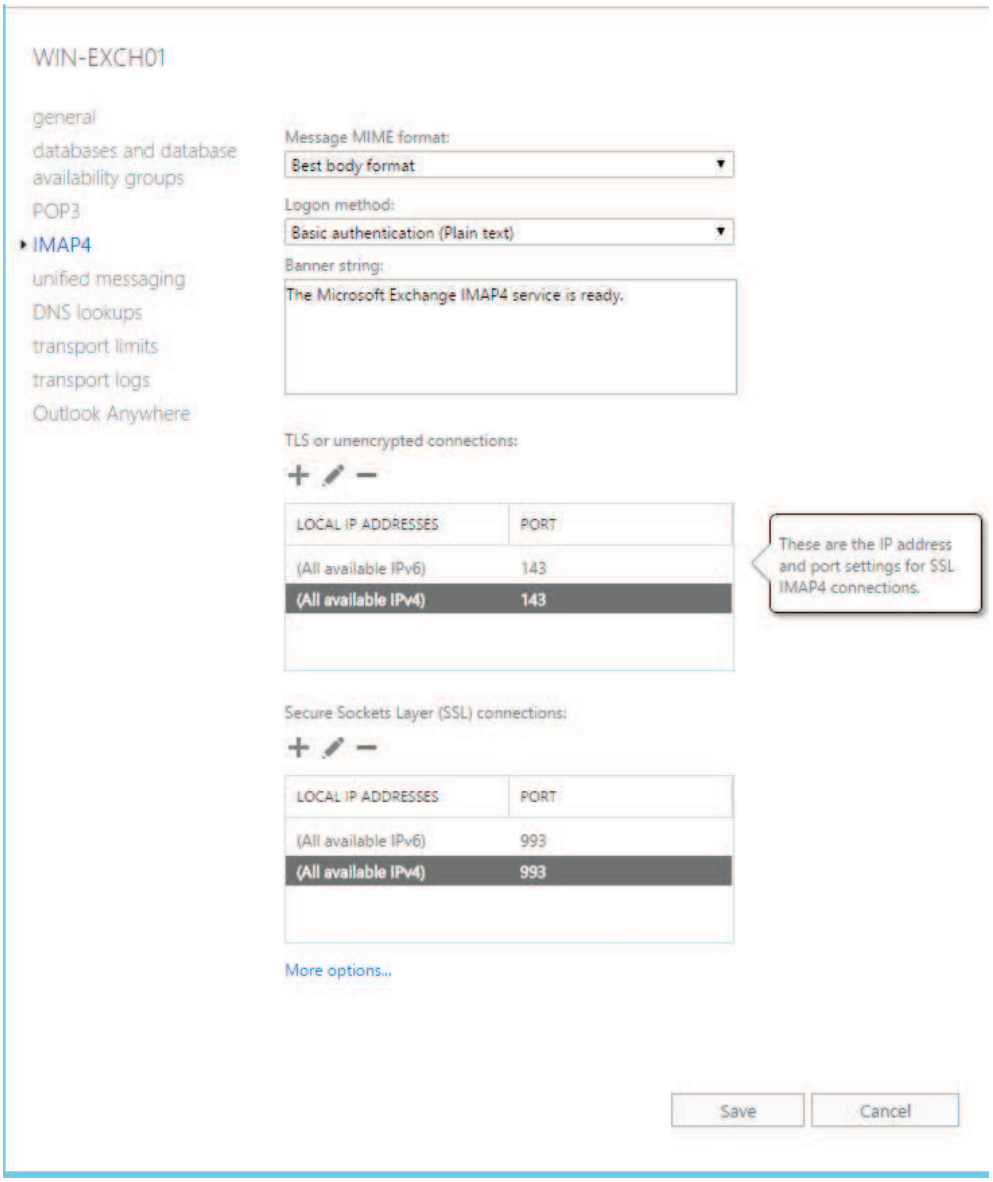



**Figure 8:** IMAP4 settings

## *OWA/ECP AUTHENTICATION*

In this setup, we are going to enable OWA authentication on Thunder ADC with Basic relay protocol and hence configure Outlook Web App (OWA) and Exchange Control Panel (ECP) authentication to Basic authentication on the Exchange Server. Make sure to set the authentication settings to be the same for both OWA and ECP and Exchange 2016 will also prompt you to do so.

***NOTE**: Certain versions of Exchange 2016 updates may cause client logoff issues with Basic authentication. Please refer to the appropriate Microsoft documentation for latest fixes and recommended settings.*

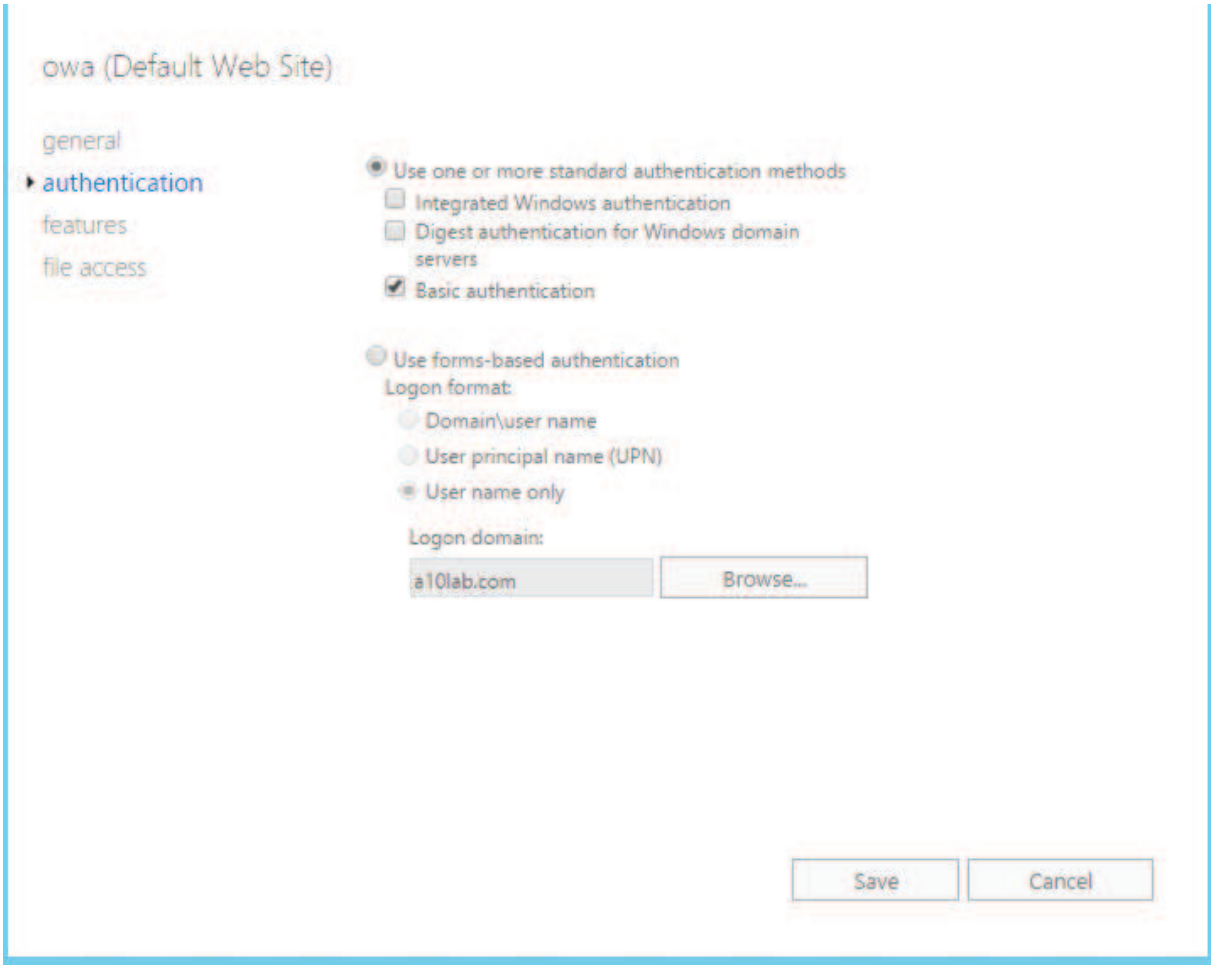



**Figure 9:** OWA authentication

Once the prerequisites have been configured, verify that incoming and outgoing mail can be received or sent before adding Thunder ADC to the solution. **Do not begin deployment of the ACOS solution unless Exchange 2016 is functioning correctly**.

# THUNDER ADC CONFIGURATION SUMMARY

This deployment guide provides step-by-step instructions based on a single VIP address configuration with multiple services using AppCentric Templates. With this option, Thunder ADC is configured with a single VIP bound to multiple Exchange services such as OWA, ActiveSync, Offline Address Book (OAB), Outlook Anywhere and Autodiscover.

The following table summarizes the Thunder ADC configuration for each Exchange service.

*TABLE 1: THUNDER ADC CONFIGURATION PARAMETERS*

| EXCHANGE SERVICE | REAL SERVERS | HEALTH MONITOR | VIP | OTHER |
|---|---|---|---|---|
| Outlook Web App (OWA) | IP: Exchange Server<br><br>Port: 80 | HTTP URL<br>GET<br>/owa/healthcheck.htm | IP: IP accessed by clients<br><br>Type: HTTPS (with SSL Offload)<br>Port: 443 | Load-Balancing method: Least Connection<br><br>Transparently redirect HTTP clients to HTTPS<br><br>Transparently add "/owa" to requests without it |
| Exchange Control Panel (ECP) | IP: Exchange Server<br><br>Port: 80 | HTTP URL<br>GET<br>/ecp/healthcheck.htm | IP: IP accessed by clients<br><br>Type: HTTPS (with SSL Offload)<br>Port: 443 | Load-Balancing method: Least Connection<br><br>Transparently redirect HTTP clients to HTTPS |
| Exchange ActiveSync | IP: Exchange Server<br><br>Port: 80 | HTTP URL<br>GET /Microsoft-Server-ActiveSync/healthcheck.htm | IP: IP accessed by clients<br><br>Type: HTTPS (with SSL Offload)<br>Port: 443 | Load-Balancing method: Least Connection<br><br>Transparently redirect HTTP clients to HTTPS |
| Outlook Anywhere (MAPI) | IP: Exchange Server<br><br>Port: 80 | HTTP URL<br>GET /mapi/healthcheck.htm | IP: IP accessed by clients<br><br>Type: HTTPS (with SSL Offload)<br>Port: 443 | Load-Balancing method: Least Connection<br><br>Transparently redirect HTTP clients to HTTPS |
| Outlook Anywhere (RPC) | IP: Exchange Server<br><br>Port: 80 | HTTP URL<br>GET /rpc/healthcheck.htm | IP: IP accessed by clients<br><br>Type: HTTPS (with SSL Offload)<br>Port: 443 | Load-Balancing method: Least Connection<br><br>Transparently redirect HTTP clients to HTTPS |
| POP3/POP3S | IP: Exchange Server<br><br>Port: 110 | TCP (port 110) | IP: IP accessed by clients<br><br>Type: POP3<br>Port 110<br><br>Type: SSL-Proxy (with SSL offload)<br>Port: 995 | Load-Balancing method: Least Connection |
| IMAP4/IMAP4S | IP: Exchange Server<br><br>Port: 143 | TCP (port 143) | IP: IP accessed by clients<br><br>Type: IMAP4<br>Port 143<br><br>Type: SSL-Proxy (with SSL offload)<br>Port: 993 | Load-Balancing method: Least Connection |
| SMTP | IP: Exchange Server<br><br>Port: 587 | TCP (port 587) | IP: IP accessed by clients<br><br>Type: SMTP (STARTTLS with SSL offload)<br>Port: 587 | Load-Balancing method: Least Connection<br><br>SMTP STARTTLS enforced |

| EXCHANGE SERVICE | REAL SERVERS | HEALTH MONITOR | VIP | OTHER |
|---|---|---|---|---|
| Exchange Web Services (EWS) | IP: Exchange Server<br><br>Port: 80 | HTTP URL<br>GET /ews/healthcheck.htm | IP: IP accessed by clients<br><br>Type: HTTPS (with SSL Offload)<br>Port: 443 | Load-Balancing method: Least Connection<br><br>Transparently redirect HTTP clients to HTTPS |
| Autodiscover | IP: Exchange Server<br><br>Port: 80 | HTTP URL<br>GET /autodiscover/ healthcheck.htm | IP: IP accessed by clients<br><br>Type: HTTPS (with SSL Offload)<br>Port: 443 | Load-Balancing method: Least Connection<br><br>Transparently redirect HTTP clients to HTTPS |
| Offline Address Book (OAB) distribution | IP: Exchange Server<br><br>Port: 80 | HTTP URL<br>GET /oab/healthcheck.htm | IP: IP accessed by clients<br><br>Type: HTTPS (with SSL Offload)<br>Port: 443 | Load-Balancing method: Least Connection<br><br>Transparently redirect HTTP clients to HTTPS |

## SESSION PERSISTENCE IN EXCHANGE 2016

In Exchange 2016, session persistence is not required. See the following link for details:

https://blogs.technet.microsoft.com/exchange/2015/10/08/load-balancing-in-exchange-2016/

## SSL CERTIFICATE CONFIGURATION

SSL Offload acts as an acceleration feature by removing the burden of processing SSL traffic from the Exchange Servers. To use SSL Offload, you need to either import an SSL Certificate or you can generate a self-signed certificate on Thunder ADC.

In this setup, we used a self-signed certificate for ease of deployment.

To generate a self-signed certificate and key pair:

- Go to ADC > SSL Management > SSL Certificates
- Click on Create

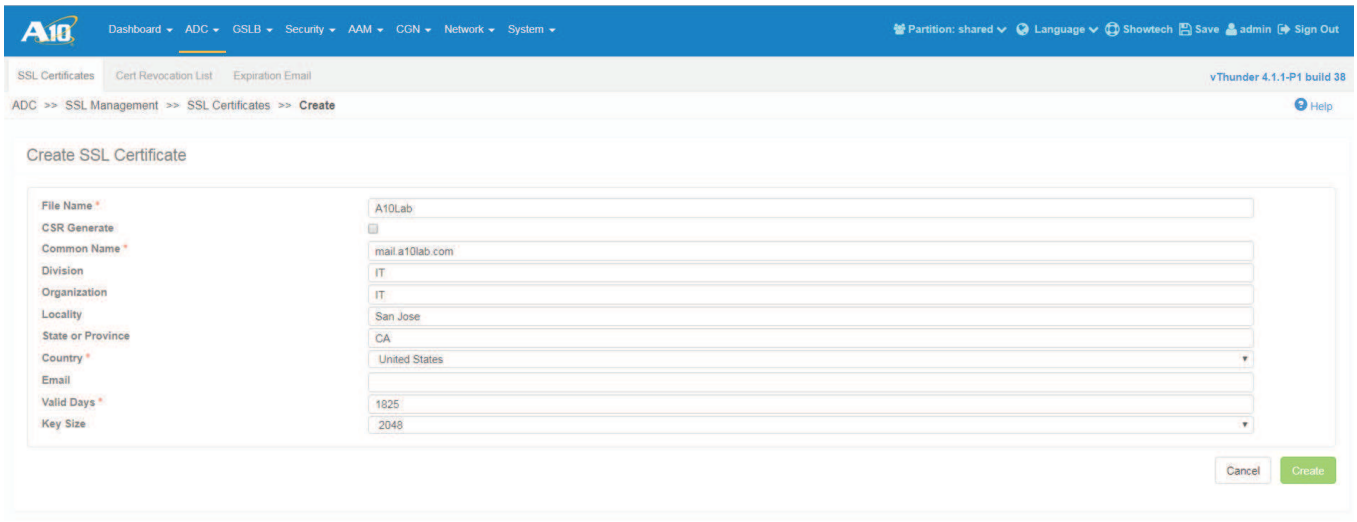



**Figure 10:** Create self-signed certificate

- File name: A10Lab
- Common name: mail.a10lab.com
- Division: IT
- Organization: IT
- Locality: San Jose
- State: CA
- Country: United States
- Valid Days: 1825
- Key Size: 2048

***NOTE**: Thunder ADC supports 1024, 2048 and 4096 bit SSL keys. The higher bit SSL key size, the more CPU processing will be required. The Thunder ADC SSL models handle the SSL transaction in hardware.*

- Click Save

# THUNDER ADC EXCHANGE CONFIGURATION USING APPCENTRIC TEMPLATES

## APPCENTRIC TEMPLATES (ACT) OVERVIEW

ACT is a wizard-based configuration tool that enables organizations to apply best practices to deploying and securing their Exchange 2016 solution with minimal effort. A10 highly recommends the use of this configuration tool for the deployment and management of Exchange 2016, since these templates were developed with a focus on best practices. For that reason, most of the subsequent points can be easily configured via AppCentric Templates.

Refer to Appendix B for details on how to acquire and import the ACT file.

## CONFIGURATION USING ACT

To access ACT, first log into Thunder ADC using the web GUI:

- IP address: Management IP address
- Default username: “admin”
- Default password: “a10”

Go to System > App Templates

If prompted to specify username and password, log into ACT using your regular admin credentials:

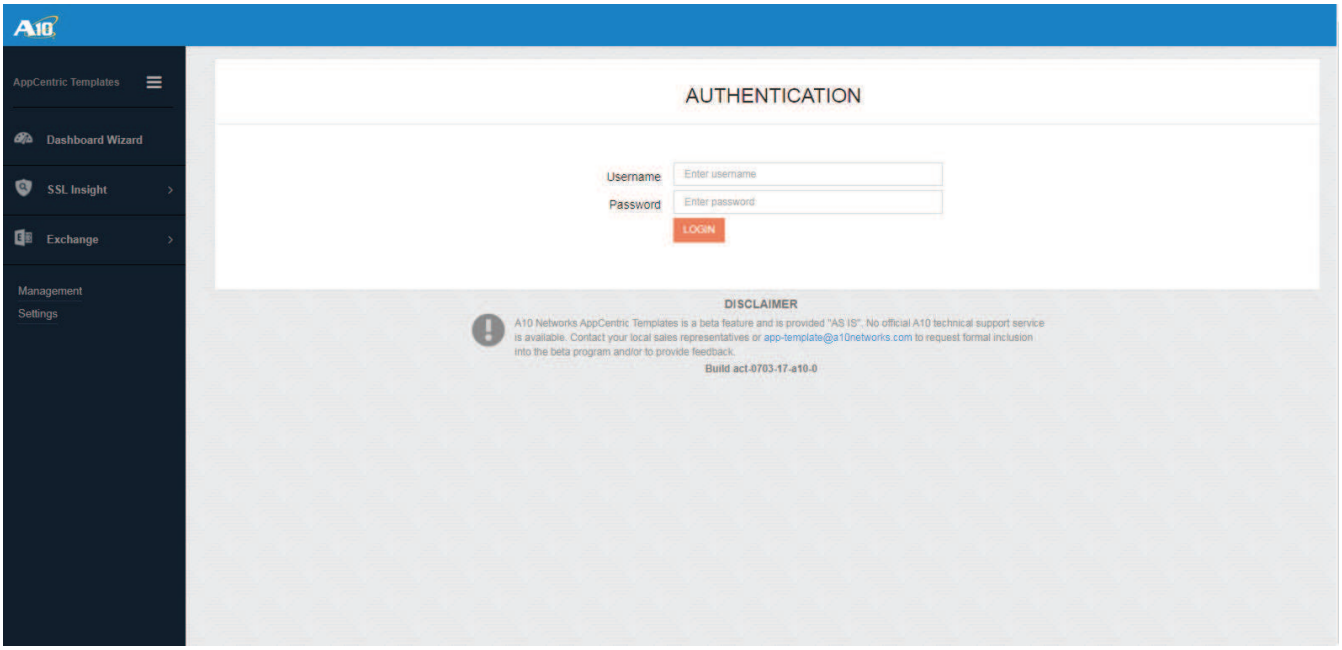



**Figure 11:** Logging into ACT

Once you've logged into ACT, select Exchange from the AppCentric Templates menu.

There are three main sections in the Exchange AppCentric Templates:

1. **Dashboard**: The dashboard gives users a view of different statistics related to the current state of the system, including traffic statistics.
2. **Wizard**: The wizard provides users with a guided flow for deployment of Exchange 2016 with Thunder ADC.
3. **Configuration**: This section provides users with the current configuration of the device as well as access to some advanced options.

## WIZARD – TOPOLOGY

In the left-pane, go to Exchange > Wizard

Depending on the mode of deployment, select either Source-NAT or Inline:

- In this deployment we've used the Inline deployment mode.

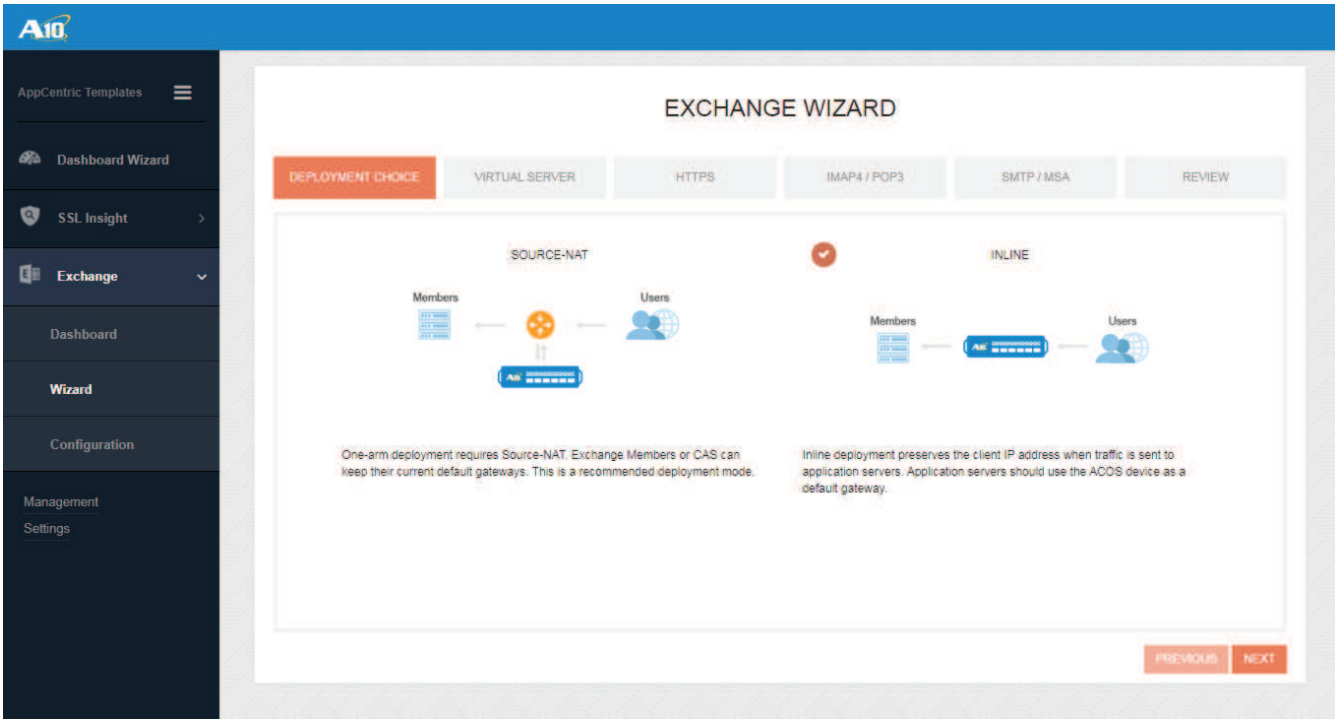



**Figure 12:** Select the topology: Source-NAT vs. Inline

## WIZARD – VIRTUAL SERVER

**Partition**: Thunder ADC supports multitenancy using Active Delivery Partitions (ADP). Every ACOS device has a shared partition, and by default, your configuration is run in this shared partition. Here we select the default shared partition.

**VIP**: 198.51.100.74

This is the public IP address that will be used by the clients to access Exchange services.

**Members**: 10.1.0.211 and 10.1.0.212

These are the real IP addresses of the Exchange (Mailbox) servers.

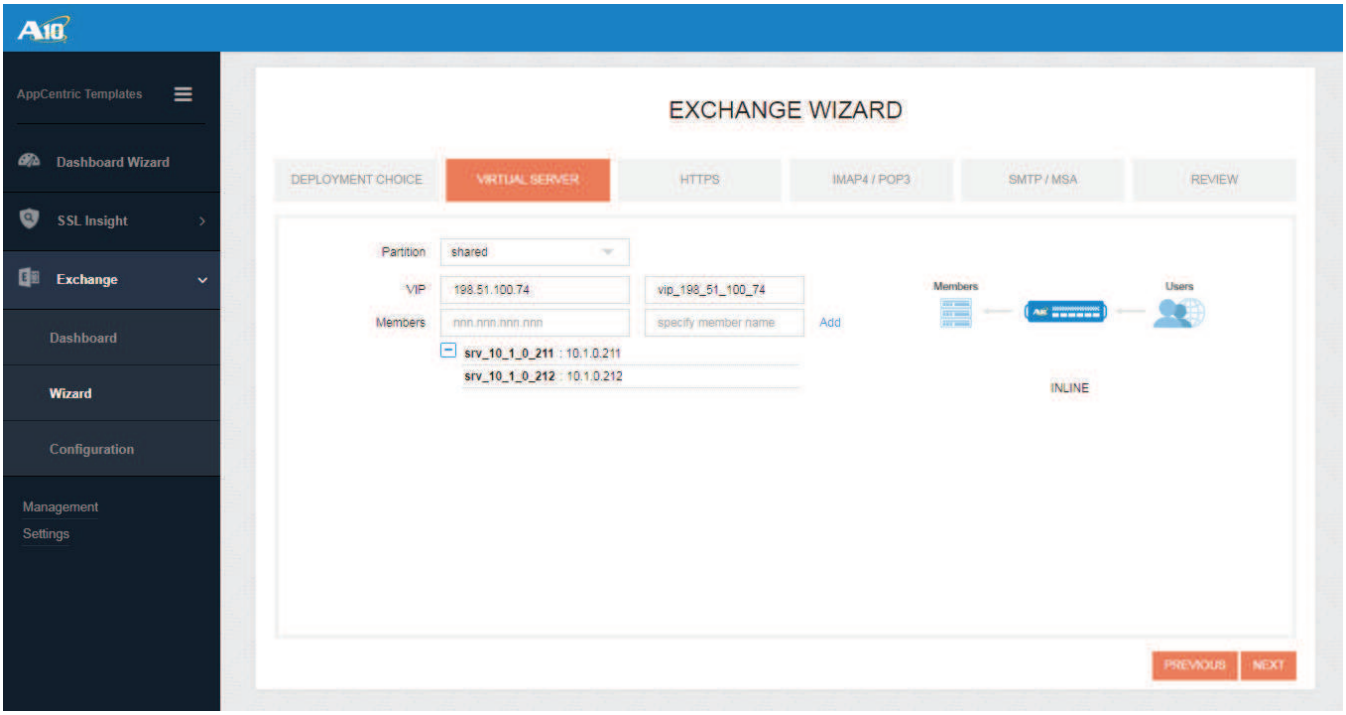



**Figure 13:** Specify VIP and real server IP addresses

## *WIZARD – HTTPS*

**SSL Mode**: SSL Offload

SSL Offload acts as an acceleration feature by removing the burden of processing SSL traffic from the Exchange Servers. Instead of having Exchange Servers handling the SSL processing, Thunder ADC decrypts and encrypts all HTTPS traffic, forwarding the traffic to the server over HTTP (unsecured).

**SSL Certificate/Key**: A10Lab (self-signed certificate/key generated earlier)

This is the certificate and key that will be used for securing the traffic between the client and Thunder ADC.

**Certificate Chain**: Depends on the certificate; not required in this example.

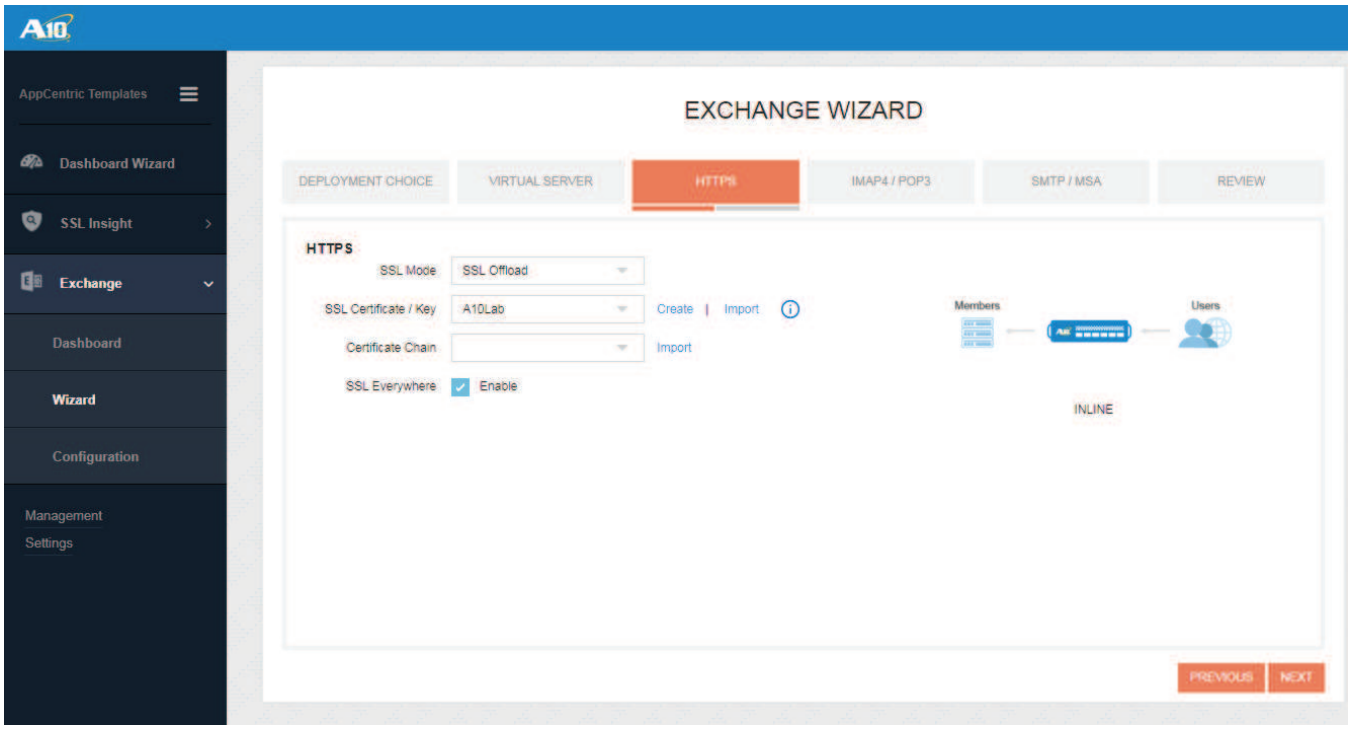



**Figure 14:** Enable SSL Offload and specify the certificate/key for encrypted traffic between the clients and Thunder ADC

SSL Everywhere: Set to Enable

This will configure the following recommended security features:

- HTTP-to-HTTPS redirection
- HTTP Strict Transport Security (HSTS)
- Perfect Forward Secrecy (PFS) cipher suites will be preferred

Click NEXT

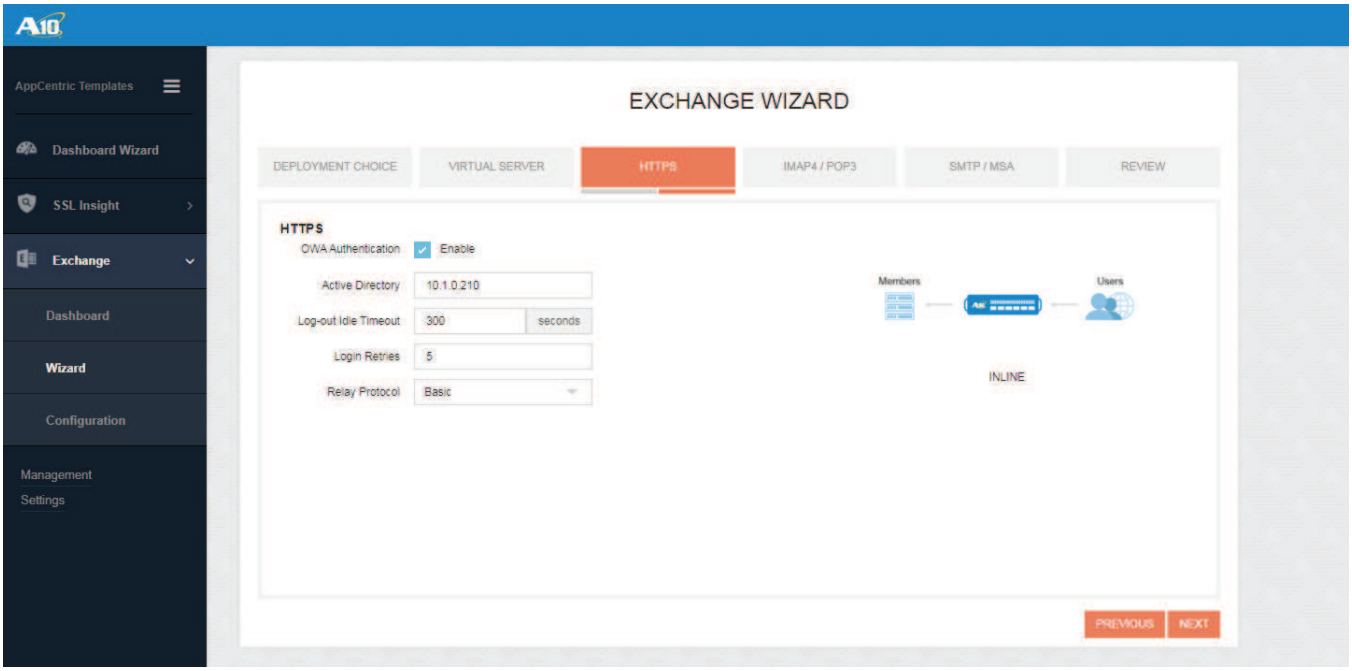



**Figure 15:** Enable OWA authentication

**OWA Authentication**: Enable

This will enable OWA authentication to be performed by Thunder ADC. On enabling this option, you will see the related configuration options such as specifying the address of the Active Directory server.

**Active Directory**: 10.1.0.210

If you enable the option of OWA Authentication, you need to additionally specify the address of Active Directory server.

**Relay Protocol**: Basic or NTLM

Specify the relay protocol to be used between Thunder ADC and the Exchange Servers.

## *WIZARD – IMAP4/POP3*

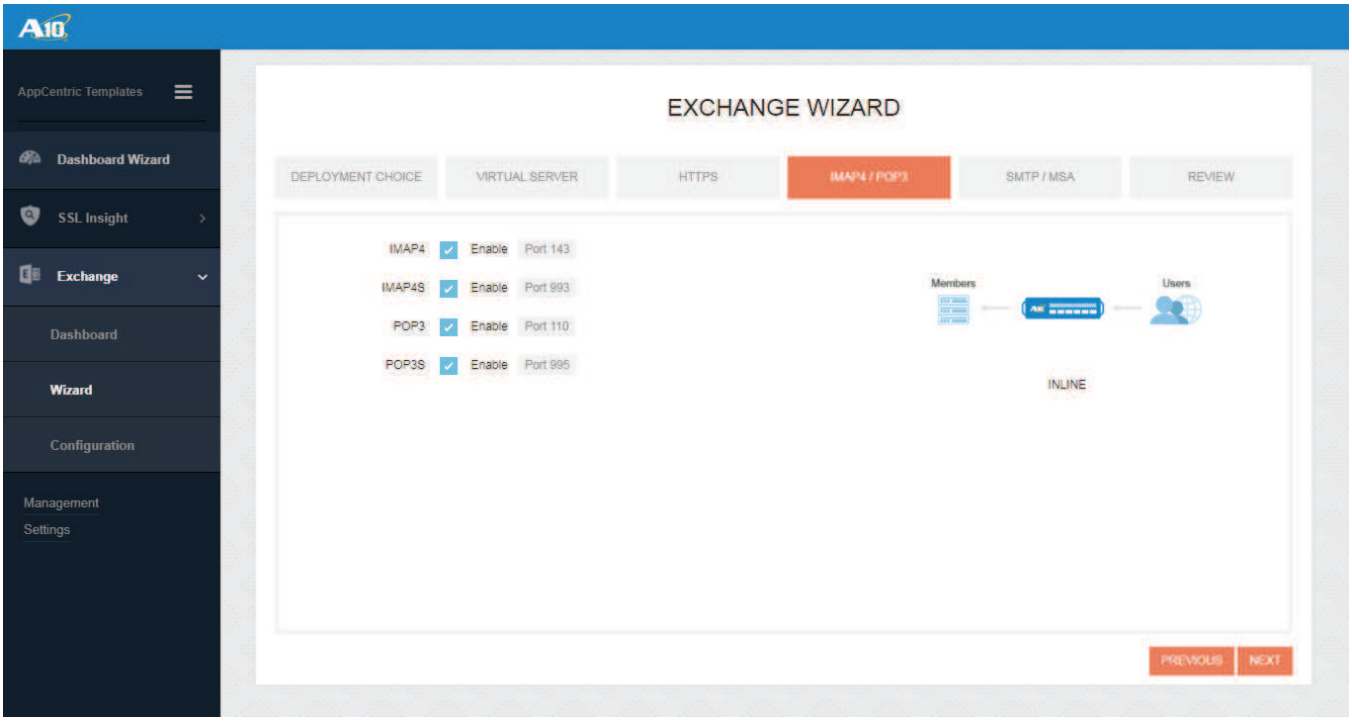



**Figure 16:** Enabling POP3/IMAP4

To enable support for POP3 and/or IMAP4 protocols, select the corresponding Enable option.

## *WIZARD – SMTP*

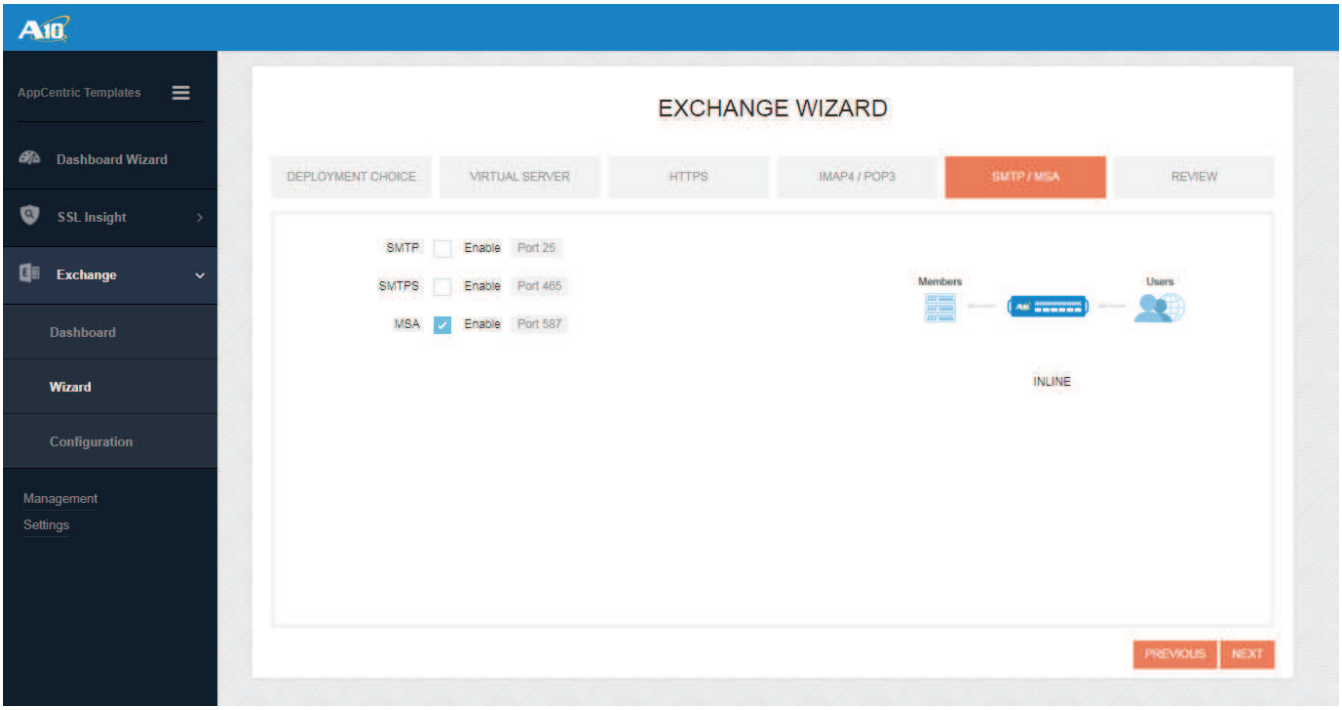



**Figure 17:** Enable SMTP on port 587

MSA: Enable

This should be the same as the setting on the Exchange Server. On Exchange Server, the default Receive connector named "Client Frontend <Server name>" in the Client Access services on the Mailbox server listens for authenticated SMTP client submissions on port 587.

The use of STARTTLS for SMTP connections on the client side will be automatically enforced with this setting.

## *WIZARD – REVIEW*

Review the configuration parameters

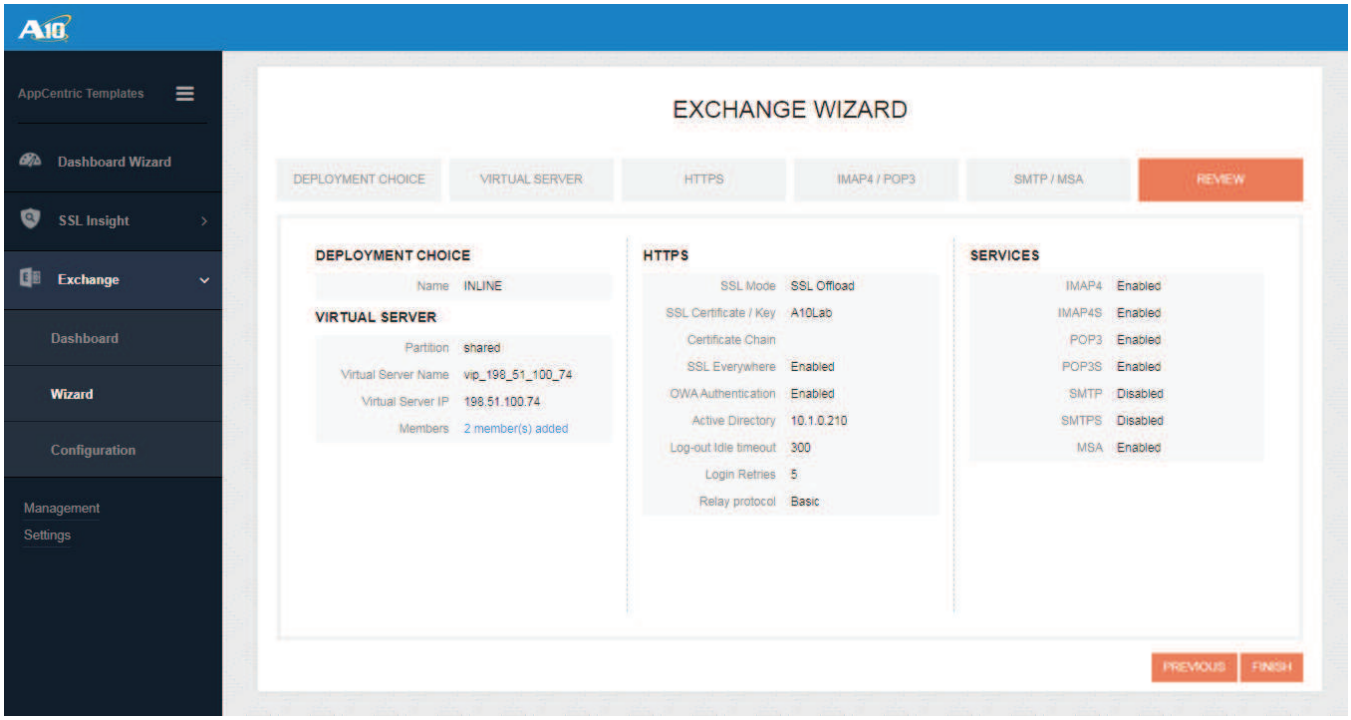



**Figure 18:** Summary of configuration parameters

Click FINISH.

You will then see a popup window with the auto-generated configuration and will be prompted to automatically configure Thunder ADC.

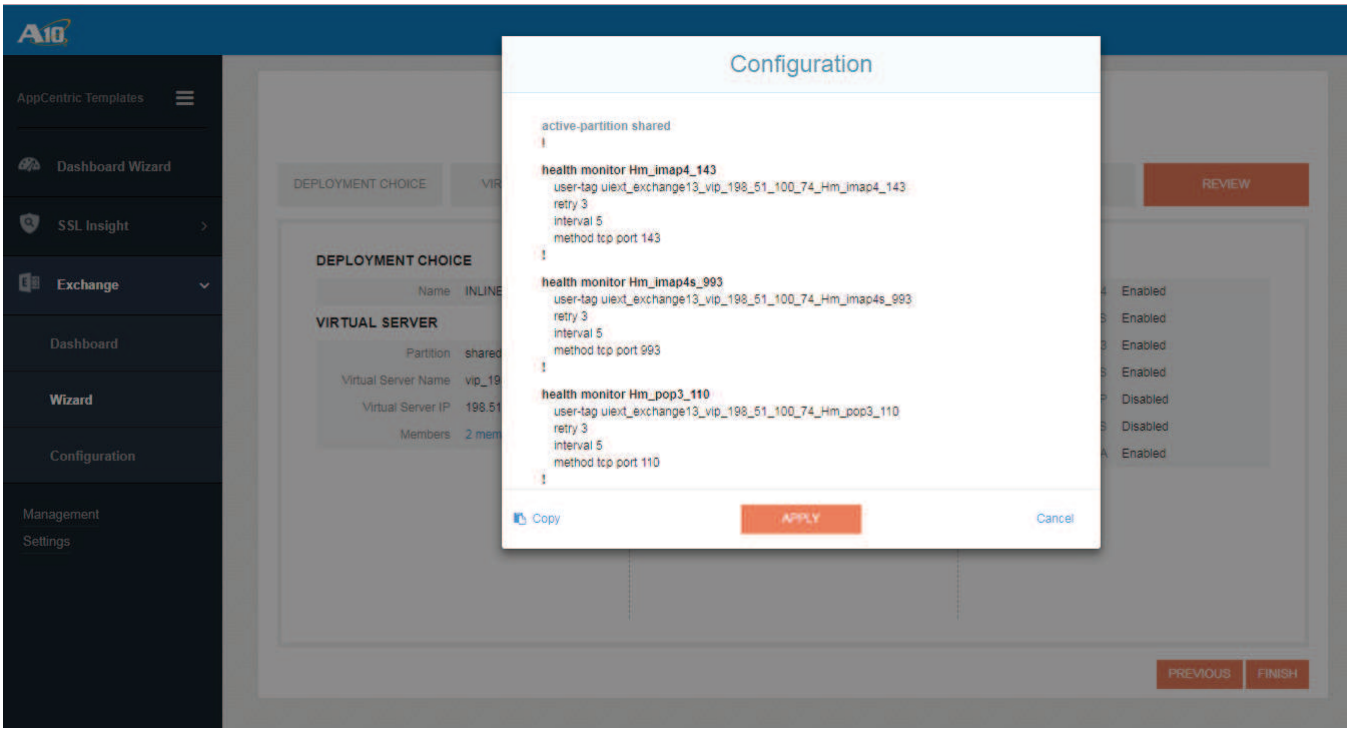



Figure 19: Exchange configuration generated by ACT

You can either click APPLY to activate the setting on the Thunder ADC device, or you can click “Copy” to copy the configuration and then manually apply through the CLI.

To view the complete configuration in text format, refer to Appendix A.

Once it’s applied, you can go to the Exchange > Configuration page to look at the current configuration applied to the Thunder ADC device and make any additional changes.

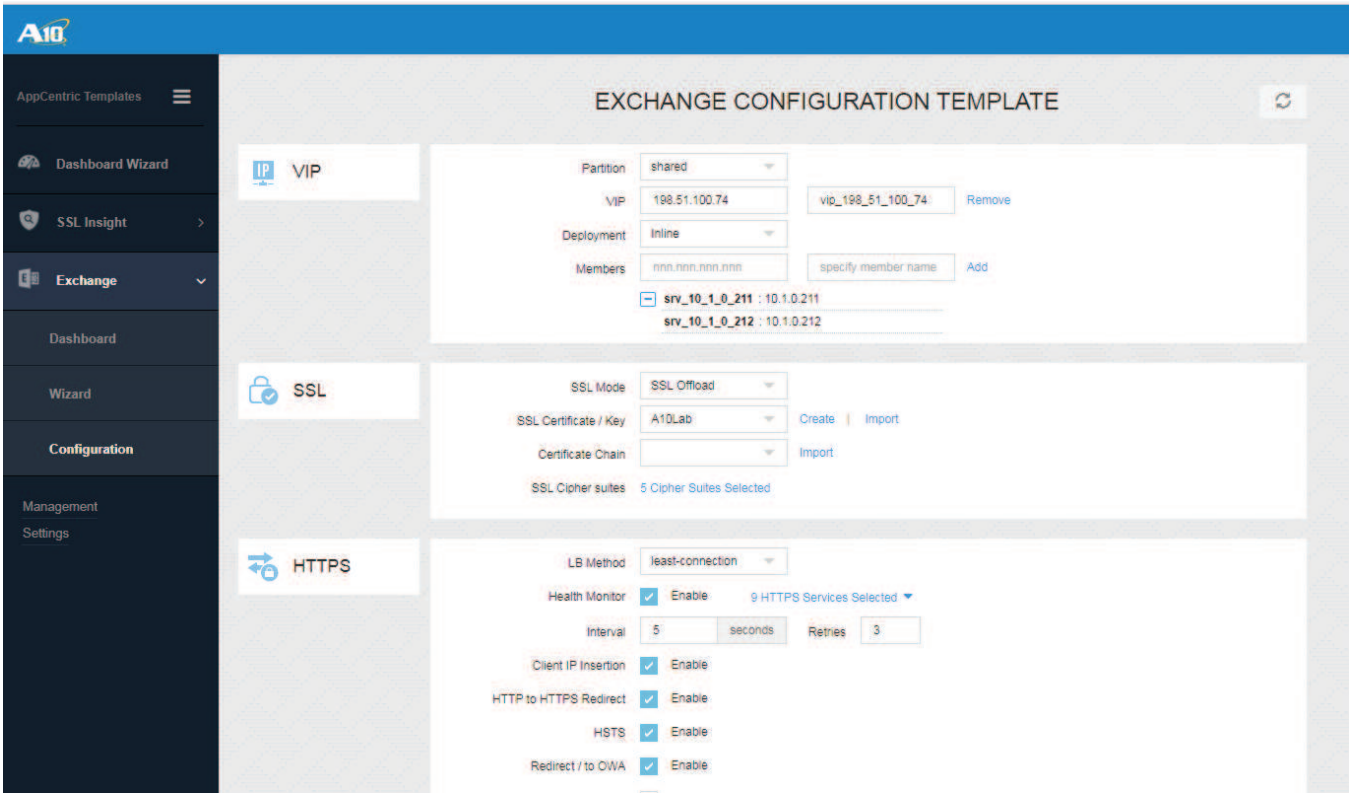



**Figure 20:** Exchange configuration parameters on Thunder ADC

## *EXCHANGE DASHBOARD*

To review the current operational status and traffic analytics for Exchange deployment, go to Exchange > Dashboard.

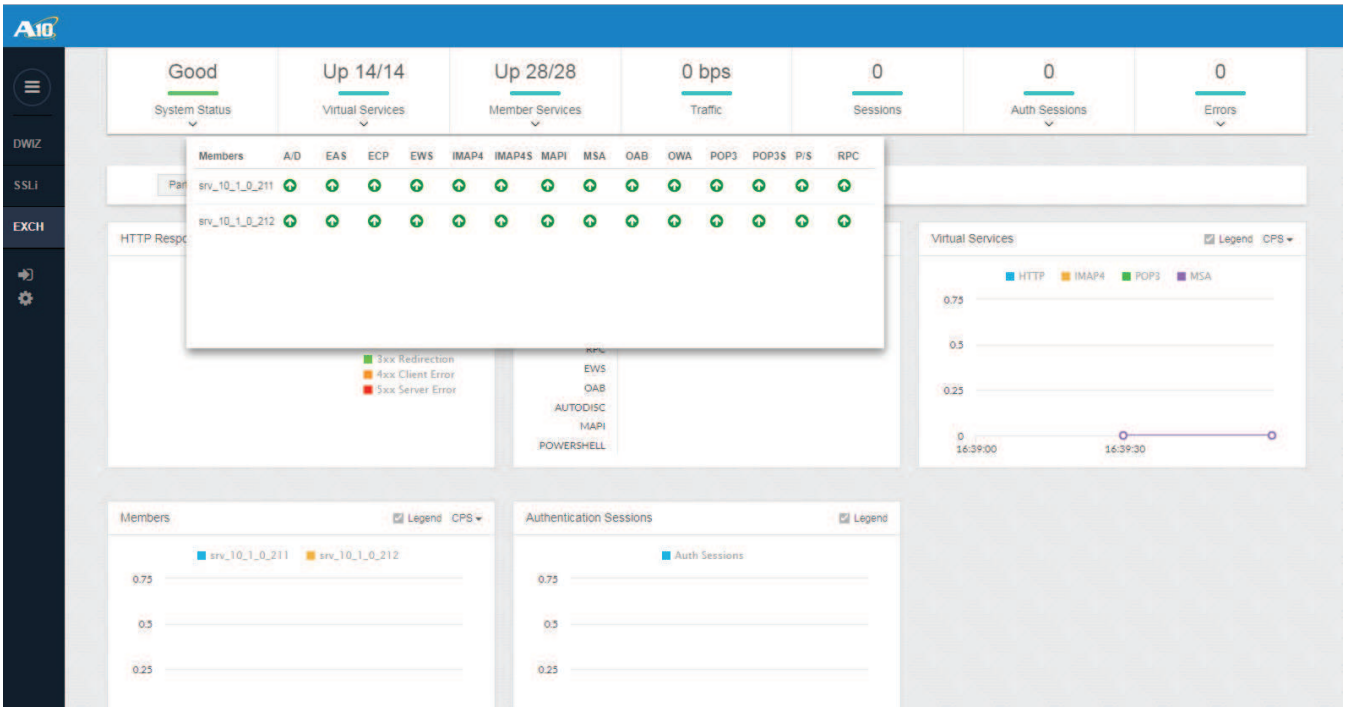



**Figure 21:** Health monitoring status of Exchange services

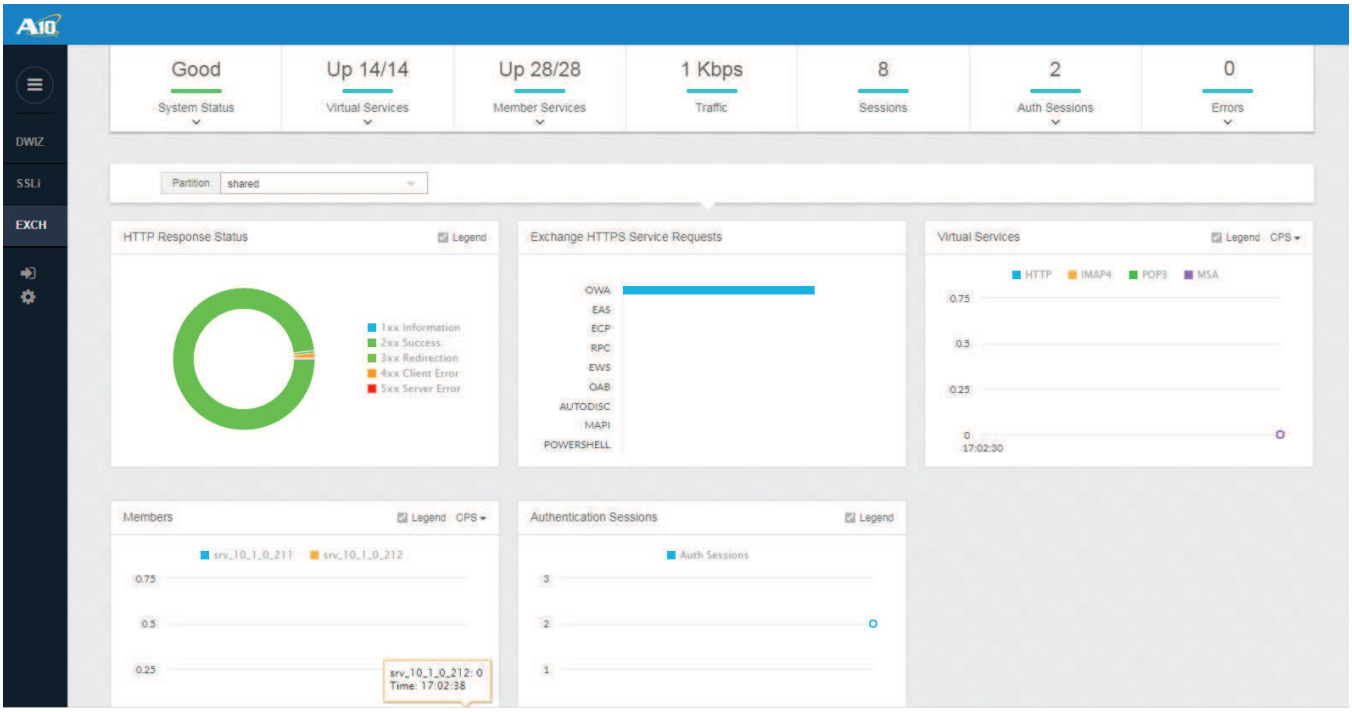



**Figure 22:** Exchange traffic statistics

# *ADDITIONAL SECURITY FEATURE – DDOS MITIGATION (OPTIONAL)*

The following section shows an additional security feature called DDoS Mitigation that can be implemented within the deployed solution.

## *DDOS MITIGATION*

This section describes an additional security feature to protect applications from Distributed Denial of Service (DDoS) attacks.

To configure this feature within the ACOS solution, go to Security > DDoS.

The DDoS protection feature is a global configuration. To enable this feature, select the necessary DDoS attacks you would like to drop. In the figure shown below, we have selected the DDoS attack mitigation required. Once completed, click Update and Save to save the configuration.

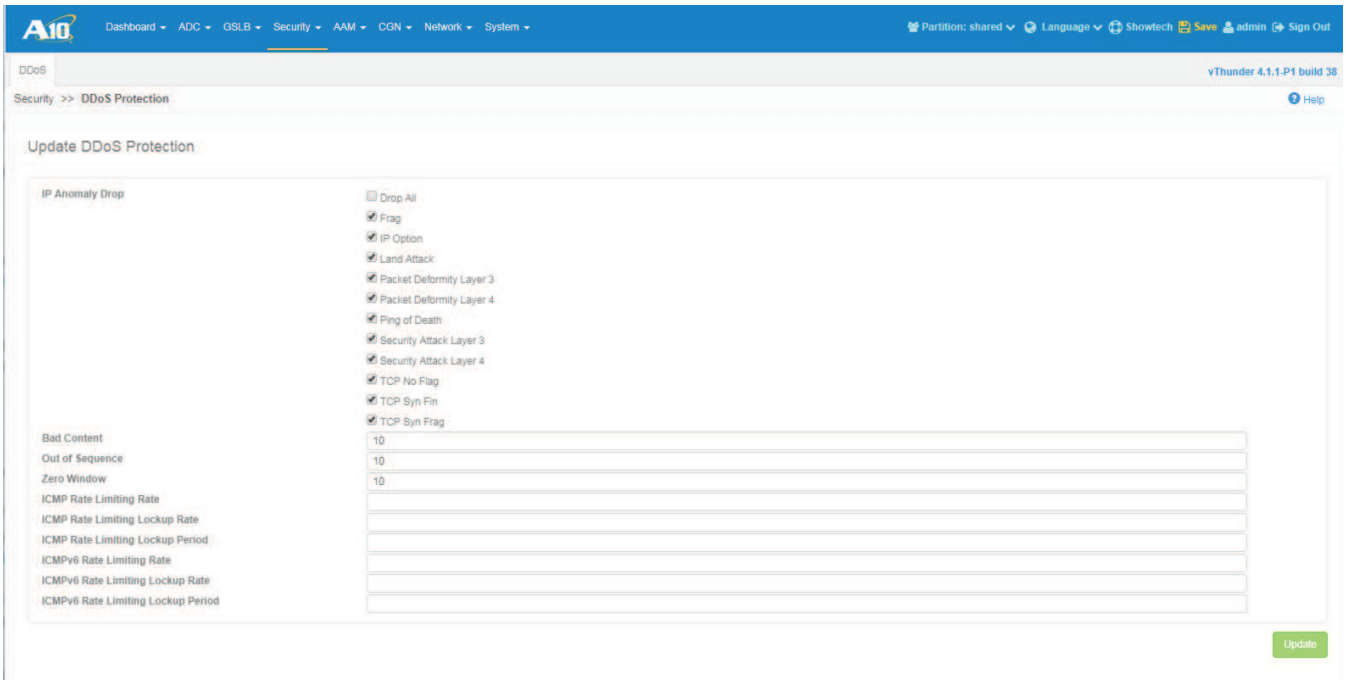



**Figure 23:** DDoS mitigation

The following IP anomaly filters are supported for system-wide Policy-Based Server Load Balancing (PBSLB), although you can also use them without PBSLB:

- Invalid HTTP or SSL payload
- Zero-length TCP window
- Out-of-sequence packet

# *SUMMARY*

This document describes how to configure Thunder ADC as a load balancer to support a Microsoft Exchange 2016 Server deployment using A10 AppCentric Templates. A10 Thunder ADC, powered by ACOS, enhances Microsoft Exchange 2016 by providing the following:

- High availability for Exchange Mailbox servers, ensuring that users can access Exchange services without disruption
- Scalability, as the Thunder ADC device transparently load balances multiple Exchange Mailbox servers
- Higher connection throughput to enhance end user experience
- Improved server performance due to server optimizations such as SSL Offload
- Highest levels of security with PFS ciphers, HSTS and HTTP-to-HTTPS redirection
- Protection against DDoS attacks using integrated DDoS protection capabilities
- Protection against web application attacks through Web Application Firewall (WAF)
- Ease of deployment with AppCentric Templates

For more information about A10 Thunder ADC products, please refer to:

https://www.a10networks.com/products/thunder-series/thunder-application_delivery_controller

https://www.a10networks.com/resources/solution-briefs

https://www.a10networks.com/resources/case-studies

# APPENDIX A – THUNDER ADC TEST CONFIGURATION

Here is the Thunder ADC configuration used in an actual test environment.

```
ip anomaly-drop packet-deformity layer-3
ip anomaly-drop packet-deformity layer-4
ip anomaly-drop security-attack layer-3
ip anomaly-drop security-attack layer-4
ip anomaly-drop bad-content 10
ip anomaly-drop frag
ip anomaly-drop ip-option
ip anomaly-drop land-attack
ip anomaly-drop ping-of-death
ip anomaly-drop tcp-no-flag
ip anomaly-drop tcp-syn-fin
ip anomaly-drop tcp-syn-frag
!
vlan 103
  untagged ethernet 2
  router-interface ve 103
!
vlan 105
  untagged ethernet 4
  router-interface ve 105
!
interface management
  ip address 10.100.2.188 255.255.255.0
  ip default-gateway 10.100.2.1
!
interface ethernet 1
!
interface ethernet 2
  enable
!
interface ethernet 3
!
interface ethernet 4
  enable
!
interface ve 103
  ip address 10.1.0.1 255.255.255.0
!
interface ve 105
  ip address 198.51.100.1 255.255.255.0
!
!
ip route 203.0.113.0 /24 198.51.100.254
!
aam authentication logon form-based owa_
logon_form_vip_198_51_100_74
  portal _act_owa_portal logon logon.html
failpage lockout.html changepasswordpage
pwdchange.html
  action-url /logon.fo
  username-variable username
  password-variable pwd
  retry 5
  user-tag uiext_exchange13_owa_logon_form_
vip_198_51_100_74
!
!
aam authentication server windows ad_auth_
server_vip_198_51_100_74
  host 10.1.0.210
  auth-protocol kerberos-disable
!
aam authentication relay http-basic Basic_
relay_vip_198_51_100_74
!
aam authentication template Owa_templ_
vip_198_51_100_74
  logon owa_logon_form_vip_198_51_100_74
  relay Basic_relay_vip_198_51_100_74
  server ad_auth_server_vip_198_51_100_74
  user-tag uiext_exchange13_Owa_templ_
vip_198_51_100_74
!
aam aaa-policy Owa_aaa_policy_
vip_198_51_100_74
  user-tag uiext_exchange13_Owa_aaa_policy_
vip_198_51_100_74
  aaa-rule 1
```

```
    uri starts-with /owa
    action allow
    authentication-template Owa_templ_
vip_198_51_100_74
!
slb common
  enable-l7-req-acct
!
health monitor Hm_imap4_143
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_imap4_143
  method tcp port 143
!
health monitor Hm_imap4s_993
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_imap4s_993
  method tcp port 993
!
health monitor Hm_pop3_110
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_pop3_110
  method tcp port 110
!
health monitor Hm_pop3s_995
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_pop3s_995
  method tcp port 995
!
health monitor Hm_msa_587
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_msa_587
  method tcp port 587
!
health monitor Hm_owa_80
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_owa_80
  method http url GET /owa/healthcheck.htm
!
health monitor Hm_eas_80
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_eas_80
  method http url GET /Microsoft-Server-
ActiveSync/healthcheck.htm
!
health monitor Hm_ecp_80
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_ecp_80
  method http url GET /ecp/healthcheck.htm
!
health monitor Hm_rpc_80
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_rpc_80
  method http url GET /rpc/healthcheck.htm
!
health monitor Hm_ews_80
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_ews_80
  method http url GET /ews/healthcheck.htm
!
health monitor Hm_oab_80
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_oab_80
  method http url GET /oab/healthcheck.htm
!
health monitor Hm_autodisc_80
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_autodisc_80
  method http url GET /autodiscover/
healthcheck.htm
!
health monitor Hm_mapi_80
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_mapi_80
  method http url GET /mapi/healthcheck.
htm
!
health monitor Hm_powershell_80
  user-tag uiext_exchange13_
vip_198_51_100_74_Hm_powershell_80
  method http url GET /powershell/
healthcheck.htm
!
slb template cipher Ccipher_
vip_198_51_100_74
  TLS1_RSA_AES_128_SHA
  TLS1_RSA_AES_256_SHA
  TLS1_ECDHE_RSA_AES_128_SHA priority 10
  TLS1_ECDHE_RSA_AES_256_SHA priority 10
  TLS1_ECDHE_RSA_AES_128_SHA256 priority
```

```
10
  user-tag uiext_exchange13_Ccipher_
vip_198_51_100_74
!
slb server srv_10_1_0_211 10.1.0.211
  user-tag uiext_exchange13_
vip_198_51_100_74_srv_10_1_0_211
  sampling-enable total-conn
  port 80 tcp
    user-tag uiext_exchange13_
vip_198_51_100_74_srv_10_1_0_211_80
  port 110 tcp
    user-tag uiext_exchange13_
vip_198_51_100_74_srv_10_1_0_211_110
  port 143 tcp
    user-tag uiext_exchange13_
vip_198_51_100_74_srv_10_1_0_211_143
  port 443 tcp
    user-tag uiext_exchange13_
vip_198_51_100_74_srv_10_1_0_211_443
  port 587 tcp
    user-tag uiext_exchange13_
vip_198_51_100_74_srv_10_1_0_211_587
!
slb server srv_10_1_0_212 10.1.0.212
  user-tag uiext_exchange13_
vip_198_51_100_74_srv_10_1_0_212
  sampling-enable total-conn
  port 80 tcp
    user-tag uiext_exchange13_
vip_198_51_100_74_srv_10_1_0_212_80
  port 110 tcp
    user-tag uiext_exchange13_
vip_198_51_100_74_srv_10_1_0_212_110
  port 143 tcp
    user-tag uiext_exchange13_
vip_198_51_100_74_srv_10_1_0_212_143
  port 443 tcp
    user-tag uiext_exchange13_
vip_198_51_100_74_srv_10_1_0_212_443
  port 587 tcp
    user-tag uiext_exchange13_
vip_198_51_100_74_srv_10_1_0_212_587
!
slb service-group autodisc_80_sg tcp
  method least-connection
  health-check Hm_autodisc_80
  user-tag uiext_exchange13_autodisc_80_sg
  member srv_10_1_0_211 80
  member srv_10_1_0_212 80
!
slb service-group eas_80_sg tcp
  method least-connection
  health-check Hm_eas_80
  user-tag uiext_exchange13_eas_80_sg
  member srv_10_1_0_211 80
  member srv_10_1_0_212 80
!
slb service-group ecp_80_sg tcp
  method least-connection
  health-check Hm_ecp_80
  user-tag uiext_exchange13_ecp_80_sg
  member srv_10_1_0_211 80
  member srv_10_1_0_212 80
!
slb service-group ews_80_sg tcp
  method least-connection
  health-check Hm_ews_80
  user-tag uiext_exchange13_ews_80_sg
  member srv_10_1_0_211 80
  member srv_10_1_0_212 80
!
slb service-group imap4_143_sg tcp
  method least-connection
  health-check Hm_imap4_143
  user-tag uiext_exchange13_imap4_143_sg
  member srv_10_1_0_211 143
  member srv_10_1_0_212 143
!
slb service-group imap4s_993_sg tcp
  method least-connection
  health-check Hm_imap4s_993
  user-tag uiext_exchange13_imap4s_993_sg
  member srv_10_1_0_211 143
  member srv_10_1_0_212 143
```

```
!
slb service-group mapi_80_sg tcp
  method least-connection
  health-check Hm_mapi_80
  user-tag uiext_exchange13_mapi_80_sg
  member srv_10_1_0_211 80
  member srv_10_1_0_212 80
!
slb service-group msa_587_sg tcp
  method least-connection
  health-check Hm_msa_587
  user-tag uiext_exchange13_msa_587_sg
  member srv_10_1_0_211 587
  member srv_10_1_0_212 587
!
slb service-group oab_80_sg tcp
  method least-connection
  health-check Hm_oab_80
  user-tag uiext_exchange13_oab_80_sg
  member srv_10_1_0_211 80
  member srv_10_1_0_212 80
!
slb service-group owa_80_sg tcp
  method least-connection
  health-check Hm_owa_80
  user-tag uiext_exchange13_owa_80_sg
  member srv_10_1_0_211 80
  member srv_10_1_0_212 80
!
slb service-group pop3_110_sg tcp
  method least-connection
  health-check Hm_pop3_110
  user-tag uiext_exchange13_pop3_110_sg
  member srv_10_1_0_211 110
  member srv_10_1_0_212 110
!
slb service-group pop3s_995_sg tcp
  method least-connection
  health-check Hm_pop3s_995
  user-tag uiext_exchange13_pop3s_995_sg
  member srv_10_1_0_211 110
  member srv_10_1_0_212 110
!
slb service-group powershell_80_sg tcp
  method least-connection
  health-check Hm_powershell_80
  user-tag uiext_exchange13_powershell_80_
sg
  member srv_10_1_0_211 80
  member srv_10_1_0_212 80
!
slb service-group rpc_80_sg tcp
  method least-connection
  health-check Hm_rpc_80
  user-tag uiext_exchange13_rpc_80_sg
  member srv_10_1_0_211 80
  member srv_10_1_0_212 80
!
slb template client-ssl Cssl_
vip_198_51_100_74
  template cipher Ccipher_
vip_198_51_100_74
  cert A10Lab
  enable-tls-alert-logging fatal
  key A10Lab
  disable-sslv3
  user-tag uiext_exchange13_Cssl_
vip_198_51_100_74
!
slb template http Url_sw_http_tmpl
  insert-client-ip
  response-header-insert strict-transport-
security:max-age=31536000
  url-switching url-case-insensitive
  url-switching url-hits-enable
  url-switching starts-with /owa service-
group owa_80_sg
  url-switching starts-with /eas service-
group eas_80_sg
  url-switching starts-with /ecp service-
group ecp_80_sg
  url-switching starts-with /rpc service-
group rpc_80_sg
  url-switching starts-with /ews service-
```

```
group ews_80_sg

  url-switching starts-with /oab service-
group oab_80_sg

  url-switching starts-with /autodisc
service-group autodisc_80_sg

  url-switching starts-with /mapi
service-group mapi_80_sg

  url-switching starts-with /powershell
service-group powershell_80_sg

  user-tag uiext_
exchange13vip_198_51_100_74_443

!

slb template smtp smtp_tmpl_
vip_198_51_100_74

  starttls client enforced

  user-tag uiext_exchange13_smtp_tmpl_
vip_198_51_100_74

!

slb virtual-server vip_198_51_100_74
198.51.100.74

  user-tag uiext_exchange13_
vip_198_51_100_74_virtualserver

  port 80 http

    service-group powershell_80_sg

    redirect-to-https

    user-tag uiext_exchange13_
vip_198_51_100_74_80_http

    sampling-enable total_conn

    sampling-enable total_fwd_bytes

    sampling-enable total_rev_bytes

  port 110 pop3

    service-group pop3_110_sg

    user-tag uiext_exchange13_
vip_198_51_100_74_110_pop3

    sampling-enable total_conn

    sampling-enable total_fwd_bytes

    sampling-enable total_rev_bytes

  port 143 imap

    service-group imap4_143_sg

    user-tag uiext_exchange13_
vip_198_51_100_74_143_imap

    sampling-enable total_conn

    sampling-enable total_fwd_bytes

    sampling-enable total_rev_bytes

  port 443 https

    aflex redirect_to_owa

    service-group powershell_80_sg

    template http Url_sw_http_tmpl

    template client-ssl Cssl_
vip_198_51_100_74

    aaa-policy Owa_aaa_policy_
vip_198_51_100_74

    user-tag uiext_exchange13_
vip_198_51_100_74_443_https

    sampling-enable total_conn

    sampling-enable total_fwd_bytes

    sampling-enable total_rev_bytes

  port 587 smtp

    service-group msa_587_sg

    template smtp smtp_tmpl_
vip_198_51_100_74

    template client-ssl Cssl_
vip_198_51_100_74

    user-tag uiext_exchange13_
vip_198_51_100_74_587_smtp

    sampling-enable total_conn

    sampling-enable total_fwd_bytes

    sampling-enable total_rev_bytes

  port 993 ssl-proxy

    service-group imap4s_993_sg

    template client-ssl Cssl_
vip_198_51_100_74

    user-tag uiext_exchange13_
vip_198_51_100_74_993_ssl-proxy

    sampling-enable total_conn

    sampling-enable total_fwd_bytes

    sampling-enable total_rev_bytes

  port 995 ssl-proxy

    service-group pop3s_995_sg

    template client-ssl Cssl_
vip_198_51_100_74

    user-tag uiext_exchange13_
vip_198_51_100_74_995_ssl-proxy

    sampling-enable total_conn

    sampling-enable total_fwd_bytes

    sampling-enable total_rev_bytes

!

end
```

# APPENDIX B – APPCENTRIC TEMPLATES UPGRADE

To upgrade ACT to the latest version, one of the following two methods can be used:

## UPGRADING ACT USING CLOUD-BASED UPDATE

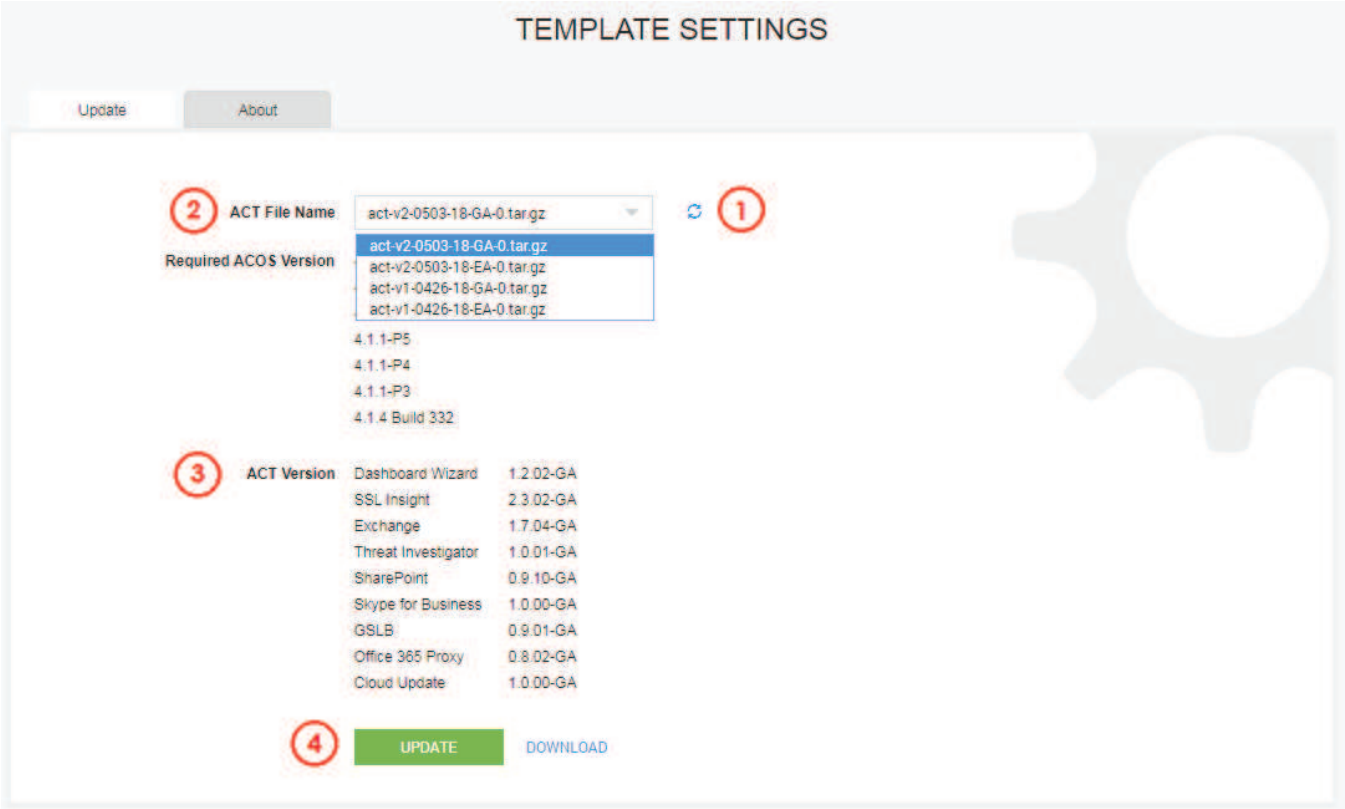
ACT can be upgraded to the latest version directly from the cloud.

To do so, login to ACOS GUI and navigate to **System > App Template**. This will take you to the current version of ACT available on your device. If prompted, login to ACT using your ACOS credentials.

From the landing page, navigate to the **Settings** page.

> ***NOTE***: *Depending on the ACT version you are currently using, you will either find the Settings link on the left pane or as a gear icon in the top right corner of the screen.*

1. Under the **Update** tab on the **Settings** page, click on the refresh icon next to "ACT File Name" dropdown menu.




2. Select the desired ACT build from the dropdown menu and verify that your ACOS version is listed below for compatibility.
3. Also make sure that the Application for which you want to upgrade ACT is included in the build.
4. Click **Update**.

> ***NOTE***: *You can find the current version of ACT running on your device by navigating to the **About** tab on the **Settings** page.*

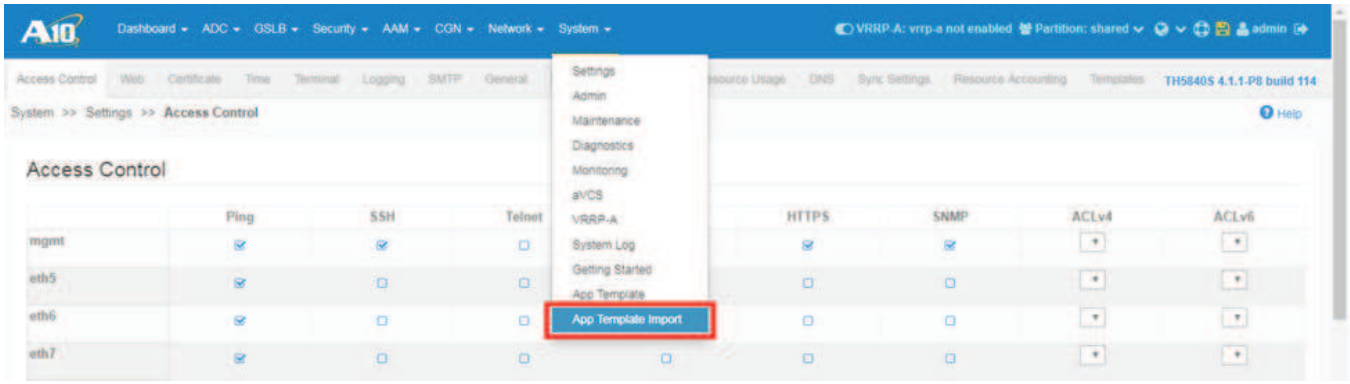
## UPGRADING ACT USING MANUAL UPDATE

If your current ACT version does not support cloud-based updates, you can use the manual update option to upgrade to an intermediary version that does support cloud-based updates. You can then update to your desired ACT version using the steps mentioned above.

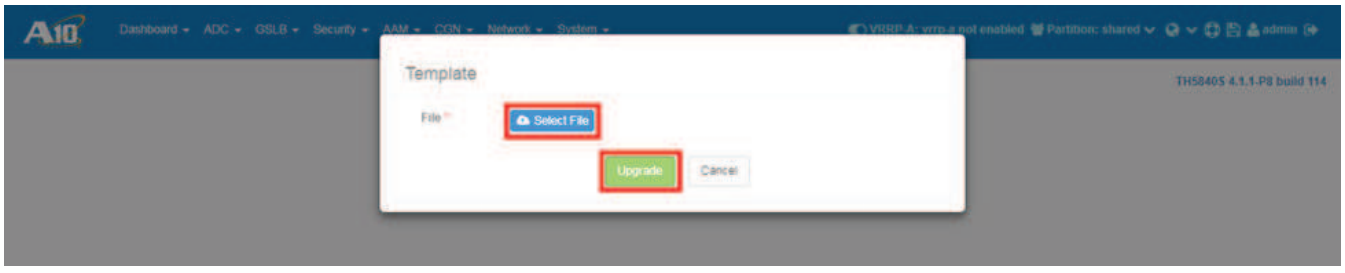
The intermediary ACT version can be downloaded as a tar.gz file to your computer from this link or by navigating to the **More** section of the **A10 Networks Support Portal**. Make sure that the package is not decompressed.


***NOTE**: This ACT version requires your device to be upgraded to ACOS version 4.1.1-P3 or later.*

To start, login to ACOS GUI and navigate to **System > App Template Import**.




The following pop-up will appear:




- Click **Select File** and browse to the package downloaded earlier.
- Click **Upgrade**.

***NOTE**: At this point, wait patiently and do not close the window or interrupt the upgrade process in any way.*

Once successfully upgraded, either click on the **Jump Now!** link that appears in the popup, or navigate to **System > App Template** from the ACOS GUI.

***NOTE**: In rare cases, after updating the ACT, you might experience that the ACT isn't loading. In such a scenario, logout from the ACOS GUI, and clear any cookies from the browser that are related to the A10 GUI or ACT. Alternatively, you can also clear the whole browser cache and then launch ACT.*

## *ABOUT A10 NETWORKS*

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com or tweet @a10Networks

## *LEARN MORE*

ABOUT A10 NETWORKS

### *CONTACT US*

a10networks.com/contact

©2018 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, A10 Lightning, A10 Harmony and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/a10-trademarks.

Part Number: A10-DG-16157-EN-06 AUG 2018