

ASA Anyconnect Remote Access via 365

[ASA Anyconnect Remote Access via 365](#)

[Introduction](#)

[Background](#)

[Network Design](#)

[Firewall DNS FQDN](#)

[Firewall Clock](#)

[CA Certificate](#)

[CA/CSR-generate/Download](#)

[Cert purchase/Download](#)

[Install CA and Identity Certs \(on ASA\)](#)

[Base ASA config](#)

[365 iDP certificate creation](#)

[365 Setup](#)

[Creation of 3 Enterprise Apps - one per pulldown](#)

[Populating Single Sign-on String in Each Enterprise Application](#)

[Populating pfx cert in Each Enterprise Application](#)

[Downloading pem certificate for ASA](#)

[ASA SAML Setup](#)

[Add Azure iDP cert to ASA](#)

[Configuring Azure as idp in ASA](#)

[Relevant strings](#)

[Adding Azure IDP under webvpn](#)

[Add ASA group-policies for each pulldown on the SAML/365 arrangement](#)

[Add tunnel-groups, associate with group-policies](#)

[365 - turn on Enterprise apps for whoever](#)

[Testing Anyconnect](#)

[Locking Down the ASA](#)

[Chromebooks and ipads](#)

[ASA Debugs](#)

[ASA show](#)

[365 certificate expiration](#)

Introduction

Background

In current versions of Cisco ASA firewall code, it is possible to configure single sign-on with SAML wherein Anyconnect and SSL-VPN firewall authentication are integrated with cloud Office 365 (or other cloud vendors) with SAML - Cisco documentation:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/vpn/asa-97-vpn-config/webvpn-cofigure-users.html#ID-2271-00000055>

[Note: This does *not* extend to ASDM - this is only for remote access such that specific 365 user accounts may access internal resources (behind the ASA) remotely.]

Advantages of 365 integration include:

- ability to require/allow password changes
- forgotten password resets without administrative involvement
- access control via accounts present in 365
- better visibility into account situation than with local ASA accounts
- integration with 365 2-factor authentication (text or Microsoft authenticator)
- ability to see Anyconnect traffic connection source by ip address in 365
- ability to see user Anyconnect pass/fail, access times in 365 logs

The ASA/365 arrangement can be used to differentiate access-to-the-network roles within the ASA by assigning different 365/SAML/Enterprise-Apps with different ASA pulldowns/group-policies/tunnel-groups.

If there is not a need for “roles”, i.e. a small network with a single administrator accessing inside resources, 365 and the ASA may be set up with a single SAML app and ASA policy.

The Anyconnect Enterprise apps within 365 can be turned on for any subset of 365 groups and/or users. One would not want “everyone” including students connecting to the ASA to access internal resources behind the ASA.

Tying Anyconnect authentication to 365 necessitates purchase/installation of a commercial Identity cert from a CA in lieu of the default/existing ASA self-signed certificate. An additional advantage of using a purchased identity cert from a CA is increased security, i.e. one would know one is really hitting the firewall instead of an imposter device. And users will not get the scary Anyconnect messages such as:

- Certificate does not match the server name
- Certificate is from an untrusted source

Disadvantages of using a purchased cert include cost (usually less than \$100/year) and maintenance of the certificate. While it is possible (and cheapest) to purchase an identity CA cert valid for 2 years (730 days) instead of one year, as of September 1, 2020, the CA/Browser forum suggests a shorter lifetime of 397 days:

<https://securityboulevard.com/2020/09/say-goodbye-to-2-year-certificates-and-hello-to-multi-year-ssl-plans/>

Use of a 1-year certificate is recommended as the industry is moving in that direction.

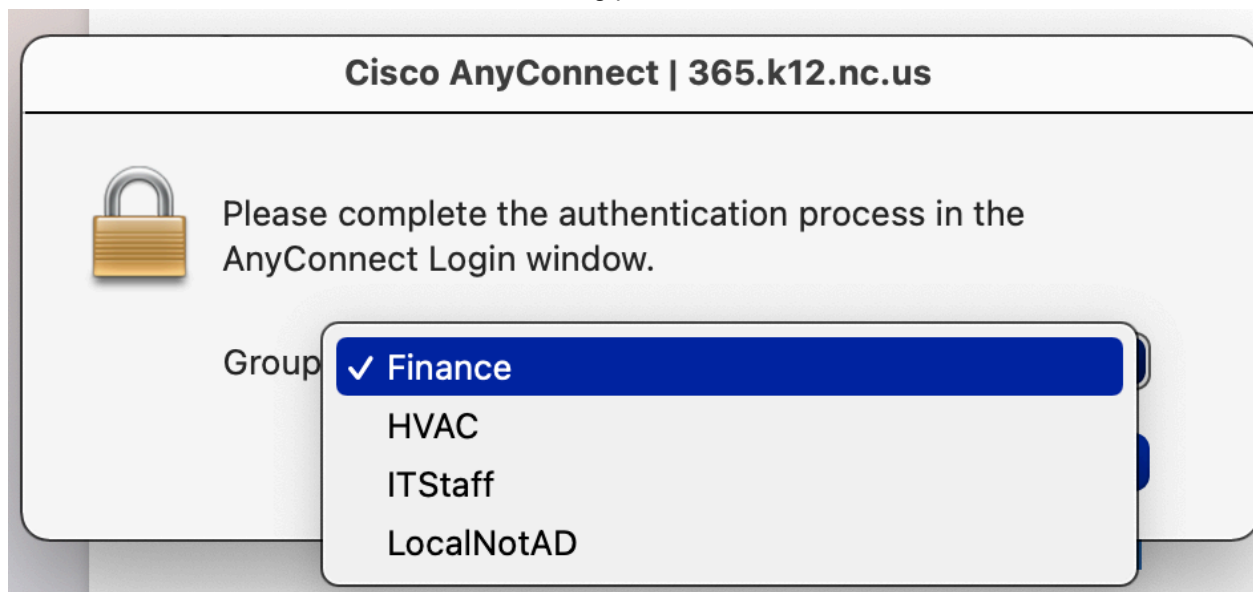
The configuration may be done via the ASDM gui in current code; we used ASDM 7.16.1 and ASA version asa9-12-4-7.

Network Design

In our example, we have 3 different roles within 365 and the ASA:

User Role	365 Enterprise App Name	365 Group	365 Test user	ASA Anyconnect Pulldown	School Network Access
Finance	CiscoAnyConnectFinance	Finance	cfo@k12o365.mcnc.org	Finance	192.168.50.12/32
HVAC	CiscoAnyConnect HVAC	Vendors	carrier@k12o365.mcnc.org	HVAC	192.168.50.40/32
IT	Cisco AnyConnect ITStaff	Admins	ddunlap@k12o365.mcnc.org	ITStaff	192.168.50.0/24

When the 3 different roles are added to the existing pulldown, the finished interface will look like this:



Firewall DNS FQDN

In order to obtain the purchased identity certificate from a CA vendor, the existing firewall will need to have a resolvable FQDN. Our firewall's hostname is:

365

And its domain:

domain-name k12.nc.us

Our FQDN 365.k12.nc.us resolves to 152.26.31.109

As configured by DIT, firewall hostnames are typically something like k12-9999-fw with domain k12.nc.us. If this is the convention on your firewall, you may open a ticket with MCNC to create a DNS entry for your firewall such as:

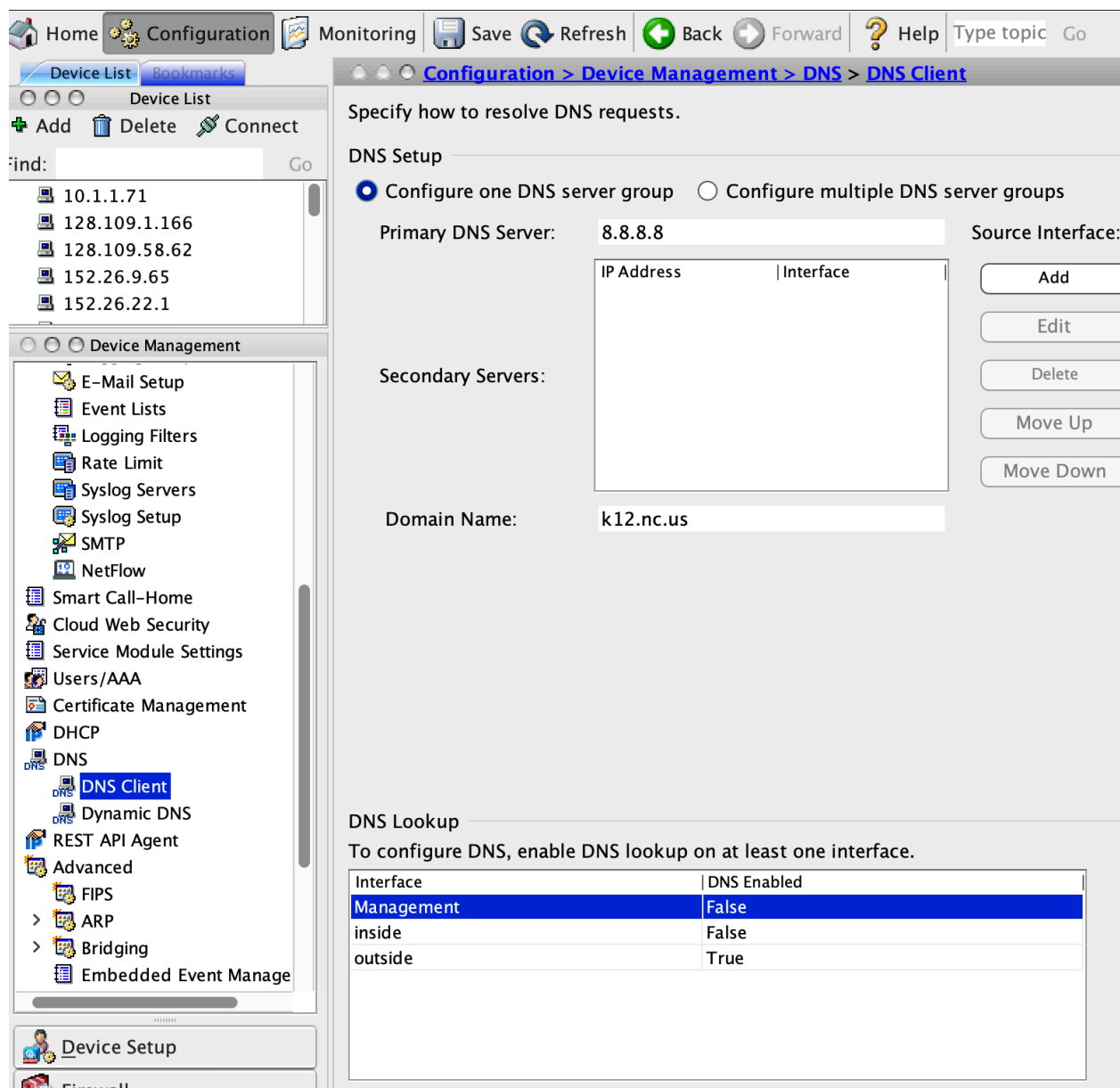
365.k12.nc.us = 152.46.31.109 (or whatever the outside ip address is for your firewall)

If you manage your own DNS, you can do the same.

The hostname and domain can be changed/checked in ASDM under Configuration > Device setup:



The firewall needs to be able to resolve its own name. Under Config > Device management > DNS, we tell the firewall to query DNS on the outside interface:



After doing this in ASDM, the CLI configuration shows:

```
hostname 365
```

```
domain-name k12.nc.us
```

```
dns domain-lookup outside
```

```
dns server-group DefaultDNS
```

```
name-server 8.8.8.8
```

After this is configured on the firewall, the firewall should be able to ping itself by FQDN and other devices should be able to ping the firewall by FQDN.

```
365# ping 365.k12.nc.us
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 152.46.31.109, timeout is 2 seconds:

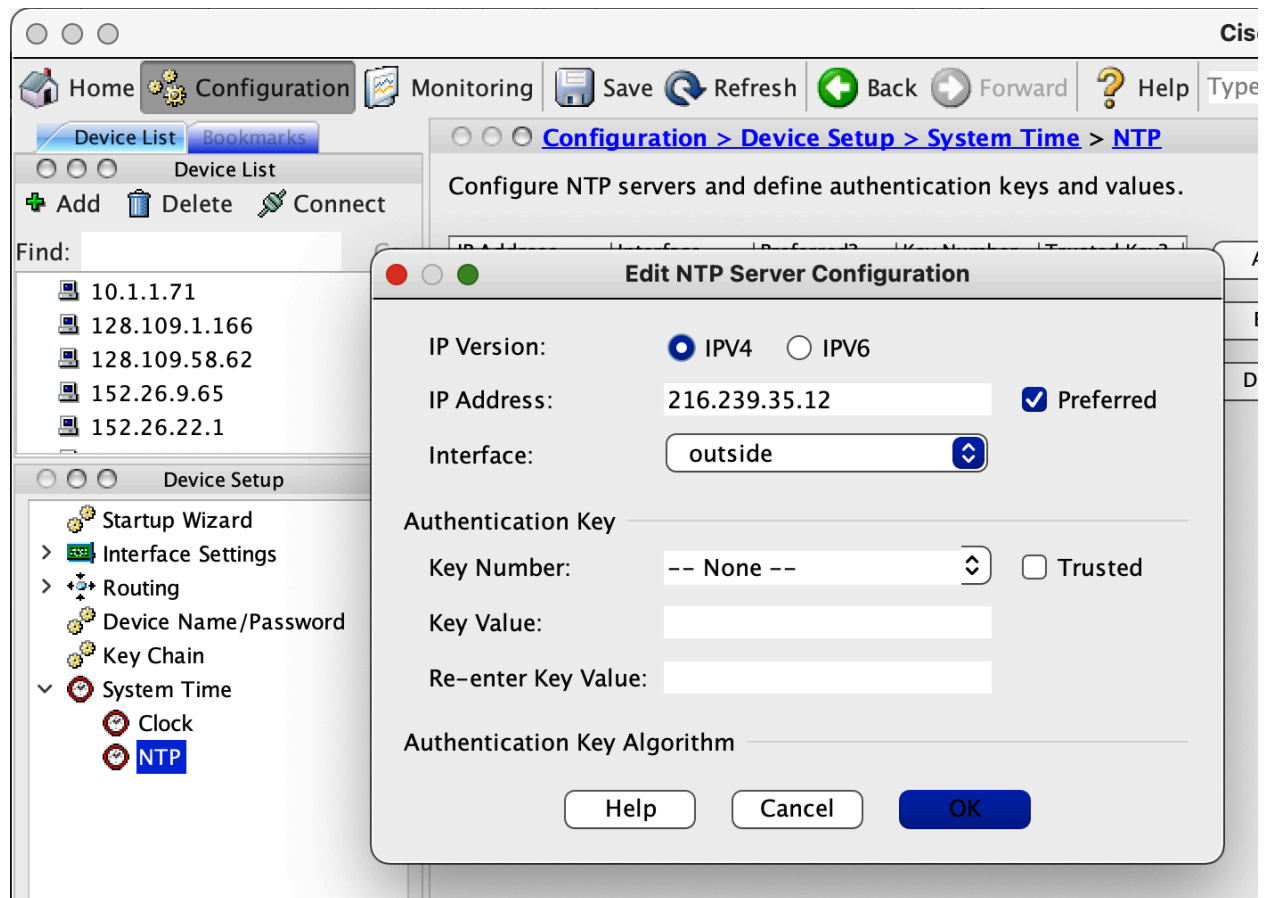
!!!!

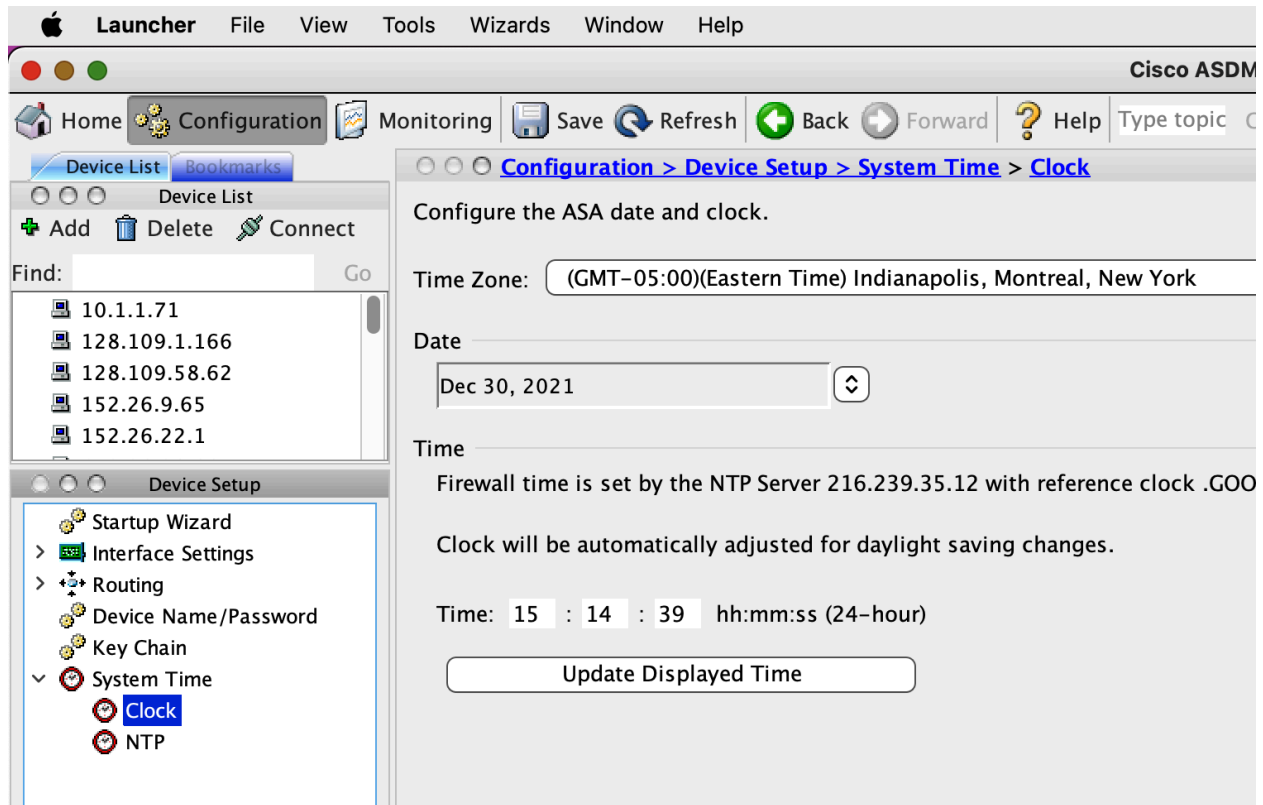
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

365#

Firewall Clock

As certificates are time-sensitive, you need to configure ntp server on the ASA if this is not already done, for example in Configuration > Device setup > NTP:





Our resulting configuration has:

```
name 216.239.35.12 time.google.com
ntp server time.google.com
```

```
clock timezone EST -5
clock summer-time EDT recurring
```

“show clock” should show the correct time.

```
365# sho clock
```

```
11:24:48.227 EST Fri Dec 31 2021
```

CA Certificate

CA/CSR-generate/Download

Because the ASA self-signed certificates are good for 10 years which is in excess of the current industry-standard 397-day maximum and there was observed twitchiness with their use, the self-signed certificate may be left on the ASA but you will need to obtain a purchased CA certificate and configure as the trustpoint.

We explored "Let's Encrypt" as those certificates are free and do work but the problem there is they expire every 3 months and require some sort of server and "bot" activity to refresh on an ASA.

We tried a wildcard certificate (for example, *.k12.nc.us) but there were security concerns with that solution; some device-types require the certificate to contain a Subject Alternative Name (SAN); not all commercial certificate vendors offer wildcard certificates; and not all vendors who provide wildcard certificates include a SAN. However, per Cisco, wildcard certificates will work.

The decision to use a firewall-specific GoDaddy certificate was based on market-share and price.

Certificate vendors by market-share are:

1. Sectigo
2. DigiCert
3. GoDaddy
4. The USERTRUST Network
5. Starfield Technologies
6. GlobalSign

Our purchase was a "1 Year Standard SSL Certificate" from GoDaddy - these are usually less than \$90 annually.

After payment for the certificate, GoDaddy instructions at:

<https://www.godaddy.com/help/generate-a-csr-certificate-signing-request-for-my-cisco-asa-5500-vpnfirewall-32068>

were used to generate a certificate-signing-request (CSR) on the ASA and submit it to GoDaddy for issuance.

The ASA's CSR would be generated by DIT if your firewall is DIT-managed.

This describes CSR generation in ASDM.

In Identity certificate > Add > CSR generation, in addition to our *CN=365.k12.nc.us* parameter for the cert, we added:

O=MCNC

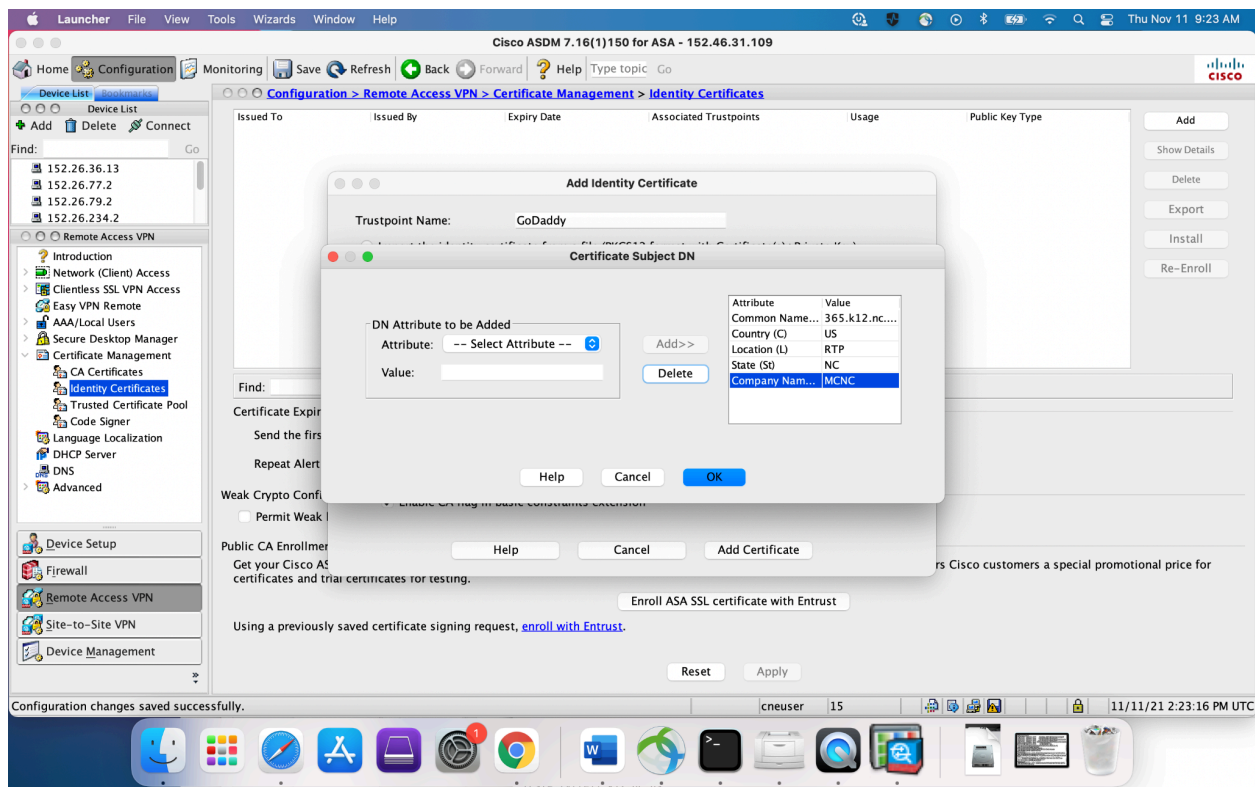
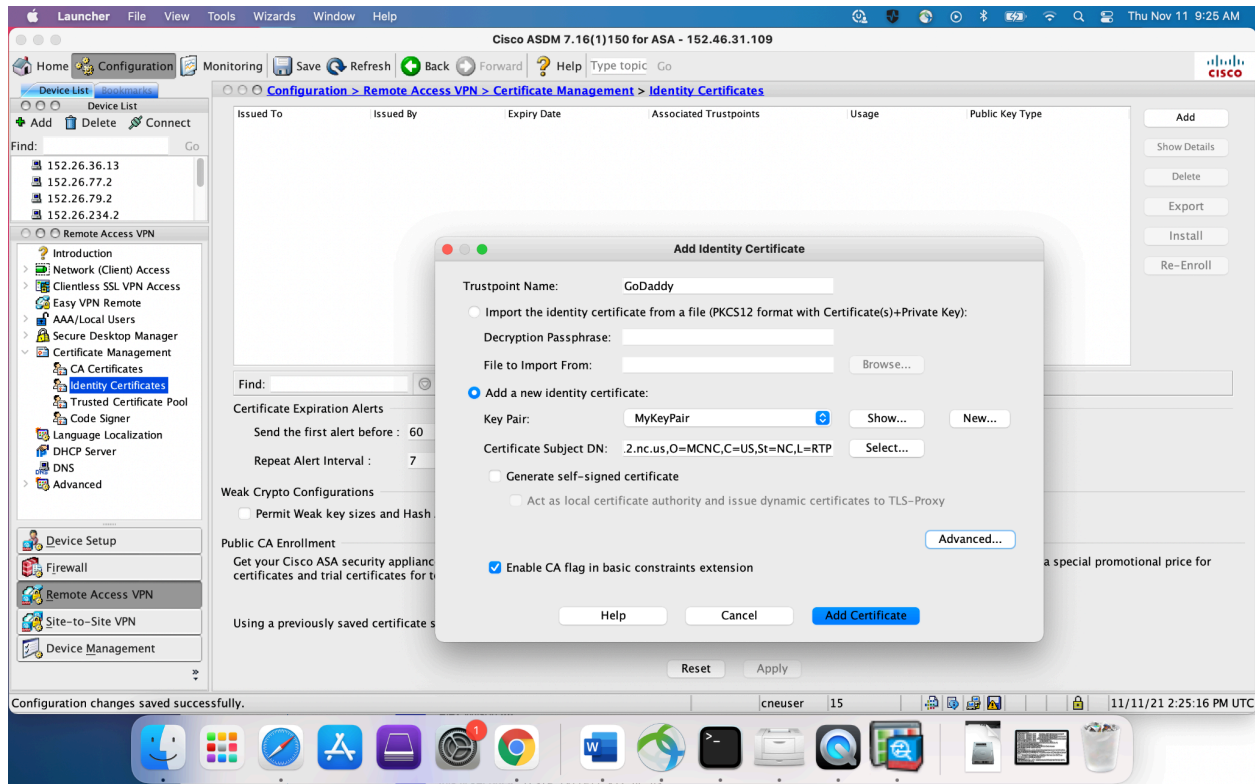
C=US

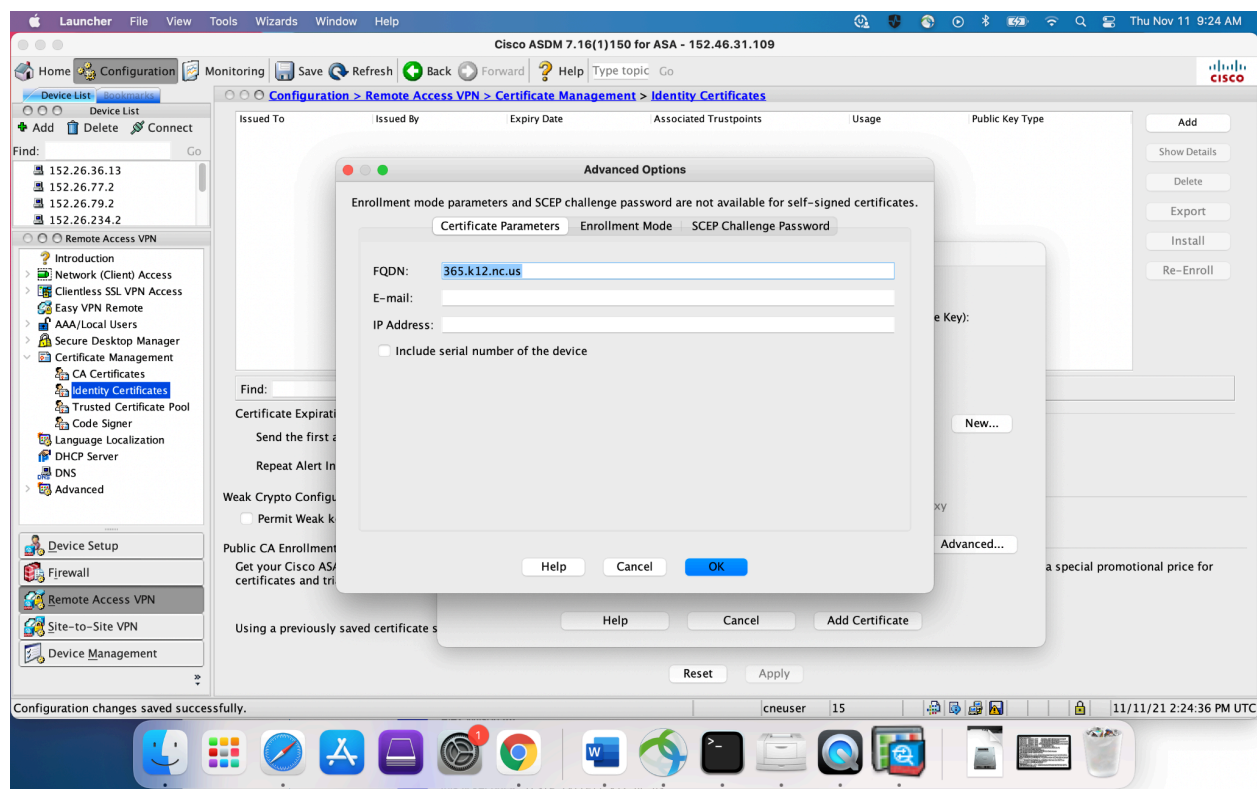
St=NC

L=RTP

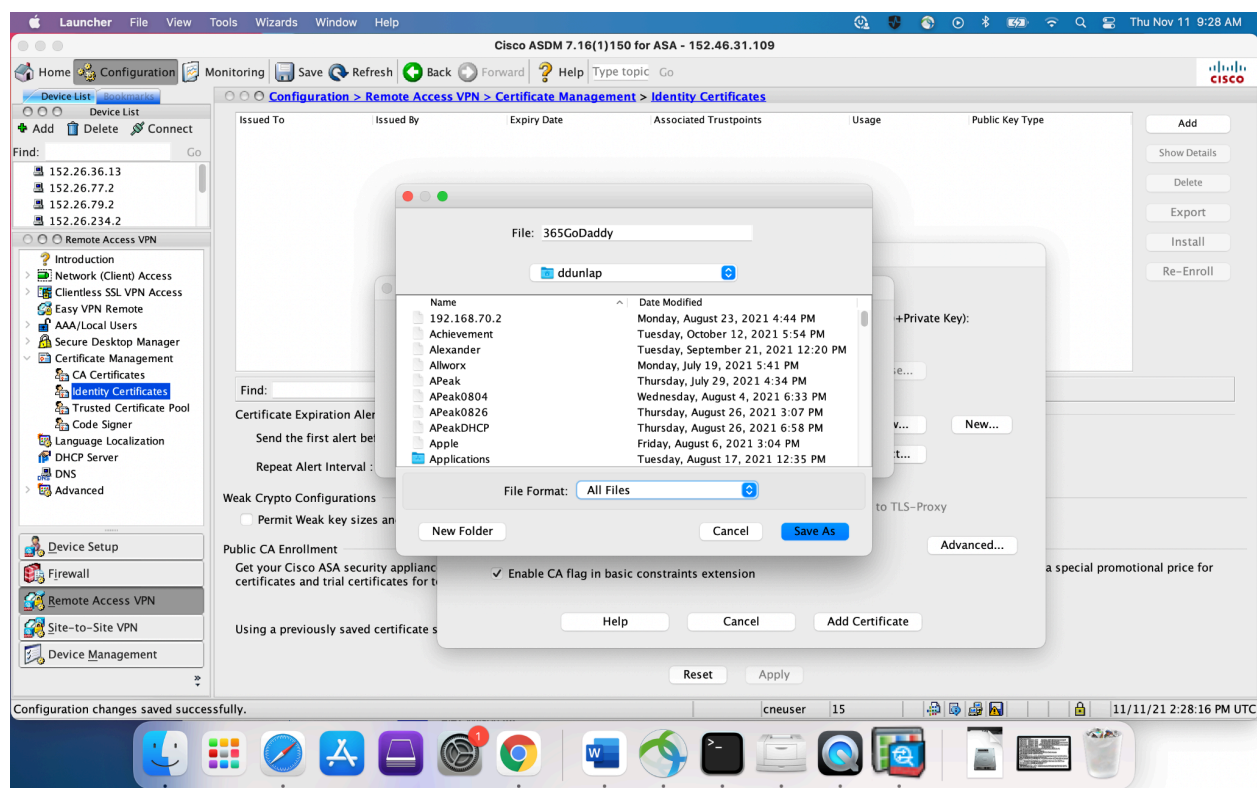
We told the ASA not to include its serial number in the CSR, thinking that hardware replacement with a different serial number could nullify the certificate.

The GoDaddy instructions say 'generate now' on the CSR - in current ASDM, this is - 'add identity certificate'. When choosing that, commands are delivered to ASA then there's the option of saving the CSR. This is a screenshot of ASDM CSR generation using the 5 CSR parameters and a chosen key-pair:



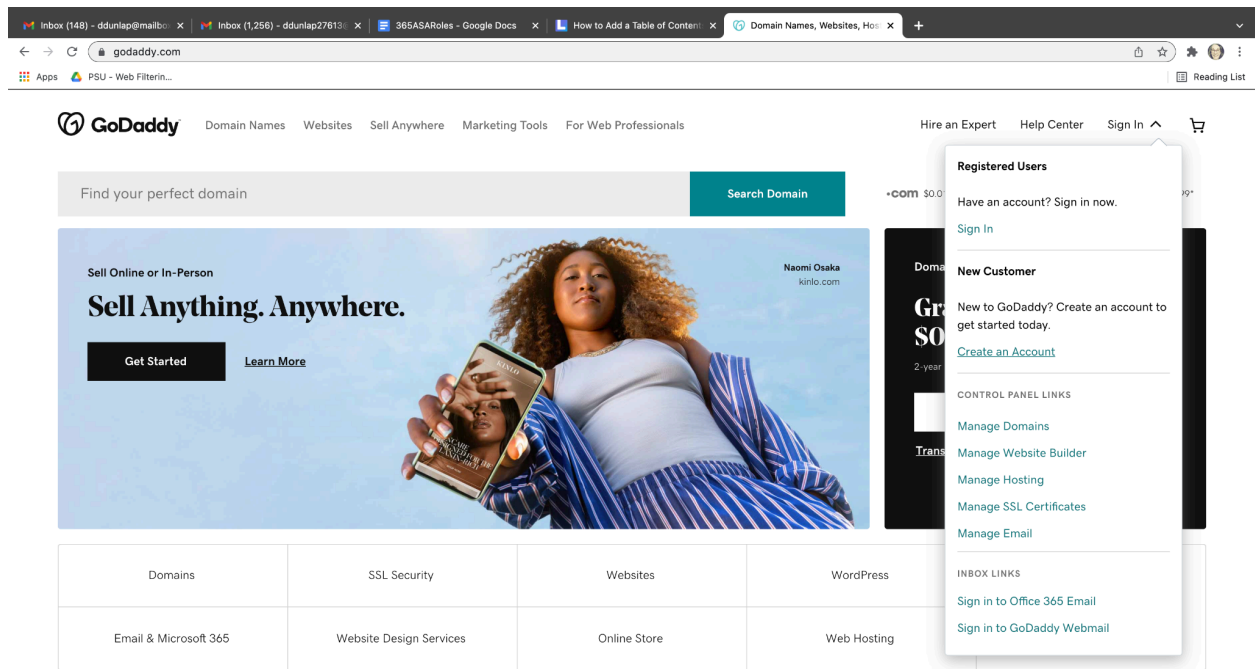


At the end of the process, you need to save the generated CSR locally as shown here:



Cert purchase/Download

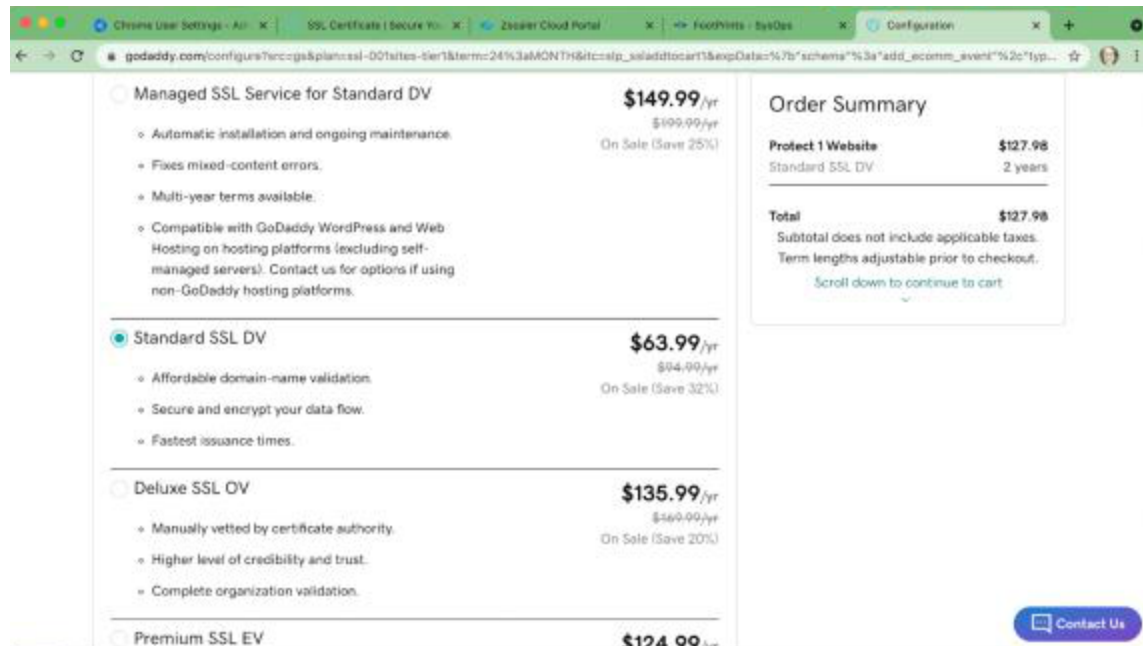
You will need to create an account on GoDaddy to purchase the certificate. There is a 'create an account' option at <https://www.godaddy.com/web-security/ssl-certificate>:



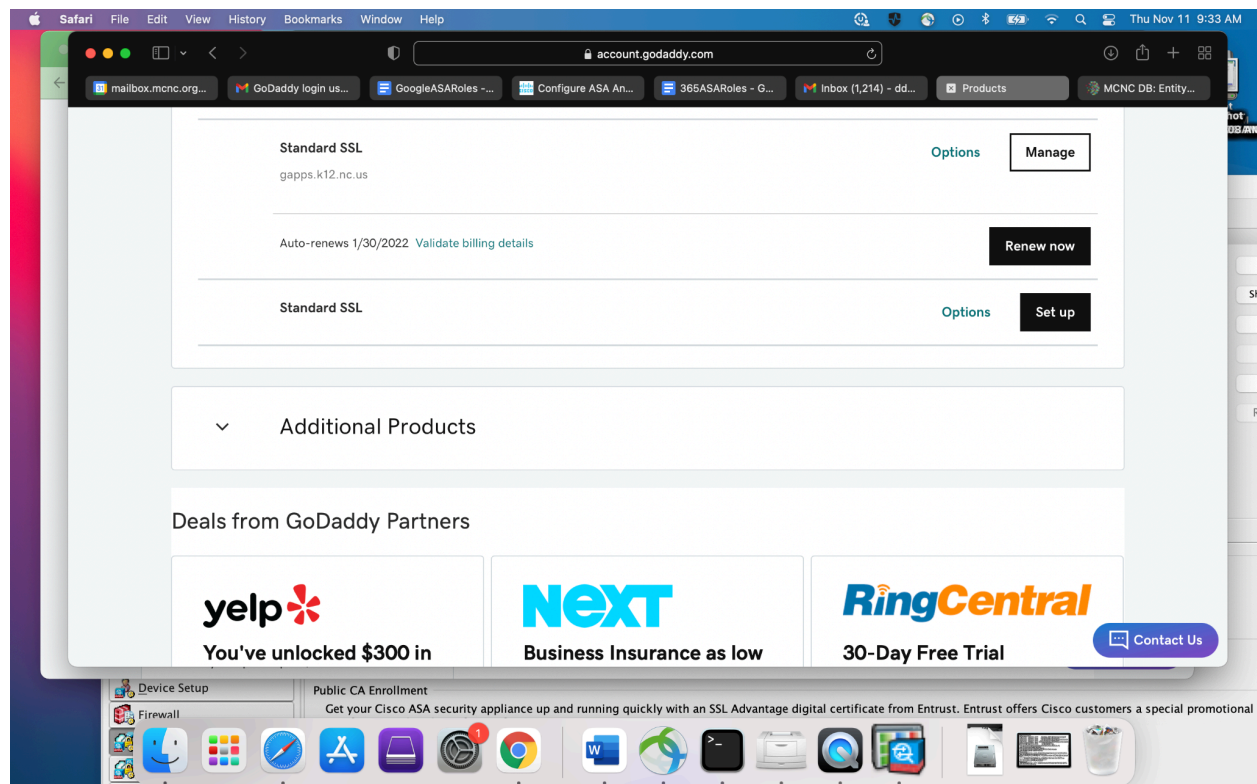
Success in 3 easy steps.

<https://sso.godaddy.com/account/create?realm=idp&path=%2Fproducts&app=account>

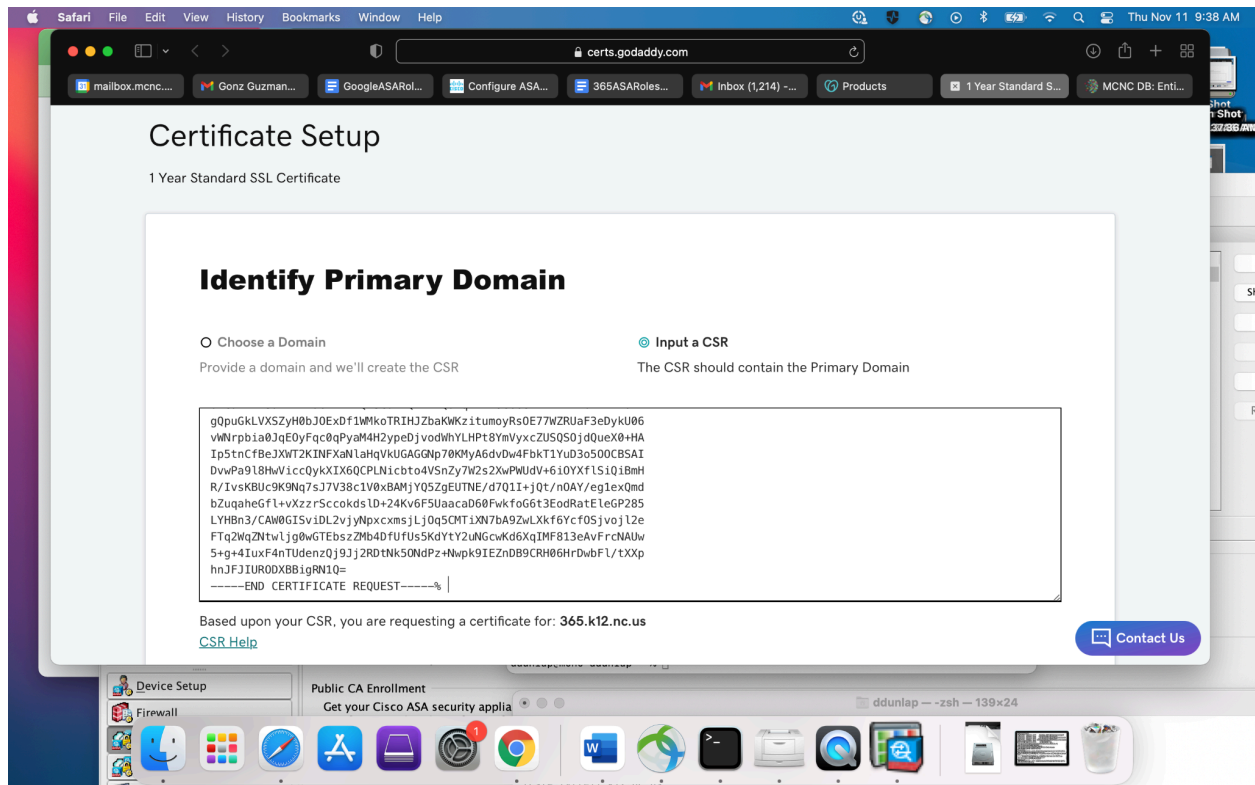
The Standard SSL DV certificate option shown below will suffice (price may vary):



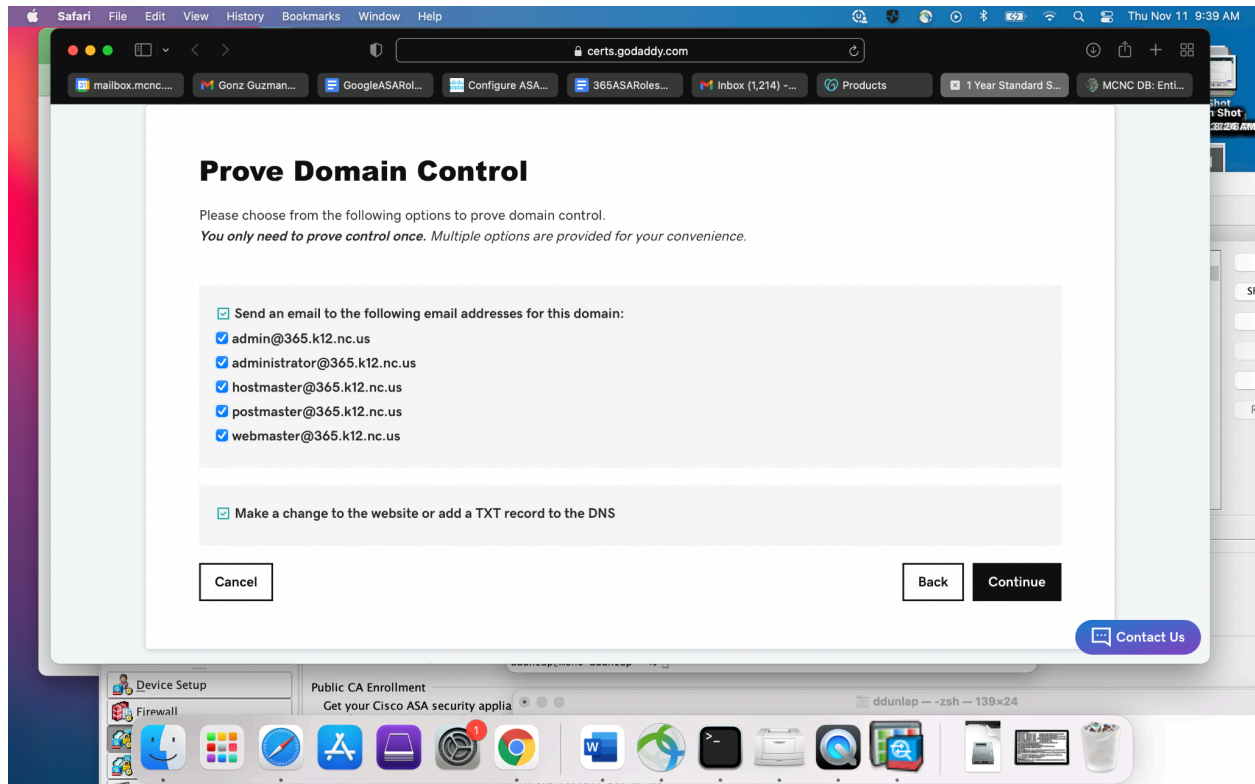
After the purchase, you should receive an email directing you to log in to GoDaddy to configure the cert, i.e. "Set up" the Standard SSL cert which you purchased - we follow their email link to:



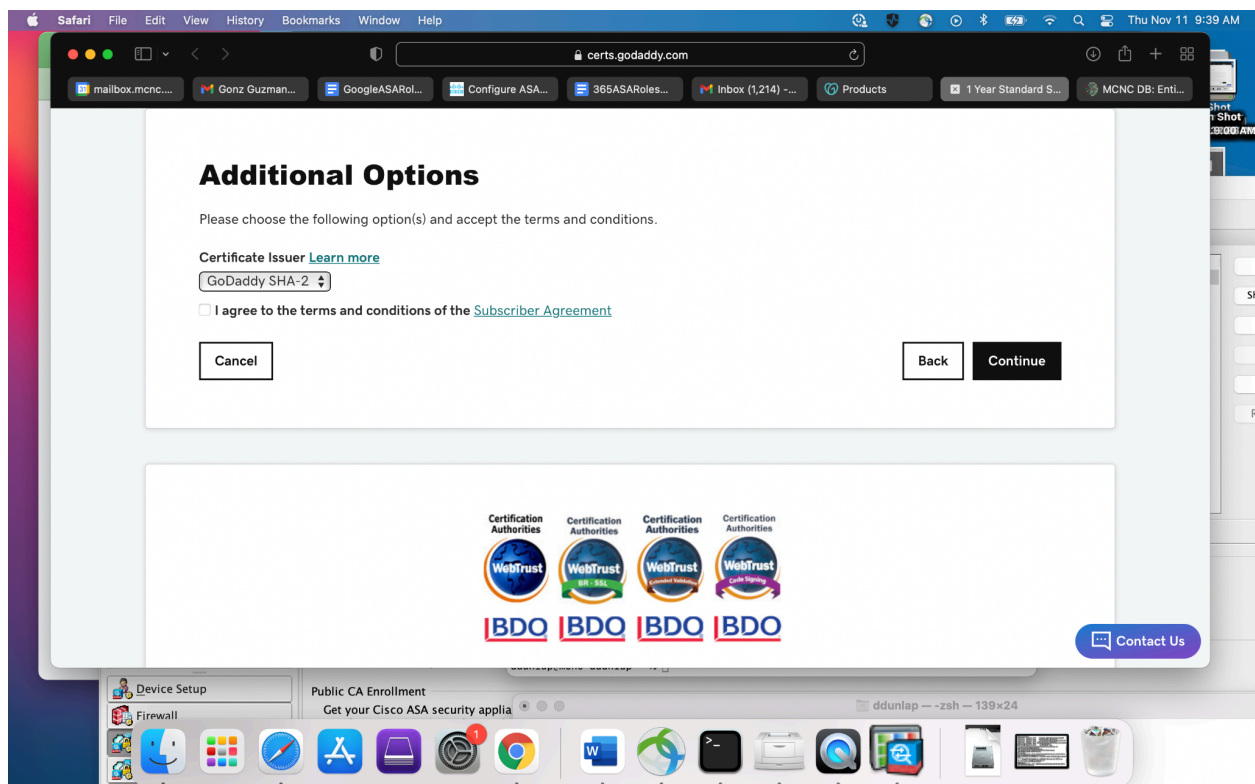
When we hit the 'Set up' button, this brings us to the screen where we can use our CSR. Since we saved our CSR from the ASA as file 365GoDaddy.txt we bring up that file and paste the BEGIN to END and all in-between:

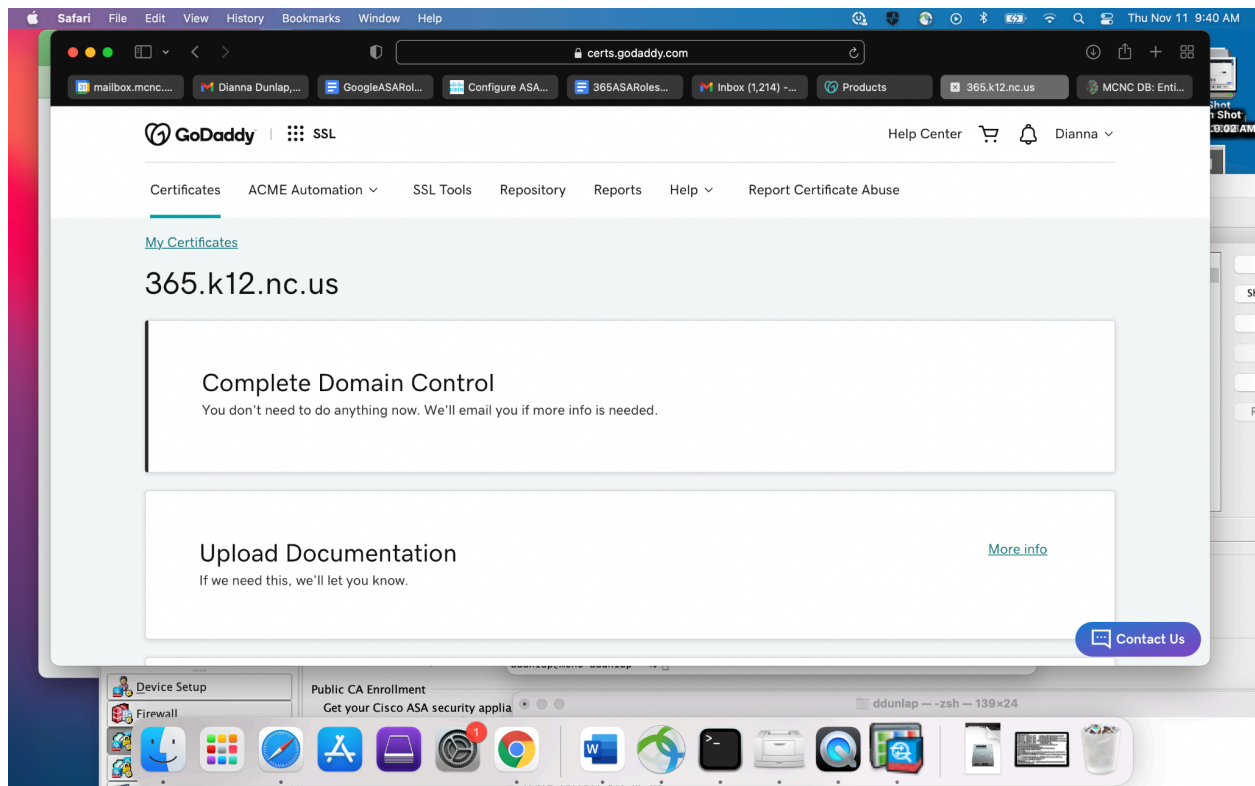
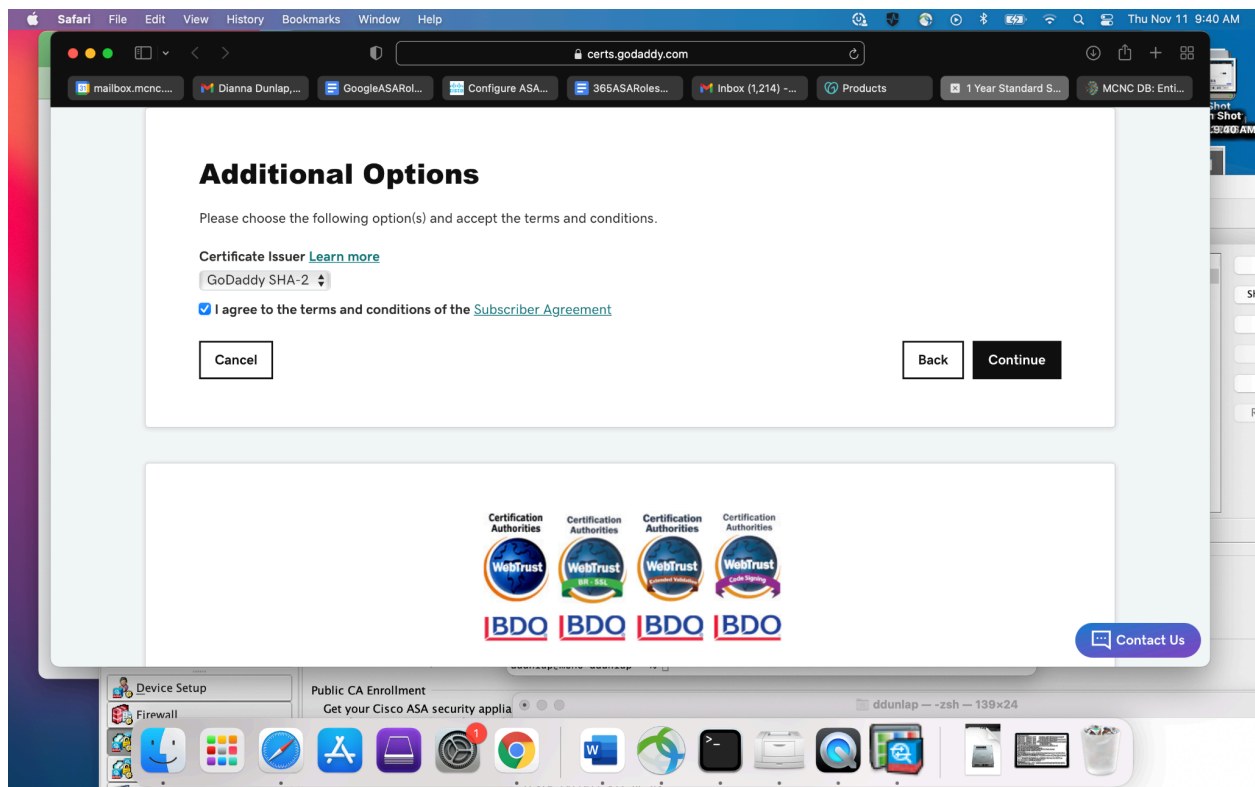


On Save/Submit, GoDaddy will display a warning about who will get email for domain verification:



On Continue, you would see and agree to the conditions:



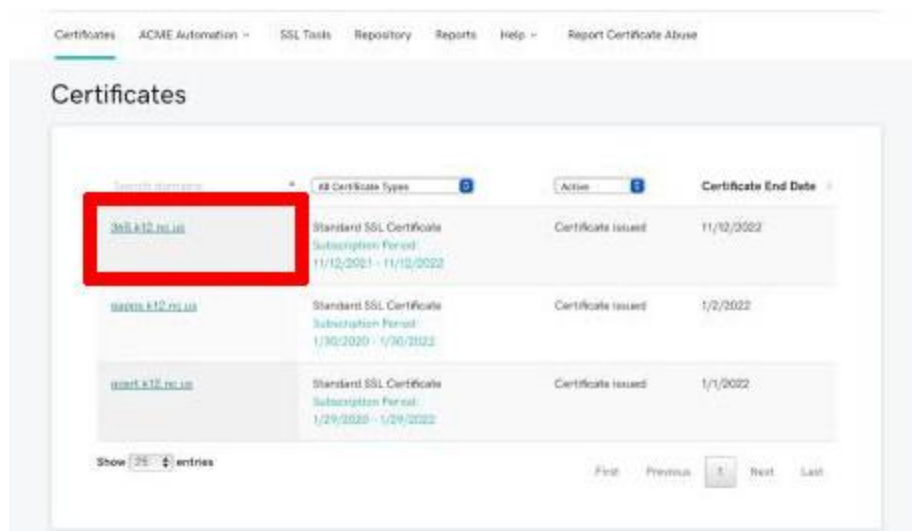


The screen shown above which says “You don’t need to do anything now” means the email has been sent to the domain owner, i.e. the [admin@](#), [administrator@](#), [hostmaster@](#), [postmaster@](#), [webmaster@](#) seen above. If “that is not you”, you would need to contact that person to alert them of the need to do domain verification.

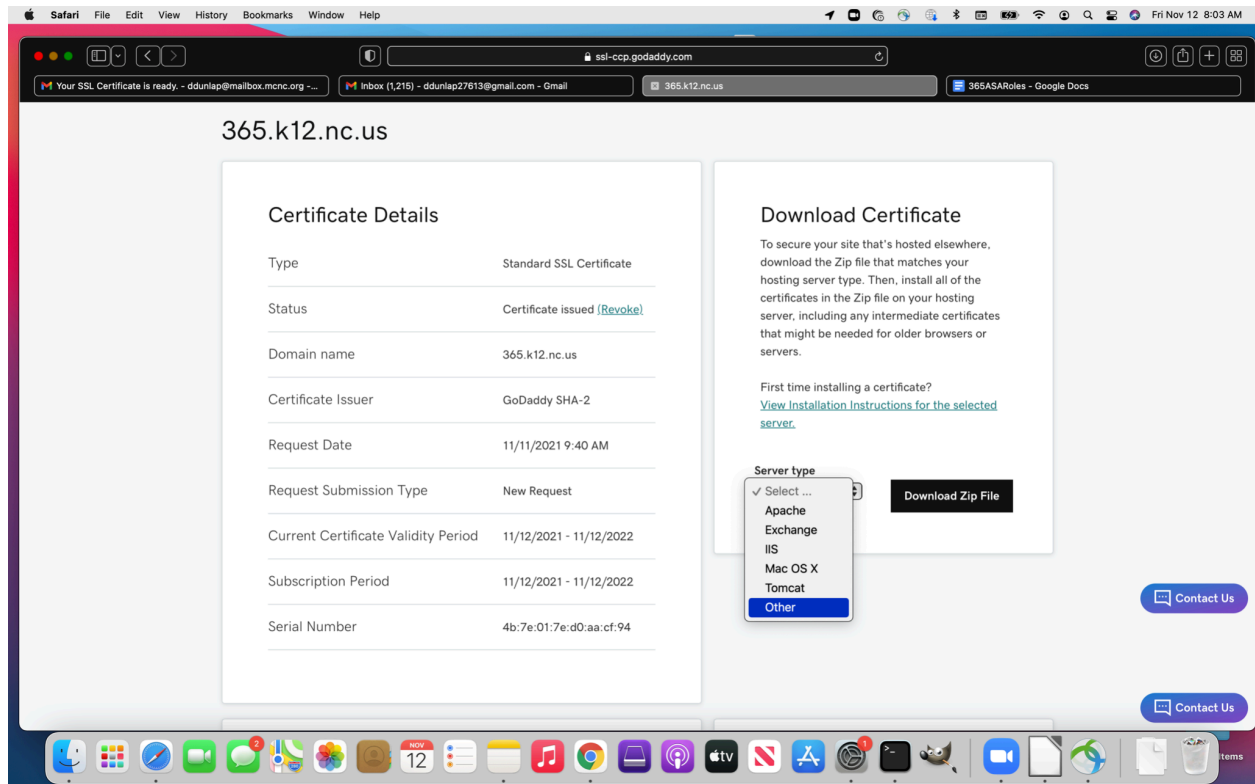
Our domain-owning person receives the request and approves, i.e. our [admin@365.k12.nc.us](#) is someone other than us.

Our domain-owning person also controls our DNS and adds the txt record GoDaddy needs as directed.

After our domain-owning person does the DNS piece, you will receive notification via GoDaddy email that the certificate is available for download with a link. On going to our link, this shows 3 certificates - we expand our 365.k12.nc.us one:



and download certificate zip bundle as type 'Other':



The above GoDaddy instructions reference unzipping the downloaded certificate file. When the certificate bundle is in-hand and unzipped, it should contain 3 files - yours would have names different than ours:

2f7eaf48dc4a3d91.crt

2f7eaf48dc4a3d91.pem

gd_bundle-g2-g1.crt

The *gd_bundle-whatever.crt* is the CA certificate referenced in the GoDaddy documentation. The *random#.crt* is the Identity certificate referenced in the GoDaddy documentation.

We did not have to use the .pem certificate.

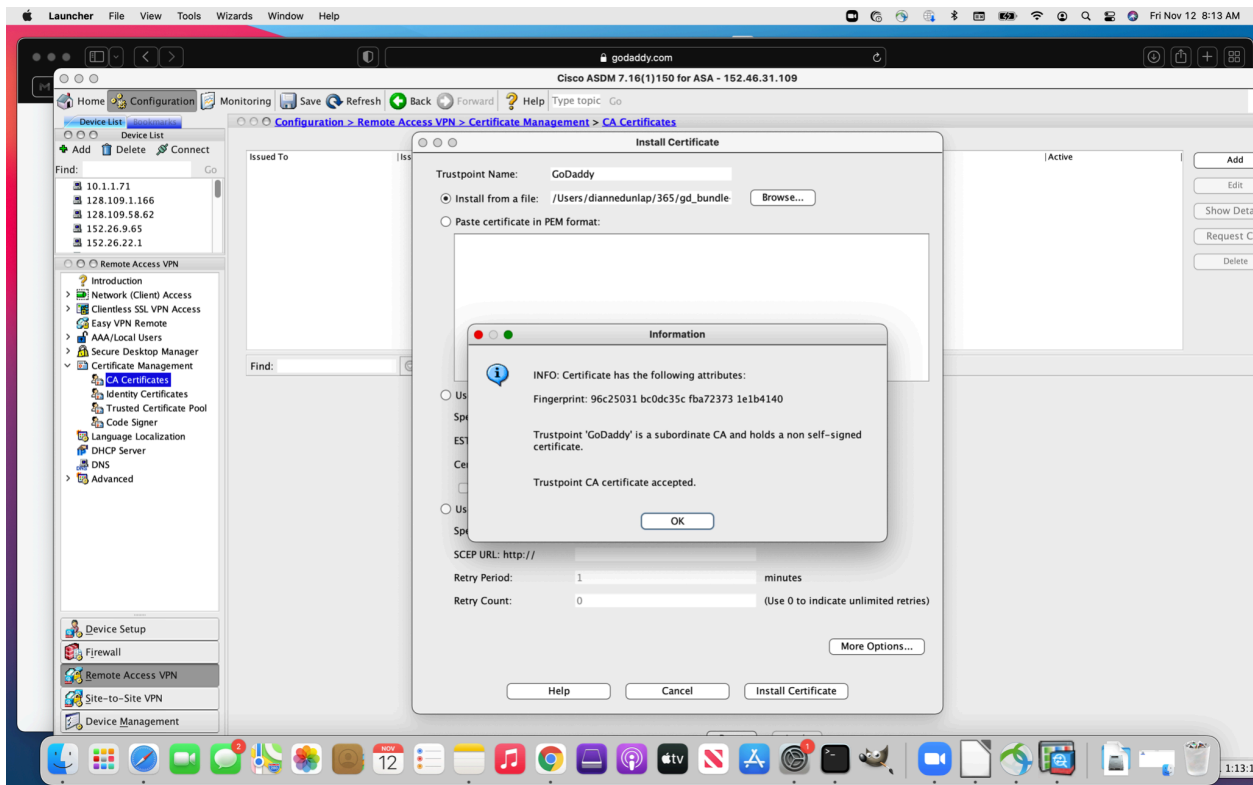
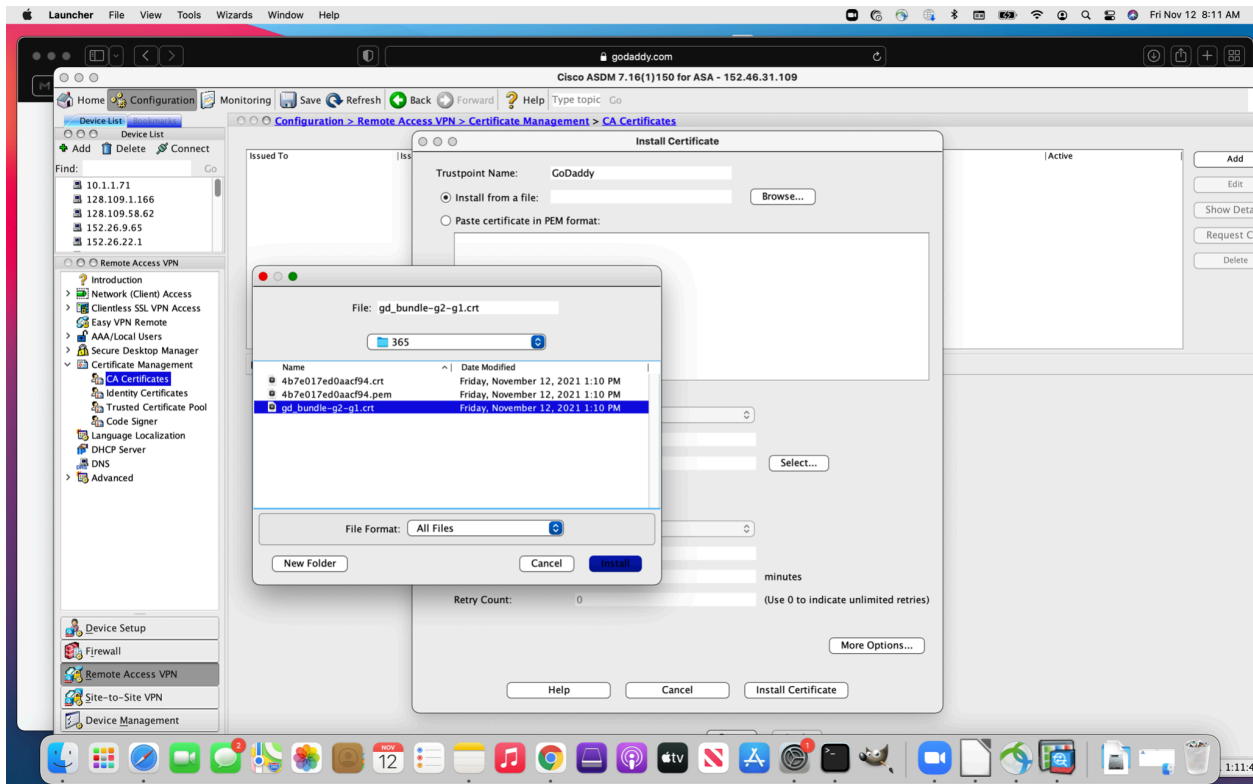
Install CA and Identity Certs (on ASA)

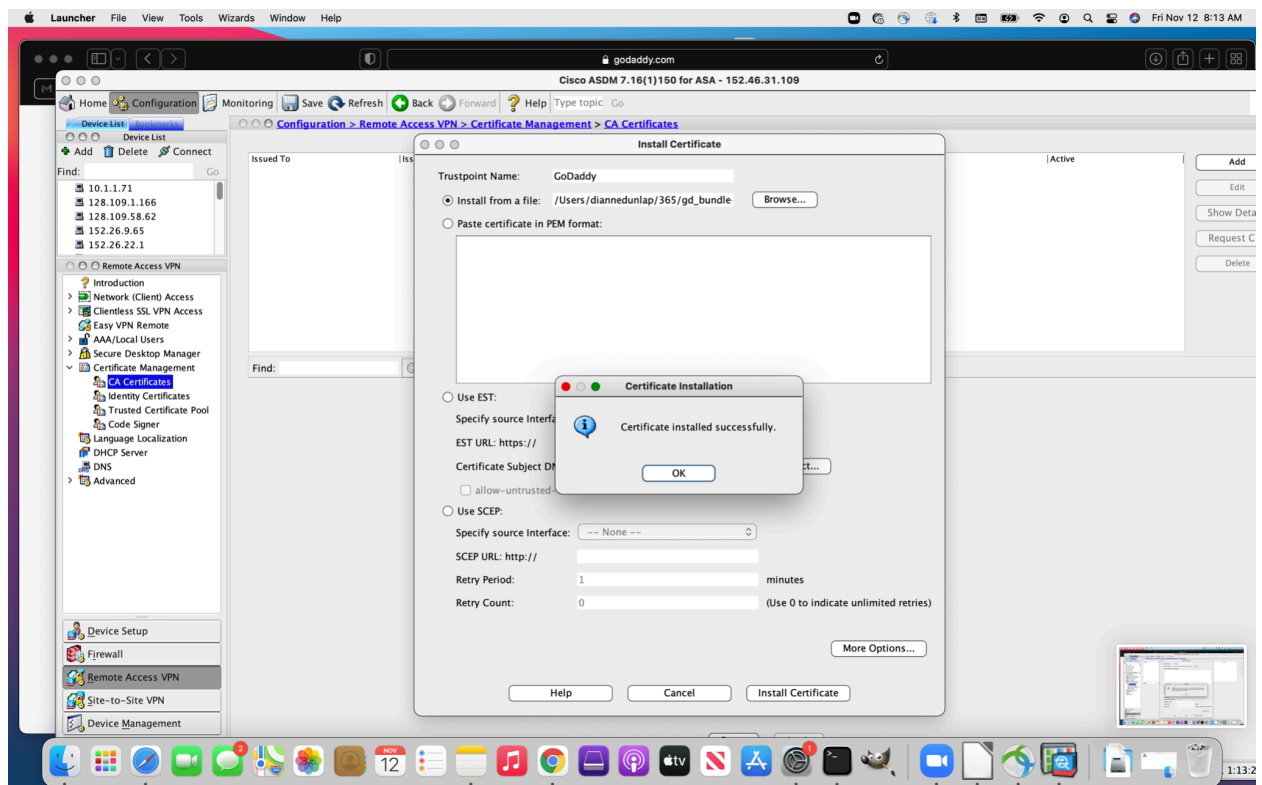
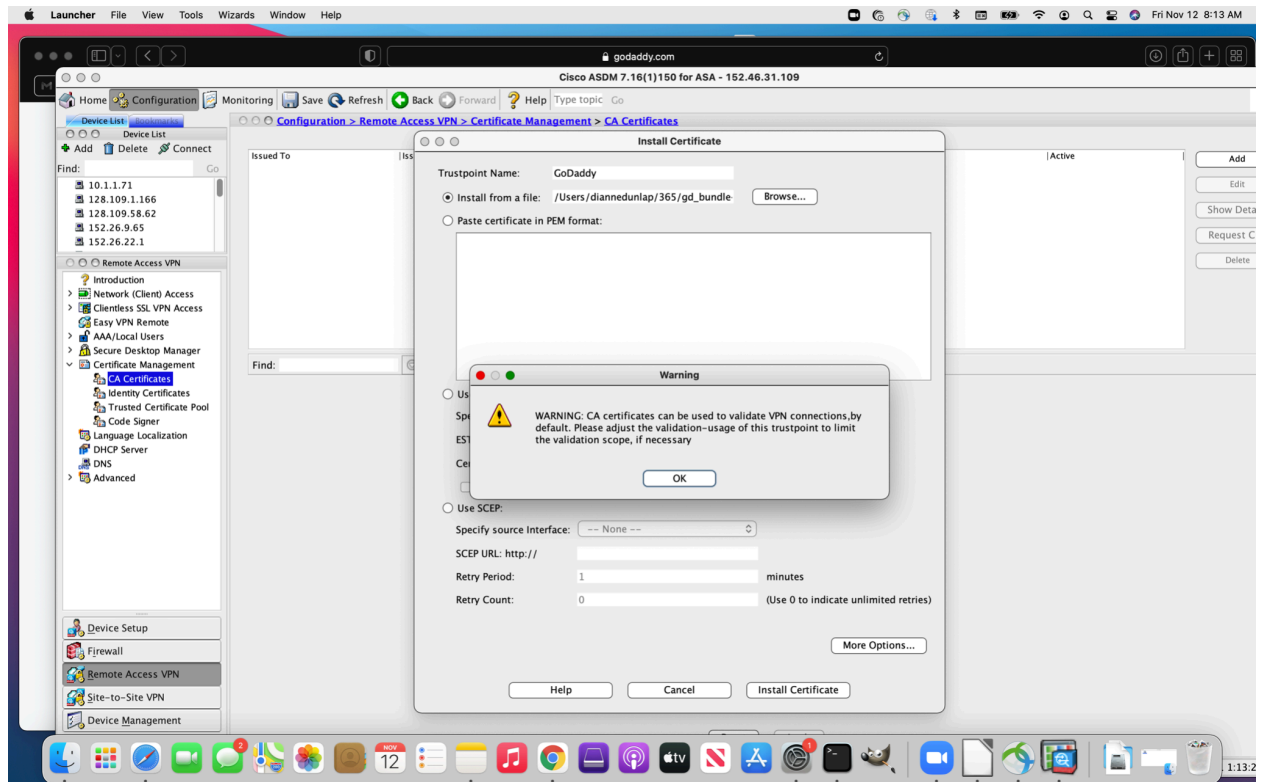
The instructions at:

<https://www.godaddy.com/help/manually-install-an-ssl-certificate-on-my-cisco-asa-5500-vpnfirewall-32070>

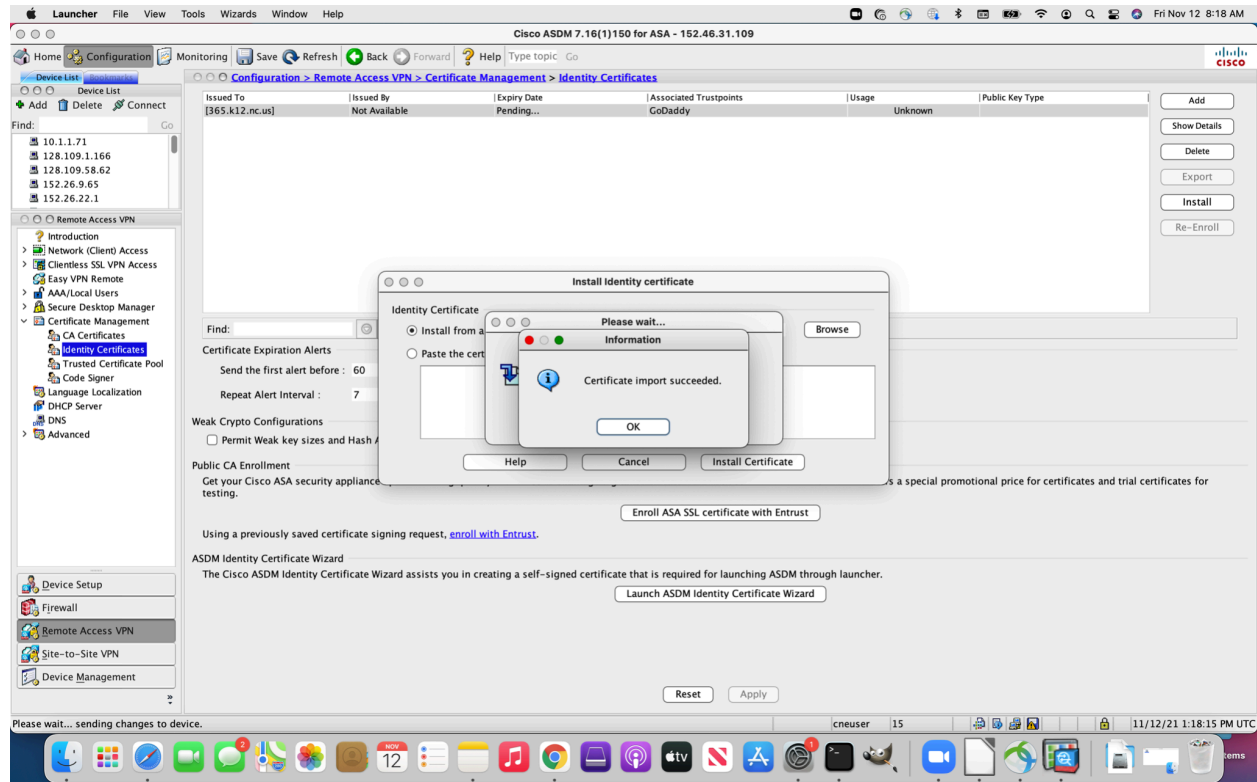
Illustrate installation of the GoDaddy certificates on the ASA as do the screenshots below.

Under ASDM Remote access > Certificates > CA certificate > we upload the *gd_bundle-g2-g1.crt* cert from our zip:



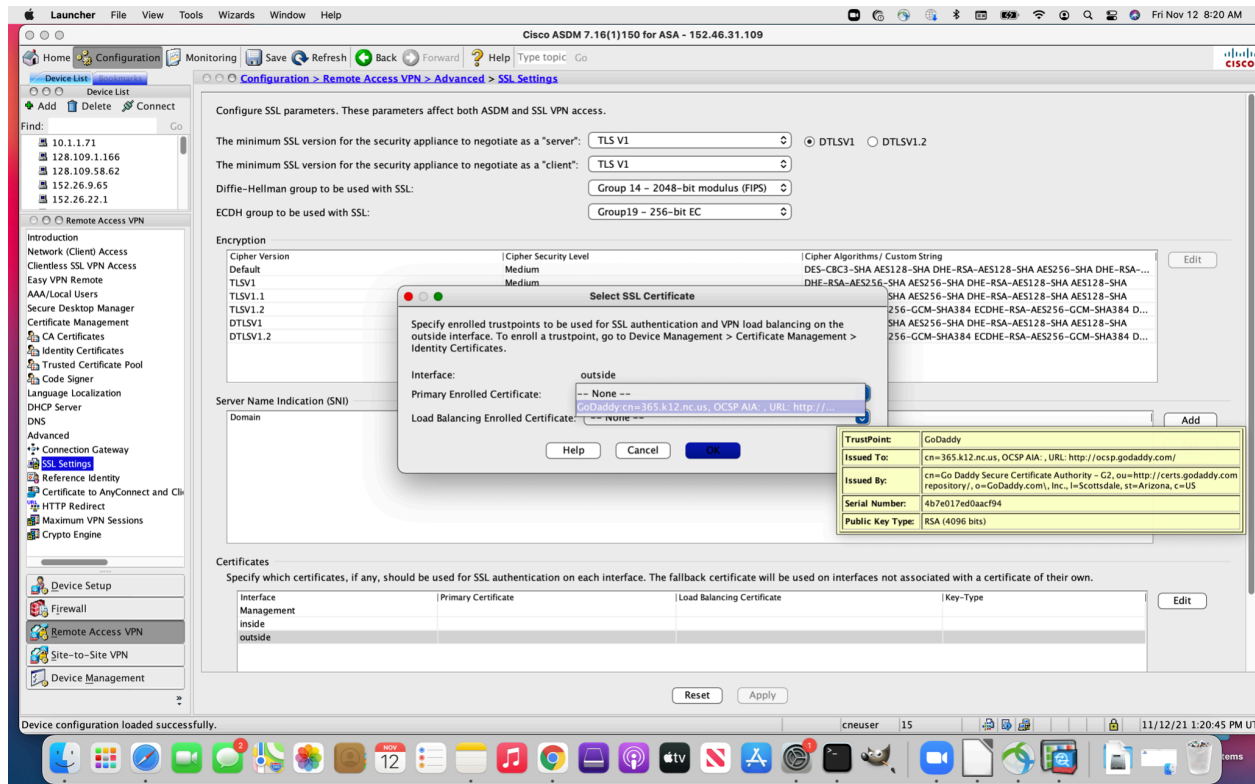


Then we go into Remote access > Certificates > Identity certificates, highlight the GoDaddy entry associated with the CSR then import the <random#>.crt identity cert.



Apply/save everything.

The GoDaddy instructions mention adding the Identity trustpoint to the outside interface - this can be done in Remote SSL > Configuration > Advanced:



Or via the command-line:
`ssl trust-point GoDaddy outside`

Base ASA config

After the CA (GoDaddy) cert installation, the scary messages about 'connection is not private' should go away when Anyconnecting to 365.k12.nc.us.

We assume that Anyconnect has previously been configured with local accounts and the VPN is currently working. In our case, the base configuration is:

```
group-policy LocalNotAD internal
group-policy LocalNotAD attributes
wins-server none
dns-server value 8.8.8.8
vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value LSplit
```

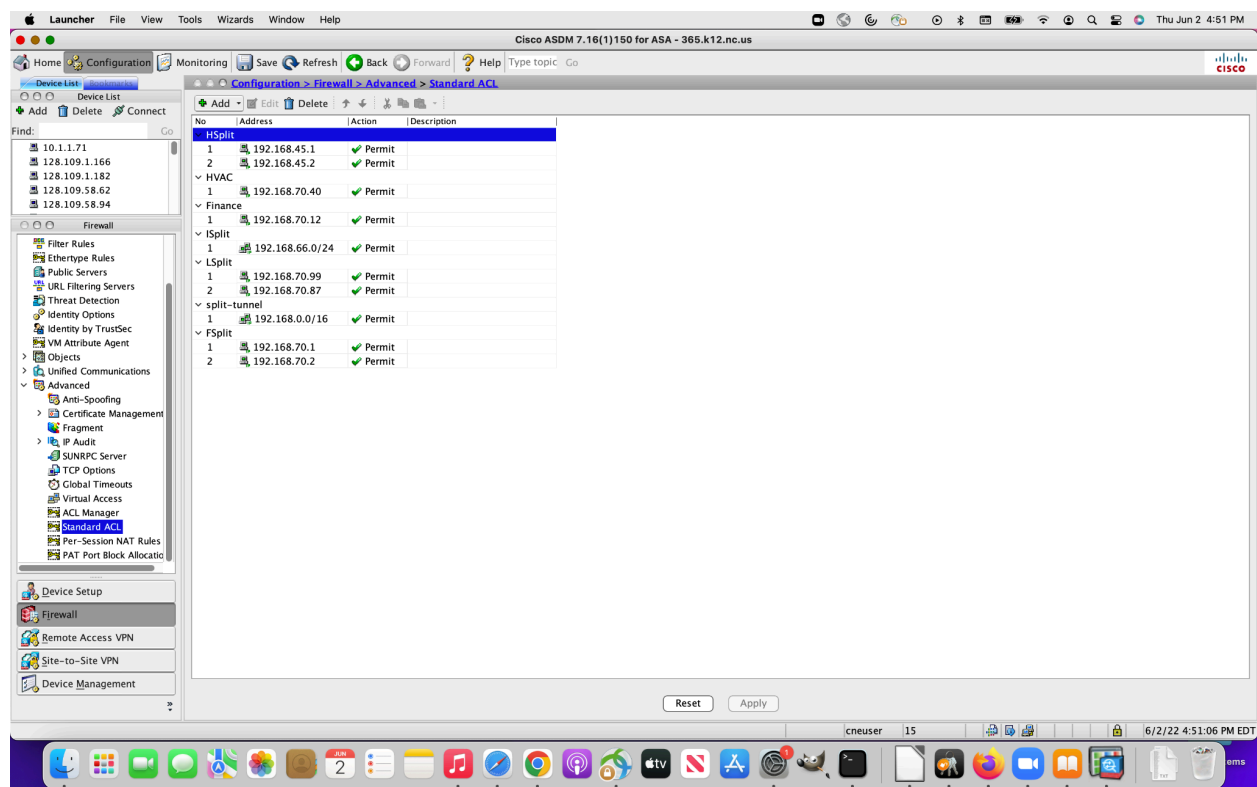
```
username LocalNotAD password ***** pbkdf2
username LocalNotAD attributes
vpn-group-policy LocalNotAD
```

```
tunnel-group LocalNotAD type remote-access
tunnel-group LocalNotAD general-attributes
address-pool cnelab
tunnel-group LocalNotAD webvpn-attributes
group-alias LocalNotAD enable
group-url https://365.k12.nc.us/LocalNotAD enable
```

```
ip local pool cnelab 10.2.3.4-10.2.3.100 mask 255.255.255.0
```

```
access-list LSplit standard permit host 192.168.50.12
```

Split tunnel access-lists are defined in the gui under Firewall > Advanced > Standard ACL:



The 3 pulldowns for the 365 SAML connections - Finance, HVAC, ITStaff - will be added to existing LocalNotAD one.

365 iDP certificate creation

Office 365 will be the iDP (Identity Provider) for the ASA which is the SP (the Service Provider).

The challenge with the Office 365 certificate arrangement is the 365 default is for each Enterprise App to have a unique certificate. The ASA assumes that the iDP uses the same cert for all pulldowns - which it does not.

Since Office 365 uses different certificates - one for each pulldown, a single self-signed certificate will be generated and uploaded to each Enterprise App in Office 365 to replace the default/different 365 certs. Then the matching/single self-signed certificate will be added to the ASA.

The drill here will be:

- Use openssl to create cert.pem on local device (*NIX or PC)
- Convert cert.pem to samlSigningCert.pfx - this includes a password
- Replace canned certs in each 365 Enterprise app with the same samlSigningCert.pfx file
- Download the resulting .pem file from one 365 Enterprise app to use in the ASA

This is on a Macbook but you can install openssl on a laptop.

```
openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1095
```

Generating a 4096 bit RSA private key

.....++

.....++

writing new private key to 'key.pem'

Enter PEM pass phrase:

Verifying - Enter PEM pass phrase:

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) []:US

State or Province Name (full name) []:NC

Locality Name (eg, city) []:RTP

Organization Name (eg, company) []:MCNC

Organizational Unit Name (eg, section) []:CNE

Common Name (eg, fully qualified host name) []:365ASA

Email Address []:

This forms cert.pem and key.pem.

Convert cert.pem to samlSigningCert.pfx so it can be uploaded in Azure - this includes a password.

```
openssl pkcs12 -export -out samlSigningCert.pfx -inkey key.pem -in cert.pem
```

You must enter the previously used password that secures private key

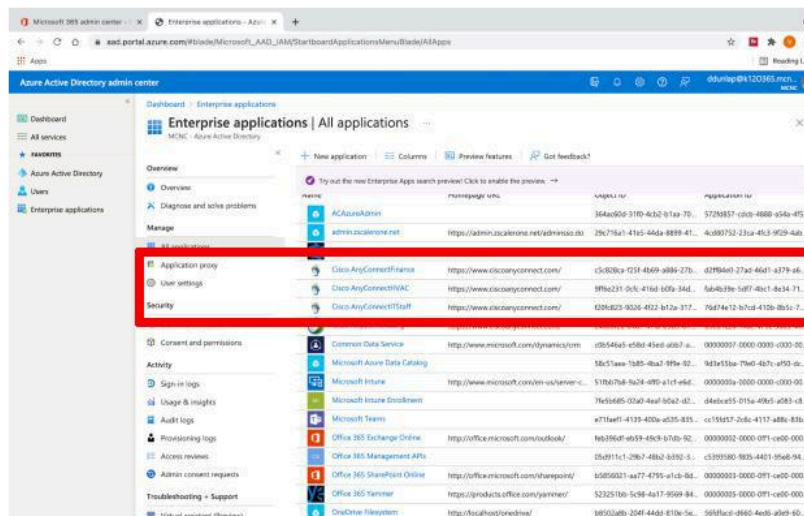
You must enter a new password to secure .pfx file

This forms samlSigningCert.pfx which will be used in 365.

365 Setup

Creation of 3 Enterprise Apps - one per pulldown

Our 3 pulldowns were created in Enterprise Applications > New application > search for Anyconnect and 'add'. Under 'Properties', we changed the logos to reflect the Finance, HVAC, and Staff arrangement. This shows our resulting 3 Enterprise apps:



Populating Single Sign-on String in Each Enterprise Application

Within each Enterprise App > Single Sign-on, we must fill in the basic SAML strings for each application respectively as seen below prior to importing the single cert into each app - you can see how these are derived from the firewall name and pulldown(s):

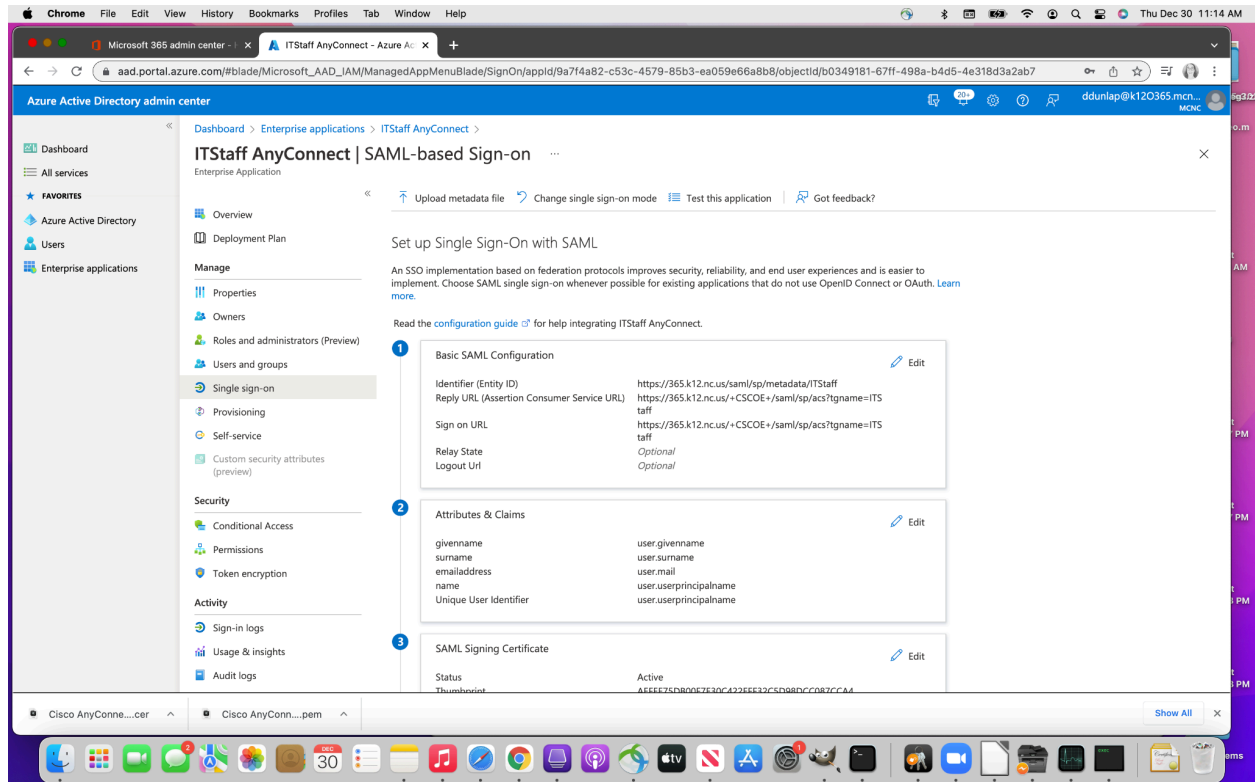
Identifier (Entity-ID) = <https://365.k12.nc.us/saml/sp/metadata/Finance>
Reply URL = <https://365.k12.nc.us/+CSCOE+/saml/sp/acs?tname=Finance>
Sign on URL = <https://365.k12.nc.us/+CSCOE+/saml/sp/acs?tname=Finance>

Identifier (Entity-ID) = <https://365.k12.nc.us/saml/sp/metadata/HVAC>
Reply URL = <https://365.k12.nc.us/+CSCOE+/saml/sp/acs?tname=HVAC>
Sign on URL = <https://365.k12.nc.us/+CSCOE+/saml/sp/acs?tname=HVAC>

Identifier (Entity-ID) = <https://365.k12.nc.us/saml/sp/metadata/ITStaff>

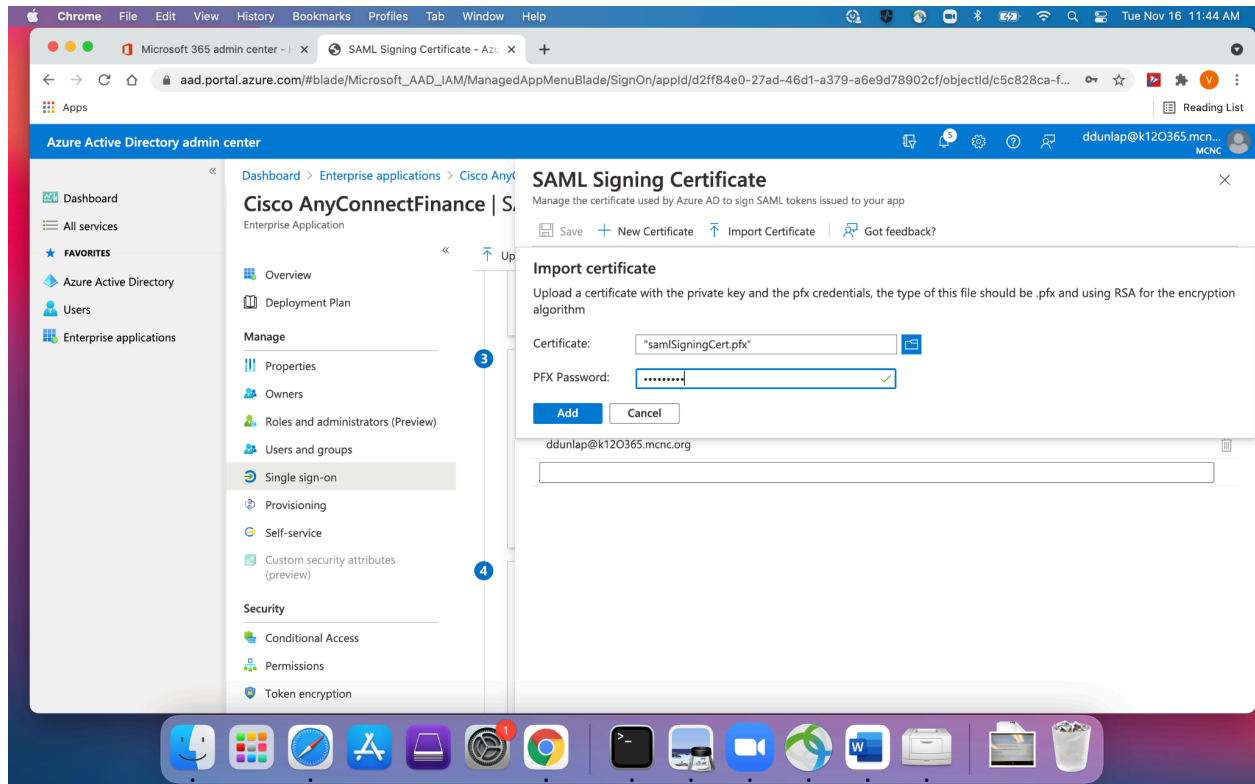
Reply URL = <https://365.k12.nc.us/+CSCOE+/saml/sp/acs?tname=ITStaff>
Sign on URL = <https://365.k12.nc.us/+CSCOE+/saml/sp/acs?tname=ITStaff>

This shows entry of the strings for one Anyconnect Enterprise App under Single Sign-on - the strings are unique per app/pulldown as seen above:



Populating pfx cert in Each Enterprise Application

Within each app, we edit the SAML signing cert - this is where we import the certificate previously created with the openssl pfx file and specify the key - this shows for the Finance Enterprise App but all 3 would be done the same way:



In the same area, make certain that the pfx certificate just uploaded is “Active” - the old/original one should not be active (in fact, it can be deleted) nor should there be multiple certificates active:

SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

 Save  New Certificate  Import Certificate |  Got feedback?

Status	Expiration Date	Thumbprint	
Active	12/29/2024, 9:04:57 AM	AEFEE75DB00F7E30C422EFF32C5D98DCC087CCA4	...
Inactive	1/28/2022, 2:38:13 PM	570A7C22E71D3684F898809212B8075A027E124D	...
Inactive	12/28/2024, 12:50:32 PM	7CD26184D3088731D904D14AC95B4FFA0B240891	...
Inactive	12/29/2024, 10:40:51 AM	6A0515A12DB019824D032381636403B8E37F3142	...

Signing Option

Sign SAML assertion

Signing Algorithm

SHA-256

Notification Email Addresses

ddunlap@k12O365.mcnc.org

Downloading pem certificate for ASA

After the strings and PFX files are present on all 3 Enterprise apps, go into any one of the 3 Enterprise Apps in 365 > Set up single sign-on > Edit > Click on the 3 dots to the right of the Active cert then do 'PEM certificate download'.

Screenshot of the Azure Active Directory admin center showing the SAML Signing Certificate page for Cisco AnyConnect. The page displays a list of certificates with columns for Status, Expiration Date, and Thumbprint. The active certificate is highlighted, and a dropdown menu is open showing options to download the certificate in various formats (Base64, PEM, Raw, Federated XML) or delete it.

Status	Expiration Date	Thumbprint
Inactive	11/21/2024, 9:58:46 AM	B98B93972D3DEC6013BC867E816D815CCC1FB172
Inactive	11/10/2024, 1:25:54 PM	734A03D50C1598998C94F3403C5CEF7C9C0277F9
Inactive	11/10/2024, 1:25:54 PM	734A03D50C1598998C94F3403C5CEF7C9C0277F9
Inactive	11/10/2024, 1:25:54 PM	734A03D50C1598998C94F3403C5CEF7C9C0277F9
Active	11/16/2024, 11:36:54 AM	0B8859D13EBAFFADB0879B9CE9266F5004E57E0

Delete all certificates except for the active one:

Screenshot of the Azure Active Directory admin center showing the SAML Signing Certificate page for Cisco AnyConnect. The page displays a list of certificates. The active certificate is highlighted, and the dropdown menu is closed. The page shows the details of the active certificate, including the Signing Option (Sign SAML assertion), Signing Algorithm (SHA-256), and Notification Email Addresses (ddunlap@k120365.mcn.org).

Status	Expiration Date	Thumbprint
Active	11/16/2024, 11:36:54 AM	0B8859D13EBAFFADB0879B9CE9266F5004E57E0

Our downloaded pem file = "Cisco AnyConnectFinance.pem".

ASA SAML Setup

Add Azure iDP cert to ASA

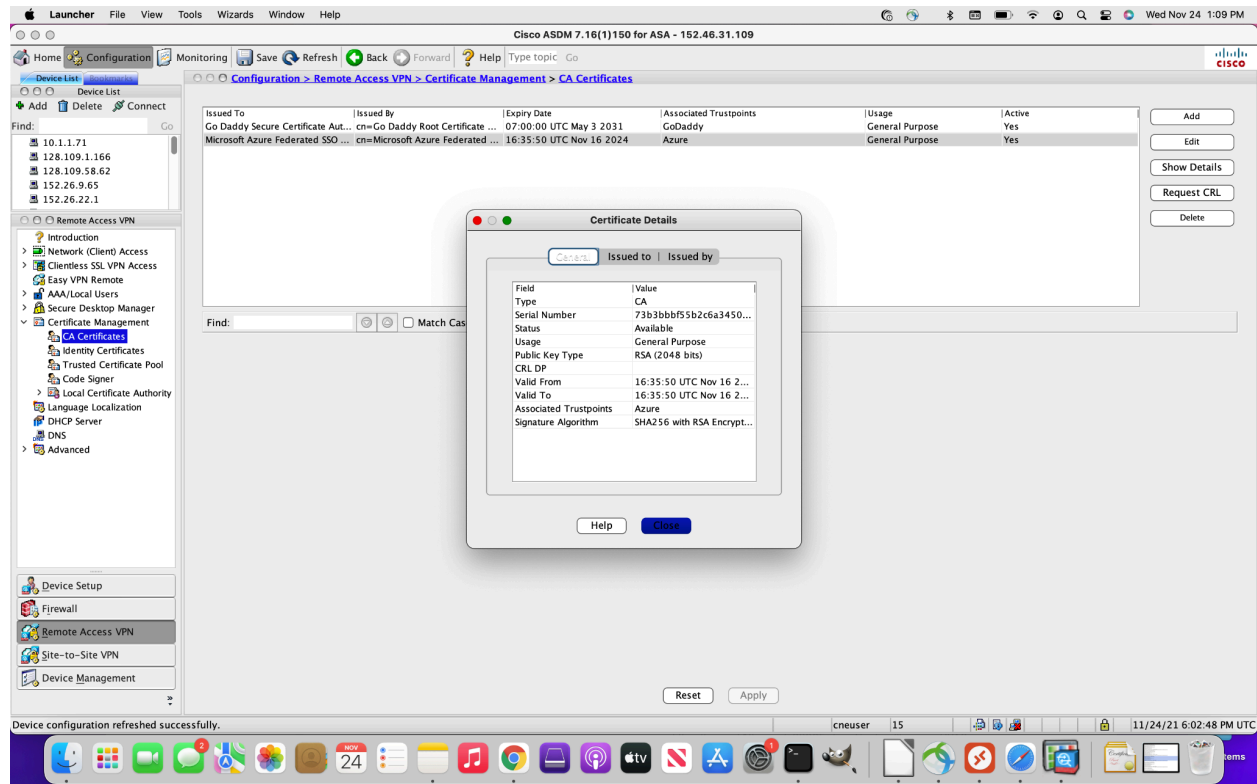
Since ASDM does not allow entry of the 365 pem cert using the 'no ca-check' option, we specify 'no ca-check' from the CLI:

```
365# conf t
365(config)# cry ca trustpoint Azure
365(config-ca-trustpoint)# no ca-check
365(config-ca-trustpoint)# exit
365(config)# exit
365# write mem
```

Write mem then go into ASDM and refresh the CLI config.

To add the cert, go into ASDM Remote access VPN > Certs > Add CA cert > name the trustpoint same as in CLI (Azure) then upload the pem file (ours was Cisco AnyConnectFinance.pem) downloaded from 365 EA'.

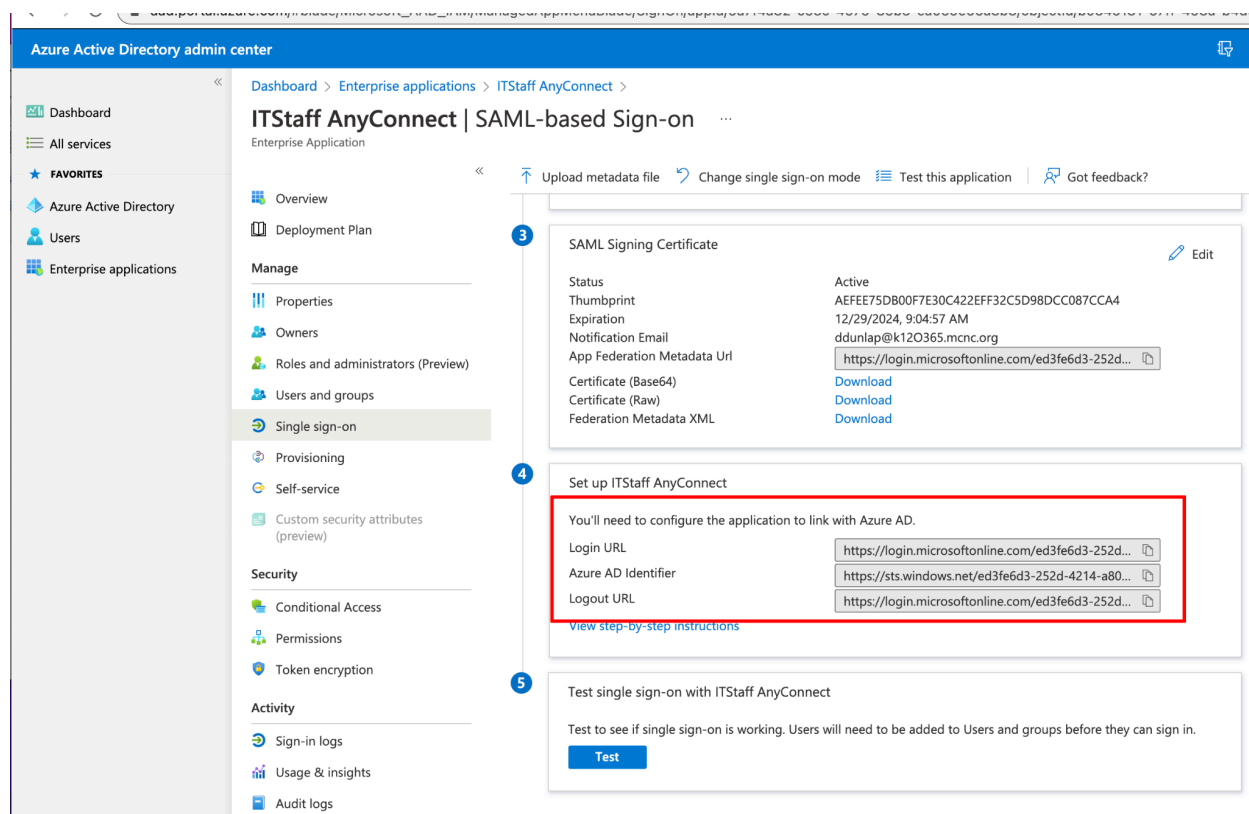
Do Apply > Save. Afterwards, certificate can be seen:



Configuring Azure as idp in ASA

Relevant strings

In Azure under the Enterprise App setups Cisco AnyConnect<whatever> there are 3 strings as shown below - paste them to notepad (these do not differ per app):



The relationship between 365 attribute nomenclature and ASA nomenclature is as follows:

String #1 Login URL in Azure (1/3) = Sign-in URL in ASA (yours would be different):
<https://login.microsoftonline.com/ed3fe6d3-252d-4214-a808-15a4def117e2/saml2>

String #2 AD Identifier (2/3) = server name in the ASA (yours would be different):
<https://sts.windows.net/ed3fe6d3-252d-4214-a808-15a4def117e2/>

String #3 Logout url (3/3) = Sign-out URL in ASA (yours would be different):
<https://login.microsoftonline.com/ed3fe6d3-252d-4214-a808-15a4def117e2/saml2>

Base url is the <https://FQDN> firewall (this is your firewall).

IDP cert is the one brought in from Azure.

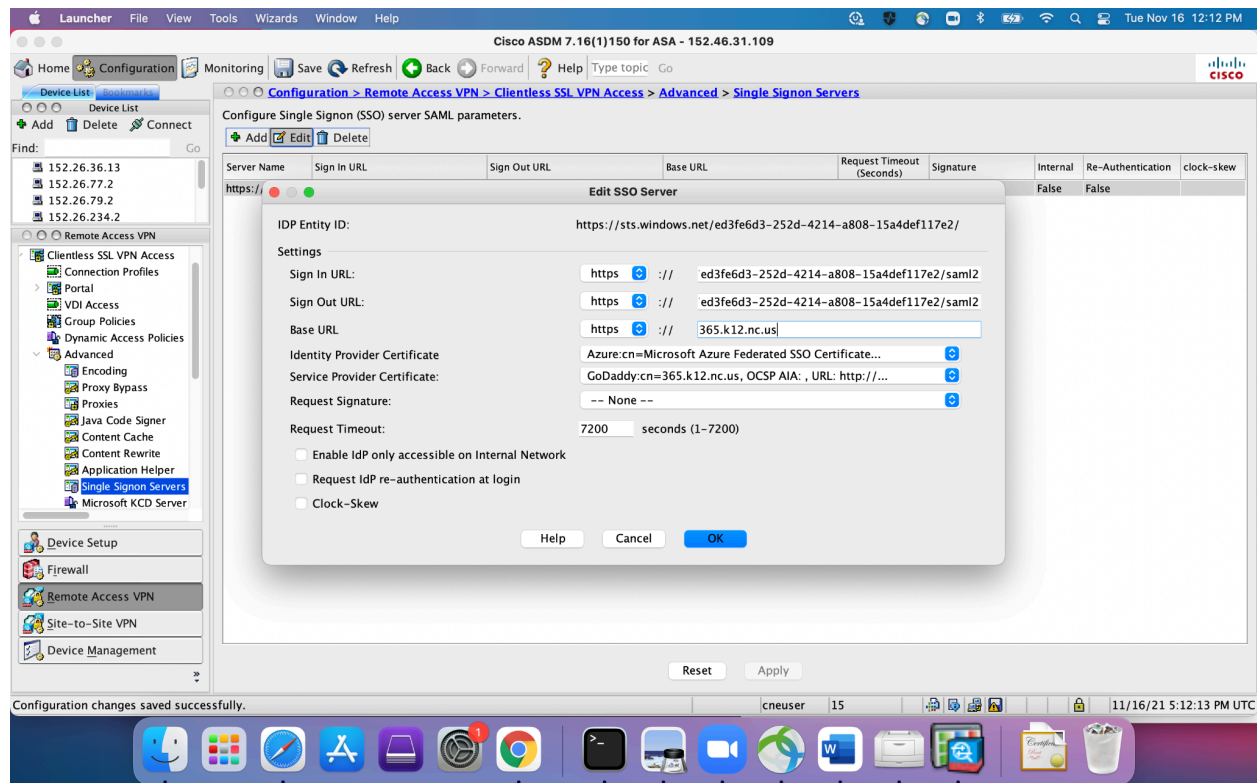
SP cert is the one issued to the FW.

Adding Azure IDP under ASA webvpn

Since the Azure (and GoDaddy) certs/trustpoints are now in the ASA, we now have to define Microsoft 365 as iDP in ASDM under Remote access > Clientless SSL VPN > Advanced > Single sign-on server.

The fields are as follows:

Sign-in URL = your login.microsoftonline.com/<whatever> (HTTPS pulldown!!!)
Sign-out URL (optional) = your login.microsoftonline.com/<whatever> (HTTPS pulldown!!!)
Base URL = FQDN-of-your-firewall (HTTPS pulldown!!!)
Identity Provider Cert = Azure one
Service Provide Cert = purchased one (like GoDaddy)
Request signature = rsa-sha256
Request timeout = 7200
Request IDP reauthentication at login



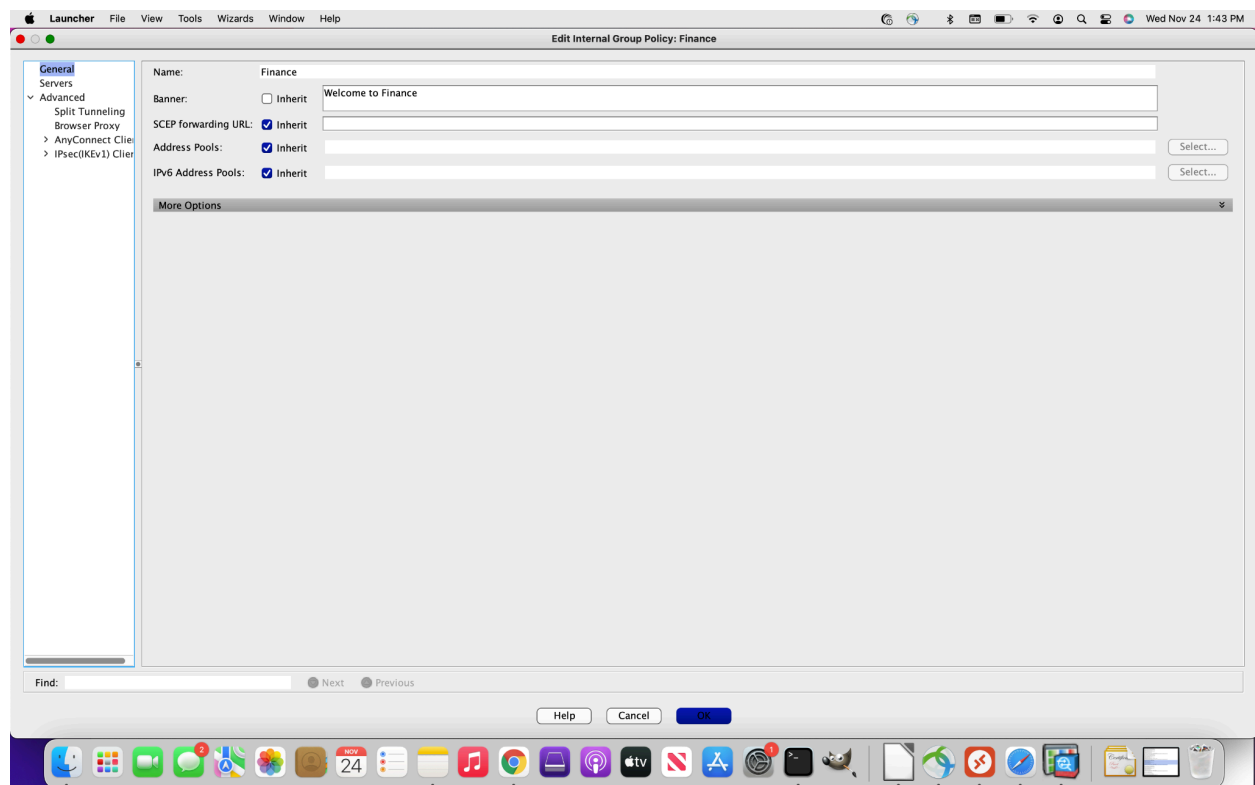
Apply and save. The finished piece of the configuration looks like this:

```
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnect-macos-4.7.04056-webdeploy-k9.pkg 1
```

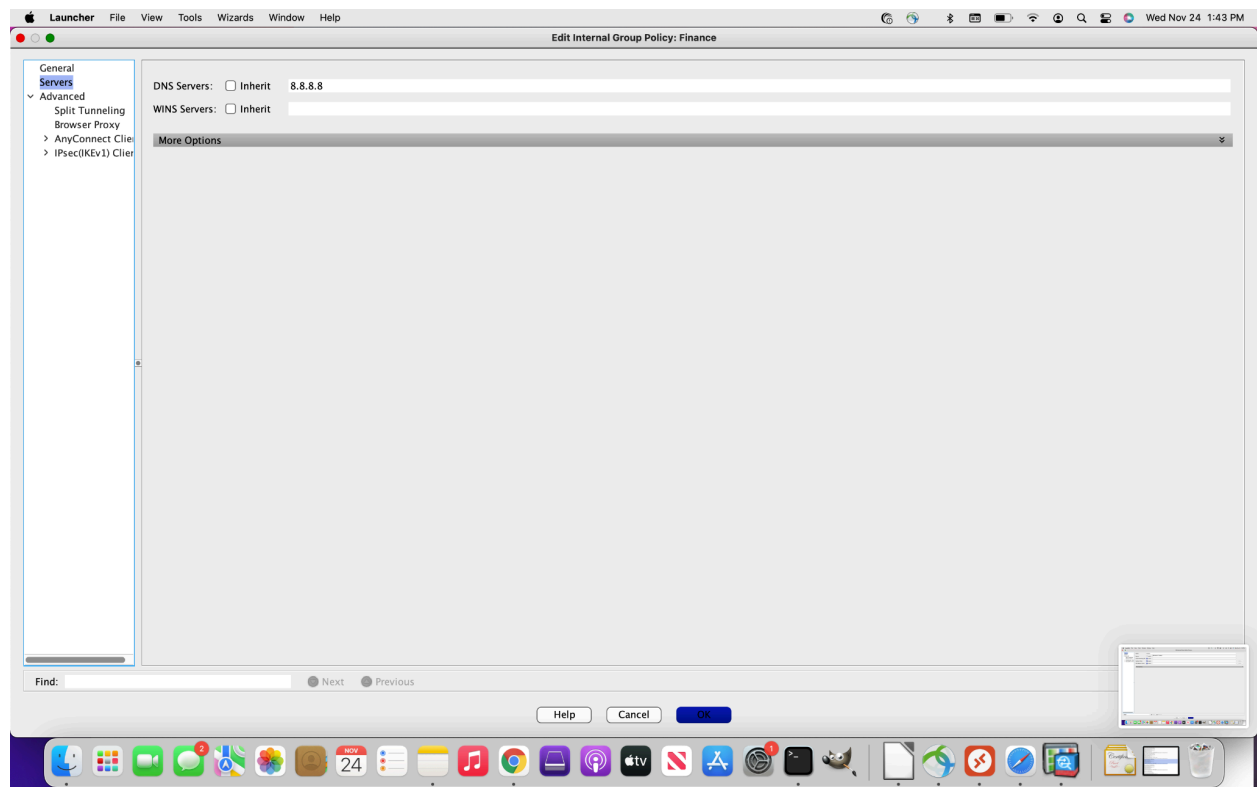
anyconnect image disk0:/anyconnect-win-4.7.04056-webdeploy-k9.pkg 2
anyconnect enable
saml idp https://sts.windows.net/ed3fe6d3-252d-4214-a808-15a4def117e2/
url sign-in https://login.microsoftonline.com/ed3fe6d3-252d-4214-a808-15a4def117e2/saml2
url sign-out https://login.microsoftonline.com/ed3fe6d3-252d-4214-a808-15a4def117e2/saml2
base-url https://365.k12.nc.us
trustpoint idp Azure
trustpoint sp GoDaddy
signature rsa-sha256
force re-authentication
timeout assertion 7200
tunnel-group-list enable
cache
disable
error-recovery disable

Add ASA group-policies for each pulldown on the SAML/365 arrangement

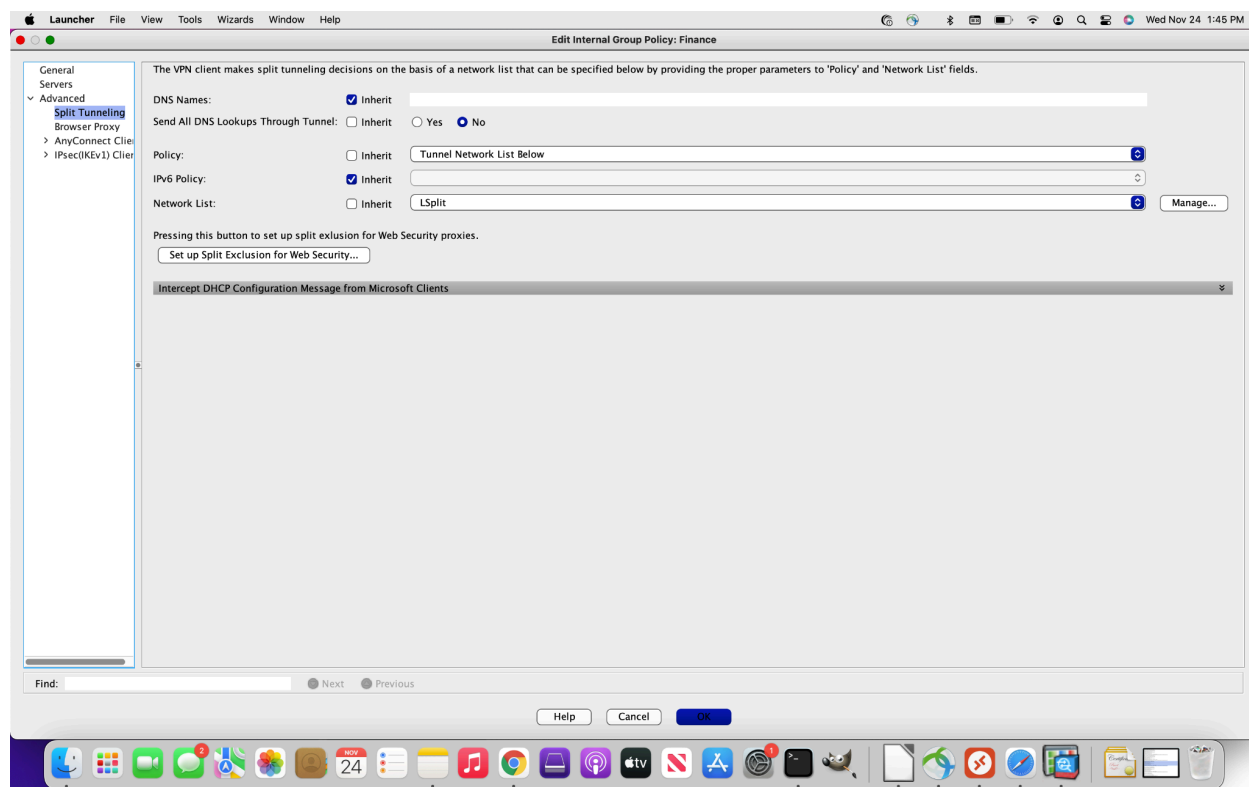
In ASDM, add group-policy - Network > Client access > Group-policies - this illustrates "Finance" - a banner is optional:



We define the DNS server:



And we have a split-tunnel list:



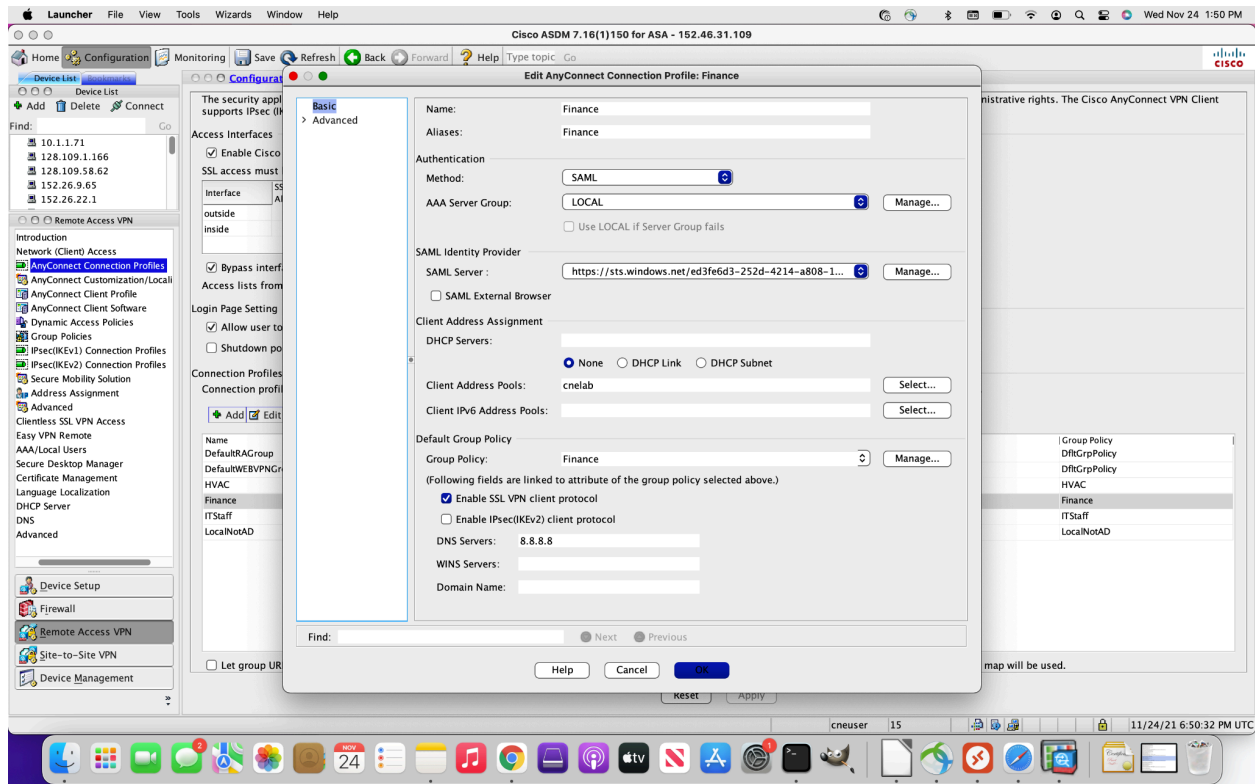
Finished, the Finance group-policy in the CLI looks like this:

```
group-policy Finance internal
group-policy Finance attributes
banner value Welcome to Finance
wins-server none
dns-server value 8.8.8.8
vpn-tunnel-protocol ikev1 l2tp-ipsec ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value LSplit
```

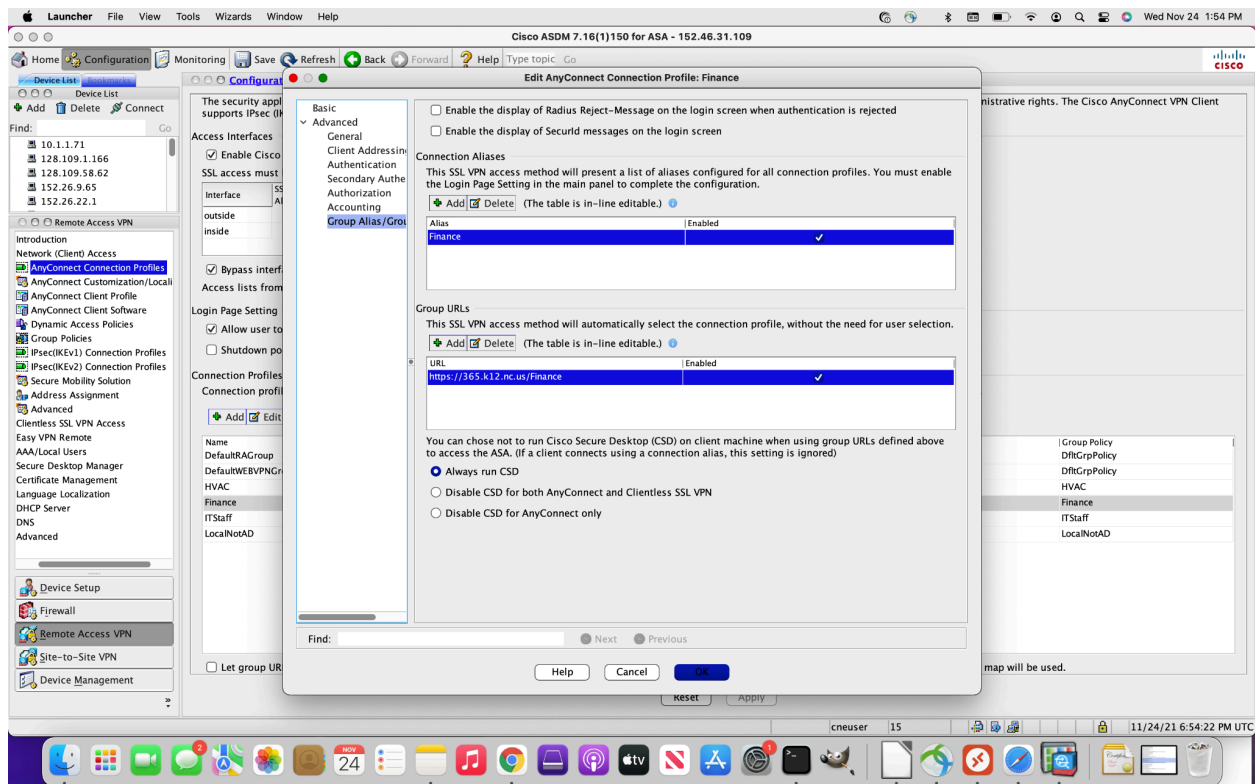
Add tunnel-groups, associate with group-policies

This is done under Remote-access VPN > AnyConnect Connection Profiles. These screenshots show the addition of “Finance” connection profile.

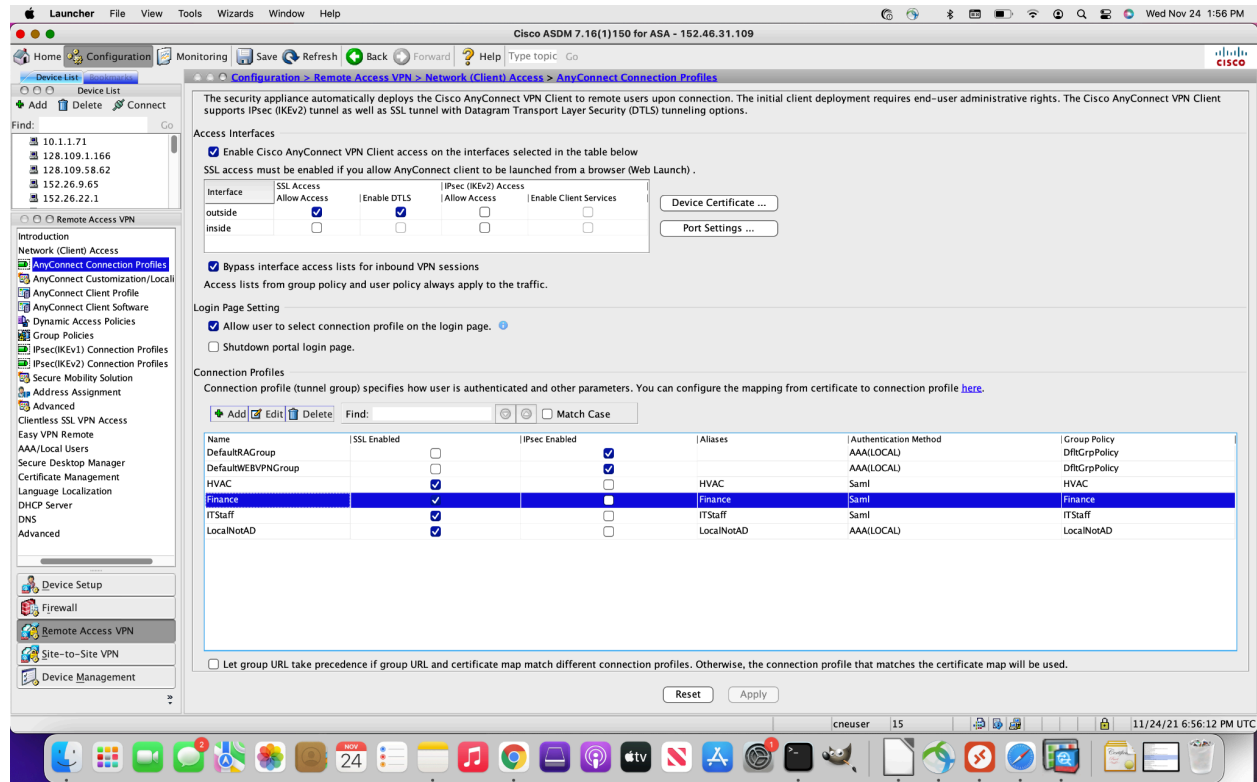
The “Finance” pulldown is configured to use the SAML server (your defined single-sign-on server string) and to do SAML for the method:



Define and associate the connection aliases and group urls (this shows "Finance"):



And associate tunnel-group Finance with group-policy Finance:

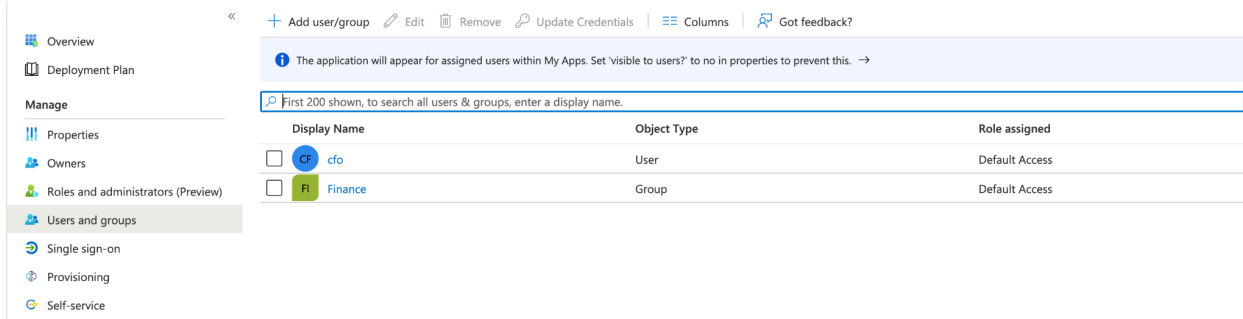


The tunnel-group area in the CLI appears thusly in our ASA for "Finance":

```
tunnel-group Finance type remote-access
tunnel-group Finance general-attributes
address-pool cnelab
default-group-policy Finance
tunnel-group Finance webvpn-attributes
authentication saml
group-alias Finance enable
group-url https://365.k12.nc.us/Finance enable
saml identity-provider https://sts.windows.net/ed3fe6d3-252d-4214-a808-15a4def117e2/
```

365 - turn on Enterprise apps for whoever

Within 365, Enterprise Apps can be turned on at the user and/or group level. This shows the app "Cisco AnyConnectFinance" turned on for user cfo as well as group Finance.



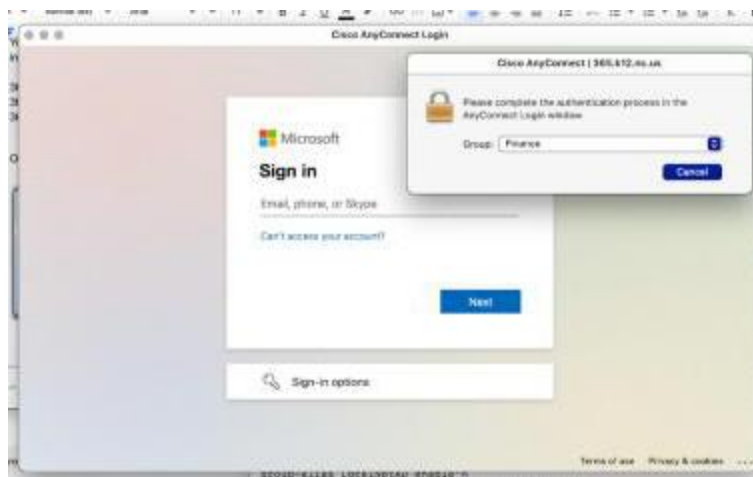
Testing Anyconnect

Since the ip address of the ASA resolves (it had to to get the certificate) and it has a CA cert, you should no longer see messages about the connection being sketchy.

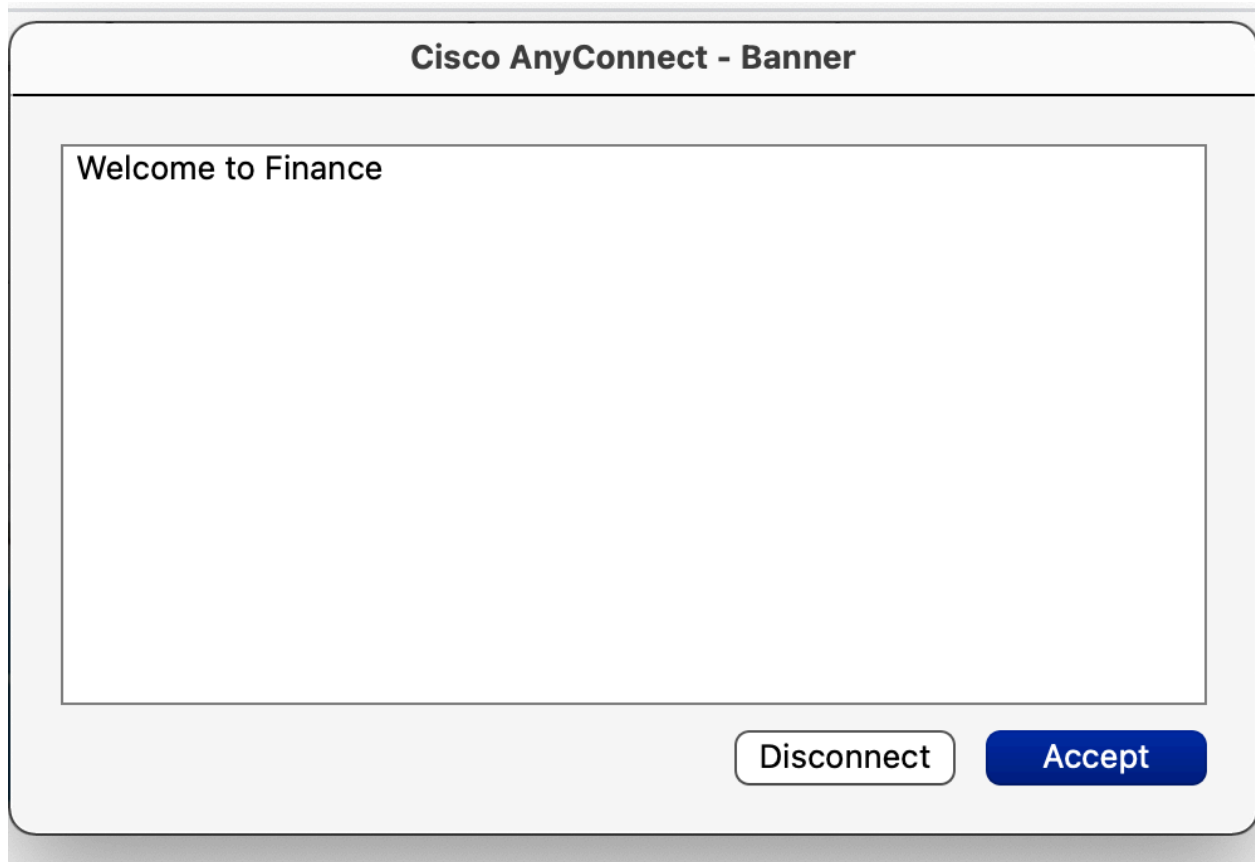
You can either Anyconnect to the firewall FQDN then choose the pulldown or enter the pulldown in the browser like:

365.k12.nc.us/ITStaff
 365.k12.nc.us/HVAC
 365.k12.nc.us/Finance

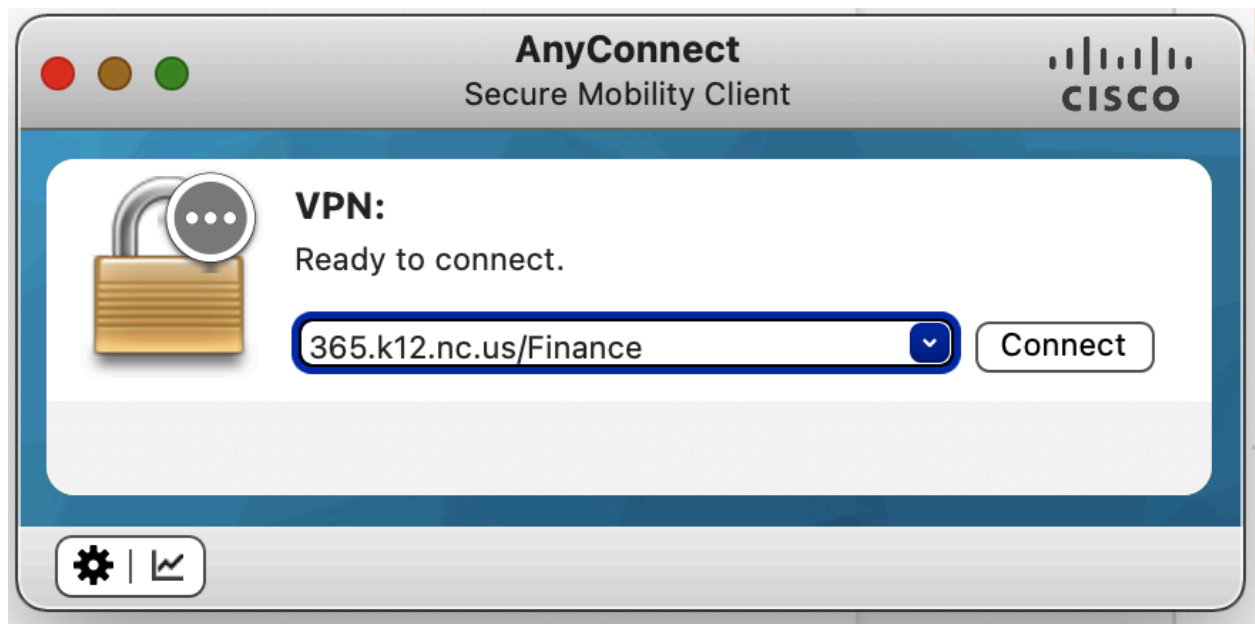
On connection to 365.k12.nc.us, the software should show the configured pulldowns.
 On connecting to a specific pulldown, the Microsoft screen should come up:



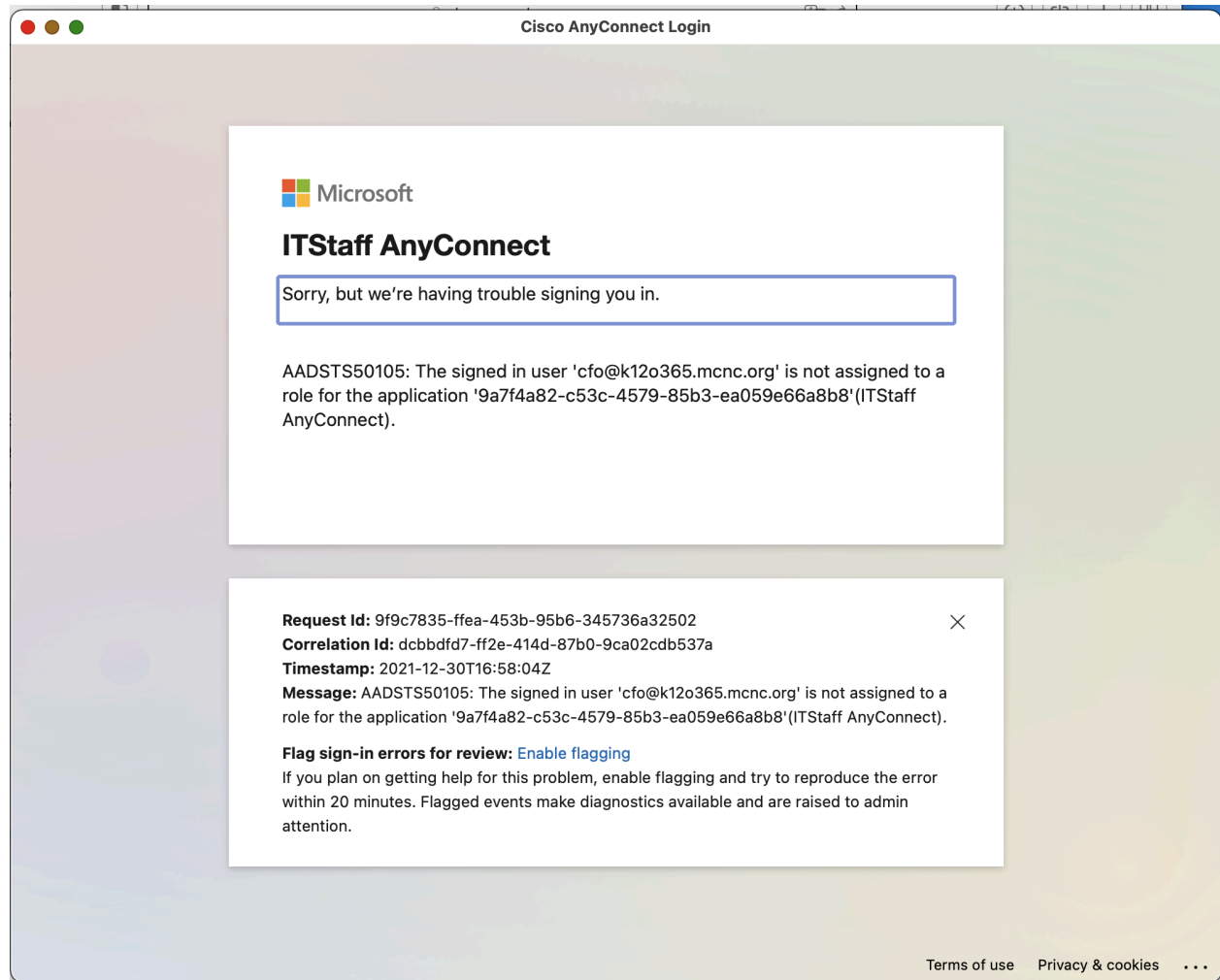
After logging into 365 with the cfo@k12o365.mcnc.org account and a brief Anyconnect flash, the successful connection message comes up if a banner is configured:



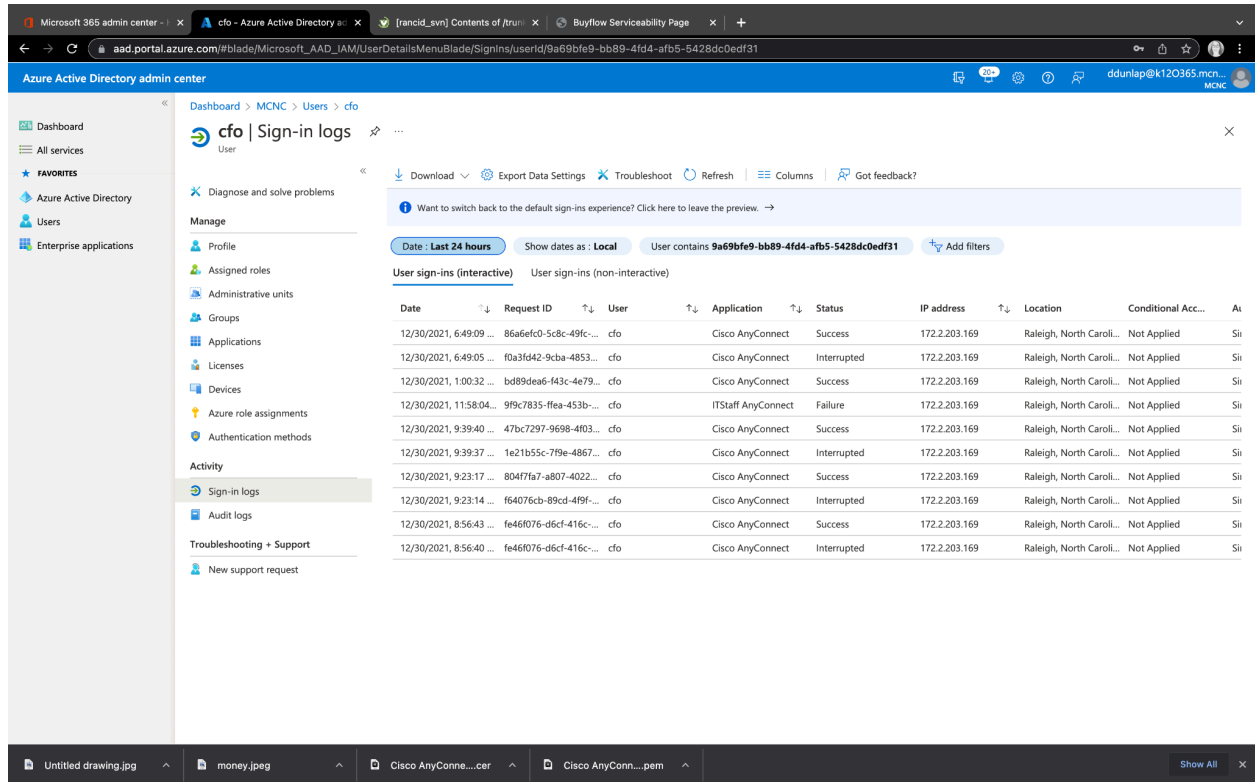
It is also possible to connect via appending the correct pulldown in Anyconnect as shown here:



If the user selects the incorrect pulldown, for example, the Finance user chooses the ITStaff pulldown, that user will get an error as 365 discovers the Finance user is not allowed access to the ITStaff Enterprise App.



The 365 logs for the user will show successful and failed attempts as well as the ip address of the connections:



Locking Down the ASA

The examples above illustrate use of grouping/pulldowns - Finance, HVAC, ITStaff - within the ASA in order to limit user access to specific host ip addresses inside the ASA network; this is tied in with 365. But suppose we wanted to be more granular and only permit access to specific ports on specific hosts inside the network?

In our example, our Finance grouping/pulldown users' access is limited by virtue of the split-tunneling access-list "LSplit"; those users can only access the Finance server at 192.168.50.12:

access-list LSplit standard permit host 192.168.50.12

But we want to further limit connections to the 192.168.50.12 server, only permitting remote-desktop on port tcp 3389. We do not want to allow tcp 389/636 ldap queries, IIS's ports 80/443, etc., so this requires an additional port-based extended access-list and use of the vpn-filter command in the group-policy:

access-list Finance_Ports extended permit tcp any host 192.168.50.12 eq 3389

group-policy Finance internal
group-policy Finance attributes
banner value Welcome to Finance
dns-server value 192.168.70.3

vpn-filter value Finance Ports
vpn-tunnel-protocol ssl-client ssl-clientless
split-tunnel-policy tunnelspecified
split-tunnel-network-list value LSplit

Chromebooks and ipads

It is possible to use Anyconnect with 365 on Chromebooks and ipads but setup was challenging. If those devices are required, you should make sure existing VPN connections (i.e. non-365) work initially as the ASA needs to be licensed for those device-types. DIT can install mobile device licenses for Chromebooks and ipads.

In order for Chromebooks to work, the command:

saml external-browser

might be needed under the tunnel-group depending on the code version.

ASA Debugs

These debugs show successful connection of
User=cfo@k12o365.mcnc.org, pulldown==Finance

debug webvpn saml 255
debug webvpn 255
debug webvpn session 255
debug webvpn request 255
debug aggregate-auth ssl 255
debug crypto ca messages 255

365# debug webvpn saml 255
INFO: debug webvpn saml enabled at level 255.
365# debug webvpn 255
INFO: debug webvpn enabled at level 255.
365# debug webvpn session 255
INFO: debug webvpn session enabled at level 255.
365# debug webvpn request 255
INFO: debug webvpn request enabled at level 255.
365# debug aggregate-auth ssl 255
debug aggregate-auth ssl enabled at level 255
365# debug crypto ca messages 255
365# SAML AUTH: SAML hash table cleanup periodic task

365# term mon
365# #0x00007f64942d9b00 (POST). Request line:/
#0x00007f64942d9b00 File to execute: /CSCOSSLC/config-auth

/CSCOSSLC/config-auth
Processing client request
XML successfully parsed
Processing request (init)
INIT-no-cert: Client has not sent a certificate
INIT-no-cert: Resolve tunnel group (Finance) alias (Finance) Cert or URL mapped NO
INIT-no-cert: Sending SAML authentication form
Generating SAML auth request
Public archive directives retrieved from cache for index 1.
rcode from handler = 0
Sending response
#0x00007f64942d83f0 (GET). Request line: /+CSCOE+/saml/sp/login
#0x00007f64942d83f0 File to execute: /+CSCOE+/saml/sp/login
Dec 30 13:00:17
[SAML] build_authnrequest:
https://login.microsoftonline.com/ed3fe6d3-252d-4214-a808-15a4def117e2/saml2?SAMLRequest=fZJLT8MwEIT%2FSuR74keSNihNpUCpVAKQAsSBC7KcDbVw7OB1ePx70gBSOcB1PZ93ZuwVqt4Oshnj3t3AywgYk%2FfeOpTzQU3G4KRXaFA61QPKqOVtc3khRcbkEHZ02ltyhPxPKEQI0XhHkt2mJo8NL8%2B2p2xR8W2eF%2BdVc35S5YwVeVUrCk5Se4h4KSvyYRPEOIIO4dRuTiNmOApF2nO7nglGZN8%2BUCSszZTBObVnah%2FjgJJS65%2BMy3qjg0ffRe%2BscZBp31No8w4WbZ6KUrRpIXiRqopVKS9V0ULH%2BRIEPSQTJNn6oGHuqiYxjHAwdD1IMq9Qk05ZBLJeHbRyNhrWP%2BvzRZk9c5E5nY0430ZxoD1E1aqo6Hby6zs6DG7%2Bnqaq6nE3ebaW6M%2FDgZ6Ff%2FumGd8npg27WapHB0OoE1noCVJY61%2FOwuglnwHoOuvpb%2B%2FwPoT&SigAlg=http%3A%2F%2Fwww.w3.org%2F2001%2F04%2Fxmldsig-more%23rsa-sha256&Signature=byxG8ozQgNYVwNnhkQgbo55YF1oB2vK0pMtGEYjke4tjEOD%2FeJ%2FRSqMTTrleyGz4OIAGHpvJgXfd%2By56SFpHfDhJzWsOetet9NKyA%2BgbJr%2B19rHQqBzJcGGuxecAMFU9kJhUHXBUkSKEnYL8k6xJgdH%2FiRAv3WcsxrfswsRgrVJ0H1WnhF9Fy36t5MUm5Dz0vth8QwOZPuuvSCTnVJSkYnLC4xMUWwmv7zg8gaeM25fejRsfQ%2Btwsx7AJbMp%2B8hPRpf7UH68GVlsgeNLeEduVSaxHldQOU7WP3tjqrLMvVGtyl8N3S8%2B0IW1056ER1kdlZm%2Fz3D0CbFc7UzfOncfT5%2FgiDraDUodVXKG94zWfVnnmzQ99ixzNBBdah1nxR9L4rQmCsb7F0p2rf77Rza4mAJKlskZhGwEfVeBEbGf52wgEypokA8AJvQIDwIZDBdKK6Wh7s%2F0ZX2B5ssTi33%2FYKH7sALBnOJbU1542pkp3g7HS601SQsRo4bHkby24mCLTjdCfSIBFb9Z51az8QkhCXm9DC5II9vJL5m39UsVVPdEibljXSU8ZW3ozINly9Bcux1yO%2F%2FYJOxxwxZHfpu
ySPzNsy0ljrXWEhrphAbV4mvH4u7qGnavORDMAPUmSAJx4%2B7yD1kRnwgOqlM%2By9y111r1XT33%2F%2FJK3JLgOimEKpM%3D
[SAML] saml_is_idp_internal: getting SAML config for tg Finance
#0x00007f64942d83f0 (POST). Request line: /+CSCOE+/saml/sp/acs
#0x00007f64942d83f0 File to execute: /+CSCOE+/saml/sp/acs
#0x00007f64942d83f0 (POST). Request line: /+webvpn+/index.html
#0x00007f64942d83f0 Hand-off to emWeb.
webvpn_allocate_auth_struct: net_handle = 0x00007f6494fa5fa0
len1/28 < len2/590
length of new buffer 0x00007f64a28c7480 is 618/954 prefix left=366
webvpn_portal.c:ewaFormSubmit_webvpn_login[4023]
webvpn_portal.c:webvpn_login_validate_net_handle[2728]
webvpn_portal.c:webvpn_login_allocate_auth_struct[2745]
webvpn_portal.c:webvpn_login_assign_app_next[2767]
webvpn_portal.c:webvpn_login_cookie_check[2788]
webvpn_portal.c:webvpn_login_set_tg_buffer_from_form[2837]

EFiY29ScEdvRW4yUVRYNWZESHdNVUNESHdjSXVkUkNpcm1jd1ZrQ0Y4Mm96VTdVYXBxeU9QVE9
OelpGcFA0YzMWtTM2dGhOc0xiZ3IHcTgxK0ZacGdTWUtYUHp6bk5VllmeINFSnNqAG1pVmMwdHJyN
FhHVkRpajhEWFVxM3pWcWZ0dUc2Sm10U2kxMVdFWVQvNFFkT0dXTT08L1NpZ25hdHVyZVZhbHVI
PjxLZXIjbmZvPjxYNTA5RGF0YT48WDUwOUNlcnRpZmljYXRIPk1JSUZaRENDQTB3Q0NRQ05BR09U
QmZIZjZUQU5CZ2txaGtpRzl3MEJBUXNGQURCME1Rc3dDUVIEVIFRR0V3SIZVekVMTUFR0ExVUVD
QXdDVGtNeEREQUtCZ05WQkFjTUEExSIVVREVOTUFzR0ExVUVDZ3dFVfVOT1F6RU1NQW9HQTFVR
UN3d0RRMDVGTfV3d0NnWURWUWFEREfNek5qVXhleKfKQmdrcWhraUc5dzBCQ1FFV0VHUmtkVzV
zWVhCQWJXTnVZeTV2Y21jd0hoY05NakV4TWpNd01UUXdORFUzV2hjTk1qUXhNakk1TVRRd05EVTN
XaklwTVFzd0NRWURWUWFHRXdkVIV6RUxNQWtHQTfVRUNBd0NUa014RERBS0JnTIZCQWNNQTF
KVVERU5NQXNHQTFVRUNd0VUVU5PUXpFTU1Bb0dBmVVFQ3d3RFEwNUZNUX3Q2dZRFZRUU
REQU16TmPVeEh6QWRCZ2txaGtpRzl3MEJDUUVXRUDSa2RXNXNZWEJBYldOdVI5NXZjbWN3Z2dJa
U1BMEduDU3FHU0liM0RRRUJBUVVBQTRJQ0R3QXdnZ0lLQW9JQ0FRRHRLNG1PTktMbXNrTFNRUG
xBWjROUmoxcU0bUVPuW1sd0xIM3dINXdxclZOTUs1TEJzR3NWZDdKVlgrY0h3dVc0RFdVUXFmS0F2
Mk5qNcTldS9nQ08ydDIleWxoWDVzVUhnbkoxWktkRlRnRzBmamtTR1M2U0REL05RakxYbkVJdkh2M
WpmTXZDYjVPYVJnT0VOMmNMZko2WmliVHRUL1BrZkczKzXRUzszTWpIQWJjQUZ5NkhGQ1NTbGZ
NNGVEYUI2ZDFW29ueFdON0Mram1hdEt0Q1NzbVg4UkNDaUM2ZEEQvMnphZ2E5N1M3UURnV0tsO
XI4dUhGVWYzSEhWNzdnTIBZYVlta0t5NXdlNmZGVIV0anZSWS90ZHU3UkJMZzhabmNYVHlqSml4N0I
qelMzdC82Yncwd3NkTXJIZkNKTnNxZ0U3YldnWi9FWThZT9sVUxOWk8yOFhkN0I3YWFuQ1NEOEEdTZ
HVWUE5wRIBKN09LWUJxcWtLTUxhMkRUNGgydzNuZm5XNnBWSXpBbG5id1N4R2UvWk55SXMxazN
vU2gzV2lnVVRULWR1dXcxSU5qMUKvYUtlSmhQeEJ3QIVYSVFNBGFJaWZ1Um0zQWc2WnkrdDJld3Q
xdEYzaGVUMDZIYklsafMDDec 30 13:00:32 [SAML] NotBefore:2021-12-30T17:55:32.068Z
NotOnOrAfter:2021-12-30T19:00:32.068Z timeout: 7200

Dec 30 13:00:32 [SAML] consume_assertion: <Session
xmlns="http://www.entrouvert.org/namespaces/lasso/0.0" Version="2"><Assertion
RemoteProviderID="https://sts.windows.net/ed3fe6d3-252d-4214-a808-15a4def117e2/"><Assertion
xmlns="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="_bd89dea6-f43c-4e79-8666-0c05b4f94002" IssueInstant="2021-12-30T18:00:32.302Z"
Version="2.0"><Issuer>https://sts.windows.net/ed3fe6d3-252d-4214-a808-15a4def117e2/</Issuer><Sign
ature xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo><CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/><Reference
URI="#_bd89dea6-f43c-4e79-8666-0c05b4f94002"><Transforms><Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/><Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></Transforms><DigestMethod
Algorithm="http://www.w3.org/2001/04/xmldsig#sha256"/><DigestValue>XZRAmjDhOz9EyNBWsiNXC
1lkDaKJR5a1cDsCm3slnNo=</DigestValue></Reference></SignedInfo><SignatureValue>UPmzLzZNYN
TkUaE+KgAVhbQRrEtK5UjEhbp9YJvZrVnPMNN0WL5dY/I+/oSNhBWfXC57RmRfxUqO6/m1JSUnwGzn
zlszZ9IHtie6OZVvej+NP5tlavhPDfy9FVFDPRgSw6r/+HWH/IVZCNA3s/SWxhBXoiagAlfJbkW8SGzBscs
TK2DXSBfoYJq8G7Xf6m3TQ5Huhmy8TCXsxTiEvV1Cl9lfvklbNvvcqsucPHyji6BLmhVipHn1Rsy6pVYp0xjt
J9IUGFID1/xjULVg61Osj33vBAUJ8mUP8n6NDEHuHM6JgPt22kZWJzt0BnyNlvsyQvjDNmaYIKvx8PzQC9
siHl61Wq8NgZKLwv8963iHHvRElgXJfmTbk5tg/2dZbjdGx25Xdch8GJ+thH8h5LaKVRv4bsaAASIPW9Fjq
U7MBs/OaU/YhshLtGQn8RL2H4yFWEINxYK0b4uyWywtJKSxU1M6YLU0CxdwaDpeXzin1Zx+e5HhIOqH
TX8u+97CdQ6IOF6JGRyp4XzZHP3TAHcoRpGoEn2QTr5fDHwMUCDHwcludRCirmcwVkcF82ozU7Uap
qyOPTONzZFpP4c30M36thNsLbgyGq81+FZpgSYKXPzznG9VYfzSEJsPhmiVc0trr4XGVDij8DXUq3zVqft
uG6JmtSi11WEYT/4QdOGWM=</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIFZDCCA0
wCCQCNAgOTBfef6TANBgkqhkiG9w0BAQsFADB0MQswCQYDVQQGEwJVUzELMAkGA1UECAwCTk
MxDDAKBgNVBACMA1JUUDENMAsgA1UECgwETUNOQzEMMAoGA1UECwwDQ05FMQwwCgYDVQ
QDDAMzNjUxH3AdBgkqhkiG9w0BCQEWEGRkdW5sYXBAWNUy5vcmcwHhcNMjExMjM0MTQwNDU

3WhcNMjQxMjI5MTQwNDU3WjB0MQswCQYDVQQUeWJVUzELMAkGA1UECAwCTkMxDDAKBgNVBAcMA1JUUDENMAAsGA1UECgwETUNOQzEMMAoGA1UECwwDQ05FMQwwCgYDVQQDDAMzNjUxHZA dBGkqhkiG9w0BCQEWEGRkdW5sYXBAbWNuYy5vcmcwggliMA0GCSqGSIb3DQEBAQUAA4ICDwAwg gIKAoICAQDtK4mONKLmSkLSQPIAZ4NRj1qKtmEOQmlwLe3wH5wqrVNMK5LBsGsVd7JVX+cHwuW4D WUQqfKA v2Nj4+Ku/gCO2t9HyhX5sUHMnJ1ZKdFTgG0fjkSGS6SDD/NQjLXnElvHv1jfMvCb5OaRgOEN 2cLfJ6ZibTtT/PkfG3+6WEK3MjHAbcAFy6HFCSSlfM4eDaB6d1VkonxWN7C+jmatKtCSsmX8RCCiC6dD/ 2zaga97S7QDgWKI9yxuHFUf3HHV77gNPYaYmkKy5we6fFVUtjvRY/tdu7RBLg8ZncXTyjJb87ljzS3t/6bw0 wsdMrHfCJNsqqE7bWgZ/EY8YN/IULNZO28Xd7B7aanCSD8GSduVPNpFPJ7OKYBqqkKMLa2DT4h2w3 nfnW6pVlZAlnbwSxGe/ZNyls1k3oSh3WigUTKQduuw1INj1I/aKKJhPxBwBUXIQMIacifuRm3Ag6Zy+t2ewt 1tF3heT06ebllhS1Wur2muVvWeiQx/ZpnE03+5ChCFpf5TXerSzKqDuhsl75OTEuHXbFqxNOTxklC7zw 1F2VcJYnYLDgGumbkby67ug48VjXK/hE4HFquVkoWHBmXIFoUpForN0sgYqwOgRHBwB9XRsiiaAi3K+ 1aRSyEQ6DbxzOWrTTRpkLe04hvcBVO4wKBOSpwa1S8tbwhMQqAQIDAQABMA0GCSqGSIb3DQEB CwUAA4ICAQBQmPH0VNIQsMuNwibq9dliIUyO7LdyePQuJPvLfg/Dns0wm7far+cK90jf9oG5W3PiungP KRJbSO2TfNj00pRgByew/X5zU237qJahYYAWzgGsKYKx3EljJW1AfPRrCzJoMeyVncX5nypvSs23CYzG wy+nMGQ2x3tHuBehcme8TAa7Z9dK8FF9WISigtfcFeBjQY8lQoualTwUSQrmull/EcsPnqcZKgAZ0T24ize kT6Yv4Q7R+JghJxqEnqbBWx4xFSeBqSqSdUJOvIsSEmfShq98dd6GWBtksMZVxl5qzjCyExtE6kiDSCoZ XMxuT2YouVzQ5T7hpHpgO9AHXKUI4cuBVA21n+eCl6rBxKdxk1r9iID5ZcHoU6eT201qbck+j1W4uHcLP oXhgHvaeMwlcZD1wV54vzvCVNTY00UpTDFIoNiTbUXTVtAt3/+nVeFojypNs5OpozNsD8gMo/butG7P4bb UKhTq/pZGKgYLoXNKLqmYwpQjiUkZ1lySS7s/ojvTmsPCqO7ECz9SB1PSxjhj1ayaUx0wNHaxU9fWyt6 xgCqxqmJbTfnTPJsNF+2e2HfJDUDjPMct1wF/boWTV+Lm1VxbSvxVK1BfrMovMUXscvzv1TWSPB0kkT RBgqhaUhPF91euaG92vCS6dk++0qTnrV7nI33mymbK0jNw==</X509Certificate></X509Data></KeyInfo ></Signature><Subject><NameID

Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">cfo@k12o365.mcnc.org</NameID ><SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><SubjectConfirmationData InResponseTo="_A15CFB0681F334E8AE98300435440A51" NotOnOrAfter="2021-12-30T19:00:32.068Z" Recipient="https://365.k12.nc.us/+CSCOE+/saml/Dec 30 13:00:32

[SAML] consume_assertion:

https://sts.windows.net/ed3fe6d3-252d-4214-a808-15a4def117e2/ cfo@k12o365.mcnc.org

[saml] webvpn_login_primary_username: SAML assertion validation succeeded

webvpn_portal.c:webvpn_login_primary_password[3637]

webvpn_portal.c:webvpn_login_secondary_username[3667]

webvpn_portal.c:webvpn_login_secondary_password[3754]

webvpn_portal.c:webvpn_login_extra_password[3805]

webvpn_portal.c:webvpn_login_set_cookie_flag[3827]

webvpn_portal.c:webvpn_login_set_auth_group_type[3851]

webvpn_login_set_auth_group_type: WEBVPN_AUTH_GROUP_TYPE = 4

webvpn_portal.c:webvpn_login_aaa_resuming[3872]

webvpn_auth.c:http_webvpn_post_authorize[2363]

http_webvpn_post_authorize: AUTH_ACCEPT, WEBVPN_AUTH_USERNAME = cfo@k12o365.mcnc.org

webvpn_auth.c:http_webvpn_auth_accept[2742]

Start timer for verifying token 543152244E581AB735FF2DB

Username "cfo@k12o365.mcnc.org" added to list with token 543152244E581AB735FF2DB

webvpn_remove_auth_handle: auth_handle = 0

http_remove_auth_handle(): handle 0 not found!

webvpn_portal.c:webvpn_login_aaa_resuming[3892]

ewaFormSubmit_webvpn_login() -> redirect status=1 ret='NULL'

webvpn_free_auth_struct: net_handle = 0x00007f6494fa5fa0

webvpn_allocate_auth_struct: net_handle = 0x00007f6494fa5fa0
webvpn_free_auth_struct: net_handle = 0x00007f6494fa5fa0
#0x00007f64942d9350 (GET). Request line:/+CSCOE+/logon.html
#0x00007f64942d9350 File to execute: /+CSCOE+/logon.html
#0x00007f64942d9350 (GET). Request line:/+CSCOE+/saml_ac_login.html
#0x00007f64942d9350 File to execute: /+CSCOE+/saml_ac_login.html
saml_auth_is_valid_token: SAML ac token being looked 543152244E581AB735FF2DB
#0x00007f64942d9350 (GET). Request line:/+CSCOU+/saml_ac.css
#0x00007f64942d9350 File to execute: /+CSCOU+/saml_ac.css
#0x00007f64942d9350 (GET). Request line:/+CSCOU+/check.png
#0x00007f64942d9350 File to execute: /+CSCOU+/check.png
#0x00007f64942d83f0 (GET). Request line:/+CSCOU+/cisco_saml.png
#0x00007f64942d83f0 File to execute: /+CSCOU+/cisco_saml.png
#0x00007f64942d9870 (GET). Request line:/+CSCOU+/csr.ttf
#0x00007f64942d9870 File to execute: /+CSCOU+/csr.ttf
#0x00007f64942d9b00 (POST). Request line:/
#0x00007f64942d9b00 File to execute: /CSCOSSLC/config-auth
/CSCOSSLC/config-auth
Processing client request
XML successfully parsed
Processing request (auth-reply)
auth-reply: aggaauthHandle unknown
Found tunnel group (Finance) alias Finance
saml_ac_v2_process_auth_request: SAML ac token being looked 543152244E581AB735FF2DB
SAML AUTH: authentication success
SAML auth request finished
Opened AAA handle 4777034
Making AAA request
webvpn_session_add() -> key = 0x1900058000
AAA request finished
Send auth complete
saml_ac_token_entry_reset_saml_session: SAML ac token being looked 543152244E581AB735FF2DB
Verification complete stop timer for token 543152244E581AB735FF2DB
Private archive directives retrieved from cache for index 1.
Public archive directives retrieved from cache for index 1.
rcode from handler = 0
Sending response
Closing AAA handle 4777034
SAML AUTH: SAML hash table cleanup periodic task
#0x00007f64942d8160 (CONNECT). Request line:/CSCOSSLC/tunnel
#0x00007f64942d8160 Hand-off to webvpn.
CSTP read buffer allocated successfully
Successfully added 27 bytes from block to CSTP read buffer
Successfully added 1634 bytes from block to CSTP read buffer
CSTP read buffer updated successfully
Anyconnect STRAP[Peer:172.2.203.169]: new public key received for session

Anyconnect STRAP[Peer:172.2.203.169]: client/server upgraded to STRAP supported version,
successfully stored the public key received

ASA show

'Show' command to look at user connection:

show vpn-sessiondb detail anyconnect

365# sho vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : cfo@k12o365.mcnc.org Index : 88
Assigned IP : 10.2.3.4 Public IP : 172.2.203.169
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx : 14640 Bytes Rx : 15760
Pkts Tx : 10 Pkts Rx : 225
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : Finance Tunnel Group : Finance
Login Time : 13:00:33 EST Thu Dec 30 2021
Duration : 0h:00m:35s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : c0a846010005800061cdf3c1
Security Grp : none

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 88.1

Public IP : 172.2.203.169

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 88.1

Public IP : 172.2.203.169

Encryption : none Hashing : none

TCP Src Port : 51180 TCP Dst Port : 443

Auth Mode : SAML

Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes

Client OS : mac-intel
Client OS Ver: 12.0.1
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Mac OS X 4.10.01075
Bytes Tx : 7320 Bytes Rx : 0
Pkts Tx : 5 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 88.2
Assigned IP : 10.2.3.4 Public IP : 172.2.203.169
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 11496
TCP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Mac OS X
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Mac OS X 4.10.01075
Bytes Tx : 7320 Bytes Rx : 2710
Pkts Tx : 5 Pkts Rx : 32
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 88.3
Assigned IP : 10.2.3.4 Public IP : 172.2.203.169
Encryption : AES256 Hashing : SHA1
Ciphersuite : AES256-SHA
Encapsulation: DTLSv1.0 UDP Src Port : 60604
UDP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Mac OS X
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Mac OS X 4.10.01075
Bytes Tx : 0 Bytes Rx : 13174
Pkts Tx : 0 Pkts Rx : 195
Pkts Tx Drop : 0 Pkts Rx Drop : 0

365 certificate expiration

When the 365 certificate expires, you will need to generate a new .pfx certificate using openssl, upload to the Enterprise Apps, make that certificate active, download a .pem file from one of the apps, and replace the old certificate in the ASA (i.e. do that part of the previous process over again).

Due to a Cisco bug - <https://quickview.cloudapps.cisco.com/quickview/bug/CSCvi23605> - it may be necessary to remove the "trustpoint idp Azure" from the webvpn area, remove the "crypto ca trustpoint Azure", add the "crypto ca trustpoint Azure" and new certificate, re-add "trustpoint idp Azure" to the webvpn area, then remove and re-add the saml setting under the tunnel-group for example:

tunnel-group Finance webvpn-attributes

no authentication saml

no saml identity-provider <https://sts.windows.net/ed3fe6d3-252d-4214-a808-15a4def117e2/>

authentication saml

saml identity-provider <https://sts.windows.net/ed3fe6d3-252d-4214-a808-15a4def117e2/>

Basically the ASA does not seem to do well with clearing the trustpoint - due to the bug, this sequence-sensitive process needs to be followed to ensure continuity. The bug is fixed in extremely current releases.

Dianne Dunlap

ddunlap@mailbox.mcnc.org

1/2022