

Thunder ADC with TLS/SSL Certificate from Sectigo Certificate Manager (SCM)

Deploy Thunder ADC with Sectigo Certificate Manager (SCM) for
TLS/SSL Certificate Enrollment and Renewal using ACME Protocol

Table of Contents

Overview.....	3
Deployment Prerequisites.....	3
Deployment Architecture	3
Sectigo SCM Configuration	4
Thunder ADC Configuration	8
Accessing Thunder ADC.....	8
General Configuration.....	9
High Availability Configuration Using VCS and VRRP-A	10
Verify Reachability to Sectigo ACME URL.....	12
Register the Site Name with a Domain Registrar and Map it to a Public IP	12
Configure SLB VIP to Respond to ACME Challenge	12
Configure ACME CA profile	13
Configure Virtual Port 443 under the VIP on Thunder ADC.....	15
Verify web access to the domain	17
Summary.....	18
Appendix	19
vThunder-LE1	19
vThunder-LE2.....	22

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.

Overview

This deployment guide contains configuration procedures for the A10 Networks® Thunder® ADC series line of high-performance application delivery controllers (ADCs) to obtain and automatically renew TLS/SSL certificates from Sectigo Certificate Manager (SCM) using ACME protocol.

Sectigo Certificate Manager (SCM) is a universal platform purpose-built to issue and manage the lifecycles of public and private digital certificates to secure every human and machine identity across the enterprise, all from a single platform. With SCM, customers can automate the issuance and management of Sectigo certificates, alongside their certificates from other publicly trusted certificate authorities (CAs) and existing private CAs, like Microsoft CA.

For more information on Sectigo Certificate Manager, visit: <https://sectigo.com/enterprise-solutions/certificate-manager>

Deployment Prerequisites

When deploying A10 Thunder ADC with Sectigo SCM, the following are prerequisites and assumptions:

- Users have some basic configuration familiarity with both the A10 Thunder ADC and Sectigo SCM, and a high-level understanding of public key infrastructure (PKI)
- The A10 Thunder ADC is running ACOS Release 5.2.1-P5 or higher
- A Sectigo Certificate Manager (SCM) account is available
- Product and version tested:
 - A VCS/HA pair of Thunder ADCs running ACOS version 5.2.1-P5
 - Sectigo SCM trial account

Note: This deployment can also be done using A10 Thunder CFW running ACOS 5.2.1-P5 or higher.

Deployment Architecture

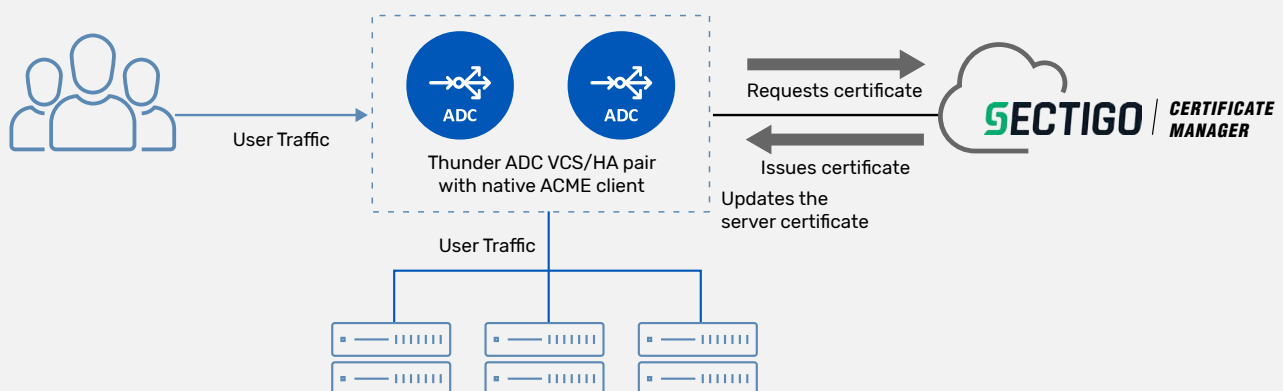


Figure 1: Architecture for deploying Thunder ADC/CFW with Sectigo Certificate Manager (SCM)

Sectigo SCM Configuration

Log in into Sectigo Certificate Manager (SCM) with the account username and password that you created when signing up for the SCM account.

For using SCM to issue certificates using the ACME protocol, you need to have the following in place:

1. Organization, and optionally, departments within the organization
2. Domain names for which the TLS/SSL certificates are to be requested. You can optionally delegate these domain names to specific departments within the organization
3. Certificate profile for the type for the type of certificate you want to be issued (e.g., TLS/SSL certificate)
4. One or more ACME accounts
5. Public or private CA that will issue the TLS/SSL certificate

For detailed instructions on setting this up, refer to Sectigo documentation at:

<https://docs.sectigo.com/scm/scm-guides/1/scm-admin-guides/scm-administrator-guide.html>

In this deployment, we have the organization “A10 Networks,” and within it, the department “Marketing” as shown:

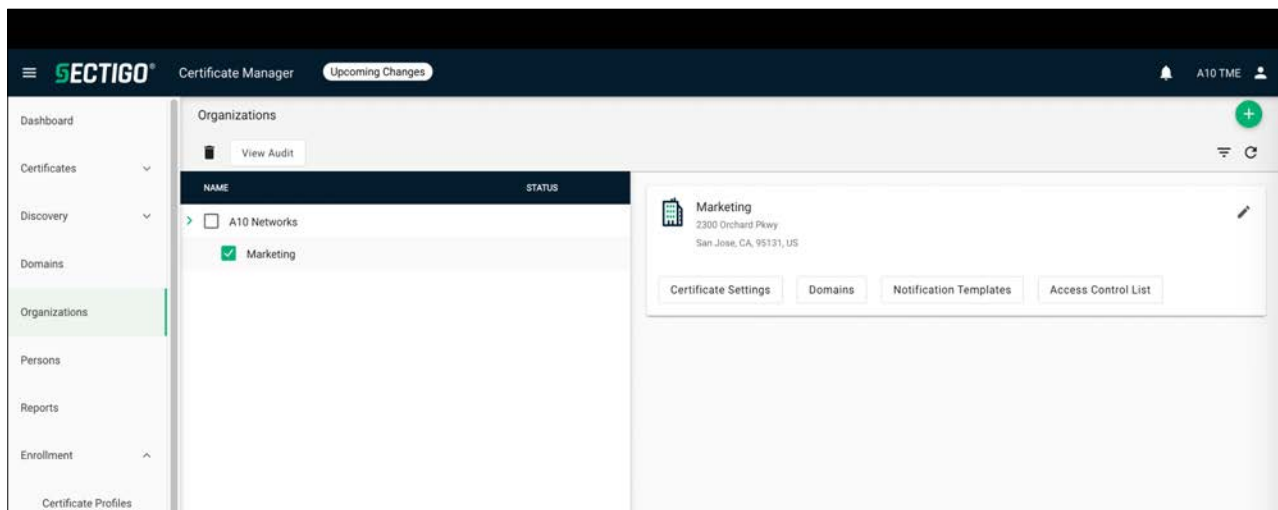


Figure 2: Certificate management hierarchy consisting of organizations and departments

Under Domains, we have the domain a10networks.com, and under it “*.a10networks.com” and “marketing.a10networks.com”:

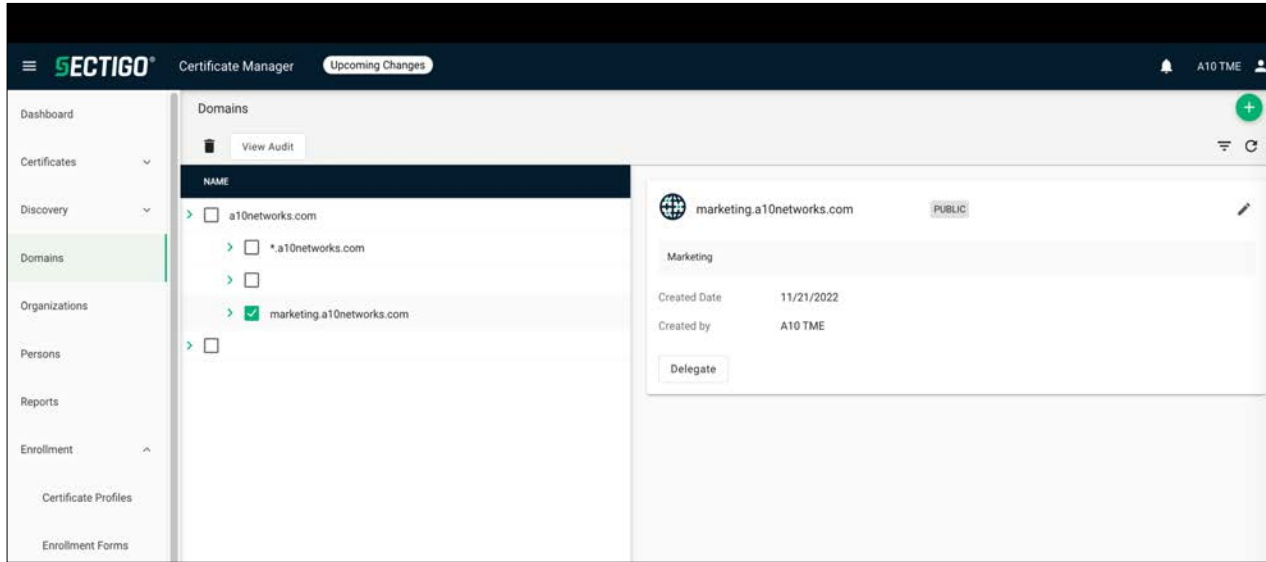


Figure 3: Domain names for which certificates are to be requested

Additionally, these domains have been delegated to the marketing department under A10 Networks organization:



Figure 4: Delegation of domains to organizations/departments

For issuing a TLS/SSL certificate, we have the certificate profile "A10SSLCertProfile":

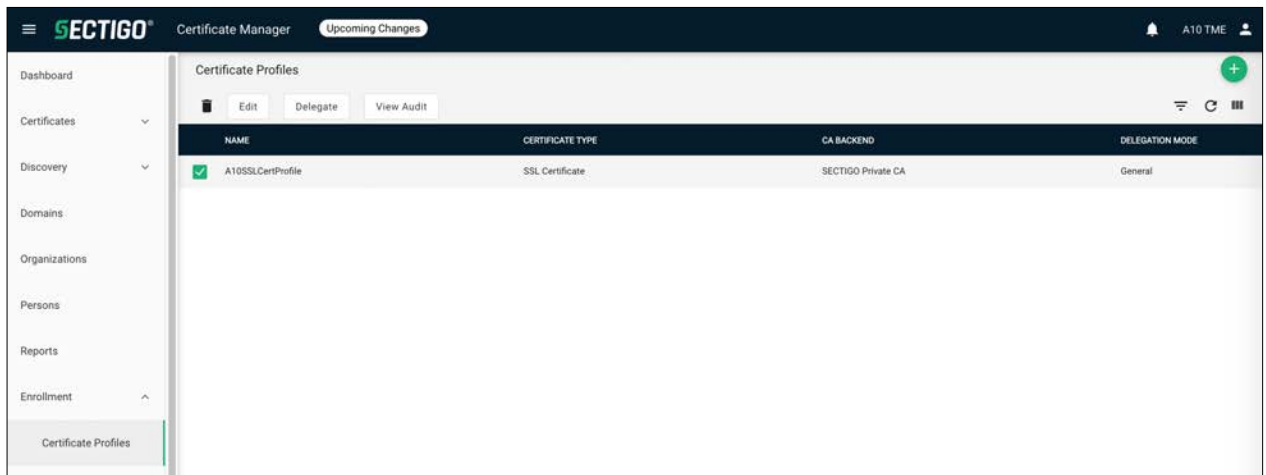


Figure 5: Certificate profile to be used for certificate issuance

The certificate profile details are as follows and can vary depending on your deployment requirements:

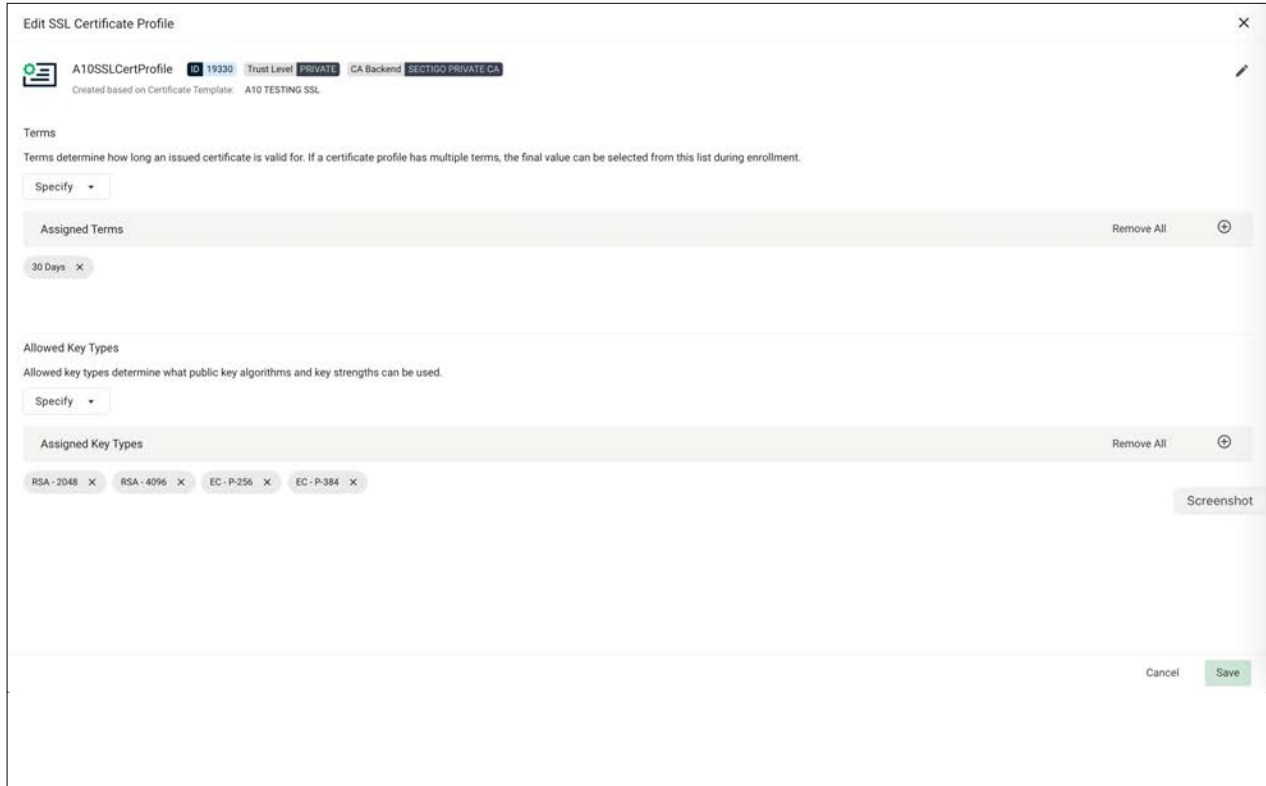


Figure 6: Certificate profile with details such as validity period, allowed key types, etc.

For requesting a certificate using the ACME protocol, we have the ACME option under Enrollment in the left pane.

Select ACME and then click on Accounts to view the list of accounts:

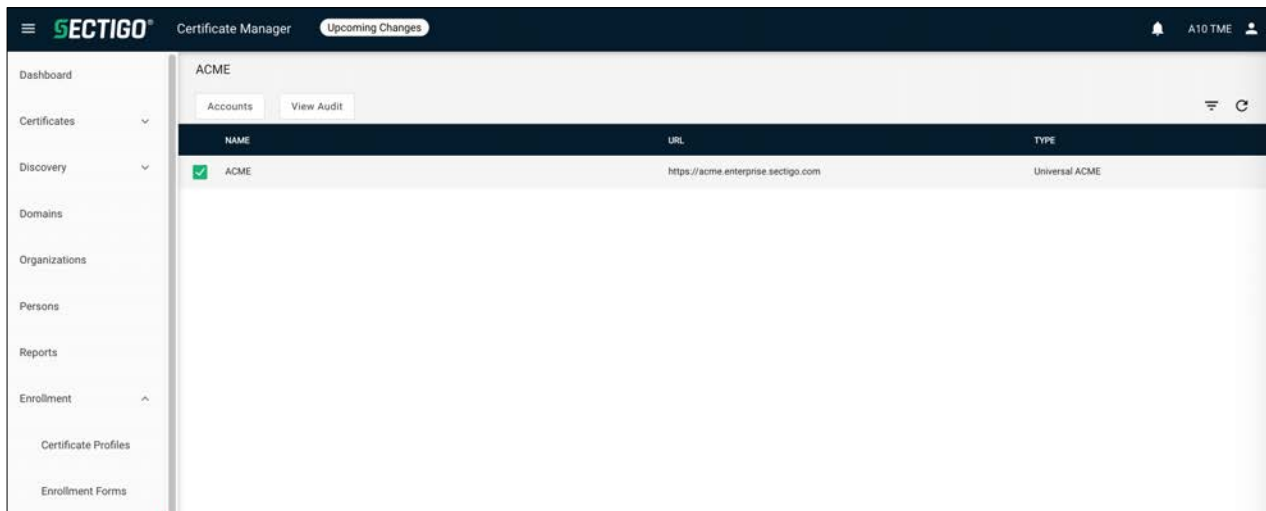
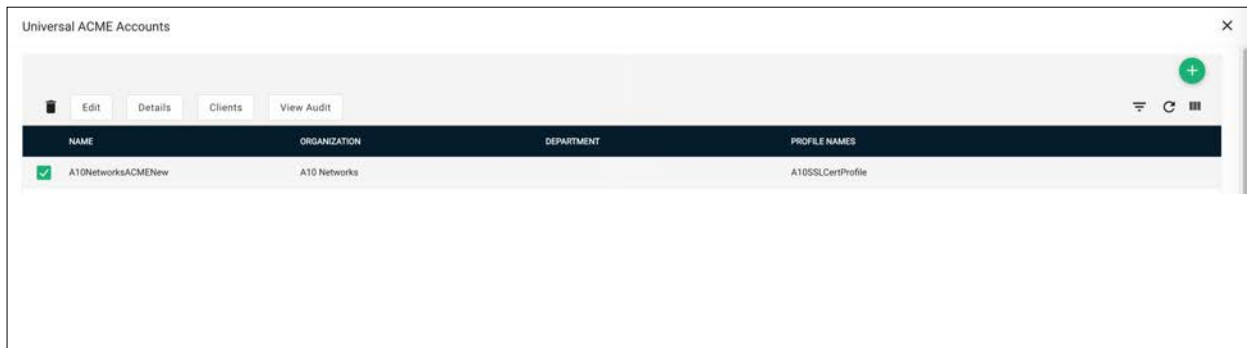


Figure 7: Certificate enrollment using ACME

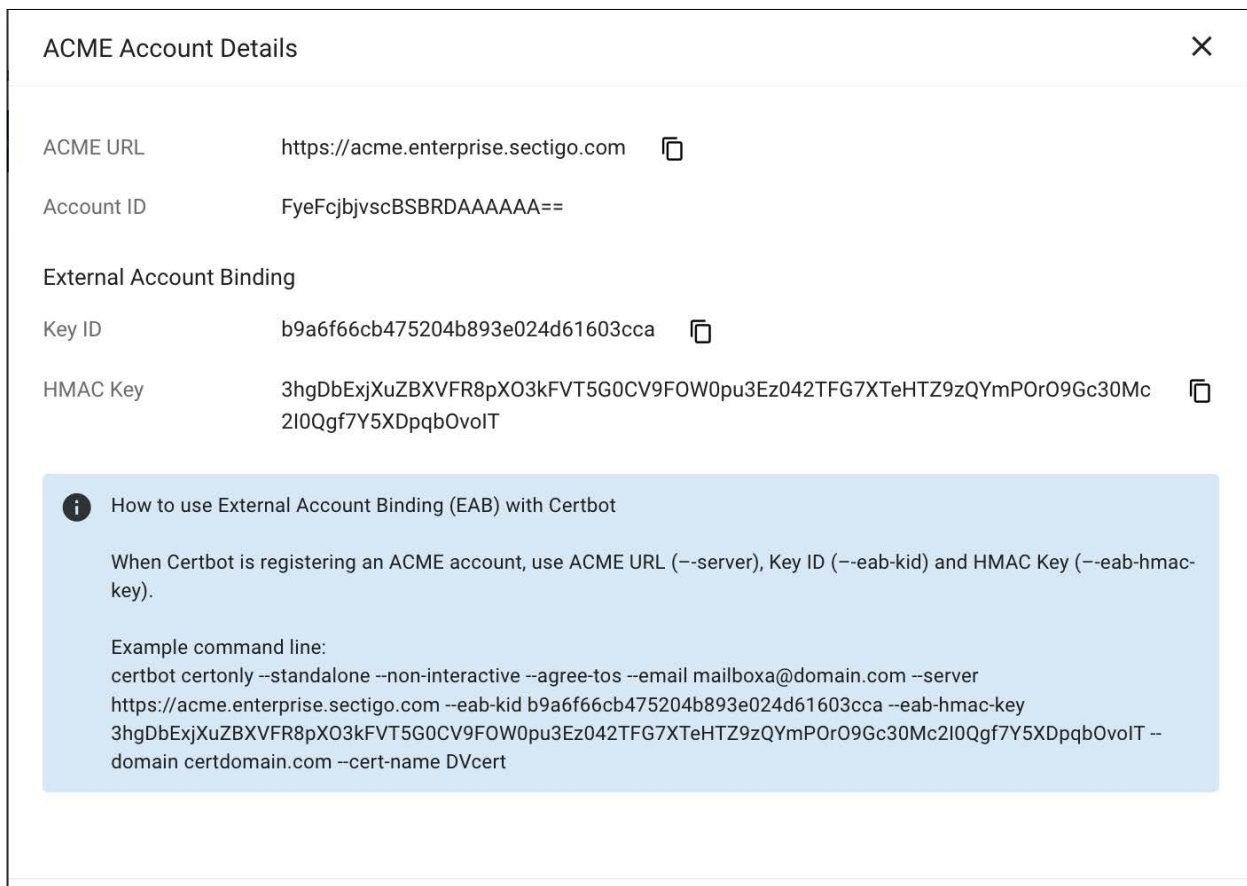
Here, we have the ACME account named "A10NetworksACMENew" and this is associated with the certificate profile "A10SSLCertProfile" that we had created earlier:



NAME	ORGANIZATION	DEPARTMENT	PROFILE NAMES
A10NetworksACMENew	A10 Networks		A10SSLCertProfile

Figure 8: List of ACME accounts

You can view the EAB credentials for an ACME account by selecting the account and then clicking "Details" from the top menu:



ACME Account Details

ACME URL: <https://acme.enterprise.sectigo.com>

Account ID: FyeFcbjvscBSBRDAAAAA==

External Account Binding

Key ID: b9a6f66cb475204b893e024d61603cca

HMAC Key: 3hgDbExjXuZBXVFR8pXO3kFVT5G0CV9FOW0pu3Ez042TFG7XTeHTZ9zQYmP0r09Gc30Mc2I0Qgf7Y5XDpqbOvoIT

How to use External Account Binding (EAB) with Certbot

When Certbot is registering an ACME account, use ACME URL (`--server`), Key ID (`--eab-kid`) and HMAC Key (`--eab-hmac-key`).

Example command line:

```
certbot certonly --standalone --non-interactive --agree-tos --email mailboxa@domain.com --server https://acme.enterprise.sectigo.com --eab-kid b9a6f66cb475204b893e024d61603cca --eab-hmac-key 3hgDbExjXuZBXVFR8pXO3kFVT5G0CV9FOW0pu3Ez042TFG7XTeHTZ9zQYmP0r09Gc30Mc2I0Qgf7Y5XDpqbOvoIT --domain certdomain.com --cert-name DVcert
```

Figure 9: ACME account details including EAB credentials

Note: The EAB credentials should be kept confidential. Here the EAB Key ID and HMAC Key are shown just for the purpose of documentation.

Finally, under Issuers > CAs, we have a private CA "A10TestingIssuingCA" that will issue the TLS/SSL certificate. Depending on your deployment needs, you can also use a Sectigo public CA instead.

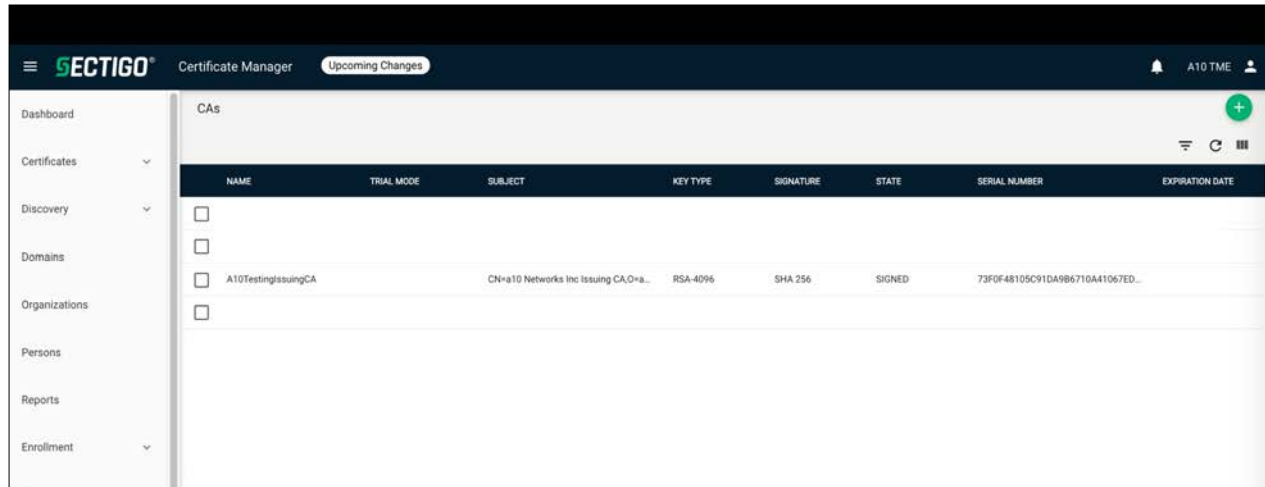


Figure 10: List of certificate authorities used to issue the certificate

Thunder ADC Configuration

Accessing Thunder ADC

To access Thunder ADC from a command line interface (CLI) or graphical user interface (GUI), follow the steps below.

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 in the [A10 Networks support portal](#).

General Configuration

Here is the general configuration of Thunder ADC devices. We plan to deploy a VCS/HA pair using A10's VCS and VRRP-A features and hence we have two Thunder devices in this setup.

Hostname	vThunder-LE1	vThunder-LE2
Management interface	10.22.10.88	10.22.10.86
Client-facing interface	10.24.44.92	10.24.44.155
Server-facing interface	10.80.80.1	10.80.80.2
Route	IP Route 0.0.0.0 /0 10.24.44.1	IP Route 0.0.0.0 /0 10.24.44.1

The user can configure this using either the GUI or CLI. This section describes the configuration steps using CLI. For steps via GUI, refer to ACOS System Configuration and Administration Guide.

vThunder-LE1	vThunder-LE2
<pre> multi-config enable ! terminal idle-timeout 0 ! ip dns primary 8.8.8.8 ! hostname vThunder-LE1 ! timezone America/Phoenix ! ntp server time.google.com prefer ! interface management ip address 10.22.10.88 255.255.252.0 ip default-gateway 10.22.8.1 ! interface ethernet 1 enable ip address 10.24.44.92 255.255.255.0 ! interface ethernet 2 enable ip address 10.80.80.1 255.255.255.0 ! ! ip route 0.0.0.0 /0 10.24.44.1 ! sflow setting local-collection ! sflow collector ip 127.0.0.1 6343 ! ! end </pre>	<pre> multi-config enable ! terminal idle-timeout 0 ! ip dns primary 8.8.8.8 ! hostname vThunder-LE2 ! timezone America/Phoenix ! ntp server time.google.com prefer ! interface management ip address 10.22.10.86 255.255.252.0 ip default-gateway 10.22.8.1 ! interface ethernet 1 enable ip address 10.24.44.155 255.255.255.0 ! interface ethernet 2 enable ip address 10.80.80.2 255.255.255.0 ! ! ip route 0.0.0.0 /0 10.24.44.1 ! sflow setting local-collection ! sflow collector ip 127.0.0.1 6343 ! ! end </pre>

High Availability Configuration Using VCS and VRRP-A

First, configure A10's Virtual Chassis System (VCS) feature along with VRRP-A. VCS enables you to manage a cluster of Thunder ADCs like a single, virtual chassis. With VCS, any configuration changes from the vMaster are automatically propagated to the vBlades.

Note: If the Thunder devices are going to run as an HA pair, then VCS is required for proper synchronization of information needed to communicate with Sectigo ACME server. A non-VCS HA configuration is not supported for this deployment.

vThunder-LE1	vThunder-LE2
<pre>vThunder-LE1(config)#vrrp-a common vThunder-LE1(config-common)#device-id 1 vThunder-LE1(config-common)#set-id 7 vThunder-LE1(config-common)#enable vThunder-LE1(config-common)#exit vThunder-LE1-Standby(config)#vcs enable vThunder-LE1-Active(config:1)#vcs floating-ip 10.22.10.90 255.255.252.0 vThunder-LE1-Active(config:1)#vcs device 1 vThunder-LE1-Active(config:1- device:1)#interfaces management vThunder-LE1-Active(config:1- device:1)#interfaces ethernet 2 vThunder-LE1-Active(config:1-device:1)#priority 125 vThunder-LE1-Active(config:1-device:1)#enable vThunder-LE1-Active(config:1-device:1)#vcs reload</pre>	<pre>vThunder-LE2(config)#vrrp-a common vThunder-LE2(config-common)#device-id 2 vThunder-LE2(config-common)#set-id 7 vThunder-LE2(config-common)#enable vThunder-LE2(config-common)#exit vThunder-LE2-Standby(config)#vcs enable vThunder-LE2-Standby(config:2)#vcs floating-ip 10.22.10.90 255.255.252.0 vThunder-LE2-Standby(config:2)#vcs device 2 vThunder-LE2-Standby(config:2- device:2)#interfaces management vThunder-LE2-Standby(config:2- device:2)#interfaces ethernet 2 vThunder-LE2-Standby(config:2-device:2)#priority 100 vThunder-LE2-Standby(config:2-device:2)#enable vThunder-LE2-Standby(config:2-device:2)#vcs reload</pre>

Via GUI:

On each Thunder device:

- Go to **System > VRRP-A > Global**, select Enable for the VRRP-A Enable field and configure the Device ID and Set ID fields, then click OK
- Go to **System > aVCS > Settings**, select Enable in the aVCS Enable field, configure the management address for the virtual chassis, then click OK
- Go to **System > aVCS > Device**, add a new device
- Go to **System > aVCS > Actions**, in the Reload Option drop-down list, select Reload and click Apply

Once configured, SSH into the VCS pair at the floating management IP, in this case, 10.22.10.90:

Note: The CLI prompt on your setup may be different depending on which Thunder device is currently the VCS vMaster. Also, the VCS vMaster may not necessarily be the same as the VRRP-A Active device.

```
vThunder-LE2-Active-vMaster[7/2]#sh vcs summary
VCS Chassis:
  VCS Enabled:                Yes
  Chassis ID:                 7
  Floating IP:                10.22.10.90
  Mask:                       255.255.252.0
  Unicast Election port:     41217
  Multicast IP:               224.0.0.210
  Multicast Port:             41217
  Version:                    5.2.1-p5.b114
  Current Discover mode:     Multicast
```

```
Members(* means local device):
ID  State      Priority IP:Port          Location
-----
1   vBlade     125    10.22.10.88:41216 Remote
                10.80.80.1:41216
2   vMaster(*) 100    10.22.10.86:41216 Local
                10.80.80.2:41216

Total: 2
vThunder-LE2-Active-vMaster[7/2]#
```

Next, configure HA by configuring the following commands on VCS vMaster.

Note: VRRP-A is the ACOS implementation of high availability that is completely different from the industry-standard implementation of Virtual Router Redundancy Protocol (VRRP). For purposes of operational familiarity, it borrows concepts from VRRP but is significantly different from VRRP. VRRP-A will not inter-operate with VRRP.

```
vrrp-a vrid 0
floating-ip 10.80.80.3
device-context 1
  blade-parameters
    priority 150
device-context 2
  blade-parameters
    priority 250
!
device-context 1
  vrrp-a peer-group
    peer 10.22.10.86
    peer 10.80.80.2
!
device-context 2
  vrrp-a peer-group
    peer 10.22.10.88
    peer 10.80.80.1
```

Via GUI:

- Open a web browser and go to the floating management IP, e.g., <https://<floating management IP>>
- Go to **System > VRRP-A > Global**, add VRRP-A configuration details
- Go to **System > VRRP-A > Vrid**, add the VRID (e.g., VRID 0)

Verify Reachability to Sectigo ACME URL

The Sectigo URL for certificate enrollment using ACME protocol is "https://acme.enterprise.sectigo.com".

Initiate a ping from the Thunder ADC CLI to verify reachability to this site:

```
vThunder-LE2-Standby-vMaster[7/2]#ping acme.enterprise.sectigo.com
PING acme.enterprise.sectigo.com (91.199.212.81) 56(84) bytes of data.
64 bytes from auth.portal.sectigo.com (91.199.212.81): icmp_seq=1 ttl=45 time=87.7 ms
64 bytes from auth.portal.sectigo.com (91.199.212.81): icmp_seq=2 ttl=45 time=82.5 ms
64 bytes from auth.portal.sectigo.com (91.199.212.81): icmp_seq=3 ttl=45 time=72.9 ms
```

Note: The Sectigo server should be reachable via a data interface (e.g., ethernet 1), not just the management interface. This is because when the Thunder ADC sends out a certificate enrollment request to the Sectigo ACME server, it will do so using a data interface and not the management interface.

Register the Site Name with a Domain Registrar and Map it to a Public IP

Register the domain name for which you want to get the certificate (e.g., marketing.a10networks.com) with a domain registrar and add a DNS record for resolving it to a public IP.

On the Thunder ADC we need to configure a virtual server with Virtual IP (VIP) that maps to this public IP. This can be done either by directly configuring the VIP with this public IP, or by configuring the VIP with a private IP and then mapping it to the public IP using NAT. The specific method by which this is achieved is specific to the deployment environment.

Configure SLB VIP to Respond to ACME Challenge

Here we configure a VIP on the Thunder ADC with a private IP address 10.24.44.94. In this setup, the private IP is mapped to the public IP of the domain name using a NAT gateway.

```
slb server apache 10.80.80.7
  health-check-disable
  port 80 tcp
    health-check-disable
  port 443 tcp
    health-check-disable
  port 8080 tcp
!
slb service-group apache tcp
  health-check-disable
  member apache 80
!
slb template persist source-ip src-persist
!
slb template virtual-port acme
  drop-unknown-conn
  reset-unknown-conn
!
slb virtual-server vip 10.24.44.94
  port 80 http
  attack-detection
  source-nat auto
  service-group apache
  template virtual-port acme
  reply-acme-challenge
```

Under port 80 http, configure the command “reply-acme-challenge” as shown.

Optionally, to protect vport 80 from attacks, you can configure the command “attack-detection” under the vport and apply SLB virtual-port template “acme” consisting of commands “drop-unknown-conn” and “reset-unknown-conn” as shown above.

Via GUI:

- To create source IP persistence template: Go to ADC > Templates > Persistence, click Create, then choose the type as Persist Source IP
- To create virtual port template: Go to ADC > Templates > SLB, click Create, then choose the type as Virtual Port
- To create servers: Go to ADC > SLB > Servers, click Create
- To create service-group: Go to ADC > SLB > Service Groups, click Create
- To create virtual-server: Go to ADC > SLB > Virtual Servers, click Create

Verify that the virtual service for port 80 is up:

```
vThunder-LE2-Demo-10.86-Active-vMaster[7/2]#sh slb virtual-server bind
Total Number of Virtual Services configured: 1
-----
*Virtual Server :vip 10.24.44.94      All Up

      +port 80  http ==>>apache                State :All Up
      +apache:80                10.80.80.7      State :Up
```

Via GUI:

- Go to **ADC > SLB > Virtual Servers**
- Select the VIP and expand the list of vports under that VIP
- Verify the status is UP

Configure ACME CA profile

Now configure the following ACME account details on the Thunder ADC:

- Enrollment URL: <https://acme.enterprise.sectigo.com/>
- Domain name for which the certificate is to be requested
- Certificate type: RSA or ECDSA certificate
- Account email
- EAB credentials: EAB key ID and HMAC key obtained from the SCM portal as shown earlier.

In addition to the above, you can specify options such as level for logging output of ACME commands (default 1 and detailed 2, including debug messages), the interval before a certificate expires to renew the certificate, etc.

Here is the ACME profile configuration on the Thunder ADC:

```
pki acme-cert sectigo-acme
url https://acme.enterprise.sectigo.com/
domain <domain name>
force
log-level 2
renew-before day 7
cert-type rsa
account-email <email-id>
eab-key-id b9a6f66cb475204b893e024d61603cca
eab-hmac-key
3hgDbExjXuZBXVFR8pX03kFVT5G0CV9F0W0pu3Ez042TFG7XTeHTZ9zQYmP0r09Gc30Mc2I0Qgf7Y5XDpqb0voIT
```

The eab-key-id and eab-hmac-key values should match the ones that were earlier obtained from SCM portal under ACME account details (figure 9).

Via GUI:

- Go to **ADC > SSL Management > ACME Certificates**, click Create

Note: The EAB credentials should be kept confidential. Here the EAB Key ID and HMAC Key has been shown just for the purpose of documentation.

If you display the running configuration, you will see that the Thunder ADC automatically encrypts the original EAB HMAC Key once it is entered:

```
pki acme-cert sectigo-acme
url https://acme.enterprise.sectigo.com/
domain <domain-name>
force
log-level 2
renew-before day 7
cert-type rsa
account-email <email-id>
eab-key-id b9a6f66cb475204b893e024d61603cca
eab-hmac-key encrypted
wCM7PPB3jz00R9pbkmxQqRvhEjc+6tdXNEpQRrAk92778o2EJBZ0akSVqY1q7VaE4imz+uuS0ChzdrSv90A7FCN5Xcr
guJ7mfl9XG1FImyXLijG97m2gu0o4X7y7i1Vk
```

To start the certificate enrollment, run the “enroll” command under the ACME profile:

```
vThunder-LE2-Active-vMaster[7/2](config:2)# pki acme-cert sectigo-acme
vThunder-LE2-Active-vMaster[7/2](config:2-acme cert:sectigo-acme)# enroll
```

Via GUI:

- Go to **ADC > SSL Management > ACME Certificates**
- Select the certificate
- Click on “Enroll” listed under Actions for the certificate

You can follow the enrollment progress using the CLI command:

```
vThunder-LE2-Active-vMaster[7/2]# sh pki acme-cert log <certificate name> follow
```

There is no equivalent GUI menu to view the certificate enrollment progress.

Once the certificate has been obtained, you can confirm the status as follows:

```
vThunder-LE2-Active-vMaster[7/2]# sh pki acme-cert status
Certificate name: sectigo-acme  status: SUCCESS
  Last enrollment/renewal: SUCCESS
  Renew at: 2022-12-07 11:04:18
```

To display the list of certificates and keys available on the Thunder ADC:

```
vThunder-LE2-Active-vMaster[7/2]# sh pki cert
Name                Type                Expiration  Status
-----
sectigo-acme        certificate/key      Dec 11 22:33:41 2022 GMT  [Unexpired, Unbound]
```

Via GUI:

- Go to **ADC > SSL Management > SSL Certificates**

You can view detailed information about the certificate using the command:

```
vThunder-LE2-Active-vMaster[7/2]# sh pki cert <certificate name>
```

Via GUI:

You cannot view certificate details using the GUI. However, you can use the GUI to first export the certificate from the Thunder device, and then view it on your local computer:

- Go to **ADC > SSL Management > SSL Certificates**
- Select the certificate and click Export

Configure Virtual Port 443 under the VIP on Thunder ADC

Create a client SSL template consisting of this certificate and key:

```
slb template client-ssl sectigo-acme-template
certificate sectigo-acme key sectigo-acme
```

Create a service group:

```
slb service-group apache8080 tcp
member apache 8080
```

Under the virtual port 443 of the VIP, apply this service-group and client SSL template:

```
slb virtual-server vip 10.24.44.94
port 443 https
source-nat auto
service-group apache8080
template persist source-ip src-persist
template client-ssl sectigo-acme-template
```

Note: You can optionally choose to encrypt the traffic between the Thunder device and the backend web servers using a server SSL template. Refer to *ACOS Application Delivery Controller Guide* for details.

Via GUI:

- To create Client SSL template: Go to **ADC > Templates > SSL**, click Create and choose the type as Client SSL
- To create service-group: Go to **ADC > SLB > Service Groups**, click Create
- To add vport 443 under an existing VIP:
 - Go to **ADC > SLB > Virtual Servers**, select the VIP and click on Edit under Actions
 - In the **Virtual Port** section, click Create to add port 443 and enter the necessary details

Confirm that vport 443 is up:

```
vThunder-LE2-Demo-10.86-Active-vMaster[7/2]#sh slb virtual-server bind
Total Number of Virtual Services configured: 2
```

```
-----
*Virtual Server :vip 10.24.44.94      All Up

      +port 80  http ==>apache                State :All Up
      +apache:80                10.80.80.7          State :Up

      +port 443 https ==>apache8080          State :All Up
      +apache:8080              10.80.80.7          State :Up
```

Via GUI:

- Go to **ADC > SLB > Virtual Servers**
- Select the VIP and expand the list of vports under that VIP
- Verify the status is UP

Optional: Enable Integrated DDoS Protection

Thunder ADC provides integrated DDoS protection features and can be configured to defend against common DDoS attacks. To configure integrated DDoS protection, configure the following:

```
icmp-rate-limit 2000
!
ip anomaly-drop bad-content 24
ip anomaly-drop drop-all
ip anomaly-drop out-of-sequence 24
ip anomaly-drop zero-window 24
```

Via GUI:

- Go to **Security > DDoS**
- Enter the DDoS protection configuration

Verify Certificate and Private Key Have Been Synchronized to Standby Thunder ADC

Verify the private key and certificate obtained from Sectigo ACME server have been synchronized to the standby Thunder ADC:

```
vThunder-LE1-Standby-vBlade[7/1]# sh pki cert
Name                Type                Expiration  Status
-----
sectigo-acme        certificate/key      Dec 11 22:33:41 2022 GMT  [Unexpired, Bound]
```

Note: If you applied the Server SSL template, you would see the corresponding certificate and key listed as well in the above output.

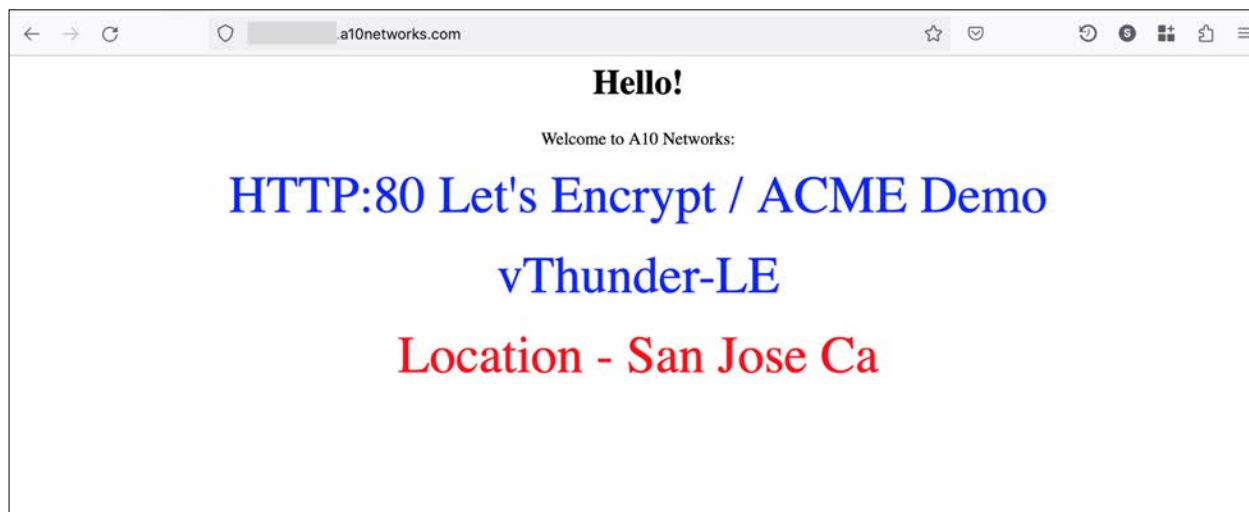
Via GUI:

On the standby Thunder device:

- Go to **ADC > SSL Management > SSL Certificates**

Verify web access to the domain

Go to the domain for which the certificate was provisioned using Sectigo Certificate Manager (SCM):



Click on the lock icon in the address bar to verify the certificate details.

Summary

This document describes how Thunder ADC can be used along with Sectigo Certificate Manager (SCM) for provisioning and automatic renewal of TLS/SSL certificates using the ACME protocol.

With a built-in ACME client, Thunder ADC greatly simplifies the process of issuance and renewal of certificates for securing traffic using TLS. In addition to this, deploying Thunder ADC provides the following benefits:

Multi/hybrid cloud deployment: Thunder ADC is available in multiple form factors (physical/virtual/container/bare metal/cloud), providing flexibility to deploy in multi-cloud and hybrid cloud environments with the same feature set. This enables consistent application and security policy enforcement irrespective of the public/private cloud in which it is deployed.

High application availability - With A10's VRRP-A feature, Thunder ADC offers high availability at the device level to ensure continued application availability within a data center or public/private cloud. In addition, with global server load balancing (GSLB) feature, customers can ensure high availability, fault tolerance, and the best user experience across multi-cloud and hybrid cloud deployments.

Centralized visibility and analytics: When deployed along with the A10 Harmony® Controller, network teams can get centralized traffic analytics for easier and faster troubleshooting, leading to a more consistent uptime and customer satisfaction.

Flexible licensing: A10's FlexPool®, a software subscription model, provides organizations the flexibility to allocate and distribute capacity across multiple sites as their business and application needs change.

For more information about Thunder ADC, please refer to:

<https://www.a10networks.com/products/thunder-adc/>

For more information on Sectigo Certificate Manager, please refer to:

<https://sectigo.com/enterprise-solutions/certificate-manager>

Appendix

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

vThunder-LE1

```
vrrp-a common
  device-id 1
  set-id 7
  enable
!
device-context 1
  vcs enable
!
device-context 2
  vcs enable
!
vcs floating-ip 10.22.10.90 255.255.252.0
!
vcs device 1
  priority 125
  interfaces management
  interfaces ethernet 2
  enable
!
vcs device 2
  priority 100
  interfaces management
  interfaces ethernet 2
  enable
!
multi-config enable
!
terminal idle-timeout 0
!
ip anomaly-drop bad-content 24
ip anomaly-drop drop-all
ip anomaly-drop out-of-sequence 24
ip anomaly-drop zero-window 24
!
ip dns primary 8.8.8.8
!
icmp-rate-limit 2000
!
device-context 1
  hostname vThunder-LE1
!
device-context 2
  hostname vThunder-LE2
!
device-context 1
  timezone America/Phoenix
```

```
!  
device-context 2  
    timezone America/Phoenix  
!  
ntp server time.google.com  
    prefer  
!  
glm use-mgmt-port  
glm enable-requests  
glm token <token-value>  
!  
device-context 1  
    interface management  
        ip address 10.22.10.88 255.255.252.0  
        ip default-gateway 10.22.8.1  
!  
device-context 2  
    interface management  
        ip address 10.22.10.86 255.255.252.0  
        ip default-gateway 10.22.8.1  
!  
interface ethernet 1/1  
    enable  
    ip address 10.24.44.92 255.255.255.0  
!  
interface ethernet 1/2  
    enable  
    ip address 10.80.80.1 255.255.255.0  
!  
interface ethernet 2/1  
    enable  
    ip address 10.24.44.155 255.255.255.0  
!  
interface ethernet 2/2  
    enable  
    ip address 10.80.80.2 255.255.255.0  
!  
vrrp-a vrid 0  
    floating-ip 10.80.80.3  
    device-context 1  
        blade-parameters  
            priority 150  
    device-context 2  
        blade-parameters  
            priority 250  
!  
device-context 1  
    vrrp-a peer-group  
        peer 10.22.10.86  
        peer 10.80.80.2  
!  
device-context 2
```

```
    vrrp-a peer-group
      peer 10.22.10.88
      peer 10.80.80.1
    !
  device-context 1
    ip route 0.0.0.0 /0 10.24.44.1
  !
  device-context 2
    ip route 0.0.0.0 /0 10.24.44.1
  !
  pki acme-cert sectigo-acme
    url https://acme.enterprise.sectigo.com/
    domain <domain-name>
    force
    log-level 2
    renew-before day 7
    cert-type rsa
    account-email <email-id>
    eab-key-id <key-id>
    eab-hmac-key encrypted <encrypted-hmac-key>
  !
  health monitor ping
  !
  health monitor http80
    method http
  !
  slb server apache 10.80.80.7
    health-check-disable
    port 80 tcp
      health-check-disable
    port 443 tcp
      health-check-disable
    port 8080 tcp
  !
  slb service-group apache tcp
    health-check-disable
    member apache 80
  !
  slb service-group apache8080 tcp
    member apache 8080
  !
  slb template client-ssl sectigo-acme-template
    certificate sectigo-acme key sectigo-acme
  !
  slb template persist source-ip src-persist
  !
  slb template virtual-port acme
    drop-unknown-conn
    reset-unknown-conn
  !
  slb virtual-server vip 10.24.44.94
```

```
port 80 http
  attack-detection
  source-nat auto
  service-group apache
  template virtual-port acme
  reply-acme-challenge
port 443 https
  source-nat auto
  service-group apache8080
  template persist source-ip src-persist
  template client-ssl sectigo-acme-template
!
sflow setting local-collection
!
sflow collector ip 127.0.0.1 6343
!
!
end
```

vThunder-LE2

```
vrrp-a common
  device-id 2
  set-id 7
  enable
!
device-context 1
  vcs enable
!
device-context 2
  vcs enable
!
vcs floating-ip 10.22.10.90 255.255.252.0
!
vcs device 1
  priority 125
  interfaces management
  interfaces ethernet 2
  enable
!
vcs device 2
  priority 100
  interfaces management
  interfaces ethernet 2
  enable
!
multi-config enable
!
terminal idle-timeout 0
!
```

```
ip anomaly-drop bad-content 24
ip anomaly-drop drop-all
ip anomaly-drop out-of-sequence 24
ip anomaly-drop zero-window 24
!
ip dns primary 8.8.8.8
!
icmp-rate-limit 2000
!
device-context 1
  hostname vThunder-LE1
!
device-context 2
  hostname vThunder-LE2
!
device-context 1
  timezone America/Phoenix
!
device-context 2
  timezone America/Phoenix
!
ntp server time.google.com
  prefer
!
glm use-mgmt-port
glm enable-requests
glm token <token-value>
!
device-context 1
  interface management
    ip address 10.22.10.88 255.255.252.0
    ip default-gateway 10.22.8.1
!
device-context 2
  interface management
    ip address 10.22.10.86 255.255.252.0
    ip default-gateway 10.22.8.1
!
interface ethernet 1/1
  enable
  ip address 10.24.44.92 255.255.255.0
!
interface ethernet 1/2
  enable
  ip address 10.80.80.1 255.255.255.0
!
interface ethernet 2/1
  enable
  ip address 10.24.44.155 255.255.255.0
!
interface ethernet 2/2
  enable
```

```
    ip address 10.80.80.2 255.255.255.0
!
vrrp-a vrid 0
  floating-ip 10.80.80.3
  device-context 1
    blade-parameters
      priority 150
  device-context 2
    blade-parameters
      priority 250
!
device-context 1
  vrrp-a peer-group
    peer 10.22.10.86
    peer 10.80.80.2
!
device-context 2
  vrrp-a peer-group
    peer 10.22.10.88
    peer 10.80.80.1
!
device-context 1
  ip route 0.0.0.0 /0 10.24.44.1
!
device-context 2
  ip route 0.0.0.0 /0 10.24.44.1
!
pki acme-cert sectigo-acme
  url https://acme.enterprise.sectigo.com/
  domain <domain-name>
  force
  log-level 2
  renew-before day 7
  cert-type rsa
  account-email <email-id>
  eab-key-id <key-id>
  eab-hmac-key encrypted <encrypted-hmac-key>
!
health monitor ping
!
health monitor http80
  method http
!
slb server apache 10.80.80.7
  health-check-disable
  port 80 tcp
    health-check-disable
  port 443 tcp
    health-check-disable
  port 8080 tcp
!
```



```
slb service-group apache tcp
  health-check-disable
  member apache 80
!
slb service-group apache8080 tcp
  member apache 8080
!
slb template client-ssl sectigo-acme-template
  certificate sectigo-acme key sectigo-acme
!
slb template persist source-ip src-persist
!
slb template virtual-port acme
  drop-unknown-conn
  reset-unknown-conn
!
slb virtual-server vip 10.24.44.94
  port 80 http
    attack-detection
    source-nat auto
    service-group apache
    template virtual-port acme
    reply-acme-challenge
  port 443 https
    source-nat auto
    service-group apache8080
    template persist source-ip src-persist
    template client-ssl sectigo-acme-template
!
sflow setting local-collection
!
sflow collector ip 127.0.0.1 6343
!
!
end
```

Learn More
About A10 Networks

Contact Us
[A10networks.com/contact](https://www.a10networks.com/contact)

©2023 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, Thunder TPS, A10 Harmony, SSLi 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/company/legal/trademarks/.

Part Number: A10-DG-16178-EN-01 FEB 2023