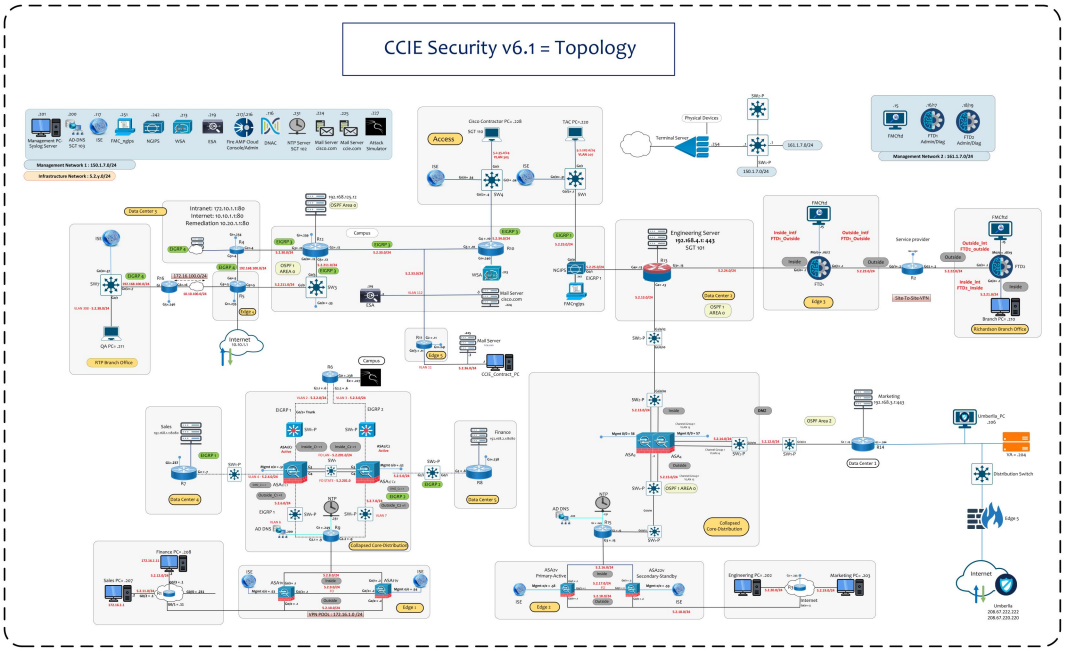
CCIE SECURITY v6.1 Real Labs--- DOO Module

Module2-DOO

Ver：1


CCIE Security v6.1 = Topology

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 days.**
- **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 172.16.1.11-172.16.20/24**
- **DACLmust permit trafiic destined to Sales server,Finance server,NTP server and DNS server.**
- **DACL must per.nit ICMP traffic between Sales PC and Finance PC.**

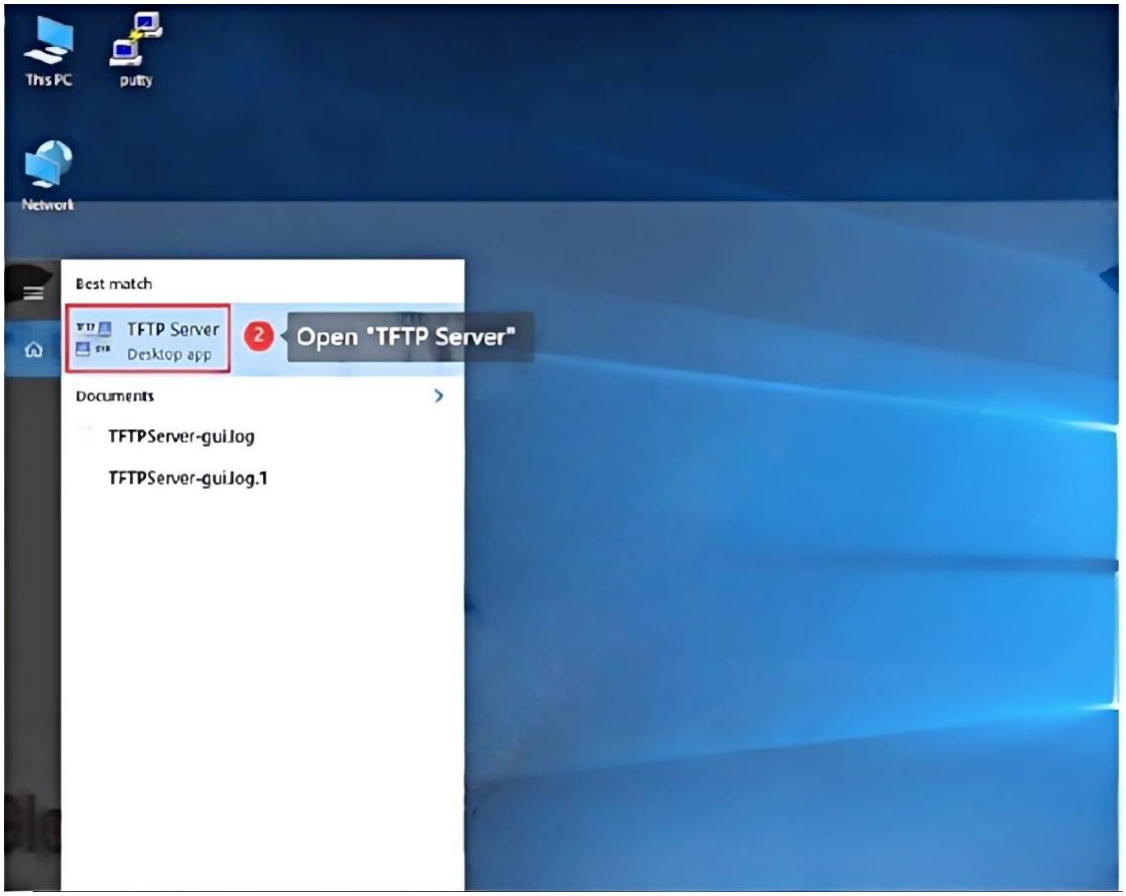
Notes:

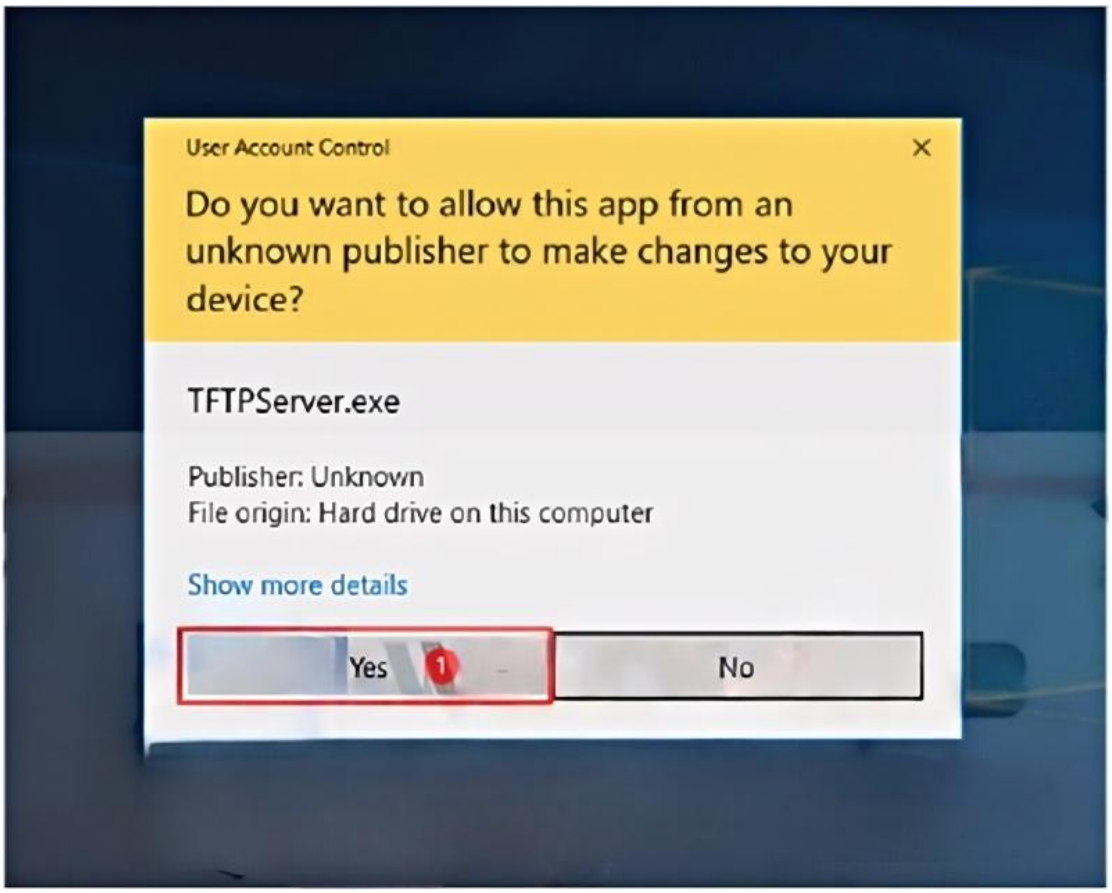
● For the deployment you must use the addresses provided under the "Addressing Tables"tab for Task 1.2

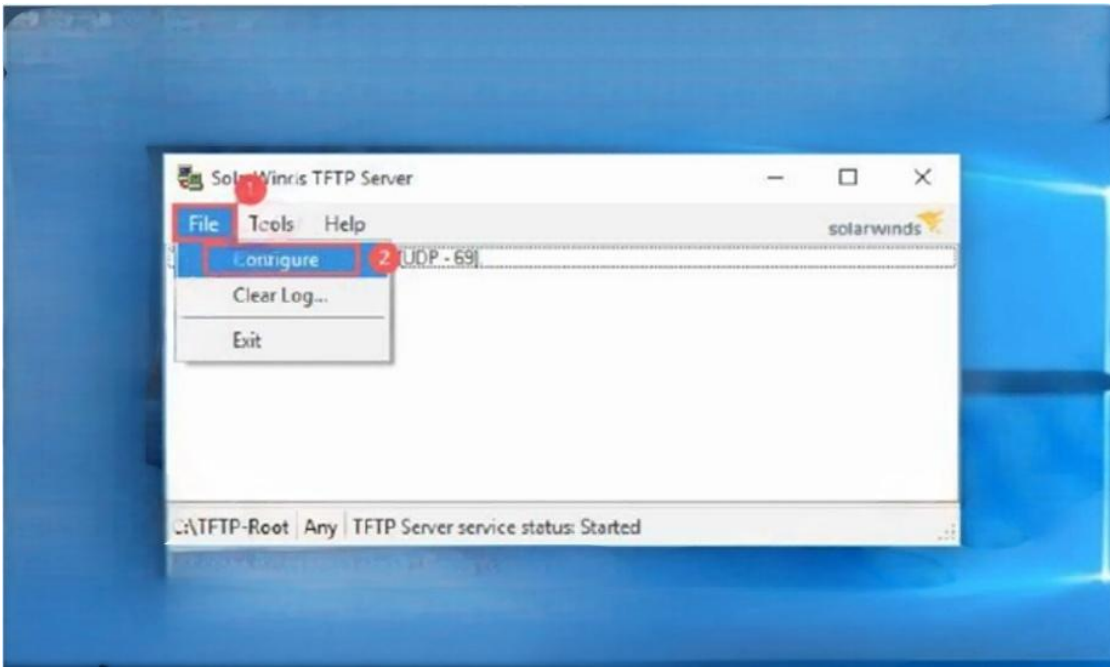
Solution：

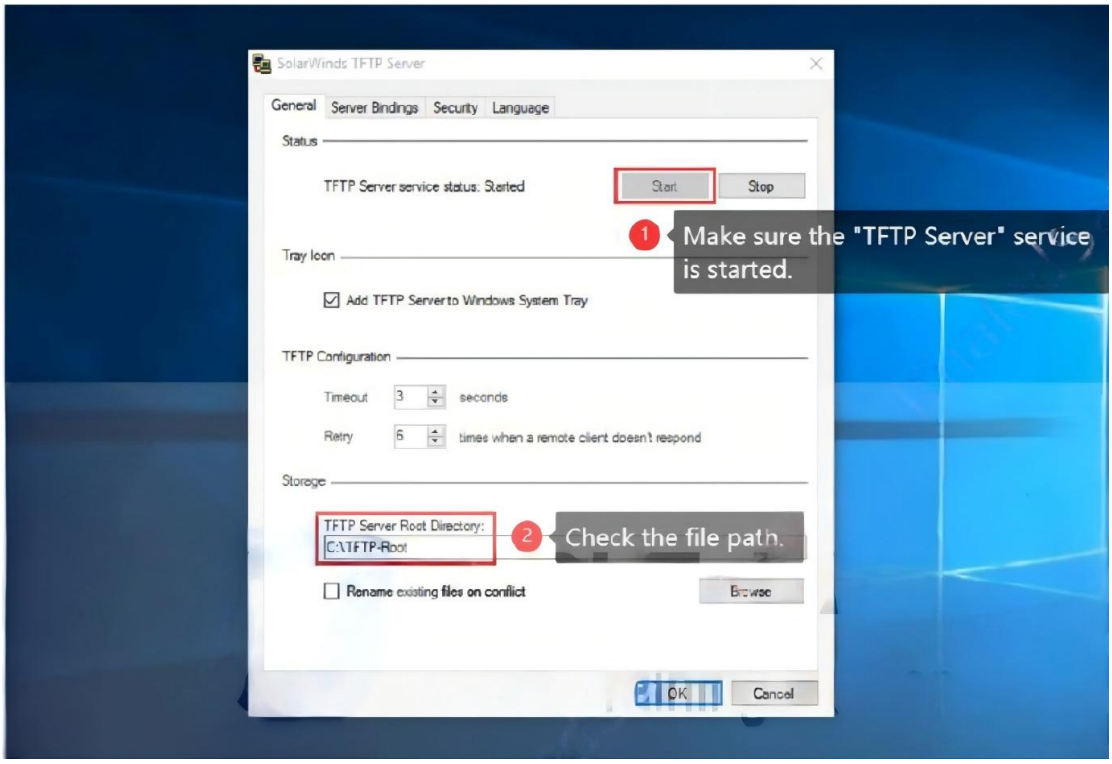
Management PC

Open TFTP server Application


This PC
putty
Network
Best match
TFTP Server
Desktop app
2
Open "TFTP Server"
Documents
TFTPServer-gui.log
TFTPServer-gui.log.1


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your device?
TFTPServer.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show more details
Yes
1
No





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..

!!!

(--Omitted here--)

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!19473166 bytes copied in 56.460 secs (347735 bytes/sec)ASA1v/pri/act#

R9:

R9(config)#ip route 172.16.1.0255.255.255.05.2.3.1

R9(config)#router eigrp 1

R9(config-router)#redistribute static

R9(config-router)#exit

R9(config)#router eigrp 2

R9(config-router)#redistribute static

R9(config-router)#exit

R9(config)#

ASA1-c1:

ASA1/c1/sec/acti(config)#route dmz 19.16.2.1 255.255.255.2555.2.5.8

ASA1/c1/sec/act(config)#router eigrp 2

ASA1/c1/sec/act(config-router)#redistribute static

ASA1/c1/sec/act(config-router)#exit

ASA1/c1/sec/act(config)#

Verify on ASA1-c1:

ASA1/c1/sec/act#show route

Routing Table:c1

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

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

o-ODR,P-periodic downloaded static route,+-replicated route

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 5.2.7.9.00:0137,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 19.16.11255.255.255.2555.2.4.7

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 Tabie: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

Ia -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 5.2.2.0255.255.255.0 is directly connected,inside

L 5.2.2.1255.255.255.255 is directly connected,inside

C 5.2.4.0255.255.255.0 is directly connected,dmz

L 5.2.4.1255.255.255.255 is directly connected,dmz

C 5.2.6.0255.255.255.0 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 161.1.7.0255.255.255.0 [170/3072]via 5.2.6.9,01:52:00,outside

D EX 172.16.0.0255.255.0.0[170/3072]via 5.2.6.9,01:52:00,outside

D EX 172.16.1.0255.255.255.0[170/3072]via 5.2.6.9,00:11:11,outside

D 192.168.1.0255.255.255.0 [90/130816]via 5.24.7,01:53:40.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 extermal type 1,N2-OSPF NSSA exernal type 2

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

i-IS-IS,su-IS-IS summary,L1-IS-IS level-1,12-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,l-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 certiticate 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

Cerificate 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 authorzed 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 VeriSignl,Inc.-For authonzed 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

Ceruificate 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 32022

end date:08:40:30 GMT Mar 312032

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 Nov82CC6

end date:23:59:59 GMT Jul 162036

Associated Trustpoints:SmartCallHome_ServerCA

ASA1v/sec/stby#

ASA1v/sec/stby#

ASA11v;

ASA1v/pri/act(contig)#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)4 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-tuinnel-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-oolicy)#webvpn

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

ASA1v/pri/act(config-goup-webvpn)#always-on-vpn profile-setting

ASA1v/pri/act(confio-group-webvpn)#exit

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

ASA1v/priect(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-tunel-policy tunnelspecified

ASA1v/pri/act(config-group-policy)#split-tuinnel-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)i 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(ccnfig-group-webvpn)#exit

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

ASA1v/priact(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(ccnfic 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

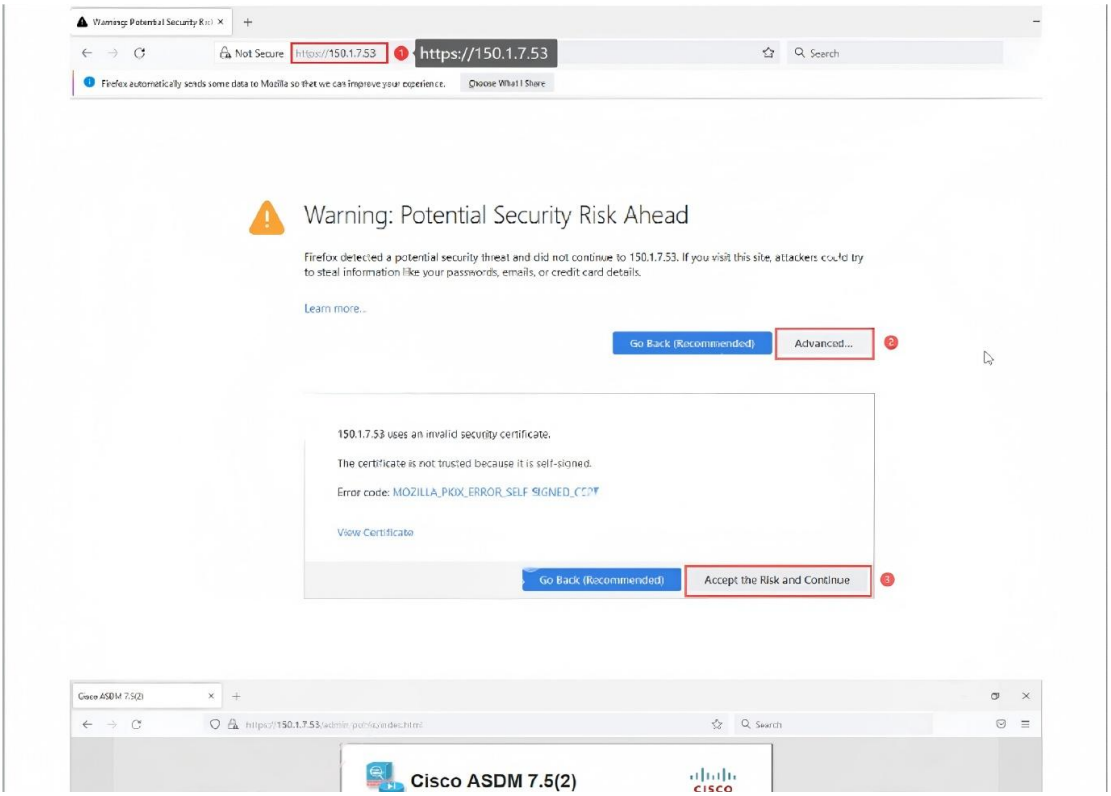
ASA1v/pri/act(config)#crypto ikev2 remote-access trustpoint ccietrust

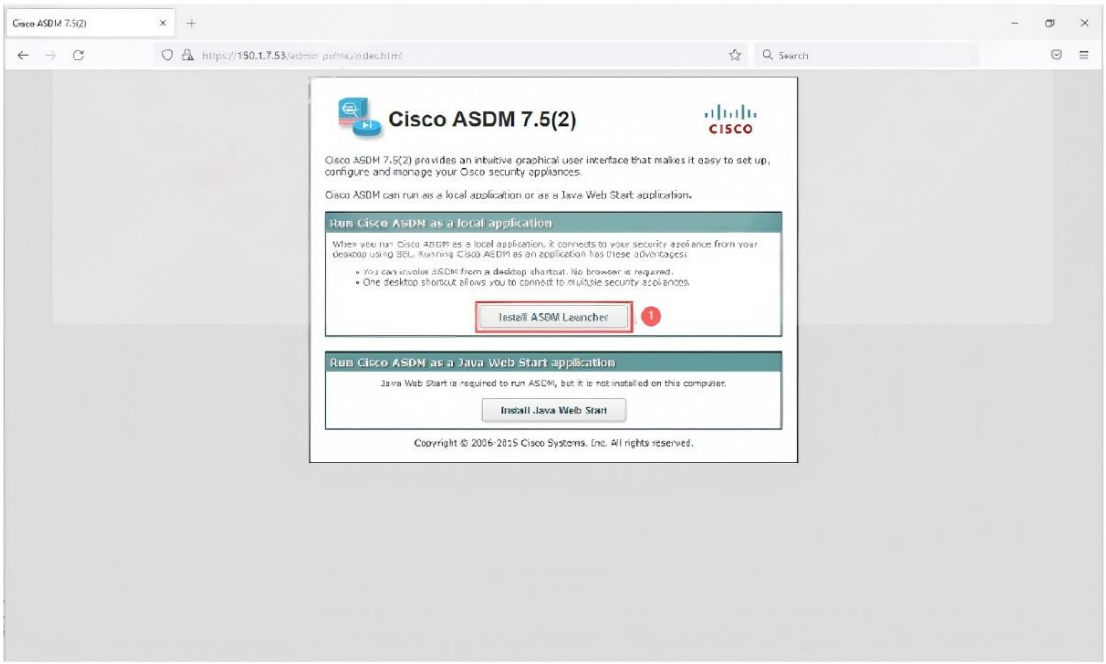
ASA1v/pri/act(config)#ssl trust-point ccietrust outside

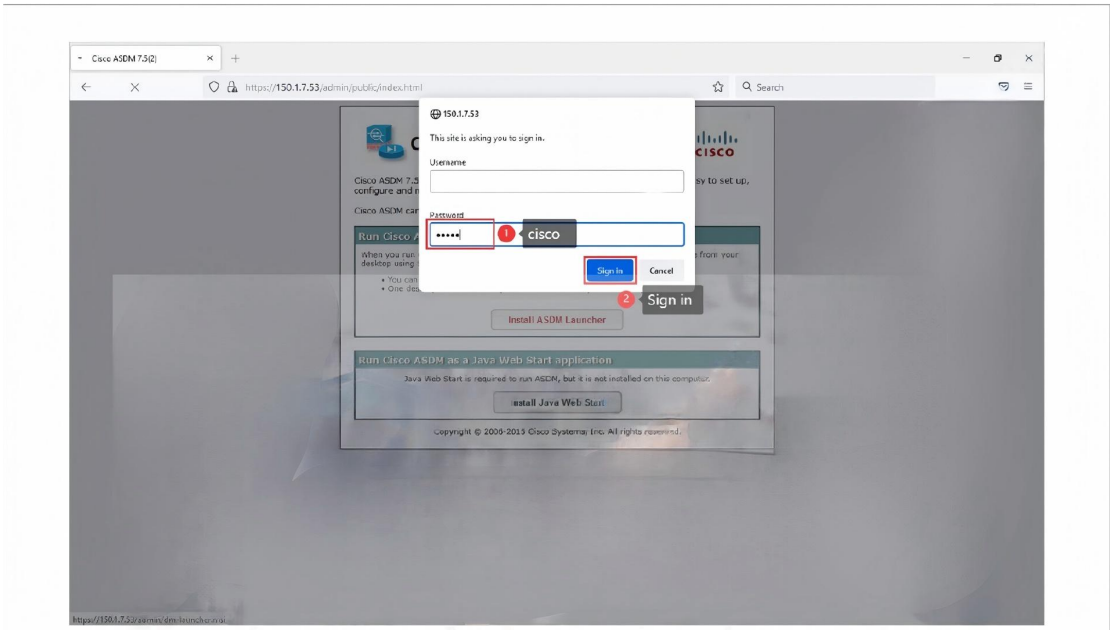
ASA1v/pri/act(config)#

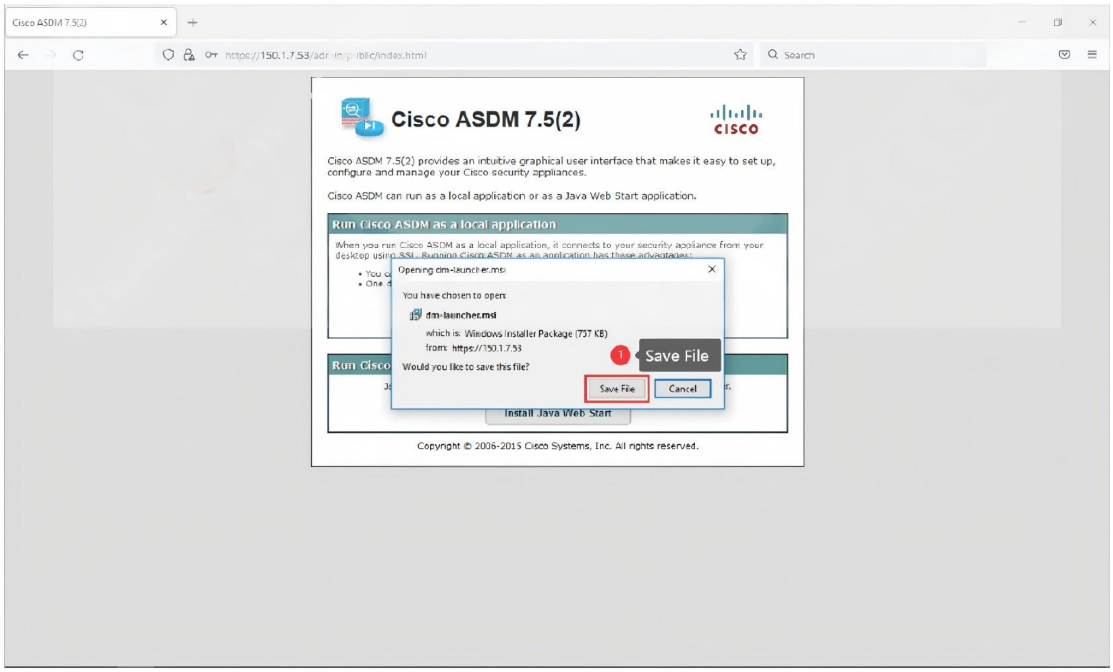
Management PC;

Download and open ASDM

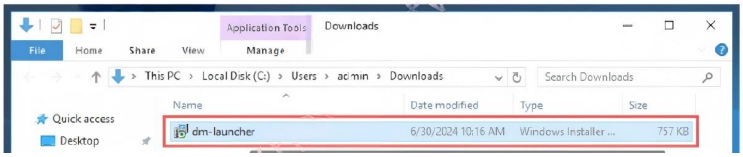


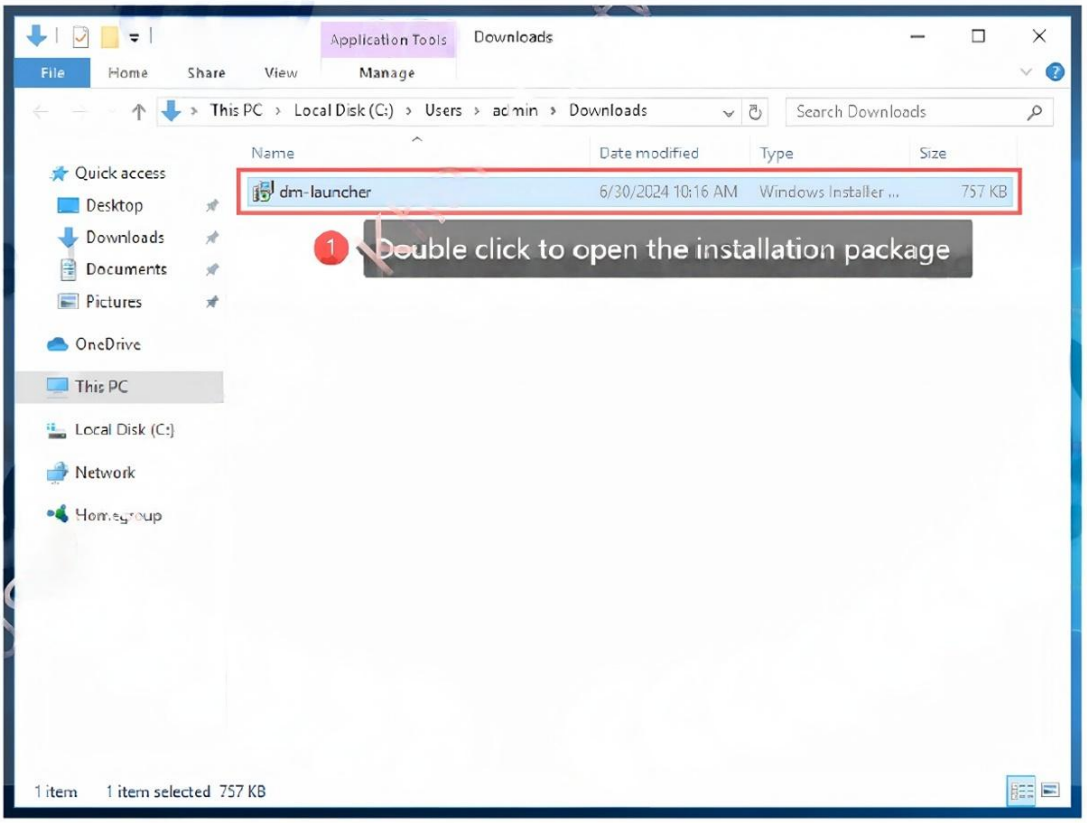


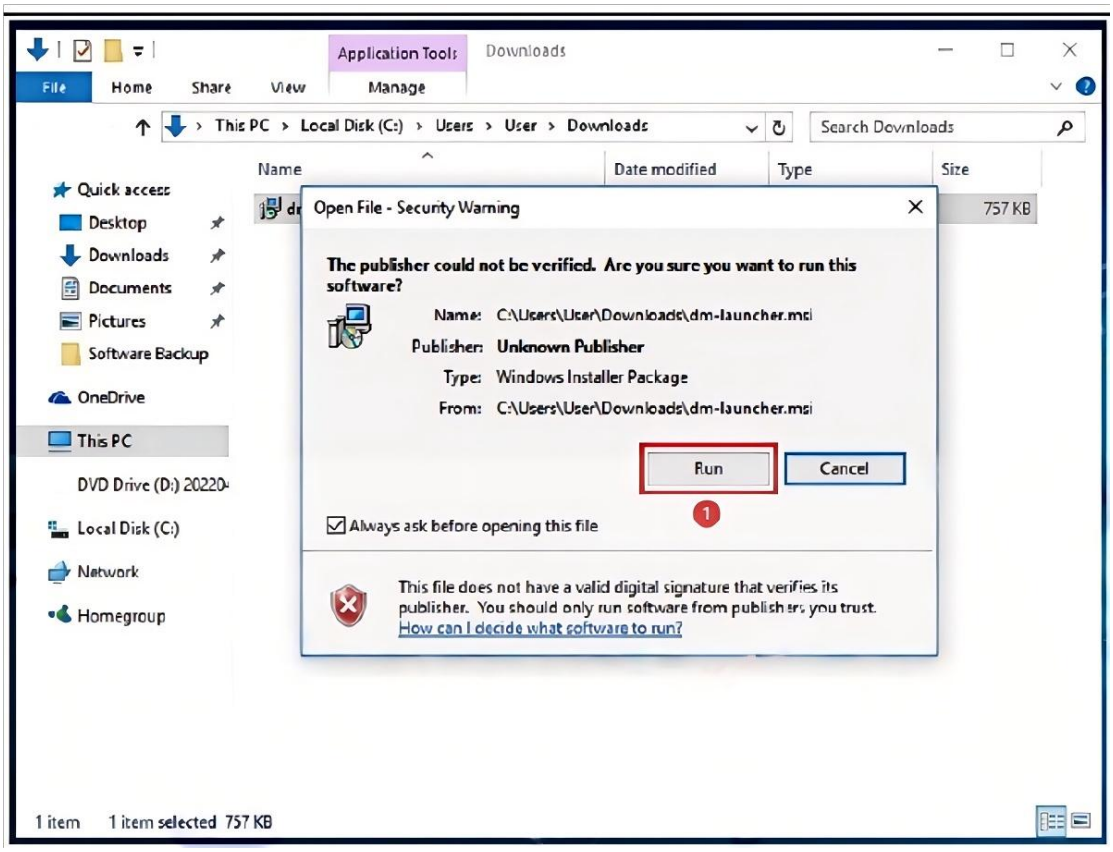

Cisco ASDM 7.5(2)
https://150.1.7.53/admin/public/index.html
150.1.7.53
This site is asking you to sign in.
Username
Password
cisco
Sign in
Cancel
Sign in
Install ASDM Launcher
Run Cisco ASDM as a Java Web Start application
Install Java Web Start

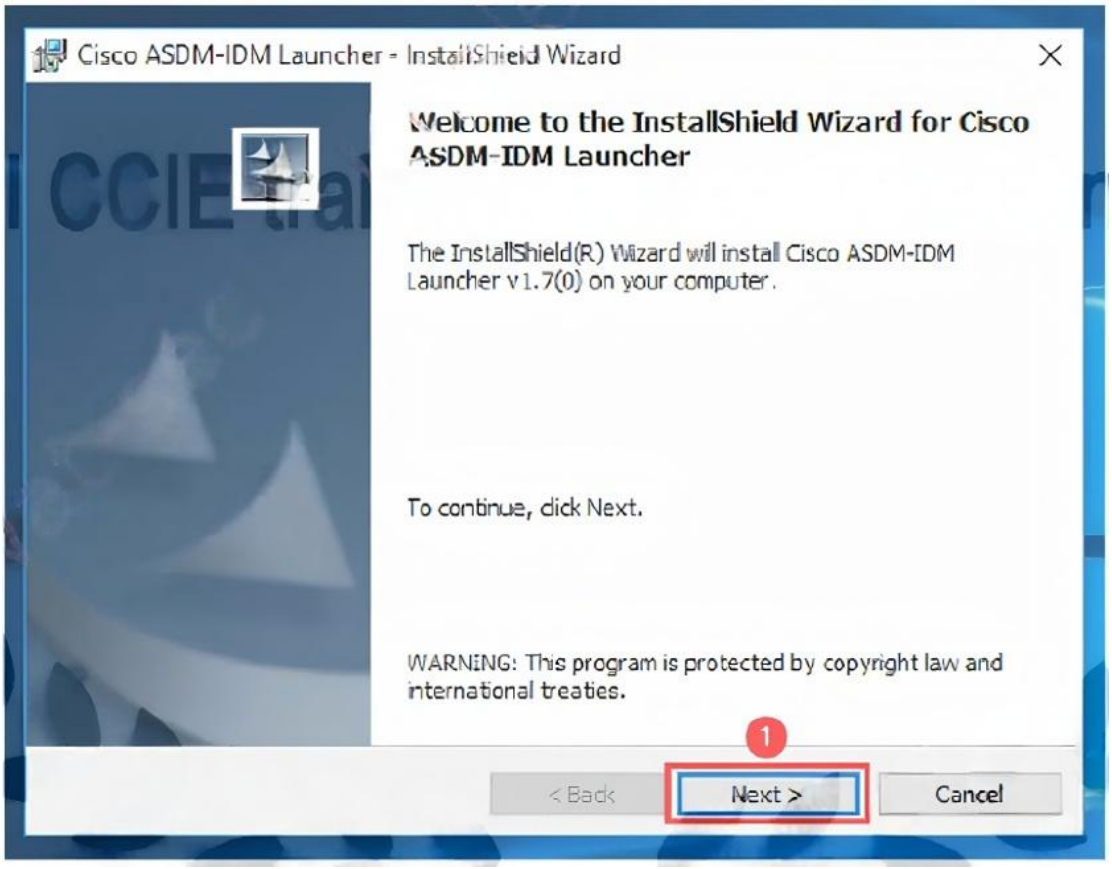

Cisco ASDM 7.5(2)
Cisco ASDM 7.5(2) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.
Cisco ASDM can run as a local application or as a Java Web Start application.
Run Cisco ASDM as a local application
Opening dm-launcher.msi
You have chosen to open
dm-launcher.msi
which is: Windows Installer Package (737 KB)
from: https://150.1.7.53
Would you like to save this file?
Save File
Cancel
Save File
Install Java Web Start
Copyright © 2006-2015 Cisco Systems, Inc. All rights reserved.

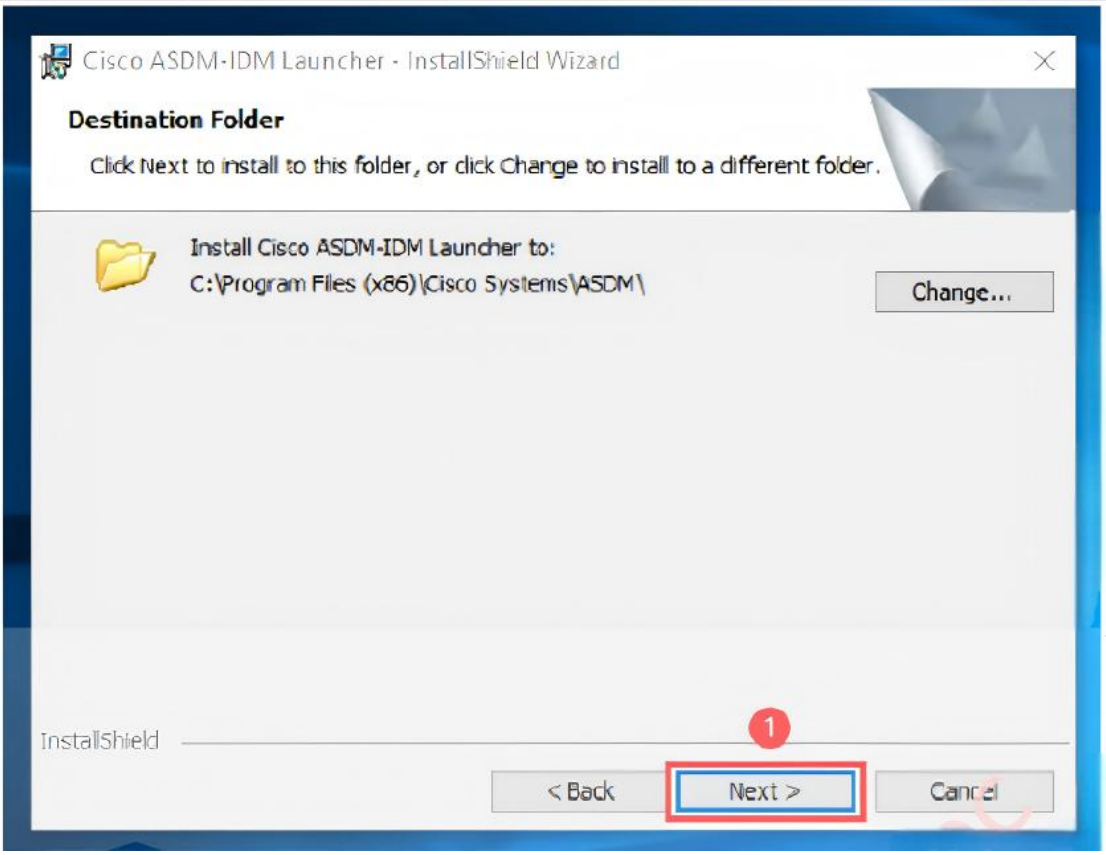

Cisco ASDM 7.5(2)
Click to open the folder
Run Cisco ASDM as a local application
Install ASDM Launcher
Run Cisco ASDM as a Java Web Start application
Install Java Web Start

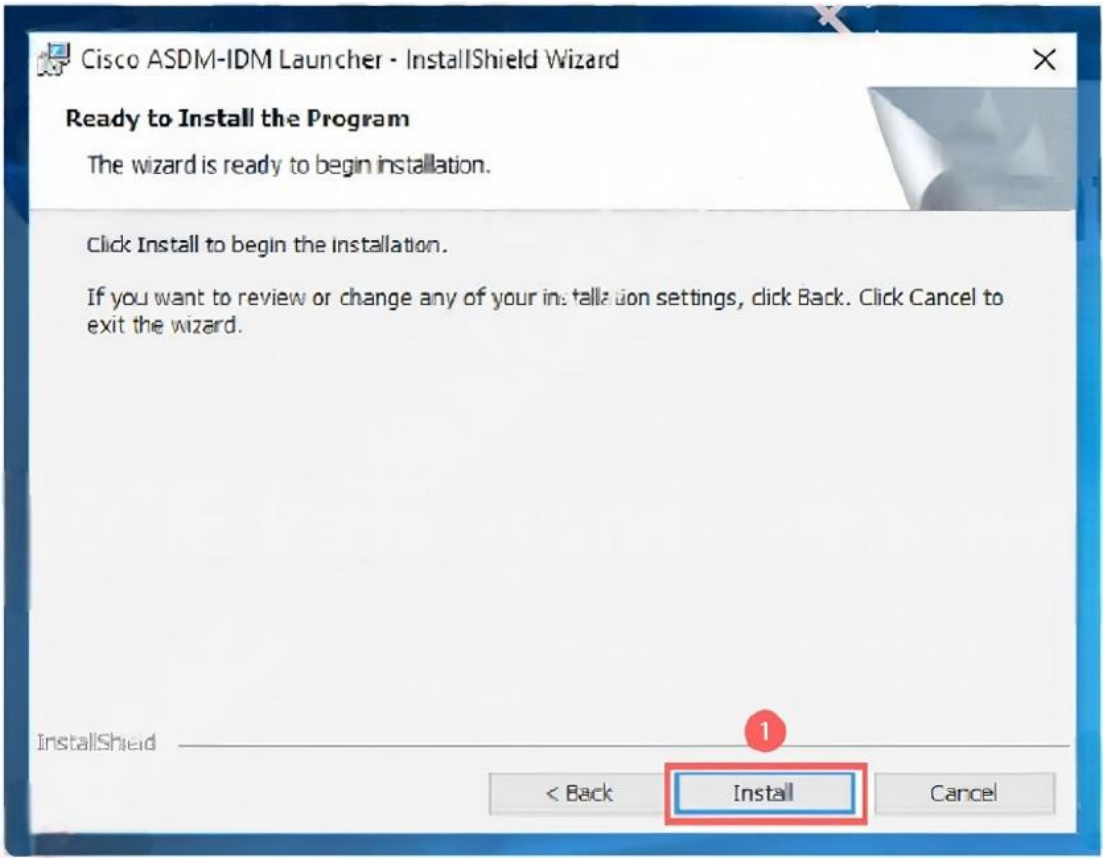

Application Tools
Downloads
File
Home
Share
View
Manage
This PC › Local Disk (C:) › Users › admin › Downloads
Search Downloads
Quick access
Desktop
dm-launcher
6/30/2024 10:16 AM
Windows Installer ...
757 KB

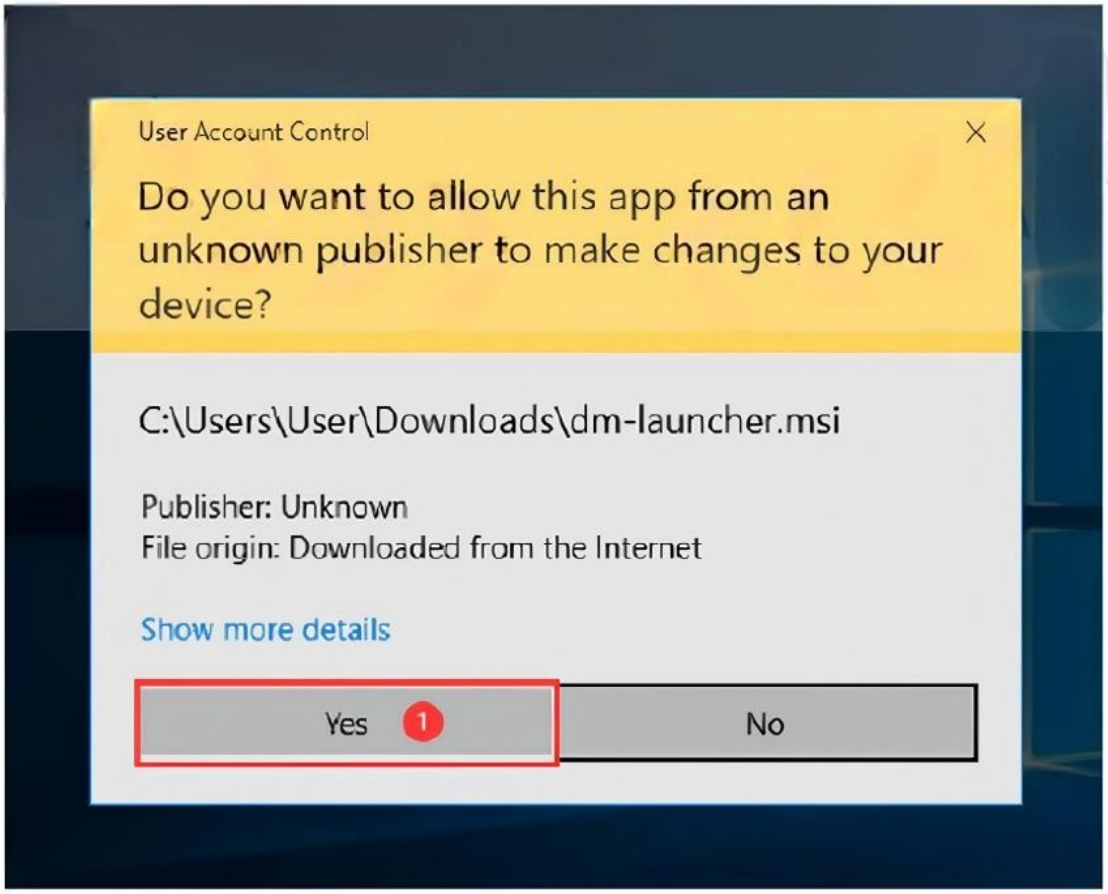

Application Tools
Downloads
File
Home
Share
View
Manage
This PC › Local Disk (C:) › Users › admin › Downloads
Search Downloads
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
OneDrive
This PC
Local Disk (C:)
Network
dm-launcher
6/30/2024 10:16 AM
Windows Installer ...
757 KB
1
Double click to open the installation package
1 item
1 item selected 757 KB

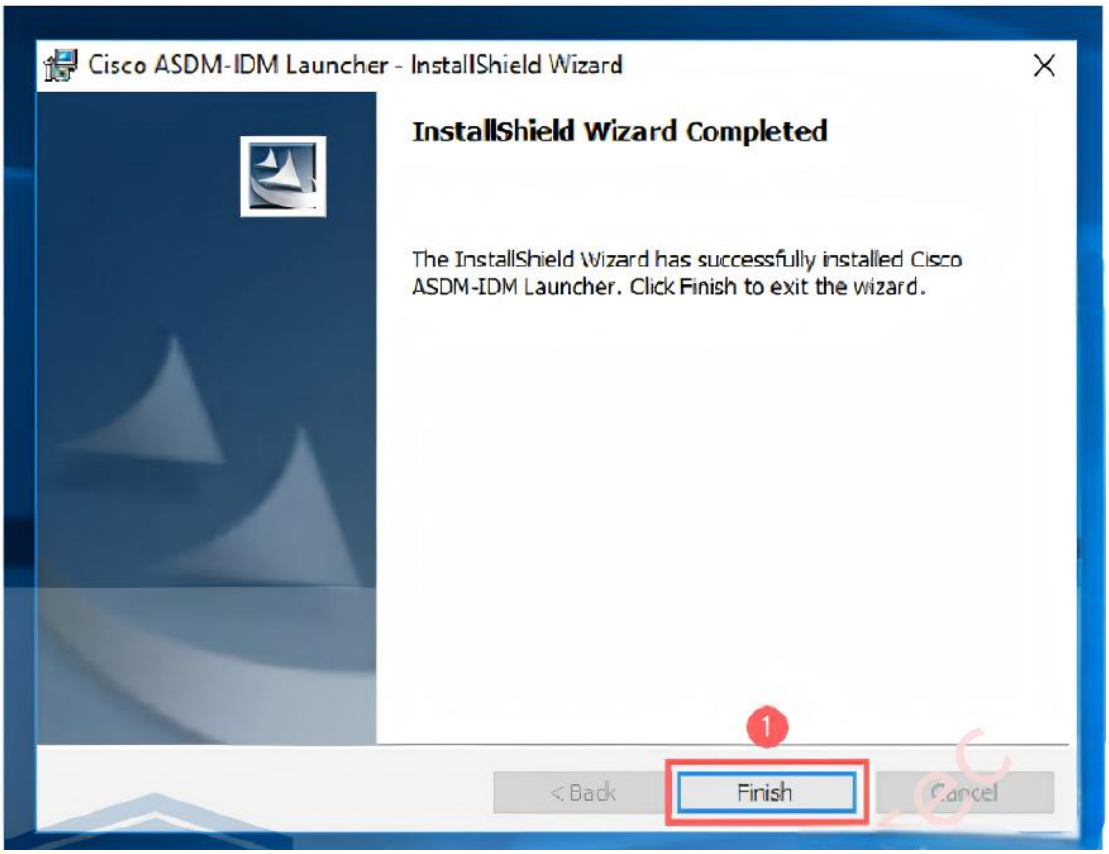

Application Tools
Downloads
File
Home
Share
View
Manage
This PC › Local Disk (C:) › Users › User › Downloads
Search Downloads
Name
Date modified
Type
Size
Quick access
Desktop
Downloads
Documents
Pictures
Software Backup
OneDrive
This PC
DVD Drive (D:) 20220
Local Disk (C:)
Network
Homegroup
757 KB
Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: C:\Users\User\Downloads\dm-launcher.msi
Publisher: Unknown Publisher
Type: Windows Installer Package
From: C:\Users\User\Downloads\dm-launcher.msi
Run
Cancel
1
Always ask before opening this file
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?
1 item
1 item selected 757 KB

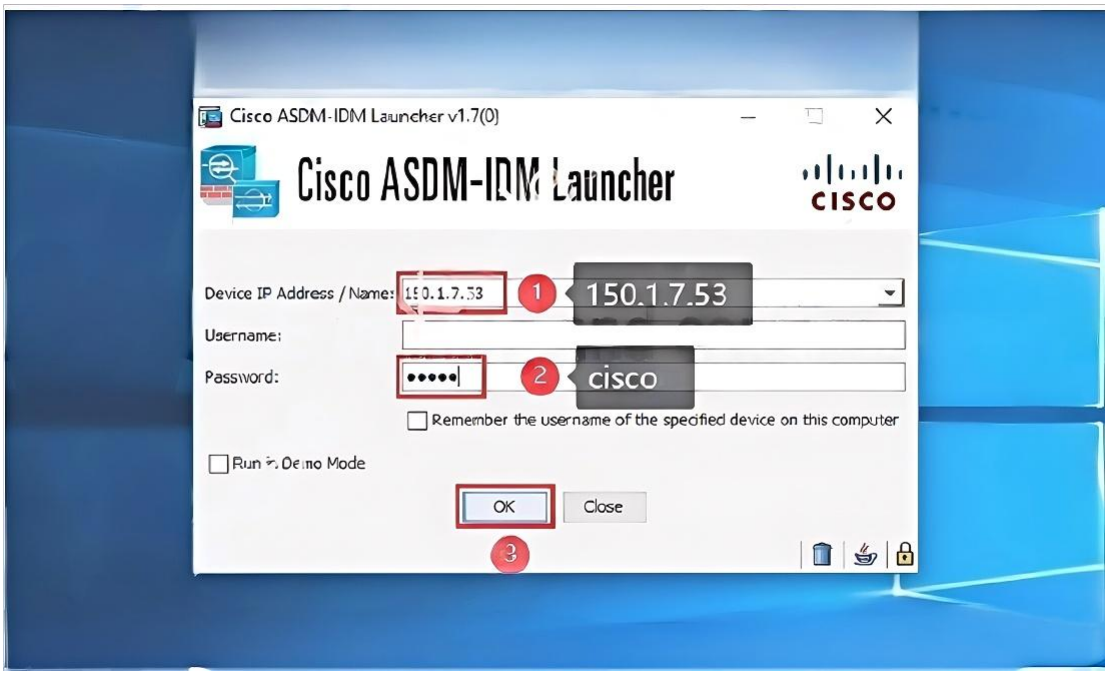

Cisco ASDM-IDM Launcher - InstallShield Wizard
Welcome to the InstallShield Wizard for Cisco ASDM-IDM Launcher
The InstallShield(R) Wizard will install Cisco ASDM-IDM Launcher v1.7(0) on your computer.
To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
1
< Back
Next >
Cancel

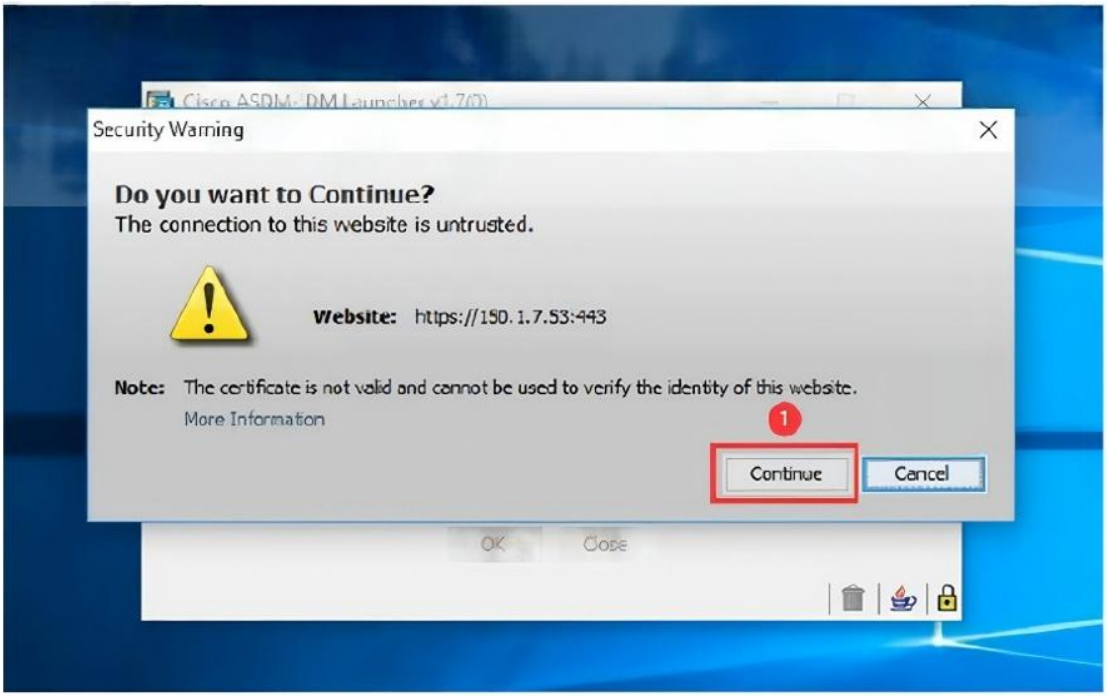

Cisco ASDM-IDM Launcher - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install Cisco ASDM-IDM Launcher to:
C:\Program Files (x86)\Cisco Systems\ASDM\
Change...
InstallShield
1
< Back
Next >
Cancel

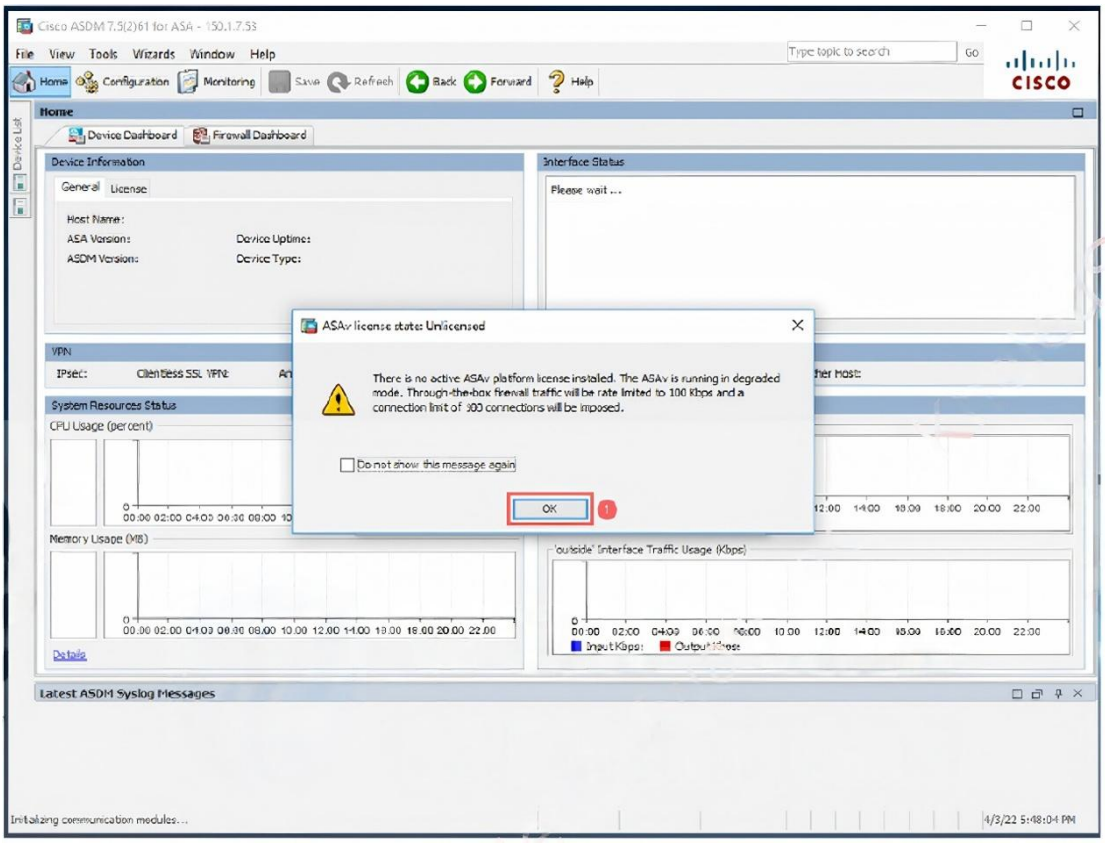

Cisco ASDM-IDM Launcher - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
1
< Back
Install
Cancel

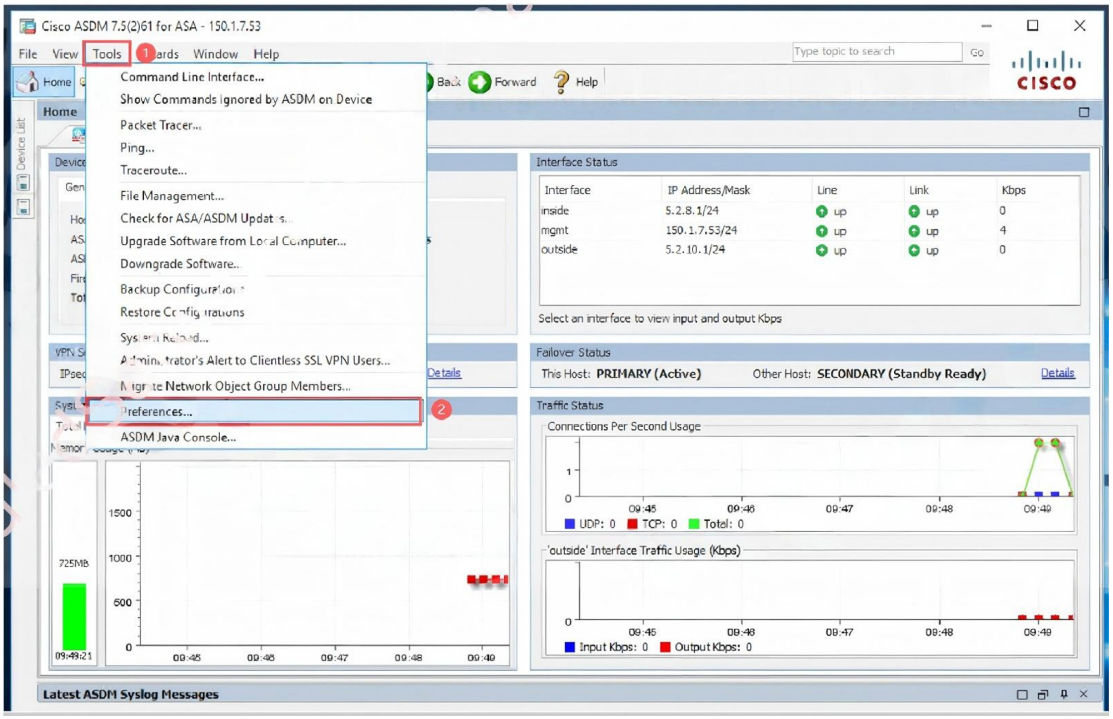

User Account Control
Do you want to allow this app from an unknown publisher to make changes to your device?
C:\Users\User\Downloads\dm-launcher.msi
Publisher: Unknown
File origin: Downloaded from the Internet
Show more details
Yes
1
No

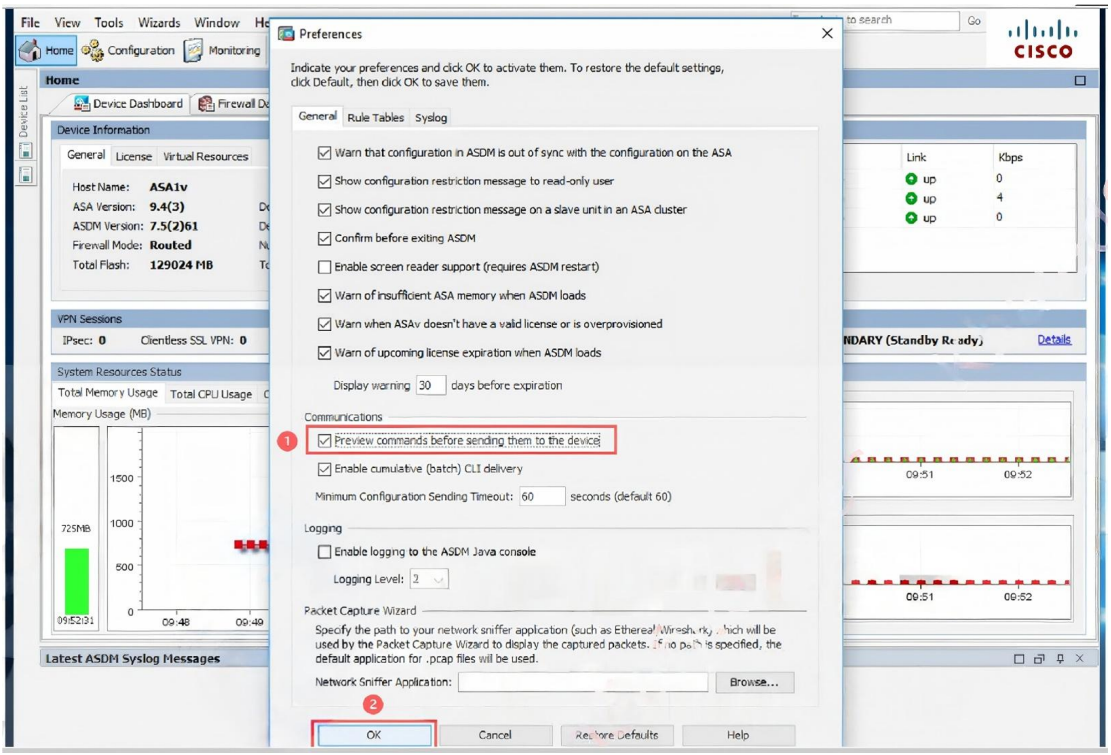

Cisco ASDM-IDM Launcher - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed Cisco ASDM-IDM Launcher. Click Finish to exit the wizard.
1
< Back
Finish
Cancel

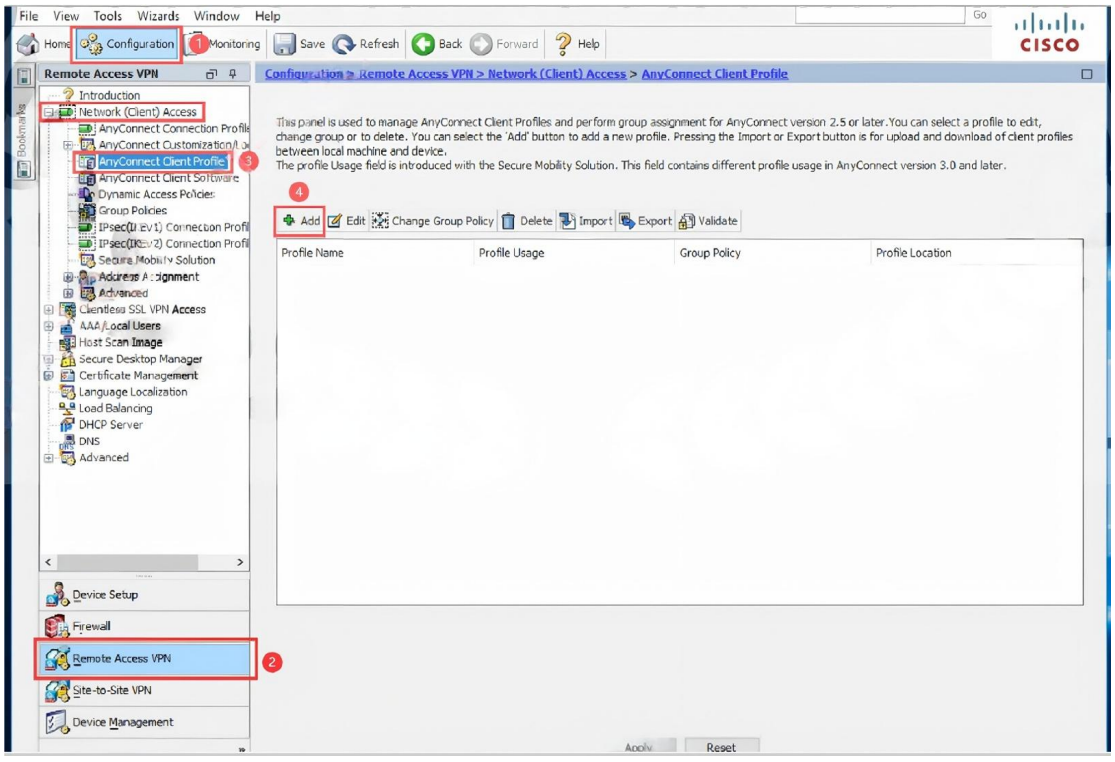

Cisco ASDM-IDM Launcher v1.7(0)
Cisco ASDM-IDM Launcher
CISCO
Device IP Address / Name:
150.1.7.53
Username:
Password:
cisco
Remember the username of the specified device on this computer
Run in Demo Mode
OK
Close
1
2
3

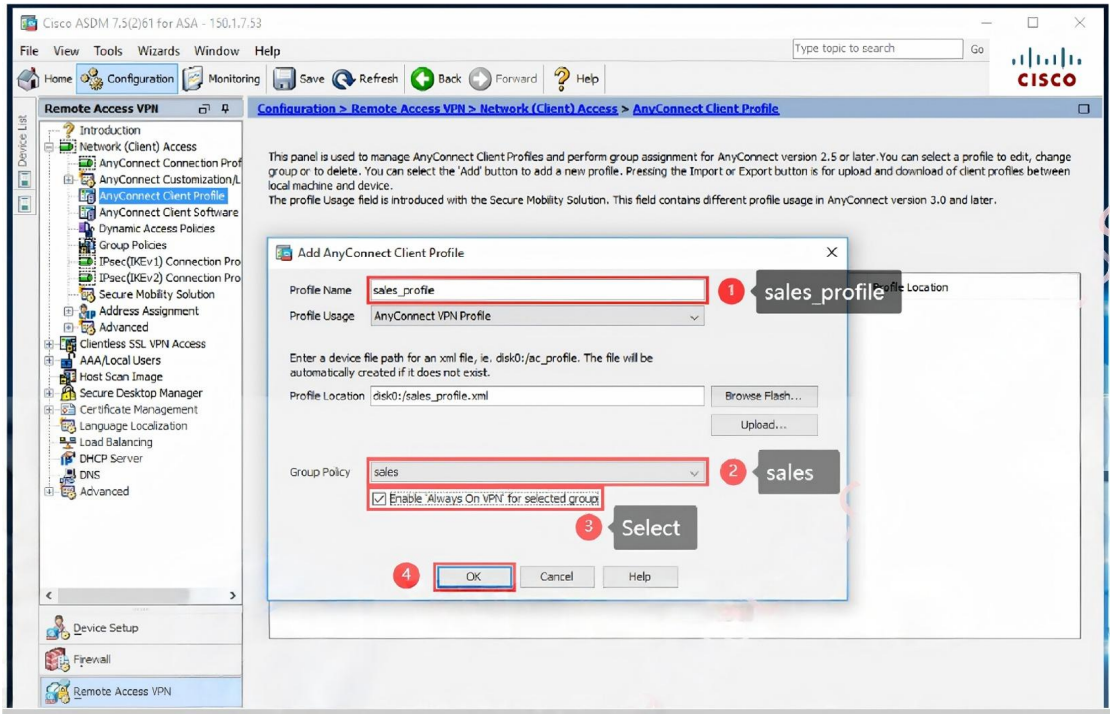

Security Warning
Do you want to Continue?
The connection to this website is untrusted.
Website: https://150.1.7.53:443
Note: The certificate is not valid and cannot be used to verify the identity of this website.
More Information
Continue
Cancel
1

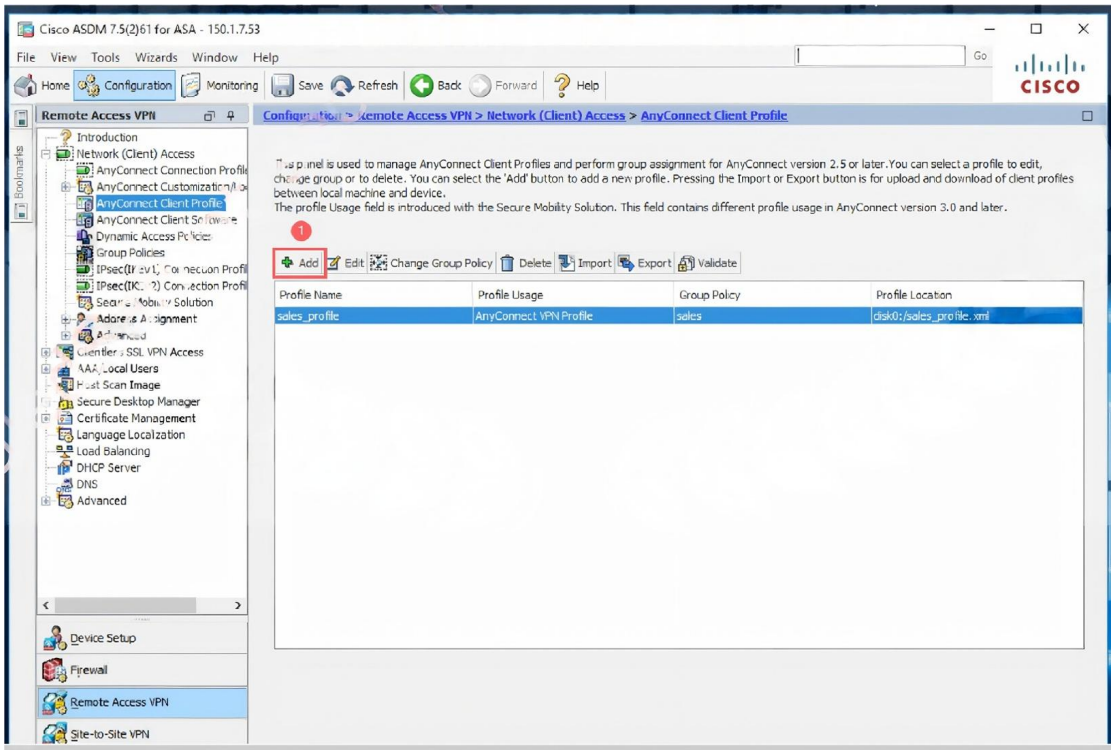

Cisco ASDM 7.5(2)61 for ASA - 150.1.7.53
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Home
Device Dashboard Firewall Dashboard
Device Information
General License
Host Name:
ASA Version:
Device Uptime:
ASDM Version:
Device Type:
Interface Status
Please wait ...
ASAv license state: Unlicensed
There is no active ASAv platform license installed. The ASAv is running in degraded mode. Through-the-box firewall traffic will be rate limited to 100 Kbps and a connection limit of 200 connections will be imposed.
Do not show this message again
OK
VPN
IPsec: Clientless SSL VPN:
System Resources Status
CPU Usage (percent)
Memory Usage (MB)
'outside' Interface Traffic Usage (Kbps)
Details
Latest ASDM Syslog Messages
Initializing communication modules...
4/3/22 5:48:04 PM

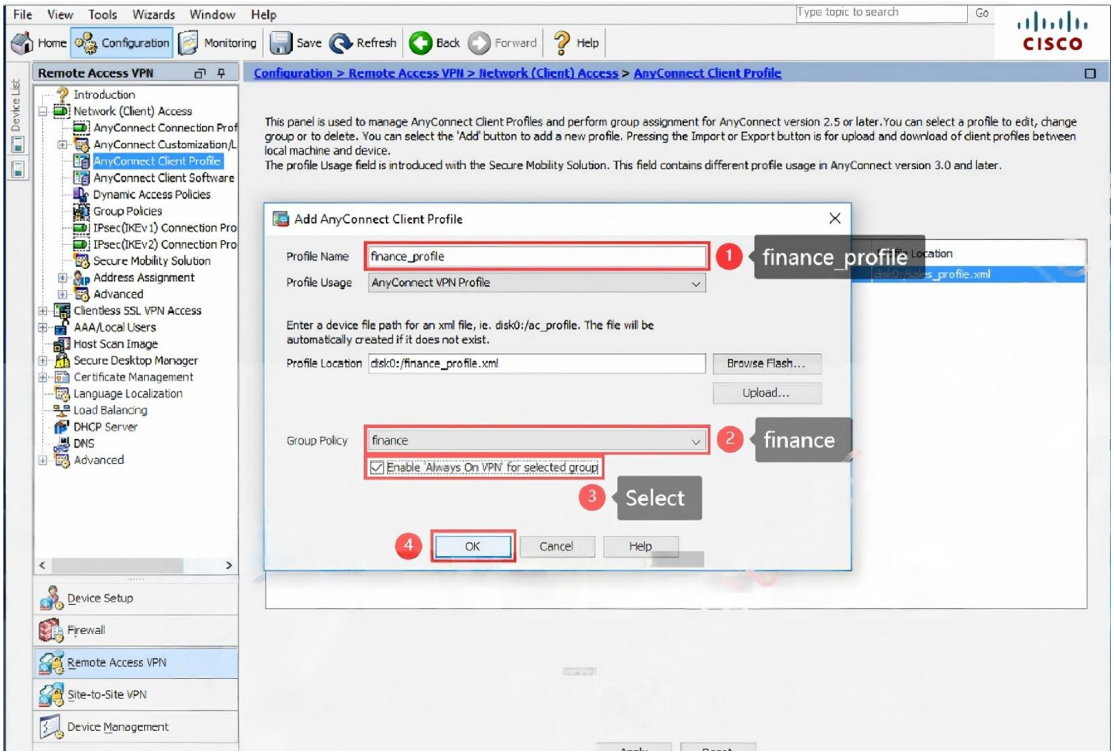

Cisco ASDM 7.5(2)61 for ASA - 150.1.7.53
File View Tools Wizards Window Help
Command Line Interface...
Show Commands Ignored by ASDM on Device
Packet Tracer...
Ping...
Traceroute...
File Management...
Check for ASA/ASDM Updates...
Upgrade Software from Local Computer...
Downgrade Software...
Backup Configurations
Restore Configurations
Reload...
Administrator's Alert to Clientless SSL VPN Users...
Migrate Network Object Group Members...
Preferences...
ASDM Java Console...
Interface Status
Interface IP Address/Mask Line Link Kbps
inside 5.2.8.1/24 up up 0
mgmt 150.1.7.53/24 up up 4
outside 5.2.10.1/24 up up 0
Select an interface to view input and output Kbps
Failover Status
This Host: PRIMARY (Active)
Other Host: SECONDARY (Standby Ready)
Details
Traffic Status
Connections Per Second Usage
UDP: 0 TCP: 0 Total: 0
'outside' Interface Traffic Usage (Kbps)
Input Kbps: 0 Output Kbps: 0
Latest ASDM Syslog Messages

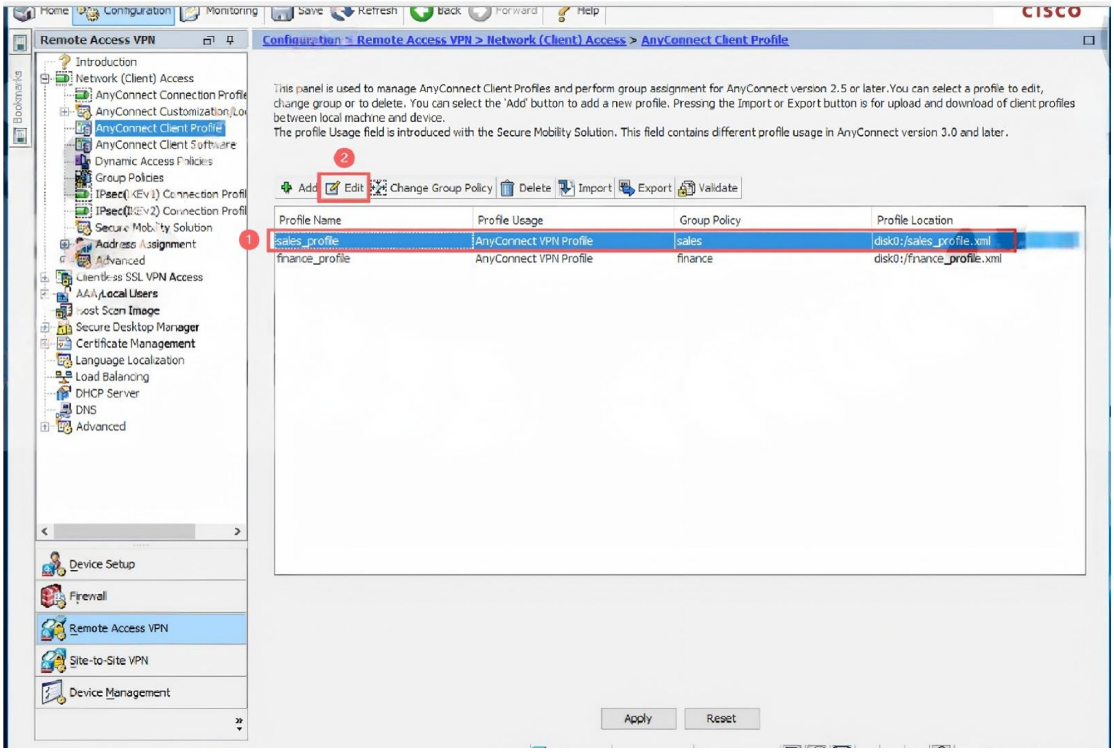

Preferences
Indicate your preferences and click OK to activate them. To restore the default settings, click Default, then click OK to save them.
General
Rule Tables
Syslog
Warn that configuration in ASDM is out of sync with the configuration on the ASA
Show configuration restriction message to read-only user
Show configuration restriction message on a slave unit in an ASA cluster
Confirm before exiting ASDM
Enable screen reader support (requires ASDM restart)
Warn of insufficient ASA memory when ASDM loads
Warn when ASAv doesn't have a valid license or is overprovisioned
Warn of upcoming license expiration when ASDM loads
Display warning 30 days before expiration
Communications
Preview commands before sending them to the device
Enable cumulative (batch) CLI delivery
Minimum Configuration Sending Timeout: 60 seconds (default 60)
Logging
Enable logging to the ASDM Java console
Logging Level: 7
Packet Capture Wizard
Specify the path to your network sniffer application (such as Ethereal/Wireshark) which will be used by the Packet Capture Wizard to display the captured packets. If no path is specified, the default application for .pcap files will be used.
Network Sniffer Application:
Browse...
OK
Cancel
Restore Defaults
Help

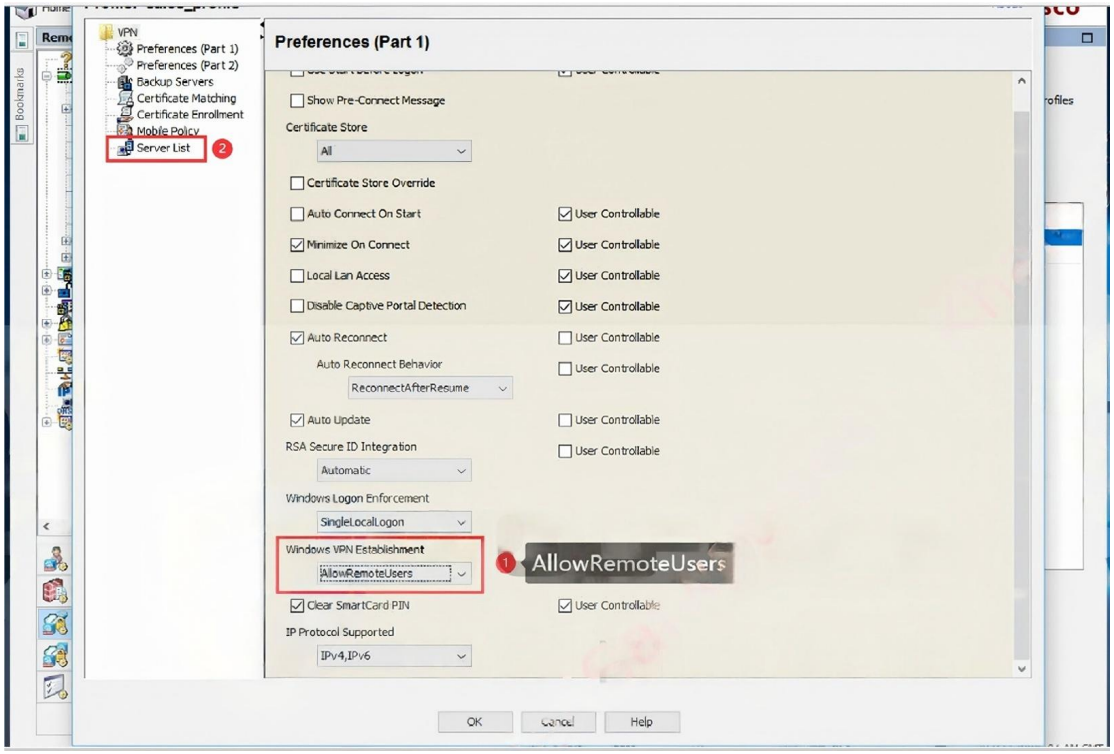

File View Tools Wizards Window Help
Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
IPsec(IKEv2) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile
This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later. You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.
Add
Edit
Change Group Policy
Delete
Import
Export
Validate
Profile Name
Profile Usage
Group Policy
Profile Location
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset

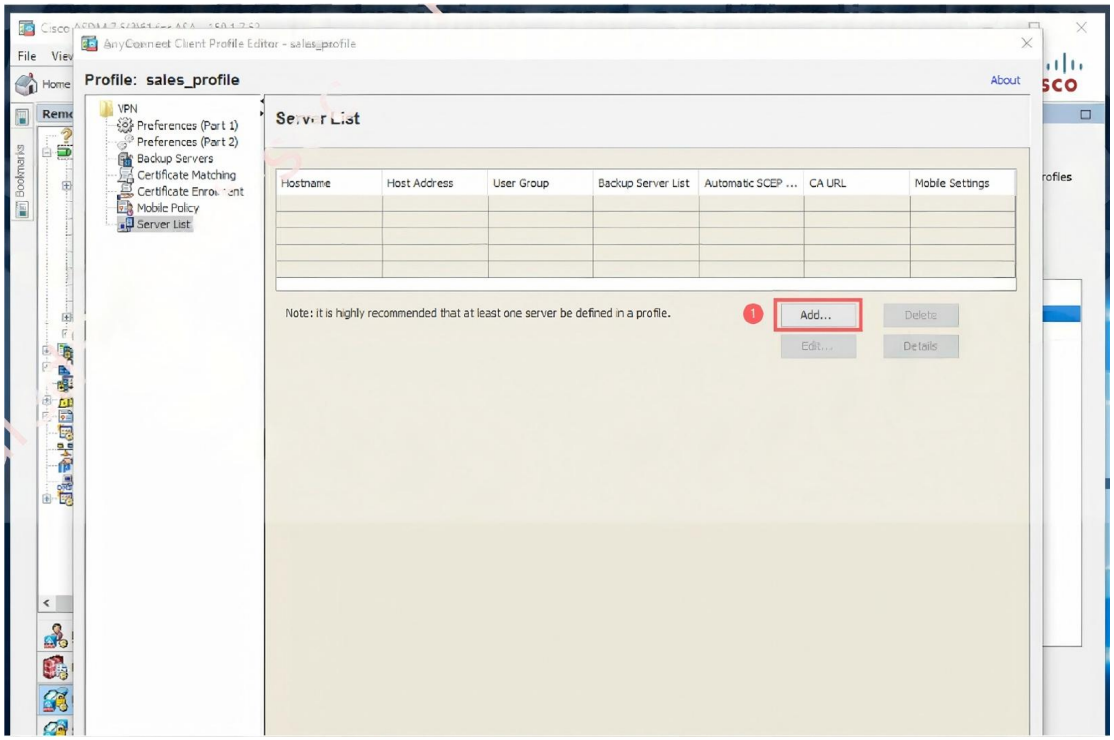

Cisco ASDM 7.5(2)61 for ASA - 150.1.7.53
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile
This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later. You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.
Add AnyConnect Client Profile
Profile Name sales_profile
Profile Usage AnyConnect VPN Profile
Enter a device file path for an xml file, ie. disk0:/ac_profile. The file will be automatically created if it does not exist.
Profile Location disk0:/sales_profile.xml
Browse Flash...
Upload...
Group Policy sales
Enable 'Always On VPN' for selected group
1 sales_profile
2 sales
3 Select
4 OK Cancel Help
Device Setup
Firewall
Remote Access VPN

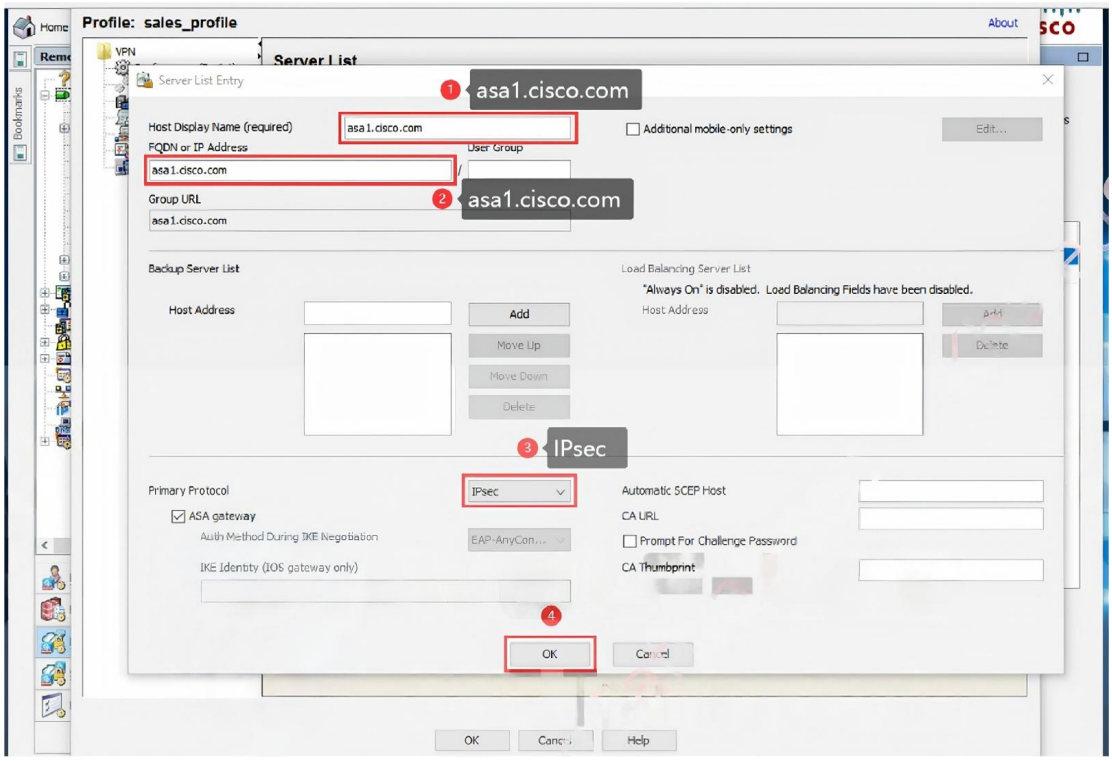

Cisco ASDM 7.5(2)61 for ASA - 150.1.7.53
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Remote Access VPN
Network (Client) Access > AnyConnect Client Profile
This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later. You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.
1
Add Edit Change Group Policy Delete Import Export Validate
Profile Name Profile Usage Group Policy Profile Location
sales_profile AnyConnect VPN Profile sales disk0:/sales_profile.xml
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN

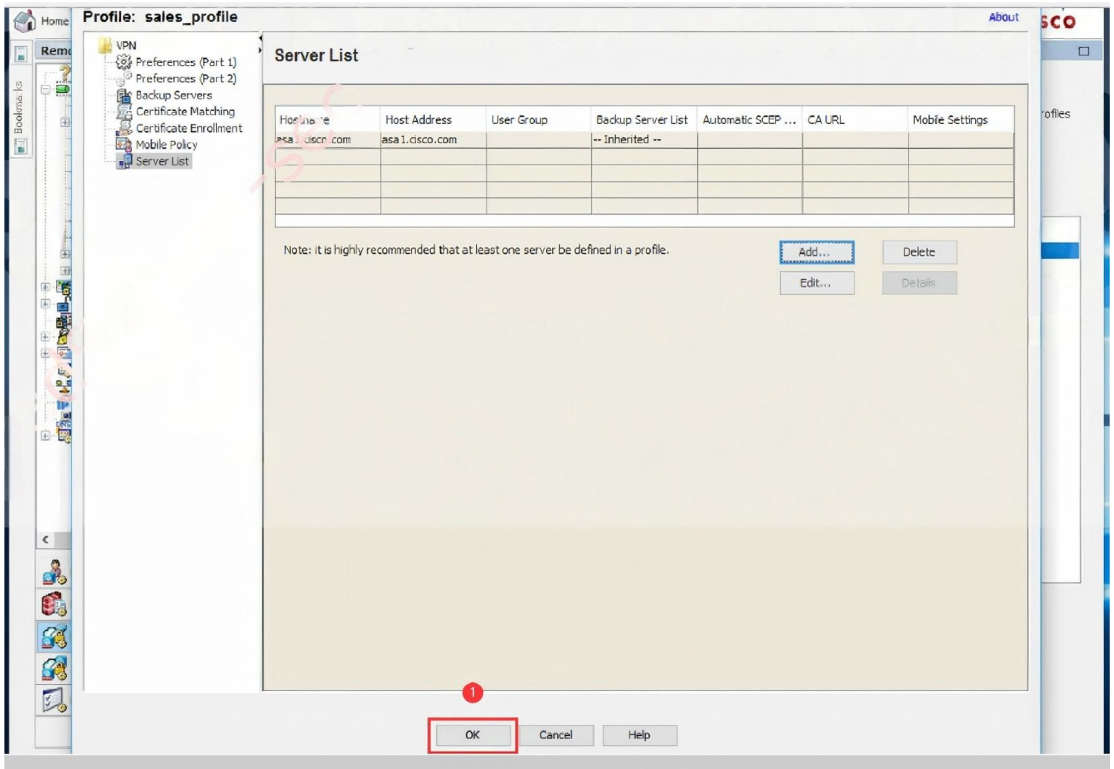

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile
This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later. You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.
Add AnyConnect Client Profile
Profile Name
finance_profile
1
Profile Usage
AnyConnect VPN Profile
Enter a device file path for an xml file, ie. disk0:/ac_profile. The file will be automatically created if it does not exist.
Profile Location
disk0:/finance_profile.xml
Browse Flash...
Upload...
Group Policy
finance
2
Enable 'Always On VPN' for selected group
3
Select
4
OK
Cancel
Help

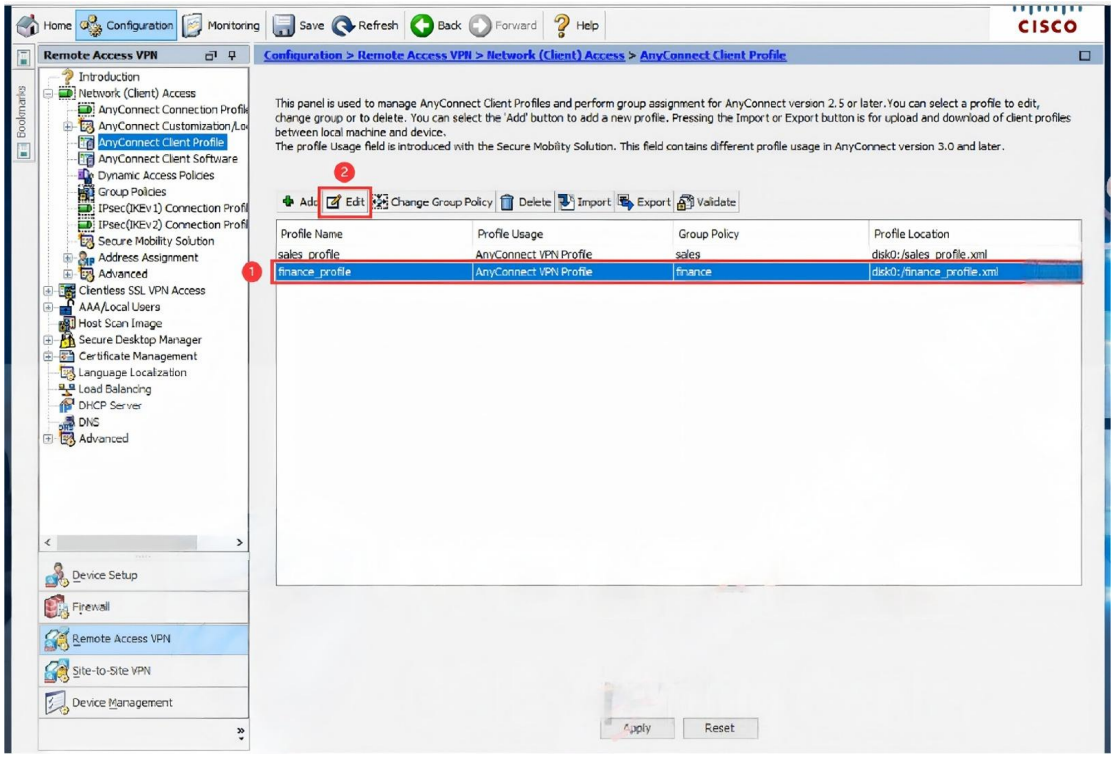

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile
This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later. You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.
2
Add
Edit
Change Group Policy
Delete
Import
Export
Validate
Profile Name
Profile Usage
Group Policy
Profile Location
1
sales_profile
AnyConnect VPN Profile
sales
disk0:/sales_profile.xml
finance_profile
AnyConnect VPN Profile
finance
disk0:/finance_profile.xml
Apply
Reset

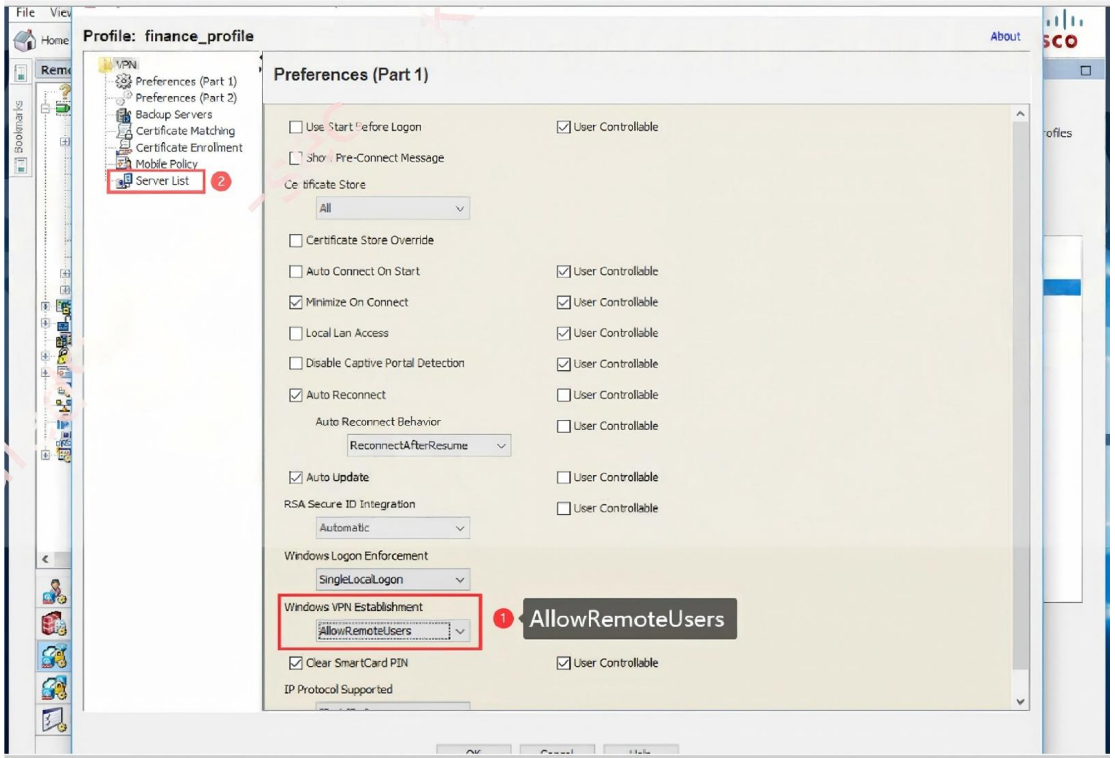

VPN
Preferences (Part 1)
Preferences (Part 2)
Backup Servers
Certificate Matching
Certificate Enrollment
Mobile Policy
Server List
2
Preferences (Part 1)
Show Pre-Connect Message
Certificate Store
All
Certificate Store Override
Auto Connect On Start
User Controllable
Minimize On Connect
User Controllable
Local Lan Access
User Controllable
Disable Captive Portal Detection
User Controllable
Auto Reconnect
User Controllable
Auto Reconnect Behavior
User Controllable
ReconnectAfterResume
Auto Update
User Controllable
RSA Secure ID Integration
User Controllable
Automatic
Windows Logon Enforcement
SingleLocalLogon
Windows VPN Establishment
AllowRemoteUsers
1
AllowRemoteUsers
Clear SmartCard PIN
User Controllable
IP Protocol Supported
IPv4,IPv6
OK
Cancel
Help

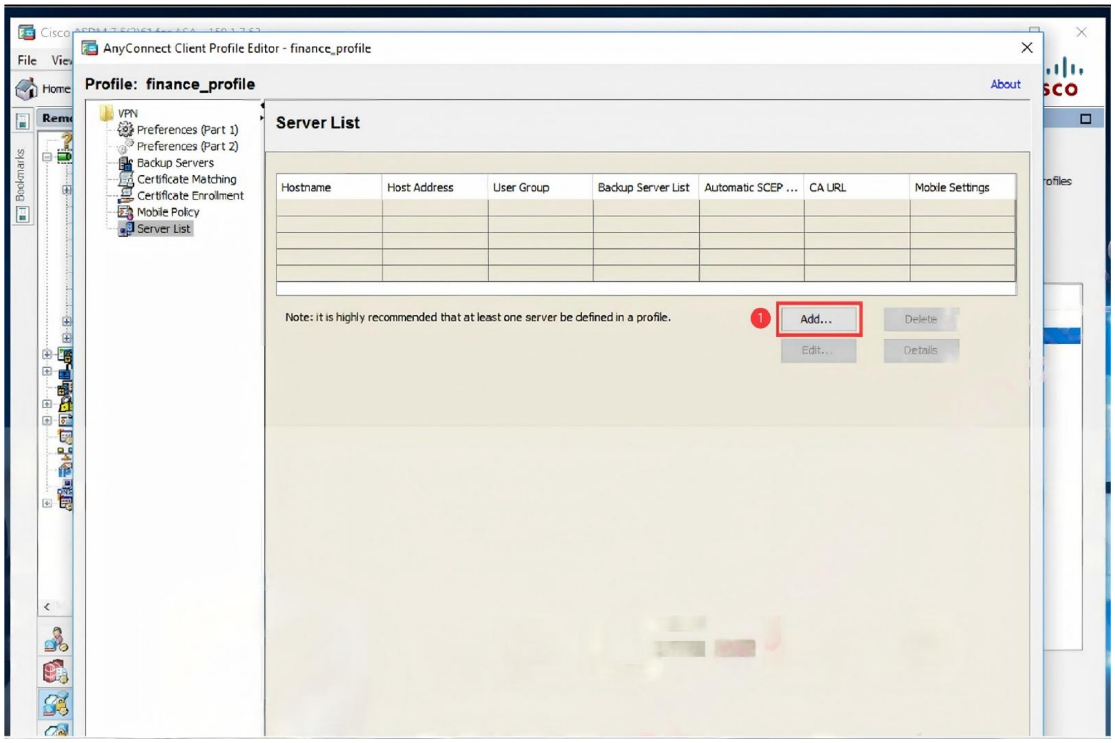

AnyConnect Client Profile Editor - sales_profile
Profile: sales_profile
About
VPN
Preferences (Part 1)
Preferences (Part 2)
Backup Servers
Certificate Matching
Mobile Policy
Server List
Hostname
Host Address
User Group
Backup Server List
Automatic SCEP ...
CA URL
Mobile Settings
Note: it is highly recommended that at least one server be defined in a profile.
1
Add...
Delete
Edit...
Details

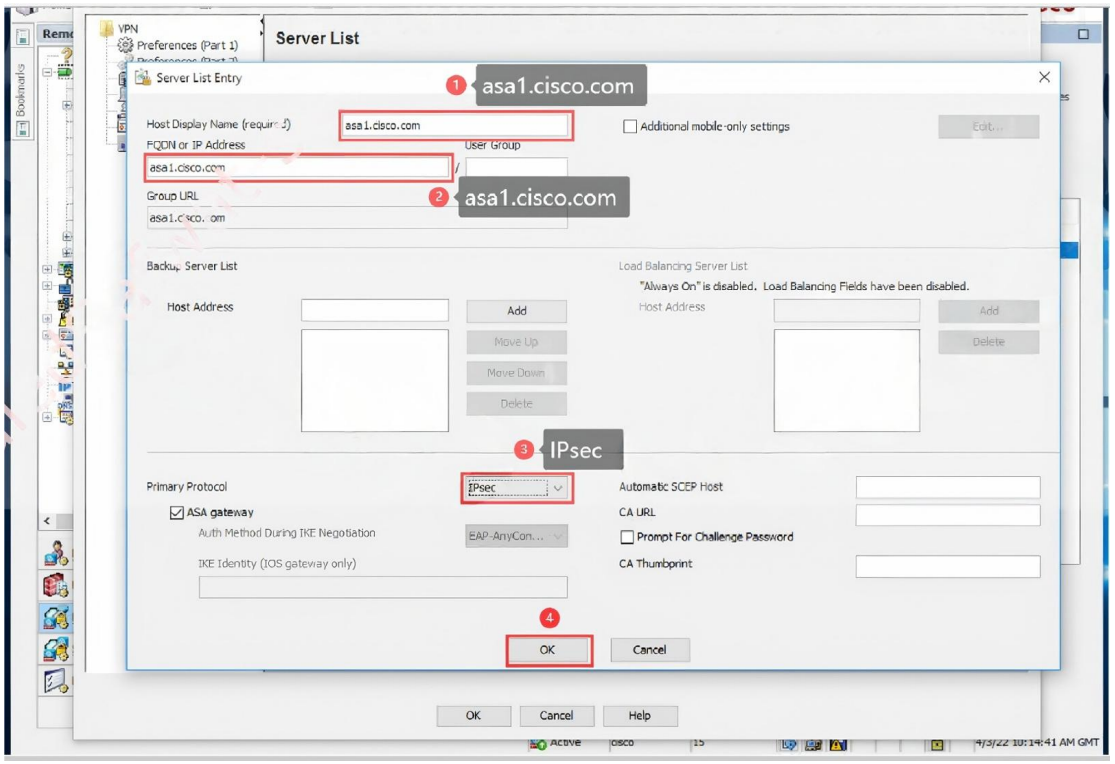

Profile: sales_profile
About
Server List
Server List Entry
1 asa1.cisco.com
Host Display Name (required)
asa1.cisco.com
Additional mobile-only settings
Edit...
FQDN or IP Address
asa1.cisco.com
User Group
Group URL
2 asa1.cisco.com
asa1.cisco.com
Backup Server List
Load Balancing Server List
"Always On" is disabled. Load Balancing Fields have been disabled.
Host Address
Add
Move Up
Move Down
Delete
3 IPsec
Primary Protocol
IPsec
Automatic SCEP Host
ASA gateway
CA URL
Auth Method During IKE Negotiation
EAP-AnyCon...
Prompt For Challenge Password
IKE Identity (IOS gateway only)
CA Thumbprint
4
OK
Cancel
OK
Help

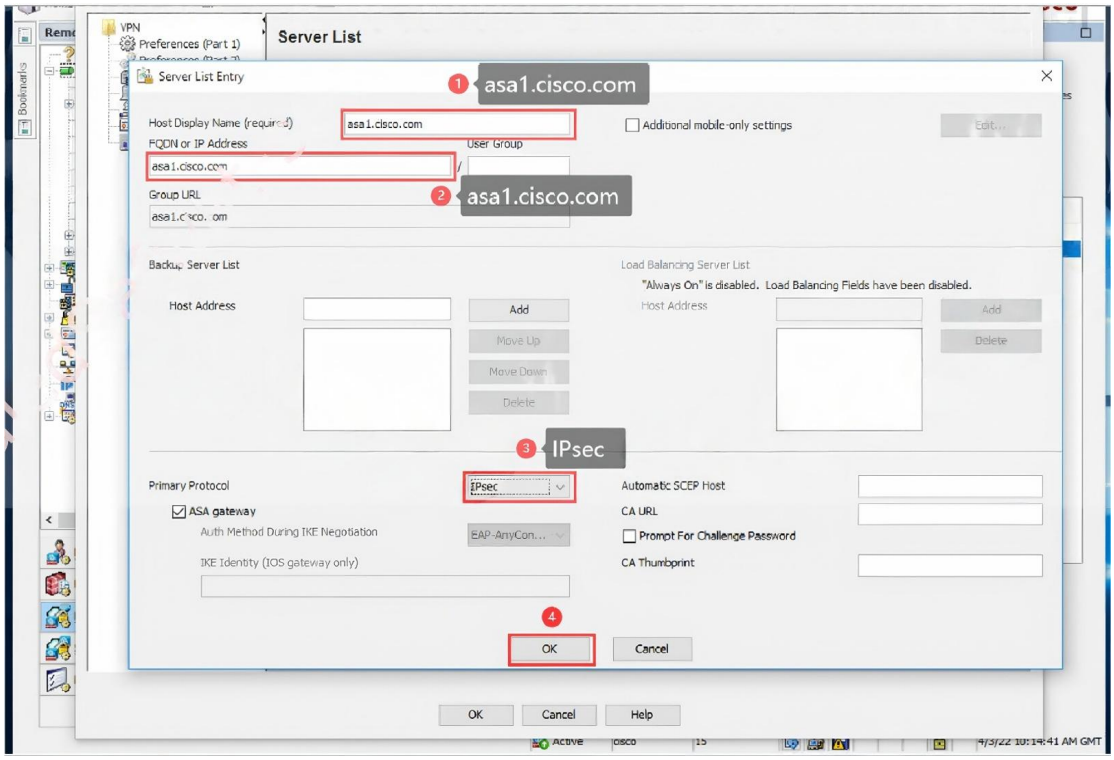

Profile: sales_profile
About
VPN
Preferences (Part 1)
Preferences (Part 2)
Backup Servers
Certificate Matching
Certificate Enrollment
Mobile Policy
Server List
Server List
Host Address
User Group
Backup Server List
Automatic SCEP ...
CA URL
Mobile Settings
asa1.cisco.com
-- Inherited --
Note: it is highly recommended that at least one server be defined in a profile.
Add...
Delete
Edit...
Details
1
OK
Cancel
Help

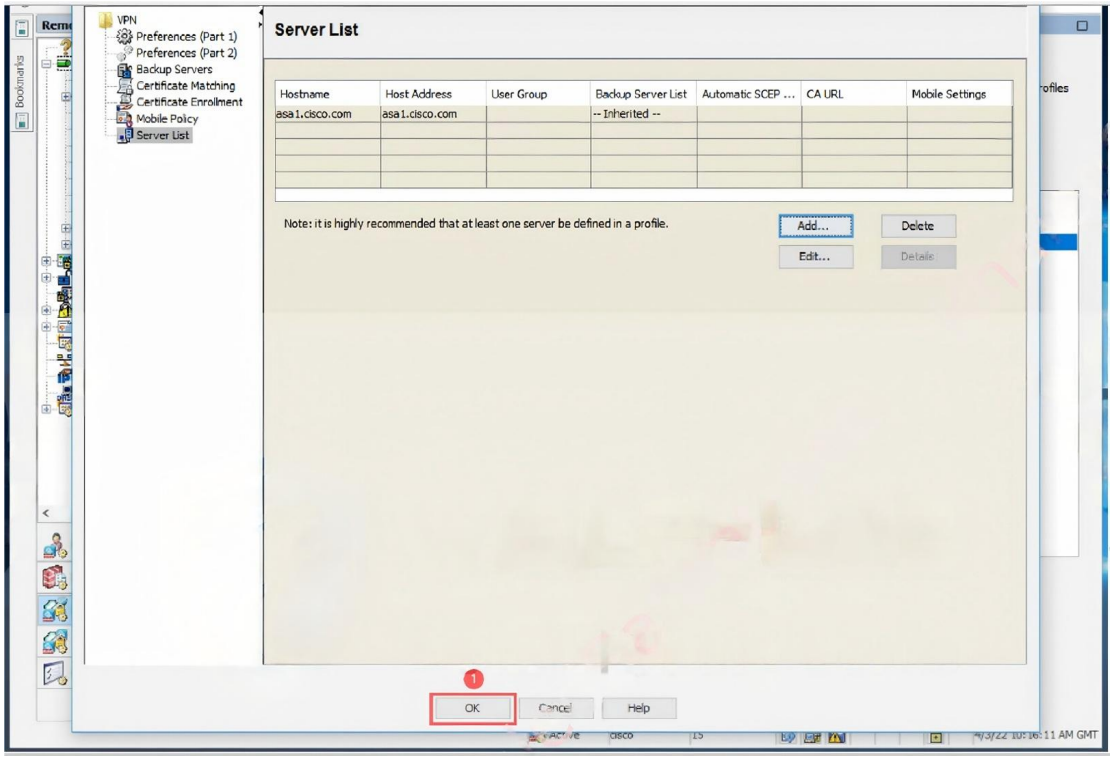

Home
Configuration
Monitoring
Save
Refresh
Back
Forward
Help
CISCO
Remote Access VPN
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Software
Dynamic Access Policies
Group Policies
IPsec(IKEv1) Connection Profiles
IPsec(IKEv2) Connection Profiles
Secure Mobility Solution
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Image
Secure Desktop Manager
Certificate Management
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later. You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.
Add
Edit
Change Group Policy
Delete
Import
Export
Validate
Profile Name
Profile Usage
Group Policy
Profile Location
sales_profile
AnyConnect VPN Profile
sales
disk0:/sales_profile.xml
finance_profile
AnyConnect VPN Profile
finance
disk0:/finance_profile.xml
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Apply
Reset

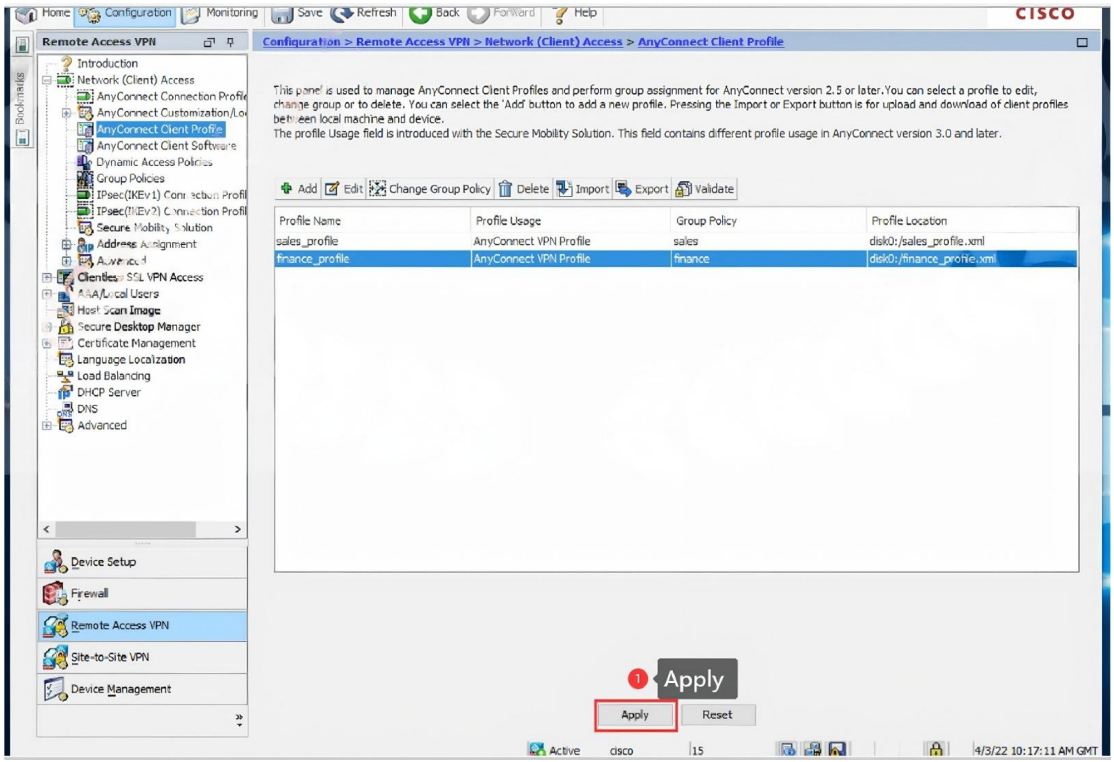

Profile: finance_profile
About
VPN
Preferences (Part 1)
Preferences (Part 2)
Backup Servers
Certificate Matching
Certificate Enrollment
Mobile Policy
Server List
Preferences (Part 1)
Use Start Before Logon
User Controllable
Show Pre-Connect Message
Certificate Store
All
Certificate Store Override
Auto Connect On Start
Minimize On Connect
Local Lan Access
Disable Captive Portal Detection
Auto Reconnect
Auto Reconnect Behavior
ReconnectAfterResume
Auto Update
RSA Secure ID Integration
Automatic
Windows Logon Enforcement
SingleLocalLogon
Windows VPN Establishment
AllowRemoteUsers
AllowRemoteUsers
Clear SmartCard PIN
IP Protocol Supported

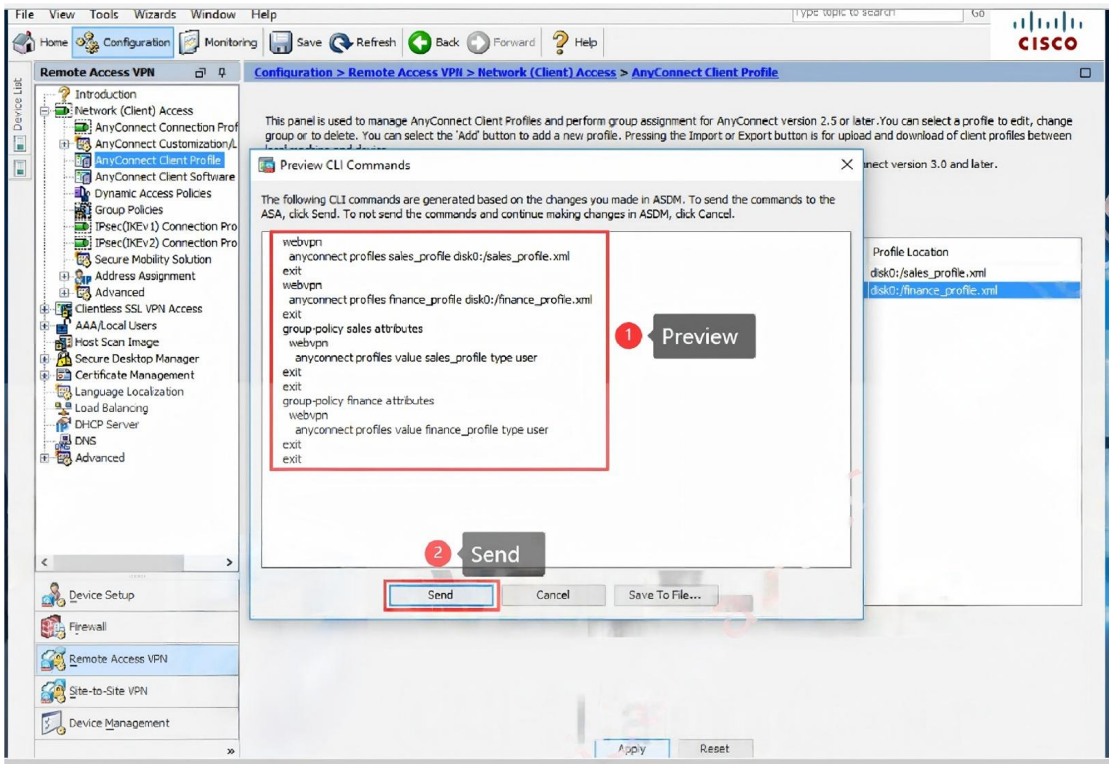

AnyConnect Client Profile Editor - finance_profile
Profile: finance_profile
About
VPN
Preferences (Part 1)
Preferences (Part 2)
Backup Servers
Certificate Matching
Certificate Enrollment
Mobile Policy
Server List
Server List
Hostname
Host Address
User Group
Backup Server List
Automatic SCEP ...
CA URL
Mobile Settings
Note: it is highly recommended that at least one server be defined in a profile.
1
Add...
Delete
Edit...
Details

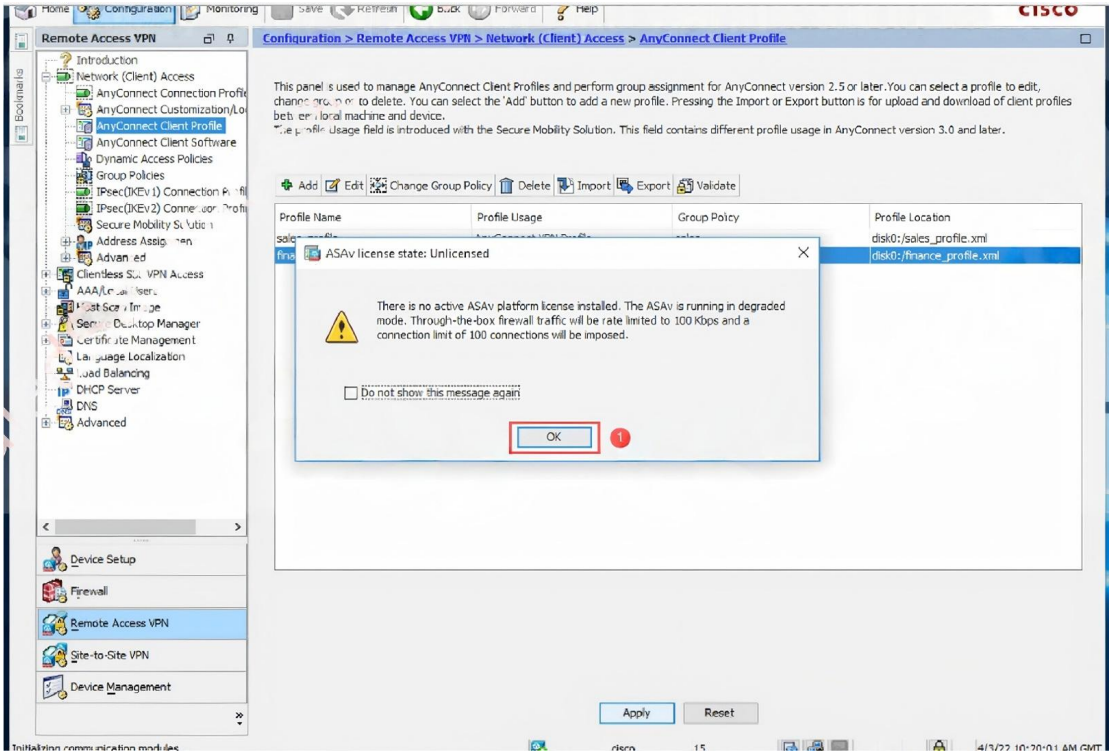

Server List
Server List Entry
1
asa1.cisco.com
Host Display Name (requir
asa1.cisco.com
Additional mobile-only settings
Edit...
FQDN or IP Address
User Group
asa1.cisco.com
2
asa1.cisco.com
Group URL
asa1.cisco.com
Backup Server List
Load Balancing Server List
"Always On" is disabled. Load Balancing Fields have been disabled.
Host Address
Add
Move Up
Move Down
Delete
Host Address
Add
Delete
3
IPsec
Primary Protocol
IPsec
ASA gateway
Auth Method During IKE Negotiation
EAP-AnyCon...
IKE Identity (IOS gateway only)
Automatic SCEP Host
CA URL
Prompt For Challenge Password
CA Thumbprint
4
OK
Cancel
OK
Cancel
Help


VPN
Preferences (Part 1)
Server List
Server List Entry
1 asa1.cisco.com
Host Display Name (required)
asa1.cisco.com
Additional mobile-only settings
Edit...
FQDN or IP Address
User Group
asa1.cisco.com
2 asa1.cisco.com
Group URL
Backup Server List
Load Balancing Server List
"Always On" is disabled. Load Balancing Fields have been disabled.
Host Address
Add
Move Up
Move Down
Delete
3 IPsec
Primary Protocol
IPsec
Automatic SCEP Host
ASA gateway
CA URL
Auth Method During IKE Negotiation
EAP-AnyCon...
Prompt For Challenge Password
IKE Identity (IOS gateway only)
CA Thumbprint
4
OK
Cancel
Help


VPN
Preferences (Part 1)
Preferences (Part 2)
Backup Servers
Certificate Matching
Certificate Enrollment
Mobile Policy
Server List
Server List
Hostname
Host Address
User Group
Backup Server List
Automatic SCEP ...
CA URL
Mobile Settings
asa1.cisco.com
asa1.cisco.com
-- Inherited --
Note: it is highly recommended that at least one server be defined in a profile.
Add...
Delete
Edit...
Details
1
OK
Cancel
Help


Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile
This panel is used to manage AnyConnect Client Profiles and perform group assignment for AnyConnect version 2.5 or later. You can select a profile to edit, change group or to delete. You can select the 'Add' button to add a new profile. Pressing the Import or Export button is for upload and download of client profiles between local machine and device.
The profile Usage field is introduced with the Secure Mobility Solution. This field contains different profile usage in AnyConnect version 3.0 and later.
Add
Edit
Change Group Policy
Delete
Import
Export
Validate
Profile Name
Profile Usage
Group Policy
Profile Location
sales_profile
AnyConnect VPN Profile
sales
disk0:/sales_profile.xml
finance_profile
AnyConnect VPN Profile
finance
disk0:/finance_profile.xml
1
Apply
Apply
Reset


Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile
Preview CLI Commands
The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the ASA, click Send. To not send the commands and continue making changes in ASDM, click Cancel.
webvpn
anyconnect profiles sales_profile disk0:/sales_profile.xml
exit
webvpn
anyconnect profiles finance_profile disk0:/finance_profile.xml
exit
group-policy sales attributes
webvpn
anyconnect profiles value sales_profile type user
exit
exit
group-policy finance attributes
webvpn
anyconnect profiles value finance_profile type user
exit
exit
1
Preview
2
Send
Send
Cancel
Save To File...
Profile Location
disk0:/sales_profile.xml
disk0:/finance_profile.xml



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 a2ed6522

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:

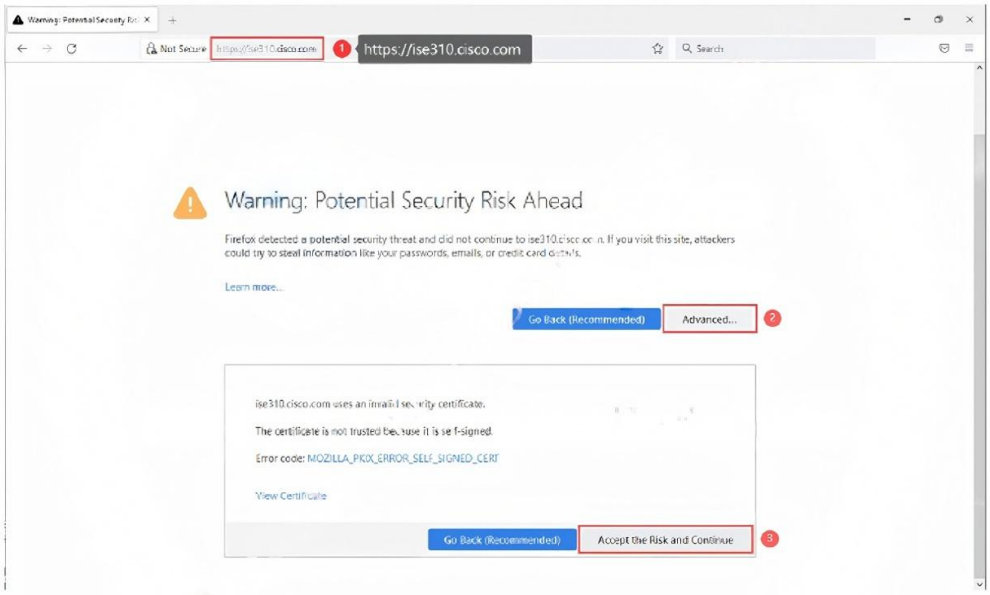
View the XML file and the configuration synchronized from the ASA11v

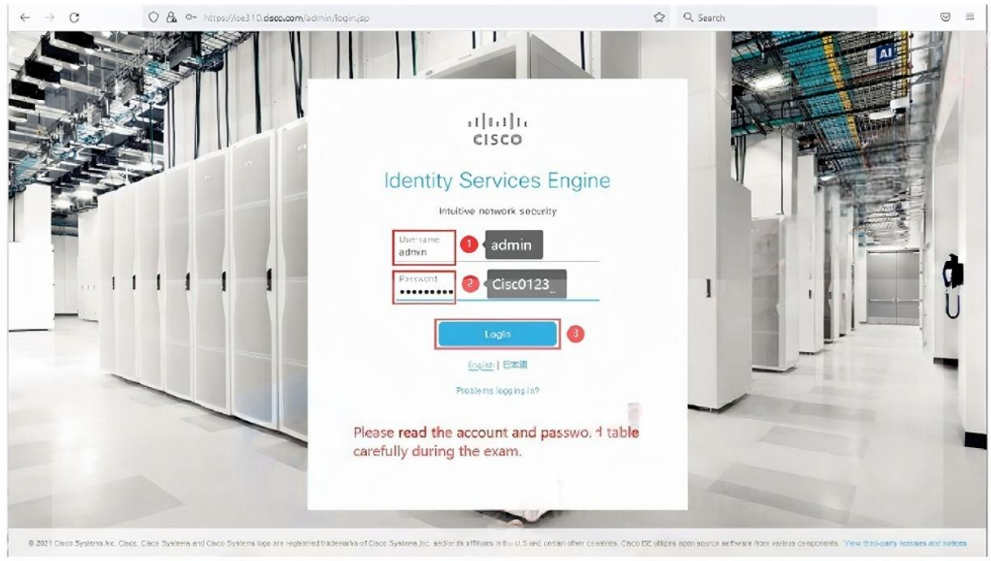
```
ASA1v/sec/stby# show run webvpn
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.2.04018-k9.pkg 1
 anyconnect profiles finance_profile disk0:/finance_profile.xml
 anyconnect profiles sales_profile disk0:/sales_profile.xml
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 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
```

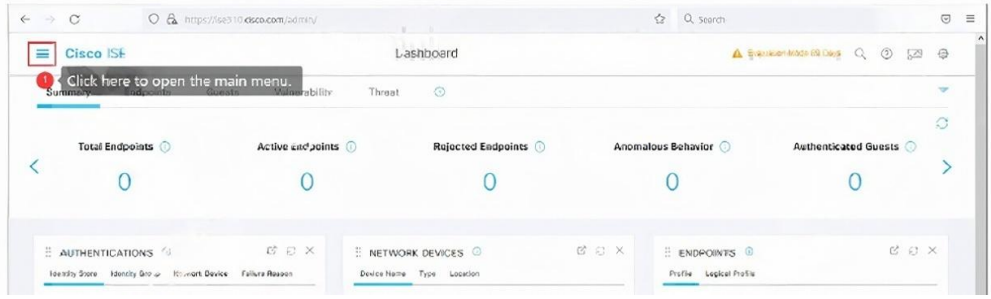
```
  anyconnect keep-installer installed
  anyconnect profiles value finance_profile type user
  always-on-vpn profile-setting
ASA1v/sec/stby#
```

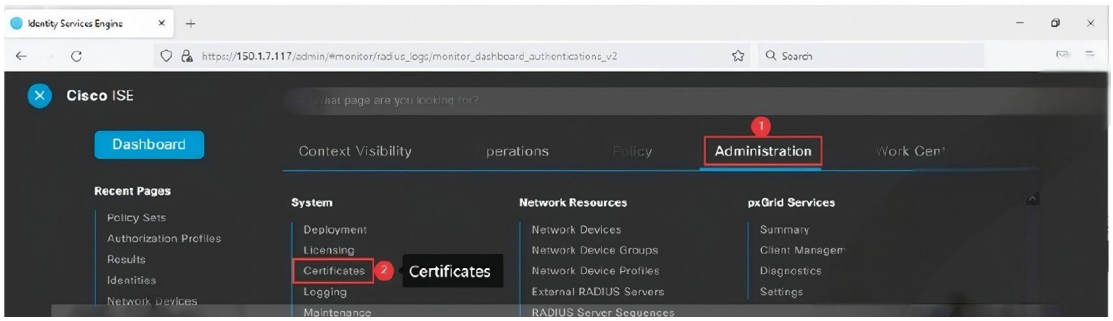
Management PC:

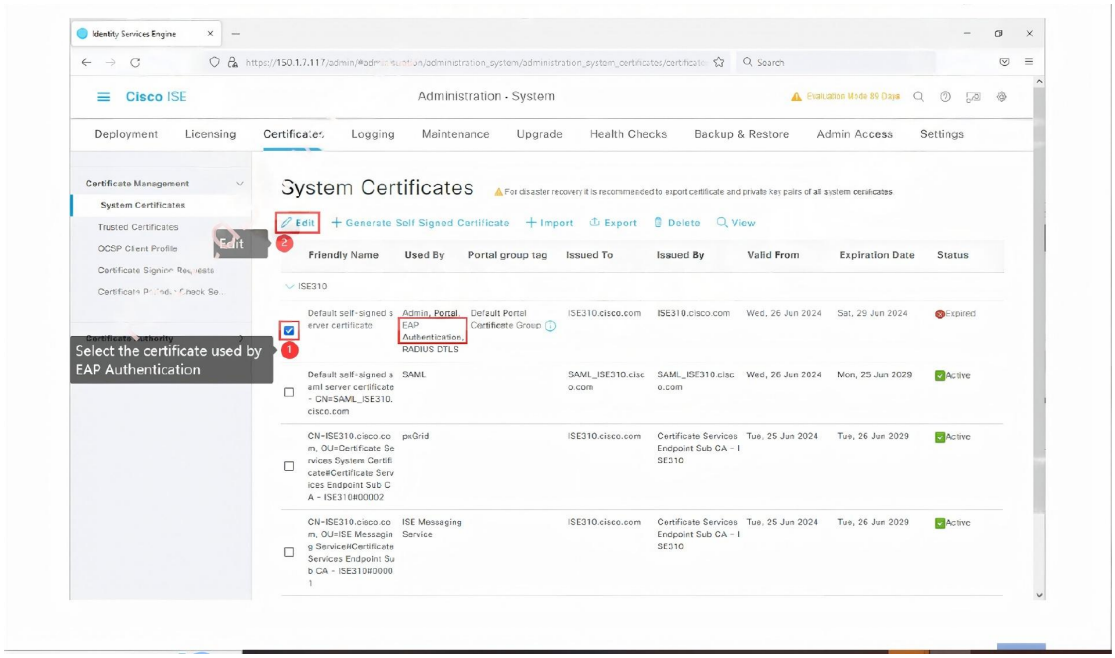
Open https://ise310.cisco.com (ISE) web page

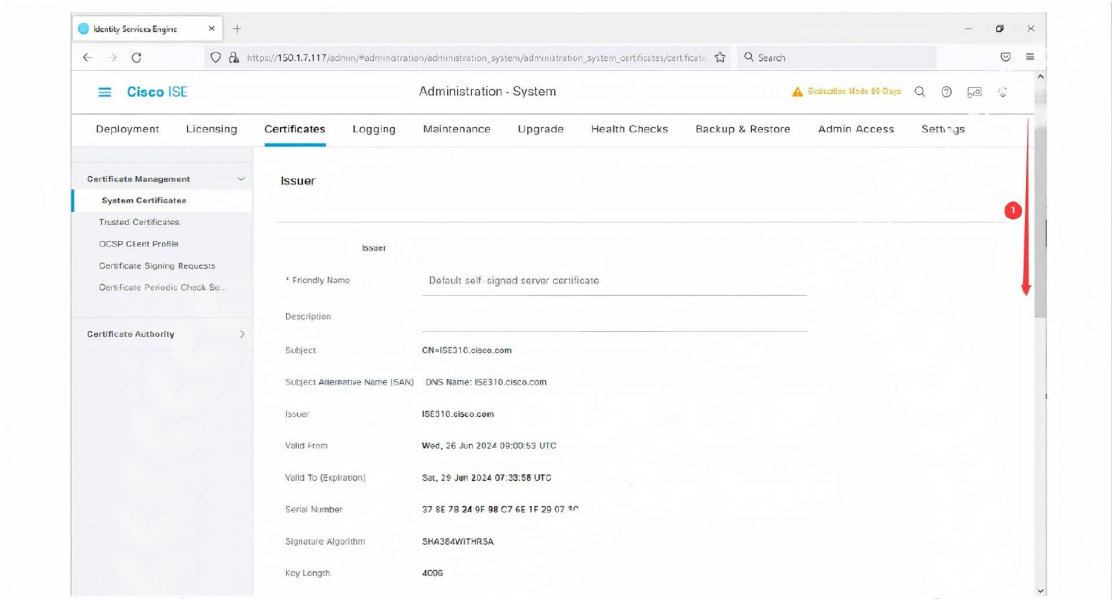


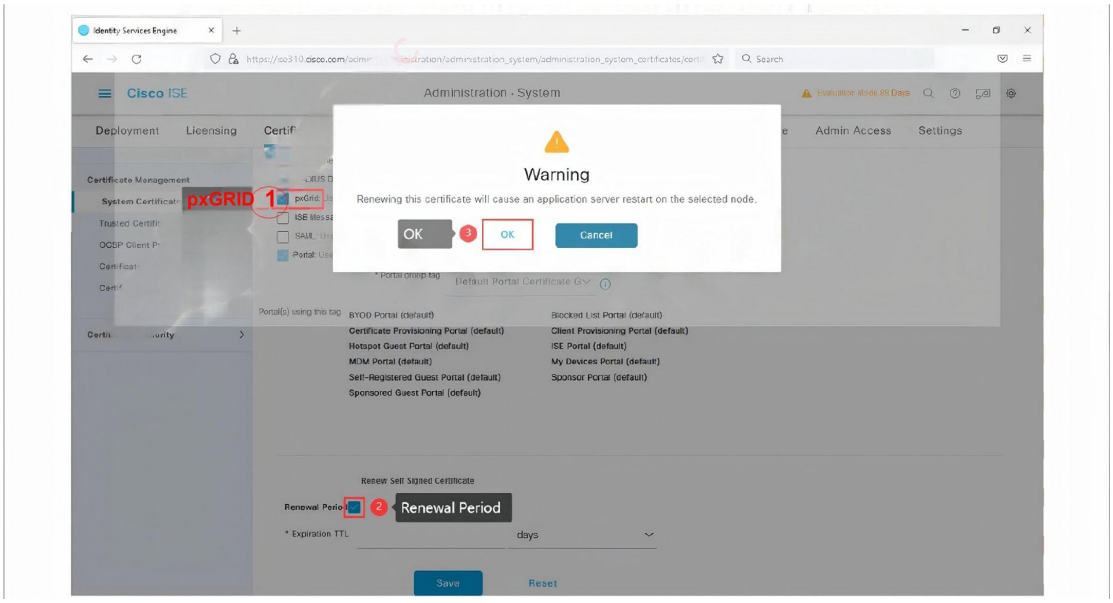


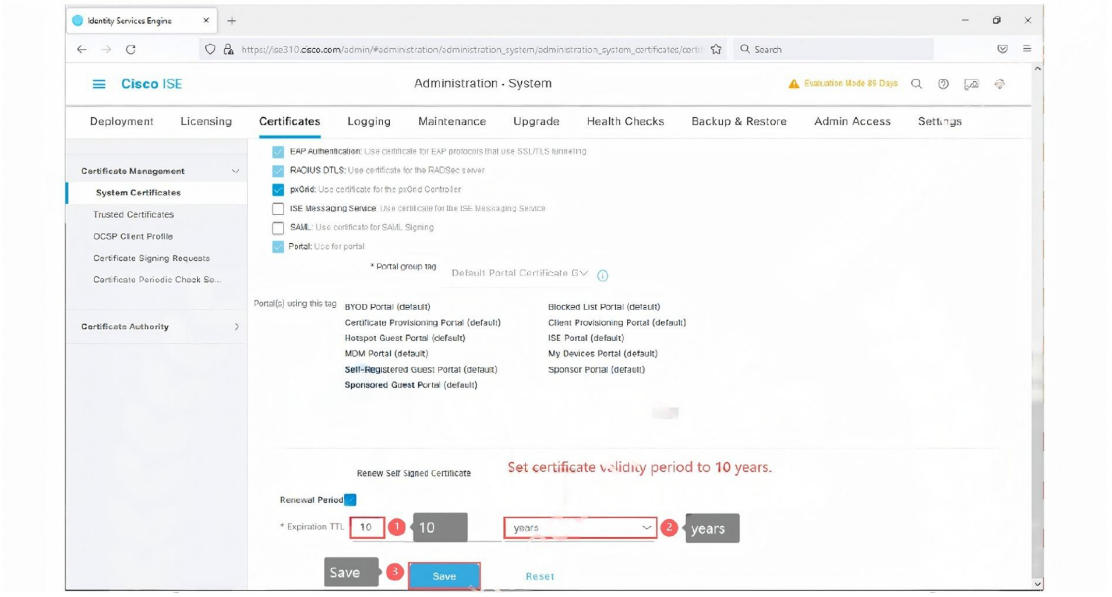


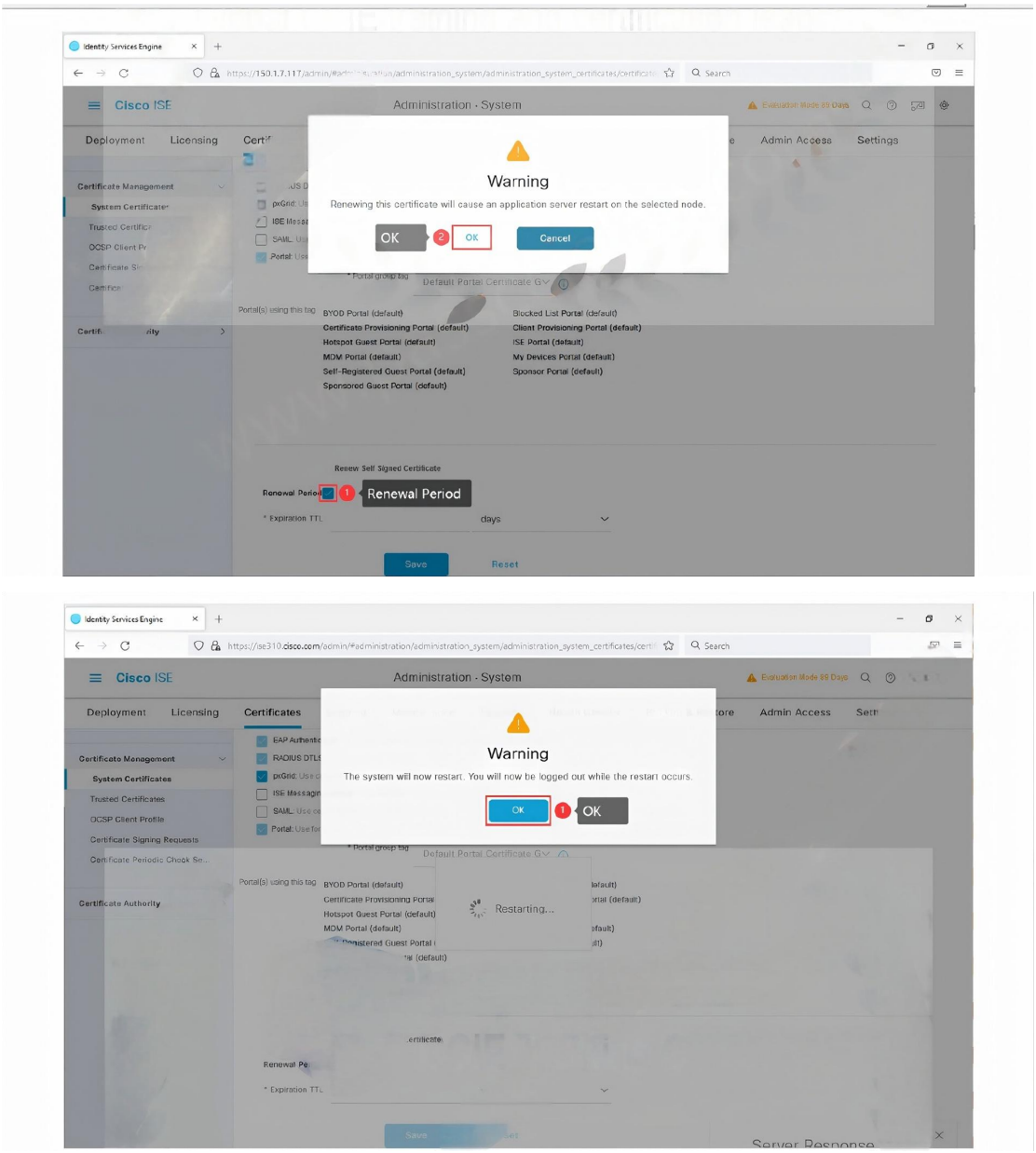

Cisco ISE
Dashboard
Context Visibility
Administration
Recent Pages
Policy Sets
Authorization Profiles
Results
Identities
Network Devices
System
Deployment
Licensing
Certificates
Logging
Maintenance
Network Resources
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
pxGrid Services
Summary
Diagnostics
Settings
Certificates


Cisco ISE
Administration - System
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Health Checks
Backup & Restore
Admin Access
Settings
Certificate Management
System Certificates
Trusted Certificates
OCSP Client Profile
System Certificates
For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.
Edit
Generate Self Signed Certificate
Import
Export
Delete
View
Friendly Name
Used By
Portal group tag
Issued To
Issued By
Valid From
Expiration Date
Status
ISE310
Default self-signed server certificate
Admin, Portal, EAP Authentication, RADIUS DTLS
Default Portal Certificate Group
ISE310.cisco.com
Wed, 26 Jun 2024
Sat, 29 Jun 2024
Expired
Default self-signed saml server certificate - CN=SAML_ISE310.cisco.com
SAML
SAML_ISE310.cisco.com
Mon, 25 Jun 2029
Active
CN=ISE310.cisco.com, OU=Certificate Services System Certificate#Certificate Services Endpoint Sub CA - ISE310#00002
pxGrid
Certificate Services Endpoint Sub CA - ISE310
Tue, 25 Jun 2024
Tue, 26 Jun 2029
CN=ISE310.cisco.com, OU=ISE Messaging Service#Certificate Services Endpoint Sub CA - ISE310#00001
ISE Messaging Service
Select the certificate used by EAP Authentication


Cisco ISE
Administration - System
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Health Checks
Backup & Restore
Admin Access
Certificate Management
System Certificates
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Se...
Certificate Authority
Issuer
Issuer
* Friendly Name
Default self-signed server certificate
Description
Subject
CN=ISE310.cisco.com
Subject Alternative Name (SAN)
DNS Name: ISE310.cisco.com
Issuer
ISE310.cisco.com
Valid From
Wed, 26 Jun 2024 09:00:53 UTC
Valid To (Expiration)
Sat, 29 Jun 2024 07:33:58 UTC
Serial Number
Signature Algorithm
SHA384WITHRSA
Key Length
4096

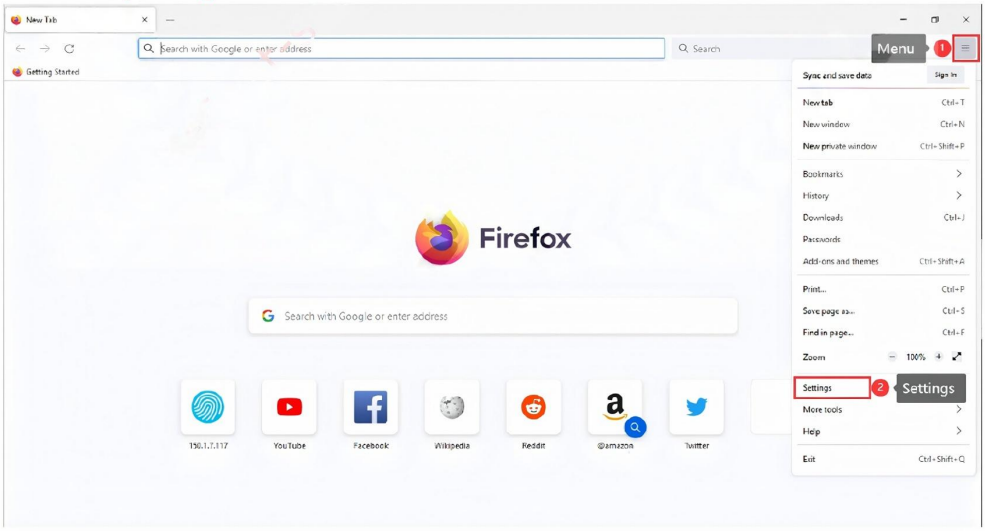

Identity Services Engine
Cisco ISE
Administration · System
Deployment
Licensing
Admin Access
Settings
Warning
Renewing this certificate will cause an application server restart on the selected node.
OK
Cancel
pxGRID
1
2
Renewal Period
3
Renew Self Signed Certificate
* Expiration TTL
days
Save
Reset

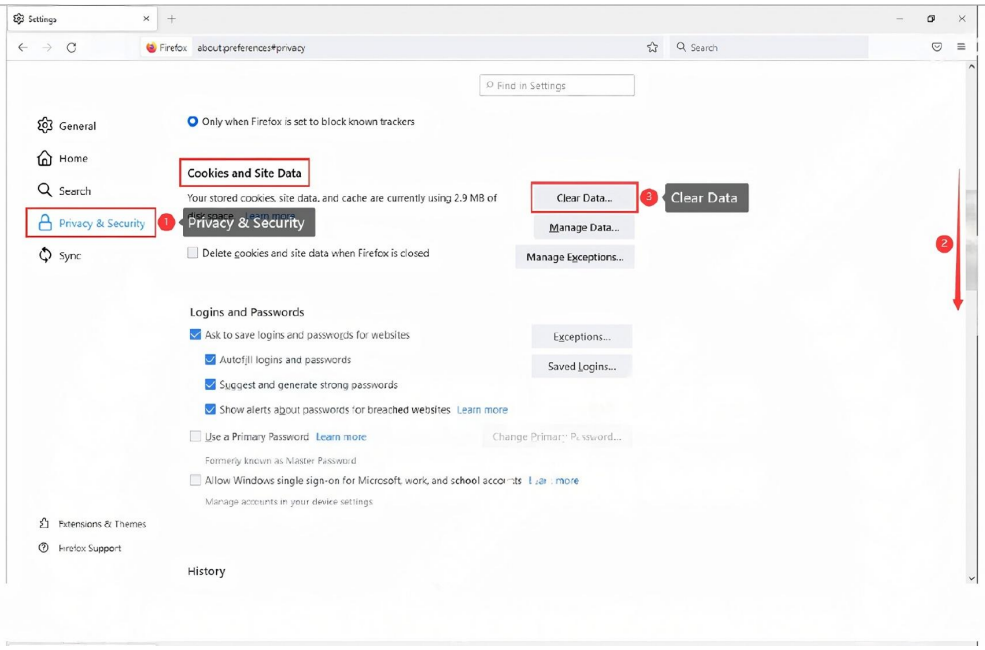

Identity Services Engine
Cisco ISE
Administration · System
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Health Checks
Backup & Restore
Admin Access
Settings
Certificate Management
System Certificates
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Periodic Check Se...
Certificate Authority
Renew Self Signed Certificate
Set certificate validity period to 10 years.
Renewal Period
* Expiration TTL
10
1
10
years
2
years
Save
3
Save
Reset

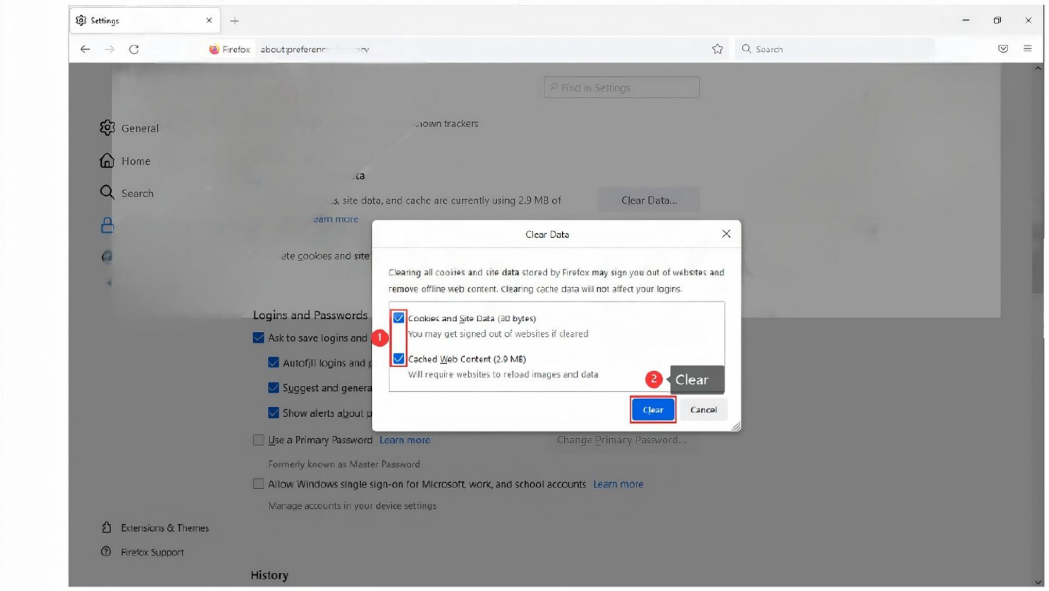

Identity Services Engine
Cisco ISE
Administration · System
Deployment
Licensing
Admin Access
Settings
Warning
Renewing this certificate will cause an application server restart on the selected node.
OK
Cancel
Renew Self Signed Certificate
Renewal Period
Expiration TTL
days
Save
Reset

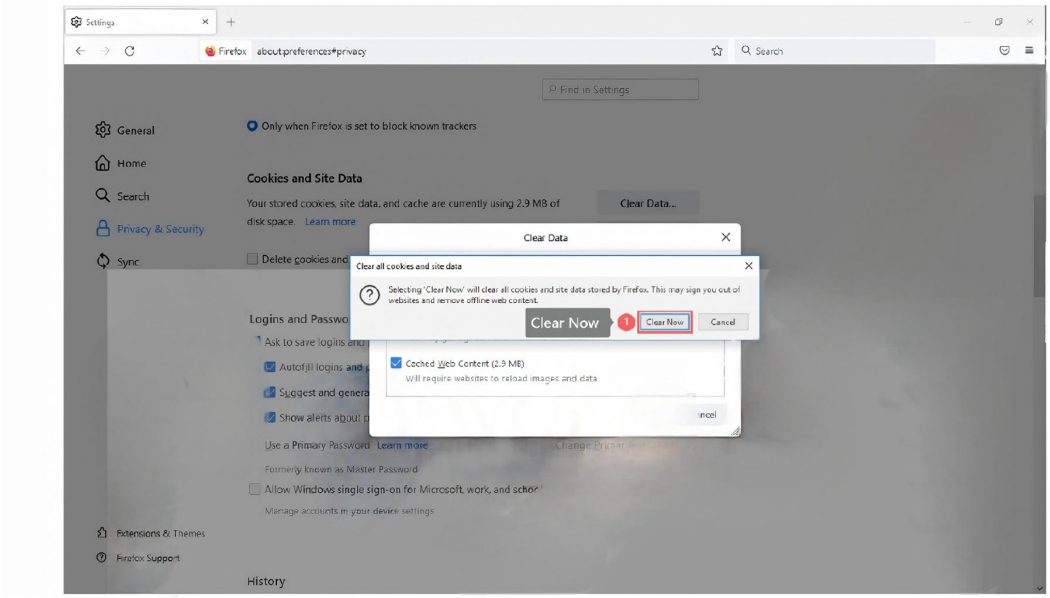
Identity Services Engine
Cisco ISE
Administration · System
Deployment
Licensing
Certificates
Admin Access
Warning
The system will now restart. You will now be logged out while the restart occurs.
OK
Restarting...
Server Response

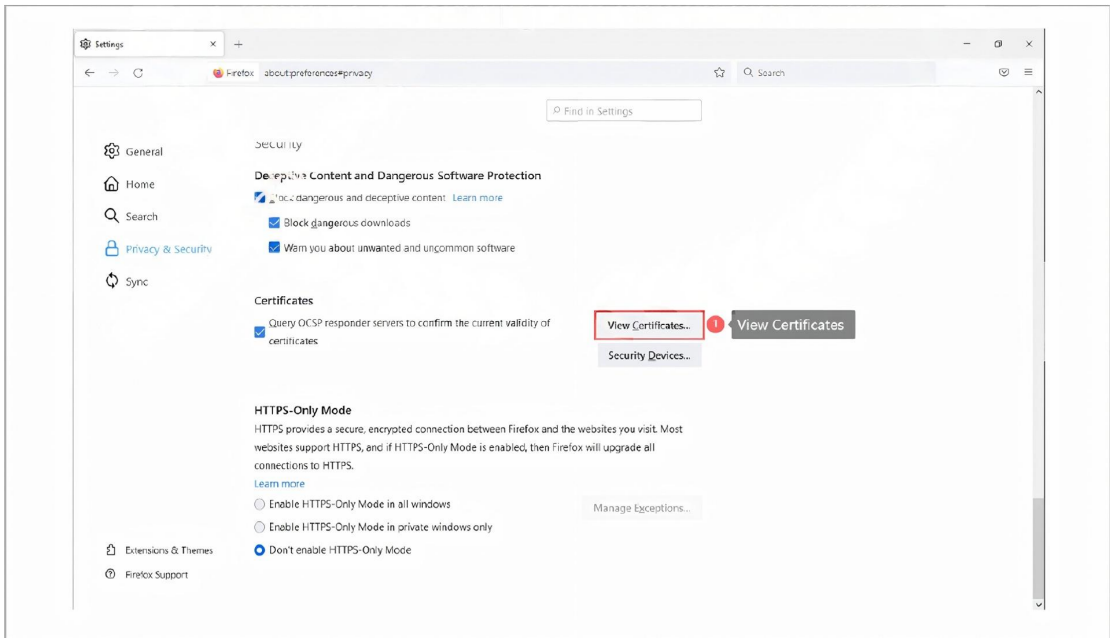
Note: After regenerating the certificate, you need to clear the browser cookies and data, clear the browser certificate, or change a browser.

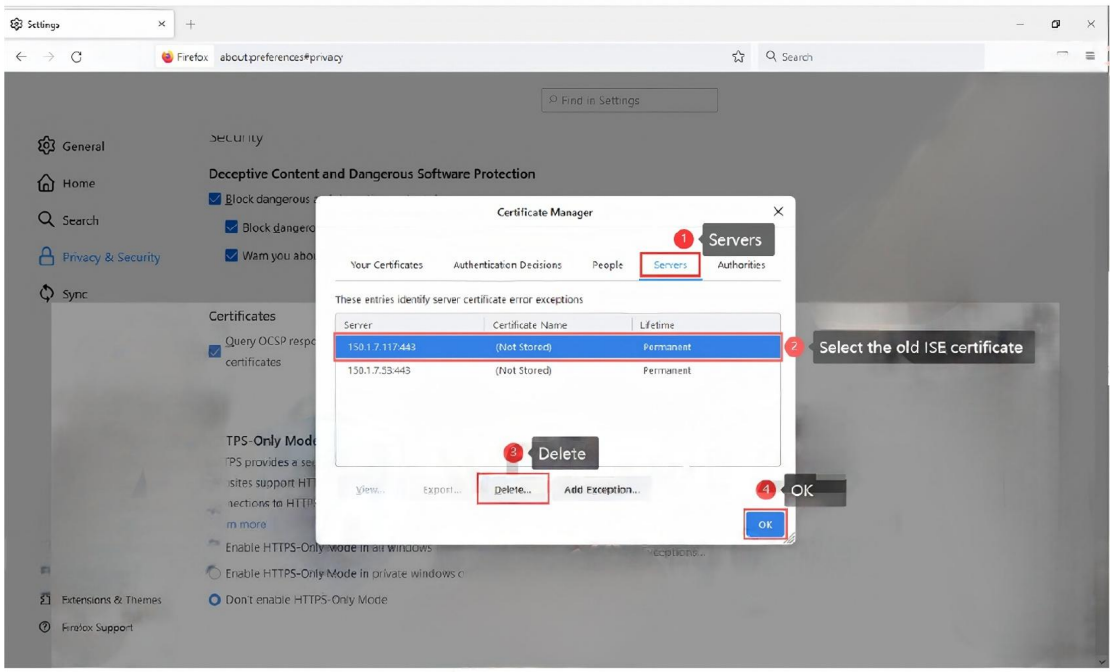


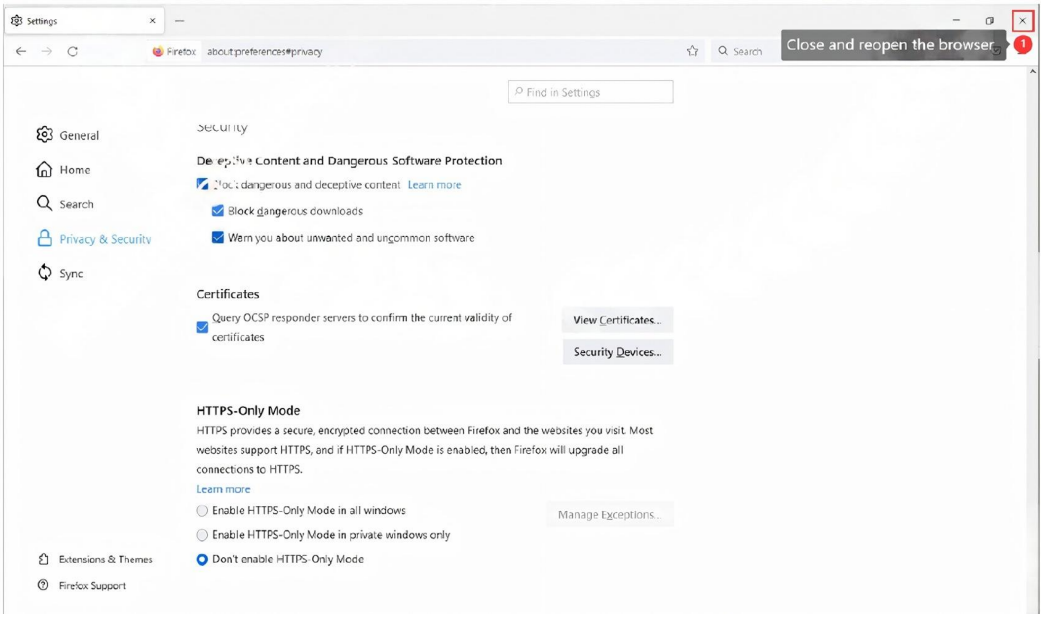


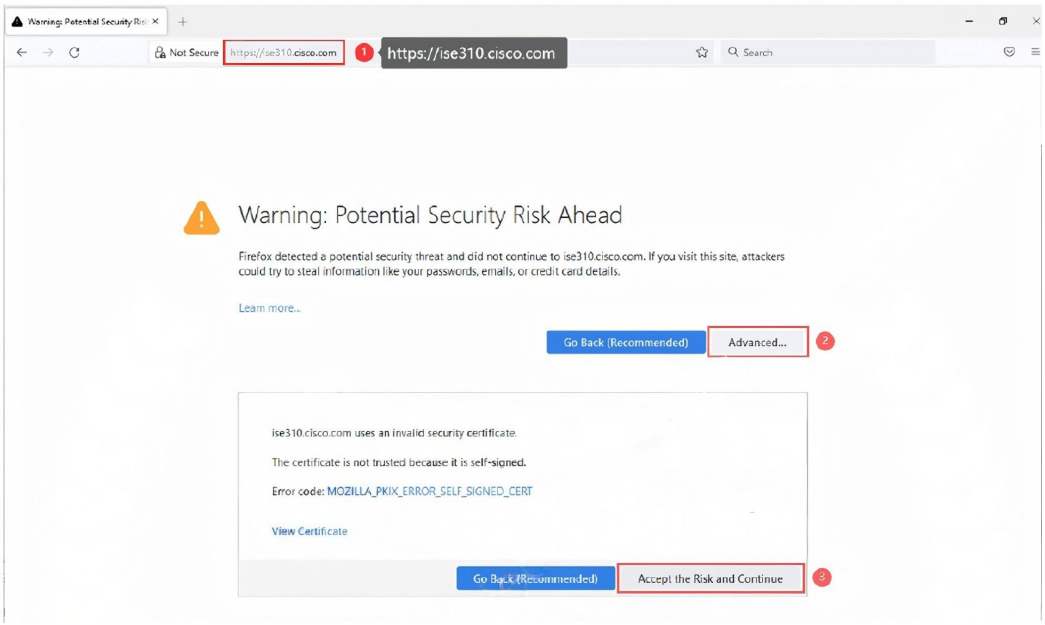

Settings
Find in Settings
General
Home
Search
Privacy & Security
Sync
Clear Data...
Clear Data
Cookies and Site Data (30 bytes)
You may get signed out of websites if cleared
Cached Web Content (2.9 MB)
Will require websites to reload images and data
Clear
Cancel
Logins and Passwords
Use a Primary Password Learn more
Change Primary Password...
Allow Windows single sign-on for Microsoft, work, and school accounts Learn more
Extensions & Themes
Firefox Support
History

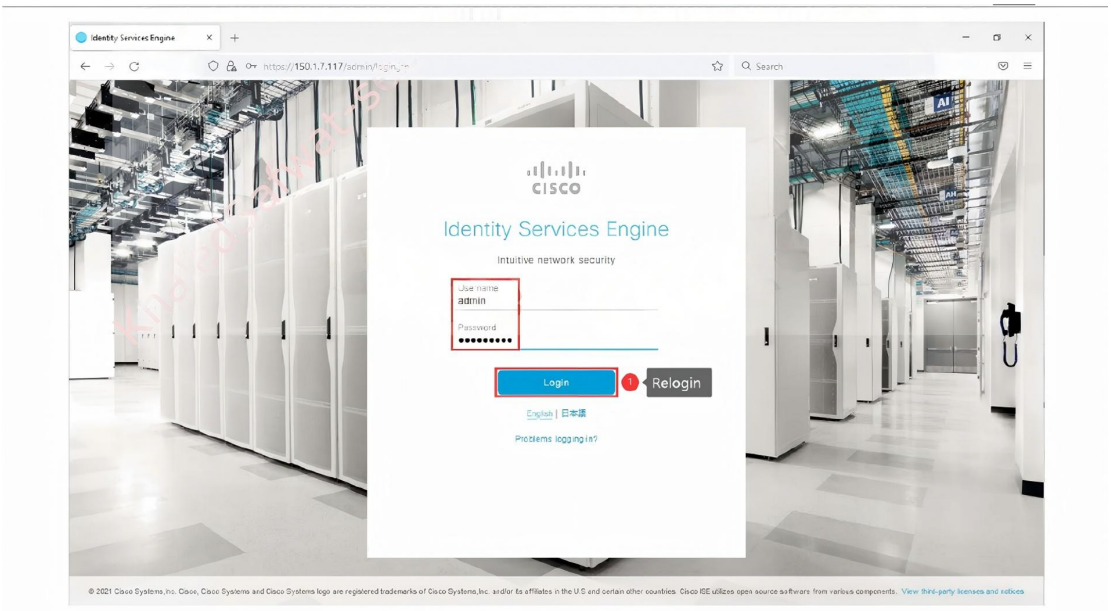

Settings
Find in Settings
General
Home
Search
Privacy & Security
Sync
Only when Firefox is set to block known trackers
Cookies and Site Data
Your stored cookies, site data, and cache are currently using 2.9 MB of disk space. Learn more
Clear Data...
Clear Data
Clear all cookies and site data
Selecting 'Clear Now' will clear all cookies and site data stored by Firefox. This may sign you out of websites and remove offline web content.
Clear Now
Cancel
Cached Web Content (2.9 MB)
Will require websites to reload images and data
Use a Primary Password Learn more
Extensions & Themes
Firefox Support
History

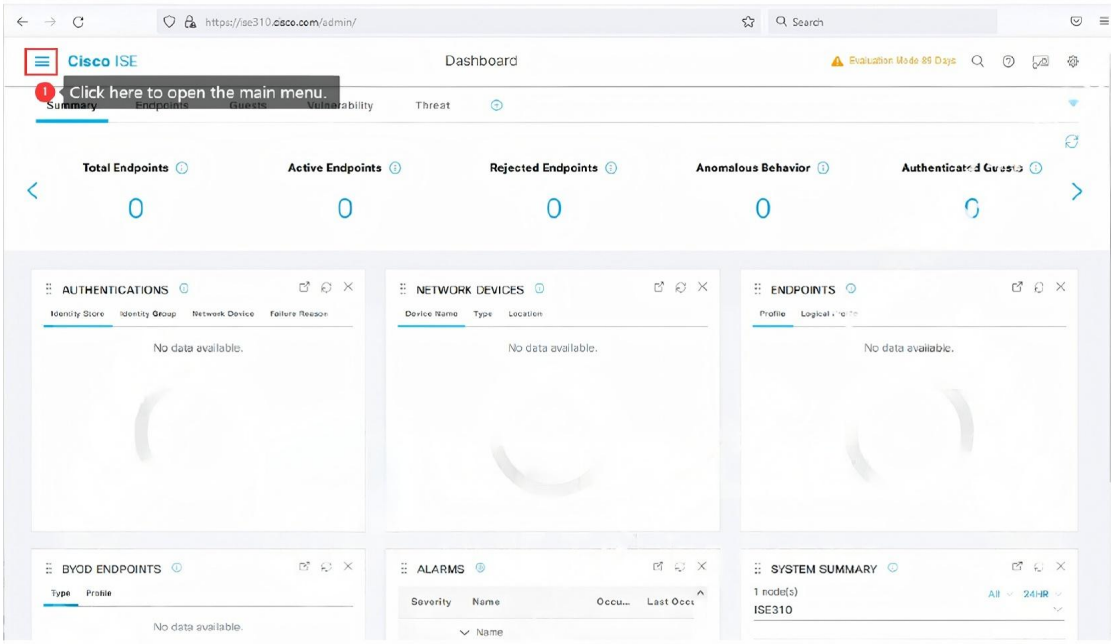

Settings
Firefox about:preferences#privacy
Search
Find in Settings
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Firefox Support
Deceptive Content and Dangerous Software Protection
Block dangerous and deceptive content Learn more
Block dangerous downloads
Warn you about unwanted and uncommon software
Certificates
Query OCSP responder servers to confirm the current validity of certificates
View Certificates...
1
View Certificates
Security Devices...
HTTPS-Only Mode
HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.
Learn more
Enable HTTPS-Only Mode in all windows
Enable HTTPS-Only Mode in private windows only
Don't enable HTTPS-Only Mode
Manage Exceptions...

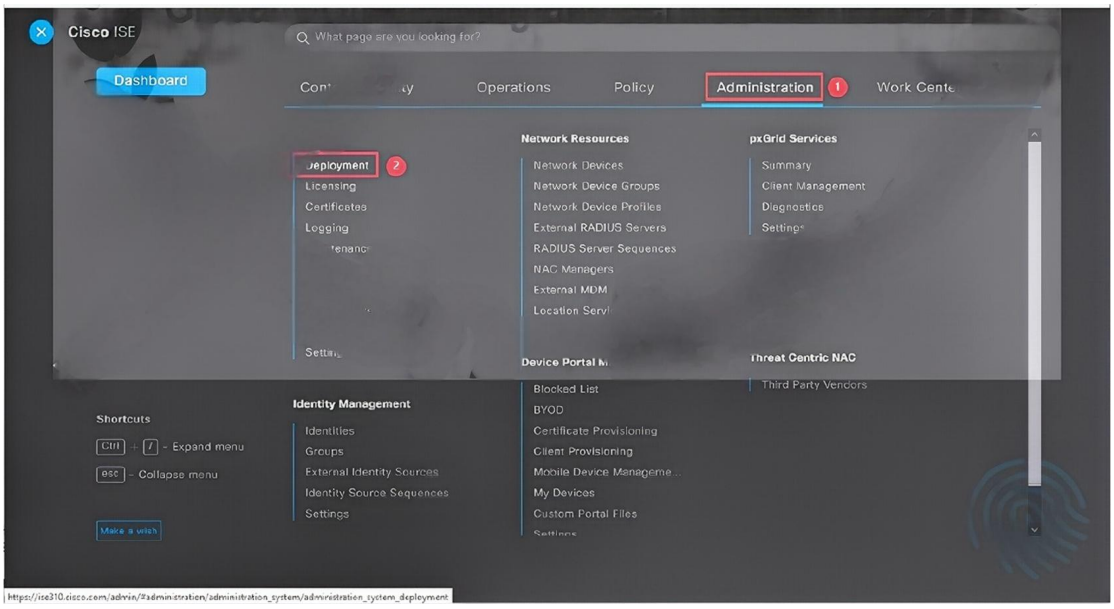

Certificate Manager
1
Servers
Your Certificates
Authentication Decisions
People
Servers
Authorities
These entries identify server certificate error exceptions
Server
Certificate Name
Lifetime
150.1.7.117:443
(Not Stored)
Permanent
2
Select the old ISE certificate
150.1.7.53:443
(Not Stored)
Permanent
3
Delete
View...
Export...
Delete...
Add Exception...
4
OK
OK

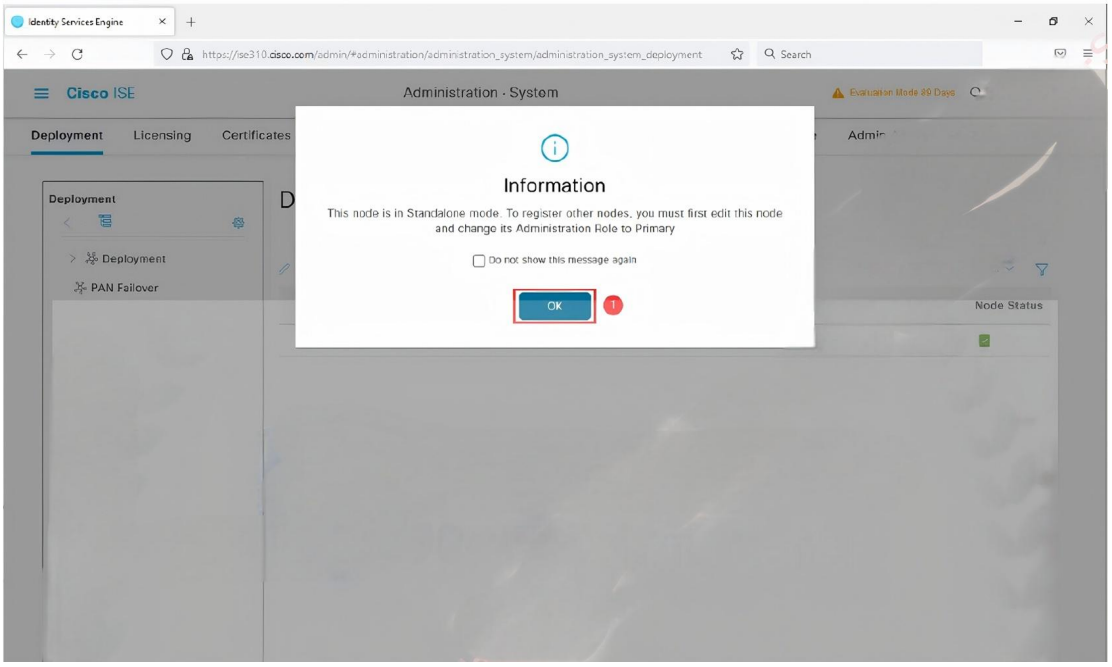

Settings
Firefox about:preferences#privacy
Search
Close and reopen the browser
1
Find in Settings
General
Home
Search
Privacy & Security
Sync
Extensions & Themes
Firefox Support
Content and Dangerous Software Protection
Block dangerous downloads
Warn you about unwanted and uncommon software
Certificates
Query OCSP responder servers to confirm the current validity of certificates
View Certificates...
Security Devices...
HTTPS-Only Mode
HTTPS provides a secure, encrypted connection between Firefox and the websites you visit. Most websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all connections to HTTPS.
Learn more
Enable HTTPS-Only Mode in all windows
Enable HTTPS-Only Mode in private windows only
Don't enable HTTPS-Only Mode
Manage Exceptions...

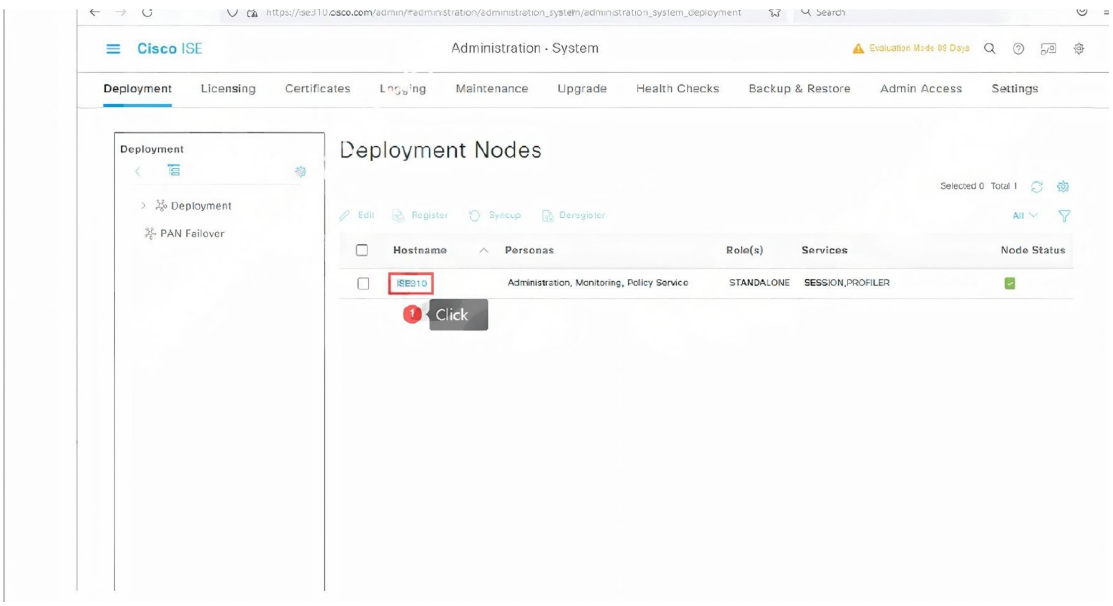

Not Secure
https://ise310.cisco.com
1
https://ise310.cisco.com
Search
Warning: Potential Security Risk Ahead
Firefox detected a potential security threat and did not continue to ise310.cisco.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
Learn more...
Go Back (Recommended)
Advanced...
2
ise310.cisco.com uses an invalid security certificate.
The certificate is not trusted because it is self-signed.
Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
View Certificate
Go Back (Recommended)
Accept the Risk and Continue
3

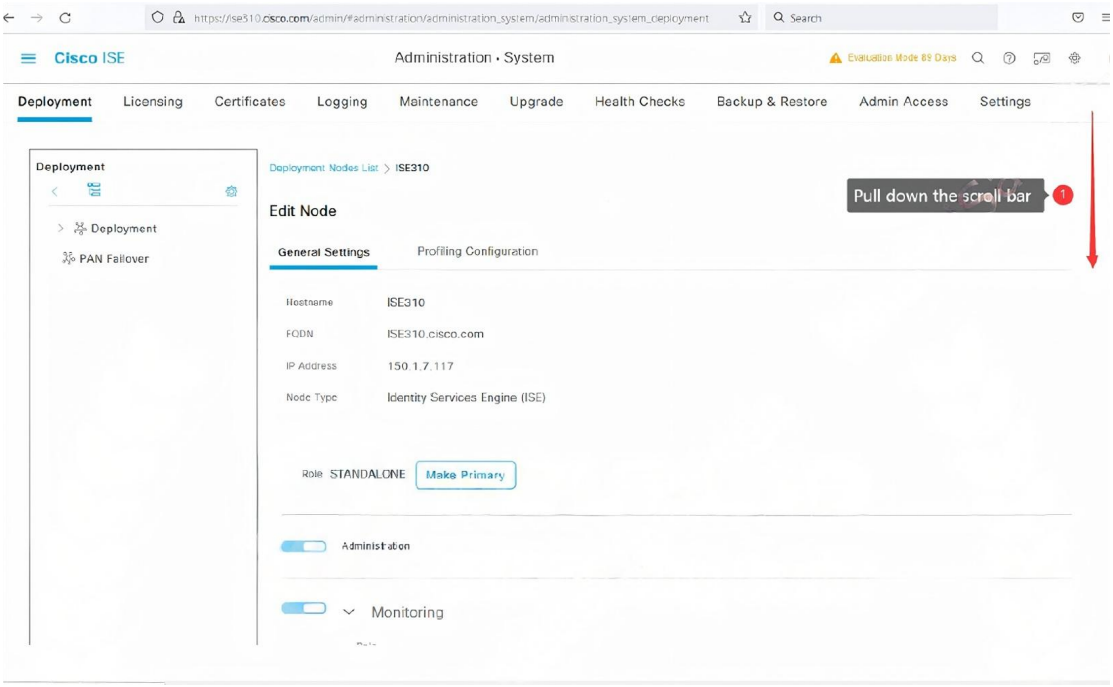

Identity Services Engine
https://150.1.7.117/admin/login.jsp
Search
CISCO
Identity Services Engine
Intuitive network security
admin
Login
Relogin
English | 日本語
Problems logging in?
© 2021 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S and certain other countries. Cisco ISE utilizes open source software from various components. View third-party licenses and notices


https://ise310.cisco.com/admin/
Search
Cisco ISE
Dashboard
Evaluation Mode 85 Days
Click here to open the main menu.
Summary
Endpoints
Guests
Vulnerability
Threat
Total Endpoints
Active Endpoints
Rejected Endpoints
Anomalous Behavior
0
0
0
0
AUTHENTICATIONS
Identity Store
Identity Group
Network Device
Failure Reason
No data available.
NETWORK DEVICES
Device Name
Type
Location
No data available.
ENDPOINTS
Profile
No data available.
BYOD ENDPOINTS
Type
Profile
No data available.
ALARMS
Severity
Name
Name
SYSTEM SUMMARY
1 node(s)
All
24HR
ISE310


Cisco ISE
What page are you looking for?
Dashboard
Operations
Policy
Administration
1
Work Cente
Deployment
2
Licensing
Certificates
Logging
Network Resources
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
External MDM
pxGrid Services
Summary
Client Management
Diagnostics
Threat Centric NAC
Third Party Vendors
Shortcuts
Ctrl + / - Expand menu
esc - Collapse menu
Identity Management
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
Blocked List
BYOD
Certificate Provisioning
Client Provisioning
My Devices
Custom Portal Files


Identity Services Engine
Cisco ISE
Administration - System
Deployment
Licensing
Certificates
Deployment
Deployment
PAN Failover
Information
This node is in Standalone mode. To register other nodes, you must first edit this node and change its Administration Role to Primary
Do not show this message again
OK
1
Node Status


Cisco ISE
Administration · System
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Health Checks
Backup & Restore
Admin Access
Settings
Deployment
Deployment
PAN Failover
Deployment Nodes
Hostname
Personas
Role(s)
Services
Node Status
ISE310
Administration, Monitoring, Policy Service
STANDALONE
SESSION,PROFILER
Click


Cisco ISE
Administration · System
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Health Checks
Backup & Restore
Admin Access
Settings
Deployment
Deployment
PAN Failover
Deployment Nodes List > ISE310
Edit Node
Pull down the scroll bar
General Settings
Profiling Configuration
Hostname
ISE310
FQDN
ISE310.cisco.com
IP Address
150.1.7.117
Node Type
Identity Services Engine (ISE)
Role STANDALONE
Make Primary
Administration
Monitoring