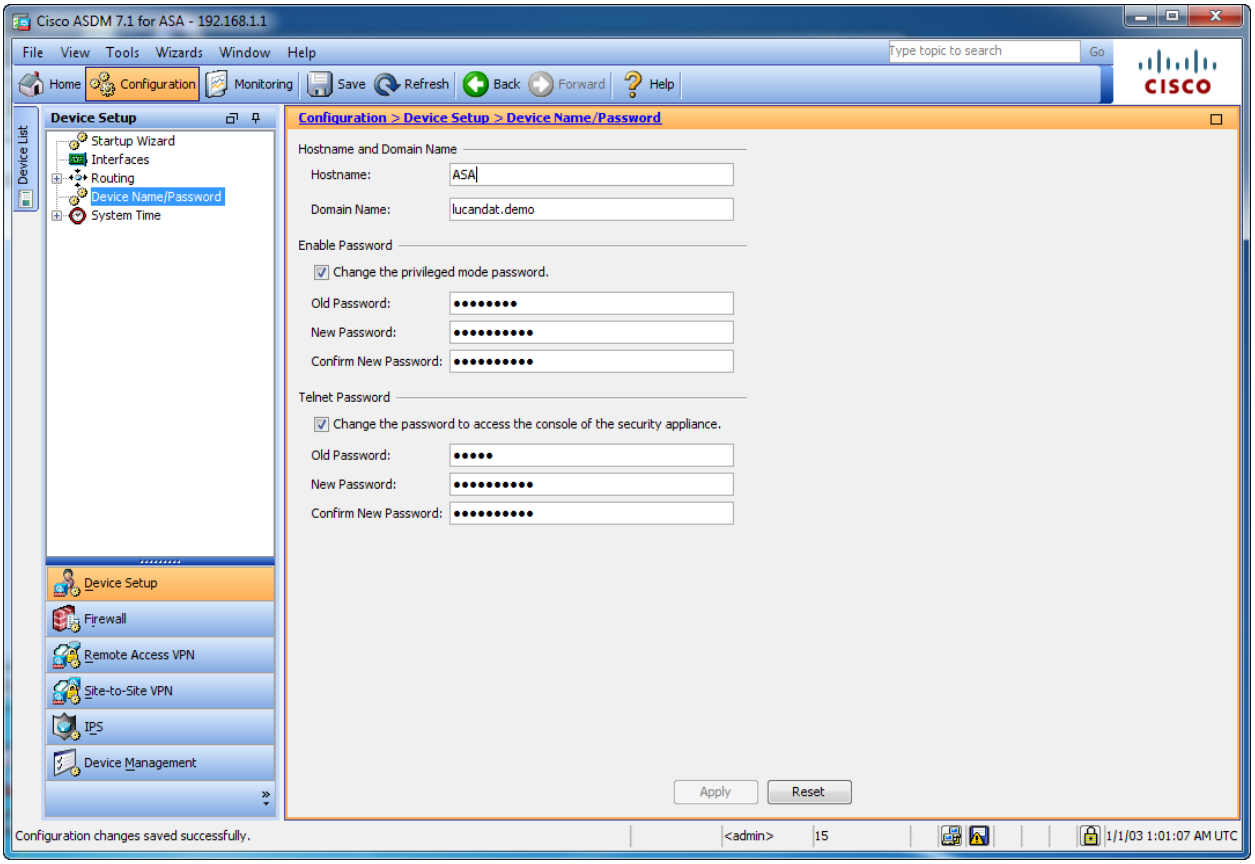
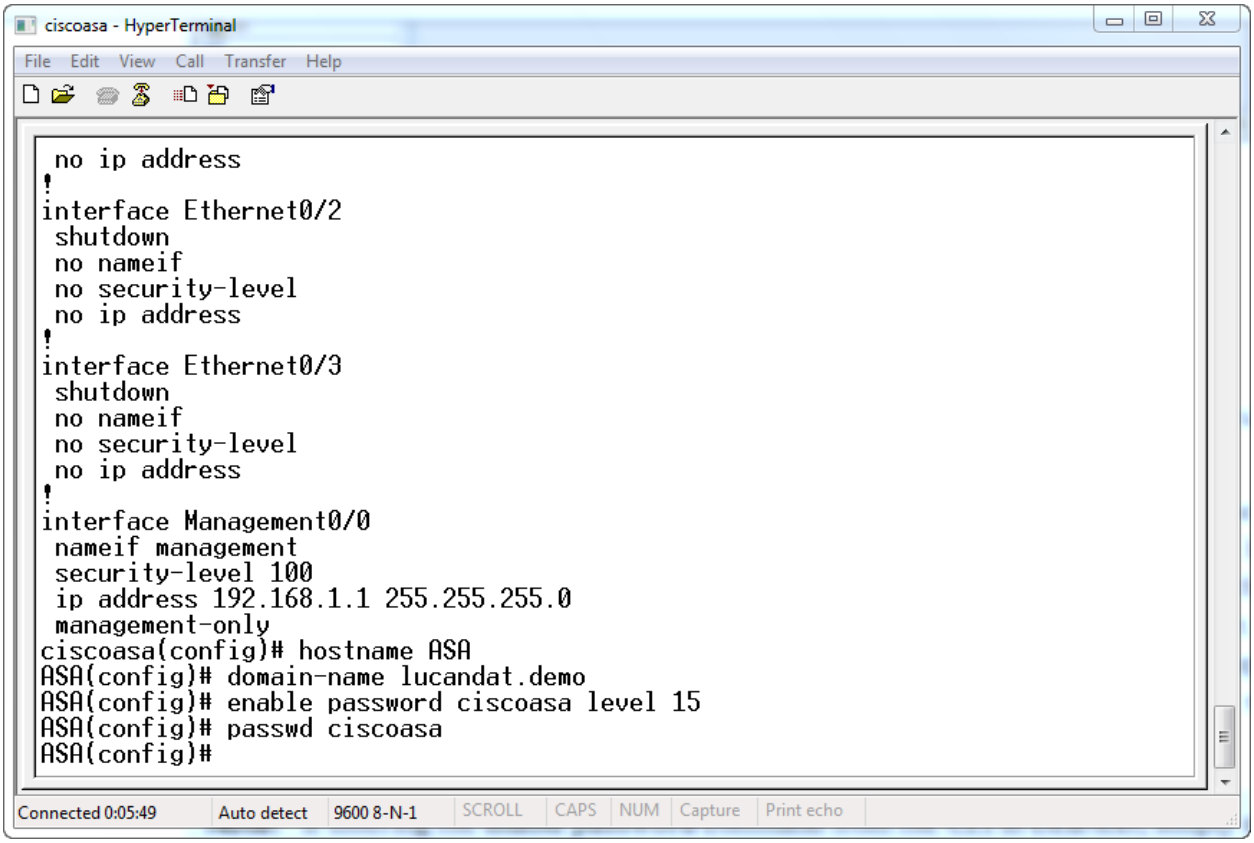
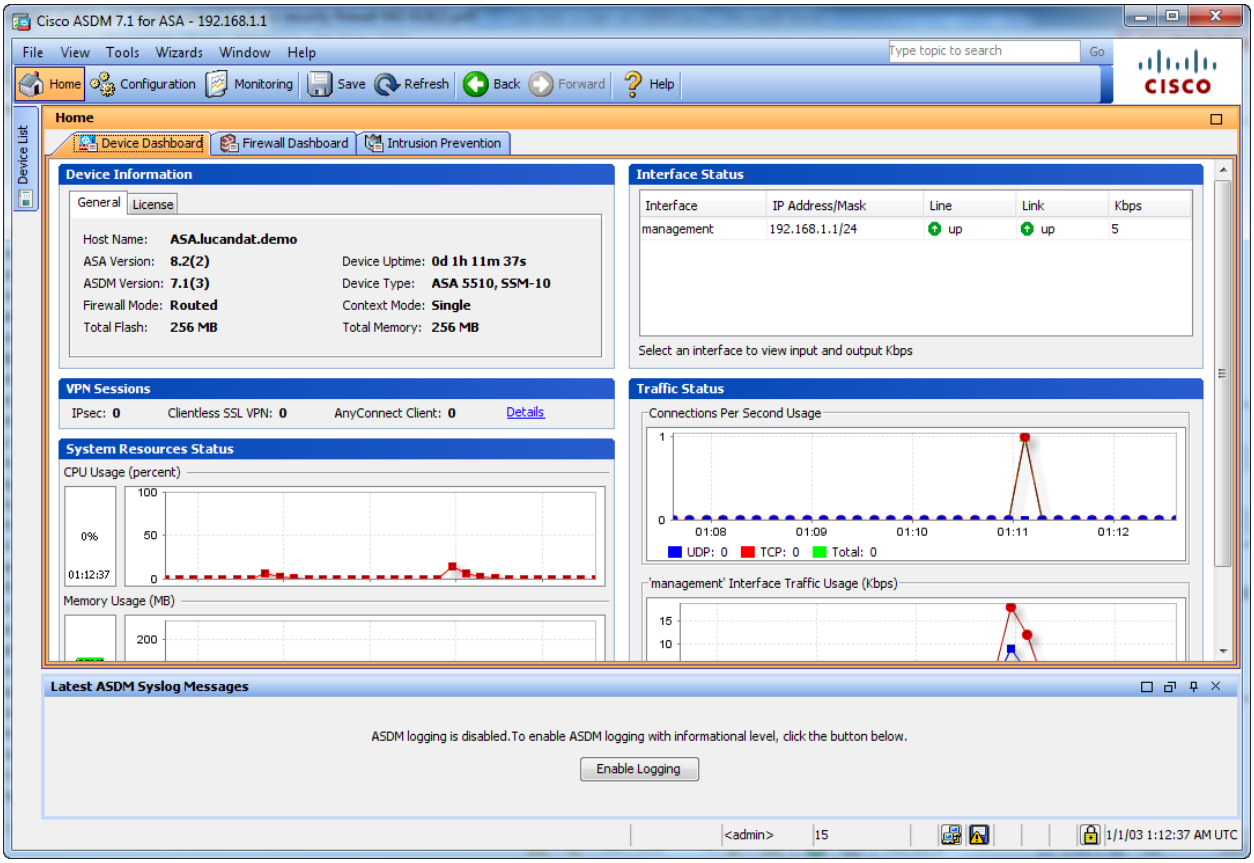
Cấu hình ASA cơ bản với ASDM



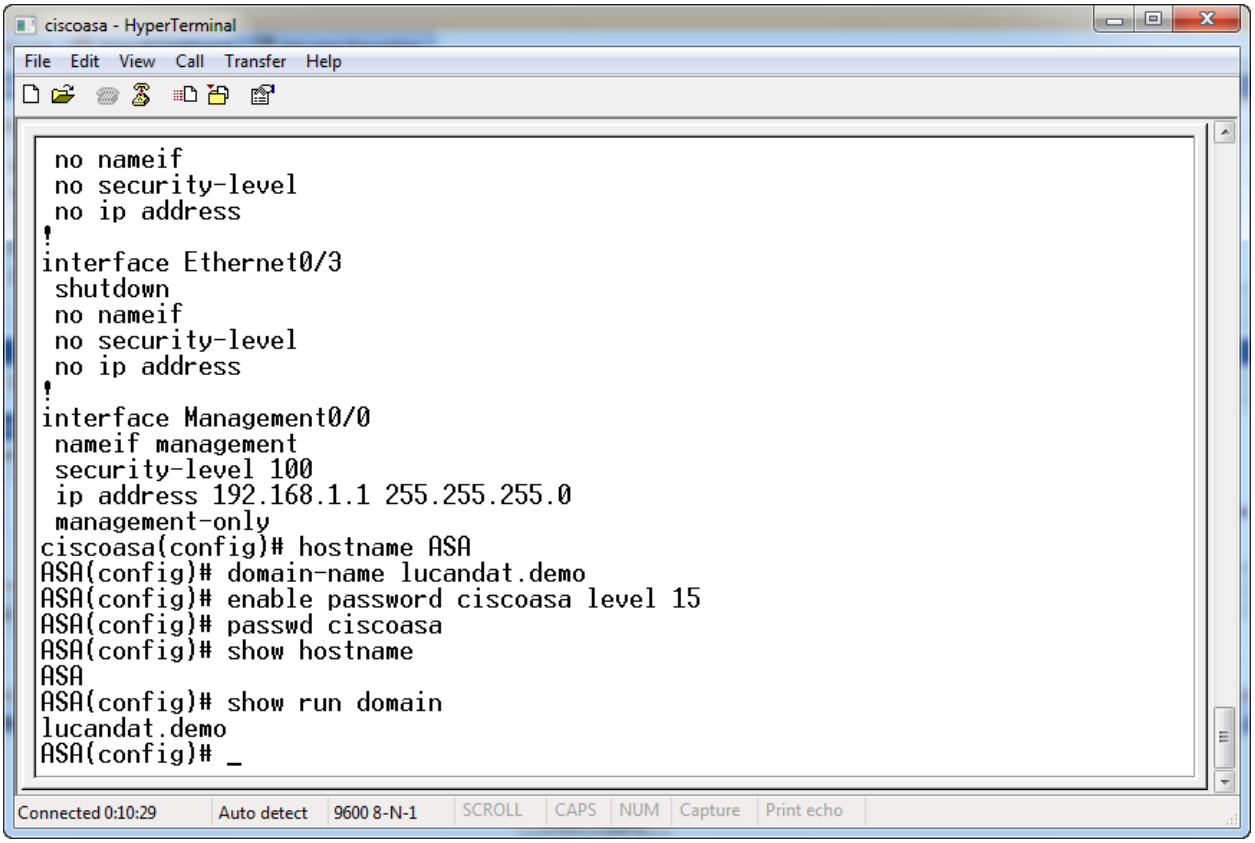
cấu hình ASA cơ bản với CLI



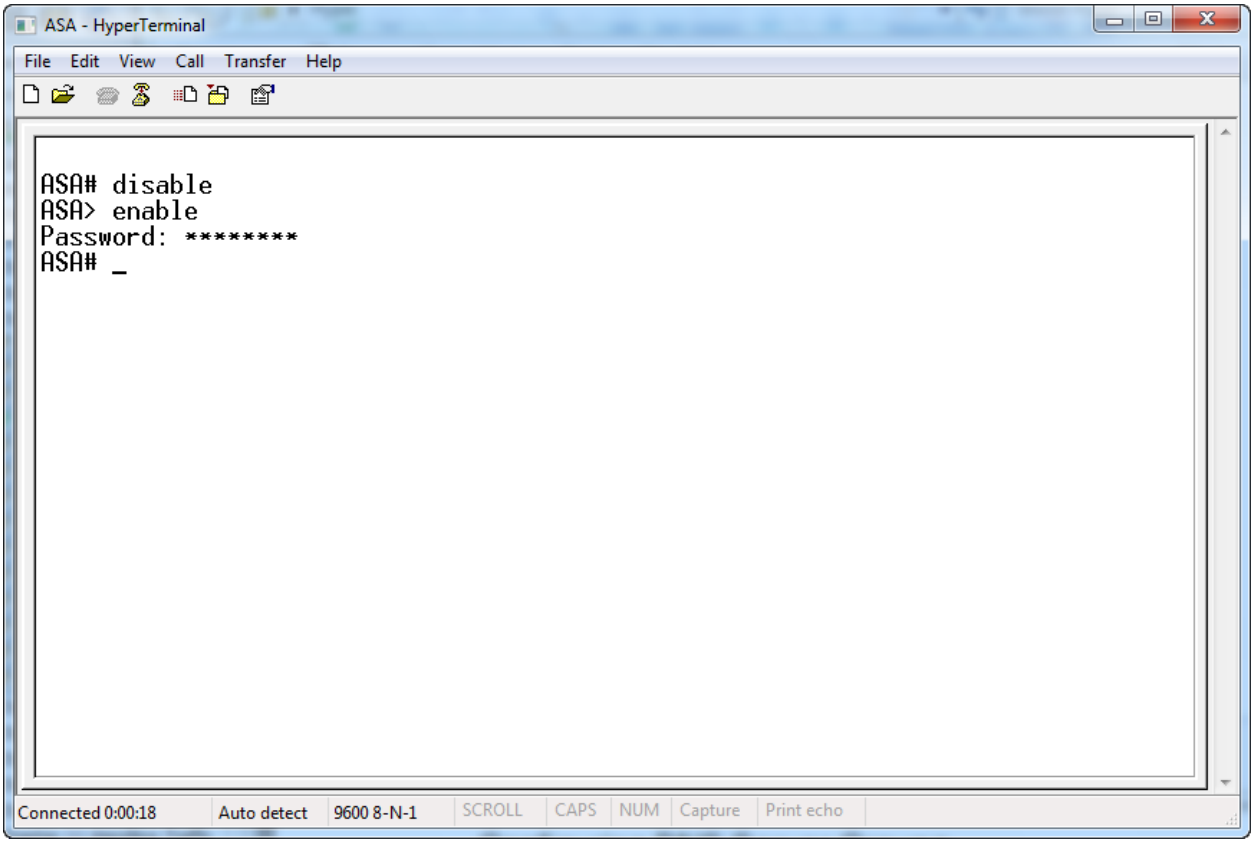
Kiểm tra thông tin cơ bản với ASDM



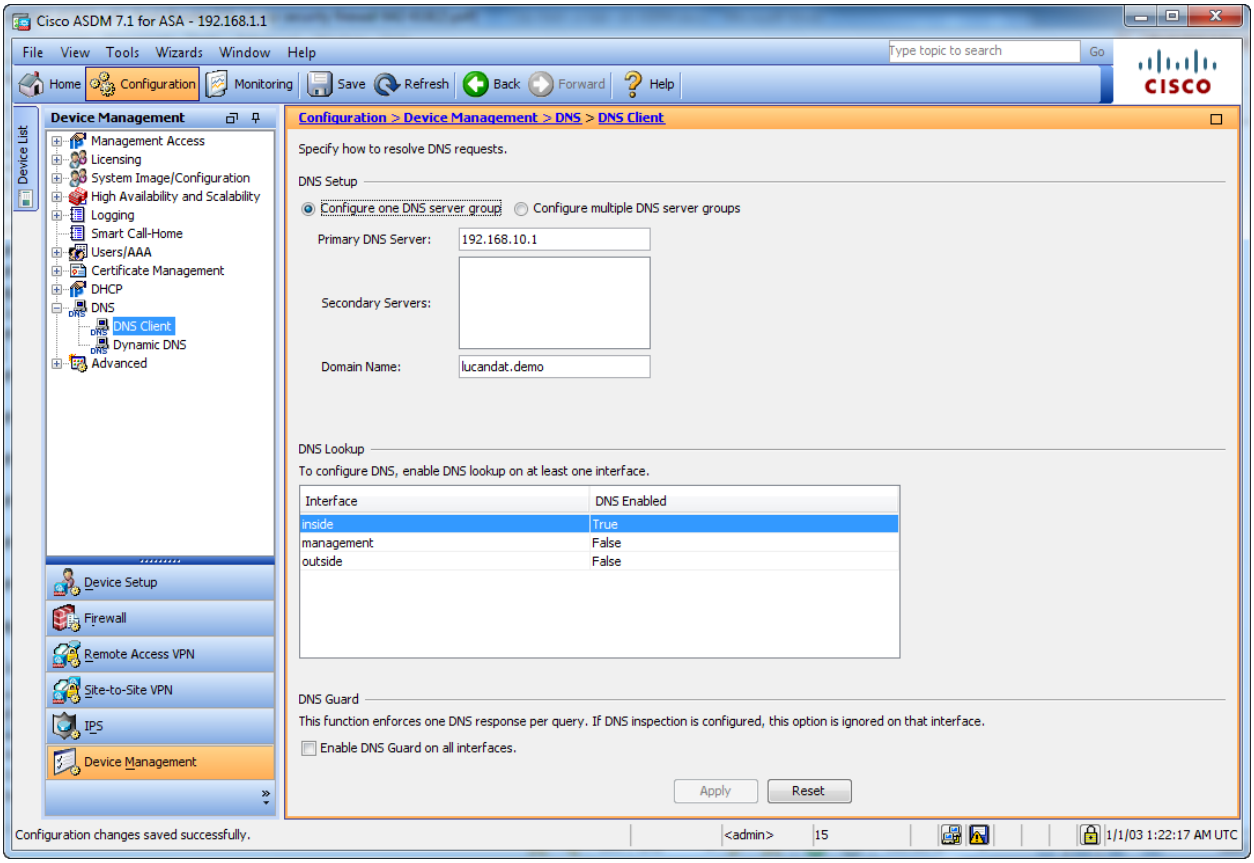
Kiểm tra thông tin cơ bản với CLI



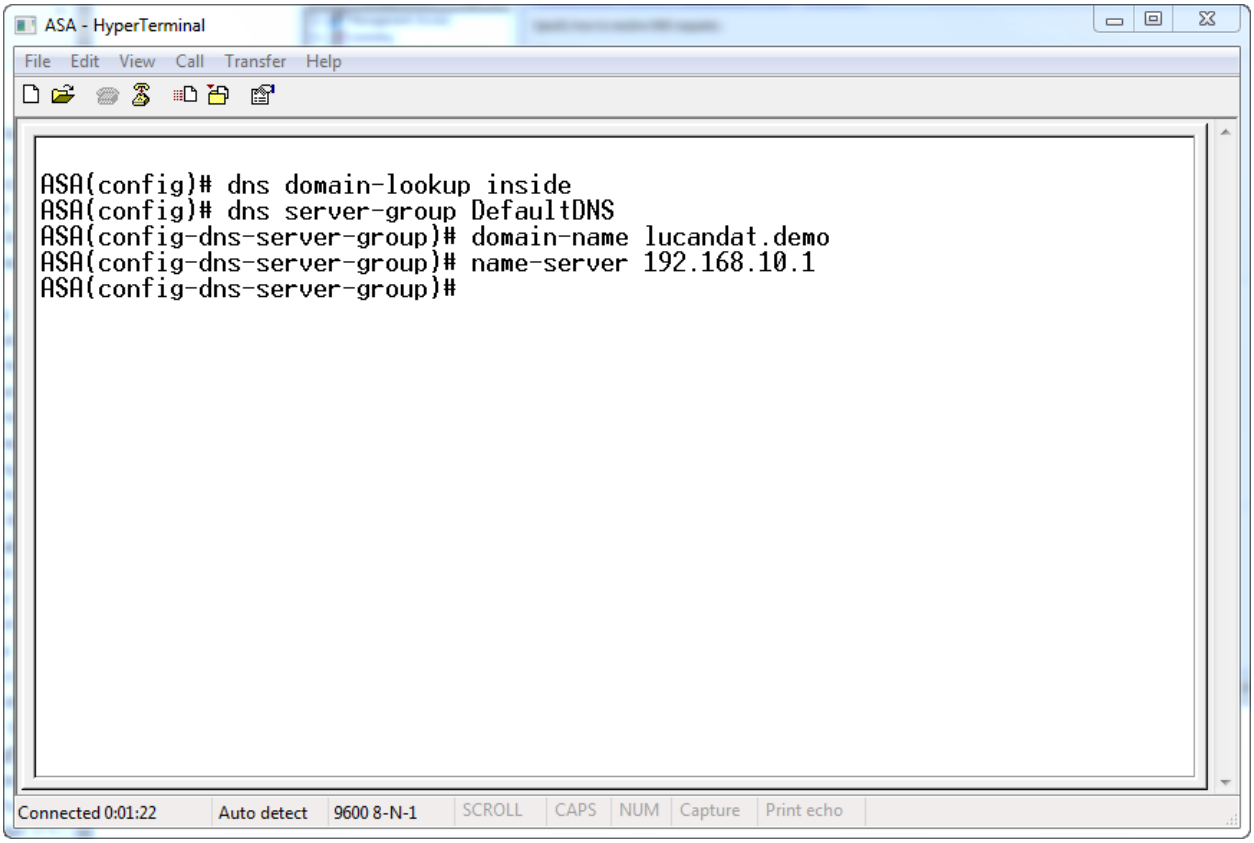
Kiểm tra chứng thực sau khi đặt password với CLI



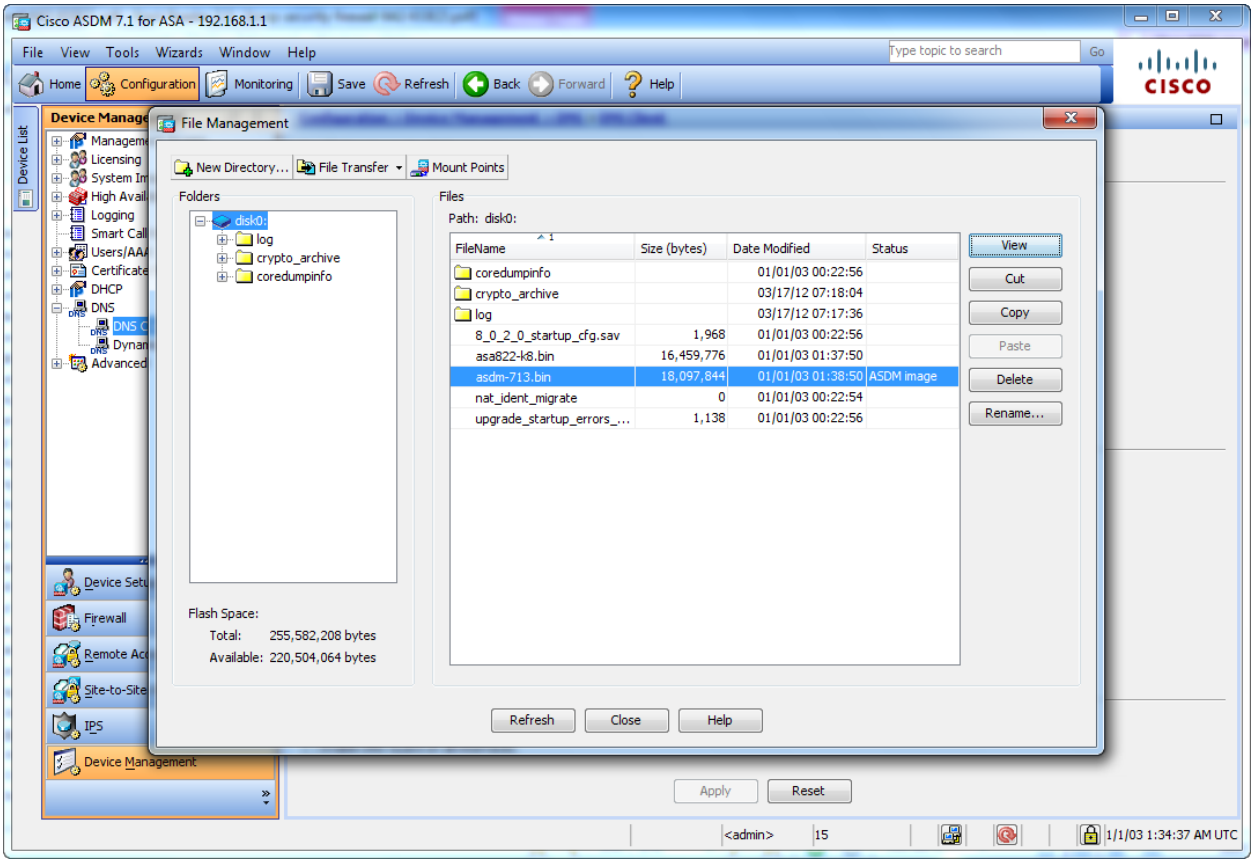
Kích hoạt DNS Client trên cổng inside



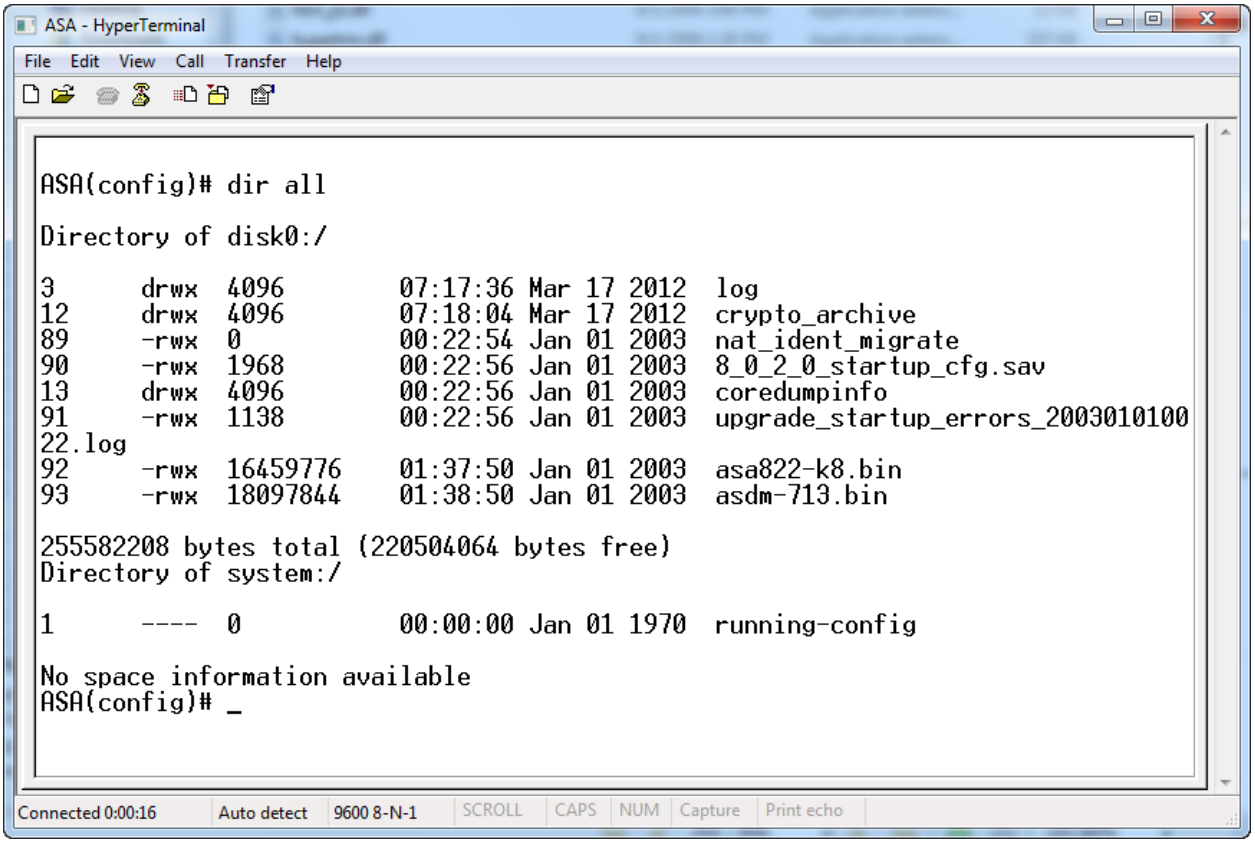
Cấu hình DNS Client với CLI



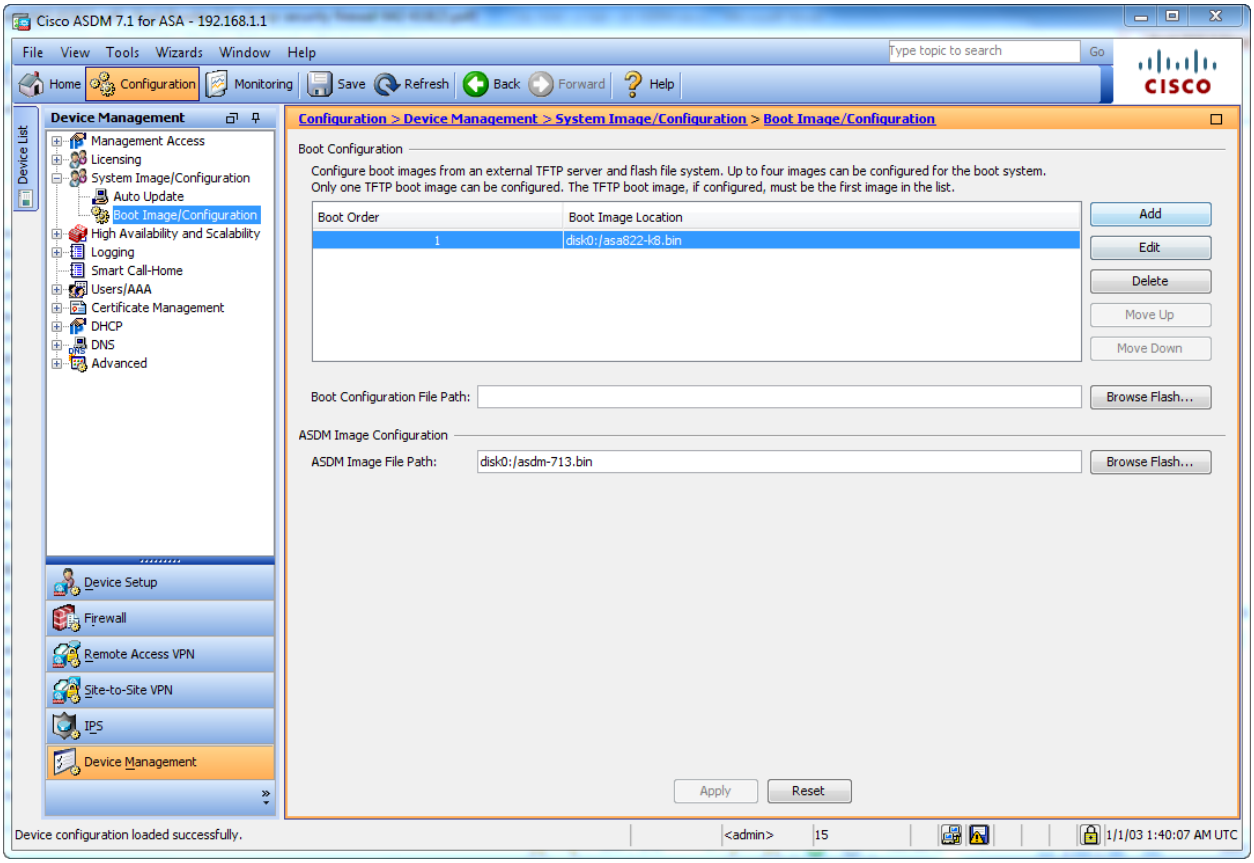
Kiểm tra các tập tin hệ thống với ASDM



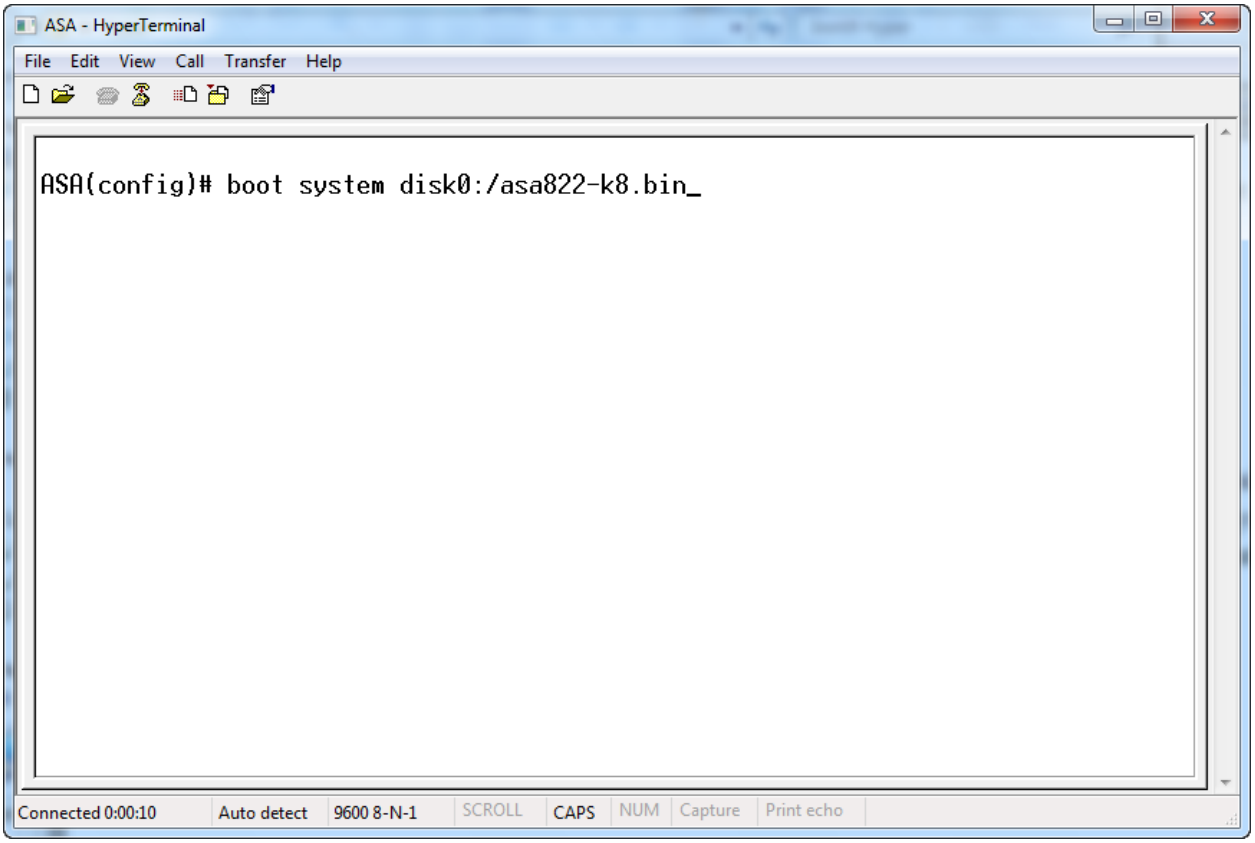
Kiểm tra file system với CLI



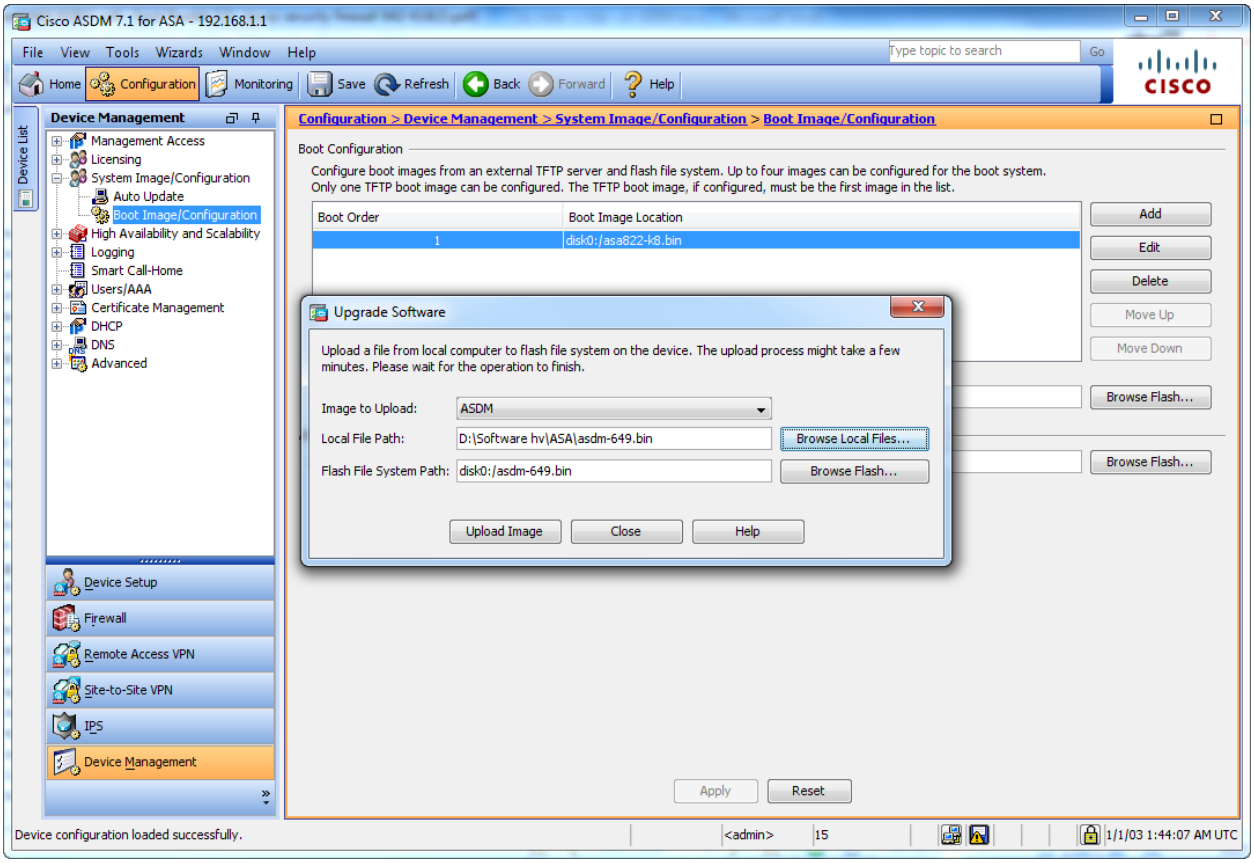
Kiểm tra thứ tự boot order của IOS



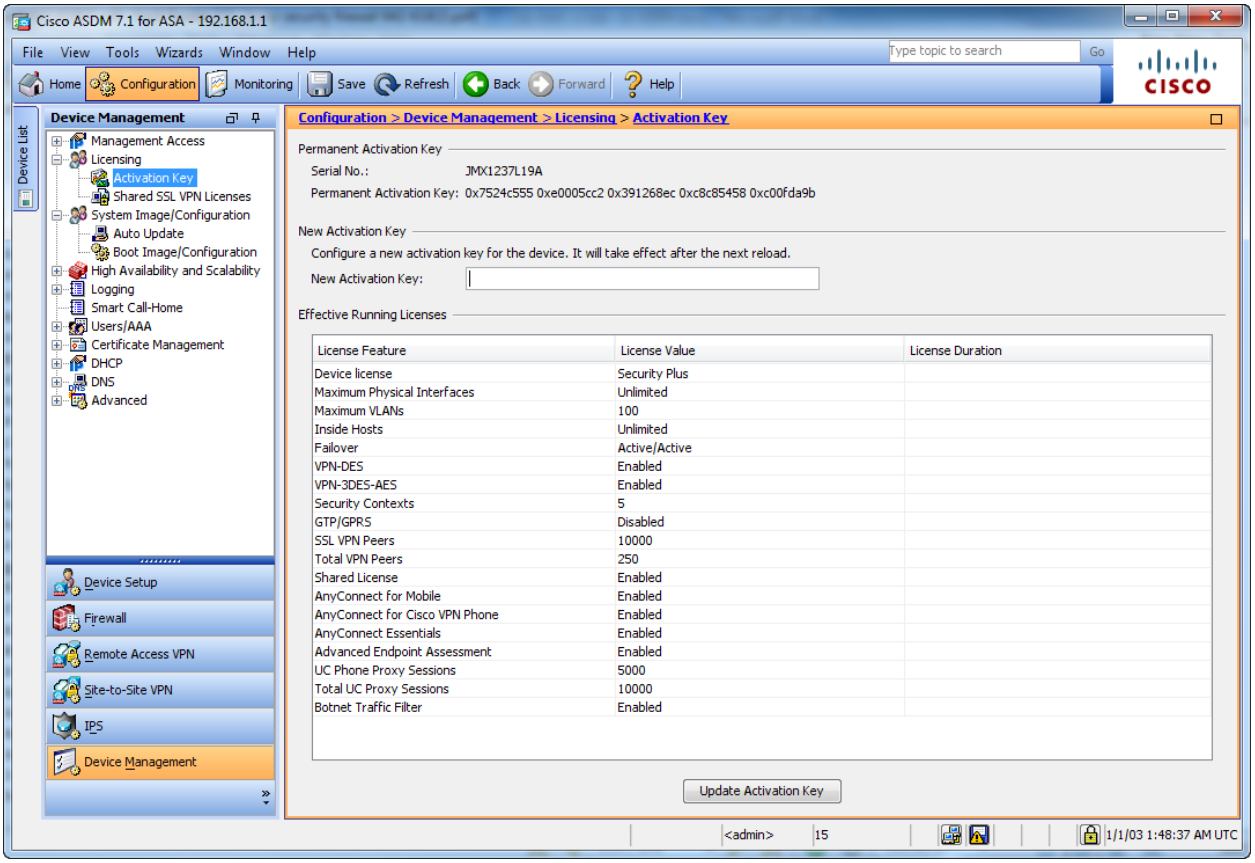
Khai báo IOS sẽ boot khi khởi động ASA với CLI



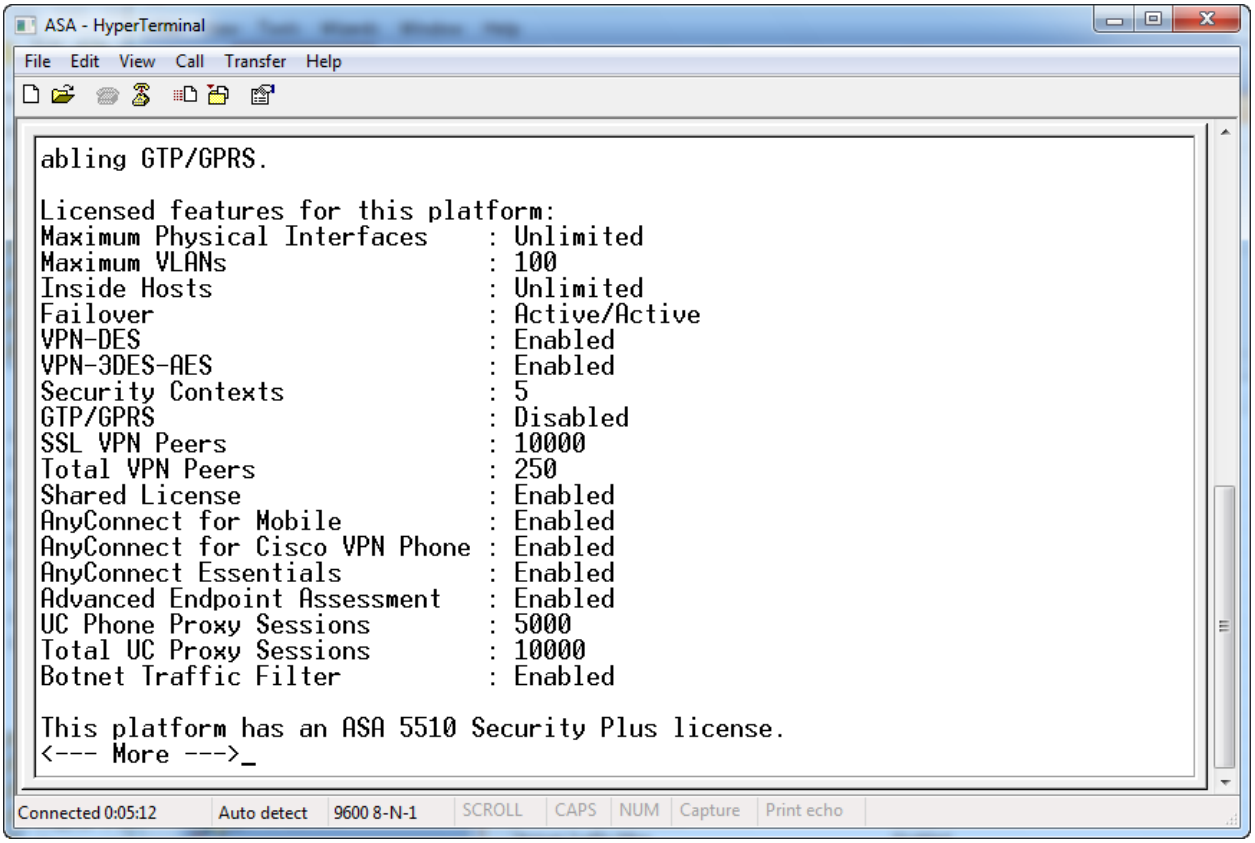
Cập nhật image ASDM



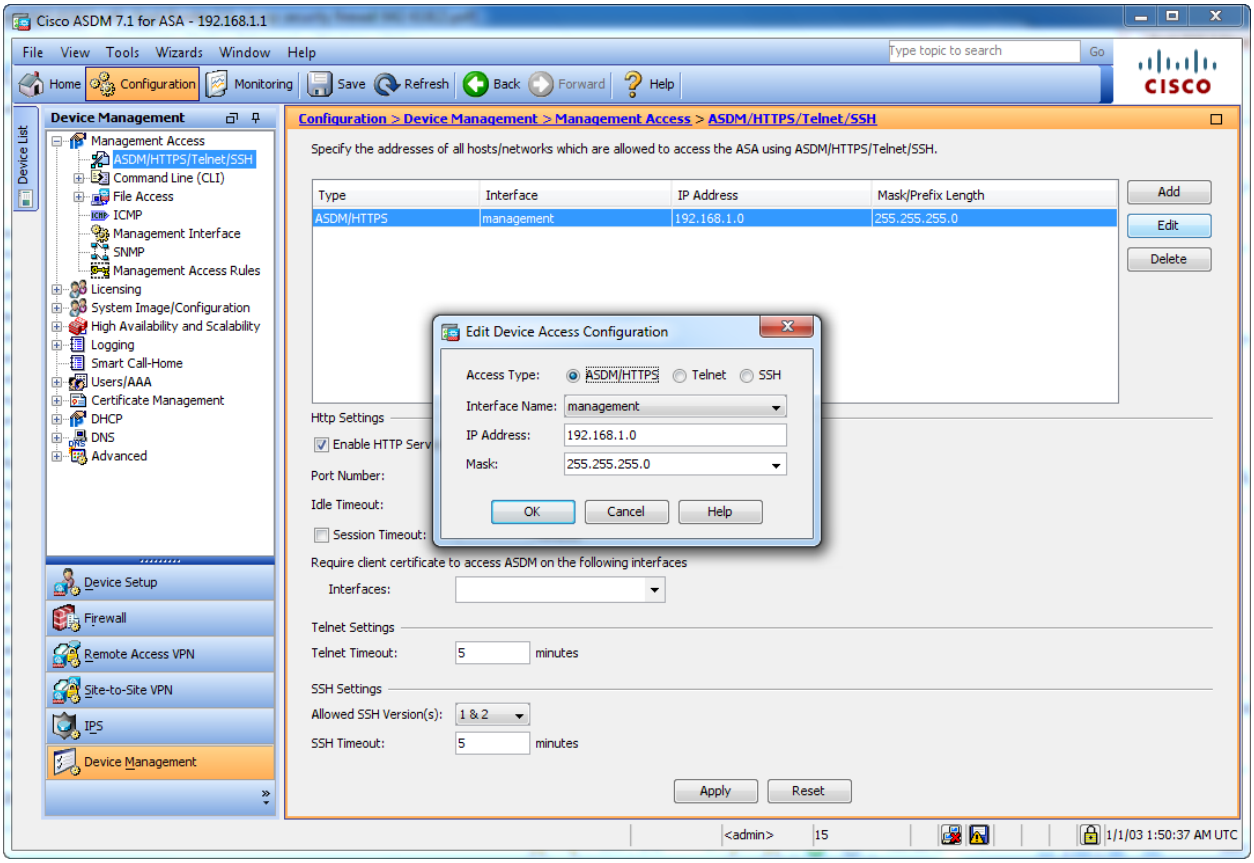
Kiểm tra active-key và cập nhật key với ASDM



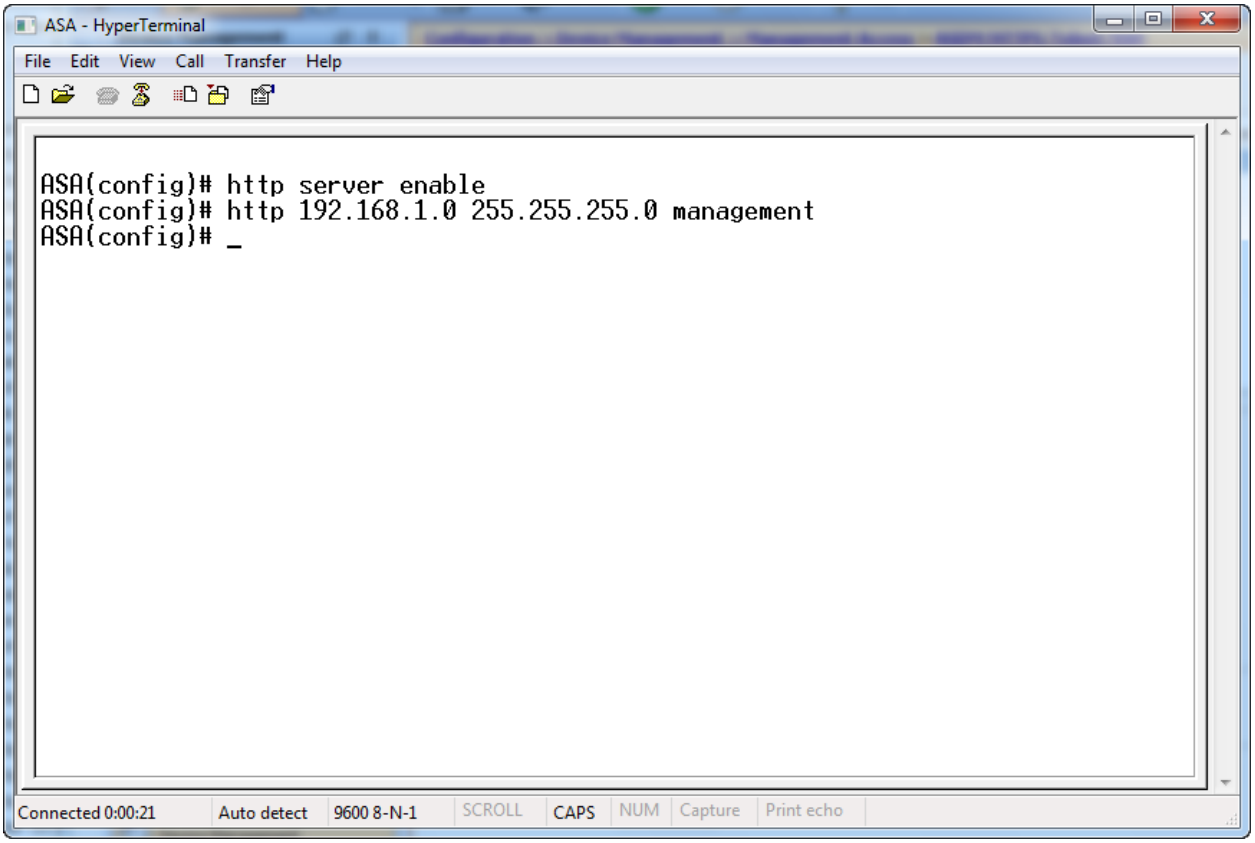
Kiểm tra và cập nhập active-key với CLI



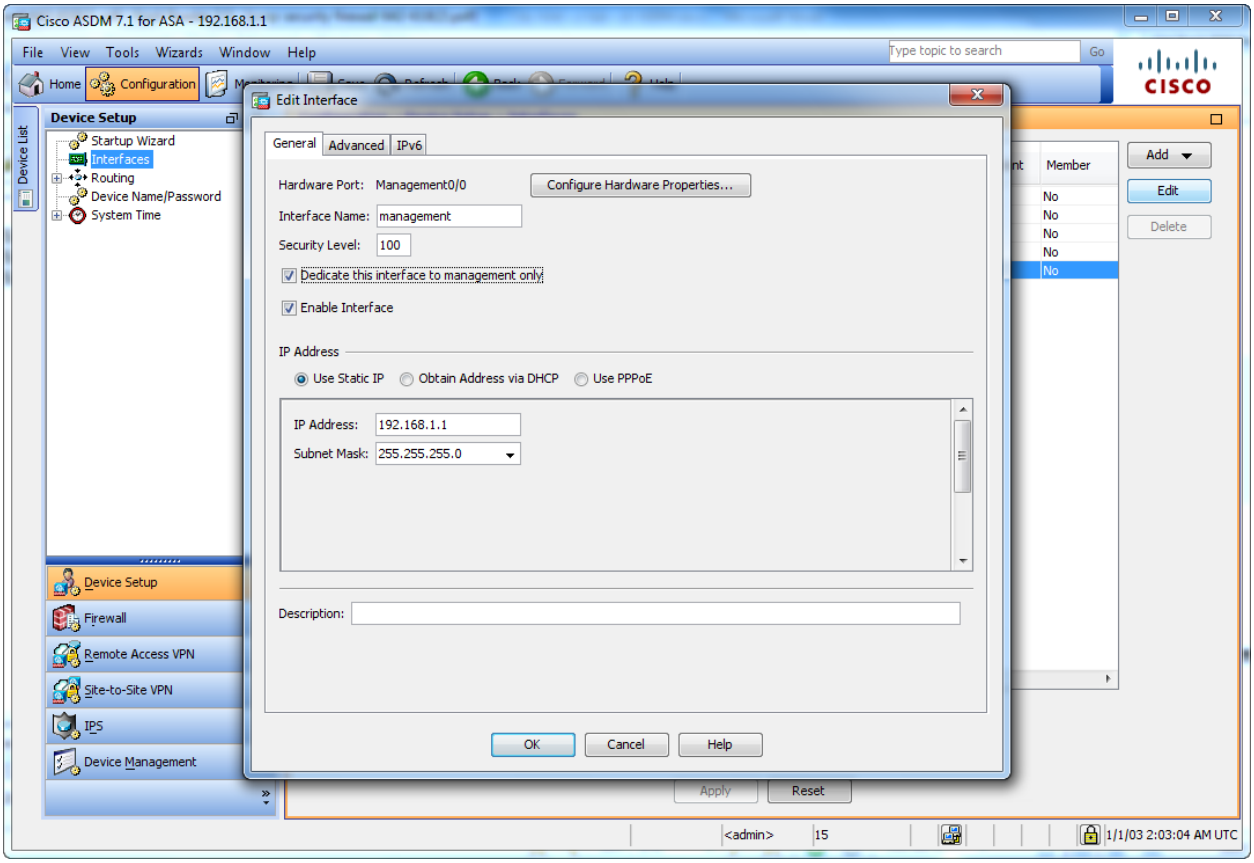
Kích hoạt cho phép truy cập ASDM qua giao diện web giao thức https



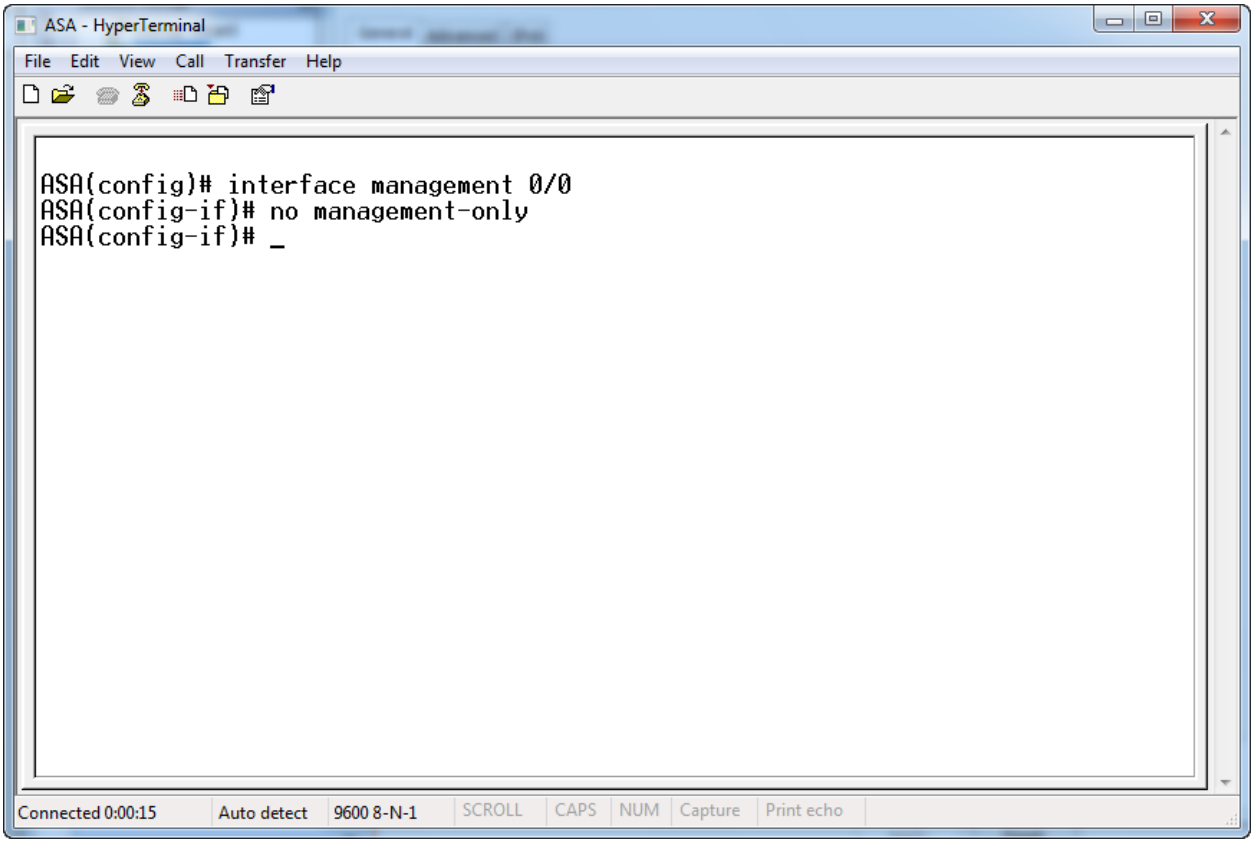
Kích hoạt giao thức http để truy cập ASDM qua giao diện wweb



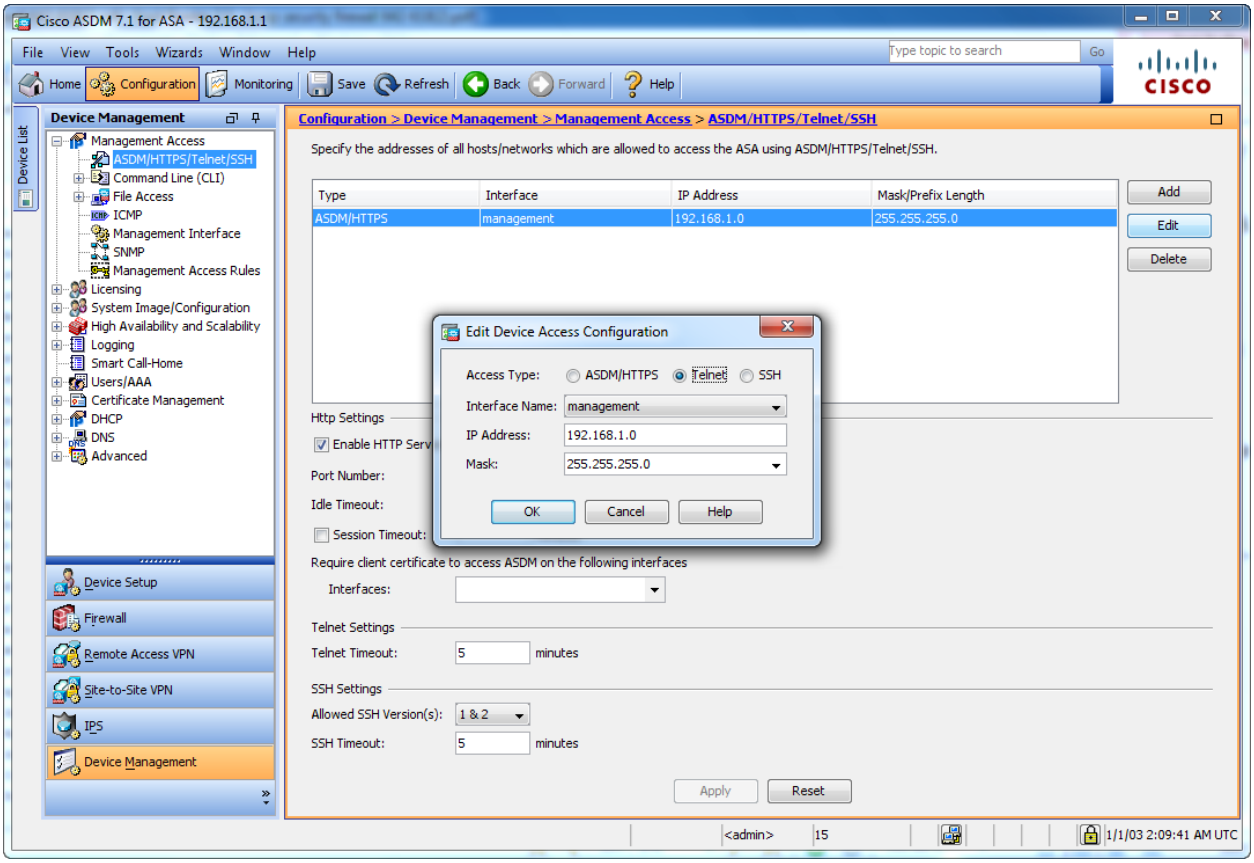
Cấu hình no management-only trên ASDM



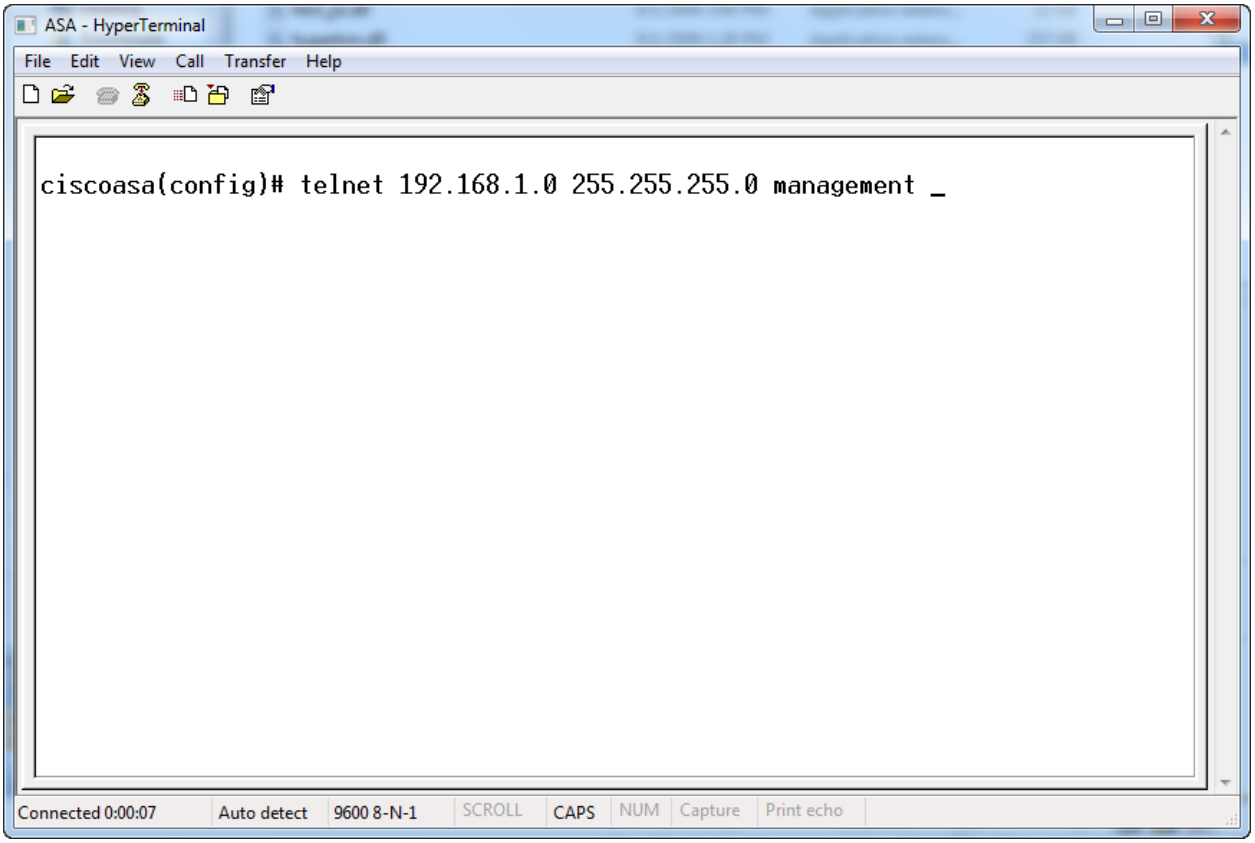
Cấu hình với dòng lệnh



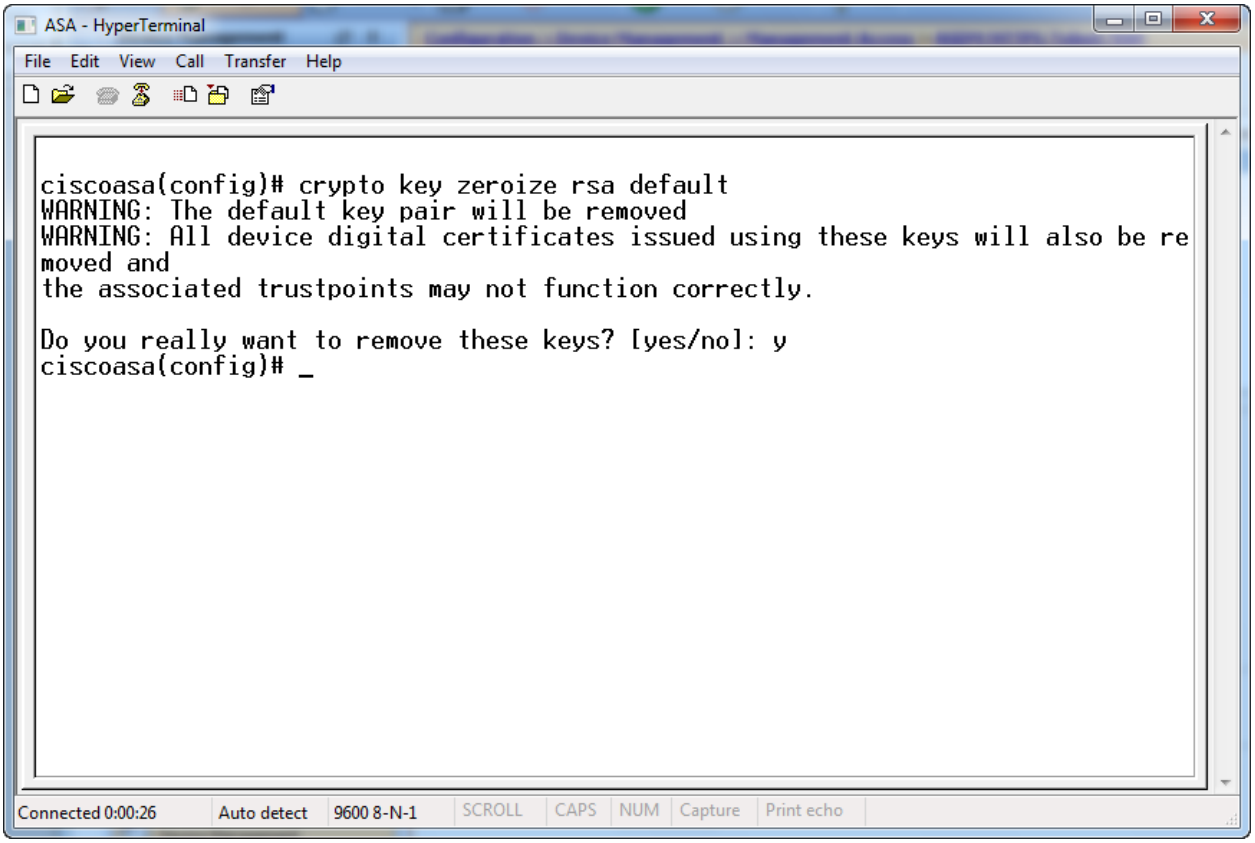
Cấu hình cho phép telnet



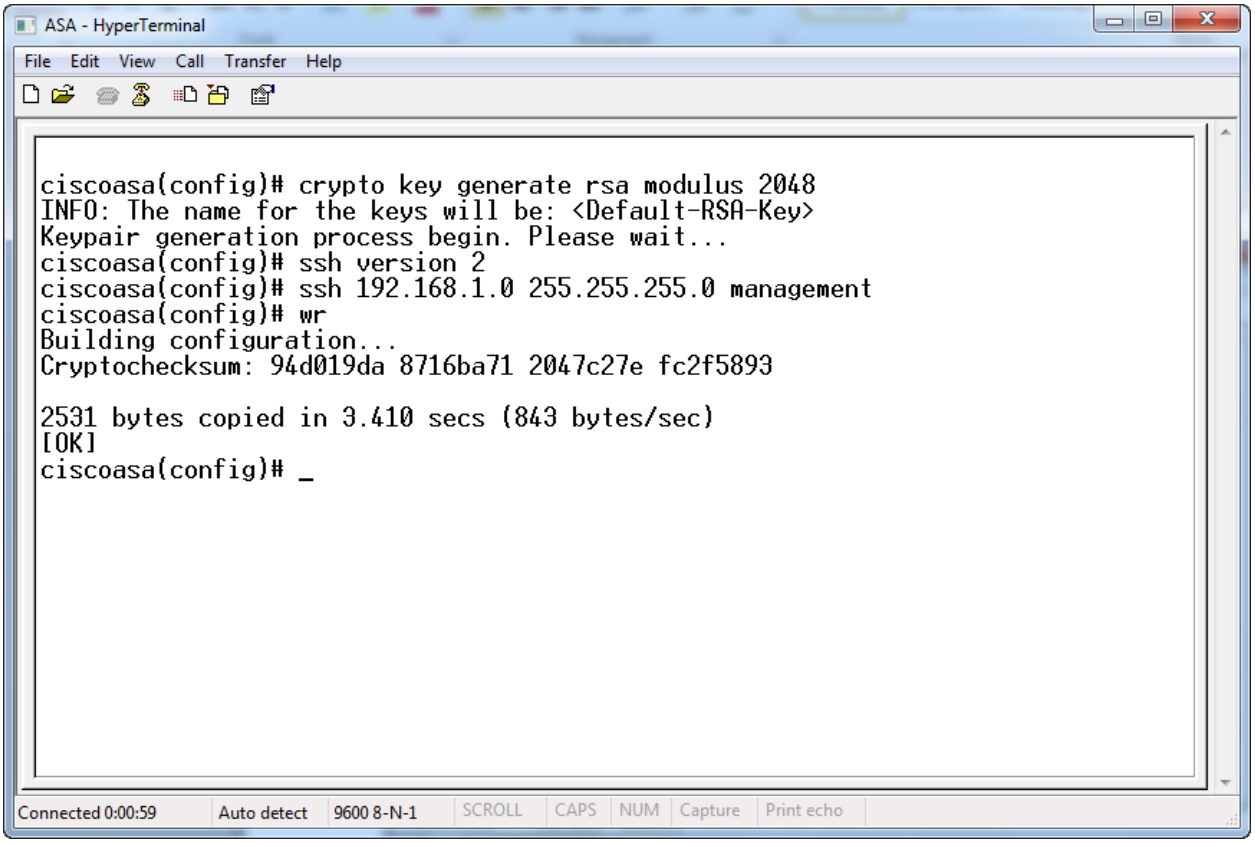
Cấu hình cho phép telnet với CLI



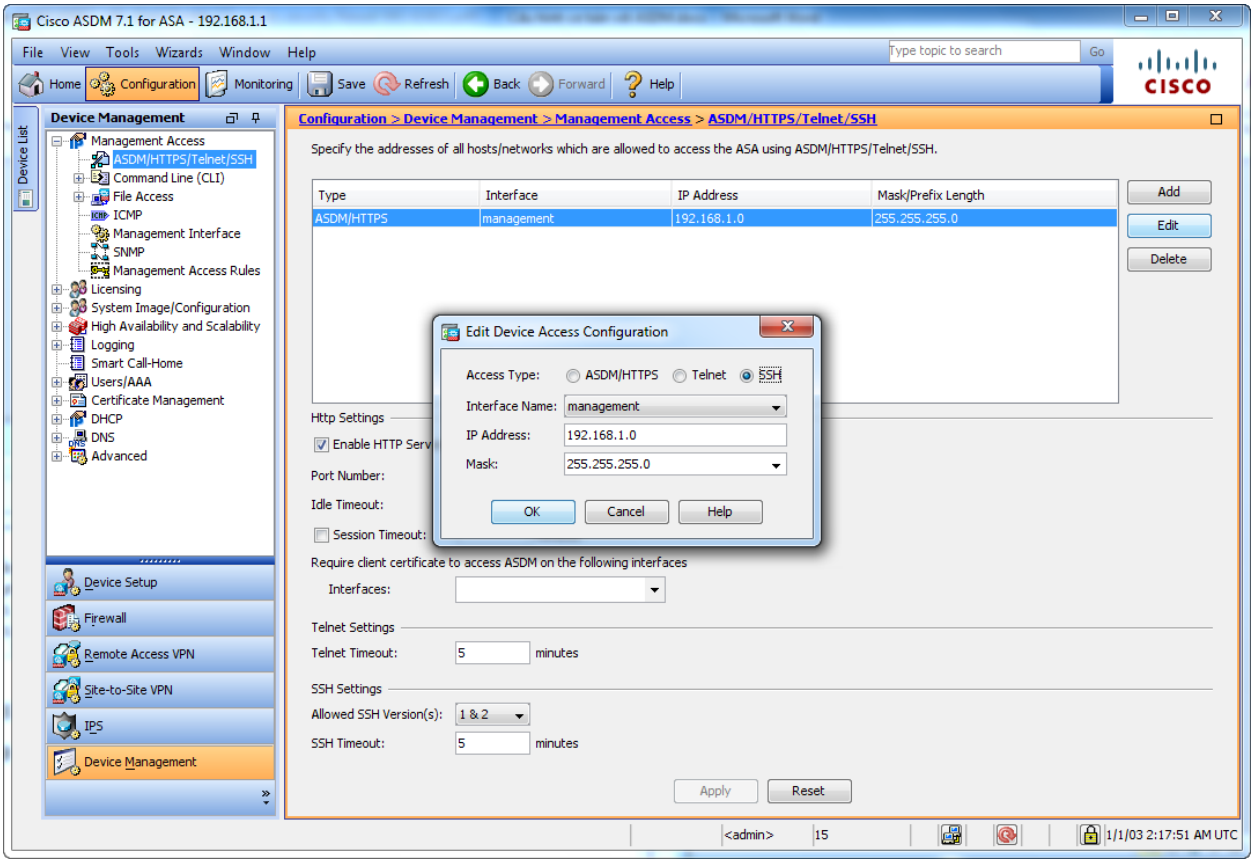
Xoá key RSA mặc định



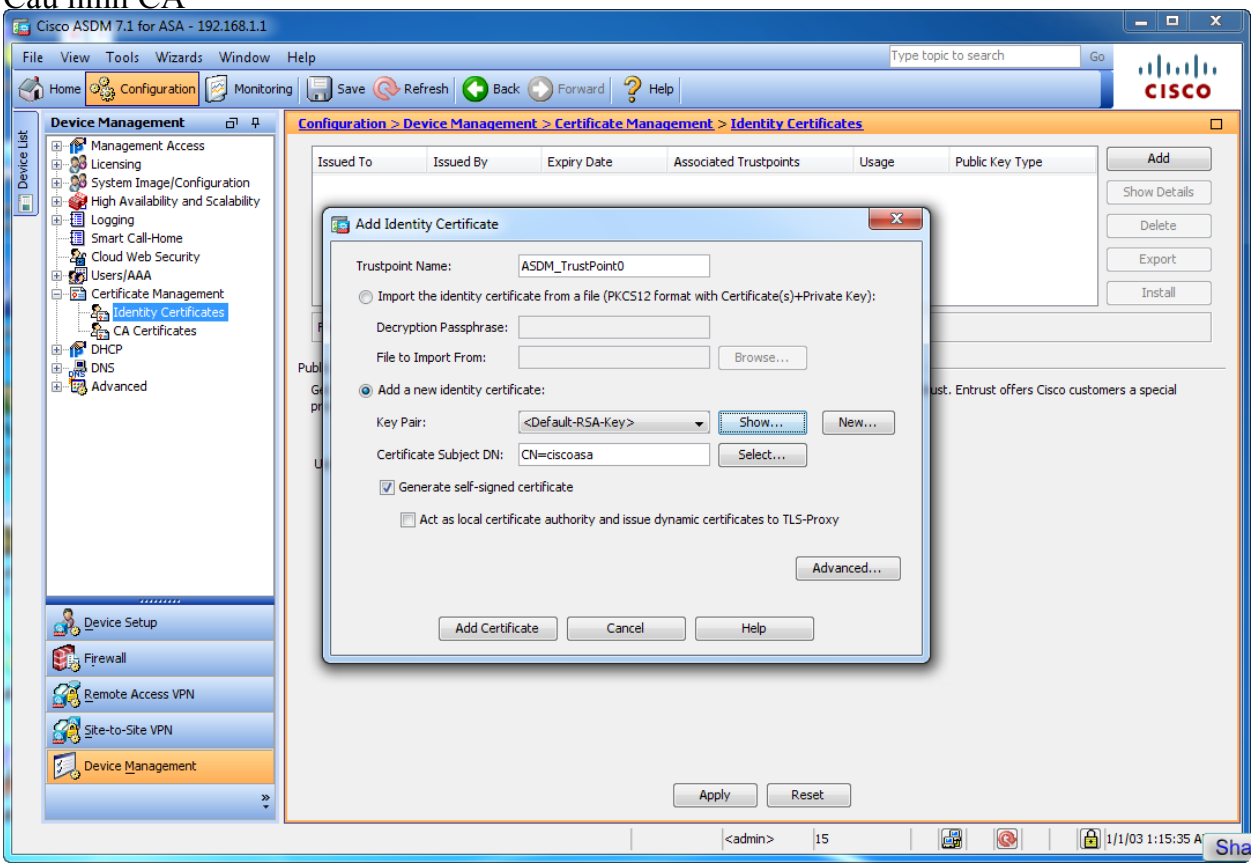
Tạo key rsa mới



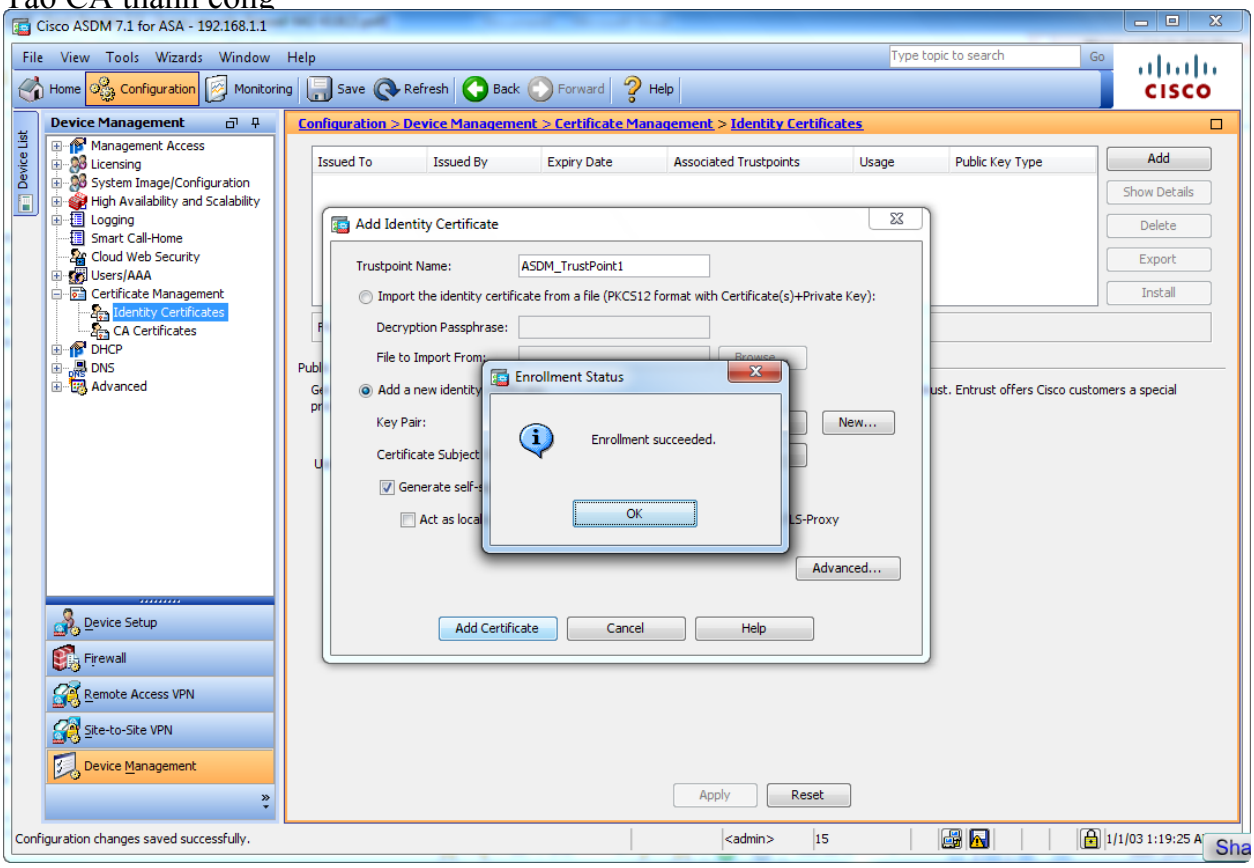
Kích hoạt ssh



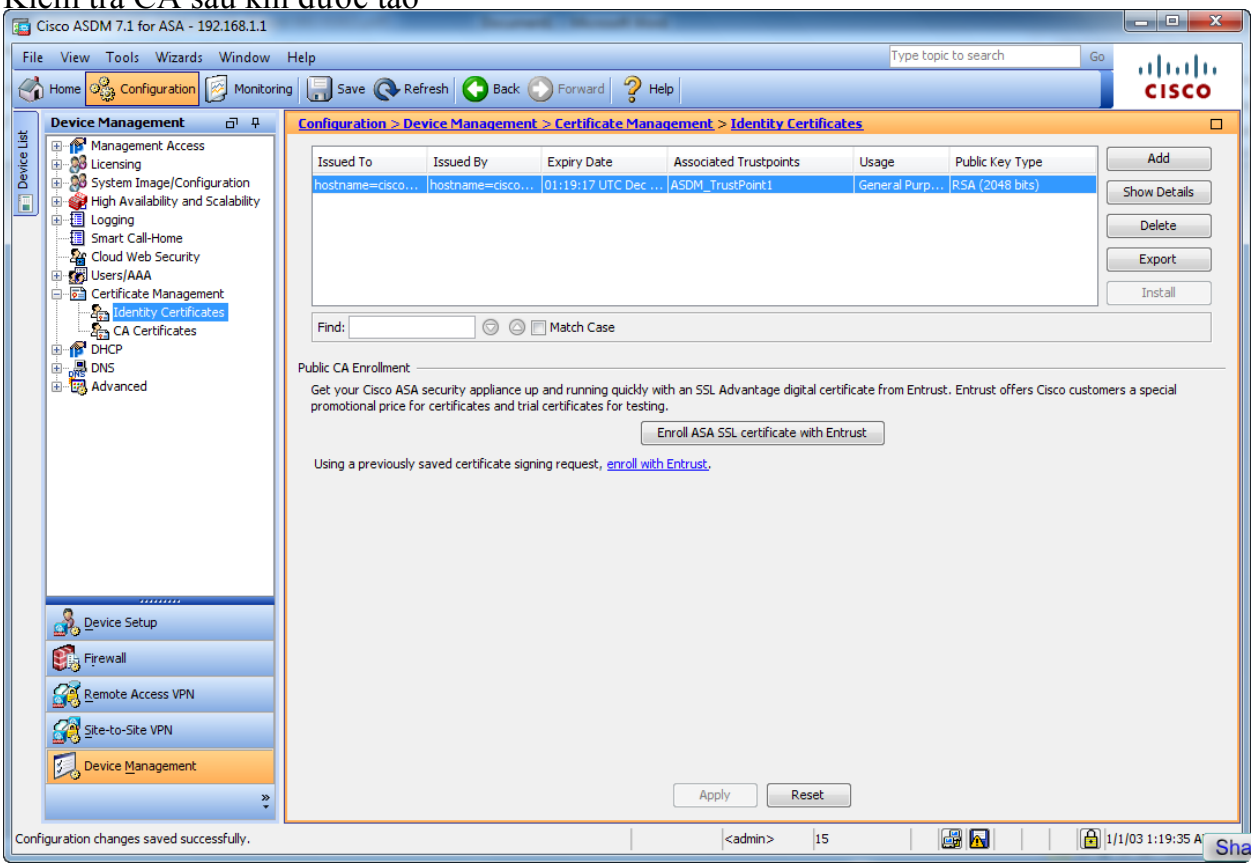
Cấu hình CA


Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalability
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
Certificate Management
Identity Certificates
CA Certificates
DHCP
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Management > Certificate Management > Identity Certificates
Issued To
Issued By
Expiry Date
Associated Trustpoints
Usage
Public Key Type
Add
Show Details
Delete
Export
Install
Add Identity Certificate
Trustpoint Name:
ASDM_TrustPoint0
Import the identity certificate from a file (PKCS12 format with Certificate(s)+Private Key):
Decryption Passphrase:
File to Import From:
Browse...
Add a new identity certificate:
Key Pair:
<Default-RSA-Key>
Show...
New...
Certificate Subject DN:
CN=ciscoasa
Select...
Generate self-signed certificate
Act as local certificate authority and issue dynamic certificates to TLS-Proxy
Advanced...
Add Certificate
Cancel
Help
Apply
Reset
<admin>
15

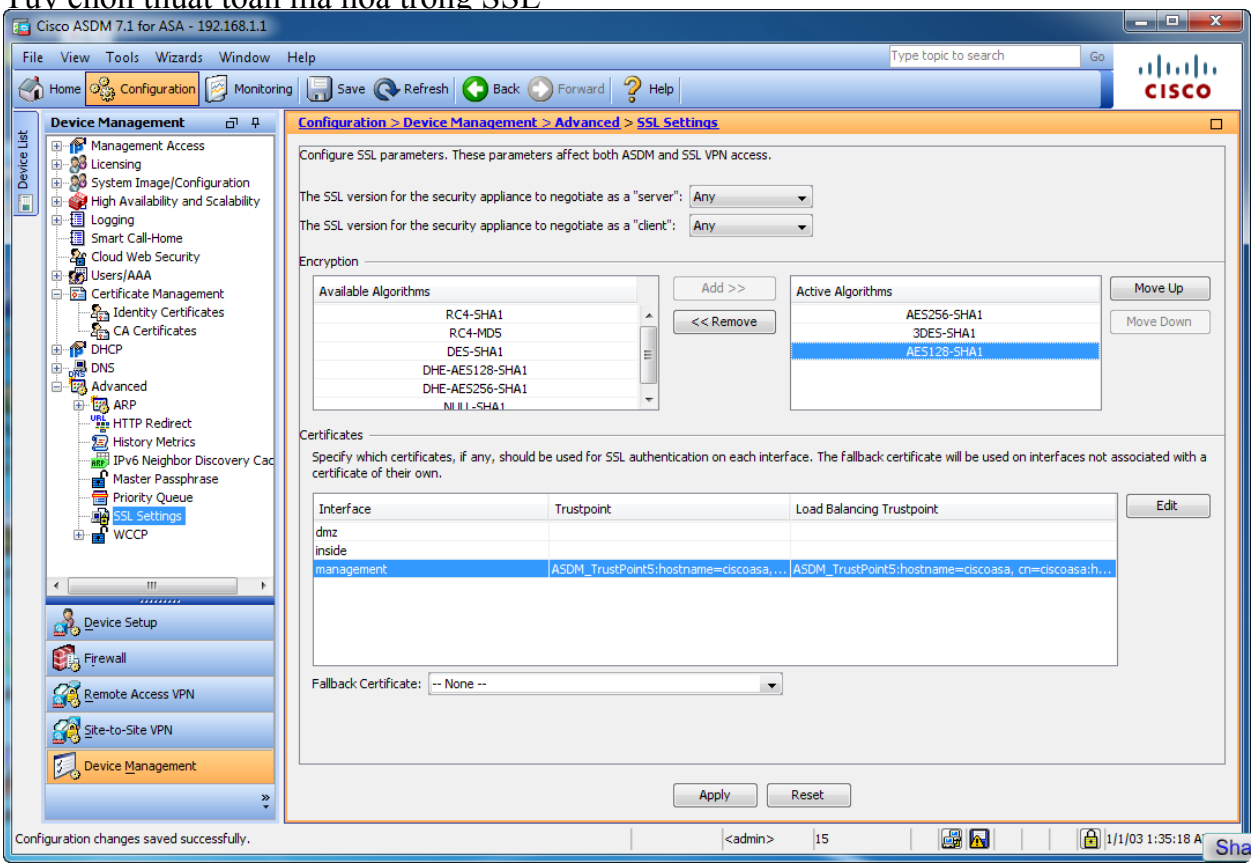
Tao CA thành công



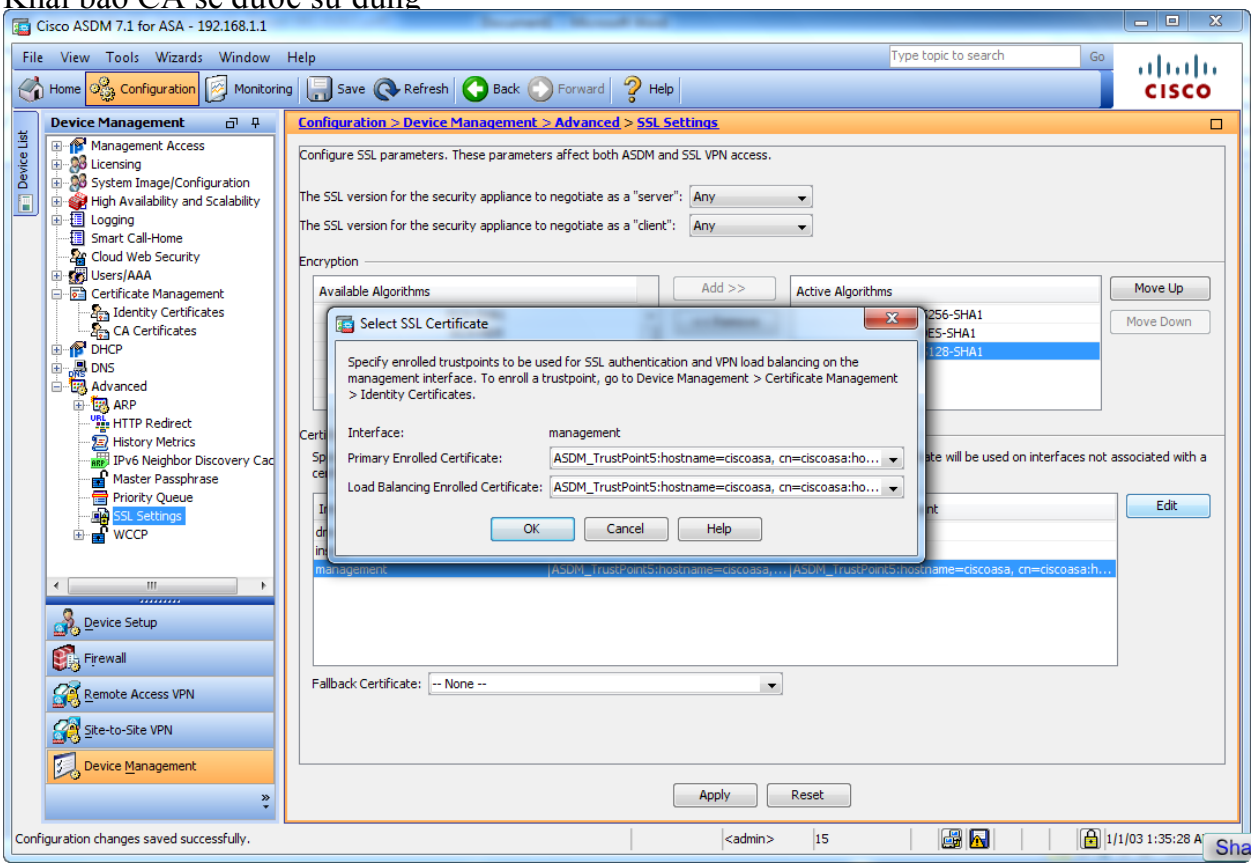
Kiểm tra CA sau khi được tạo



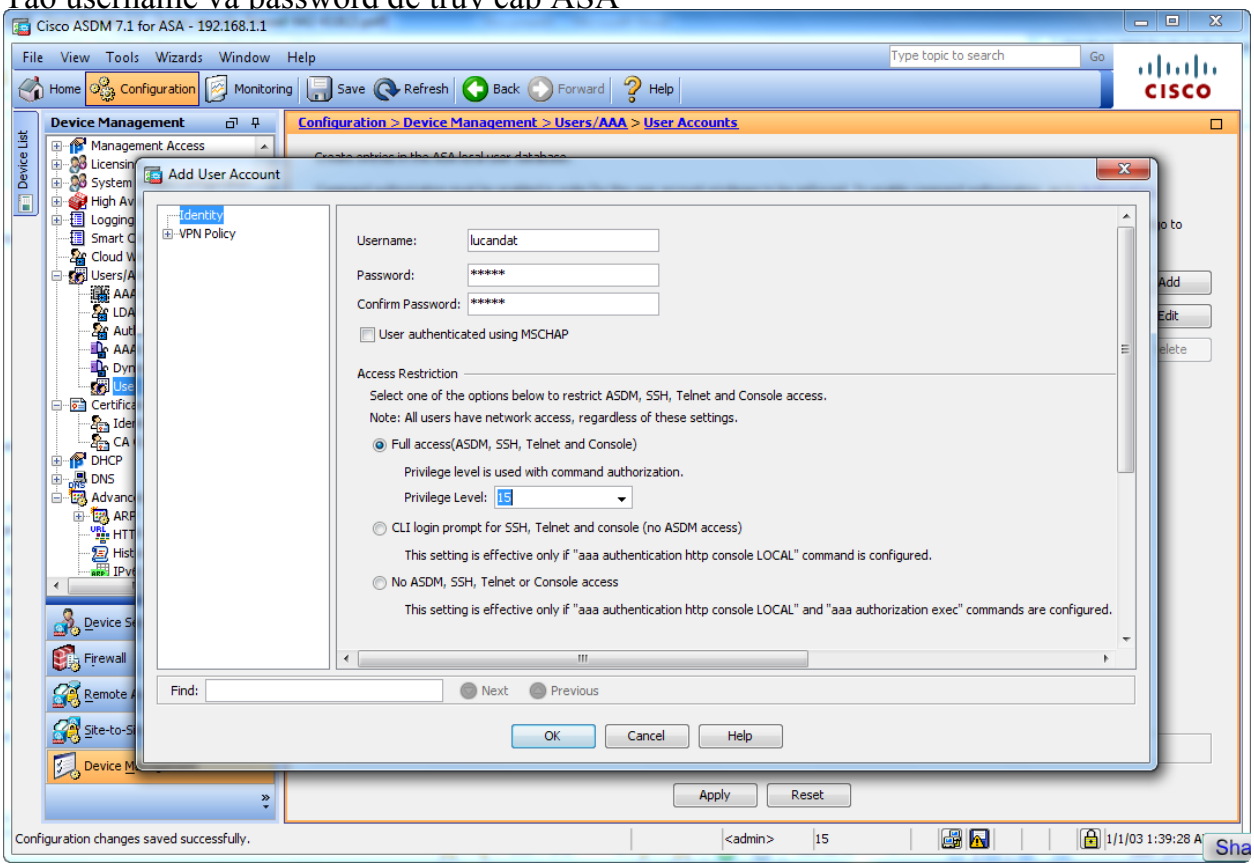
Tùy chọn thuật toán mã hóa trong SSL



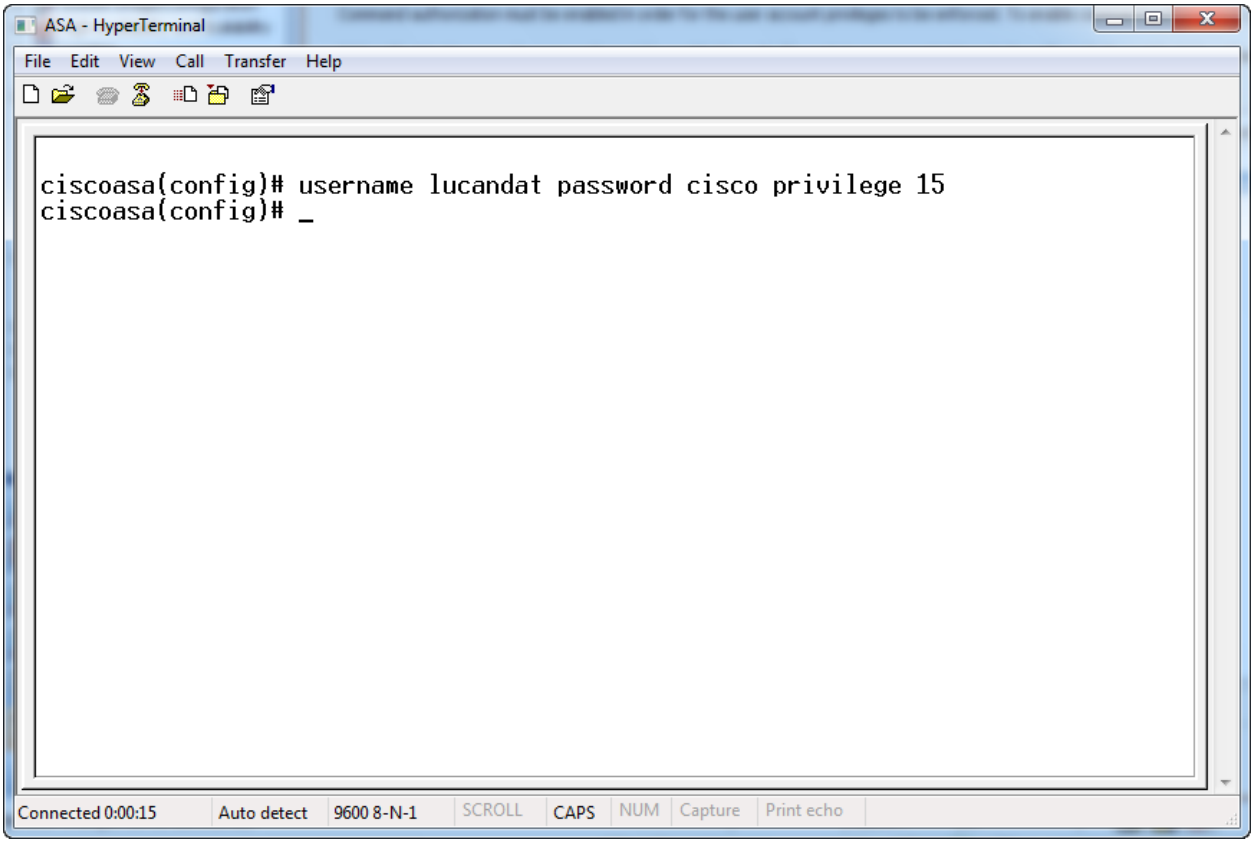
Khai báo CA sẽ được sử dụng



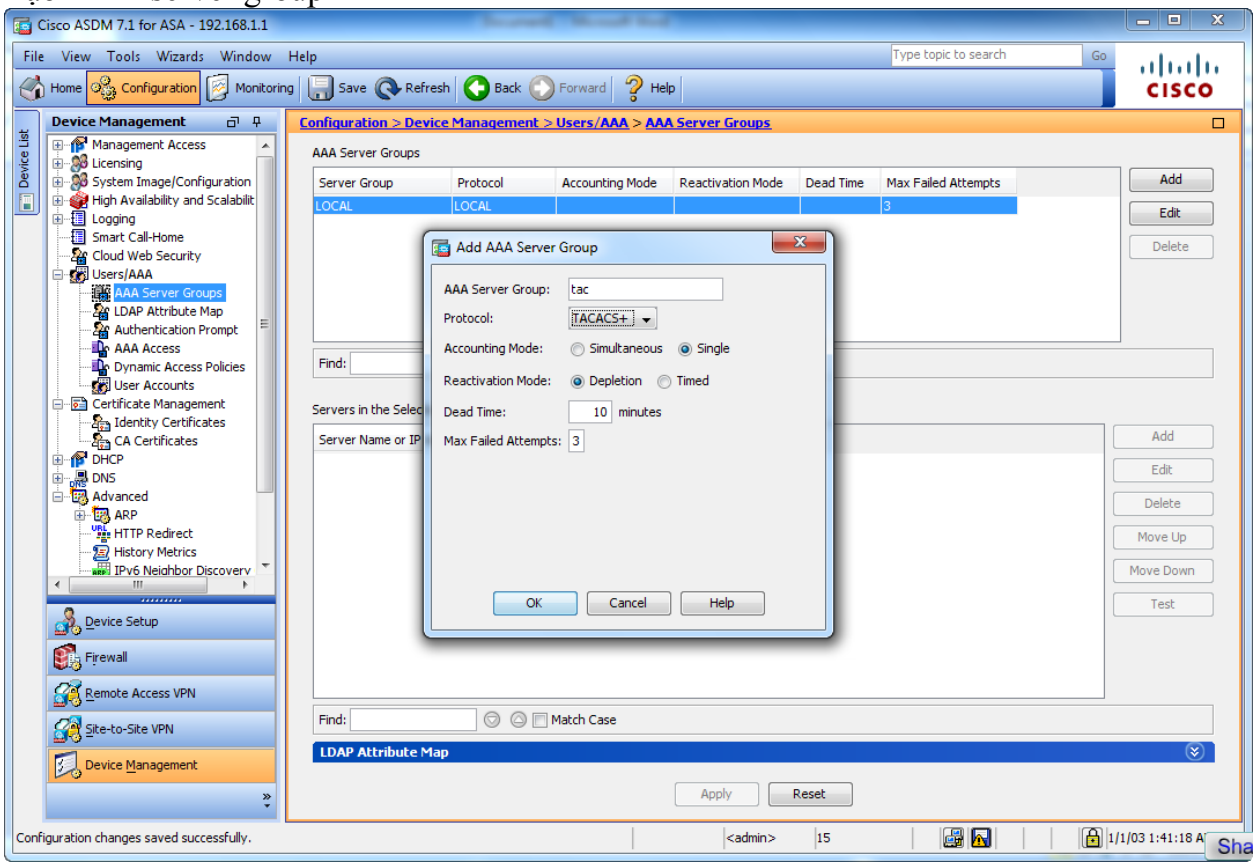
Tạo username và password để truy cập ASA



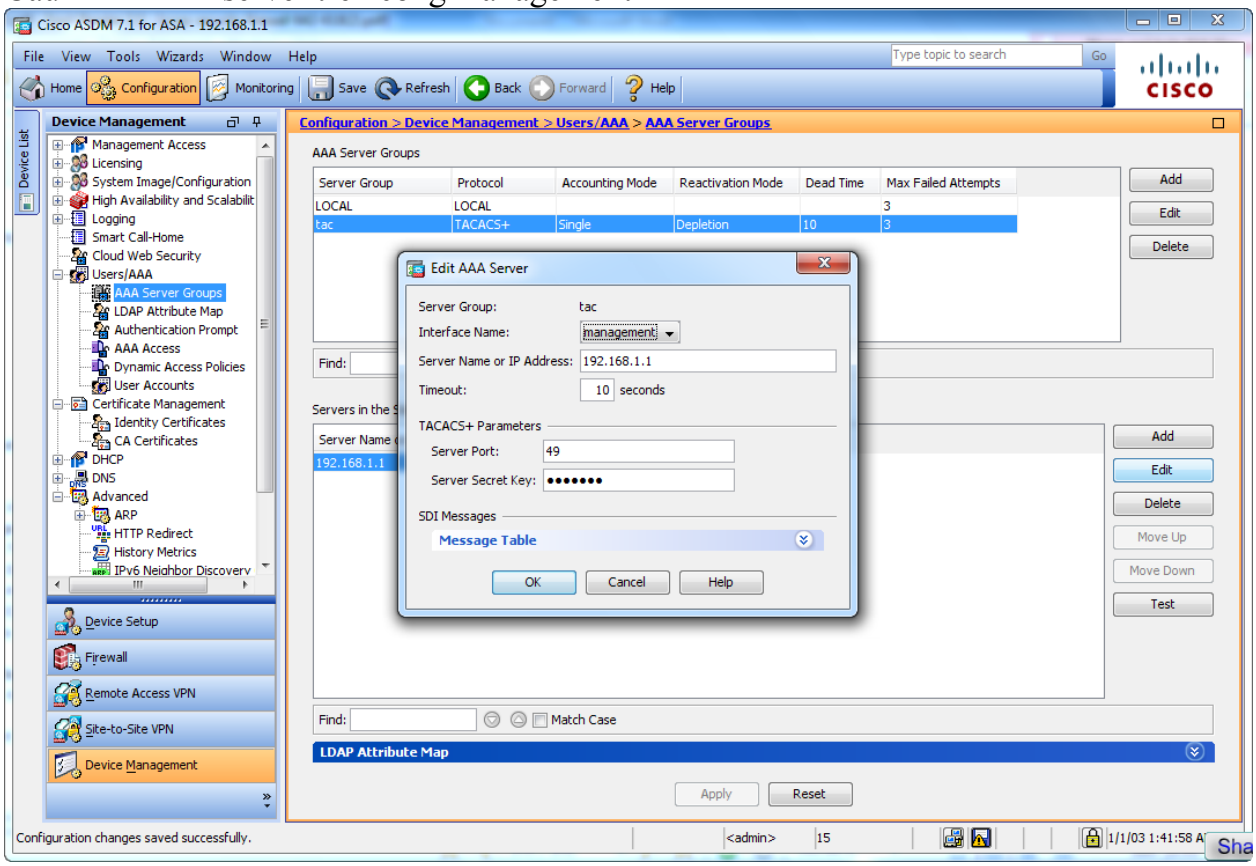
Tạo username và password bằng CLI



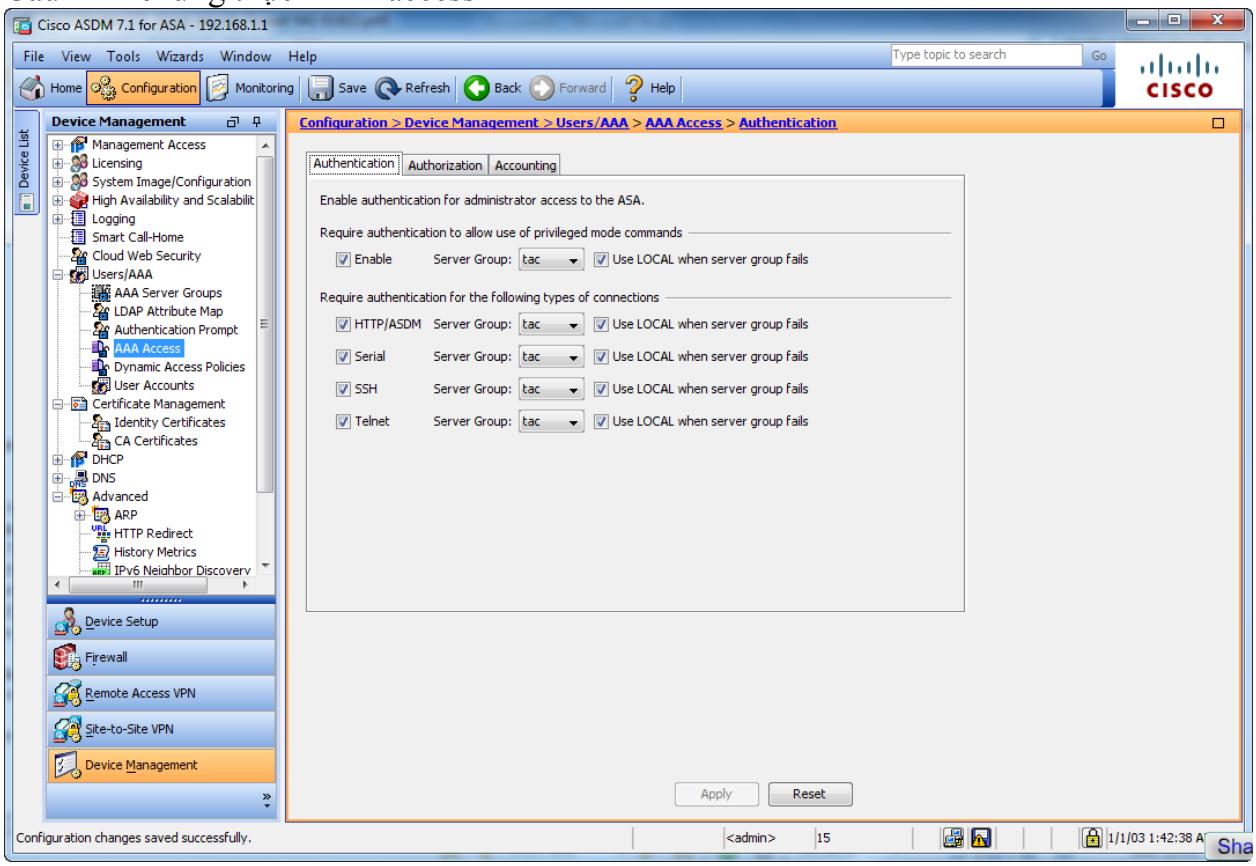
Tạo AAA server group



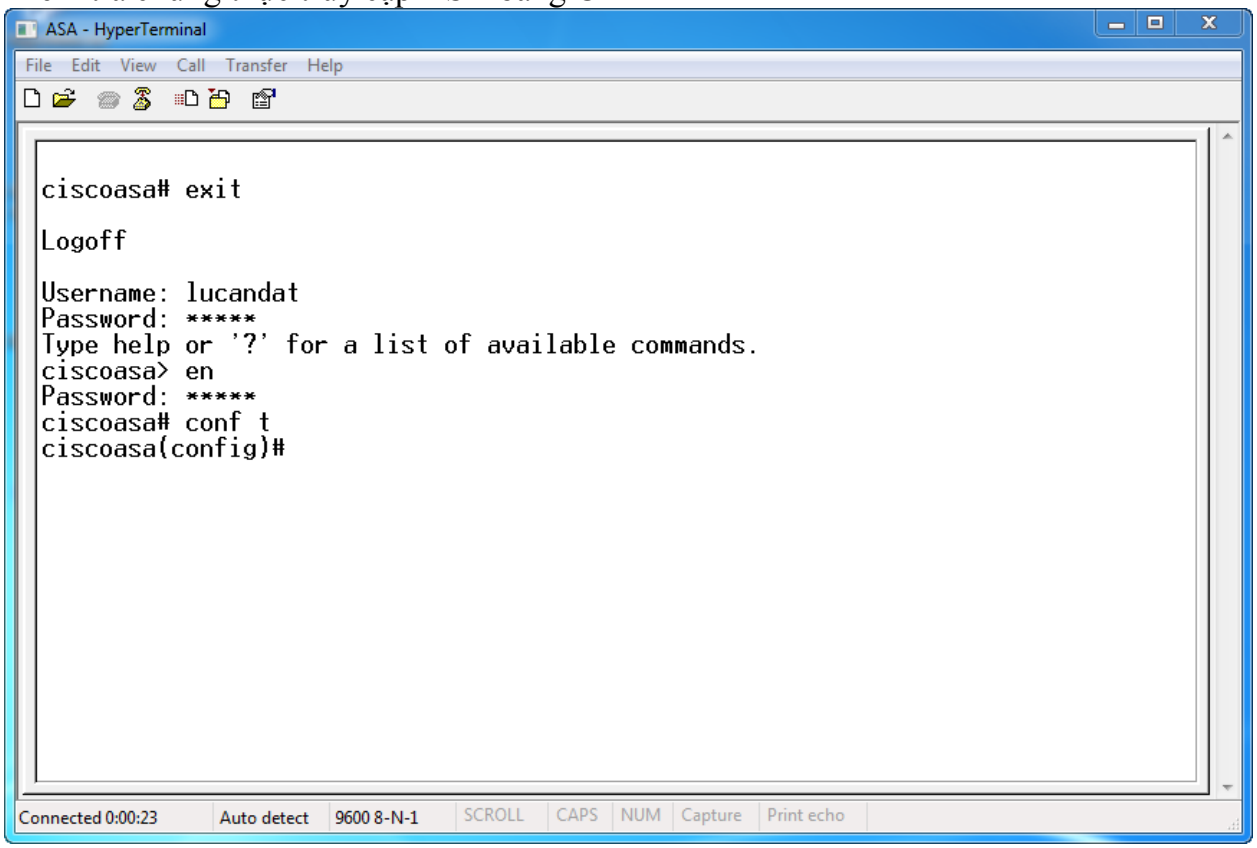
Cấu hình AAA server trên cổng management

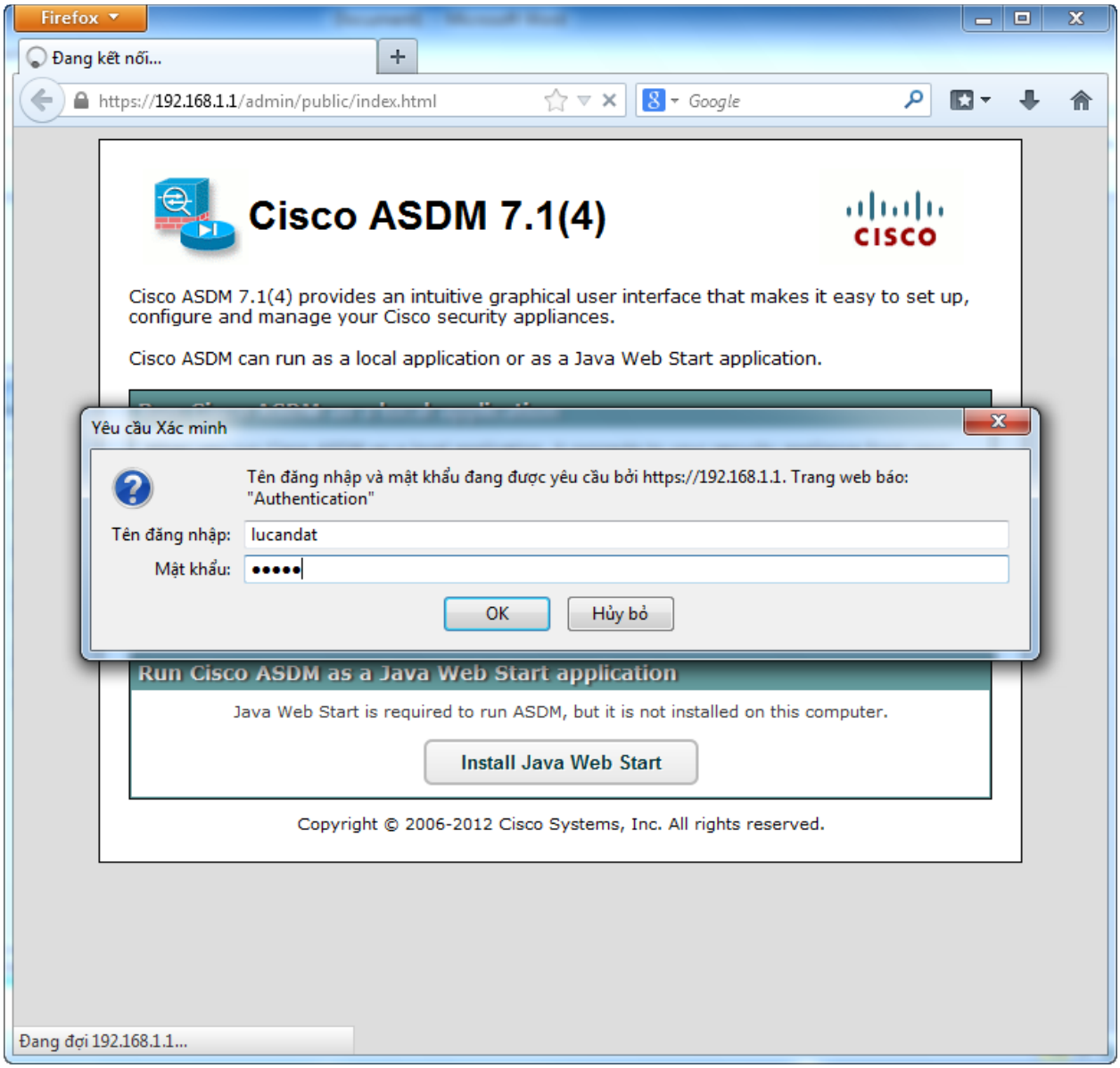


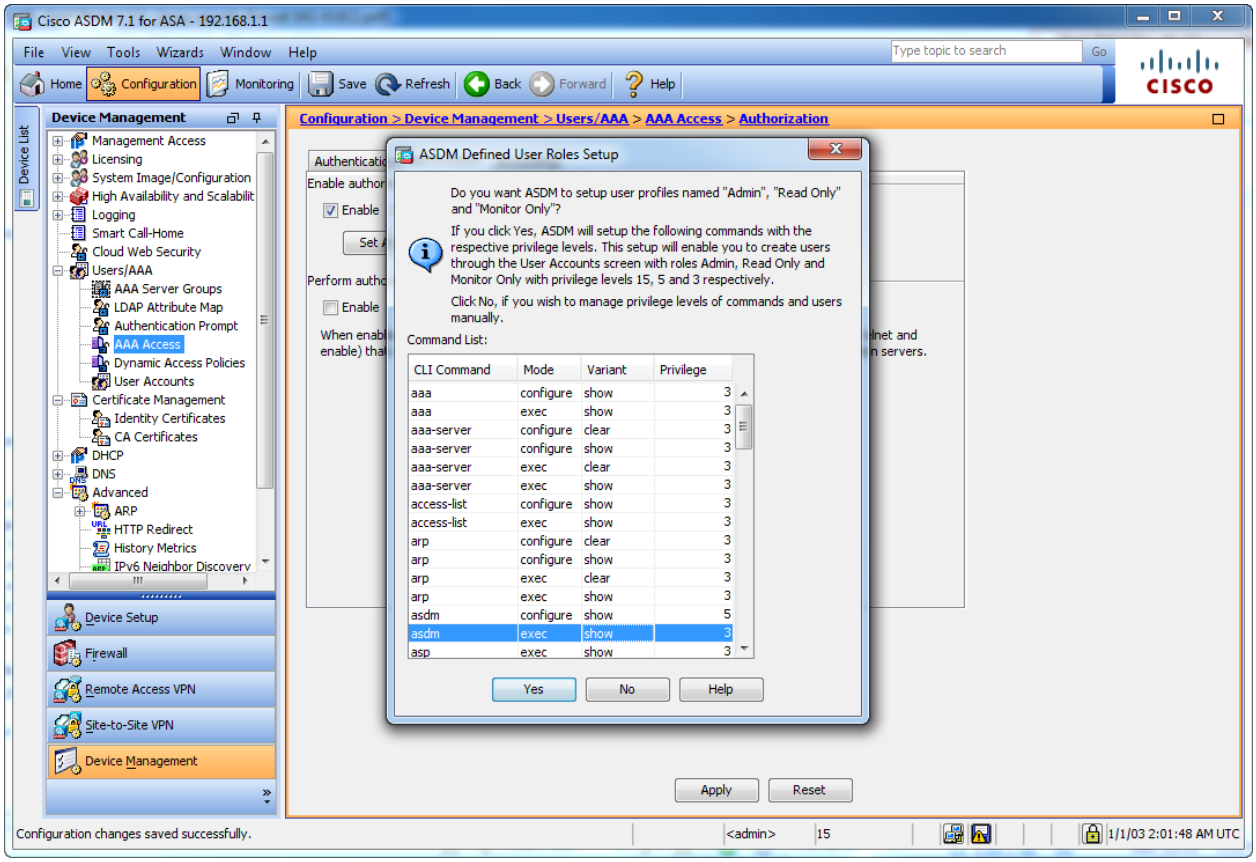
Cấu hình chứng thực AAA access

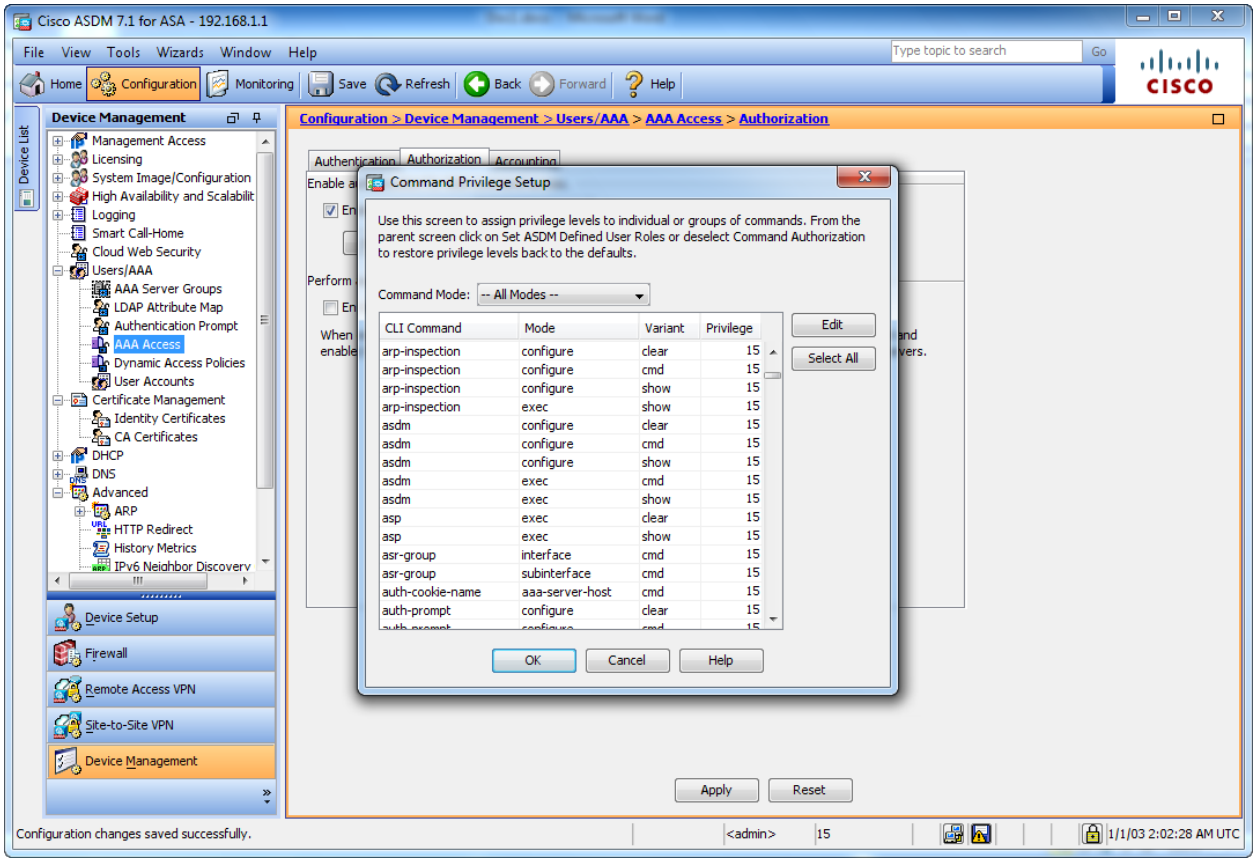


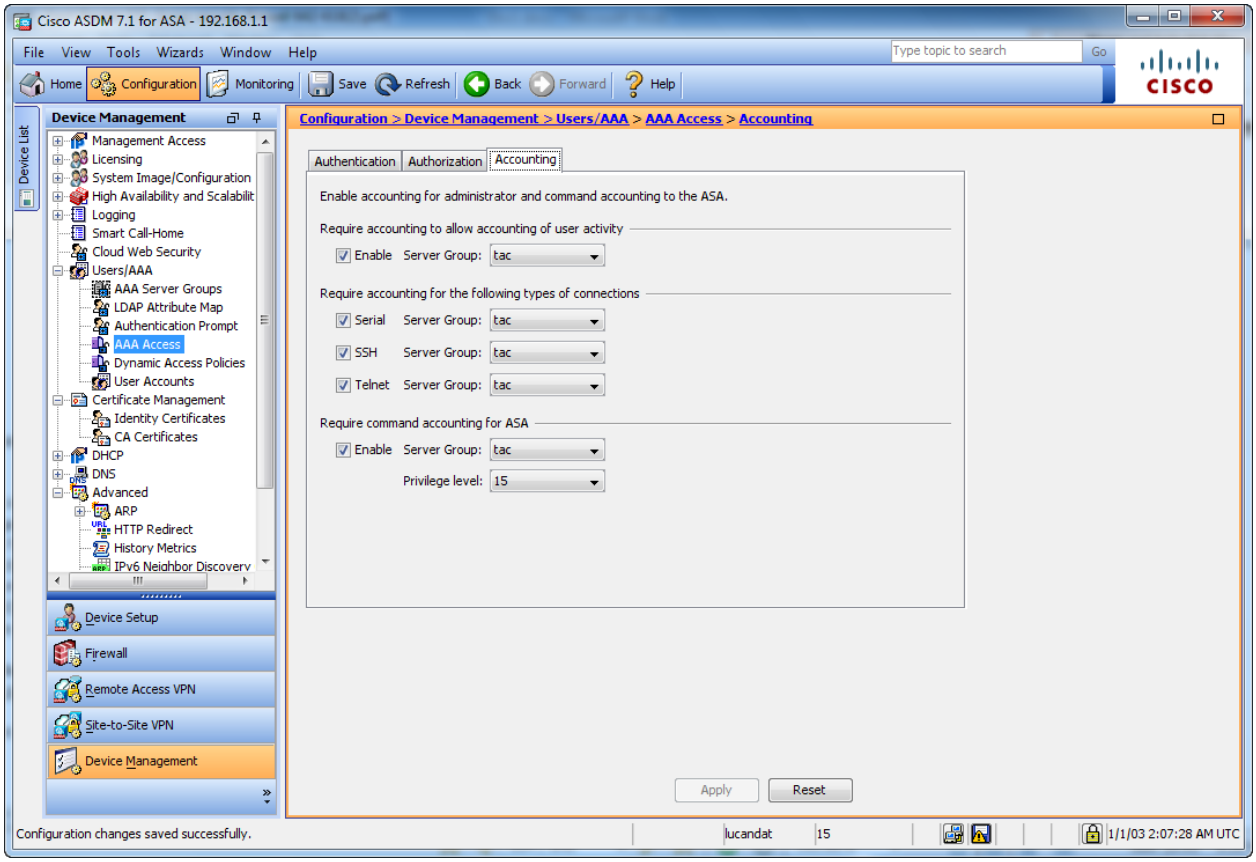
Kiểm tra chứng thực truy cập ASA bằng CLI

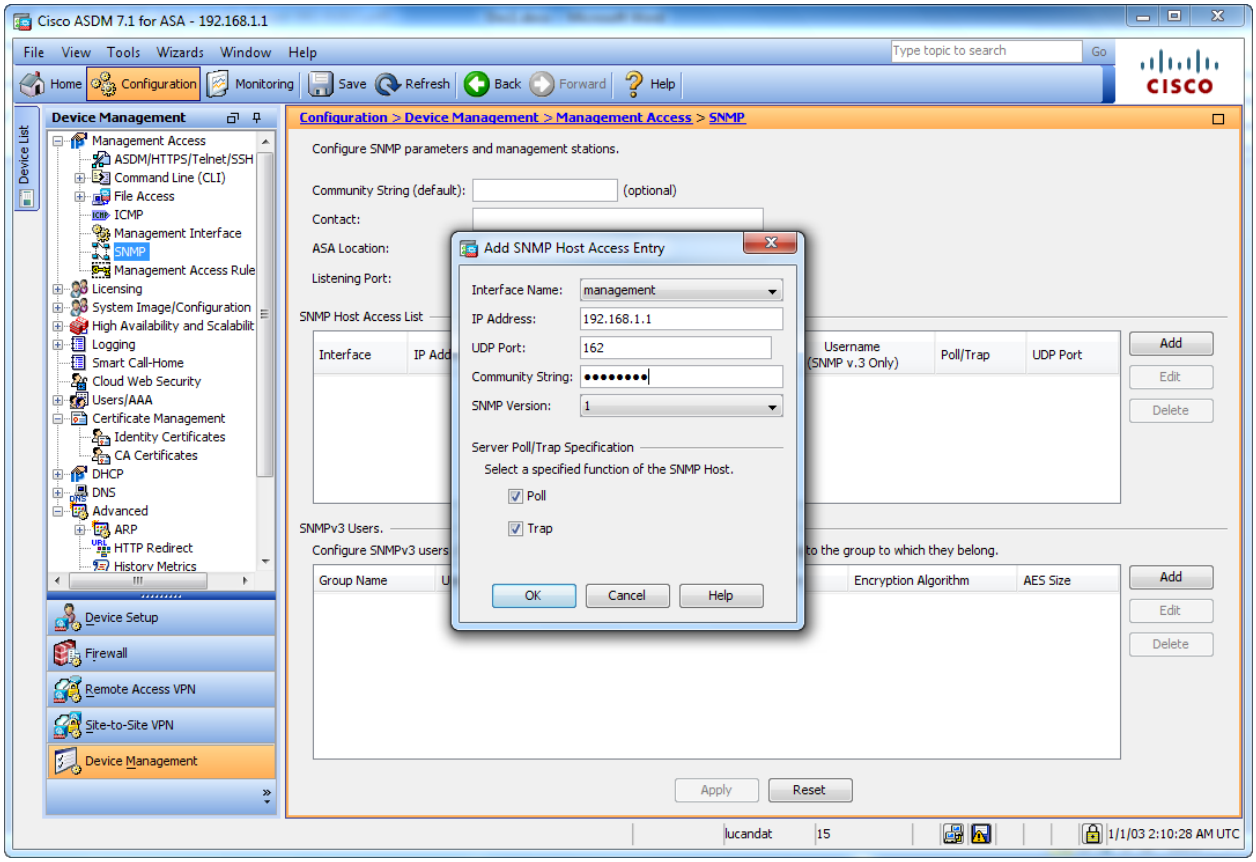


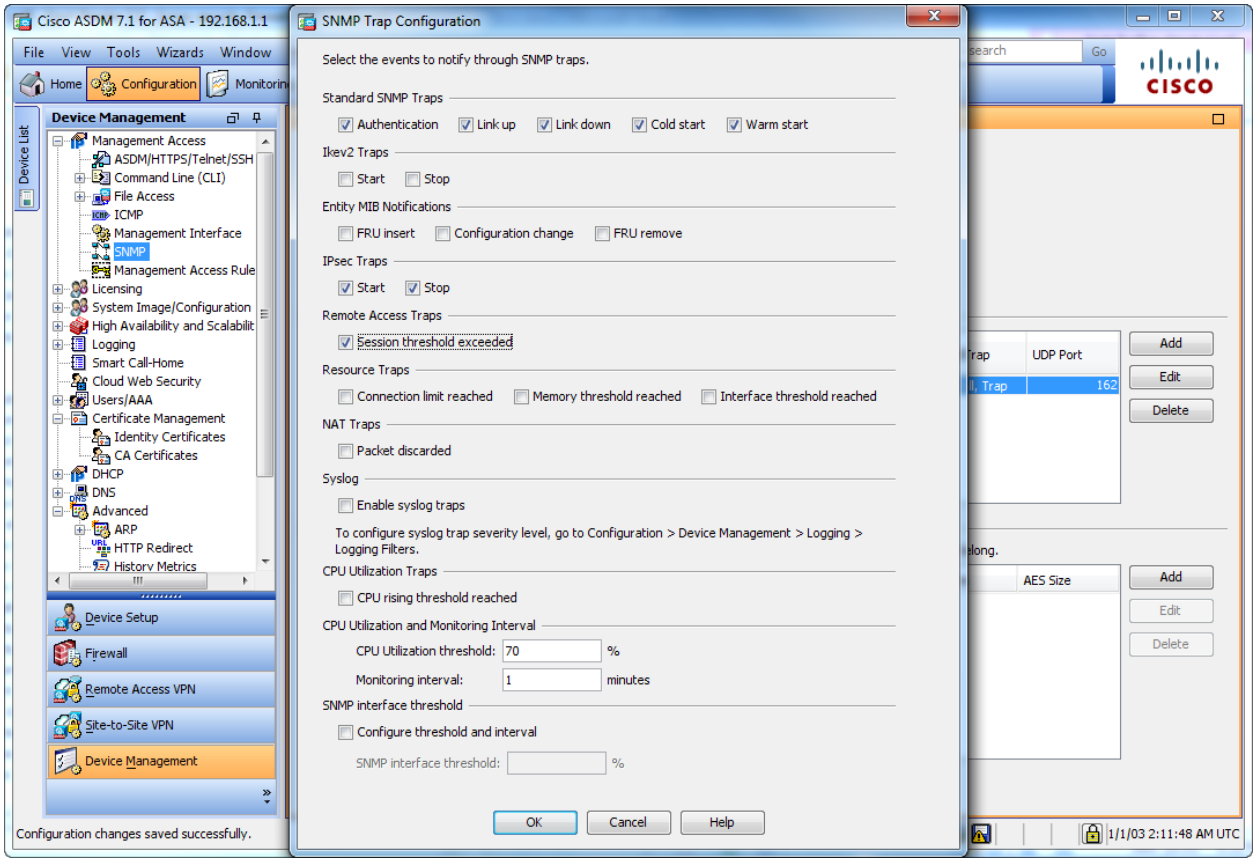

Firefox
Đang kết nối...
https://192.168.1.1/admin/public/index.html
Google
Cisco ASDM 7.1(4)
CISCO
Cisco ASDM 7.1(4) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.
Cisco ASDM can run as a local application or as a Java Web Start application.
Yêu cầu Xác minh
Tên đăng nhập và mật khẩu đang được yêu cầu bởi https://192.168.1.1. Trang web báo: "Authentication"
Tên đăng nhập:
lucandat
Mật khẩu:
OK
Hủy bỏ
Run Cisco ASDM as a Java Web Start application
Java Web Start is required to run ASDM, but it is not installed on this computer.
Install Java Web Start
Copyright © 2006-2012 Cisco Systems, Inc. All rights reserved.
Đang đợi 192.168.1.1...

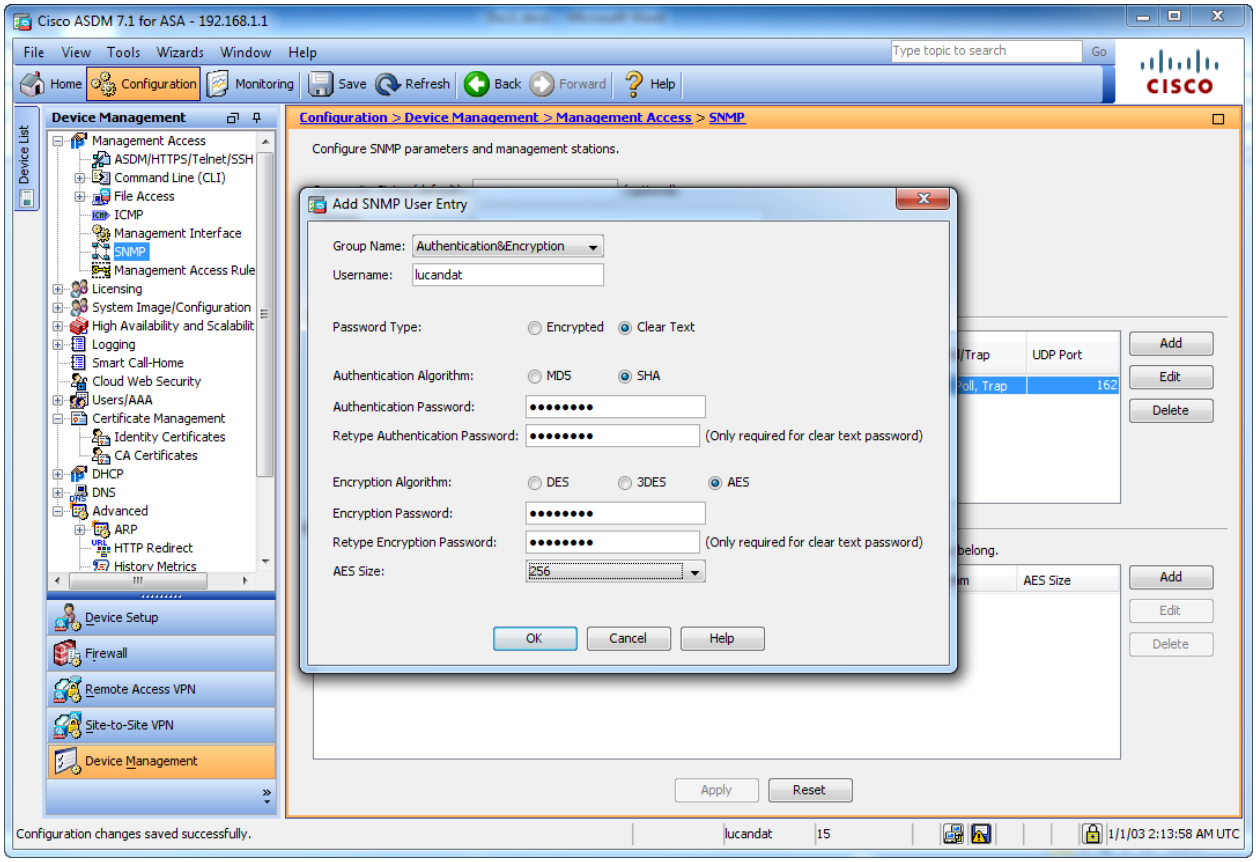

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Certificate Management
Identity Certificates
CA Certificates
DHCP
DNS
Advanced
ARP
HTTP Redirect
History Metrics
IPv6 Neighbor Discoverv
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authorization
Authenticatic
Enable author
Enable
Set
Perform autho
Enable
When enabl
enable) tha
net and
n servers.
Apply
Reset
ASDM Defined User Roles Setup
Do you want ASDM to setup user profiles named "Admin", "Read Only" and "Monitor Only"?
If you click Yes, ASDM will setup the following commands with the respective privilege levels. This setup will enable you to create users through the User Accounts screen with roles Admin, Read Only and Monitor Only with privilege levels 15, 5 and 3 respectively.
Click No, if you wish to manage privilege levels of commands and users manually.
Command List:
CLI Command Mode Variant Privilege
aaa configure show 3
aaa exec show 3
aaa-server configure clear 3
aaa-server configure show 3
aaa-server exec clear 3
aaa-server exec show 3
access-list configure show 3
access-list exec show 3
arp configure clear 3
arp configure show 3
arp exec clear 3
arp exec show 3
asdm configure show 5
asdm exec show 3
asp exec show 3
Yes
No
Help
Configuration changes saved successfully.
<admin>
15
1/1/03 2:01:48 AM UTC


Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Certificate Management
Identity Certificates
CA Certificates
DHCP
DNS
Advanced
ARP
HTTP Redirect
History Metrics
IPv6 Neighbor Discoverv
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authorization
Authentication Authorization Accounting
Command Privilege Setup
Use this screen to assign privilege levels to individual or groups of commands. From the parent screen click on Set ASDM Defined User Roles or deselect Command Authorization to restore privilege levels back to the defaults.
Command Mode: -- All Modes --
CLI Command Mode Variant Privilege
arp-inspection configure clear 15
arp-inspection configure cmd 15
arp-inspection configure show 15
arp-inspection exec show 15
asdm configure clear 15
asdm configure cmd 15
asdm configure show 15
asdm exec cmd 15
asdm exec show 15
asp exec clear 15
asp exec show 15
asr-group interface cmd 15
asr-group subinterface cmd 15
auth-cookie-name aaa-server-host cmd 15
auth-prompt configure clear 15
Edit
Select All
OK
Cancel
Help
Apply
Reset
Configuration changes saved successfully.
<admin>
15
1/1/03 2:02:28 AM UTC

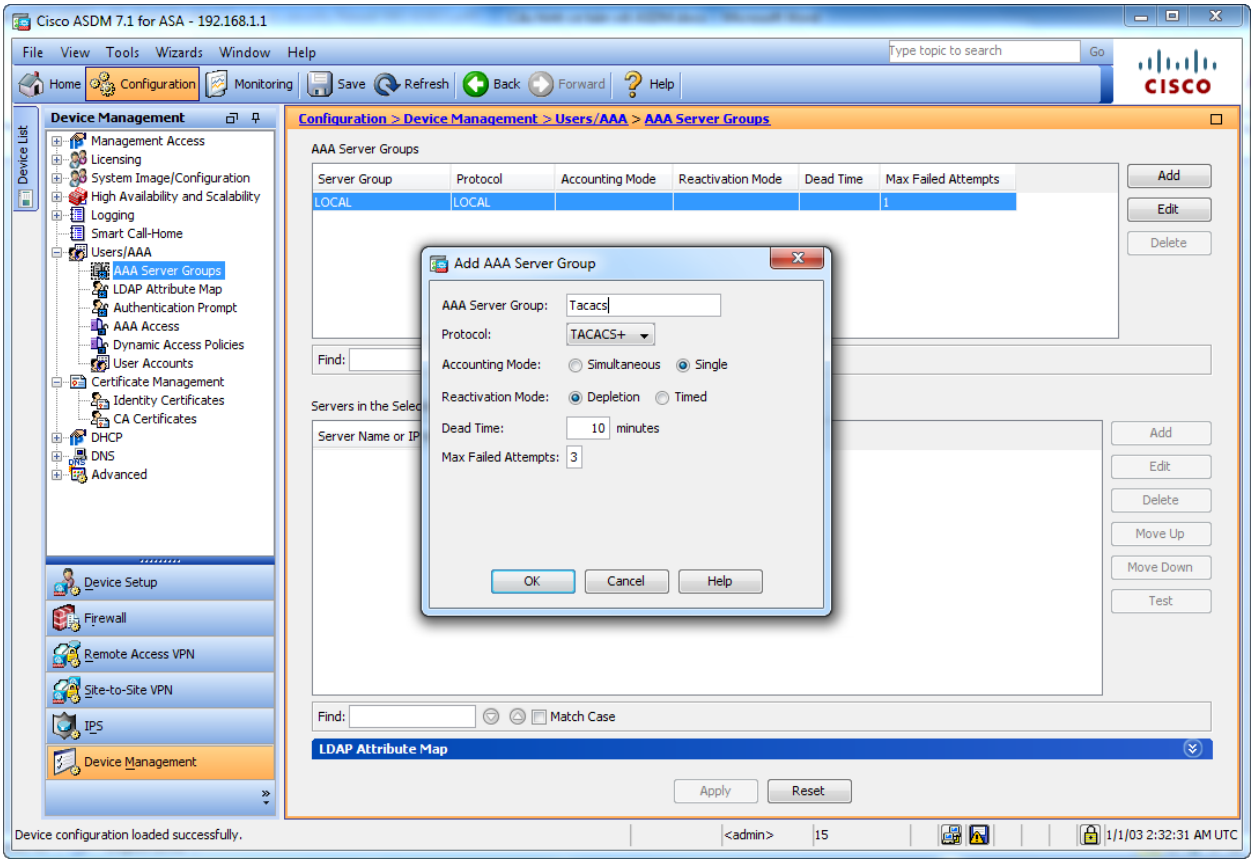

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Certificate Management
Identity Certificates
CA Certificates
DHCP
DNS
Advanced
ARP
HTTP Redirect
History Metrics
IPv6 Neighbor Discoverv
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Accounting
Authentication
Authorization
Accounting
Enable accounting for administrator and command accounting to the ASA.
Require accounting to allow accounting of user activity
Enable
Server Group:
tac
Require accounting for the following types of connections
Serial
SSH
Telnet
Require command accounting for ASA
Privilege level:
15
Apply
Reset
Configuration changes saved successfully.
lucandat
15
1/1/03 2:07:28 AM UTC

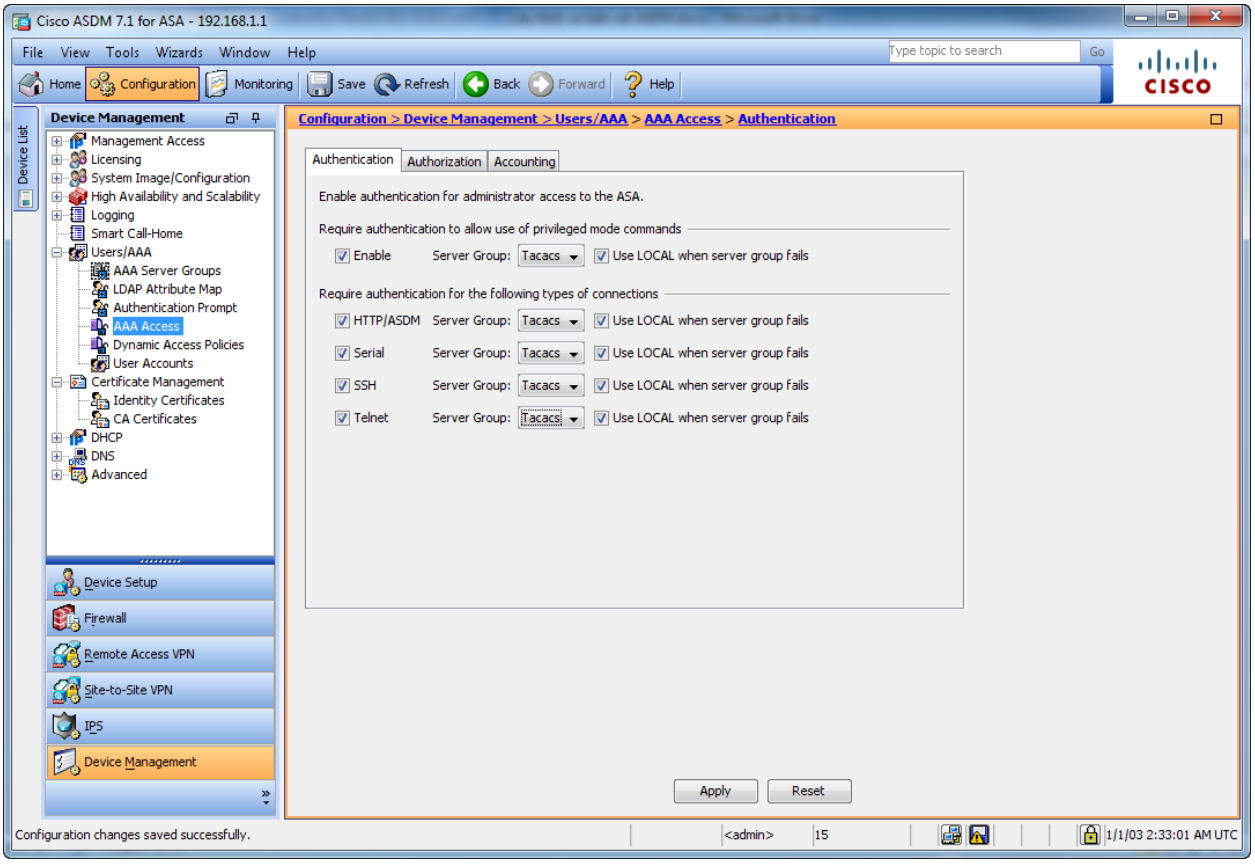

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device Management
Management Access
ASDM/HTTPS/Telnet/SSH
Command Line (CLI)
File Access
ICMP
Management Interface
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
Certificate Management
Identity Certificates
CA Certificates
DHCP
DNS
Advanced
ARP
HTTP Redirect
History Metrics
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Management > Management Access > SNMP
Configure SNMP parameters and management stations.
Community String (default):
(optional)
Contact:
ASA Location:
Listening Port:
SNMP Host Access List
Interface
Username (SNMP v.3 Only)
Poll/Trap
UDP Port
Add
Edit
Delete
SNMPv3 Users.
Configure SNMPv3 users
to the group to which they belong.
Group Name
Encryption Algorithm
AES Size
Add
Edit
Delete
Apply
Reset
Add SNMP Host Access Entry
Interface Name: management
IP Address: 192.168.1.1
UDP Port: 162
Community String:
SNMP Version: 1
Server Poll/Trap Specification
Select a specified function of the SNMP Host.
Poll
Trap
OK
Cancel
Help
lucandat
15
1/1/03 2:10:28 AM UTC


Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window
Home Configuration Monitoring
Device Management
Management Access
ASDM/HTTPS/Telnet/SSH
Command Line (CLI)
File Access
ICMP
Management Interface
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
Certificate Management
Identity Certificates
CA Certificates
DHCP
DNS
Advanced
ARP
HTTP Redirect
History Metrics
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration changes saved successfully.
SNMP Trap Configuration
Select the events to notify through SNMP traps.
Standard SNMP Traps
Authentication
Link up
Link down
Cold start
Warm start
Ikev2 Traps
Start
Stop
Entity MIB Notifications
FRU insert
Configuration change
FRU remove
IPsec Traps
Start
Stop
Remote Access Traps
Session threshold exceeded
Resource Traps
Connection limit reached
Memory threshold reached
Interface threshold reached
NAT Traps
Packet discarded
Syslog
Enable syslog traps
To configure syslog trap severity level, go to Configuration > Device Management > Logging > Logging Filters.
CPU Utilization Traps
CPU rising threshold reached
CPU Utilization and Monitoring Interval
CPU Utilization threshold: 70 %
Monitoring interval: 1 minutes
SNMP interface threshold
Configure threshold and interval
SNMP interface threshold: %
OK
Cancel
Help
Search
Go
CISCO
Trap
UDP Port
Trap
162
Add
Edit
Delete
AES Size
Add
Edit
Delete
1/1/03 2:11:48 AM UTC

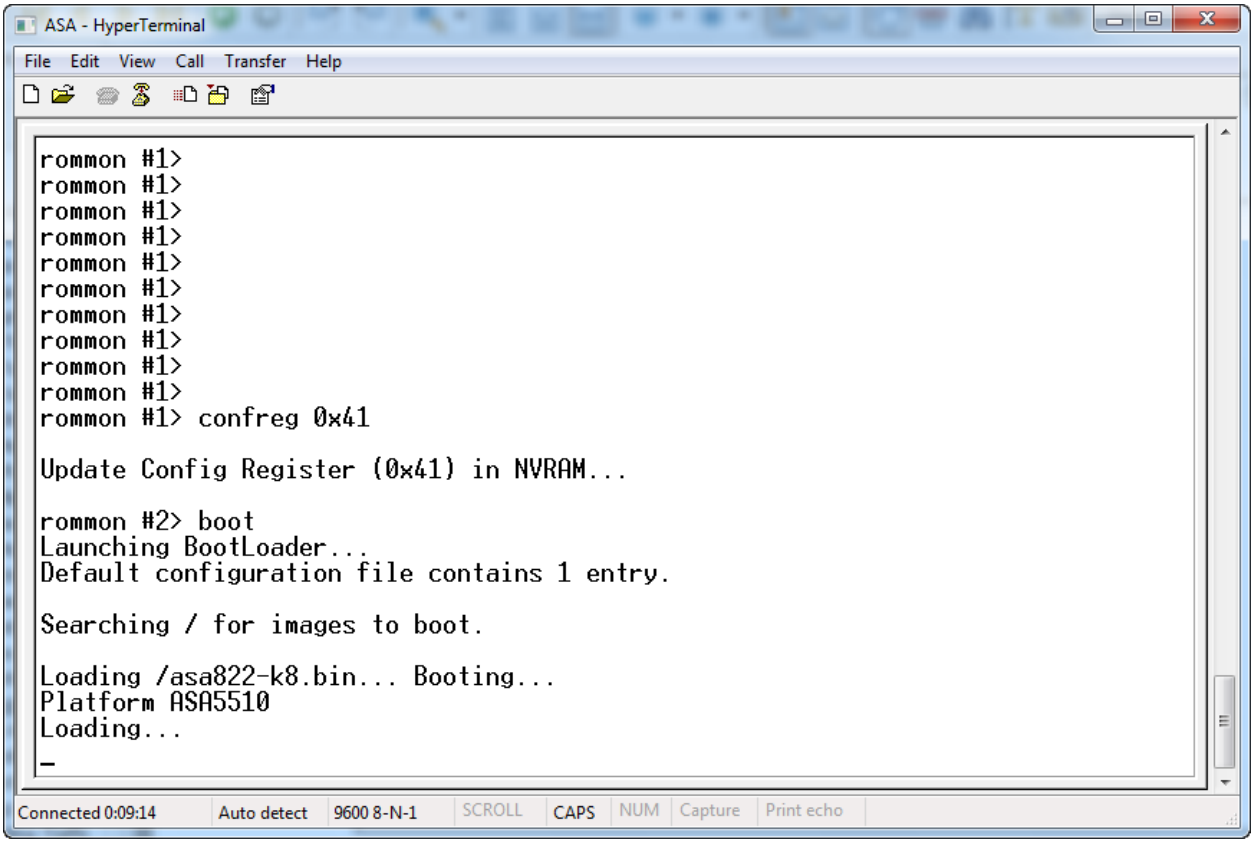

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
ASDM/HTTPS/Telnet/SSH
Command Line (CLI)
File Access
ICMP
Management Interface
SNMP
Management Access Rule
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
Certificate Management
Identity Certificates
CA Certificates
DHCP
DNS
Advanced
ARP
HTTP Redirect
History Metrics
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Management > Management Access > SNMP
Configure SNMP parameters and management stations.
Add SNMP User Entry
Group Name: Authentication&Encryption
Username: lucandat
Password Type: Encrypted Clear Text
Authentication Algorithm: MD5 SHA
Authentication Password: ••••••••
Retype Authentication Password: ••••••••
(Only required for clear text password)
Encryption Algorithm: DES 3DES AES
Encryption Password: ••••••••
Retype Encryption Password: ••••••••
(Only required for clear text password)
AES Size: 256
OK
Cancel
Help
/Trap
UDP Port
oll, Trap
162
Add
Edit
Delete
belong.
AES Size
Add
Edit
Delete
Apply
Reset
Configuration changes saved successfully.
lucandat
15
1/1/03 2:13:58 AM UTC

Tạo AAA Server GROUP

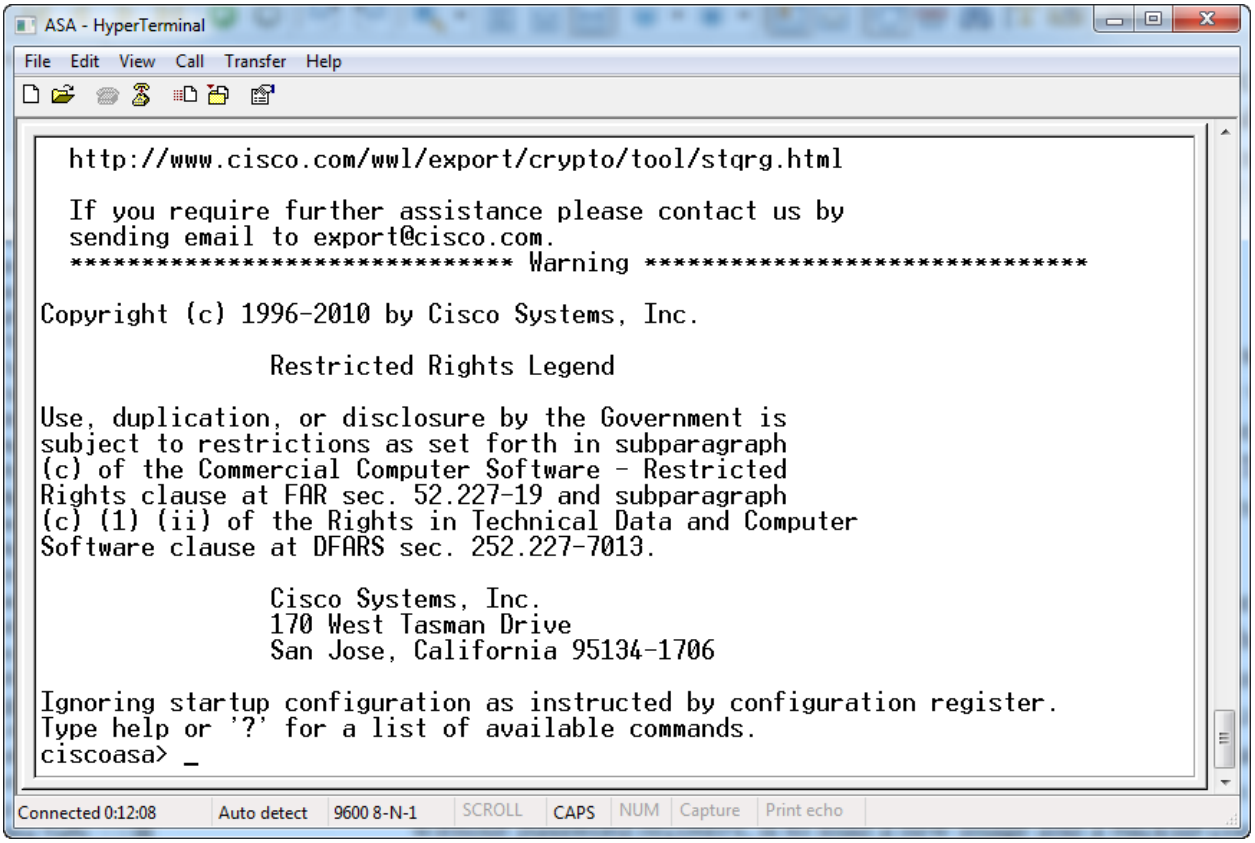



Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalability
Logging
Smart Call-Home
Users/AAA
AAA Server Groups
LDAP Attribute Map
Authentication Prompt
AAA Access
Dynamic Access Policies
User Accounts
Certificate Management
Identity Certificates
CA Certificates
DHCP
DNS
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
IPS
Device Management
Configuration > Device Management > Users/AAA > AAA Access > Authentication
Authentication
Authorization
Accounting
Enable authentication for administrator access to the ASA.
Require authentication to allow use of privileged mode commands
Enable
Server Group:
Tacacs
Use LOCAL when server group fails
Require authentication for the following types of connections
HTTP/ASDM
Serial
SSH
Telnet
Apply
Reset
Configuration changes saved successfully.
<admin>
15
1/1/03 2:33:01 AM UTC

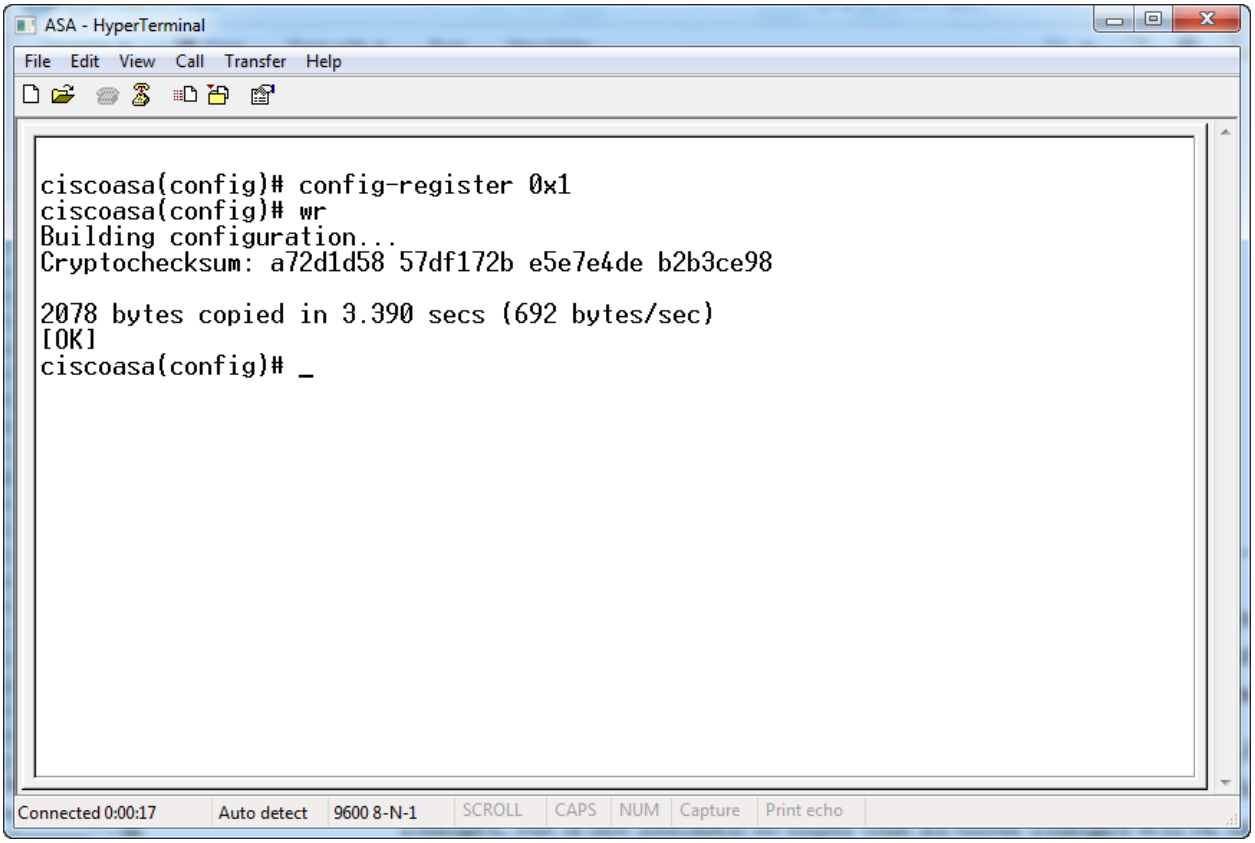
Khôi phục mật khẩu bằng cách nhấn ESC hay Break khi khởi động ASA



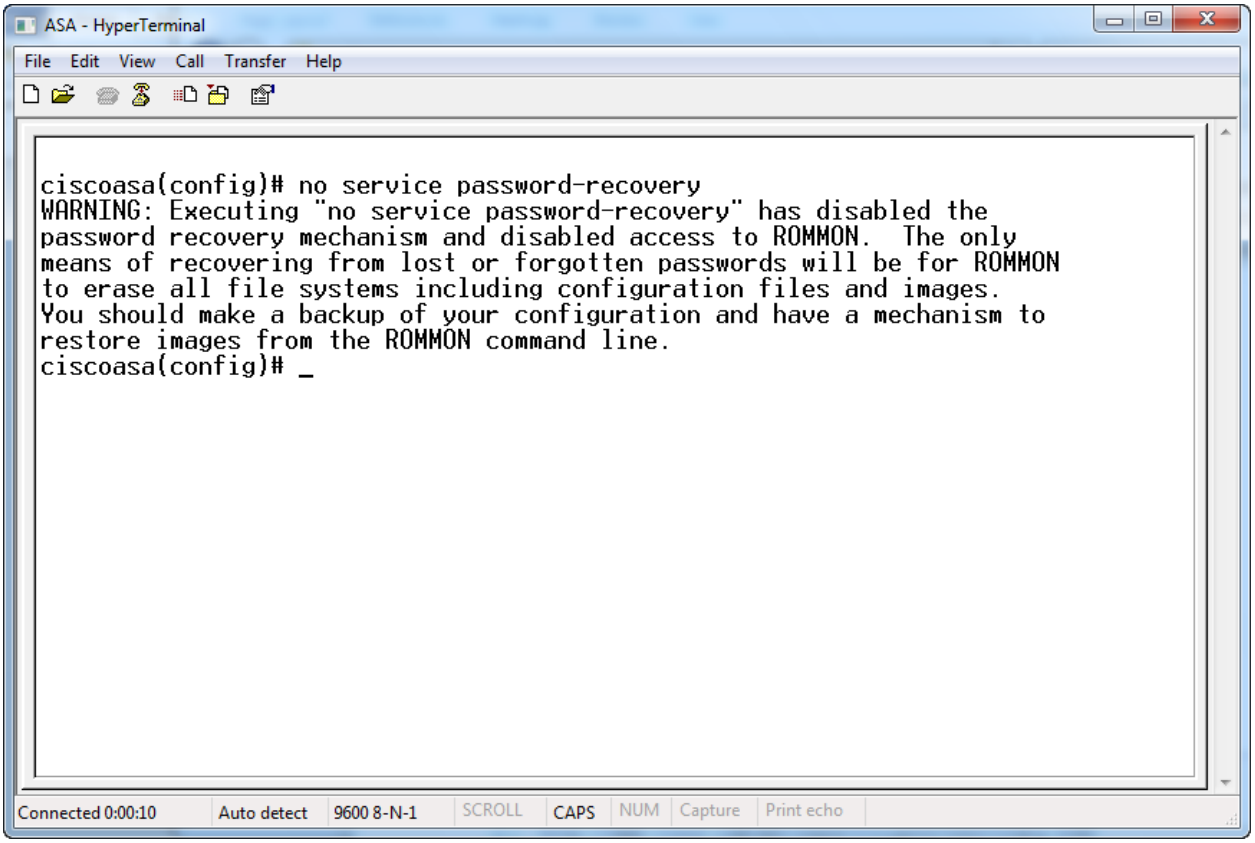
Giao diện sau khi phục hồi password



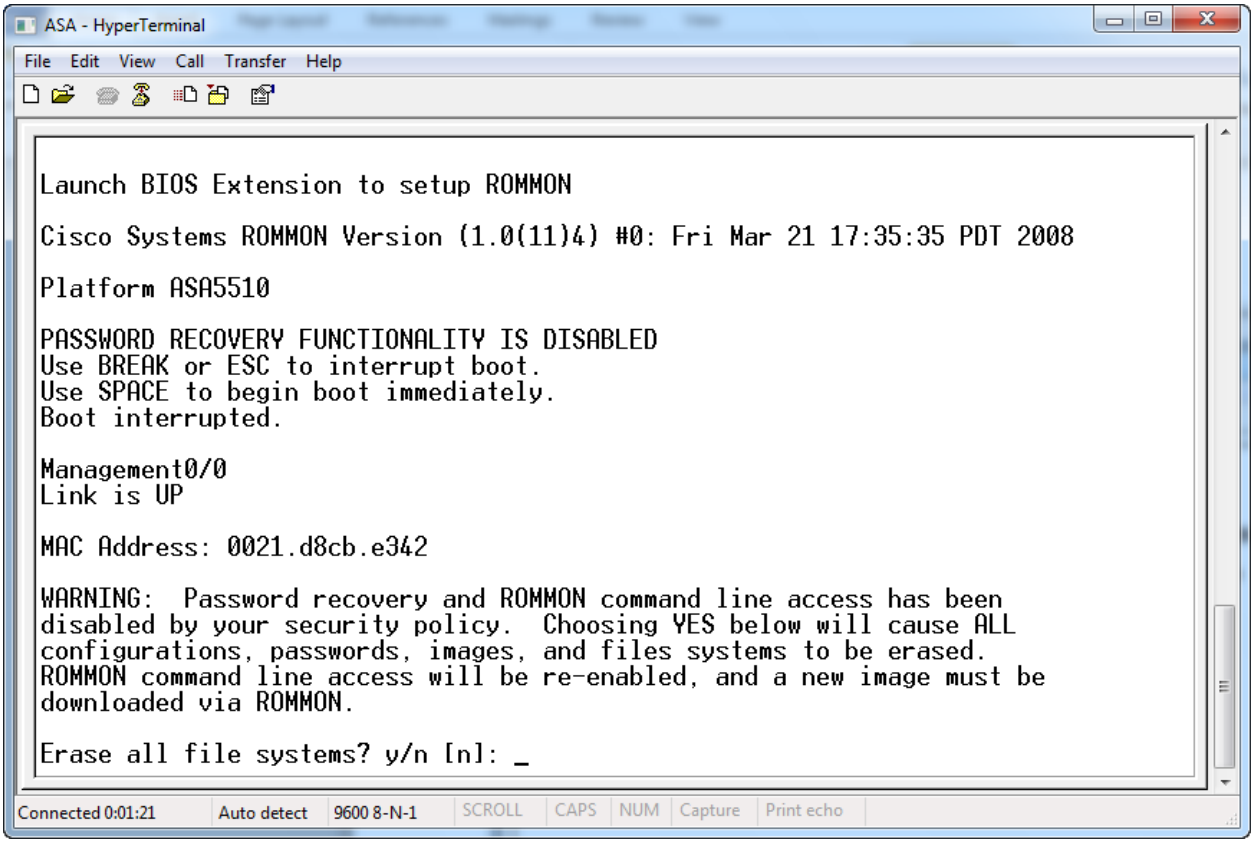
Cấu hình cho phép lần sau khởi động bình thường



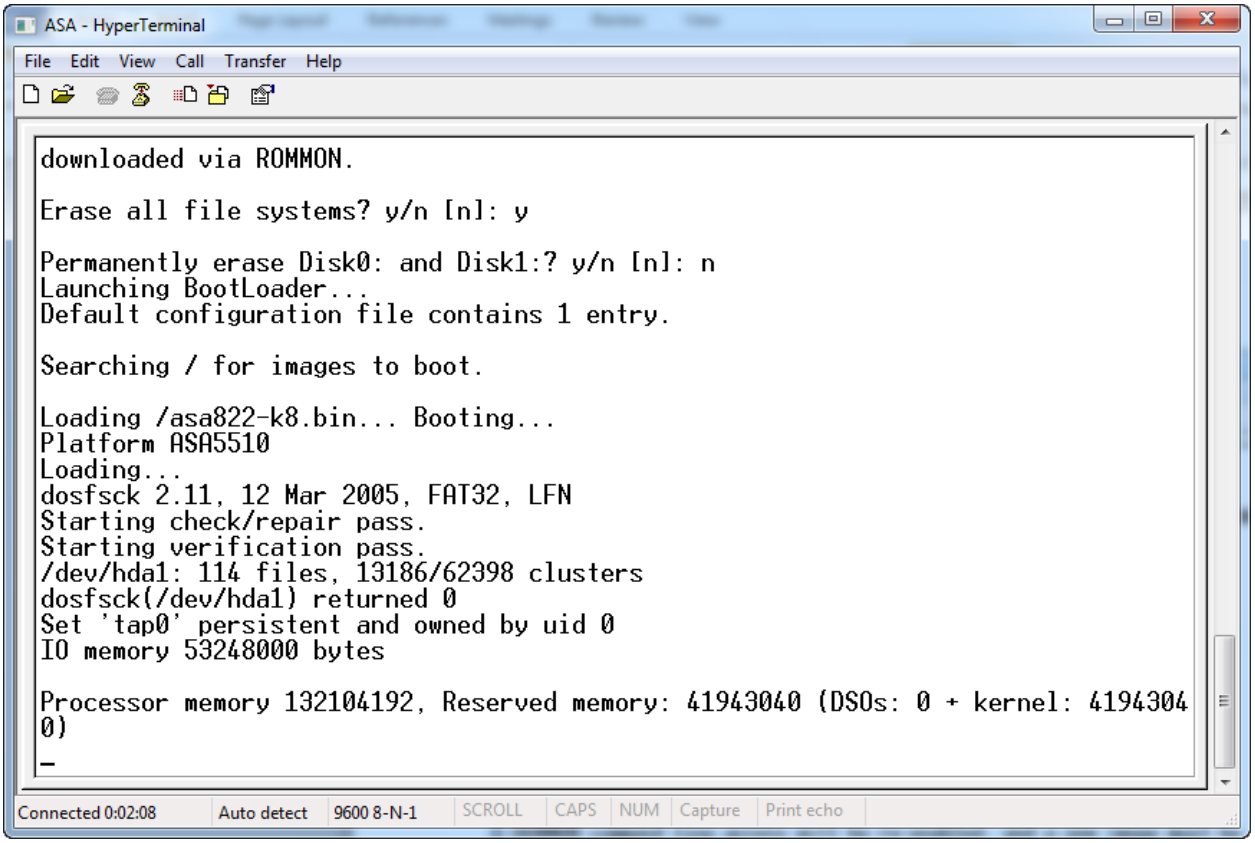
Cấu hình service password-recovery



Sau khi cấu hinh no service password-recovery, ASA bắt buộc user phải xoá tất cả cấu hình.



ASA khởi động lại



ASA sau khi boot xong sẽ trở lại giao diện cấu hình mặc định không có password