

# ALOHA LOAD BALANCER MANAGING SSL – CHAINED CERTIFICATES

## "APPNOTE" #0024 – MANAGING SSL – CHAINED CERTIFICATES

*This application note is intended to help you implement SSL management via chained certificates within the ALOHA Load Balancer solution.*

### CONSTRAINT

Have the entire chain of certificates up to the Trusted Root Certification Authority.

### OBJECTIVE

Correctly implement chained certificates and eliminate the "invalid chain" error in the Aloha interface.



### COMPLEXITY



### VERSIONS CONCERNED

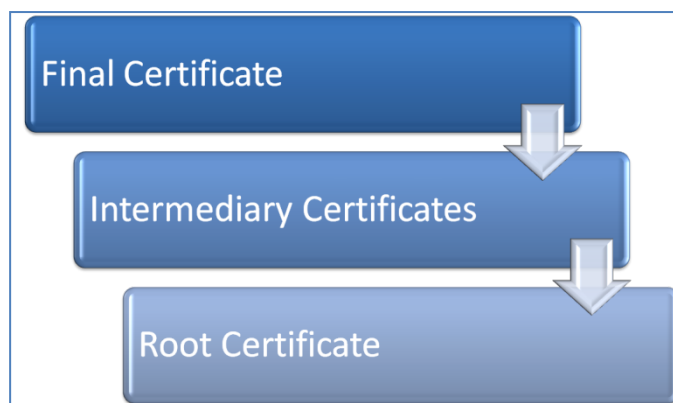
V 3.x and later

### ERROR MESSAGE

Frontends SSL					
Nom	Domaine	Début	Fin	Statut	
SSL	testsrv	09/15/09 11:38:58	09/13/19 11:38:58	Chaîne invalide	 

[Nouveau](#)

### CHAIN OF CERTIFICATES



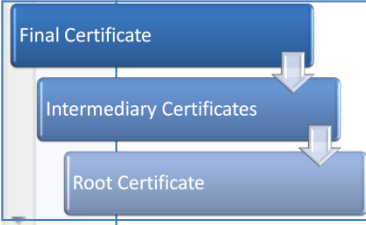
In order to implement chained certificates, the certificate chain must be verifiable. Therefore Aloha needs to know the precise order of all the certificates in the chain.

# Frontend: SSL

**Certificat:**



**Sujet:** /C=FR/ST=IdF/L=Paris/O=Exotest/CN=testsrv/emailAddress=me@exotest  
**Emetteur:** /C=FR/ST=IdF/L=Paris/O=Exotest/CN=Exotest CA/emailAddress=me@exotest  
**Validité:** 09/15/09 11:38:58 - 09/13/19 11:38:58  
**Statut:** Valide

```
-----BEGIN CERTIFICATE-----
MIIDijCCAvOgAwIBAgIBATANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEw
JGUjEMMAoGA1UECBMSWRGMQ4wDAYDVQQHEwVYXJpczEQMA4GA1UEChMH
...
0ZDjY4Gtb+k9J5sUWACMFZd76pwkoa8KdRS1WVG1WvAuyZmKmj a49F4fdZ
/oMuhwWpwW2rhIh1j/fYidw/V1DEdUzKZQni7CPGdqsGa3801TJ1zQ==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDKzCCApSgAwIBAgIJALzRcyPQOTNiMA0GCSqGSIb3DQEBBQUAMG0xCz
AJBgNVBAYTAkZSMQwwCgYDVQQIEwNJZEYxZDdjAMBGNVBAcTBVBhcmlzMRAw
...
RgKOG3XDnAPICUYm0u6r883X6scrSFTkGBOAnLPmD4fMyqGycrQnGqX2Vc
UomkAd2QiXhVGIASqsNW19qX0KdbmxV9NX35LyL4LTA=
-----END CERTIFICATE-----
```



Annuler MàJ

## RESULTS

Frontends SSL					
Nom	Domaine	Début	Fin	Statut	
SSL	testsrv	09/15/09 11:38:58	09/13/19 11:38:58	Valide	 

**Nouveau**

The Aloha device does not check whether the root certificate has been delivered by a "Trusted root Certification Authority". As a result, although the status is valid on the Aloha device, the browser may indicate that the security certificate presented was not issued by an approved certification authority.

## BASIC TROUBLESHOOTING

If you nevertheless continue to obtain an invalid status, you must check whether one of the intermediate certificates or the root certificate has expired.