

CCIE SECURITY v6.1 Real Labs--- DOO Module

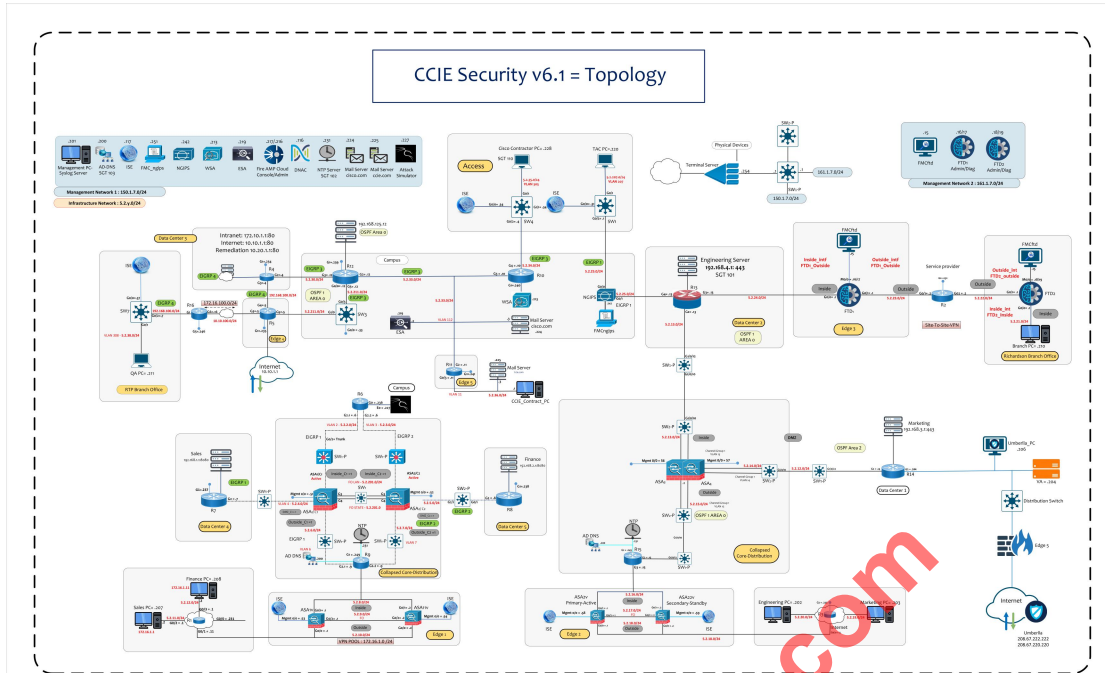
Module2-DOO

Ver: 1

Part 1

©www.passccielab.com all rights reserved.

www.passccielab.com



1.2 Anyconnect VPN on ASA1v/ASA11v

You have been asked to configure a remote VPN solution in the interface Edge 1 layer of the network to support traffic from the Sales and Finance organization. The requirements are as follows:

- Clients must be able to establish remote VPN sessions with an idle timeout of 1 day.
- Active Directory must be used for the authentication.
- Only traffic that is destined for the Sales server, Finance server and NTP server must be encrypted.
- Traffic between Sales PC and Finance PC should be allowed.
- For the Sales organization, the address must be assigned from the block of 172.16.1.1-172.16.1.10/24
- For the Finance organization, the addresses must be assigned from the block of 172.16.1.11-172.16.1.20/24
- DACL must permit traffic destined to Sales server, Finance server, NTP server and DNS server.
- DACL must permit ICMP traffic between Sales PC and Finance PC.

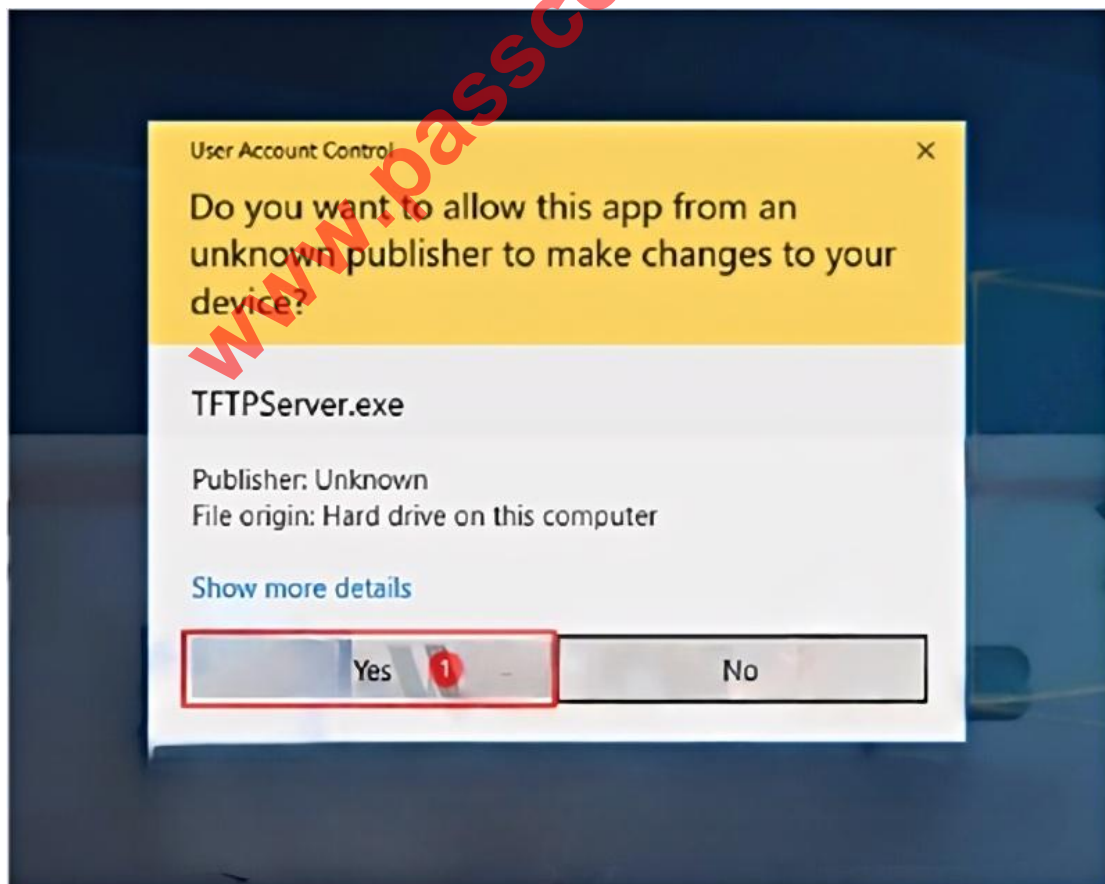
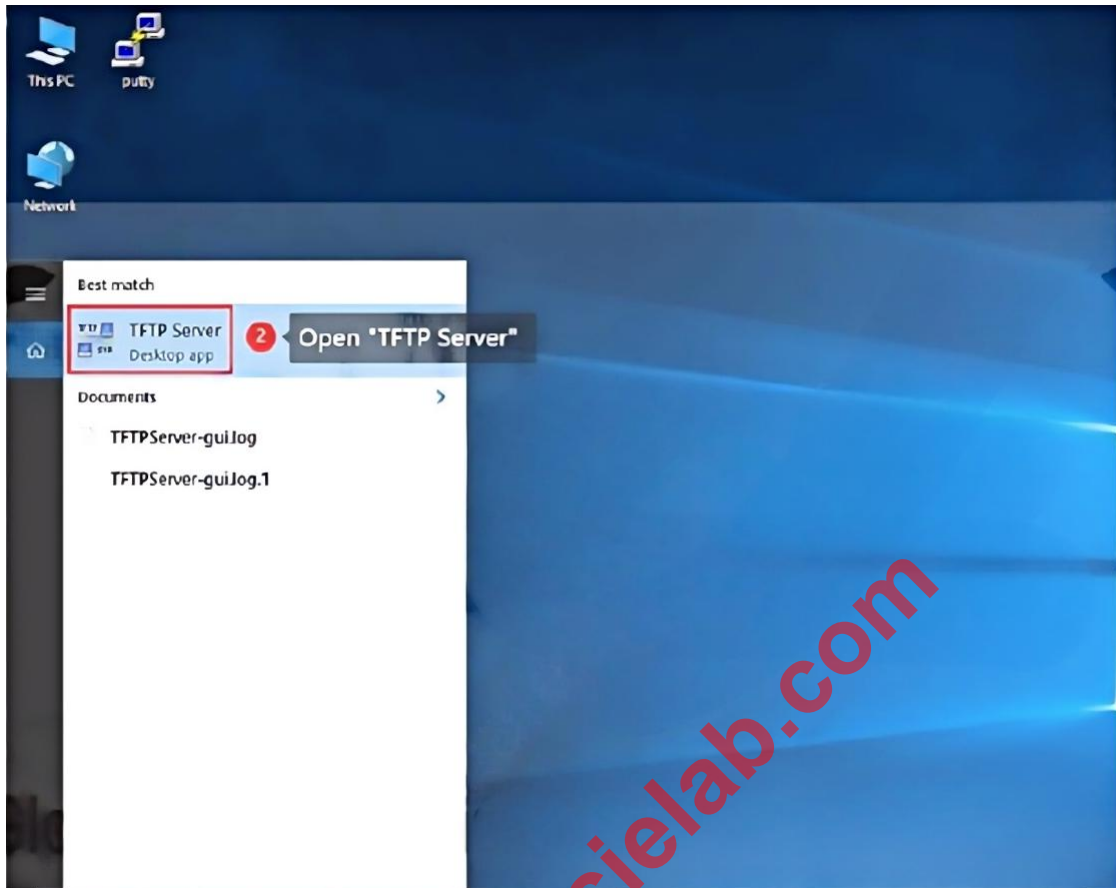
Notes:

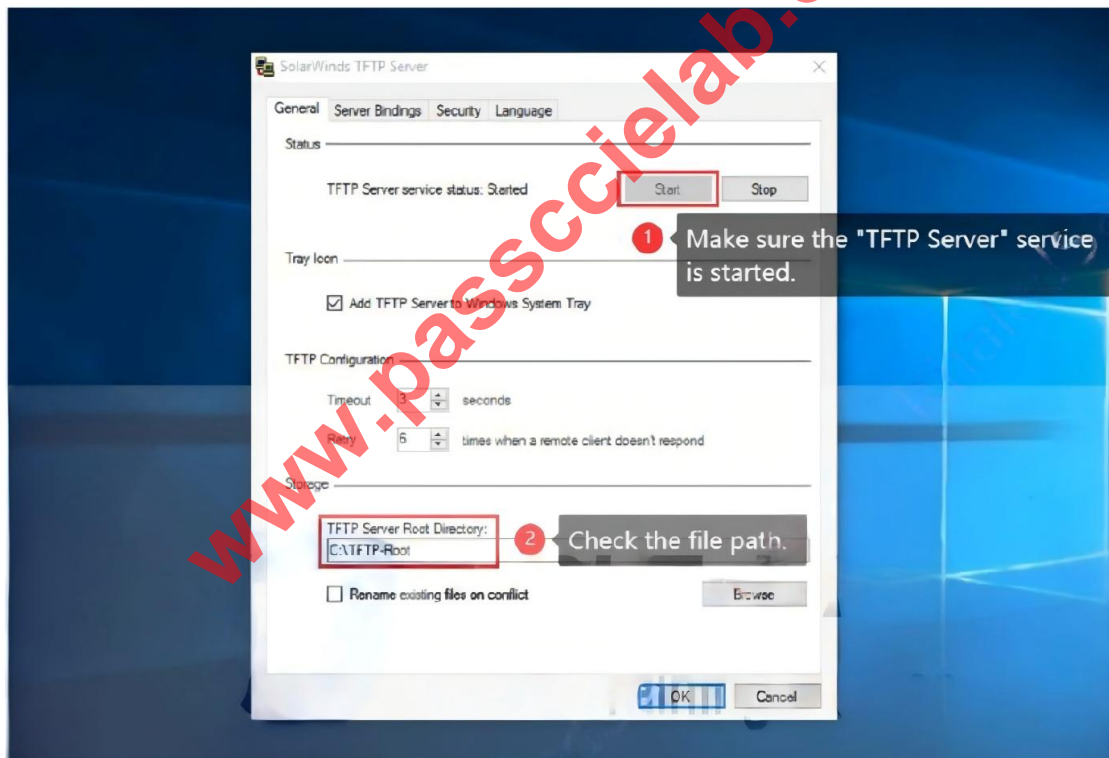
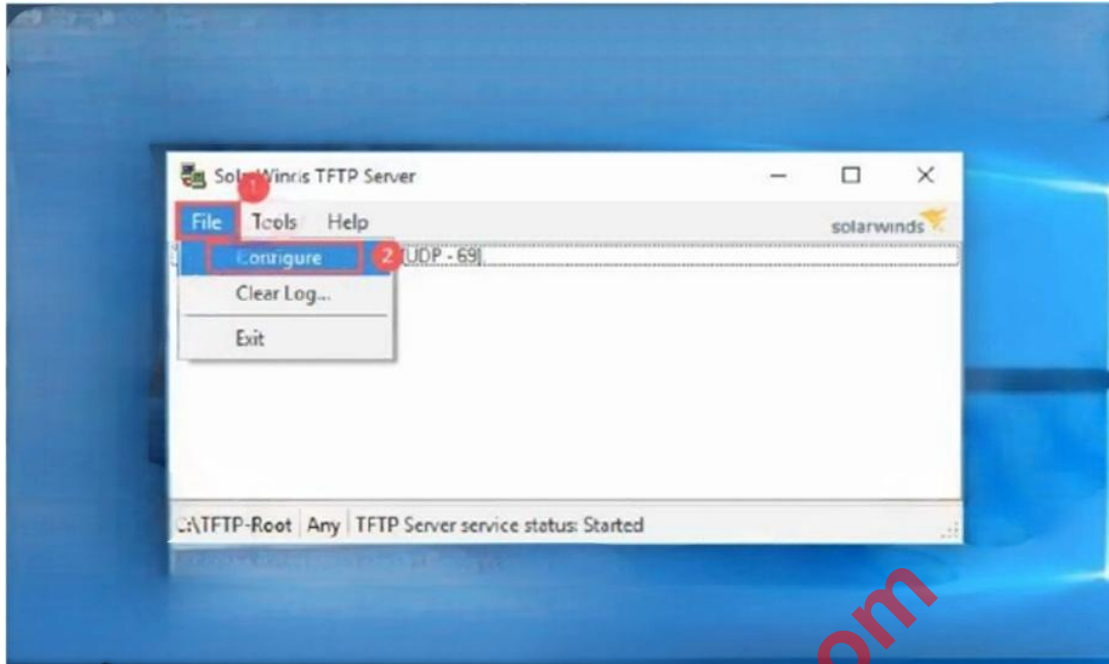
- For the deployment you must use the addresses provided under the "Addressing Tables" tab for Task 1.2

Solution:

Management PC

Open TFTP server Application





ASA3:

ASA3/ASA3/slaver#dir

leaderDirectory of disk0:/

(--Omitted here--)

110 -rwx 19473166 06:28:30 Nov 252020 anyconnect-win-4.2.04018-k9.pkg

(--Omitted here--)

4118085632 bytes total(711901184 bytes free)

ASA3/ASA3/master#

ASA3/SA3/master#copy disk0:/anyconnect-win-4.2.04018-k9.pkg tftp:

Source filename [anyconnect-win-4.2.04018-k9.pkg]?<Press "Enter">

Address or name of remote host []?150.1.7.201

Destination filename [anyconnect-win-4.2.04018-k9.pkg]?<Press

"Enter">!!!

(--Omitted here--)

!!19473166 bytes copied in 24.870

secs(811381 bytes/sec)ASA3/ASA3/slaver#

ASA1v:

ASA1v/pri/act#dir

Directory of disk0:/

(--There is no anyconnect-win-4.2.04018-k9.pkg here--)

8571076608 bytes total (8559845376 bytes free)

ASA1v/pri/act#

ASA1v/pri/act#copy tftp:anyconnect-win-4.2.04018-k9.pkg disk0:

Address or name of remote host []?150.1.7.201

Source filename [anyconnect-win-4.2.04018-k9.pkg]?<Press"Enter">

Destination filename [anyconnect-win-4.2.04018-k9.pkg]? <Press"Enter">

Accessing tftp://150.1.7.201/anyconnect-win-4.2.04018-k9.pkg..

!!

!!!!!!!

(--Omitted here--)

!!

!!!!!!!

Writing file disk0:/anyconnect-win-4.2.04018-k9.pkg..

Gateway of last resort is not set

C 5.2.3.0255.255.255.0 is directly connected,inside

L 5.2.3.1255.255.255.255 is directly connected,inside

C 5.2.5.0255.255.255.0 is directly connected,dmz

L 5.2.5.1255.255.255.255 is directly connected,dmz

C 5.2.7.0255.255.255.0 is directly connected,outside

L 5.2.7.1255.255.255.255 is directly connected,outside

S 19.16.2.1255.255.255.255[1/0]via 5.2.5.8.dmz

DEX 161.1.7.0255.255.255.0 [170/3072]via 5.2.7.9,00:00:37,outside

D EX 172.16.0.0255.255.0.0[170/3072]via 5.2.7.9,00:00:37,outside

DEX 172.16.1.0255.255.255.0 [170/3072]via 5.2.7.9,00:01:37,outside

D 192.168.2.0255.255.255.0 [90/130816]via 5.2.5.8,00:01:41,dmz

ASA1/c1/sec/act#

ASA2-c2;

ASA1/c2/pri/act(config)#route dmz 19.16.11255.255.255.255.2.4.7

ASA1/c2/pri/act(config)router eigrp 1

ASA1/c2/pri/act(config-router)#redistribute staticASA1/c2/pri/act(config-router)#exit

ASA1/c2/pri/act(config)#

Verify on ASA2-c2:

ASA1/c2/pri/act#show route

Routing Table:c2

Codes.L-local,C-connected,S-static,R-RIP,M-mobile,B-BGP

D -EIGRP,EX-EIGRP external,O-OSPF,IA-OSPF inter area

N1 -OSPF NSSA external type 1,N2-OSPF NSSA external type 2

E1 -OSPF external type 1,E2-OSPF external type 2

I -IS-IS,su-IS-IS summary,L1-IS-IS level-1,L2-IS-IS level-2

la -IS-IS inter area*-candidate default,U-per-user static routeo-

O -DR,P-periodic downloaded static route,+-replicated route

Gateway of last resort is not set

C 5.2.2.0/255.255.255.0 is directly connected,inside

L 5.2.2.1255.255.255.255 is directly connected,inside

C 5.2.4.0/255.255.255.0 is directly connected,dmz

L 5.2.4.1255.255.255.255 is directly connected,dmz

C 5.2.6.0/255.255.255.0 is directly connected,outside

L 5.2.6.1255.255.255.255 is directly connected,outside

S 19.16.1.1255.255.255.255[1/0]via 5.2.4.7,dmz

DEX 161.1.7.0/255.255.255.0 [170/3072]via 5.2.6.9,01:52:00,outside

D EX 172.16.0.0/255.255.0.0[170/3072]via 5.2.6.9,01:52:00,outside

D EX 172.16.1.0/255.255.255.0[170/3072]via 5.2.6.9,00:11:11,outside

D 192.168.1.0/255.255.255.0 [90/130816]via 5.2.4.7,01:53:40,dmz

ASA1/c2/pri/act#

R9:

R9#show ip route eigrp

Codes:L-local,C-connected,S-static,R-RIP,M-mobile,B-BGP

D-EIGRP,EX-EIGRP external,O-OSPF,IA-OSPF inte,area

N1-OSPF NSSA external type 1,N2-OSPF NSSA external type 2

E1-OSPF external type 1,E2-OSPF external type 2

i-IS-IS,su-IS-IS summary,L1-IS-IS level-1,I2-IS-IS level-2

ia -IS-IS inter area,★-candidate default,U-per-user static route

o-ODR,P-periodic downloaded static route,H-NHRP,I-LISP

a-application route

+--replicated route,-next hop override,p-overrides from PIR

Gateway of last resort is not set

5.0.0.0/8 is variably subnetted,10 subnets,2 masks

D 5.2.2.0/24 [90/3072]via 5.2.6.1,02:03:28,GigabitEthernet2.1

D 5.2.3.C/24 [90/3072]via 5.2.7.1,00:04:54,GigabitEthernet2.2

D 5.240/24 [90/3072]via 5.2.6.1,02:03:28.GigabitEthernet2.1
D 5.2.5.0/24 [90/3072]via 5.2.7.1,00:04:54,GigabitEthernet2.2
DEX 19.16.1.1 [170/3072]via 5.2.6.1,00:12:01,GigabitEthernet2.1
DEX 19.16.2.1 [170/3072]via 5.2.7.1,00:04:54,GigabitEthernet2.2
D 192.168.1.0/24 [90/131072]via 5.2.6.1,02:03:28,GigabitEthernet2.1
D 192.168.2.0/24 [90/131072]via 5.2.7.1,00:04:52,GigabitEthernet2.2

R9#

ASA11v:

ASA1v/pri/act(config)#route inside 19.16.1.1255.255.255.2555.2.8.9
ASA1v/pri/act(config)#route inside 19.16.2.1255.255.255.2555.2.8.9
ASA1v/pri/act(config)#route inside 150.1.7.200255.255.255.2555.2.8.9
ASA1v/pri/act(config)#route inside 150.1.7.231 255.255.255.2555.2.8.9
ASA1v/pri/act(config)# dns domain-lookup inside
ASA1v/pri/act(config)# dns domain-server 150.1.7.200
ASA1v/pri/act(config)#domain-name cisco.com
ASA1v/pri/act(config)#http server enable
ASA1v/pri/act(config)#http 150.1.7.0255.255.255.0 mgmt
ASA1v/pri/act(config)#crypto key generate rsa label cciekey modulus 1024
INFO:The name for the keys will be:cciekey
Keypair generation process begin.Please wait..
ASA1v/pri/act(config)#
ASA1v/pri/act(config)#crypto ca trustpoint ccietrust
ASA1v/pri/act(config-ca-trustpoint)#enrollment self
ASA1v/pri/act(config-ca-trustpoint)#fqdn asa1.cisco.com
ASA1v/pri/act(config-ca-trustpoint)#subject-name CN=asa1.cisco.com
ASA1v/pri/act(config-ca-trustpoint)#keypair cciekey
ASA1v/pri/act(config-ca-trustpoint)#exit
ASA1v/pri/act(config)#crypto ca enroll ccietrust
WARNING:The certificate enrollment is configured with an fqdn

that differs from the system fqdn.If this certificate will be
used for VPN authentication this may cause connection problems.

Would you like to continue with this enrollment?[yes/no]:**yes**

%The fully-qualified domain name in the certificate will be:asa1.cisco.com

%Include the device serial number in the subject name?[yes/no]:**no**

Generate Self-Signed Certificate?[yes/no]:**yes**

ASA1v/pri/act(config)#

Verify on **ASA11v**:

ASA1v/pri/act#show crypto ca certificate

Certificate

Status:Available

Status Available

Certificate Serial Number:d24f4962

Certificate Usage:General

PurposePublic Key Type:RSA(1024 bits)

Signature Algorithm:SHA1 with RSA Encryption

Issuer Name:

hostname=asa1.cisco.com

cn=asa1.cisco.com

Subject Name:

hostname=asa1.cisco.com

cn=asa1.cisco.com

Validity Date:

start date:08:40:30 GMT Apr 32022

end date:08:40:30 GMT Mar 312032

Associated Trustpoints:ccietrust

CA Certificate

Status:Available

Certificate Serial Number:18dad19e267de8bb4a2158cdcc6b3b4a

Certificate Usage:General Purpose

Public Key Type:RSA(2048 bits)

Signature Algorithm:SHA1 with RSA Encryption

Issuer Name:

cn=VeriSign Class 3 Public Primary Certification Authority-G5

ou=(c)2006 Verisign\,Inc.-For authorized use only

ou=VeriSign Trust Network

o=VeriSign\,Inc.

c=US

Subject Name:

cn=VeriSign Class 3 Public Primary Certification Authority-G5

ou=(c)2006 Verisign\,Inc.-For authorized use only

ou=VeriSign Trust Networko=VeriSign\,Inc.

c=US

Validity Date:

start date:00:00:00 GMT Nov 82CC6

end date.:23:59:59 GMT Jul 162036

Associated Trustpoints:SmartCallHome ServerCA

ASA1v/pri/act#

Verify on ASA1v.

ASA1v/sec/stby#snow crypto ca certificate

Certificate

Status:Available

Certificate Serial Number:d24f4962

Certificate Usage:General Purpose

Public Key Type:RSA(1024 bits)

Signature Algorithm:SHA1 with RSA Encryption

Issuer Name;

hostname=asa1.cisco.com

cn=asa1.cisco.comSubject Name:

hostname=asa1.cisco.com

cn=asa1.cisco.com

Validity Date:

start date:08:40:30 GMT Apr 3 2022

end date:08:40:30 GMT Mar 31 2032

Associated Trustpoints:ccietrust

CA Certificate

Associated Trustpoints:ccietrust

CA Certificate

Status:Available

Certificate Serial Number:18dad19e267de8bb4a2158cdcc6b3b4a

Certificate Usage:General Purpose

Public Key Type:RSA(2048 bits)

Signature Algorithm:SHA1 with RSA Encryption

Issuer Name:

cn=VeriSign Class 3 Public Primary Certification Authority-G5

ou=(c)2006 Verisign, Inc.-For authorized use only

ou=VeriSign Trust Network

o=VeriSign, Inc.

c=US

Subject Name:

cn=VeriSign Class 3 Public Primary Certification Authority -G5

ou=(c)2006 Verisign, Inc.-For authorized use on,

ou=VeriSign Trust Network

o=VeriSign, Inc.

c=US

Validity Date:

start date:00:00:00 GMT Nov 8 2006

end date:23:59:59 GMT Jul 16 2036

Associated Trustpoints:SmartCallHome_ServerCA

ASA1v/sec/stby#

ASA1v/sec/stby#

ASA11v;

```

ASA1v/pri/act(config)#webvpn
ASA1v/priact(config-webvpn)#enable outside
INFO:WebVPN and DTLS are enabled on'outside'.
ASA1v/pri/act(config-webvpn)#anyconnect image disk0:/anyconnect-win-4.2.04018-k9.pkg
ASA1v/pri/act(config-webvpn)#anyconnect enable
ASA1v/pri/act(config-webvpn)#tunnel-group-list enable
ASA1v/pri/act(config-webvpn)#exit
ASA1v/pri/act(config)#access-list sales standard permit host 19.16.1.1
ASA1v/pri/act(config)#access-list sales standard permit host 150.1.7.231
ASA1v/pri/act(config)#access-list sales standard permit 172.16.1.0255.255.255.0
ASA1v/pri/act(config)#access-list finance standard permit host 19.16.2.1
ASA1v/pri/act(config)#access-list finance standard permit host 150.1.7.231
ASA1v/pri/act(config)#access-list finance standard permit 172.16.1.0255.255.255.0
ASA1v/pri/act(config)#ip local pool salespool 172.16.1.1-172.16.1.10 mask 255.255.255.0
ASA1v/pri/act(config)#ip local pool financepool 172.16.1.11-172.16.1.20 mask 255.255.255.0
ASA1v/pri/act(config)#group-policy sales internal
ASA1v/pri/act(config-group-policy)#dns-server value 150.1.7.200
ASA1v/pri/act(config-group-policy)#vpn-idle-timeout
1440ASA1v/pri/act(config-group-policy)#vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
ASA1v/pri/act(config-group-policy)#split-tunnel-policy tunnelspecified
ASA1v/pri/act(config-group-policy)#split-tunnel-network-list value sales
ASA1v/pri/act(config-group-policy)#split-dns value cisco.com
ASA1v/pri/act(config-group-policy)#default-domain value cisco.com
ASA1v/pri/act(config-group-policy)#address-pools value salespool
ASA1v/pri/act(config-group-policy)#webvpn
ASA1v/pri/act(config-group-webvpn)#anyconnect keep-installer installed
ASA1v/pri/act(config-group-webvpn)#always-on-vpn profile-setting
ASA1v/pri/act(config-group-webvpn)#exit
ASA1v/pri/act(config-group-policy)#exit
ASA1v/pri/act(config)#group-policy finance internal

```

ASA1v/pri/act(config)#group-policy finance attributes

ASA1v/pri/act(config-group-policy)#dns-server value 156.1.7.200

ASA1v/pri/act(config-group-policy)#vpn-idle-timeout 1440

ASA1v/pri/act(config-group-policy)#vpn-tunnel-protocol ikev2 ssl-client ssl-clientless

ASA1v/pri/act(config-group-policy)#split-tunnel-policy tunnelspecified

ASA1v/pri/act(config-group-policy)#split-tunnel-network-list value finance

ASA1v/pri/act(config-group-policy)#split-dns value cisco.com

ASA1v/pri/act(config-group-policy)#default-domain value cisco.com

ASA1v/pri/act(config-group-policy)#address-pools value financepool

ASA1v/pri/act(config-group-policy)#webvpn

ASA1v/pri/act(config-group-policy)#anyconnect keep-installer installed

ASA1v/pri/act(config-group-policy)#always-on-vpn profile-setting

ASA1v/pri/act(config-group-policy)#exit

ASA1v/pri/act(ccnfig-group-policy)#exit

ASA1v/pri/act(config)#aaa-server ISE protocol radius

ASA1v/pri/act(config-aaa-server-group)#dynamic-authorization

ASA1v/pri/act(config-group-policy)#vpn-tunnel-protocol ikev2 ssl-client ssl-clientless

ASA1v/pri/act(config-group-policy)#split-tunnel-policy tunnelspecified

ASA1v/pri/act(config-group-policy)#split-tunnel-network-list value finance

ASA1v/pri/act(config-group-policy)#split-dns value cisco.com

ASA1v/pri/act(config-group-policy)#default-domain value cisco.com

ASA1v/pri/act(config-group-policy)#address-pools value financepool

ASA1v/pri/act(config-group-policy)#webvpn

ASA1v/pri/act(config-group-policy)#anyconnect keep-installer installed

ASA1v/pri/act(config-group-policy)#always-on-vpn profile-setting

ASA1v/pri/act(ccnfig-group-policy)#exit

ASA1v/pri/act(config-group-policy)#exit

ASA1v/pri/act(config)#aaa-server ISE protocol radius

ASA1v/pri/act(config-aaa-server-group)#dynamic-authorization

ASA1v/pri/act(config-aaa-server-group)#interim-accounting-update

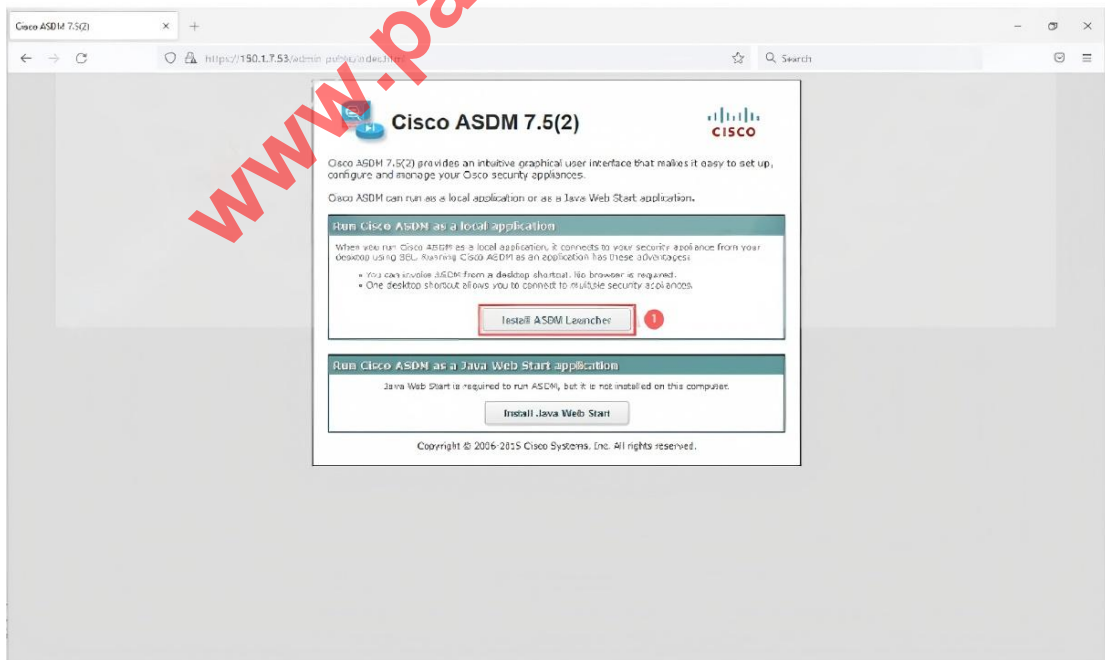
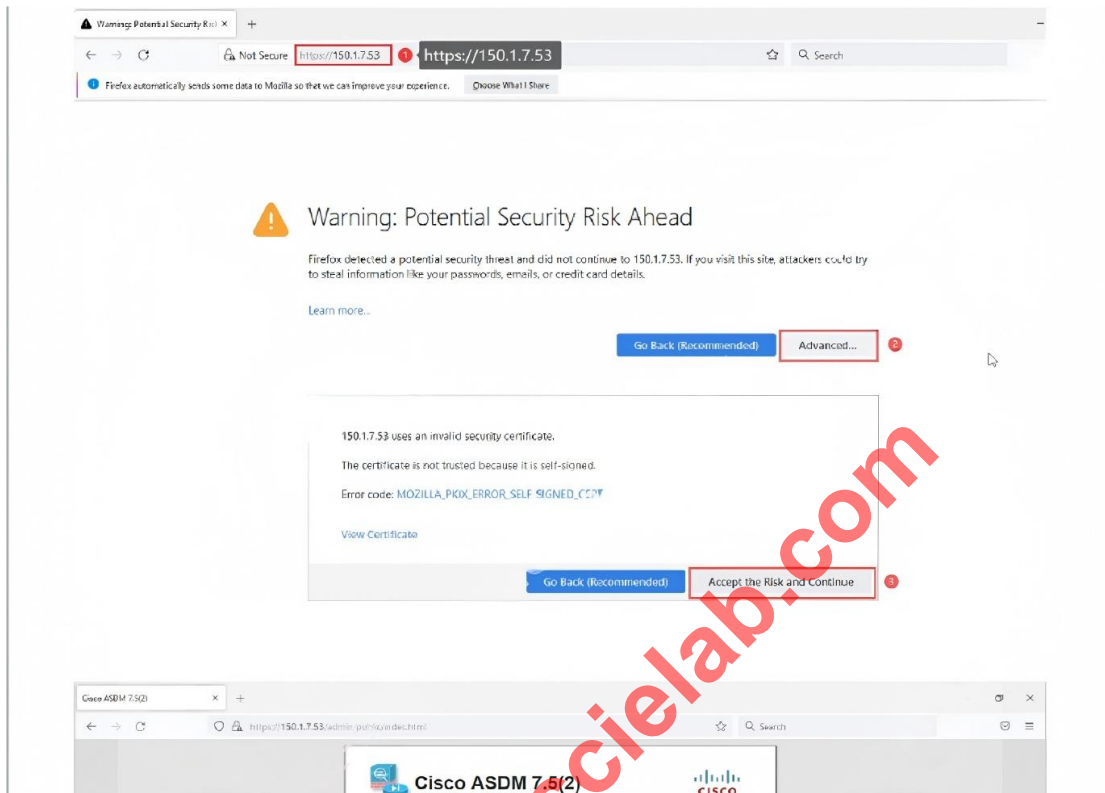
```
ASA1v/pri/act(config-aaa-server-group)#exit
ASA1v/pri/act(config)#aaa-server ISE(mgmt)host 150.1.7.117
ASA1v/pri/act(config-aaa-server-host)#key cisco
ASA1v/pri/act(config-aaa-server-host)#exit
ASA1v/pri/act(config)#tunnel-group sales type remote-access
ASA1v/pri/act(config)#tunnel-group sales general-attributes
ASA1v/pri/act(config-tunnel-general)#authentication-server-group ISE
ASA1v/pri/act(config-tunnel-general)#accounting-server-group ISE
ASA1v/pri/act(config-tunnel-general)#default-group-policy sales
ASA1v/pri/act(config-tunnel-general)#exit
ASA1v/pri/act(config)#tunnel-group sales webvpn-attributes
ASA1v/pri/act(config-tunnel-webvpn)#group-alias sales enable
ASA1v/pri/act(config-tunnel-webvpn)#exit
ASA1v/pri/act(config)#tunnel-group finance type remote-access
ASA1v/pri/act(config)#tunnel-group finance general-attributes
ASA1v/pri/act(config-tunnel-general)#authentication-server-group ISE
ASA1v/pri/act(config-tunnel-general)#accounting-server-group ISE
ASA1v/pri/act(config-tunnel-general)#default-group-policy finance
ASA1v/pri/act(config-tunnel-general)#exit
ASA1v/pri/act(config)#tunnel-group finance webvpn-attributes
ASA1v/pri/act(config-tunnel-webvpn)#group-alias finance enable
ASA1v/pri/act(config-tunnel-webvpn)#exit
ASA1v/pri/act(config)#group-policy sales attributes
ASA1v/pri/act(config-group-policy)#group-lock value sales
ASA1v/pri/act(config-group-policy)#exitASA1v/pri/act(config)#group-policy finance attributes
ASA1v/pri/act(config-group-policy)#group-lock value finance
ASA1v/pri/act(config-group-policy)#exit
ASA1v/pri/act(config)#i crypto ikev2 policy 10
ASA1v/pri/act(config-ikev2-policy)#encryption aes-255
ASA1v/pri/act(config-ikev2-policy)#integrity sha256
```

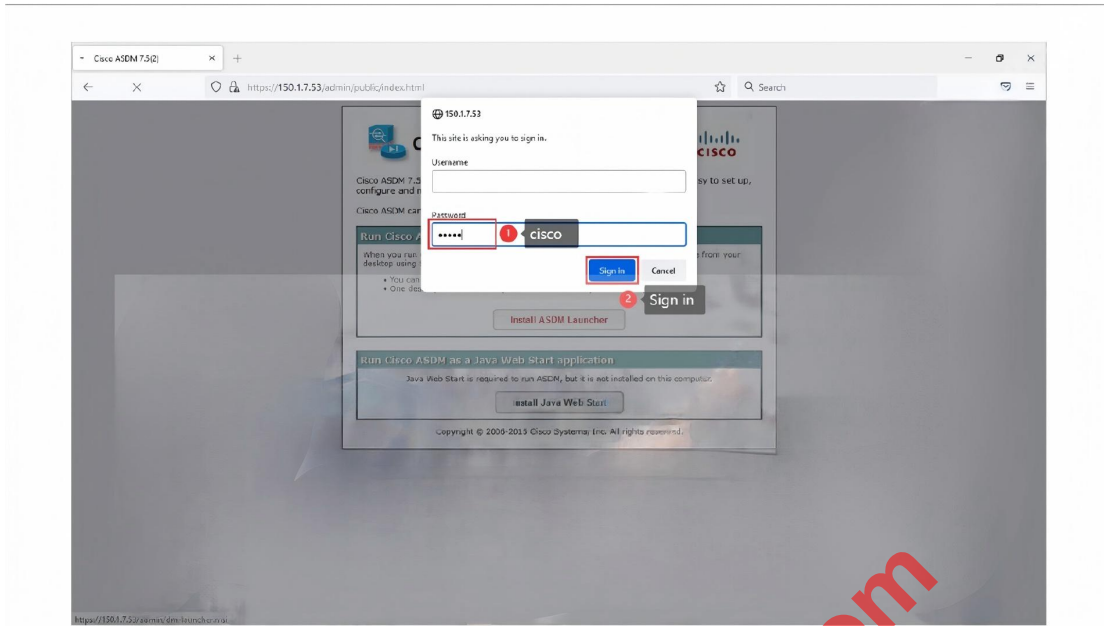
```
ASA1v/pri/act(config-ikev2-policy)#group 2ASA1v/pri/act(config-ikev2-policy)#exit
ASA1v/pri/act(config)crypto ipsecikev2 ipsec-proposal VPN
ASA1v/pri/act(config-ipsec-proposal)#protocol esp encryption aes-256
ASA1v/pri/act(config-ipsec-proposal)#protocol esp integrity sha-256
ASA1v/pri/act(config-ipsec-proposal)#exit
ASA1v/pri/act(config)#crypto dynamic-map DMAP 10 set ikev2 ipsec-proposal VPN
ASA1v/pri/act(config)i crypto dynamic-map DMAP 10 set reverse-route
ASA1v/pri/act(ccnfig crypto map CMAP65535 ipsec-isakmp dynamic DMAP
ASA1v/pri/act(contig)#crypto map CMAP interface outside
ASA1v/priact(config)#crypto ikev2 enable outside client-services port 443
ASA1v/pri/act(config)#crypto ikev2 remote-access trustpoint ccietrust
ASA1v/pri/act(config)#ssl trust-point ccietrust outside
ASA1v/pri/act(config)#
```

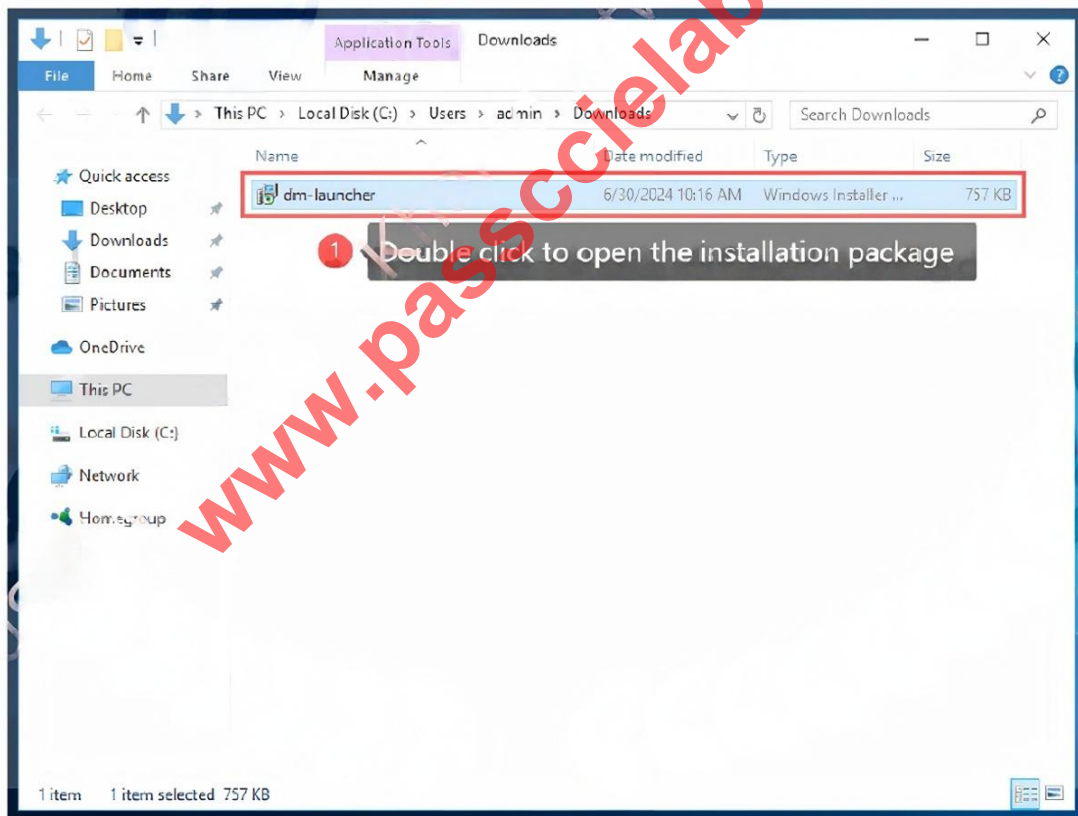
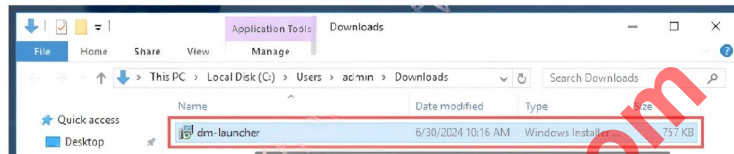
www.passccielab.com

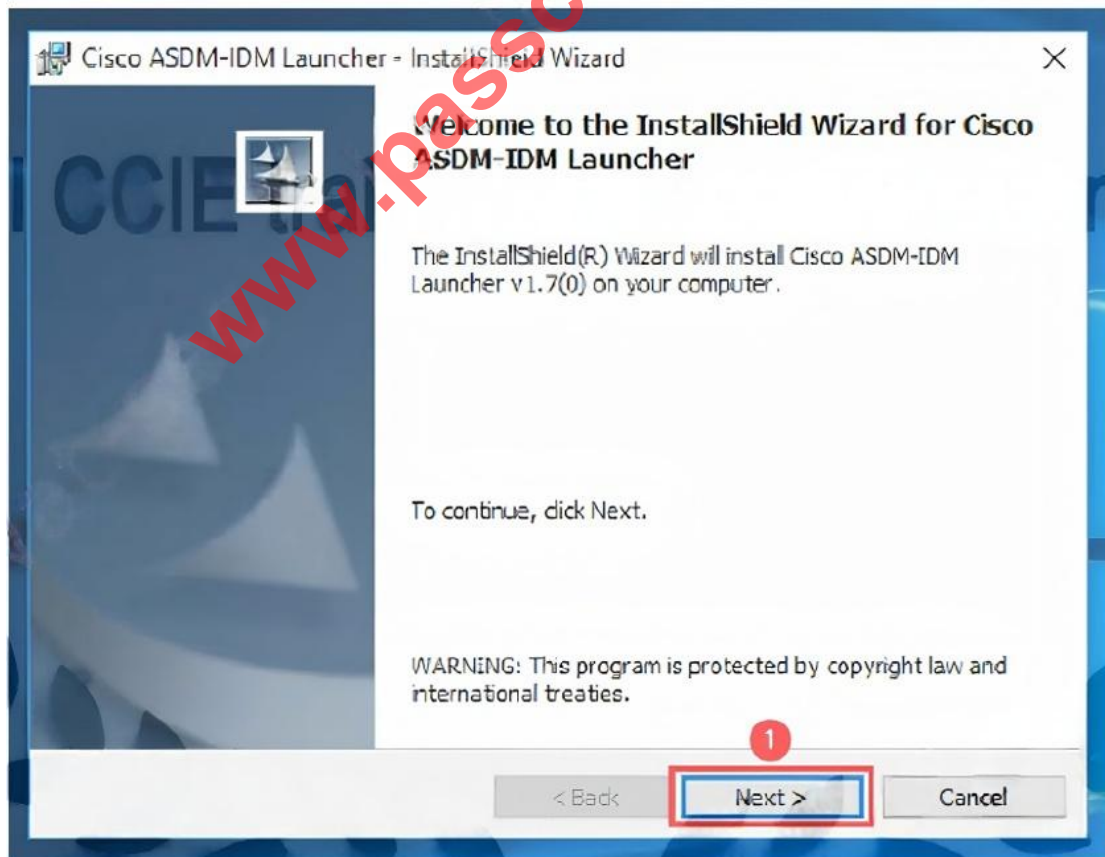
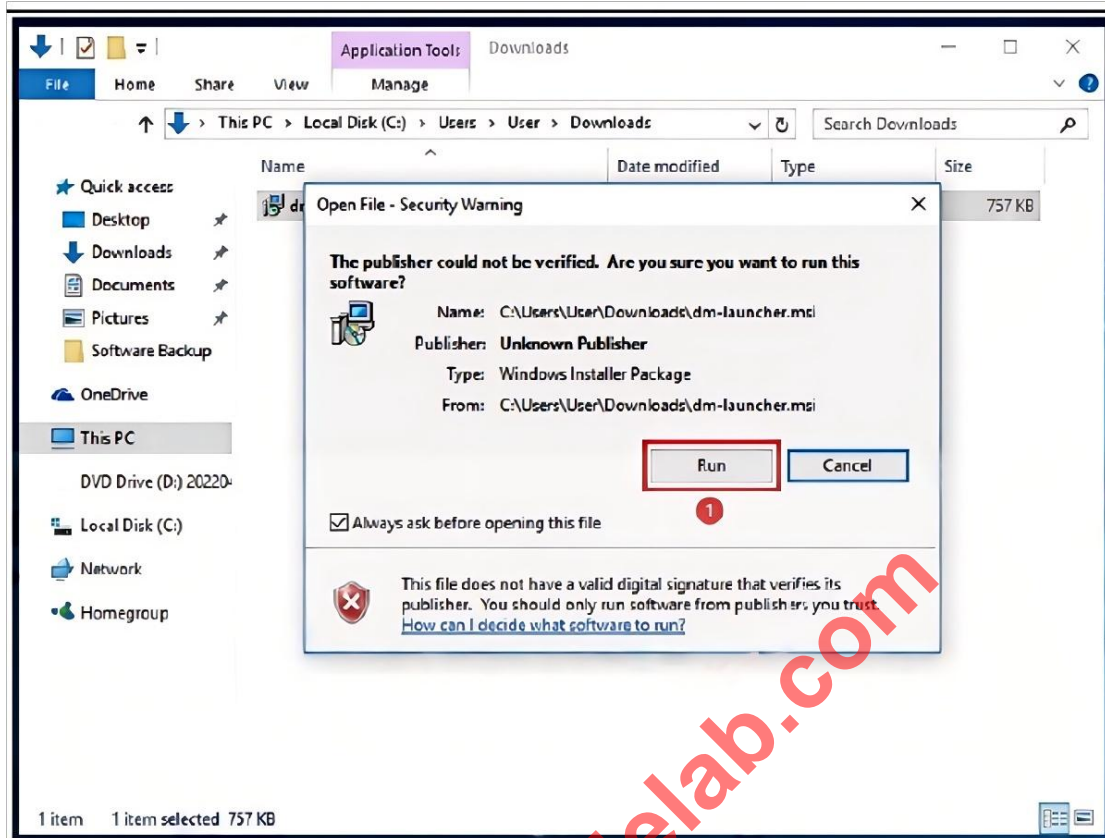
Management PC;

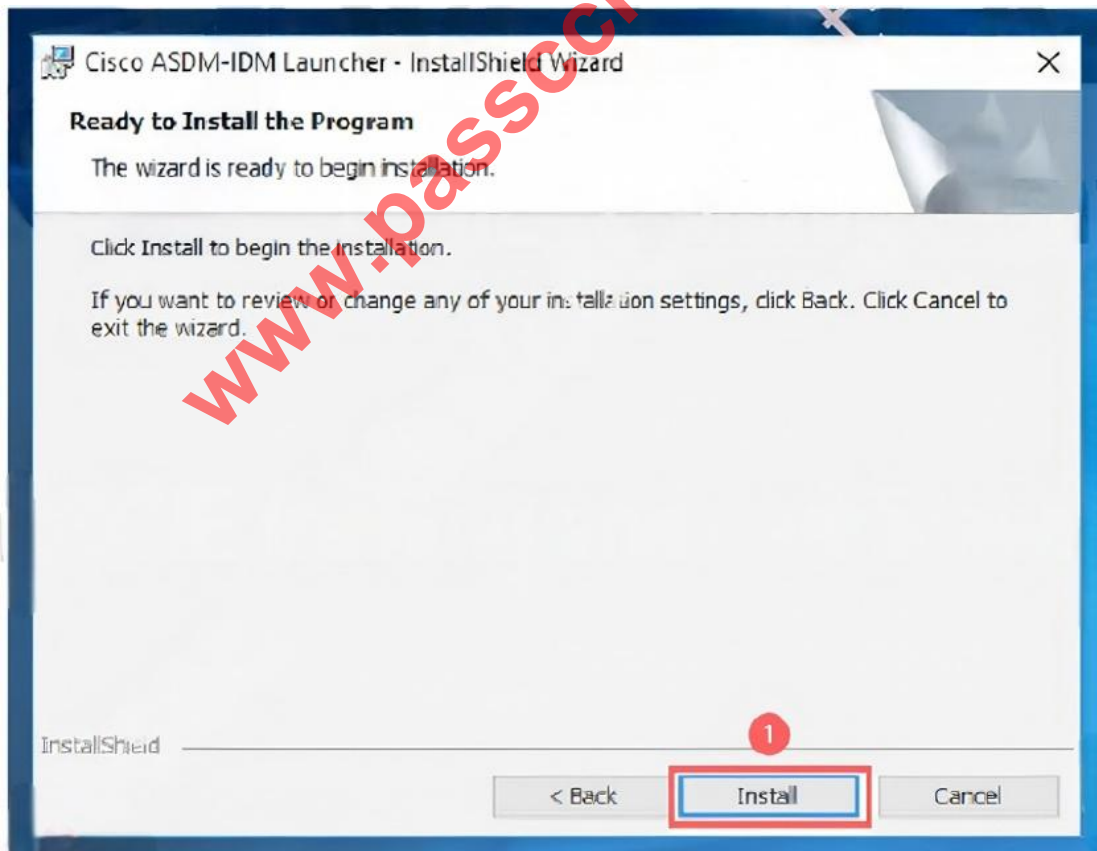
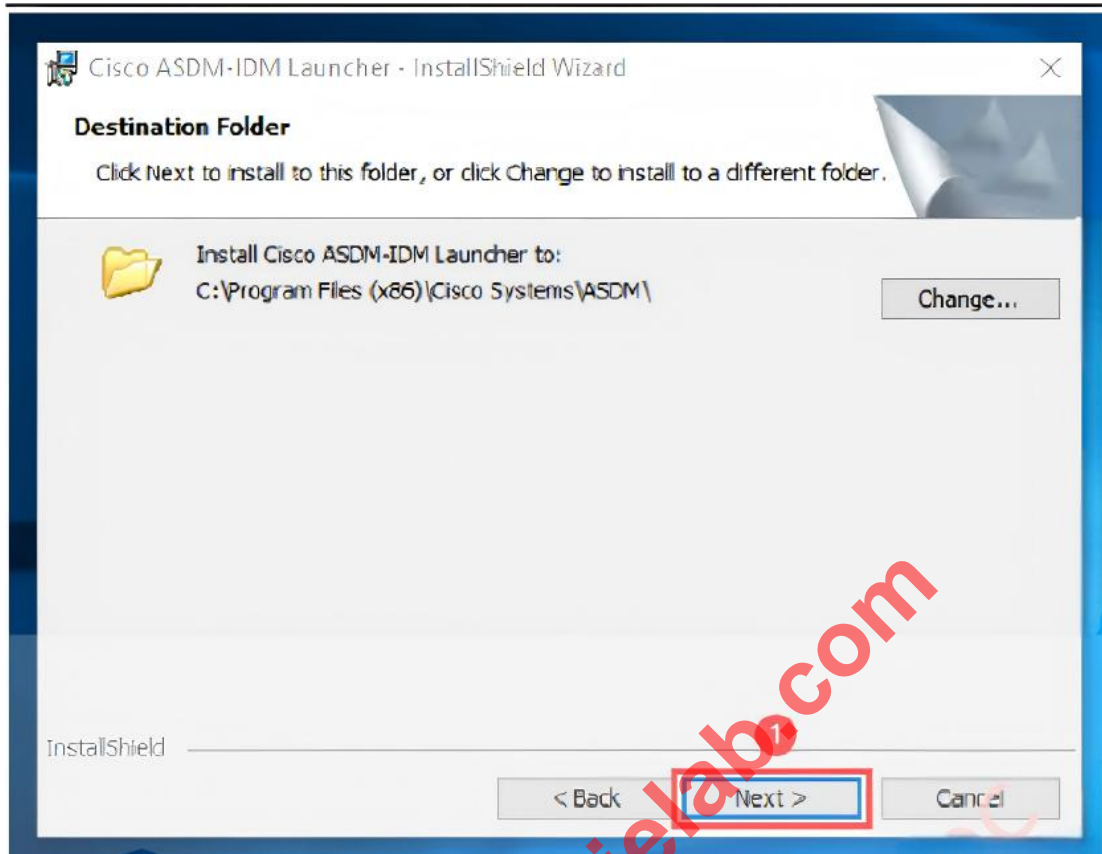
Download and open ASDM

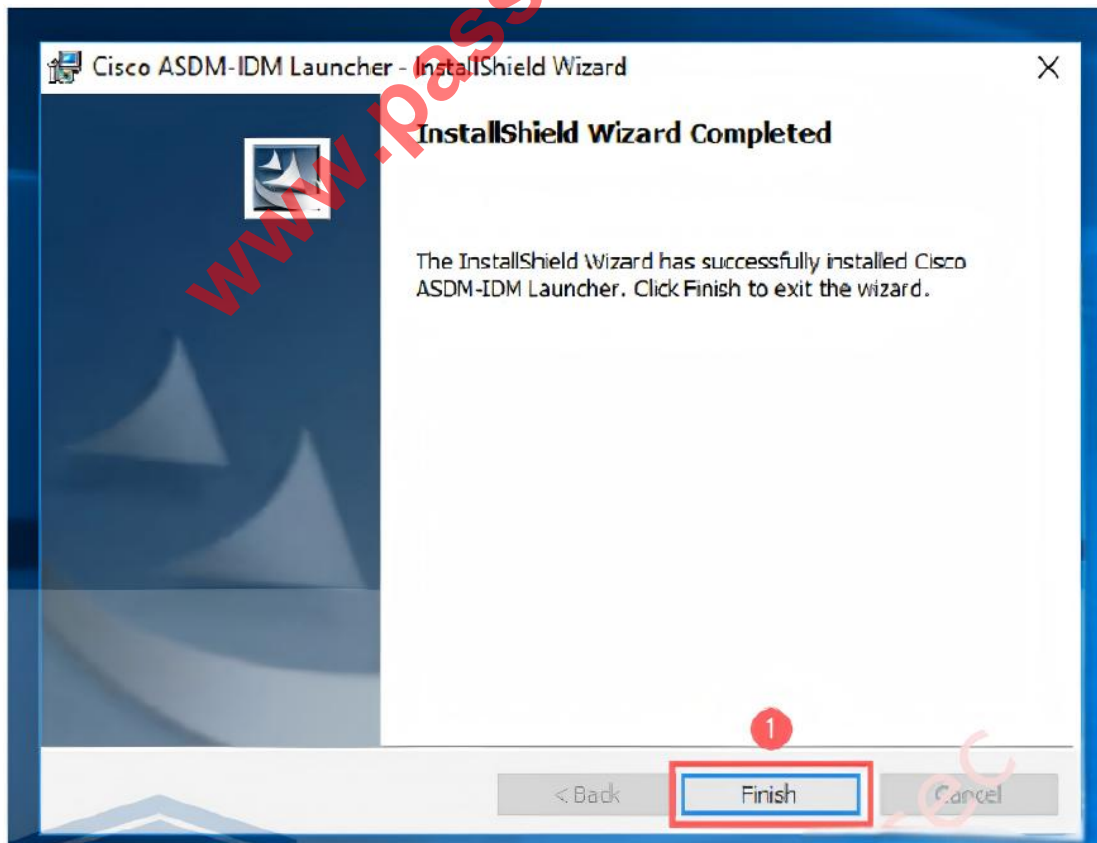


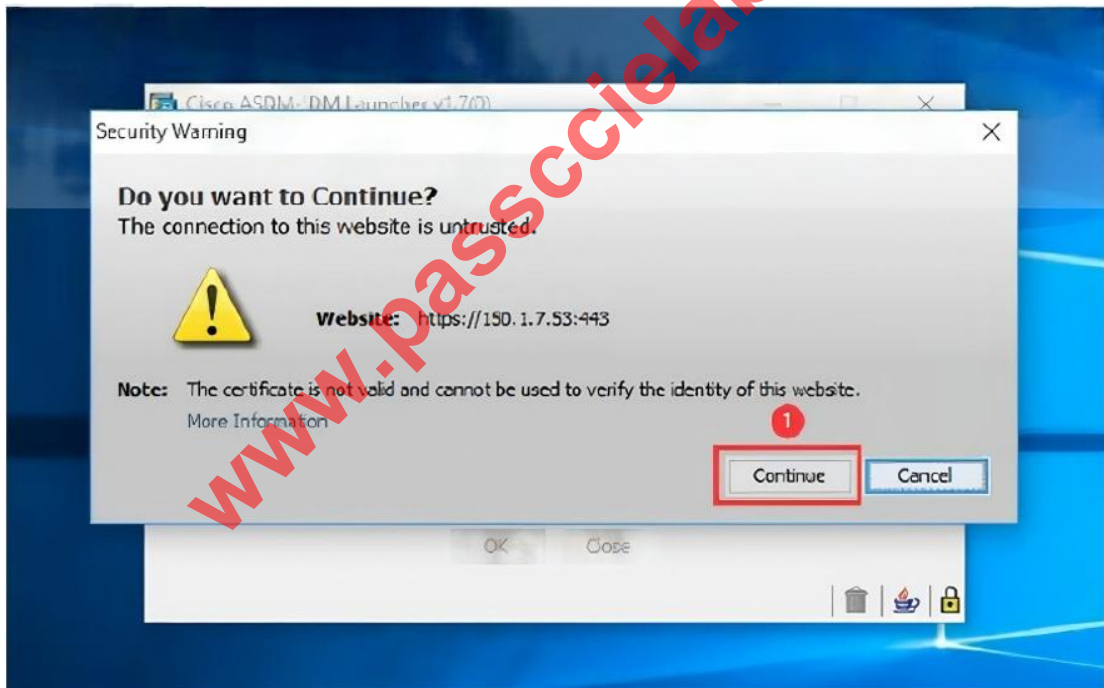
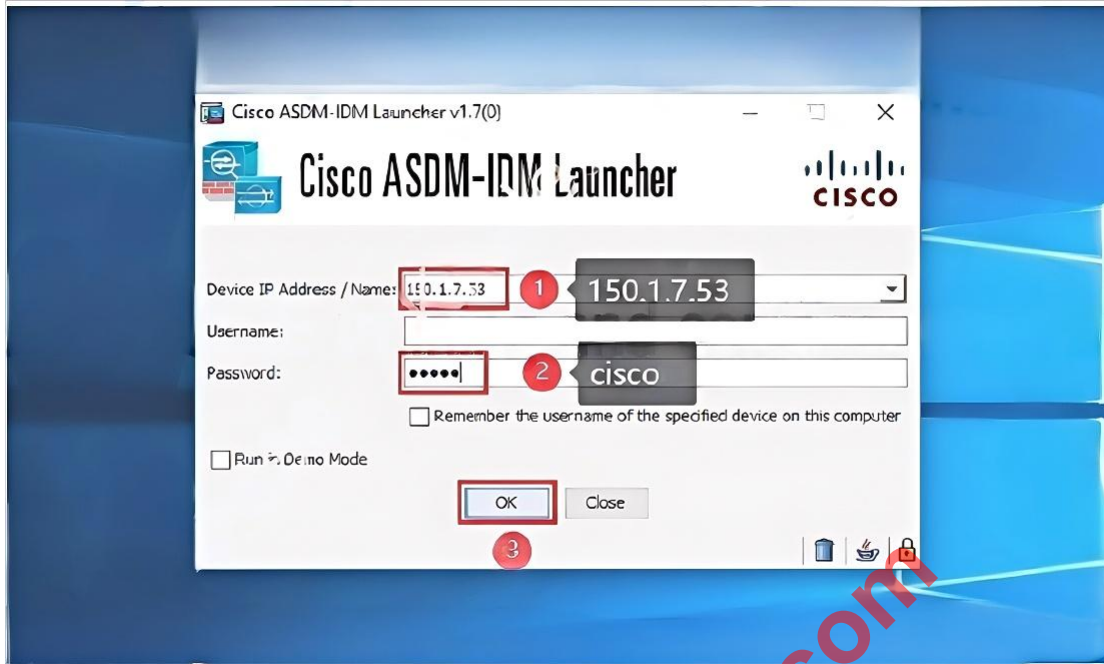


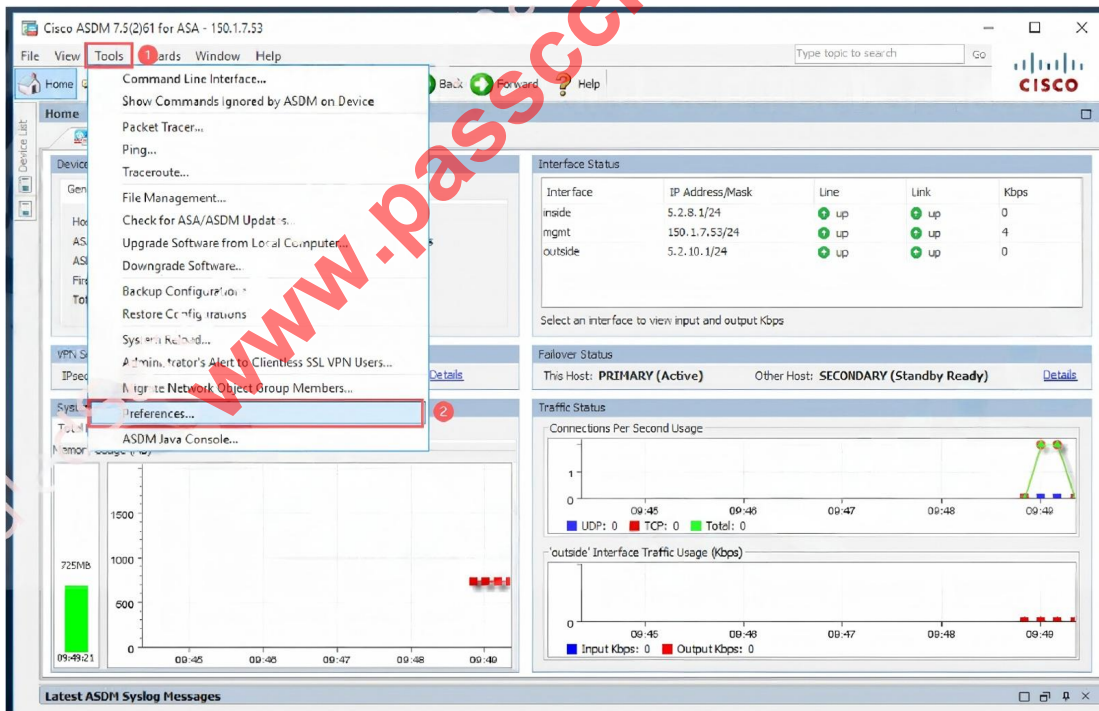
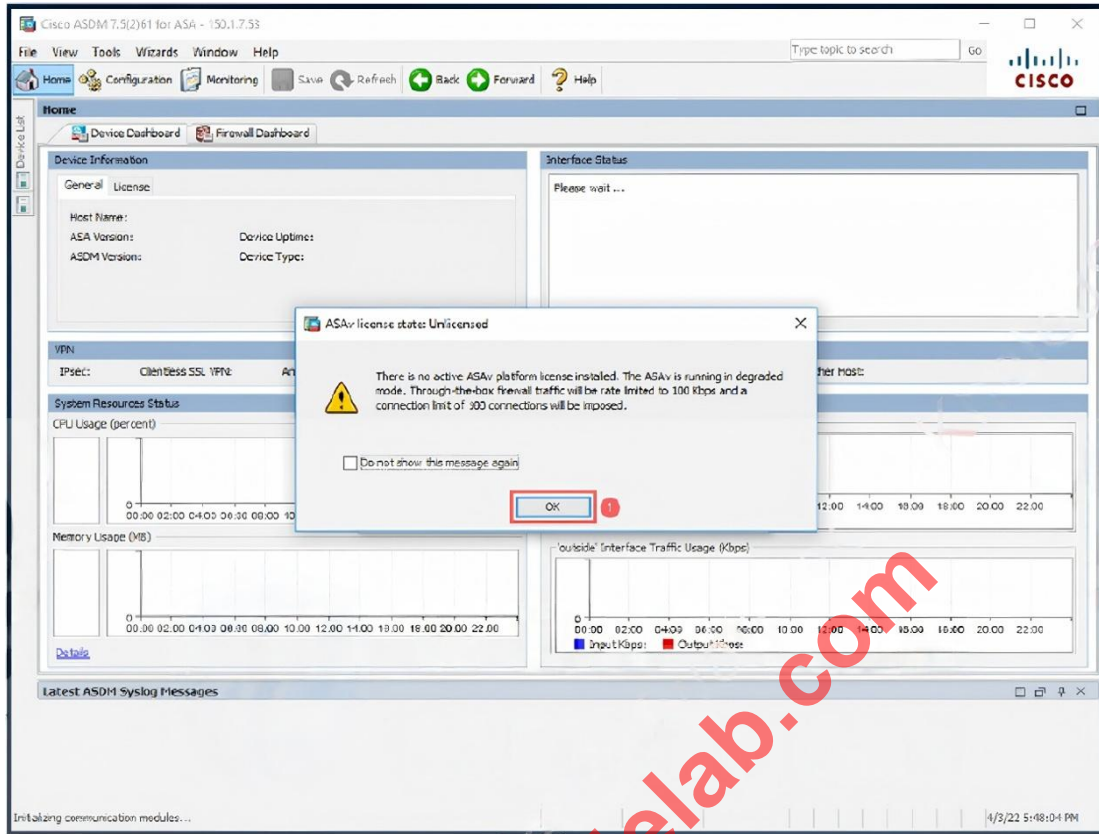


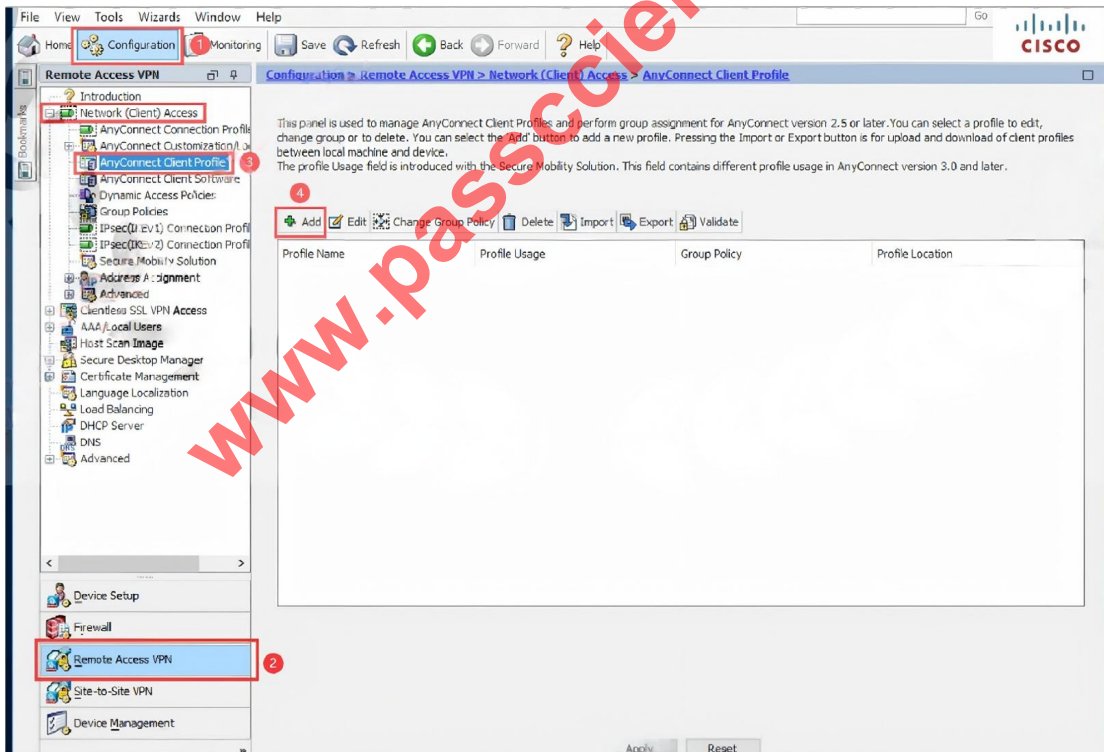
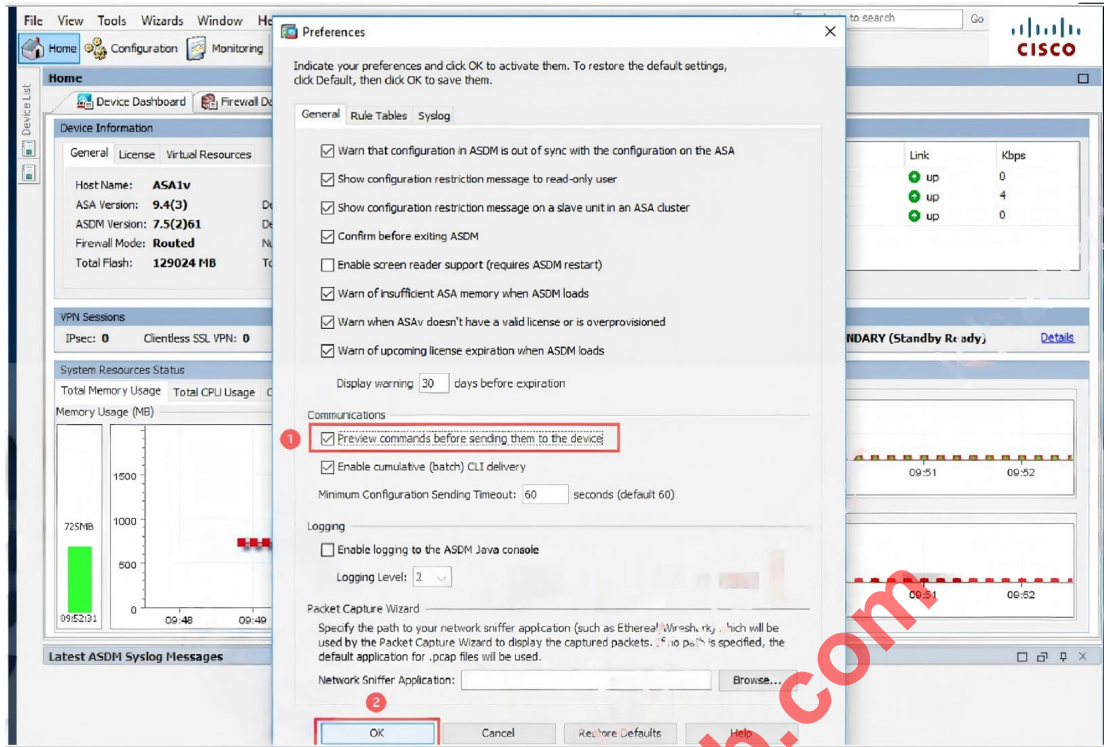


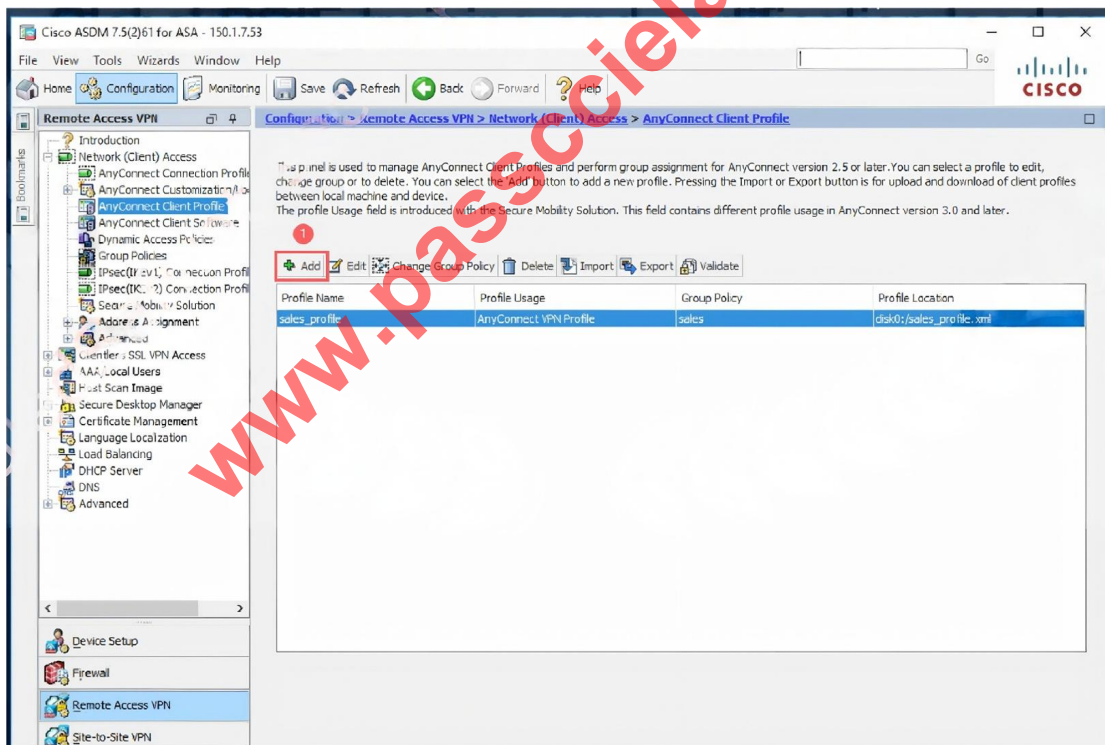
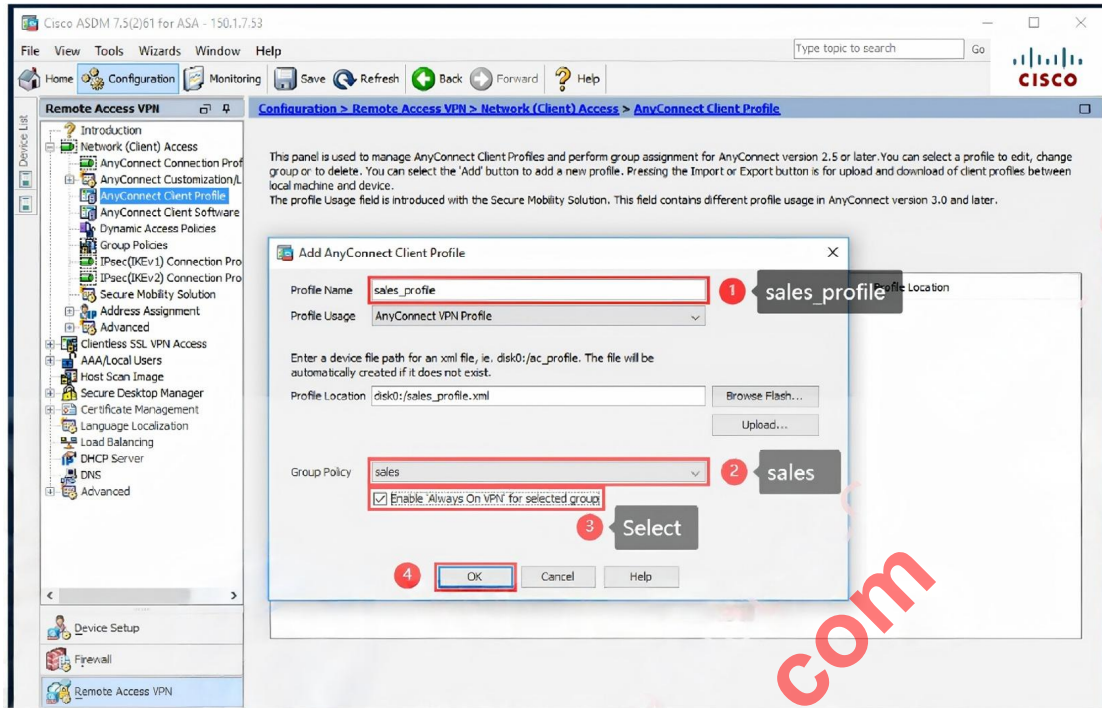


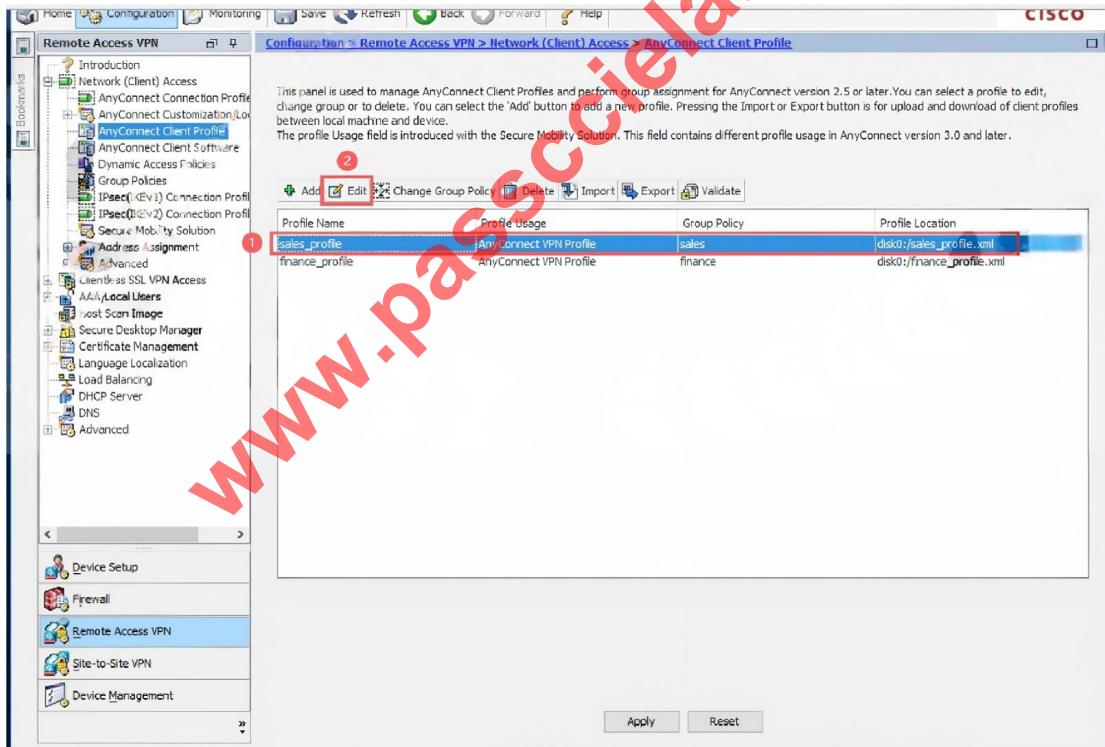
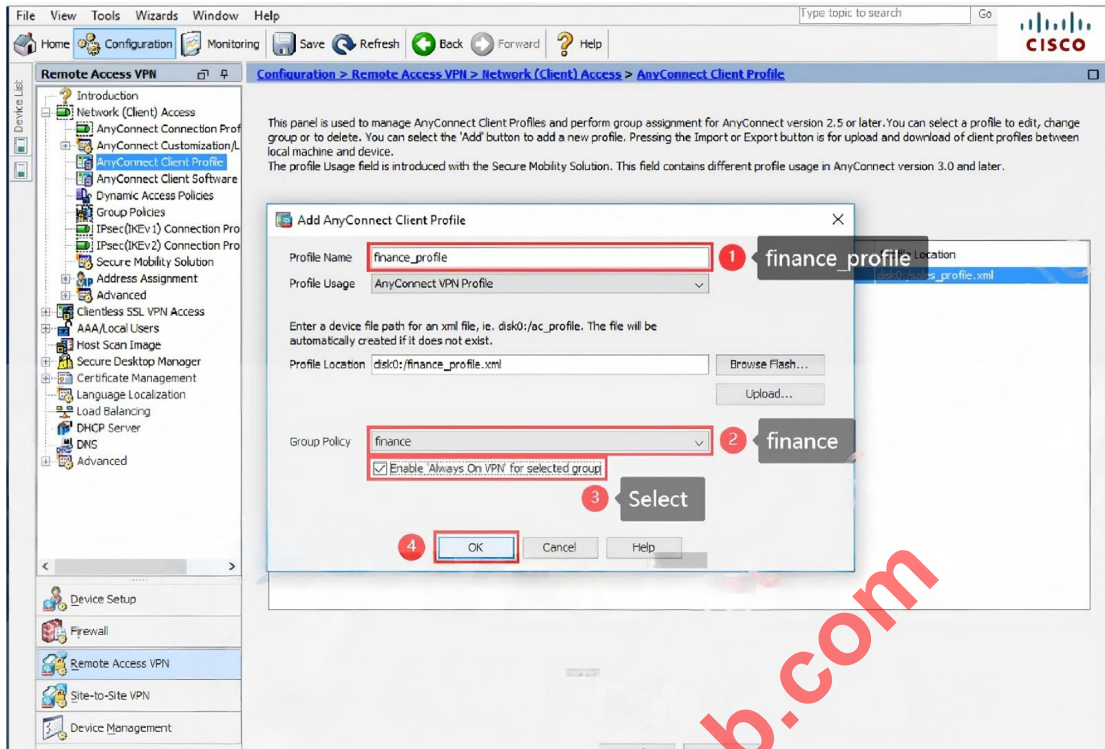


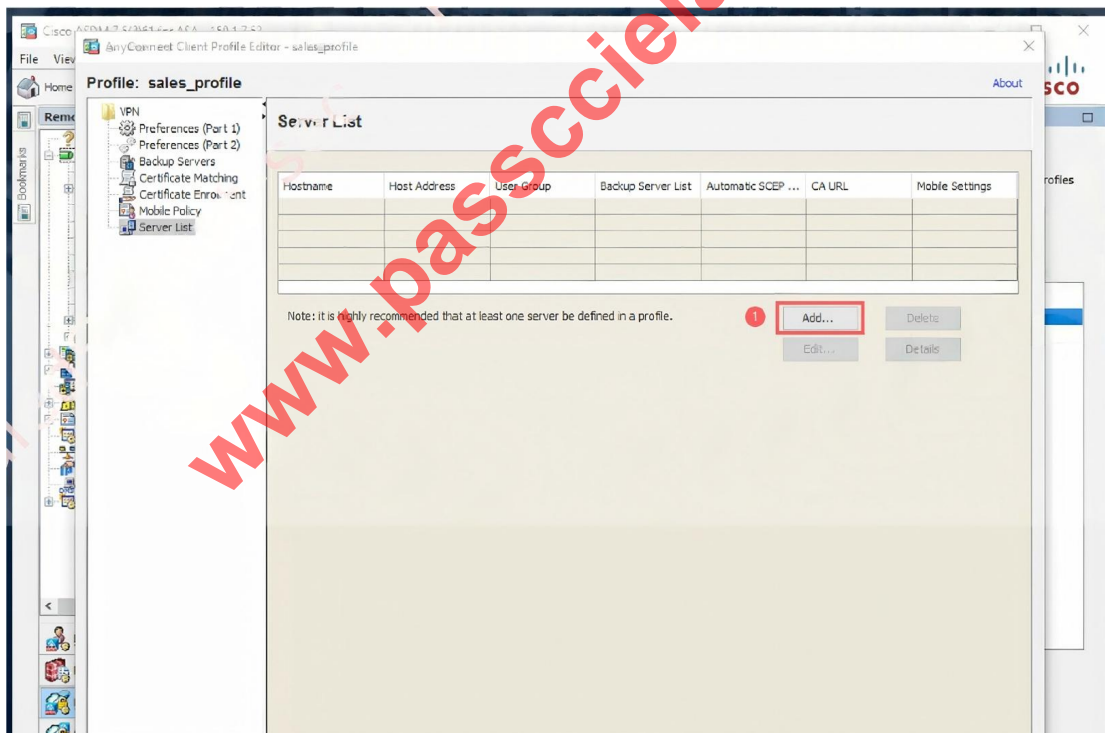
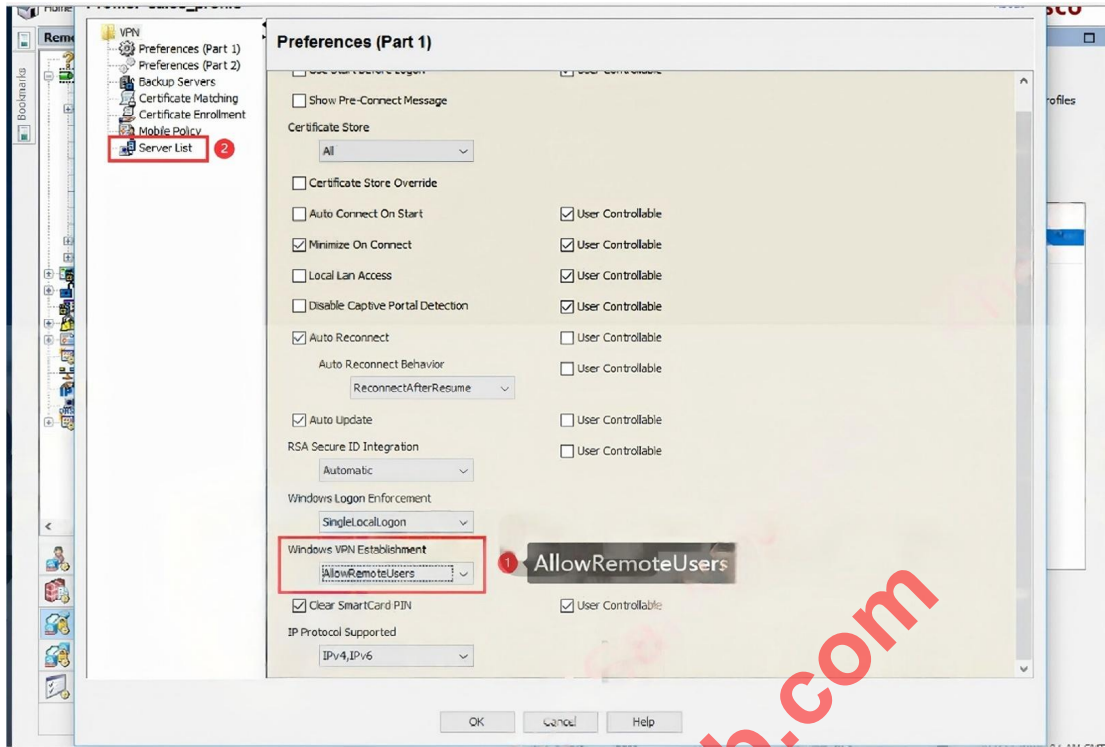


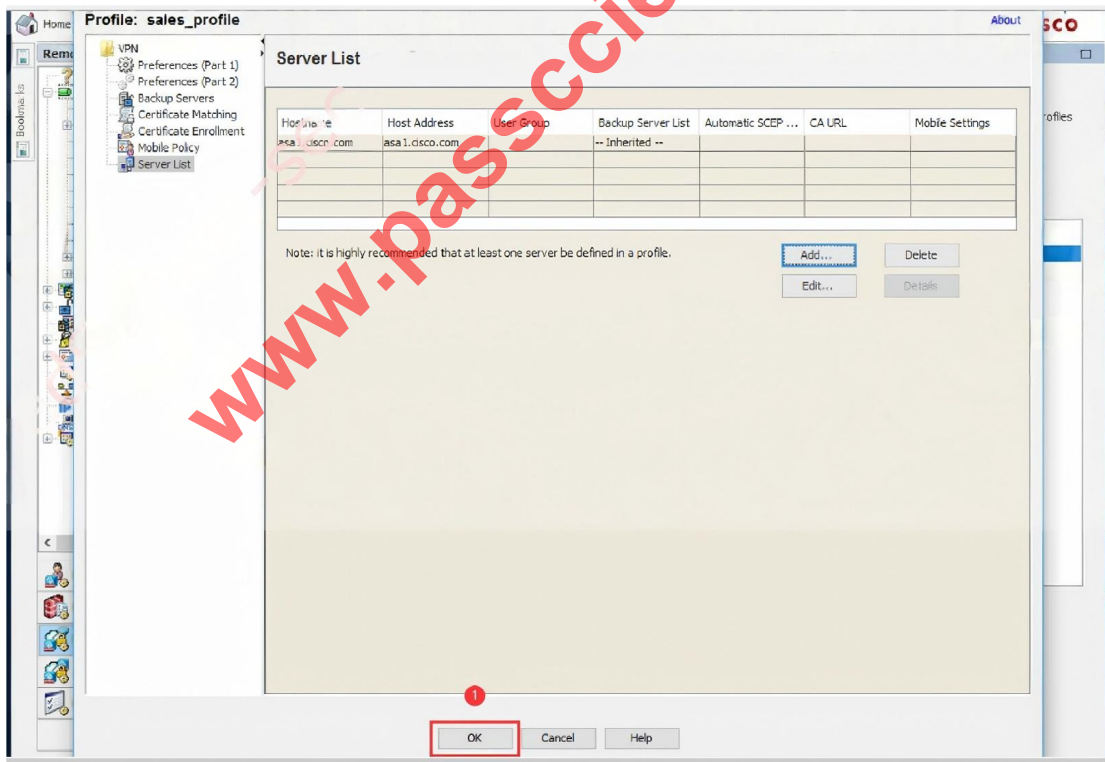
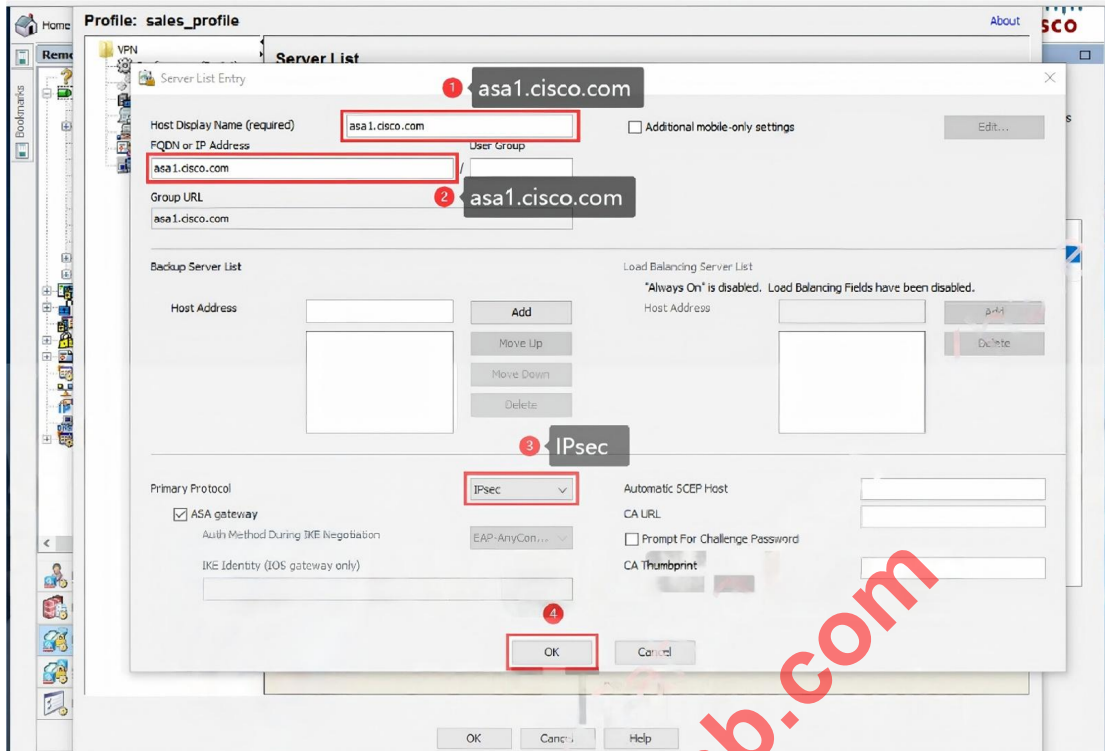


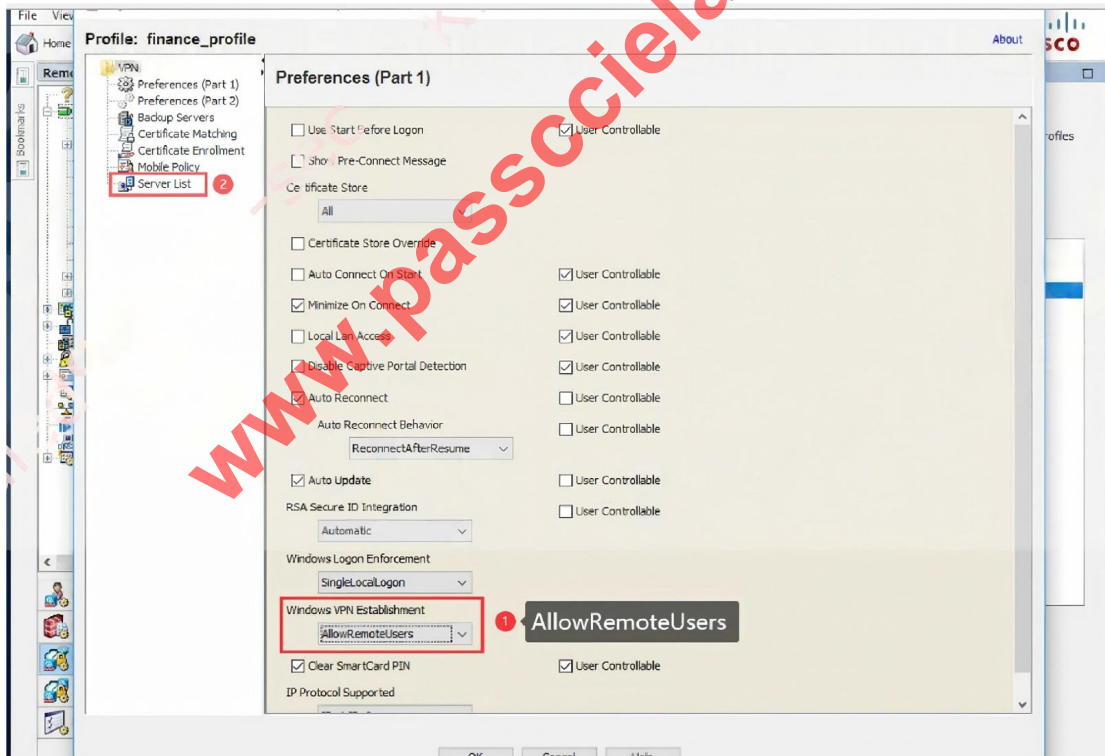
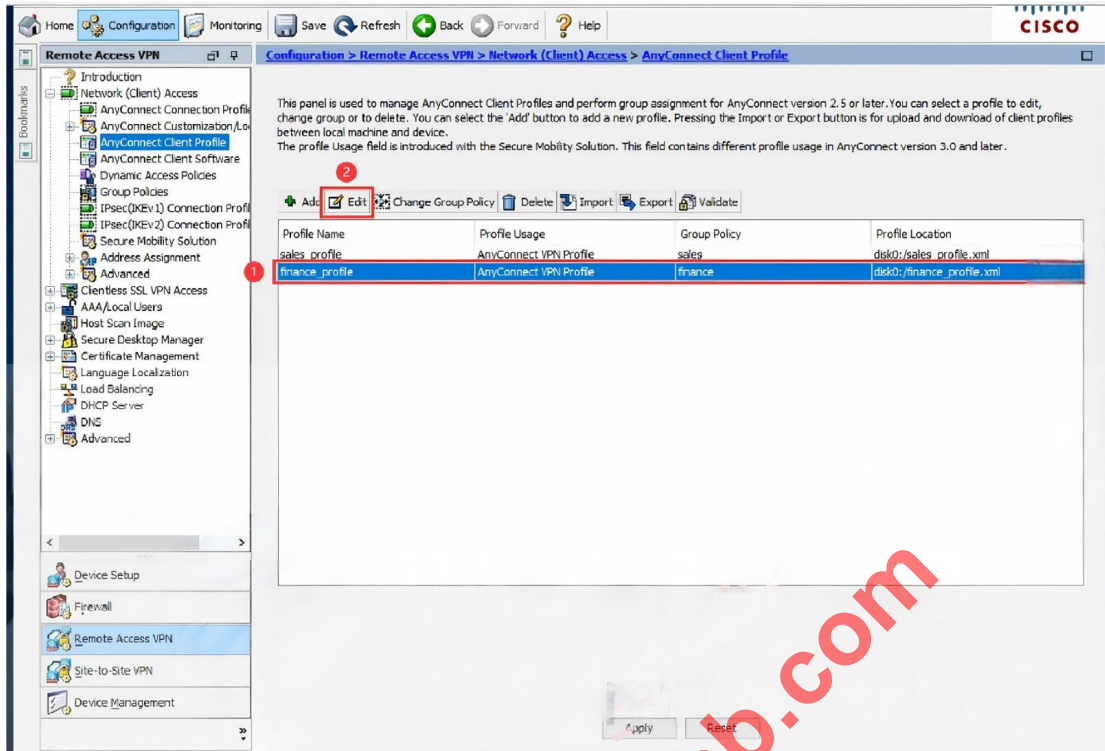


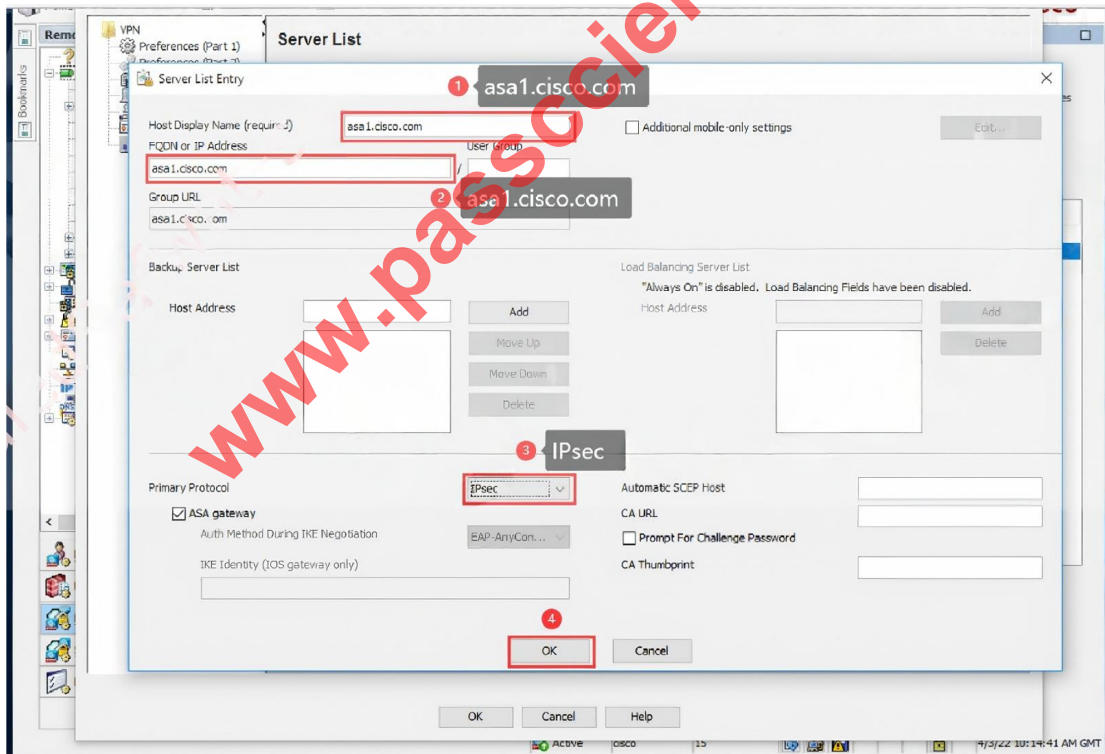
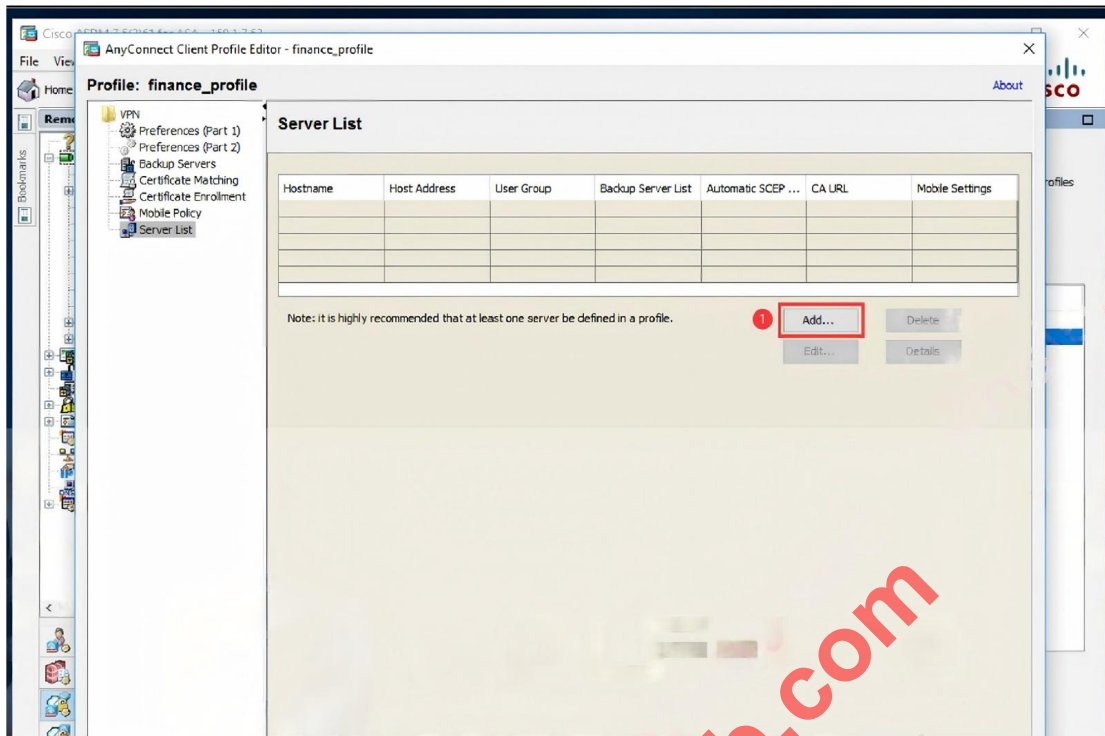


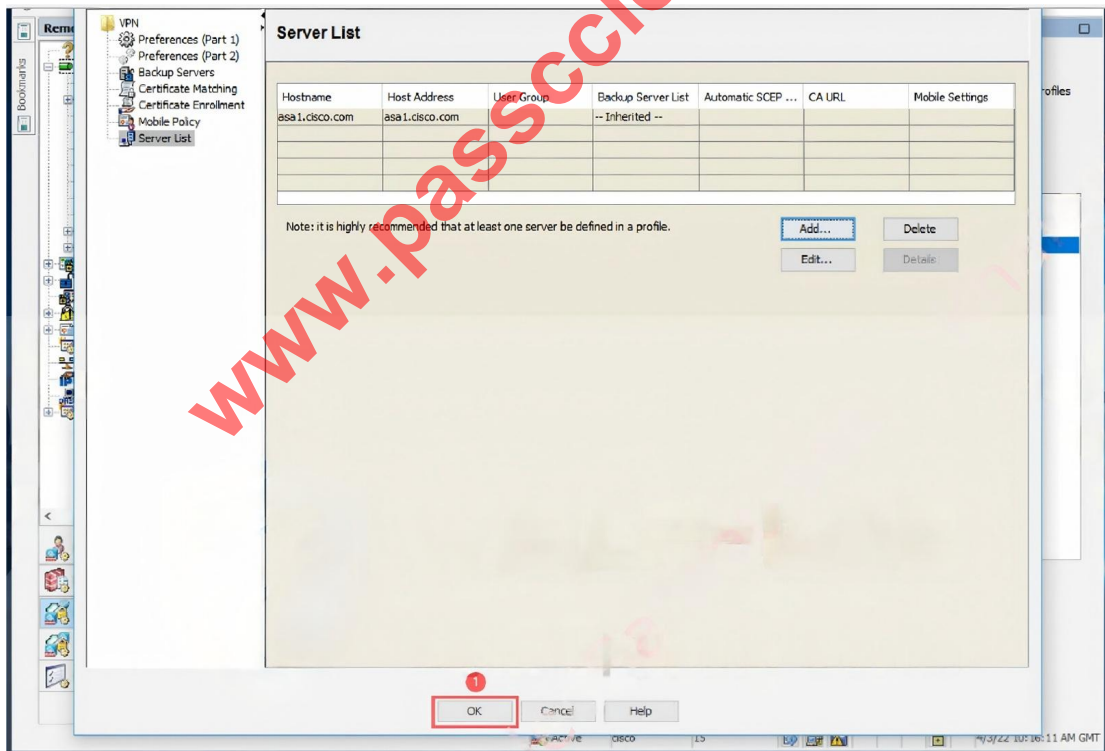
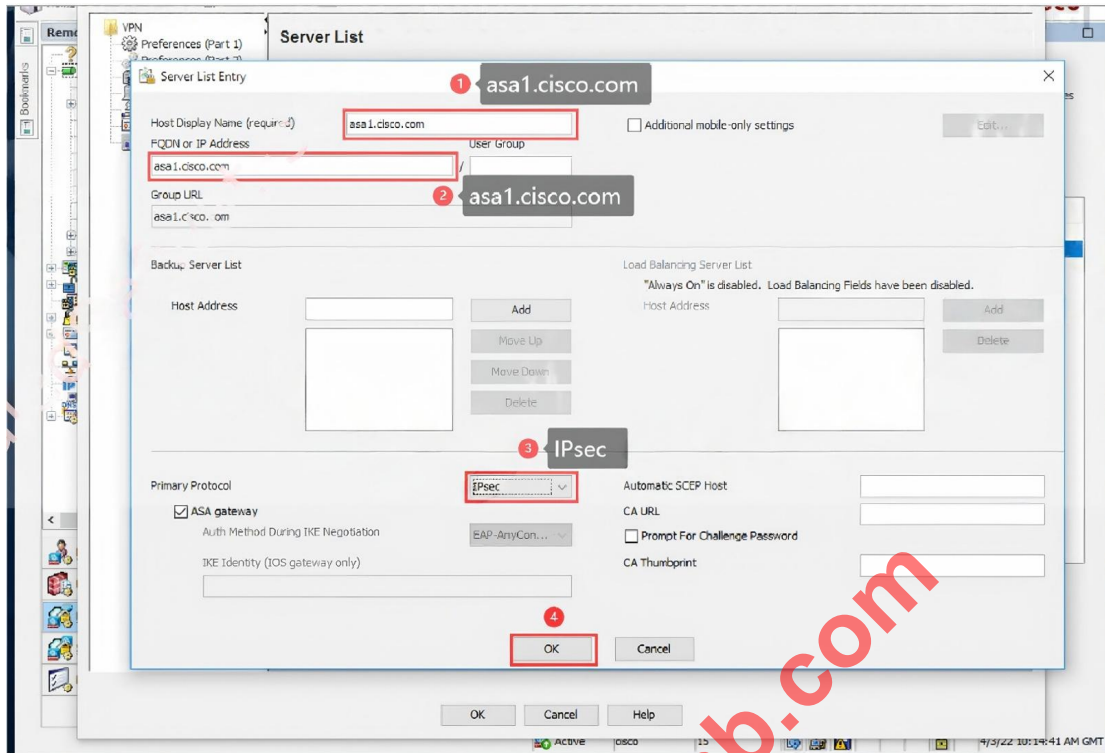


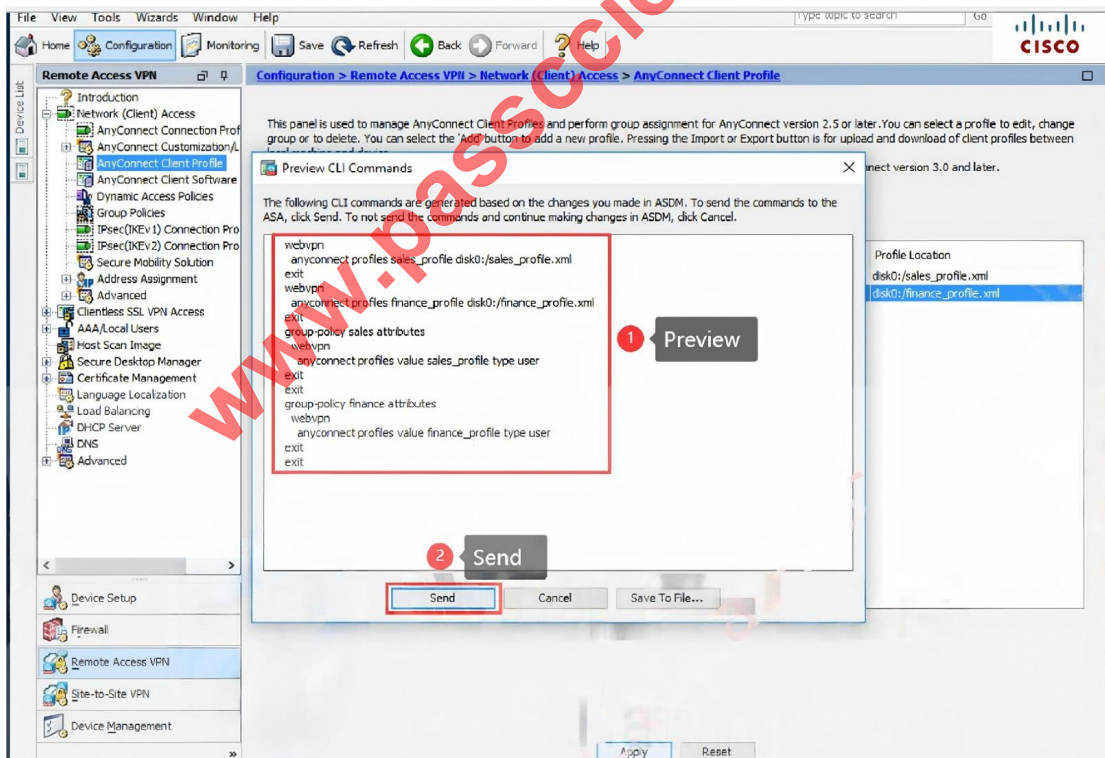
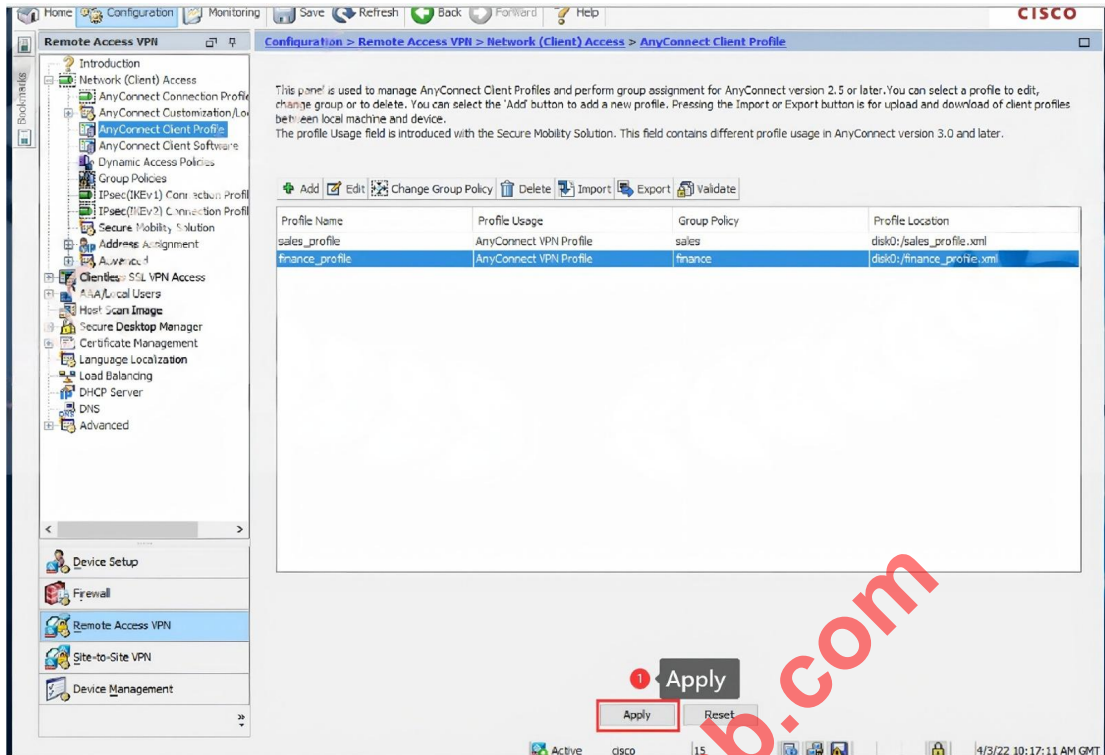


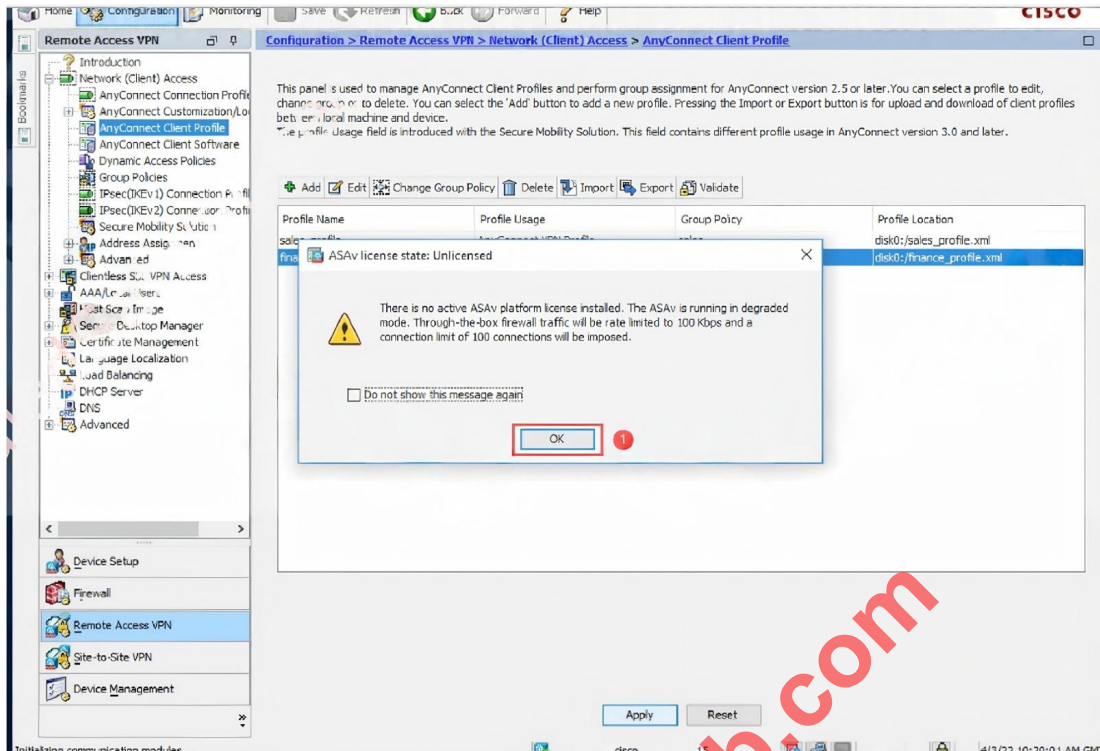












Verify on ASA11v:

ASA1v/pri/act# dir

Directory of disk0:/

(--Omitted here--)

```

62  -rwx  19473166   06:24:06 Apr 08 2022  anyconnect-win-4.2.04018-k9.pkg
70  -rwx   2552      07:32:57 Apr 08 2022  sales_profile.xml
71  -rwx   2552      07:32:58 Apr 08 2022  finance_profile.xml
    
```

8571076608 bytes total (8540147712 bytes free)

ASA1v/pri/act#

ASA1v/pri/act# show running-config webvpn

```

webvpn
  enable outside
  anyconnect image disk0:/anyconnect-win-4.2.04018-k9.pkg 1
  anyconnect profiles finance_profile disk0:/finance_profile.xml
  anyconnect profiles sales_profile disk0:/sales_profile.xml
  anyconnect enable
  tunnel-group-list enable
  cache
  disable
  error-recovery disable
    
```

ASA1v/pri/act# show running-config group-policy

```

group-policy sales internal
group-policy sales attributes
  dns-server value 150.1.7.200
vpn-idle-timeout 1440
    
```

```

vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
group-lock value finance
split-tunnel-policy tunnelspecified
split-tunnel-network-list value finance
default-domain value cisco.com
split-dns value cisco.com
address-pools value financepool
webvpn
  anyconnect keep-installer installed
  anyconnect profiles value finance_profile type user
  always-on-vpn profile-setting
ASA1v/pri/act#
ASA1v/pri/act# write
Building configuration...
Cryptochecksum: 25a919ad 94931e63 2804d1c9 a2ed6f22

```

```

11970 bytes copied in 0.170 secs
[OK]
ASA1v/pri/act#

```

Verify on ASA1v:

By checking, it is found that the XML file and related configuration commands are missing.

```
ASA1v/sec/stby# dir
```

Directory of disk0:/

```
(--Omitted here--, The sales_profile.xml and finance_profile.xml files were not found)
63  -rwx 19473166  06:25:37 Apr 08 2022  anyconnect-win-4.2.04018-k9.pkg
```

8571076608 bytes total (8540151808 bytes free)

```
ASA1v/sec/stby# show running-config webvpn
```

```

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.2.04018-k9.pkg 1
anyconnect enable
tunnel-group-list enable
cache
  disable
error-recovery disable

```

```
ASA1v/sec/stby# show run group-policy
```

```

group-policy sales internal
group-policy sales attributes
  dns-server value 150.1.7.200
  vpn-idle-timeout 1440
  vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
  group-lock value sales
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value sales

```

```

split-dns value cisco.com
address-pools value salespool
webvpn
  anyconnect keep-installer installed
  always-on-vpn profile-setting
group-policy finance internal
group-policy finance attributes
  dns-server value 150.1.7.200
  vpn-idle-timeout 1440
  vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
group-lock value finance
split-tunnel-policy tunnelspecified
    
```

```

split-tunnel-network-list value finance
default-domain value cisco.com
split-dns value cisco.com
address-pools value financepool
webvpn
  anyconnect keep-installer installed
  always-on-vpn profile-setting
ASA1v/sec/stby#
    
```

ASA11v:

Download two XML files from ASA11v: [sales_profile.xml](#) & [finance_profile.xml](#)

ASA1v/pri/act# copy disk0:sales_profile.xml tftp:

Source filename [sales_profile.xml]? <Press "Enter">

Address or name of remote host []? 150.1.7.201

Destination filename [sales_profile.xml]? <Press "Enter">

!

2552 bytes copied in 0.40 secs

ASA1v/pri/act#

ASA1v/pri/act# copy disk0:finance_profile.xml tftp:

Source filename [finance_profile.xml]? <Press "Enter">

Address or name of remote host []? 150.1.7.201

Destination filename [finance_profile.xml]? <Press "Enter">

!

```

Source filename [sales_profile.xml]? <Press "Enter">

Address or name of remote host []? 150.1.7.201

Destination filename [sales_profile.xml]? <Press "Enter">
!
2552 bytes copied in 0.40 secs
ASA1v/pri/act#
ASA1v/pri/act# copy disk0:finance_profile.xml tftp:

Source filename [finance_profile.xml]? <Press "Enter">

Address or name of remote host []? 150.1.7.201

Destination filename [finance_profile.xml]? <Press "Enter">
!
2552 bytes copied in 0.40 secs
ASA1v/pri/act#
    
```

ASA1v:
Use TFTP to upload two XML files: sales_profile.xml & finance_profile.xml

```

ASA1v/sec/stby# copy tftp:sales_profile.xml disk0:

Address or name of remote host [150.1.7.201]? <Press "Enter">

Source filename [sales_profile.xml]? <Press "Enter">

Destination filename [sales_profile.xml]? <Press "Enter">
    
```

```

Accessing tftp://150.1.7.201/sales_profile.xml...!
Writing file disk0:/sales_profile.xml...
!
2552 bytes copied in 0.90 secs
ASA1v/sec/stby# copy tftp:finance_profile.xml disk0:

Address or name of remote host [150.1.7.201]? <Press "Enter">

Source filename [finance_profile.xml]? <Press "Enter">

Destination filename [finance_profile.xml]? <Press "Enter">

Accessing tftp://150.1.7.201/finance_profile.xml...!
Writing file disk0:/finance_profile.xml...
!
2552 bytes copied in 0.70 secs
ASA1v/sec/stby# dir
    
```

```

Directory of disk0:/

(--Omitted here--)
63  -rwx 19473166   06:25:37 Apr 08 2022  anyconnect-win-4.2.04018-k9.pkg
65  -rwx  2552      07:51:13 Apr 08 2022  sales_profile.xml
66  -rwx  2552      07:51:24 Apr 08 2022  finance_profile.xml
    
```

```

8571076608 bytes total (8540143616 bytes free)

ASA1v/sec/stby#

ASA11v:  

Synchronize the configuration to ASA1v and save
    
```

```

ASA11v:
Synchronize the configuration to ASA1v and save

ASA1v/pri/act# write standby
Building configuration...
[OK]
ASA1v/pri/act# Beginning configuration replication: Sending to mate.
End Configuration Replication to mate

ASA1v/pri/act# write
Building configuration...
Cryptochecksum: 69276496 1603fca2 87f99336 6ffc0de0

11970 bytes copied in 0.180 secs
[OK]
    
```

ASA1v/pri/act#

ASA1v:
View the XML file and the configuration synchronized from the ASA11v

```

ASA1v/sec/stby# show run webvpn
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.2.04018-k9.pkg 1
anyconnect profiles finance_profile disk0:/finance_profile.xml
anyconnect profiles sales_profile disk0:/sales_profile.xml
anyconnect enable
tunnel-group-list enable
cache
  disable
error-recovery disable
ASA1v/sec/stby# show run group-policy
group-policy sales internal
group-policy sales attributes
  dns-server value 150.1.7.200
  vpn-idle-timeout 1440
  vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
  group-lock value sales
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value sales
  default-domain value cisco.com
  split-dns value cisco.com
  address-pools value salespool
webvpn
  anyconnect keep-installer installed
    
```

```

anyconnect profiles value sales_profile type user
always-on-vpn profile-setting
group-policy finance internal
group-policy finance attributes
  dns-server value 150.1.7.200
  vpn-idle-timeout 1440
  vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
  group-lock value finance
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value finance
  default-domain value cisco.com
  split-dns value cisco.com
  address-pools value financepool
webvpn
    
```

anyconnect keep-installer installed
anyconnect profiles value finance_profile type user
always-on-vpn profile-setting
ASA1v/sec/stby#

Management PC:
Open <https://ise310.cisco.com> (ISE) web page

