

ALOHA for Exchange

Configuration guide

Document version: v 1.0

**Aloha for exchange
version concerned:** v 1.0

Last update date: April, the 04th, 2012



1	Introduction	5
1.1	About Exceliance	5
1.2	About this guide	5
1.3	Appliance supported	5
1.4	Aloha firmware versions supported	5
1.5	Microsoft Exchange version supported	5
1.6	Document history	5
1.7	Disclaimer	6
1.8	Exchange supported architectures	6
2	Introduction to Microsoft Exchange 2010	7
2.1	Exchange 2010 architecture	7
2.2	Client Access Services	8
2.3	SMTP load-balancing.....	8
2.3.1	Using DNS.....	8
2.3.2	Using a load-balancer	8
2.4	Ports and protocols	9
2.5	Server affinity.....	9
2.6	Why using a load-balancer in an Exchange 2010 platform	9
3	Deployment	11
3.1	Virtual appliances.....	11
3.1.1	Virtual hardware requirements:	11
4	Basic Network configuration	12
4.1	Virtual appliance	12
4.1.1	Network configuration at boot prompt.....	13
4.1.2	Network configuration through DHCP.....	13
4.2	Network configuration using the Web User Interface.....	14
4.2.1	Local Network	14
4.2.2	High availability	15
5	Exchange 2010 load-balancing configuration.....	17

5.1	WUI login	17
5.2	Configuration tab	17
5.3	CAS Servers.....	18
5.4	HTTP based Services.....	18
5.4.1	Disabling HTTP based services.....	18
5.4.2	SSL offloading	19
5.4.3	SSL Forwarding	20
5.5	IMAP service.....	21
5.5.1	Clear IMAP service	22
5.5.2	IMAPs service without SSL offloading	22
5.5.3	IMAPs service with SSL offloading.....	23
5.5.4	IMAP and IMAPs service without SSL offloading.....	24
5.5.5	IMAP and IMAPs service with SSL offloading	24
5.6	POP service	26
5.6.1	Clear POP service.....	26
5.6.2	POPs service without SSL offloading	26
5.6.3	POPs service with SSL offloading	27
5.6.4	POP and POPs service without SSL offloading	28
5.6.5	POP3 and POP3s service with SSL offloading	29
5.7	RPC services.....	30
5.7.2	Disabling RPC services	31
5.8	SMTP service	31
5.8.1	Clear SMTP service	31
5.8.2	SMTPs service without SSL offloading	32
5.8.3	SMTPs service with SSL offloading	33
5.8.4	SMTP and SMTPs services without SSL offloading	34
5.8.5	SMTP and SMTPs services with SSL offloading	35
6	Services.....	37
6.1	Services description	37
6.2	Services running status	37

6.3	Services startup status	38
7	Setup tab.....	39
7.1	Information	39
7.2	Configuration.....	39
7.3	Firmware.....	40
7.4	System.....	40
7.5	Licenses	40
8	Microsoft Exchange 2010 procedures.....	41
8.1	Set static TCP Port for MS Exchange RPC Client Access service	41
8.1.1	Procedure for Exchange 2010	41
8.1.2	Procedure for Exchange 2010 SP1 and SP2	41
8.2	Set static TCP Port for MS Exchange Address Book service	41
8.2.1	Procedure for Exchange 2010	41
8.2.2	Procedure for Exchange 2010 SP1 and SP2	42

1 Introduction

1.1 About Exceliance

Exceliance is a software company, editing the Application Delivery Controller named **ALOHA Load-Balancer**.

Headquartered in Jouy-en-Josas (Yvelines, France), Exceliance is part of the EXOSEC group. Whole staff (including R&D and technical support) is based in France.

Exceliance has currently around 100 customers in the banking, retail groups, energy and e-commerce industries and public sector. Exceliance solutions are also used by many hosting providers.

The ALOHA Load-balancer is designed to improve performance, guarantee quality of service and ensure the availability of critical business applications, by dynamically balancing flows and queries on the company's various servers.

1.2 About this guide

This guide first explains in the main lines about how Microsoft Exchange 2010 is designed and why a Load-Balancer makes sense with such platform.

The latest version of this guide can be downloaded from Exceliance website: <http://www.exceliance.fr/>.

1.3 Appliance supported

All ALOHA for exchange appliances can be used with Microsoft Exchange 2010.

1.4 Aloha firmware versions supported

ALOHA for Exchange 1.0 and above are supported to load-Balance Microsoft Exchange 2010.

1.5 Microsoft Exchange version supported

ALOHA for exchange can be used with the following versions of Microsoft Exchange:

- Microsoft exchange 2010
- Microsoft exchange 2010 SP1
- Microsoft exchange 2010 SP2

1.6 Document history

Version	Date	Changes summary
V1.0	April 04th, 2012	Initial release

1.7 Disclaimer

The Exchange 2010 configuration tips provided in this guide are purely informational. For more information about Microsoft Exchange 2010 tools and how to use them, please refer to Microsoft web site which is fully and properly documented.

This guide does not provide information on how to setup an Exchange 2010 CAS array.

1.8 Exchange supported architectures

The ALOHA for Exchange is a load-balancer purposely edited for Microsoft Exchange 2010.

It's fast and easy to setup and can be used in **simple Exchange architectures**, listed below:

- From 2 to 4 CAS servers in the same CAS array
- Exchange 2010 services must be available on all CAS servers
- If SSL offloading is enabled, all the HTTP based services must share the same fqdn

For more complex architectures where ALOHA for Exchange can't be used, then a regular ALOHA Load-Balancer would do the job without any issues.

2 Introduction to Microsoft Exchange 2010

Microsoft Exchange provides businesses with email, calendar and contacts on the PC, phone and web.

One of the most interesting point of Microsoft Exchange 2010 is that you can now dedicates **roles** to servers. This new way of working allows administrators to build redundant platforms, using a load-balancer to allow users to get connected to the services.

Thanks to its new design, Microsoft exchange is now **scalable**.

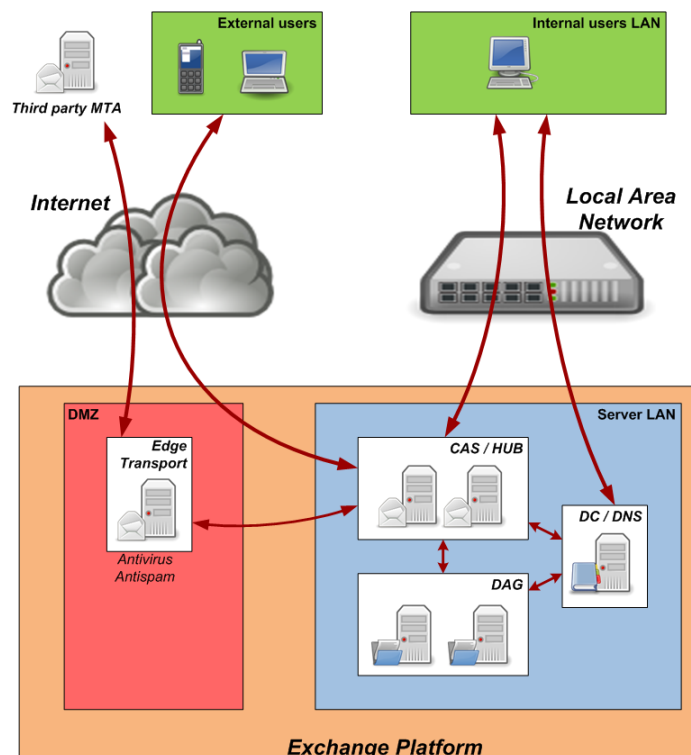
There are 5 roles: Mailbox, Client Access, Hub Transport, Unified Messaging and Edge Transport Server.

Role	Purpose
Client Access	Frontend servers on which client will get connected to access their emails, contacts and agenda
Edge Transport Server	handles the internet facing mail flow, with security features (anti-virus and anti-spam)
Hub Transport	Exchange 2010 mail router, within the organization
Mailbox	Servers hosting mails (in mailboxes) public folders
Unified Messaging	Enables the ability to deliver fax and voicemail to Outlook 2010 clients

The ALOHA for exchange 2010 can balance services from Client Access and Hub Transport.

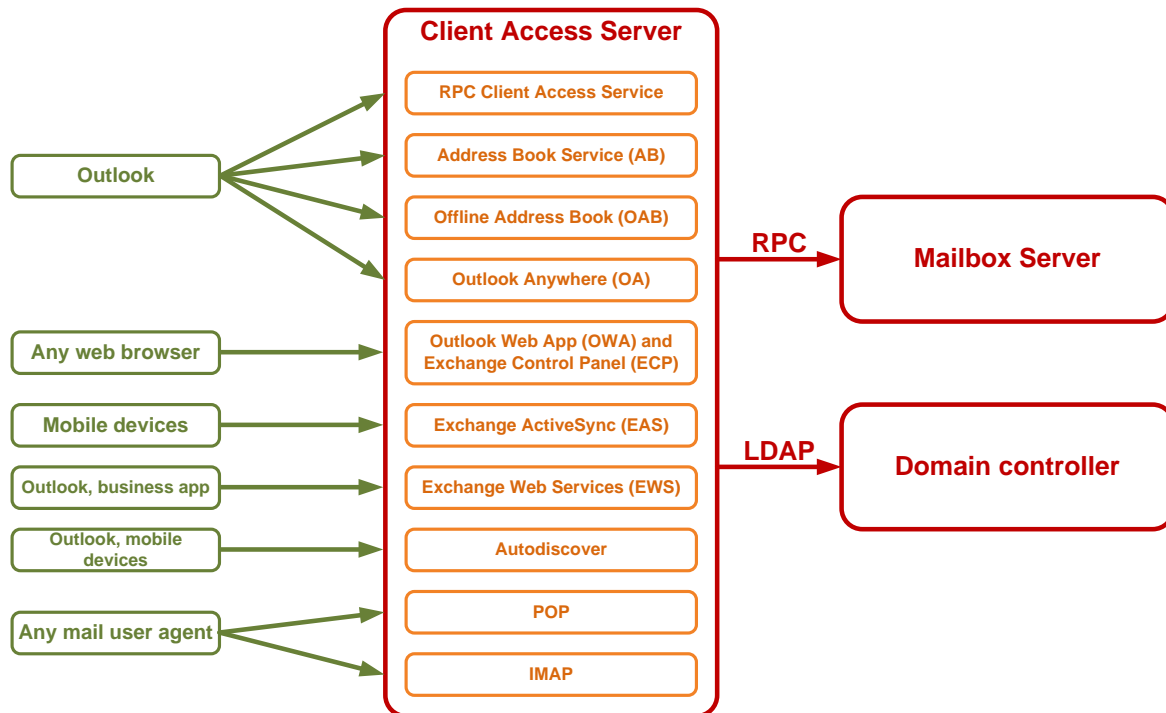
2.1 Exchange 2010 architecture

The diagram below shows how the different roles are used in an Exchange 2010 platform:



2.2 Client Access Services

The diagram below shows the services hosted by the CAS server and the interaction with both Active Directory and mailbox server. It also shows the client type per service.



Basically, the ALOHA for exchange will stand between the **clients** and the **Client Access Servers**.

2.3 SMTP load-balancing

2.3.1 Using DNS

SMTP load-balancing can be achieved by setting up two or more DNS MX (Mail eXchanger) entries, each one pointing to an Exchange HUB server.

A SMTP client would use first the MX record with the lowest preference, then try the next higher preference.

2.3.2 Using a load-balancer

A load-balancer can be used to load-balance SMTP. You need a single MX entry, pointing to the load-balancer.

The load-balancer would balance requests among SMTP servers configured behind it.

Of course, you we can combine both solutions.

2.4 Ports and protocols

The table below summarizes the different ports and protocol involved on the Client Access servers:

TCP port	Protocol	CAS Service
80 and 443	HTTP	<ul style="list-style-type: none"> - Autodiscover (AS) - Exchange ActiveSync (EAS) - Exchange Control Panel (ECP) - Offline Address Book (OAB) - Outlook Anywhere (OA) - Outlook Web App (OWA)
110 and 995	POP3	POP3
135	TCP	RPC EndPoint Mapper (EPM)
143 and 993	IMAP4	IMAP4
60000	TCP	Static port for RPC Client Access Service
60001	TCP	Static port Address Book Service

The static ports for both RPC Client Access and Address Book service are chosen randomly by default. Microsoft recommends that any port within the range 59531 to 60554 should be used, and that the same ports should be used on all Client Access Servers within the same AD site.

Read Chapter 8 of this guide for more details on how to configure static ports on Microsoft Exchange CAS servers.

2.5 Server affinity

Affinity depends on the service. The table below summarizes the affinity requirements per service:

Persistence required	Persistence recommended	No persistence required
Exchange Control Panel (ECP)	Address Book Service (AB)	AutoDiscover (AD)
Exchange Web Service (EWS)	Exchange ActiveSync (EAS)	Offline Address Book (OAB)
Outlook Web App (OWA)	Outlook Anywhere (OA)	POP3
RPC Client Access Service	Remote PowerShell	IMAP4

2.6 Why using a load-balancer in an Exchange 2010 platform

First of all, even if Exchange 2010 provides services arrays, to ensure high-availability, it does not provide any load balancing mechanism.

That mean we need a third party appliance to balance traffic across Client Access Servers and services.

The services that can be load-balanced are the ones hosted by the Client Access Servers as well as SMTP for HUB Transport and Edge Transport Servers.

Using a load-balancer to load-balance Microsoft Exchange 2010 will bring some benefits:

- **Application aware health checking**

A load-balancer provides application layer health check which provides the status of the service itself and are more efficient than a simple ping.

- **Granular persistence methods**

Depending on Exchange service, client software and architecture, different persistence methods can be applied.

- **SSL offloading**

A load-balancer can handle SSL connection for the CAS array servers. That way, CAS servers can focus on their jobs.

- **Scale up**

Building an architecture with a load-balancer allows scale up

- **Scale out**

Splitting services on the load-balancer side, at the cost of more VIP and IP used, brings the ability to scale out the CAS array, dedicating some servers to services.

3 Deployment

3.1 Virtual appliances

The deployment of the Virtual appliance depends on the Hypervisor.

They are packaged to make the deployment easy using tools provided by Hypervisors.

Please read the deployment guide related to your hypervisor for more details.

They are available on Exceliance Web site.

3.1.1 Virtual hardware requirements:

Please find below the minimal and recommended virtual hardware for the Aloha for Exchange Virtual Appliance:

- **Memory:** at least 512m, 1G recommended.
- **vCPU:** if no SSL offloading, 1 is enough, otherwise 2 recommended.
- **Network cards:** 1

4 Basic Network configuration

This chapter explains how to setup the very first network configuration which will allow you to get connected to the Aloha Web User Interface.

4.1 Virtual appliance

When booting with factory settings, the ALOHA for Exchange virtual appliance will **prompt you for 10 seconds** to choose between two types of configuration:

- Network configuration through DHCP
- Setting up manually network configuration



The **default** setting is to use **DHCP**.

Please read chapter "4.1.1 Network configuration at boot prompt".

The picture below shows the prompt:

```
/sbin/cpumask -m 2 /usr/sbin/haproxy -L LOCAL -p /var/run/haproxy.pid -D -q -f
/etc/haproxy/global.def -f /var/state/haproxy.run
==> start haproxy Done.
# Starting stunnel ...
Configuration is empty
==> start stunnel Done.
# Starting collectd ...
/usr/sbin/collectd -C /etc/collectd/collectd.conf -P /var/run/collectd.pid
==> start collectd Done.
# Starting httpd ...
HTTPS enabled
/opt/nginx/bin/nginx -c /var/state/httpd.conf
==> start httpd Done.
# Starting f2cgi ...
sudo -u www -E /opt/f2cgi/sbin/f2cgi -f /etc/f2cgi/f2cgi.conf -s /var/run/f2cg
i/f2cgi.socket -p /var/run/f2cgi/f2cgi.pid
==> start f2cgi Done.
# Starting wui ...
/sbin/cpumask -m 12 /opt/wui/bin/wui -f /var/state/wui.conf -g adm
==> start wui Done.
Warning: No IP configuration found !
Warning: DHCP configuration is available for test purpose only.
Warning: ALOHA does not performs any renew at end of lease time.
Warning: A static IP configuration is recommended.
Retrieve IP using DHCP or configure static ... 10sec (D/s)?
```

If you missed the prompt and no DHCP is available on the network, then the ALOHA for Exchange appliance will autoconfigure the following IP address: 192.168.0.200.



If you missed the prompt, just reset the Virtual appliance and get ready on your hypervisor console

4.1.1 Network configuration at boot prompt

When the prompt below appears, you have 10 seconds to choose between **DHCP** (type "D") or **static** (type "s") configuration.

```
Warning: No IP configuration found !
Warning: DHCP configuration is available for test purpose only.
Warning: ALOHA does not performs any renew at end of lease time.
Warning: A static IP configuration is recommended.
Retrieve IP using DHCP or configure static ... 10sec (D/s)?
```

Type "s" to configure a static IP.

The appliance will then ask three questions:

- The IP address you want to configure on the appliance
- The subnet
- The appliance default gateway

The picture below shows an example of configuration:

```
Configure IP manually
Use IP address (192.168.0.200)? 10.0.0.17
Use netmask (255.255.255.0)? 255.255.0.0
Use default gateway (none)? 10.0.1.1
Commit and save this configuration (N/y)?
```

Type "y" to validate your configuration.

You can now access your Appliance **Web User Interface** at the address <https://10.0.0.17:4444/>.

The picture below shows the appliance telling you where to find the WUI:

```
Access WEB User Interface :
https://10.0.0.17:4444/
```

4.1.2 Network configuration through DHCP

 This type of configuration is not recommended in a production environment.

The appliance will failover to DHCP configuration when you let it boot or when you type "D" when prompted:

```
Warning: No IP configuration found !
Warning: DHCP configuration is available for test purpose only.
Warning: ALOHA does not performs any renew at end of lease time.
Warning: A static IP configuration is recommended.
Retrieve IP using DHCP or configure static ... 10sec (D/s)?
```

At the end of the boot, it will display on the console the URL where you can the **Web User Interface** is available:

```
Access WEB User Interface :
https://10.0.4.233:4444/
```

4.2 Network configuration using the Web User Interface

In the WUI, there is a **network** configuration tab.

It displays the configuration options below:

Local Network Settings

Hostname:	<input type="text"/>
Address:	<input type="text" value="10.0.0.17"/>
Netmask:	<input type="text" value="255.255.0.0"/>
Gateway:	<input type="text" value="10.0.1.1"/>
vLAN Identifier:	<input type="text"/> <input type="button" value="X"/> <input type="button" value="✓"/>

Static Routes

	Network Address	Network Mask	Router Address
Route 1:	<input type="text"/>	<input type="text"/>	<input type="text"/>
Route 2:	<input type="text"/>	<input type="text"/>	<input type="text"/>
Route 3:	<input type="text"/>	<input type="text"/>	<input type="text"/>
Route 4:	<input type="text"/>	<input type="text"/>	<input type="text"/>

High Availability

Role:	<input type="text" value="disabled"/> <input type="button" value="X"/> <input type="button" value="✓"/>
-------	---

4.2.1 Local Network

This area allows you to setup the LAN configuration of the Aloha.

4.2.1.1 Settings

- **Hostname:** this is the Aloha hostname
- **Address:** Aloha IP address where you want it to be reachable
- **Netmask:** the netmask related to the IP address
- **Gateway:** default gateway where the Aloha will forward all the traffic
- **vLAN Identifier:** only if you traffic is tagged on Aloha's interface. Just type here the Vlan number.
- Click on the **VALIDATION** button if required.

4.2.1.2 Static Routes

If you need to route some subnets to a different gateway than the default one, just setup static route in this form.

Click on the **VALIDATION** button  if required.

4.2.2 High availability

High availability is a mechanism which allows an IP address to move from a failed / sick device to a safer one.

We allow only an **Active/Passive cluster**.

When enabled, you'll have to setup the Virtual IP address which will move between the devices.

 Of course, **this is the IP address you'll have to redirect your DNS to.**

4.2.2.1 Disabling High availability

By default, high availability is **disabled**.

Which means you can use a standalone Aloha For Exchange, even if it's safer to use a cluster.

4.2.2.2 Configuring the Master node

From the **role** form select box, choose the **master** option:

High Availability

Role:	<input style="width: 80%;" type="text" value="master"/> <input type="button" value="X"/> <input type="button" value="✓"/>
Options	
Virtual Service Address:	<input style="width: 80%;" type="text" value="192.168.0.253"/>
Cluster Identifier:	<input style="width: 80%;" type="text" value="253"/> <input type="button" value="X"/> <input type="button" value="✓"/>

Click on the **VALIDATION** button  if required.

4.2.2.2.1 Options

- **Virtual Service Address:** This is the Virtual IP address which will be allowed to move from the Master to the Backup, in case of trouble on the Master Aloha For Exchange.
- **Cluster Identifier:** This is the VRRP ID associated to this cluster.

 The Cluster Identifier must be **unique on the LAN**.
The **master** and the **backup** nodes **must share the same Cluster Identifier**.

Click on the **VALIDATION** button  if required.

4.2.2.3 Configuring the Backup node

From the **role** form select box, choose the **backup** option:

High Availability	<input type="text"/>	
	Role:	<input type="text" value="backup"/> <input type="button" value="X"/> <input type="button" value="✓"/>
Options	Virtual Service Address:	<input type="text" value="192.168.0.253"/>
	Cluster Identifier:	<input type="text" value="253"/> <input type="button" value="X"/> <input type="button" value="✓"/>

Click on the **VALIDATION** button if required.

4.2.2.3.1 Options

- **Virtual Service Address:** This is the Virtual IP address which will be allowed to move from the Master to the Backup, in case of trouble on the Master Aloha For Exchange.
- **Cluster Identifier:** This is the VRRP ID associated to this cluster.

 The Cluster Identifier must be **unique on the LAN**.
The **master** and the **backup** nodes **must share the same Cluster Identifier**.

Click on the **VALIDATION** button if required.

5 Exchange 2010 load-balancing configuration

5.1 WUI login

The default login is “**admin**” and the default password is “**admin**”.



5.2 Configuration tab


To configure the ALOHA for Exchange appliance, click on the tab named **config**.

In this tab, you have access to several areas:

- **CAS Servers:** IP addresses of your CAS servers. You can configure up to 4 CAS servers
- **HTTP(s) Services:** Let you configure Exchange 2010 HTTP based services:
 - Outlook Web App
 - Exchange Control Panel
 - Offline Address Book
 - Auto discover
 - Exchange Web Services
 - Active Sync
 - Outlook Anywhere
- **IMAP service**
- **POP service**
- **RPC based services:** configuration Exchange 2010 RPC based services:
 - EndPoint Mapper
 - Client Access
 - Address Book
- **SMTP(s) service:** allows you to configure Microsoft Exchange HUB servers

Each time you modify an area or a sub-area, then two buttons will be turned on:

- **OK** or **VALIDATION** button: , use it to apply local update
- **CANCEL** button: , use it to undo local update

 Don't forget to **VALIDATE** your configuration each time it's required.

5.3 CAS Servers

This area allows you to configure **the IP addresses** of your **CAS servers**. Just fill up the form with the IP addresses, like in the picture below:

CAS Servers	
CAS1 Address:	10.0.0.15
CAS2 Address:	10.0.0.16
CAS3 Address:	
CAS4 Address:	

Click on the **VALIDATION** button .

5.4 HTTP based Services

This area allows you to configure the following Exchange 2010 services:

- Outlook Web App
- Exchange Control Panel
- Offline Address Book
- Auto discover
- Exchange Web Services
- Active Sync
- Outlook Anywhere

5.4.1 Disabling HTTP based services

For some reason, you might want to disable Exchange 2010 HTTP based services.

To achieve this, just choose the option "**disabled**" on the select box, like in the image below:

HTTP(s) Service	
HTTP(s) Service:	disabled

There is no other option to setup.



Bear in mind that when disabling HTTP based services, no Auto discover will be available! So it's highly recommended to never disabled HTTP based services.

Click on the **VALIDATION** button  if required.

5.4.2 SSL offloading

The ALOHA for Exchange appliance can process SSL instead of your CAS servers.

The advantage of such configuration is that the appliance would see all the requests in clear and so it can perform advanced routing and persistence method.

In order to enable **SSL offloading**, choose the option "ssl-offload" from the select box.

The following options would then appear:

HTTP(s) Service

HTTP(s) Service:

Options

Host Name:	<input type="text" value="mail.mydomain.local"/>
Virtual Service HTTPs port:	<input type="text" value="443"/>
Redirect HTTP port:	<input type="text" value="80"/>
CAS Servers HTTP port:	<input type="text" value="80"/>
Timeout:	<input type="text" value="25"/>

Certificate

Common Name:	mail.mydomain.local
From:	02/21/12 16:11:56
Until:	02/18/22 16:11:56
Status:	self signed
Certificate .pfx or .pem:	<input type="button" value="Choisissez un fichier"/> <input type="text" value="Aucun f...choisi"/>
File password:	<input type="text"/>

HTTP and Web Services

Outlook Web Access:	<input type="text" value="enabled"/>
Exchange Control Panel:	<input type="text" value="enabled"/>
Offline Address Book:	<input type="text" value="enabled"/>
Auto discover:	<input type="text" value="enabled"/>
Exchange Web Services:	<input type="text" value="enabled"/>
Active Sync:	<input type="text" value="enabled"/>
Outlook Anywhere:	<input type="text" value="enabled"/>

Click on the **VALIDATION** button if required.

5.4.2.1 Options

- **Host Name:** the FQDN of your HTTP based services. This option will be used for health checking and HTTP to HTTPS redirection.

- **Virtual Service HTTPs port:** the port on which the appliance will listen for HTTPs requests (default 443).
- **Redirect HTTP port:** the port on which the appliance will listen for HTTP traffic, to redirect it to HTTPS (default 80).
- **CAS Servers HTTP port:** the port configured on the CAS servers for HTTP based services (default 80)
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button  if required.

5.4.2.2 Certificate

- **Certificate .pfx or .pem:** Point it to the file containing the certificate
- **File password:** If the file is protected by a passphrase, then type it here, it will be used when inserting the certificate in the appliance.

Click on the **VALIDATION** button  if required.

5.4.2.3 HTTP and Web Services

- **Outlook Web App:** should have the same state as **Exchange Control Panel**, this is Exchange Webmail.
- **Exchange Control Panel:** should have the same status as **Outlook Web App**, used by the Webmail.
- **Offline Address Book:** allows download of the address book.
- **Auto discover:** should always be enabled, used by clients to discover Exchange configuration.
- **Exchange Web Services:** should always be enabled, used by clients.
- **Active Sync:** service to keep smartphone synchronized.
- **Outlook Anywhere:** also known as RPC over HTTPs, easy configuration for remote outlook clients.

Click on the **VALIDATION** button  if required.

5.4.3 SSL Forwarding

The ALOHA for Exchange can forward HTTPS traffic to the CAS servers without modifying it. This is called **SSL Forwarding**.

In order to enable SSL forwarding, choose the option "**ssl-forward**" from the select box.

The following options would appear:

HTTP(s) Service

HTTP(s) Service:

Options

Host Name:	<input type="text" value="mail.mydomain.local"/>
Virtual Service HTTPs port:	<input type="text" value="443"/>
Redirect HTTP port:	<input type="text" value="80"/>
CAS Servers HTTP port:	<input type="text" value="80"/>
CAS Servers HTTPs port:	<input type="text" value="443"/>
Timeout:	<input type="text" value="25"/> <input type="button" value="X"/> <input type="button" value="✓"/>

Click on the **VALIDATION** button if required.

5.4.3.1 Options

- **Host Name:** the FQDN of your HTTP based services. This option will be used for health checking and for HTTP to HTTPs redirection, if required.
- **Virtual Service HTTPs port:** the port on which the appliance will listen for HTTPs requests (default 443).
- **Redirect HTTP port:** the port on which the appliance will listen for HTTP traffic, to redirect it to HTTPs (default 80).
- **CAS Servers HTTP port:** the port configured on the CAS servers for HTTP based services (default 80)
- **CAS Servers HTTPs port:** the port configured on the CAS servers for HTTPs based services (default 443)
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button if required.

5.5 IMAP service

This service may be used only if non-outlook clients have to be connected on the Exchange platform.

It is **disabled** by default:

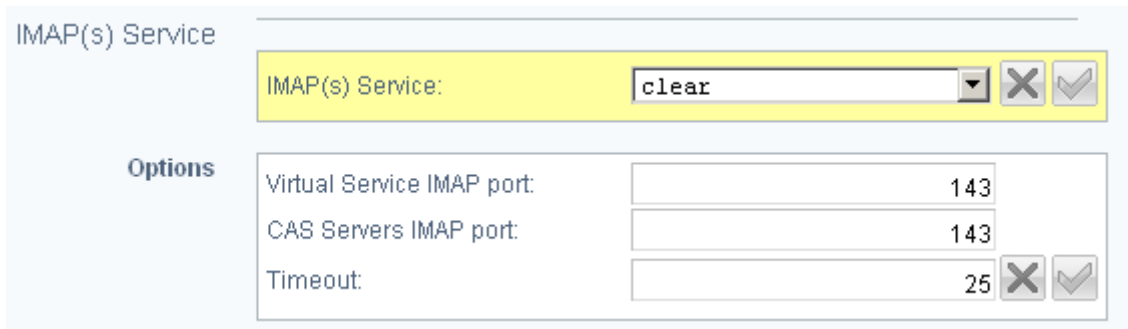
IMAP(s) Service

IMAP(s) Service:

5.5.1 Clear IMAP service

When configured in **clear**, the appliance will forward only clear IMAP port to the CAS servers.

The picture below shows the options available for such usage:



The screenshot shows the 'IMAP(s) Service' configuration window. The 'IMAP(s) Service' dropdown is set to 'clear'. Under the 'Options' section, there are three input fields: 'Virtual Service IMAP port' (143), 'CAS Servers IMAP port' (143), and 'Timeout' (25). Each field has a 'Validation' button (a green checkmark icon) to its right.

Click on the **VALIDATION** button  if required.

5.5.1.1 Options

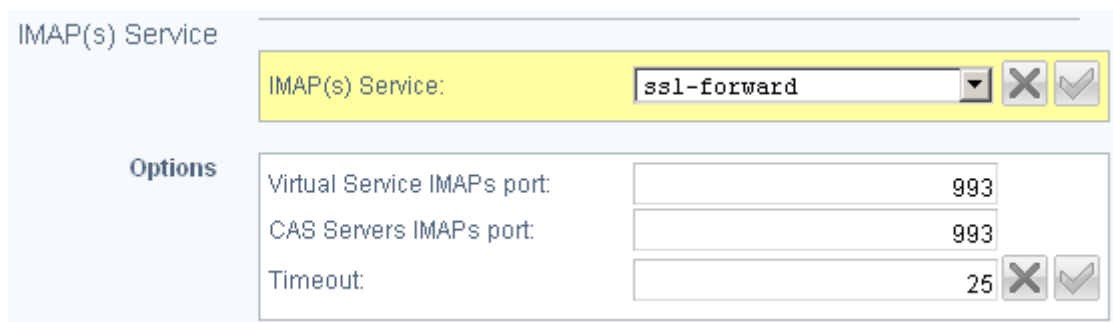
- **Virtual Service IMAP port:** the port on which the appliance will listen for clear IMAP traffic (default 143).
- **CAS Servers IMAP port:** the clear IMAP port configured on the CAS servers (default 143)
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button  if required.

5.5.2 IMAPs service without SSL offloading

The appliance can forward IMAPs traffic to the CAS servers without offloading SSL, this is call **ssl-forward**.

The picture below shows the options available for such usage:



The screenshot shows the 'IMAP(s) Service' configuration window. The 'IMAP(s) Service' dropdown is set to 'ssl-forward'. Under the 'Options' section, there are three input fields: 'Virtual Service IMAPs port' (993), 'CAS Servers IMAPs port' (993), and 'Timeout' (25). Each field has a 'Validation' button (a green checkmark icon) to its right.

Click on the **VALIDATION** button  if required.

5.5.2.1 Options

- **Virtual Service IMAPs port:** the port on which the appliance will listen for IMAPs traffic (default 993).
- **CAS Servers IMAPs port:** the IMAPs port configured on the CAS servers (default 993).
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button  if required.

5.5.3 IMAPs service with SSL offloading

The appliance can listen for IMAPs traffic, process the SSL offloading then forward it in clear the CAS servers, this is call **ssl-offload**.

The picture below shows the options available for such usage:

IMAP(s) Service

IMAP(s) Service:

Options

Virtual Service IMAPs port:	<input type="text" value="993"/>	
CAS Servers IMAP port:	<input type="text" value="143"/>	
Timeout:	<input type="text" value="25"/>	<input type="button" value="X"/> <input type="button" value="✓"/>

Certificate

Common Name:	mail.xlc.local	
From:	12/29/11 14:06:14	
Until:	12/28/12 14:06:14	
Status:	self signed	
Certificate .pfx or .pem:	<input type="button" value="Choisissez un fichier"/>	<input type="text" value="Aucun f...choisi"/>
File password:	<input type="text"/>	<input type="button" value="📁"/>

Click on the **VALIDATION** button  if required.

5.5.3.1 Options

- **Virtual Service IMAPs port:** the port on which the appliance will listen for IMAPs traffic (default 993).
- **CAS Servers IMAP port:** the clear IMAP port configured on the CAS servers (default 143).
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button  if required.

5.5.3.2 Certificate

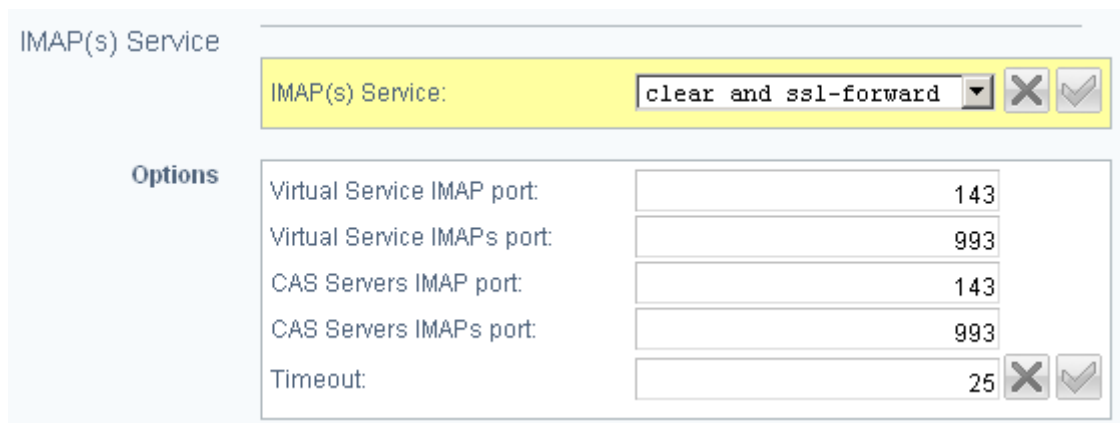
- **Certificate .pfx or .pem:** Point it to the file containing the certificate
- **File password:** If the file is protected by a passphrase, then type it here, it will be used when inserting the certificate in the appliance.

Click on the **VALIDATION** button  if required.

5.5.4 IMAP and IMAPs service without SSL offloading

The appliance can listen for both IMAP and IMAPs traffic, and forward them to the CAS servers, this is called **clear and ssl-forwarding**.

The picture below shows the options available for such usage:



The screenshot shows the configuration for the IMAP(s) Service. The 'IMAP(s) Service' dropdown is set to 'clear and ssl-forward'. Below it, the 'Options' section contains the following fields:

Virtual Service IMAP port:	143
Virtual Service IMAPs port:	993
CAS Servers IMAP port:	143
CAS Servers IMAPs port:	993
Timeout:	25

Click on the **VALIDATION** button  if required.

5.5.4.1 Options

- **Virtual Service IMAP port:** the port on which the appliance will listen for clear IMAP traffic (default 143).
- **Virtual Service IMAPs port:** the port on which the appliance will listen for IMAPs traffic (default 993).
- **CAS Servers IMAP port:** the clear IMAP port configured on the CAS servers (default 143).
- **CAS Servers IMAPs port:** the IMAPs port configured on the CAS servers (default 993).
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button  if required.

5.5.5 IMAP and IMAPs service with SSL offloading

The appliance can listen for both IMAP and IMAPs traffic, process the SSL if required then forward it in clear to the CAS servers, this is called **clear and ssl-offloading**.

The picture below shows the options available for such usage:


IMAP(s) Service

IMAP(s) Service: clear and ssl-offload ✕ ✓

Options

Virtual Service IMAP port:	<input style="width: 90%;" type="text" value="143"/>	
Virtual Service IMAPs port:	<input style="width: 90%;" type="text" value="993"/>	
CAS Servers IMAP port:	<input style="width: 90%;" type="text" value="143"/>	
Timeout:	<input style="width: 90%;" type="text" value="25"/>	✕ ✓

Certificate

Common Name:	mail.xlc.local	
From:	12/29/11 14:06:14	
Until:	12/28/12 14:06:14	
Status:	self signed	
Certificate .pfx or .pem:	Choisissez un fichier	Aucun f...choisi
File password:	<input style="width: 90%;" type="text"/>	

Click on the **VALIDATION** button  if required.

5.5.5.1 Options

- **Virtual Service IMAP port:** the port on which the appliance will listen for clear IMAP traffic (default 143).
- **Virtual Service IMAPs port:** the port on which the appliance will listen for IMAPs traffic (default 993).
- **CAS Servers IMAP port:** the clear IMAP port configured on the CAS servers (default 143).
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button  if required.

5.5.5.2 Certificate

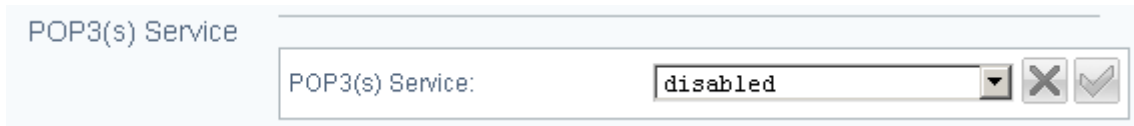
- **Certificate .pfx or .pem:** Point it to the file containing the certificate
- **File password:** If the file is protected by a passphrase, then type it here, it will be used when inserting the certificate in the appliance.

Click on the **VALIDATION** button  if required.

5.6 POP service

This service may be used only if non-outlook clients have to be connected on the Exchange platform.

It is **disabled** by default:



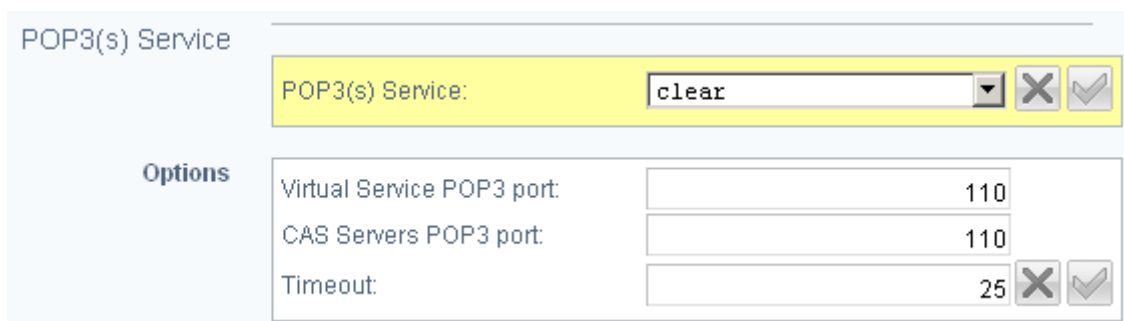
POP3(s) Service

POP3(s) Service:

5.6.1 Clear POP service

When configured in **clear**, the appliance will forward only the clear POP traffic.

The picture below shows the options available for such usage:



POP3(s) Service

POP3(s) Service:

Options

Virtual Service POP3 port:	<input type="text" value="110"/>
CAS Servers POP3 port:	<input type="text" value="110"/>
Timeout:	<input type="text" value="25"/> <input type="button" value="X"/> <input type="button" value="✓"/>

Click on the **VALIDATION** button if required.

5.6.1.1 Options

- **Virtual Service POP port:** the port on which the appliance will listen for clear POP traffic (default 110).
- **CAS Servers POP port:** the clear POP port configured on the CAS servers (default 110)
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button if required.

5.6.2 POPs service without SSL offloading

The appliance can forward POPs traffic to the CAS servers without offloading SSL, this is call **ssl-forward**.

The picture below shows the options available for such usage:

POP3(s) Service

POP3(s) Service:

Options

Virtual Service POP3s port:	<input type="text" value="995"/>
CAS Servers POP3s port:	<input type="text" value="995"/>
Timeout:	<input type="text" value="25"/> <input type="button" value="X"/> <input type="button" value="✓"/>

Click on the **VALIDATION** button if required.

5.6.2.1 Options

- **Virtual Service POPs port:** the port on which the appliance will listen for POPs traffic (default 995).
- **CAS Servers POPs port:** the POPs port configured on the CAS servers (default 995).
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button if required.

5.6.3 POPs service with SSL offloading

The appliance can listen for POPs traffic, process SSL then forward it in clear the CAS servers, this is call **ssl-offload**.

The picture below shows the options available for such usage:

POP3(s) Service

POP3(s) Service:

Options

Virtual Service POP3s port:	<input type="text" value="995"/>
CAS Servers POP3 port:	<input type="text" value="110"/>
Timeout:	<input type="text" value="25"/> <input type="button" value="X"/> <input type="button" value="✓"/>

Certificate

Common Name:	mail.mydomain.local
From:	02/21/12 16:11:56
Until:	02/18/22 16:11:56
Status:	self signed
Certificate .pfx or .pem:	<input type="button" value="Choisissez un fichier"/> Aucun f...choisi
File password:	<input type="text"/> <input type="button" value="📁"/>

Click on the **VALIDATION** button  if required.

5.6.3.1 Options

- **Virtual Service POPs port:** the port on which the appliance will listen for POPs traffic (default 995).
- **CAS Servers POP port:** the clear POP port configured on the CAS servers (default 110).
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button  if required.

5.6.3.2 Certificate

- **Certificate .pfx or .pem:** Point it to the file containing the certificate
- **File password:** If the file is protected by a passphrase, then type it here, it will be used when inserting the certificate in the appliance.



Click on the **VALIDATION** button  if required.

5.6.4 POP and POPs service without SSL offloading



The appliance can listen for both POP and POPs traffic, then forward it to the CAS servers, this is called **clear and ssl-forwarding**.

The picture below shows the options available for such usage:

POP3(s) Service

POP3(s) Service: clear and ssl-forward  

Options

Virtual Service POP3 port:	110
Virtual Service POP3s port:	995
CAS Servers POP3 port:	110
CAS Servers POP3s port:	995
Timeout:	25  

Click on the **VALIDATION** button  if required.

5.6.4.1 Options

- **Virtual Service POP3 port:** the port on which the appliance will listen for clear POP3 traffic (default 110).

- **Virtual Service POP3s port:** the port on which the appliance will listen for POP3s traffic (default 995).
- **CAS Servers POP3 port:** the clear POP3 port configured on the CAS servers (default 110).
- **CAS Servers POP3s port:** the POP3 port configured on the CAS servers (default 995).
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button  if required.

5.6.5 POP3 and POP3s service with SSL offloading

The appliance can listen for both POP3 and POP3s traffic, process the SSL if required then forward it in clear to the CAS servers, this is called **clear and ssl-offloading**.

The picture below shows the options available for such usage:

POP3(s) Service

POP3(s) Service:

Options

Virtual Service POP3 port:	110
Virtual Service POP3s port:	995
CAS Servers POP3 port:	110
Timeout:	25

Certificate

Common Name:	mail.mydomain.local
From:	02/21/12 16:11:56
Until:	02/18/22 16:11:56
Status:	self signed
Certificate .pfx or .pem:	<input type="button" value="Choisissez un fichier"/> <input type="text" value="Aucun f...choisi"/>
File password:	<input type="text"/>

Click on the **VALIDATION** button  if required.

5.6.5.1 Options

- **Virtual Service POP3 port:** the port on which the appliance will listen for clear POP3 traffic (default 110).
- **Virtual Service POP3s port:** the port on which the appliance will listen for POP3s traffic (default 995).
- **CAS Servers POP3 port:** the clear POP3 port configured on the CAS servers (default 110).

- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button  if required.

5.6.5.2 Certificate

- **Certificate .pfx or .pem:** Point it to the file containing the certificate
- **File password:** If the file is protected by a passphrase, then type it here, it will be used when inserting the certificate in the appliance.

Click on the **VALIDATION** button  if required.

5.7 RPC services

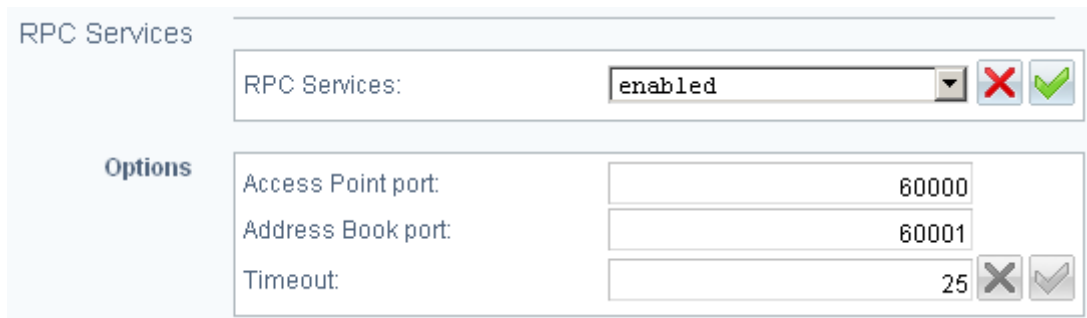
The **RPC services** are used by **outlook clients** to get connected on the CAS Servers..





There are two services to load-balance:

- Client Access
- Address Book

The **RPC services** are enabled by default.

The picture below shows the RPC services configuration:



RPC Services	
RPC Services:	enabled  
Options	
Access Point port:	60000
Address Book port:	60001
Timeout:	25  

Click on the **VALIDATION** button  if required.

5.7.1.1 Options

- **Access Point port:** the Client Access port configured on your CAS servers (must be fixed in the registry).
- **Address Book port:** the Address Book port configured on your CAS servers (must be fixed in the registry).

Click on the **VALIDATION** button  if required.

5.7.2 Disabling RPC services

It is possible to disable RPC services, if not needed in your infrastructure:

RPC Services

RPC Services:

Click on the **VALIDATION** button if required.

5.8 SMTP service

This service may be used if you want to load-balance SMTP service to HUB servers.

It is **disabled** by default:

SMTP(s) Service

SMTP(s) Service:

Click on the **VALIDATION** button if required.

5.8.1 Clear SMTP service

When configured in **clear**, the appliance will forward the clear SMTP traffic only.

The picture below shows the options available for such usage:

SMTP(s) Service

SMTP(s) Service:

HUB Servers

HUB1 Address:

HUB2 Address:

HUB3 Address:

HUB4 Address:

Options

Virtual Service SMTP port:

HUB Servers SMTP port:

Timeout:

Click on the **VALIDATION** button if required.

5.8.1.1 HUB Servers

This area allows you to configure **the IP addresses** of your **HUB servers**. Just fill up the form with the IP addresses, like in the picture below:

HUB Servers	HUB1 Address:	<input type="text" value="192.168.0.21"/>	<input type="button" value="X"/> <input type="button" value="✓"/>
	HUB2 Address:	<input type="text" value="192.168.0.22"/>	
	HUB3 Address:	<input type="text"/>	
	HUB4 Address:	<input type="text"/>	

5.8.1.2 Options

- **Virtual Service SMTP port:** the port on which the appliance will listen for clear SMTP traffic (default 25).
- **HUB Servers SMTP port:** the clear SMTP port configured on the HUB servers (default 25)
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button if required.

5.8.2 SMTPs service without SSL offloading

The appliance can forward SMTPs traffic to the HUB servers without offloading SSL, this is call **ssl-forward**.

The picture below shows the options available for such usage:

SMTP(s) Service	
SMTP(s) Service:	<input type="text" value="ssl-forward"/> <input type="button" value="X"/> <input type="button" value="✓"/>
HUB Servers	
HUB1 Address:	<input type="text" value="192.168.0.21"/>
HUB2 Address:	<input type="text" value="192.168.0.22"/>
HUB3 Address:	<input type="text"/>
HUB4 Address:	<input type="text"/> <input type="button" value="X"/> <input type="button" value="✓"/>
Options	
Virtual Service SMTPs port:	<input type="text" value="587"/>
HUB Servers SMTPs port:	<input type="text" value="587"/>
Timeout:	<input type="text" value="25"/> <input type="button" value="X"/> <input type="button" value="✓"/>

Click on the **VALIDATION** button if required.

5.8.2.1 Options








- **Virtual Service SMTPs port:** the port on which the appliance will listen for SMTPs traffic (default 587).
- **HUB Servers SMTPs port:** the SMTPs port configured on the HUB servers (default 587).
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button  if required.

5.8.3 SMTPs service with SSL offloading

The appliance can listen for SMTPs traffic, process SSL then forward it in clear the HUB servers, this is call **ssl-offload**.

The picture below shows the options available for such usage:

SMTP(s) Service	
SMTP(s) Service:	<input type="text" value="ssl-offload"/>  
HUB Servers	
HUB1 Address:	<input type="text" value="192.168.0.21"/>
HUB2 Address:	<input type="text" value="192.168.0.22"/>
HUB3 Address:	<input type="text"/>
HUB4 Address:	<input type="text"/>
	 
Options	
Virtual Service SMTPs port:	<input type="text" value="587"/>
HUB Servers SMTP port:	<input type="text" value="25"/>
Timeout:	<input type="text" value="25"/>
	 
Certificate	
Common Name:	<input type="text" value="mail.mydomain.local"/>
From:	<input type="text" value="02/21/12 16:11:56"/>
Until:	<input type="text" value="02/18/22 16:11:56"/>
Status:	<input type="text" value="self signed"/>
Certificate .pfx or .pem:	<input type="text" value="Choisissez un fichier"/> <input type="text" value="Aucun f...choisi"/>
File password:	<input type="text"/>
	

Click on the **VALIDATION** button  if required.

5.8.3.1 Options

- **Virtual Service SMTPs port:** the port on which the appliance will listen for SMTPs traffic (default 587).
- **HUB Servers SMTP port:** the clear SMTP port configured on the HUB servers (default 25).
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button if required.

5.8.3.2 Certificate

- **Certificate .pfx or .pem:** Point it to the file containing the certificate
- **File password:** If the file is protected by a passphrase, then type it here, it will be used when inserting the certificate in the appliance.

Click on the VALIDATION button if required.

5.8.4 SMTP and SMTPs services without SSL offloading

The appliance can listen for both SMTP and SMTPs traffic, then forward them to the HUB servers, this is called **clear and ssl-forwarding**.

The picture below shows the options available for such usage:

SMTP(s) Service	
SMTP(s) Service:	clear and ssl-forward <input type="checkbox"/> <input checked="" type="checkbox"/>
HUB Servers	
HUB1 Address:	192.168.0.21
HUB2 Address:	192.168.0.22
HUB3 Address:	
HUB4 Address:	<input type="checkbox"/> <input checked="" type="checkbox"/>
Options	
Virtual Service SMTP port:	25
Virtual Service SMTPs port:	587
HUB Servers SMTP port:	25
HUB Servers SMTPs port:	587
Timeout:	25 <input type="checkbox"/> <input checked="" type="checkbox"/>

Click on the **VALIDATION** button if required.

5.8.4.1 Options

- **Virtual Service SMTP port:** the port on which the appliance will listen for clear SMTP traffic (default 25).
- **Virtual Service SMTPs port:** the port on which the appliance will listen for SMTPs traffic (default 587).
- **HUB Servers SMTP port:** the clear SMTP port configured on the HUB servers (default 25).
- **HUB Servers SMTPs port:** the SMTP port configured on the HUB servers (default 587).
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button  if required.

5.8.5 SMTP and SMTPs services with SSL offloading

The appliance can listen for both SMTP and SMTPs traffic, process the SSL if required then forward it in clear to the HUB servers, this is called **clear and ssl-offloading**.

The picture below shows the options available for such usage:

SMTP(s) Service

SMTP(s) Service:	clear and ssl-offload	✕	✓
------------------	-----------------------	---	---


HUB Servers

HUB1 Address:	192.168.0.21		
HUB2 Address:	192.168.0.22		
HUB3 Address:			
HUB4 Address:			
		✕	✓

Options

Virtual Service SMTP port:	25		
Virtual Service SMTPs port:	587		
HUB Servers SMTP port:	25		
Timeout:	25		
		✕	✓

Certificate

Common Name:	mail.mydomain.local		
From:	02/21/12 16:11:56		
Until:	02/18/22 16:11:56		
Status:	self signed		
Certificate .pfx or .pem:	Choisissez un fichier	Aucun f...choisi	
File password:			

Click on the **VALIDATION** button  if required.

5.8.5.1 Options

- **Virtual Service SMTP port:** the port on which the appliance will listen for clear SMTP traffic (default 25).
- **Virtual Service SMTPs port:** the port on which the appliance will listen for SMTPs traffic (default 587).
- **HUB Servers SMTP port:** the clear SMTP port configured on the HUB servers (default 25).
- **Timeout:** the time in seconds the appliance will let a connection opened if no traffic is passing through (default 25).

Click on the **VALIDATION** button  if required.

5.8.5.2 Certificate

- **Certificate .pfx or .pem:** Point it to the file containing the certificate
- **File password:** If the file is protected by a passphrase, then type it here, it will be used when inserting the certificate in the appliance.













Click on the **VALIDATION** button  if required.

6 Services

The Services TAB from the WUI allows you to Start, Stop, Restart and Reload services running on the Aloha For exchange Appliance.

The TAB also tells you if the service is currently running or not and if it's configured to start up when Aloha for exchange boots up.

The picture below shows the content of this tab:

		Status	Startup	Actions
	system		Auto.	
	vrrp		Auto.	
	haproxy		Auto.	
	stunnel		Auto.	

There are 4 columns in the table:

1. Service Name
2. Service Status
3. Startup configuration
4. Actions



6.1 Services description

There are four services available:

1. **system**: the kernel and heart of the appliance
2. **vrrp**: the high availability protocol
3. **haproxy**: the load-balancing and health checking software
4. **stunnel**: the SSL accelerator

6.2 Services running status

There are two running statuses available:

1. **OK status**: when the service is up and running, the icon is green: 
2. **NOK status**: when the service is stopped, the icon is red: 

6.3 Services startup status

There are two startup statuses available, which refer to the status of the service when the appliance boots up:

1. **Manual:** the service won't start automatically
2. **Auto:** the service will start automatically

7 Setup tab

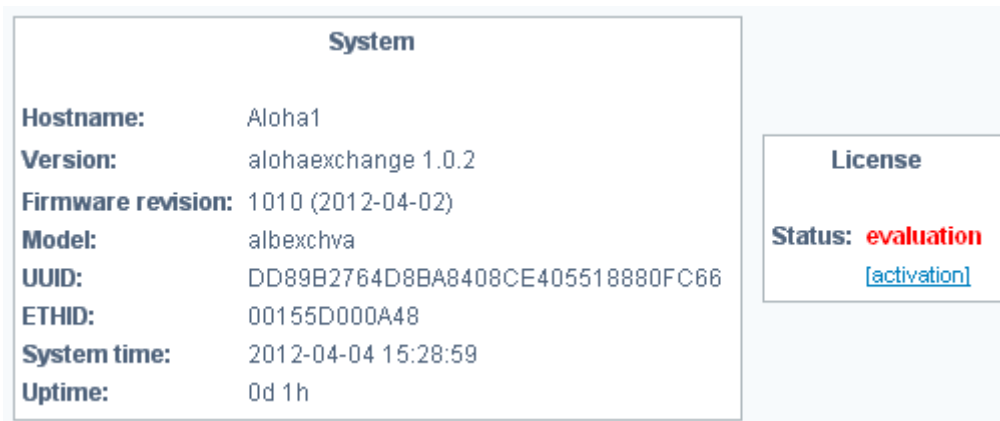
This tab has multiple purposes. It allows you to:

- get your system information
- get an evaluation or an activation licence from Exceliance for your product
- save your configuration
- update the firmware
- change system parameters and admin password
- update your licence

7.1 Information

From this area, you can get information about your product, the running version and both ETHID and UUID which are required to get a license.

The picture below shows an example it:



The screenshot shows two panels. The left panel, titled "System", lists the following information:

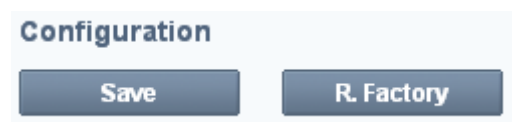
Hostname:	Aloha1
Version:	alohaexchange 1.0.2
Firmware revision:	1010 (2012-04-02)
Model:	albexchva
UUID:	DD89B2764D8BA8408CE405518880FC66
ETHID:	00155D000A48
System time:	2012-04-04 15:28:59
Uptime:	0d 1h

The right panel, titled "License", shows the status as "evaluation" in red text and a blue link labeled "[activation]" below it.

If you want to get an evaluation or an activation license, just click on the link **[activation]**. You'll be redirected to a pre-filled form on Exceliance website.

7.2 Configuration

The picture below shows what this area looks like:



The screenshot shows a "Configuration" section with two buttons: "Save" and "R. Factory".

This area allows you to save your current configuration to the disk, to ensure you'll recover it if the Aloha reboots.

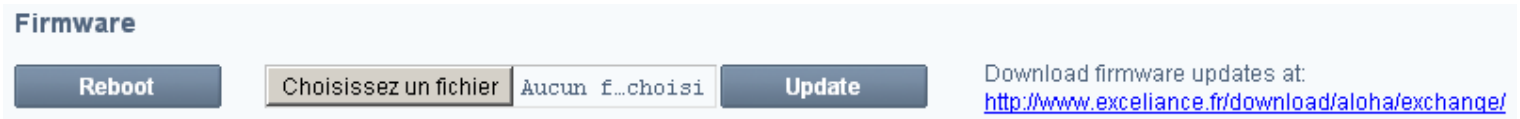
Just click on the **save** button.

You can also reset your Aloha to factory defaults.

Just click on the **R. Factory** button, then on **reboot** button from the **firmware** area, **without saving!!**

7.3 Firmware

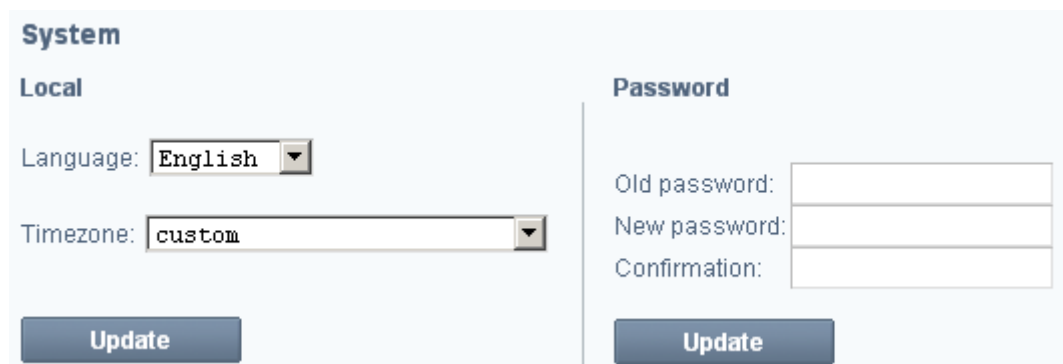
This area allows you to download and update your Aloha for Exchange version.



- Click on the link <http://www.exceliance.fr/download/aloha/exchange/> to download a new firmware version.
- Point the form to the downloaded firmware
- Click on **Update**.
- Once updated, click on **Reboot**

7.4 System

This area allows you to change the **WUI language** and the **timezone** and to update the **admin password**.



Just fill up the right form for your needs then click on the **Update** button.

7.5 Licenses

This area allows you to manage your licenses:



Once you've registered on Excelsiance website, you'll receive a mail with a link where you can download your license file. Download it, point the form to the file, then click **Add** and **Save**.

8 Microsoft Exchange 2010 procedures

8.1 Set static TCP Port for MS Exchange RPC Client Access service

More information about this procedure can be found here:

<http://social.technet.microsoft.com/wiki/contents/articles/configure-static-rpc-ports-on-an-exchange-2010-client-access-server.aspx>

8.1.1 Procedure for Exchange 2010

On your CAS servers, do:

1. Open regedit
2. Browse to the key
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MExchangeRPC
3. Create a new key named **ParametersSystem**
4. Under this key create a **REG_DWORD** named **TCP/IP Port**
5. **Right click** then **Modify** on the TCP/IP Port REG_DWORD
6. Fill the form: **Value** with the TCP port number and check **Decimal** base.
7. Click on **OK**



Microsoft recommends using a port from the range **59531 to 60554**, and the same one on all the CAS servers.



Bear in mind that the port number must be different for **RPC Client Access** and **Address Book service**.

8.1.2 Procedure for Exchange 2010 SP1 and SP2

This is the same procedure than Exchange 2010. Please read paragraph 8.1.1.

8.2 Set static TCP Port for MS Exchange Address Book service

8.2.1 Procedure for Exchange 2010

On your CAS servers, do:

1. Open an explorer window
2. Browse to **C:\Program Files\Microsoft\Exchange Server\V14\Bin** directory
3. **Open the file named microsoft.exchange.addressbook.service.exe.config** with notepad
4. Find the string **RpcTcpPort**
5. **Replace the Value by the TCP port number you want**
6. **Close the file**



Microsoft recommends using a port from the range **59531 to 60554**, and the same one on all the CAS servers.

8.2.2 Procedure for Exchange 2010 SP1 and SP2

On your CAS servers, do:

1. Open regedit
2. Browse to the key
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\MSExchangeAB\Parameters
3. Under this key create a **REG_SZ** named **RpcTcpPort**
4. **Right click** then **Modify** on the RpcTcpPort REG_SZ
5. Fill the field **Value** with the TCP port number you want
6. Click on **OK**



Microsoft recommends using a port from the range **59531 to 60554**, and the same one on all the CAS servers.



When upgrading Exchange 2010 to SP1, it is recommended to create this registry key before the upgrade, that way, once the CAS server would reboot, there won't be any outage.