

ASDM sur ASA 5520

Cisco Adaptive Security Device Manager

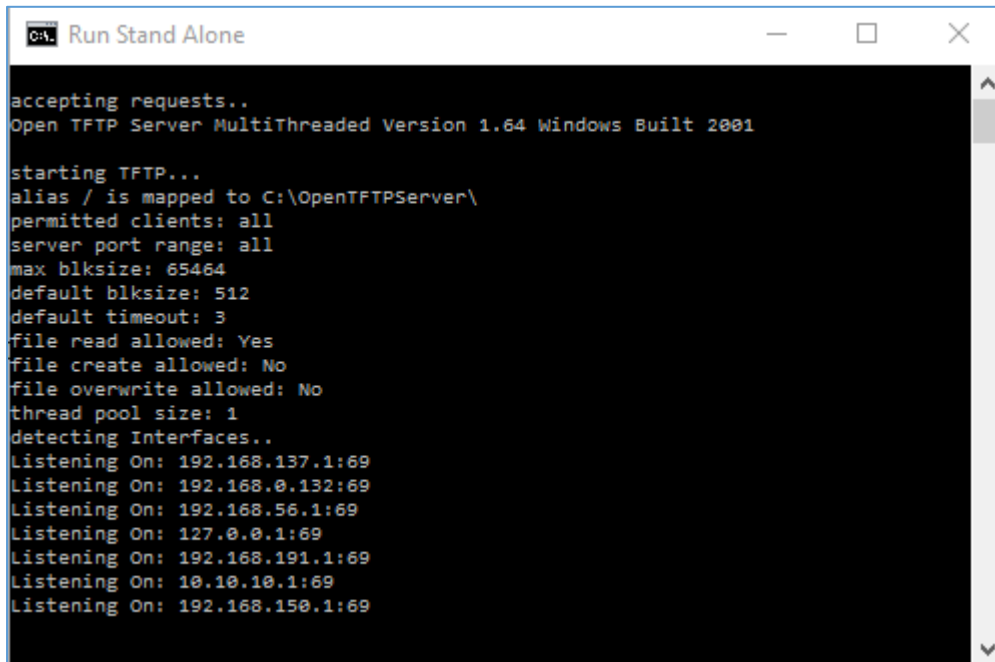
Table des matières

1	Installer ASDM	2
1.1	Transférer ASDM par TFTP	2
1.2	Configurer HTTPS sur le routeur	5
1.3	Installer ASDM Launcher.....	7
1.4	Accéder à ASDM.....	10
2	Dépannage	13

1 Installer ASDM

1.1 Transférer ASDM par TFTP

- 1) Installer et démarrer le serveur TFTP sur votre machine physique :

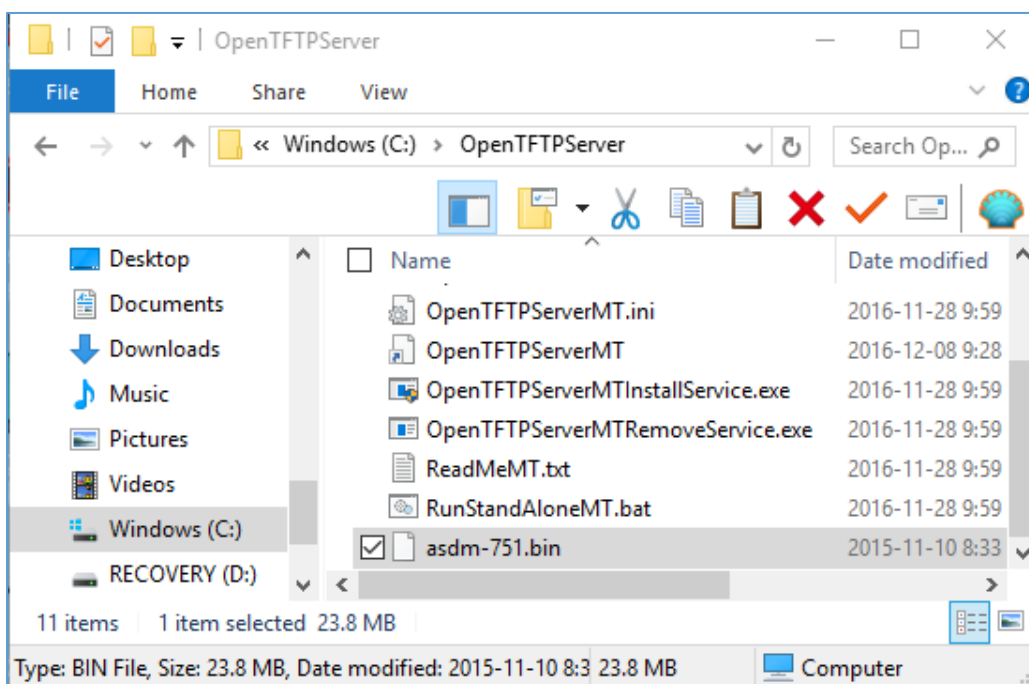


```
Run Stand Alone

accepting requests..
Open TFTP Server MultiThreaded Version 1.64 Windows Built 2001

starting TFTP...
alias / is mapped to C:\OpenTFTPServer\
permitted clients: all
server port range: all
max blksize: 65464
default blksize: 512
default timeout: 3
file read allowed: Yes
file create allowed: No
file overwrite allowed: No
thread pool size: 1
detecting Interfaces..
Listening On: 192.168.137.1:69
Listening On: 192.168.0.132:69
Listening On: 192.168.56.1:69
Listening On: 127.0.0.1:69
Listening On: 192.168.191.1:69
Listening On: 10.10.10.1:69
Listening On: 192.168.150.1:69
```

- 2) Placer le fichier *asdm-751.bin* dans le répertoire TFTP:



3) Tester la connectivité entre la machine physique et l'interface du routeur:

```
C:\Users\admin>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=3ms TTL=255
Reply from 10.10.10.10: bytes=32 time=4ms TTL=255
Reply from 10.10.10.10: bytes=32 time=7ms TTL=255
Reply from 10.10.10.10: bytes=32 time=7ms TTL=255

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 7ms, Average = 5ms

C:\Users\admin>
```

4) Transférer le fichier *asdm-751.bin* de la machine physique vers le routeur:

```
ciscoasa# copy tftp: flash:

Address or name of remote host [10.10.10.1]?

Source filename [asdm-751.bin]?

Destination filename [asdm-751.bin]?

Accessing tftp://10.10.10.1/asdm-751.bin...!!!!!!!!!!!!!!!!!!!!!!
Writing current ASDM file disk0:/asdm-751.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
25025292 bytes copied in 53.200 secs (472175 bytes/sec)
ciscoasa#
```

5) Vérifier le transfert:

```
ciscoasa# dir

Directory of disk0:/

10      drwx  16384          14:12:38 Dec 12 2016  log
19      drwx  16384          14:12:56 Dec 12 2016  coredumpinfo
74      -rwx  25025292       05:01:36 Dec 13 2016  asdm-751.bin

1073446912 bytes total (1047281664 bytes free)
```

6) Vérifier la version:

```
ciscoasa# show version
```

```
Cisco Adaptive Security Appliance Software Version 9.1(5)21  
Device Manager Version 7.5(1)
```

1.2 Configurer HTTPS sur le routeur

- 1) Configurer le serveur HTTPS et autorisé l'accès:

```
ciscoasa# conf t
ciscoasa(config)# http server enable
ciscoasa(config)# http 10.10.10.0 255.255.255.0 outside
```

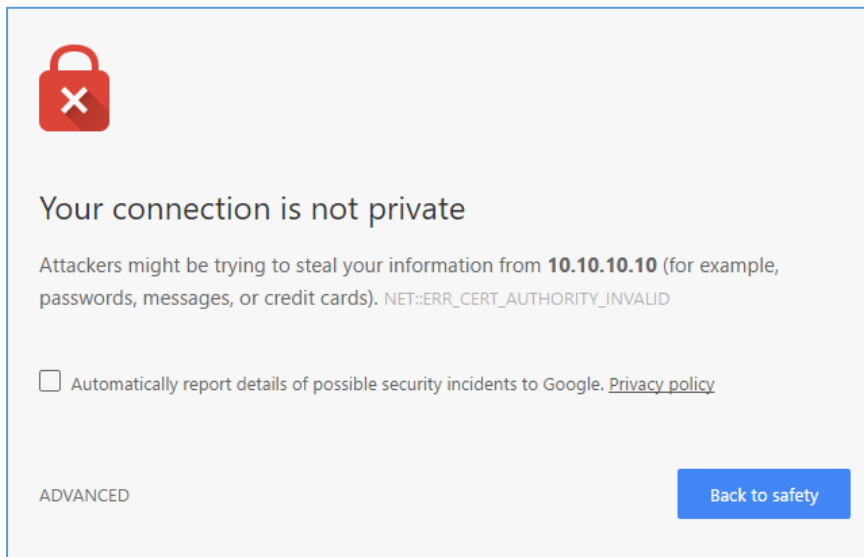
- 2) Sauvegarder la configuration:

```
ciscoasa(config)# wr
Building configuration...
Cryptochecksum: 784c9267 073285f6 46508ea2 44abb825

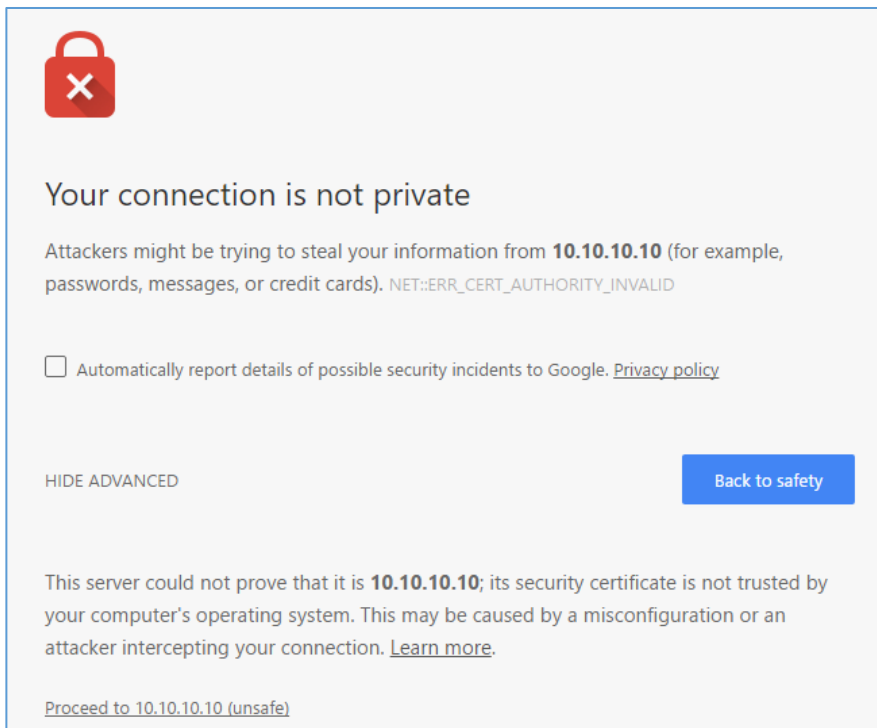
2940 bytes copied in 0.700 secs
[OK]
```

- 3) Accéder via HTTPS au routeur:

<https://10.10.10.10>

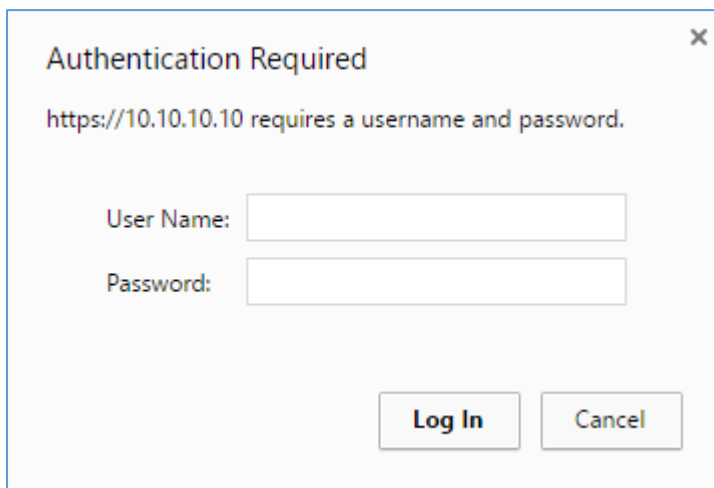


Cliquer sur *ADVANCED*



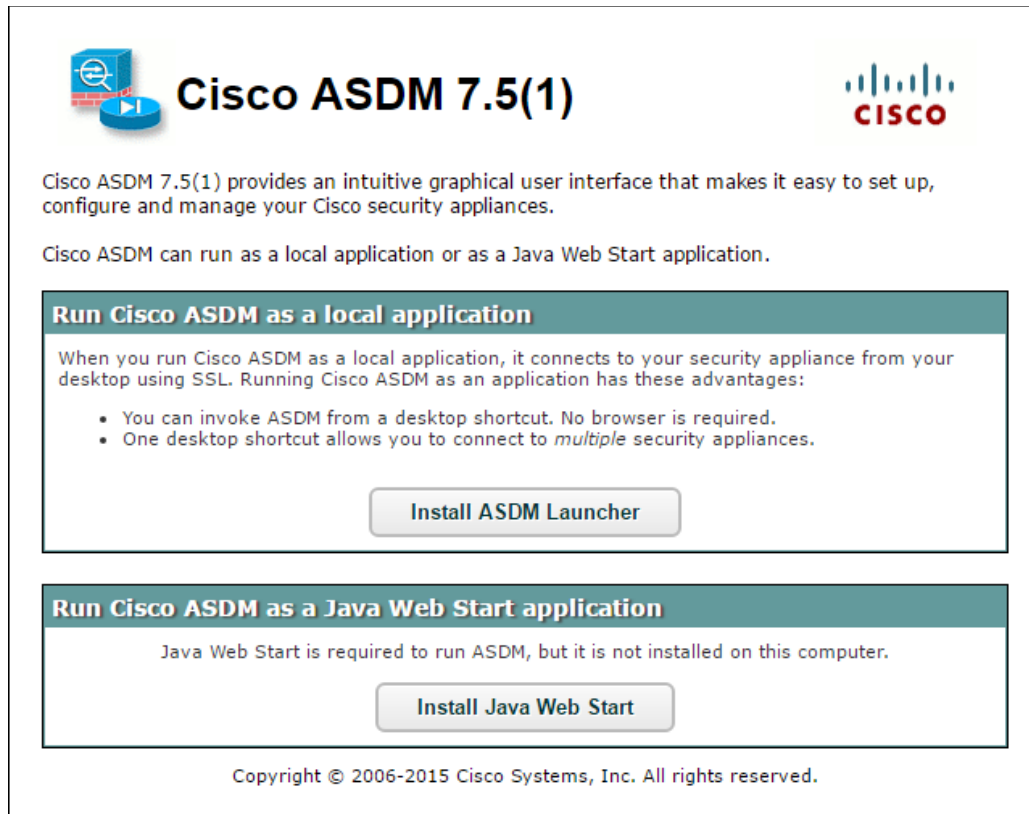
Cliquer sur *Proceed to 10.10.10 (unsafe)*

- 4) Cliquer sur Log In pour se connecter sans s'authentifier :

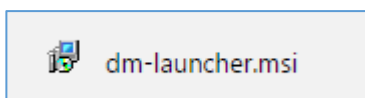


1.3 Installer ASDM Launcher

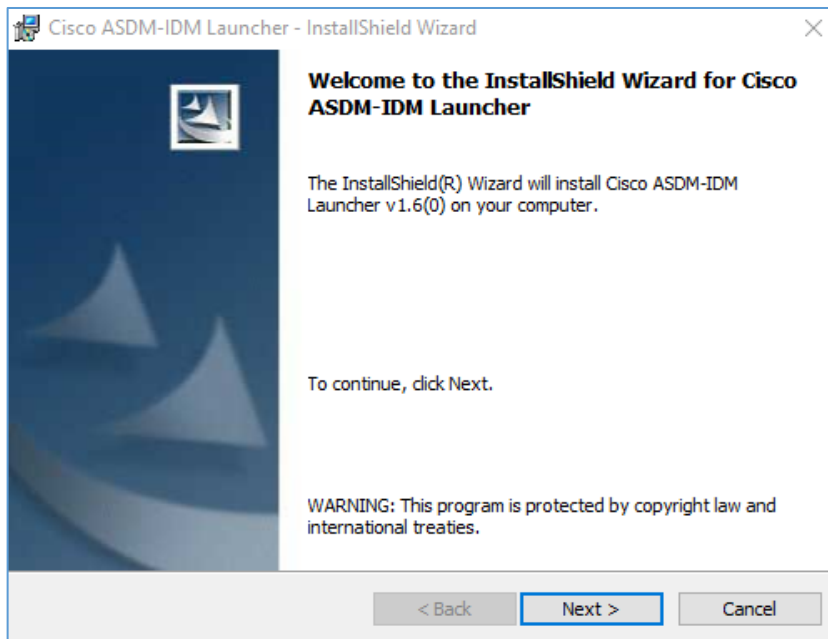
- 1) Cliquer sur *Install ASDM Launcher* pour lancer le téléchargement:



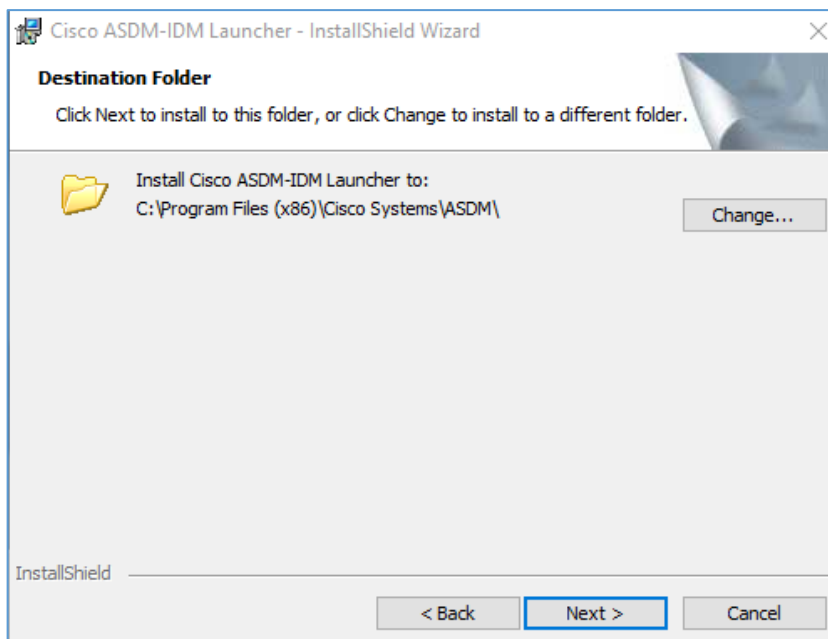
- 2) Lancer l'installation du .msi :



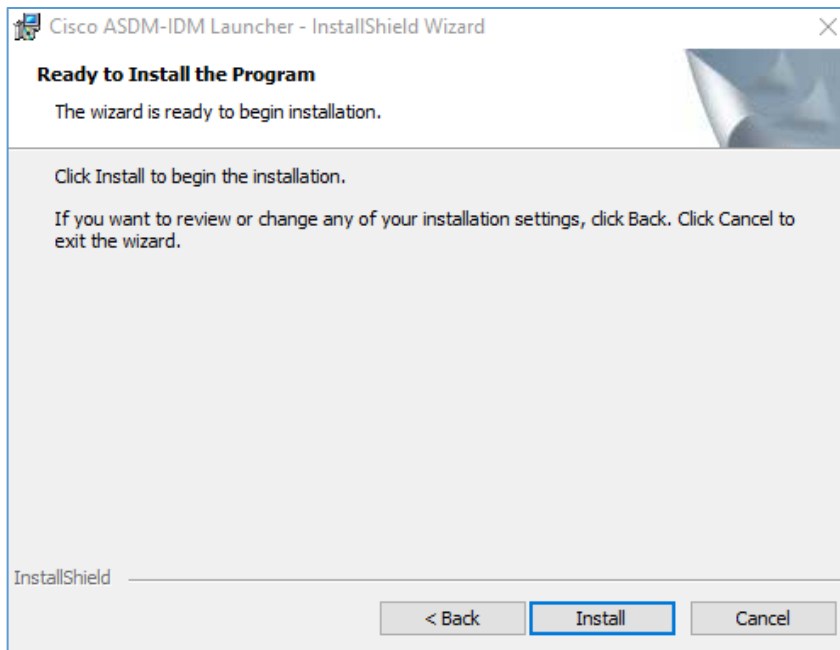
3) Cliquer sur *Next* pour Continuer :



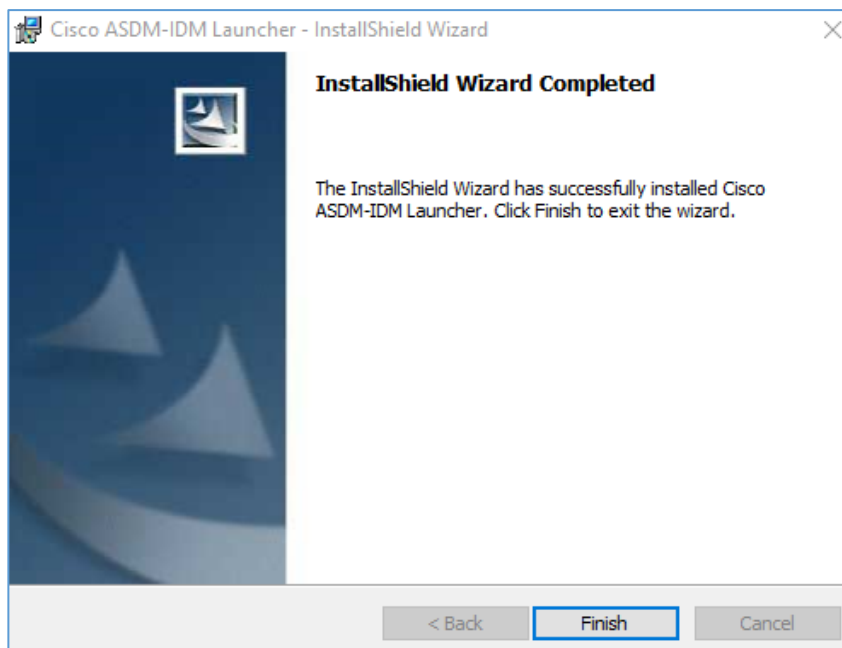
4) Cliquer sur *Next* pour Continuer :



5) Cliquer sur *Install* pour Continuer :

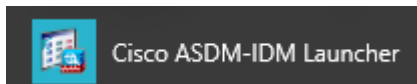


6) Cliquer sur *Finish*

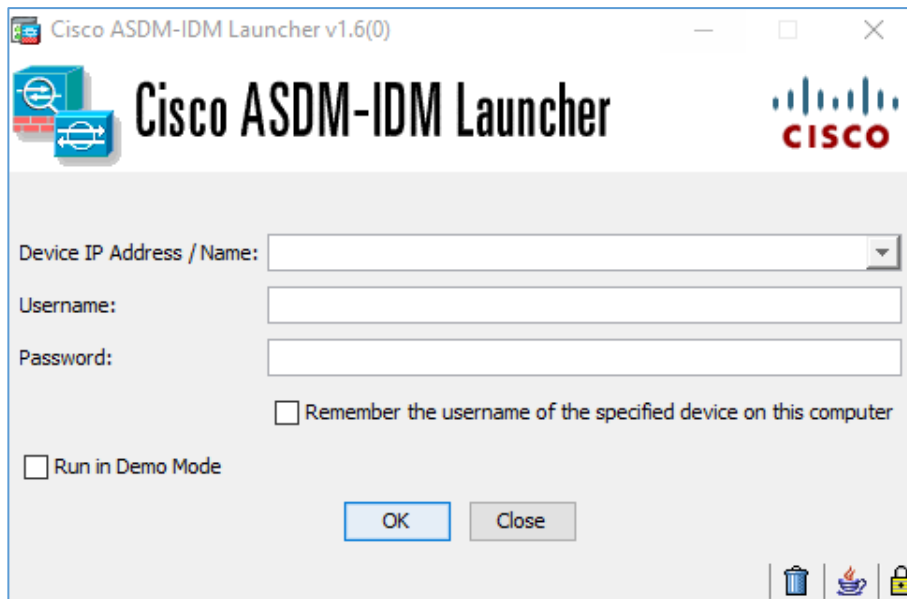


1.4 Accéder à ASDM

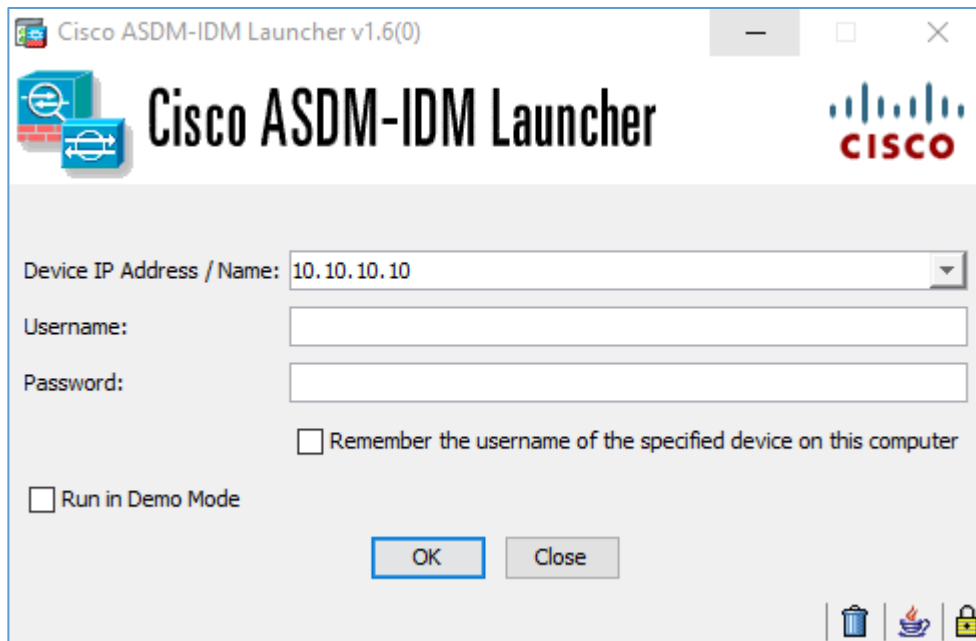
- 1) Lancer Cisco ASDM-IDM Launcher



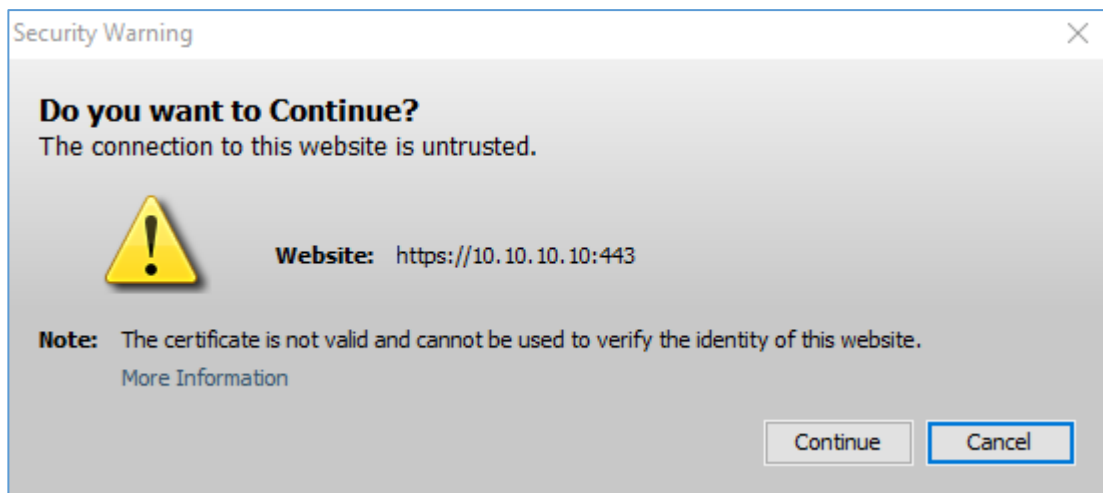
- 2) La fenêtre de login s'affiche



3) La fenêtre de login s'affiche

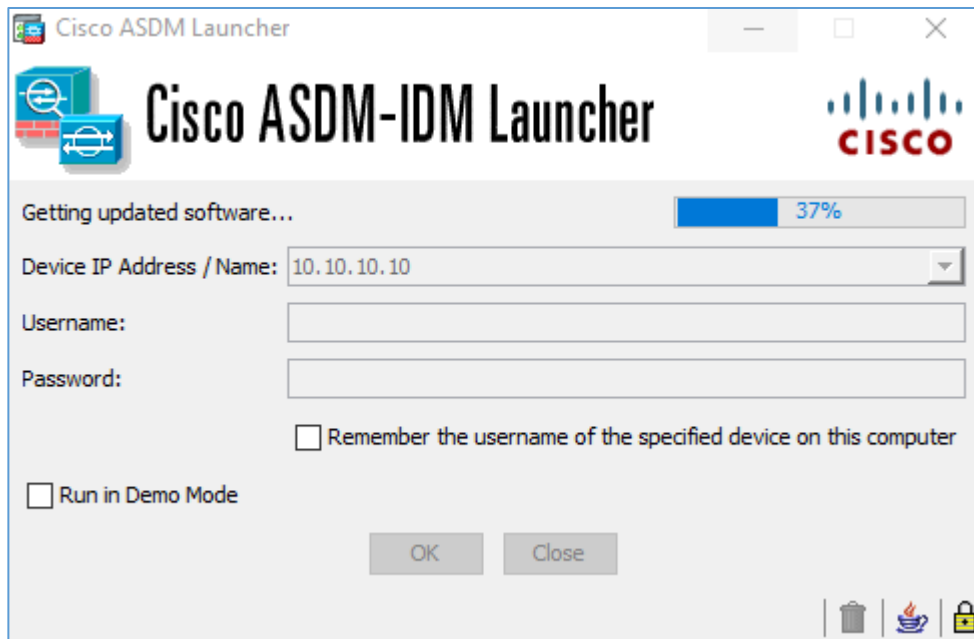


4) Accepter le warning de sécurité

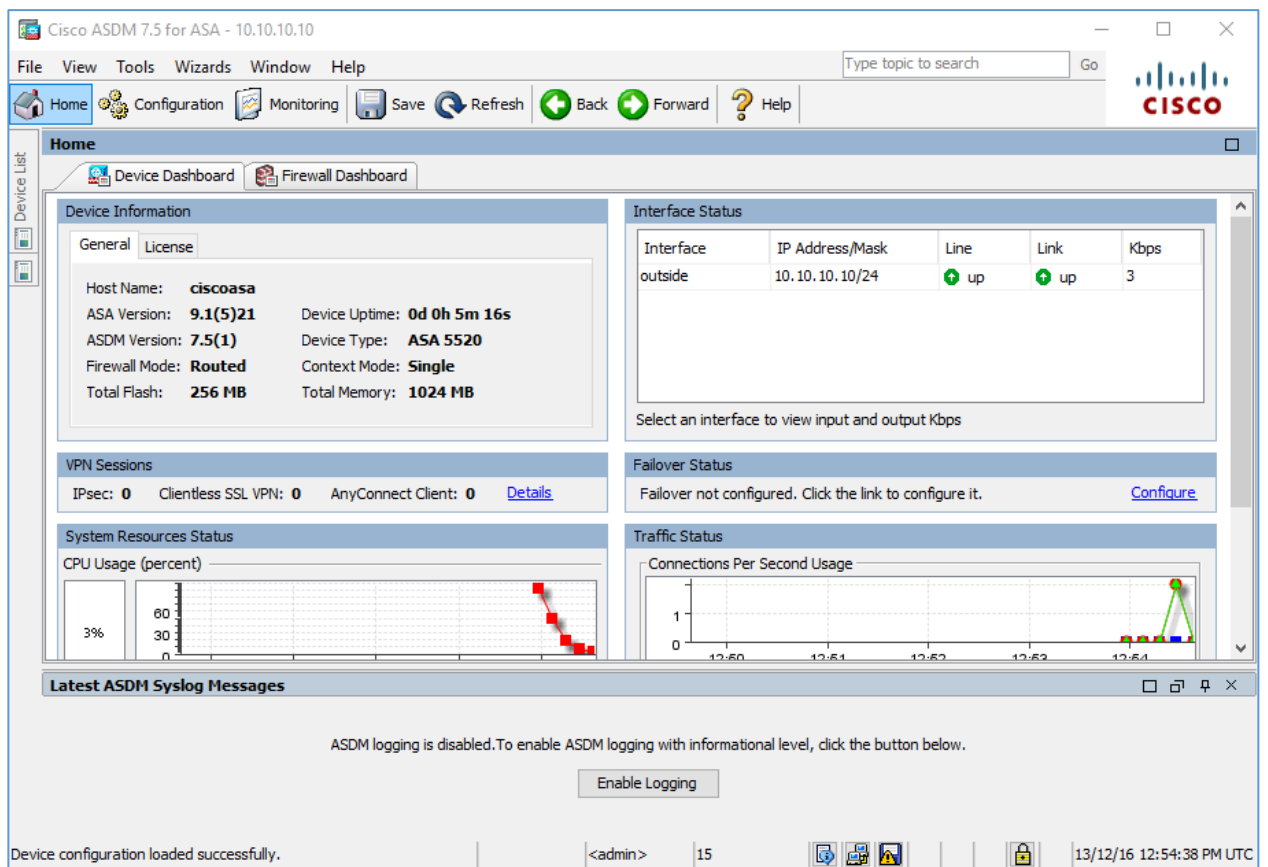


En cas d'erreur, voir section dépannage.

5) La barre de progression s'affiche



6) La console ASDM s'affiche



2 Dépannage

En cas de problème, activer le logging et analyser les messages d'erreur.

```
ciscoasa(config)# logging enable  
  
ciscoasa(config)# logging console 6  
ciscoasa(config)# %ASA-5-111008: User 'enable_15' executed the  
'logging console 6' command.  
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0,  
executed 'logging console 6'
```

```
ciscoasa(config)# no logging enable  
ciscoasa(config)# %ASA-5-111008: User 'enable_15' executed the  
'no logging enable' command.  
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0,  
executed 'no logging enable'
```

Souvent, il faut ajouter plusieurs méthodes d'encryptions pour la session réussie.

```
ciscoasa(config)# ssl encryption 3des-sha1 aes128-sha1 des-sha1
```