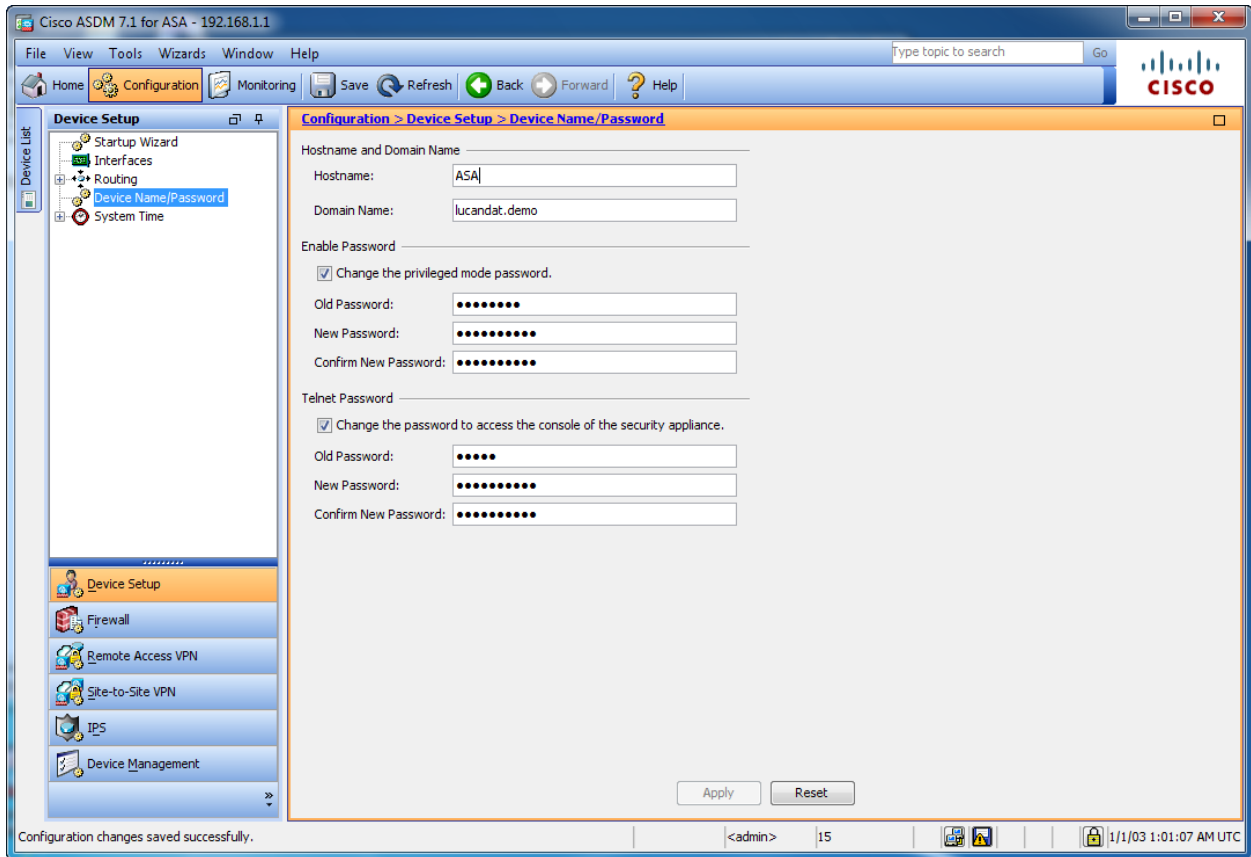
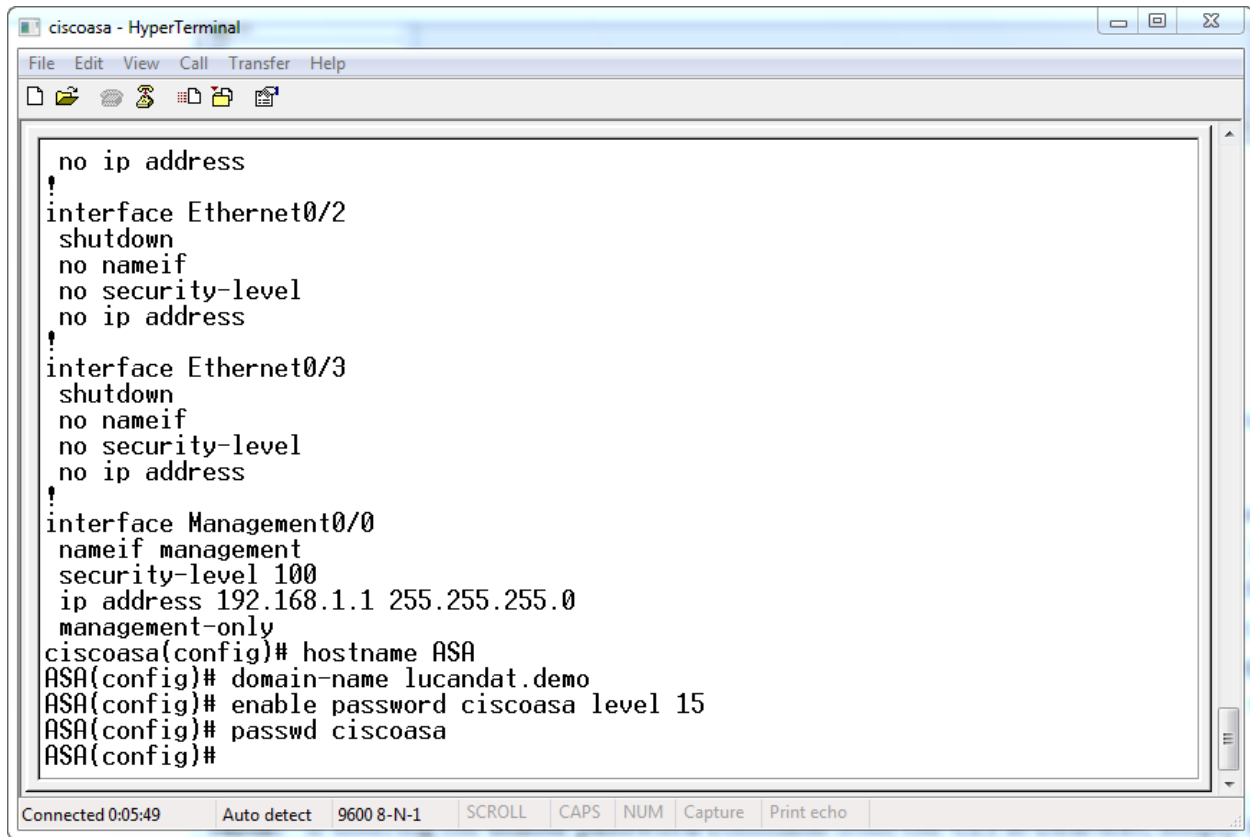


Cấu hình ASA cơ bản với ASDM



cấu hình ASA cơ bản với CLI



```
ciscoasa - HyperTerminal
File Edit View Call Transfer Help
no ip address
!
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
management-only
ciscoasa(config)# hostname ASA
ASA(config)# domain-name lucandat.demo
ASA(config)# enable password ciscoasa level 15
ASA(config)# passwd ciscoasa
ASA(config)#
Connected 0:05:49 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Kiểm tra thông tin cơ bản với ASDM

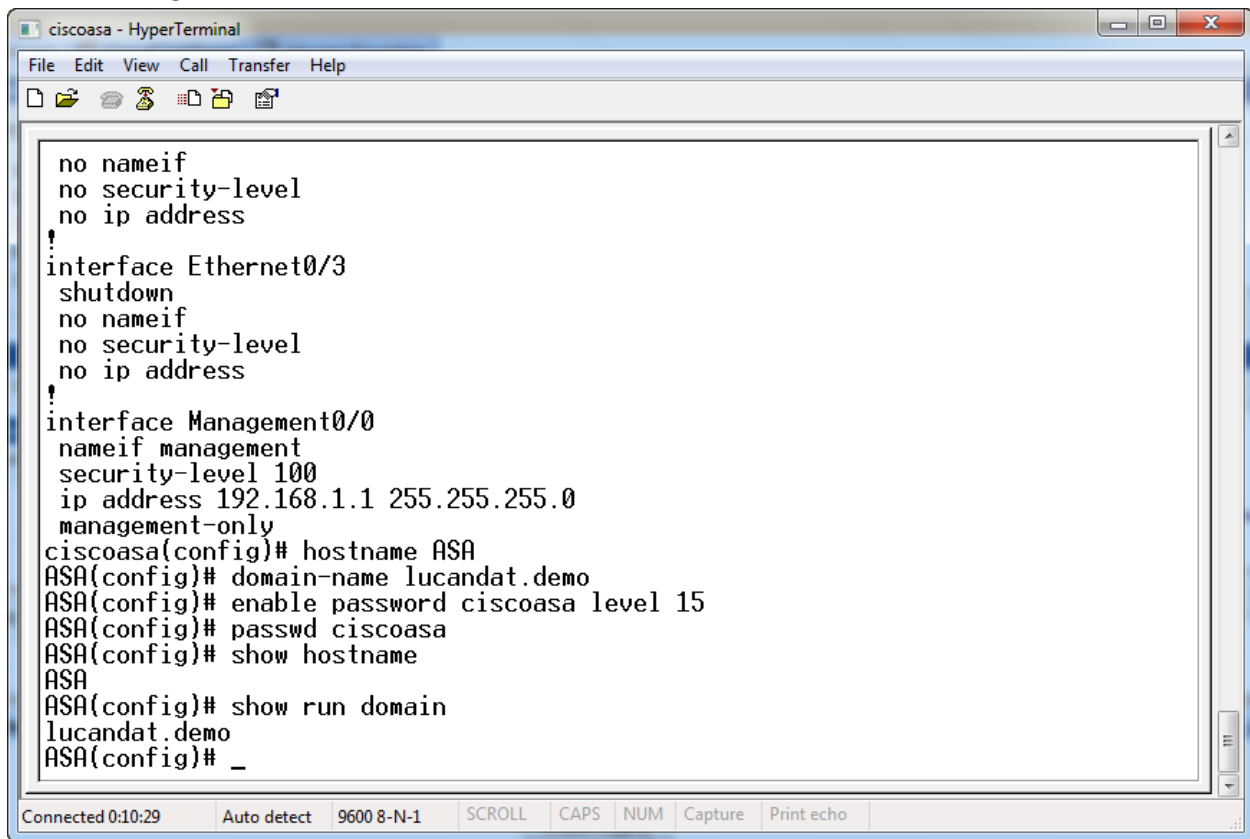
The screenshot displays the Cisco ASDM 7.1 for ASA interface for the device 192.168.1.1. The interface includes a menu bar (File, View, Tools, Wizards, Window, Help) and a navigation bar with Home, Configuration, Monitoring, Save, Refresh, Back, Forward, and Help buttons. The main content area is divided into several sections:

- Device Information:** Shows general and license details for the device. Host Name: **ASA.lucandat.demo**. ASA Version: **8.2(2)**. ASDM Version: **7.1(3)**. Firewall Mode: **Routed**. Total Flash: **256 MB**. Device Uptime: **0d 1h 11m 37s**. Device Type: **ASA 5510, SSM-10**. Context Mode: **Single**. Total Memory: **256 MB**.
- Interface Status:** A table showing the status of the 'management' interface.

Interface	IP Address/Mask	Line	Link	Kbps
management	192.168.1.1/24	+	up	5
- VPN Sessions:** Shows 0 IPsec, 0 Clientless SSL VPN, and 0 AnyConnect Client sessions.
- System Resources Status:** Displays CPU Usage (percent) and Memory Usage (MB) graphs. CPU usage is currently at 0%.
- Traffic Status:** Shows Connections Per Second Usage and Interface Traffic Usage (Kbps) graphs. The UDP, TCP, and Total connection counts are all 0.
- Latest ASDM Syslog Messages:** A message indicating that ASDM logging is disabled and providing an 'Enable Logging' button.

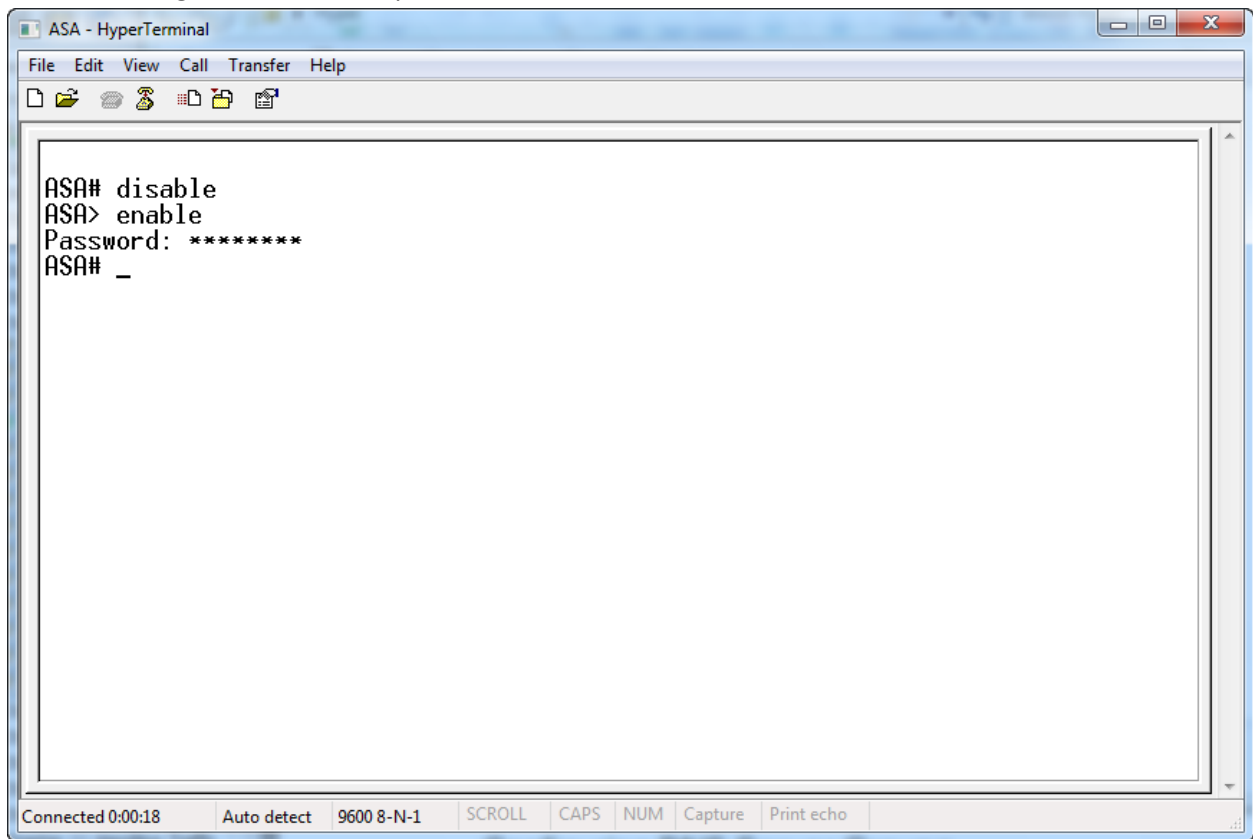
The bottom status bar shows the user is logged in as '<admin>' with 15 sessions, and the time is 1/1/03 1:12:37 AM UTC.

Kiểm tra thông tin cơ bản với CLI



```
ciscoasa - HyperTerminal
File Edit View Call Transfer Help
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
nameif management
security-level 100
ip address 192.168.1.1 255.255.255.0
management-only
ciscoasa(config)# hostname ASA
ASA(config)# domain-name lucandat.demo
ASA(config)# enable password ciscoasa level 15
ASA(config)# passwd ciscoasa
ASA(config)# show hostname
ASA
ASA(config)# show run domain
lucandat.demo
ASA(config)# _
Connected 0:10:29 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Kiểm tra chứng thực sau khi đặt password với CLI



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window contains a menu bar with "File", "Edit", "View", "Call", "Transfer", and "Help". Below the menu bar is a toolbar with icons for file operations. The main area of the window displays the following text:

```
ASA# disable
ASA> enable
Password: *****
ASA# _
```

At the bottom of the window, there is a status bar with the following information: "Connected 0:00:18", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Kích hoạt DNS Client trên cổng inside

The screenshot shows the Cisco ASDM 7.1 for ASA - 192.168.1.1 interface. The left sidebar shows the 'Device Management' tree with 'DNS Client' selected. The main content area is titled 'Configuration > Device Management > DNS > DNS Client' and contains the following configuration options:

Specify how to resolve DNS requests.

DNS Setup

Configure one DNS server group Configure multiple DNS server groups

Primary DNS Server:

Secondary Servers:

Domain Name:

DNS Lookup

To configure DNS, enable DNS lookup on at least one interface.

Interface	DNS Enabled
inside	True
management	False
outside	False

DNS Guard

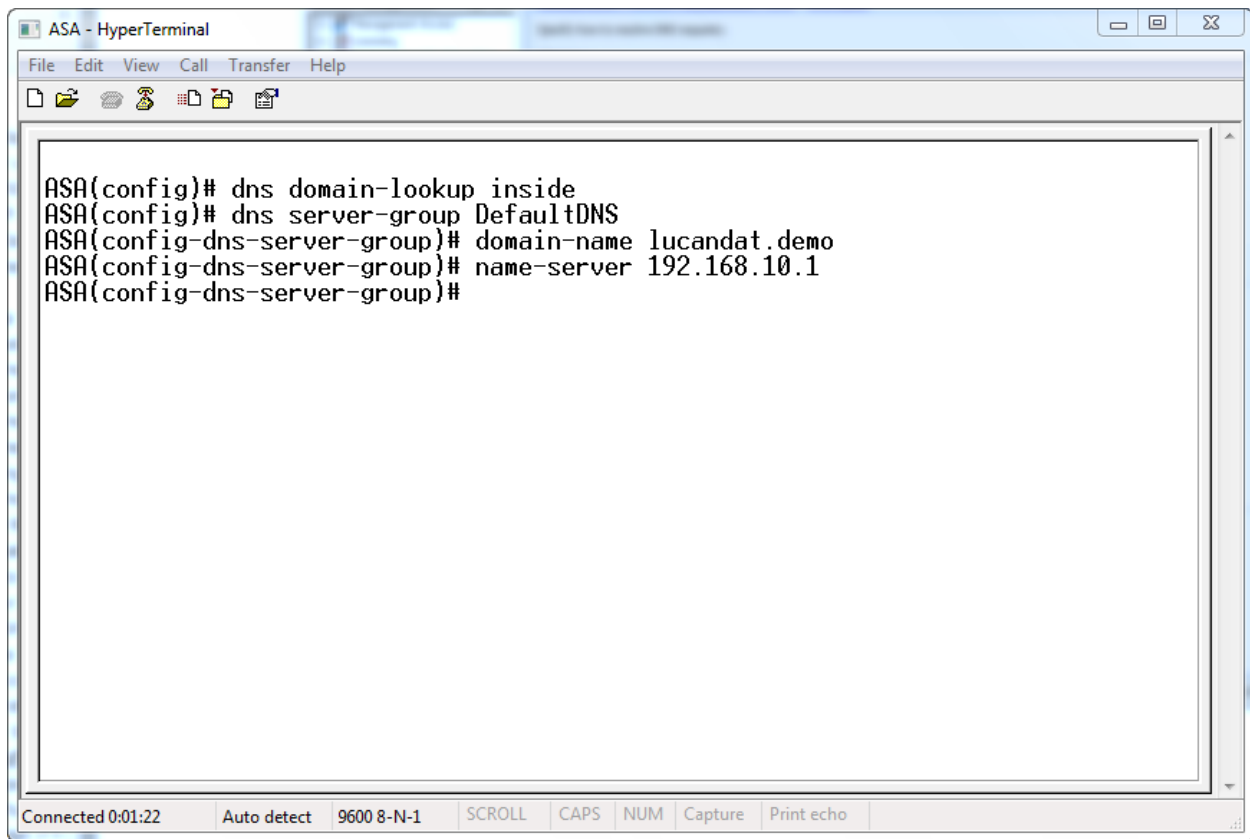
This function enforces one DNS response per query. If DNS inspection is configured, this option is ignored on that interface.

Enable DNS Guard on all interfaces.

Apply Reset

Configuration changes saved successfully. <admin> 15 1/1/03 1:22:17 AM UTC

Cấu hình DNS Client với CLI



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window contains a terminal session with the following commands and prompts:

```
ASA(config)# dns domain-lookup inside
ASA(config)# dns server-group DefaultDNS
ASA(config-dns-server-group)# domain-name lucandat.demo
ASA(config-dns-server-group)# name-server 192.168.10.1
ASA(config-dns-server-group)#
```

The terminal window also displays a menu bar (File, Edit, View, Call, Transfer, Help), a toolbar with icons for file operations, and a status bar at the bottom with the following information: Connected 0:01:22, Auto detect, 9600 8-N-1, SCROLL, CAPS, NUM, Capture, Print echo.

Kiểm tra các tập tin hệ thống với ASDM

The screenshot shows the Cisco ASDM 7.1 for ASA interface. The main window is titled "File Management" and displays the contents of the "disk0:" drive. The interface includes a "Device List" on the left, a "Flash Space" section, and a "Files" table.

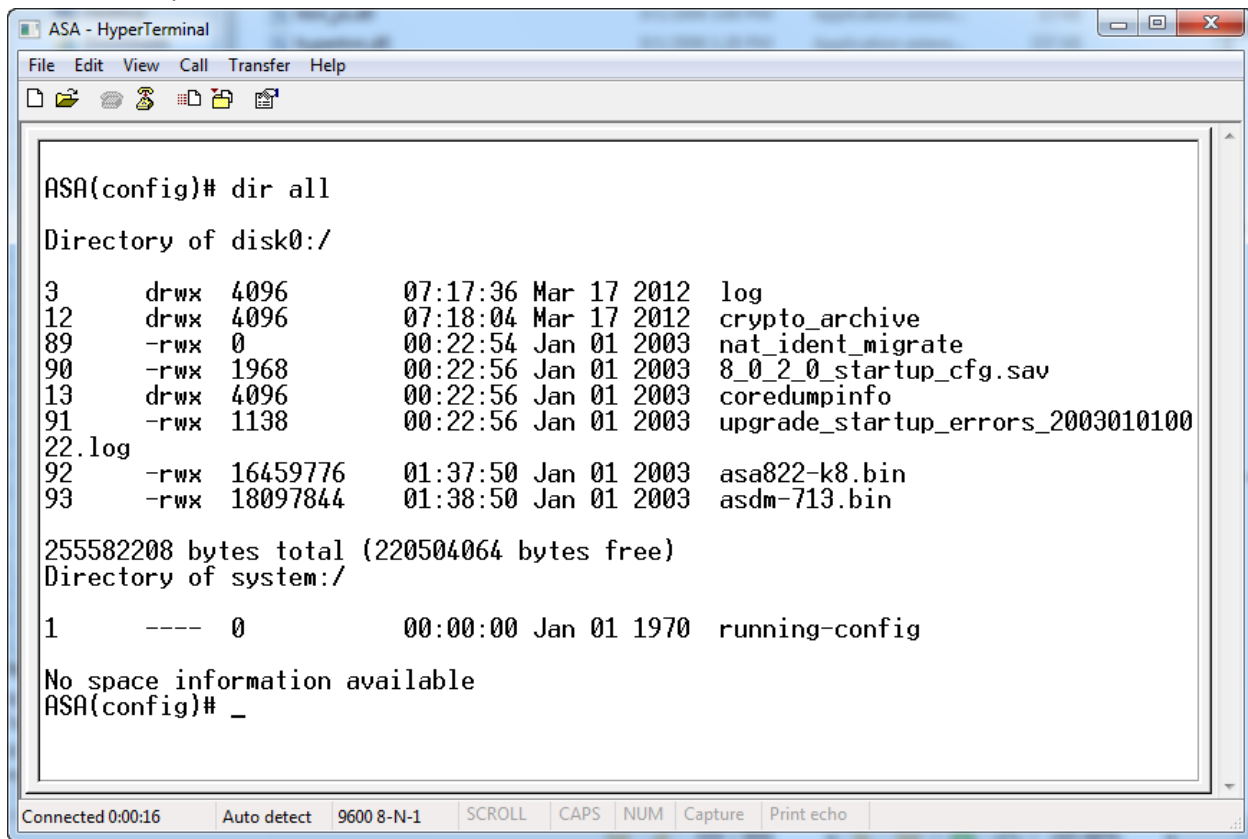
Flash Space:
Total: 255,582,208 bytes
Available: 220,504,064 bytes

Files Table:

FileName	Size (bytes)	Date Modified	Status
coredumpinfo		01/01/03 00:22:56	
crypto_archive		03/17/12 07:18:04	
log		03/17/12 07:17:36	
8_0_2_0_startup_cfg.sav	1,968	01/01/03 00:22:56	
asa822-k8.bin	16,459,776	01/01/03 01:37:50	
asdm-713.bin	18,097,844	01/01/03 01:38:50	ASDM image
nat_ident_migrate	0	01/01/03 00:22:54	
upgrade_startup_errors_...	1,138	01/01/03 00:22:56	

The "asdm-713.bin" file is highlighted in blue. The interface also includes buttons for "View", "Cut", "Copy", "Paste", "Delete", and "Rename..." on the right side of the table.

Kiểm tra file system với CLI



```
ASA - HyperTerminal
File Edit View Call Transfer Help
ASA(config)# dir all
Directory of disk0:/
3      drwx  4096      07:17:36 Mar 17 2012  log
12     drwx  4096      07:18:04 Mar 17 2012  crypto_archive
89     -rwx   0          00:22:54 Jan 01 2003  nat_ident_migrate
90     -rwx  1968      00:22:56 Jan 01 2003  8_0_2_0_startup_cfg.sav
13     drwx  4096      00:22:56 Jan 01 2003  coredumpinfo
91     -rwx  1138      00:22:56 Jan 01 2003  upgrade_startup_errors_2003010100
22.log
92     -rwx 16459776    01:37:50 Jan 01 2003  asa822-k8.bin
93     -rwx 18097844    01:38:50 Jan 01 2003  asdm-713.bin

255582208 bytes total (220504064 bytes free)
Directory of system:/
1      ----  0          00:00:00 Jan 01 1970  running-config

No space information available
ASA(config)# _
```

Connected 0:00:16 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Kiểm tra thứ tự boot order của IOS

The screenshot shows the Cisco ASDM 7.1 for ASA configuration interface. The breadcrumb path is **Configuration > Device Management > System Image/Configuration > Boot Image/Configuration**. The main content area is titled "Boot Configuration" and contains the following text: "Configure boot images from an external TFTP server and flash file system. Up to four images can be configured for the boot system. Only one TFTP boot image can be configured. The TFTP boot image, if configured, must be the first image in the list."

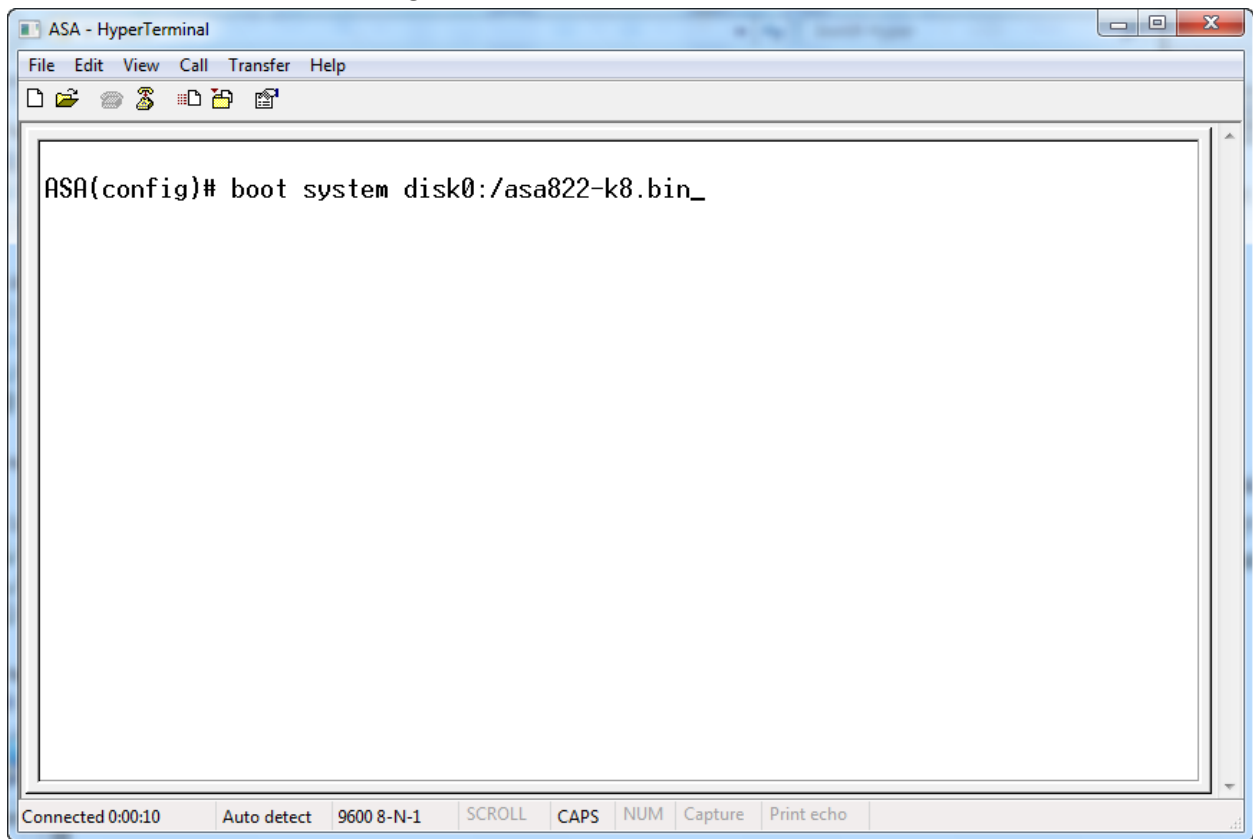
Boot Order	Boot Image Location
1	disk0:/asa822-k8.bin

Below the table, there are fields for "Boot Configuration File Path:" and "ASDM Image File Path:" (containing "disk0:/asdm-713.bin").

At the bottom of the configuration area, there are "Apply" and "Reset" buttons.

The status bar at the bottom of the window shows "Device configuration loaded successfully.", the user is "<admin>", and the page number is "15". The date and time are "1/1/03 1:40:07 AM UTC".

Khai báo IOS sẽ boot khi khởi động ASA với CLI



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window has a menu bar with "File", "Edit", "View", "Call", "Transfer", and "Help". Below the menu bar is a toolbar with icons for file operations. The main terminal area displays the command "ASA(config)# boot system disk0:/asa822-k8.bin_" entered. At the bottom of the window, there is a status bar with the following information: "Connected 0:00:10", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

```
ASA(config)# boot system disk0:/asa822-k8.bin_
```

Cập nhật image ASDM

The screenshot displays the Cisco ASDM 7.1 for ASA interface. The main window is titled "Cisco ASDM 7.1 for ASA - 192.168.1.1". The navigation pane on the left shows the "Device Management" tree with "Boot Image/Configuration" selected. The main content area is titled "Configuration > Device Management > System Image/Configuration > Boot Image/Configuration". It contains a "Boot Configuration" section with a table of boot images and a list of actions.

Boot Order	Boot Image Location
1	disk0:/asa822-k8.bin

Buttons for "Add", "Edit", "Delete", "Move Up", "Move Down", "Browse Flash...", "Apply", and "Reset" are visible.

An "Upgrade Software" dialog box is open in the foreground. It prompts the user to upload a file from a local computer to the flash file system. The fields are:

- Image to Upload: ASDM
- Local File Path: D:\Software hv\ASA\asdm-649.bin
- Flash File System Path: disk0:/asdm-649.bin

Buttons for "Browse Local Files...", "Browse Flash...", "Upload Image", "Close", and "Help" are present in the dialog.

At the bottom of the main window, a status bar shows "Device configuration loaded successfully.", the user is logged in as "<admin>", and the time is "1/1/03 1:44:07 AM UTC".

Kiểm tra active-key và cập nhật key với ASDM

Cisco ASDM 7.1 for ASA - 192.168.1.1

Configuration > Device Management > Licensing > Activation Key

Permanent Activation Key

Serial No.: JMK1237L19A

Permanent Activation Key: 0x7524c555 0xe0005cc2 0x391268ec 0xc8c85458 0xc00fda9b

New Activation Key

Configure a new activation key for the device. It will take effect after the next reload.

New Activation Key:

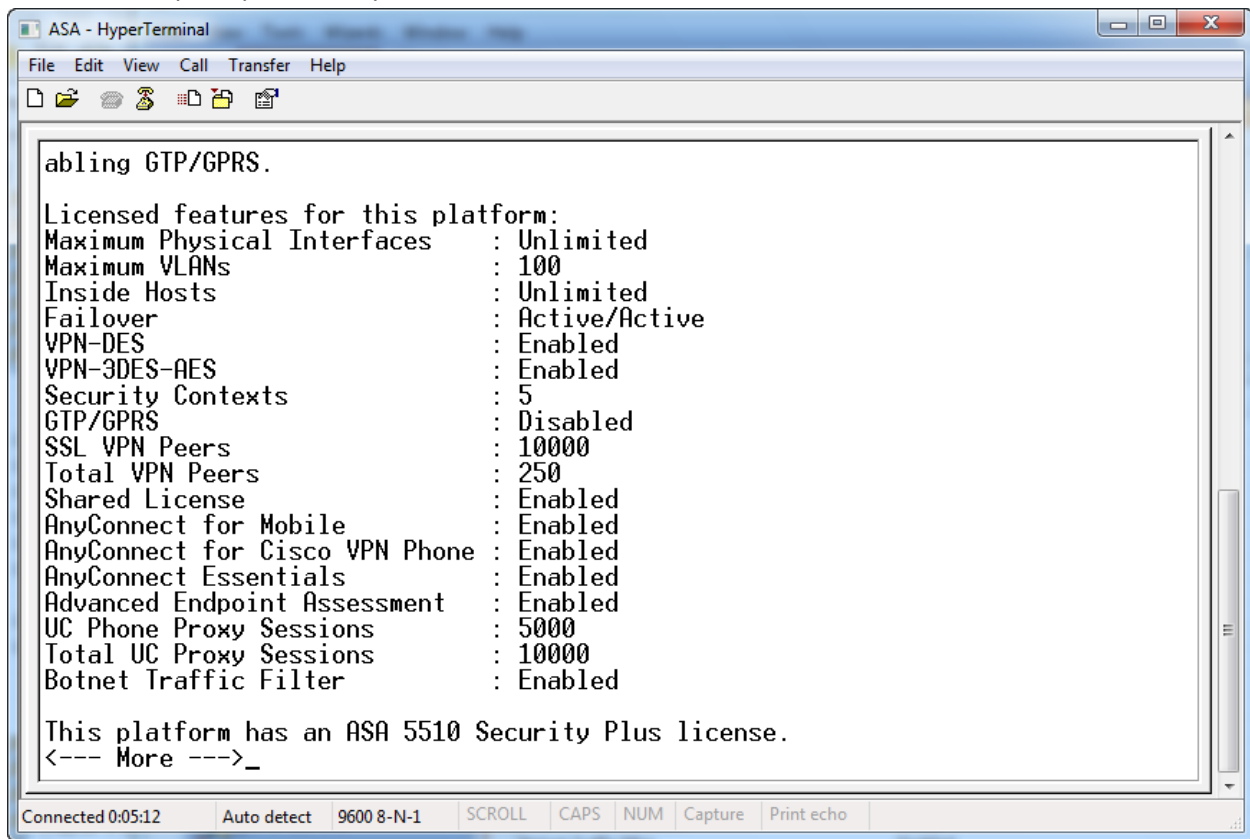
Effective Running Licenses

License Feature	License Value	License Duration
Device license	Security Plus	
Maximum Physical Interfaces	Unlimited	
Maximum VLANs	100	
Inside Hosts	Unlimited	
Fallover	Active/Active	
VPN-DES	Enabled	
VPN-3DES-AES	Enabled	
Security Contexts	5	
GTP/GPRS	Disabled	
SSL VPN Peers	10000	
Total VPN Peers	250	
Shared License	Enabled	
AnyConnect for Mobile	Enabled	
AnyConnect for Cisco VPN Phone	Enabled	
AnyConnect Essentials	Enabled	
Advanced Endpoint Assessment	Enabled	
UC Phone Proxy Sessions	5000	
Total UC Proxy Sessions	10000	
Botnet Traffic Filter	Enabled	

Update Activation Key

<admin> 15 1/1/03 1:48:37 AM UTC

Kiểm tra và cập nhật active-key với CLI



```
ASA - HyperTerminal
File Edit View Call Transfer Help
ablings GTP/GPRS.
Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs              : 100
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Security Contexts          : 5
GTP/GPRS                    : Disabled
SSL VPN Peers               : 10000
Total VPN Peers             : 250
Shared License              : Enabled
AnyConnect for Mobile       : Enabled
AnyConnect for Cisco VPN Phone : Enabled
AnyConnect Essentials       : Enabled
Advanced Endpoint Assessment : Enabled
UC Phone Proxy Sessions     : 5000
Total UC Proxy Sessions     : 10000
Botnet Traffic Filter        : Enabled

This platform has an ASA 5510 Security Plus license.
<--- More --->_
Connected 0:05:12 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

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

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Cisco ASDM 7.1 for ASA - 192.168.1.1". The navigation pane on the left shows the "Device Management" tree, with "ASDM/HTTPS/Telnet/SSH" selected. The main content area is titled "Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH".

The main configuration area contains a table with the following data:

Type	Interface	IP Address	Mask/Prefix Length
ASDM/HTTPS	management	192.168.1.0	255.255.255.0

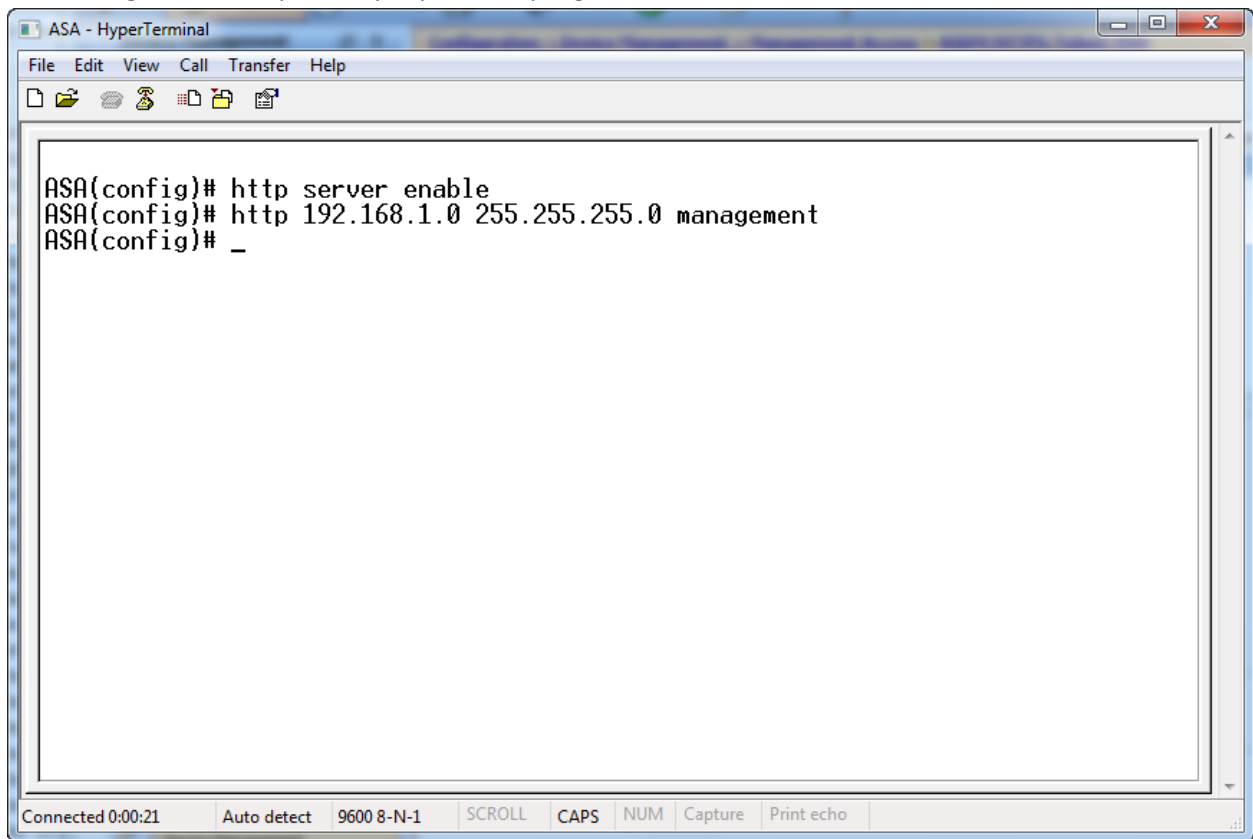
An "Edit Device Access Configuration" dialog box is open, showing the following settings:

- Access Type: ASDM/HTTPS Telnet SSH
- Interface Name: management
- IP Address: 192.168.1.0
- Mask: 255.255.255.0

The dialog box also includes "OK", "Cancel", and "Help" buttons. The main configuration page includes sections for "Http Settings" (with "Enable HTTP Service" checked), "Port Number", "Idle Timeout", "Session Timeout", "Require client certificate to access ASDM on the following interfaces" (with an empty "Interfaces" dropdown), "Telnet Settings" (with "Telnet Timeout" set to 5 minutes), and "SSH Settings" (with "Allowed SSH Version(s)" set to "1 & 2" and "SSH Timeout" set to 5 minutes). "Apply" and "Reset" buttons are at the bottom of the main configuration area.

The status bar at the bottom shows the user is logged in as "<admin>" with a session ID of "15" and the date/time "1/1/03 1:50:37 AM UTC".

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



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window has a menu bar with "File", "Edit", "View", "Call", "Transfer", and "Help". Below the menu bar is a toolbar with icons for file operations. The main area of the window displays the following text:

```
ASA(config)# http server enable
ASA(config)# http 192.168.1.0 255.255.255.0 management
ASA(config)# _
```

At the bottom of the window, there is a status bar with the following information: "Connected 0:00:21", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Cấu hình no management-only trên ASDM

The screenshot displays the Cisco ASDM 7.1 for ASA configuration environment. The main window shows the 'Device Setup' tree on the left, with 'Interfaces' selected. The 'Edit Interface' dialog box is open, showing the configuration for the 'management' interface. The 'General' tab is active, and the 'Dedicate this interface to management only' checkbox is checked. The IP address is set to 192.168.1.1 with a subnet mask of 255.255.255.0. The 'Description' field is empty. The 'Hardware Port' is Management0/0. The 'Security Level' is 100. The 'Enable Interface' checkbox is also checked. The 'IP Address' section has 'Use Static IP' selected. The 'Apply' and 'Reset' buttons are visible at the bottom of the dialog box. The status bar at the bottom shows the user is logged in as '<admin>' and the time is 1/1/03 2:03:04 AM UTC.

Cisco ASDM 7.1 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration

Device Setup

- Startup Wizard
- Interfaces
- Routing
- Device Name/Password
- System Time

Device List

- Device Setup
- Firewall
- Remote Access VPN
- Site-to-Site VPN
- IPS
- Device Management

Edit Interface

General Advanced IPv6

Hardware Port: Management0/0 [Configure Hardware Properties...](#)

Interface Name: management

Security Level: 100

Dedicate this interface to management only

Enable Interface

IP Address

Use Static IP Obtain Address via DHCP Use PPPoE

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

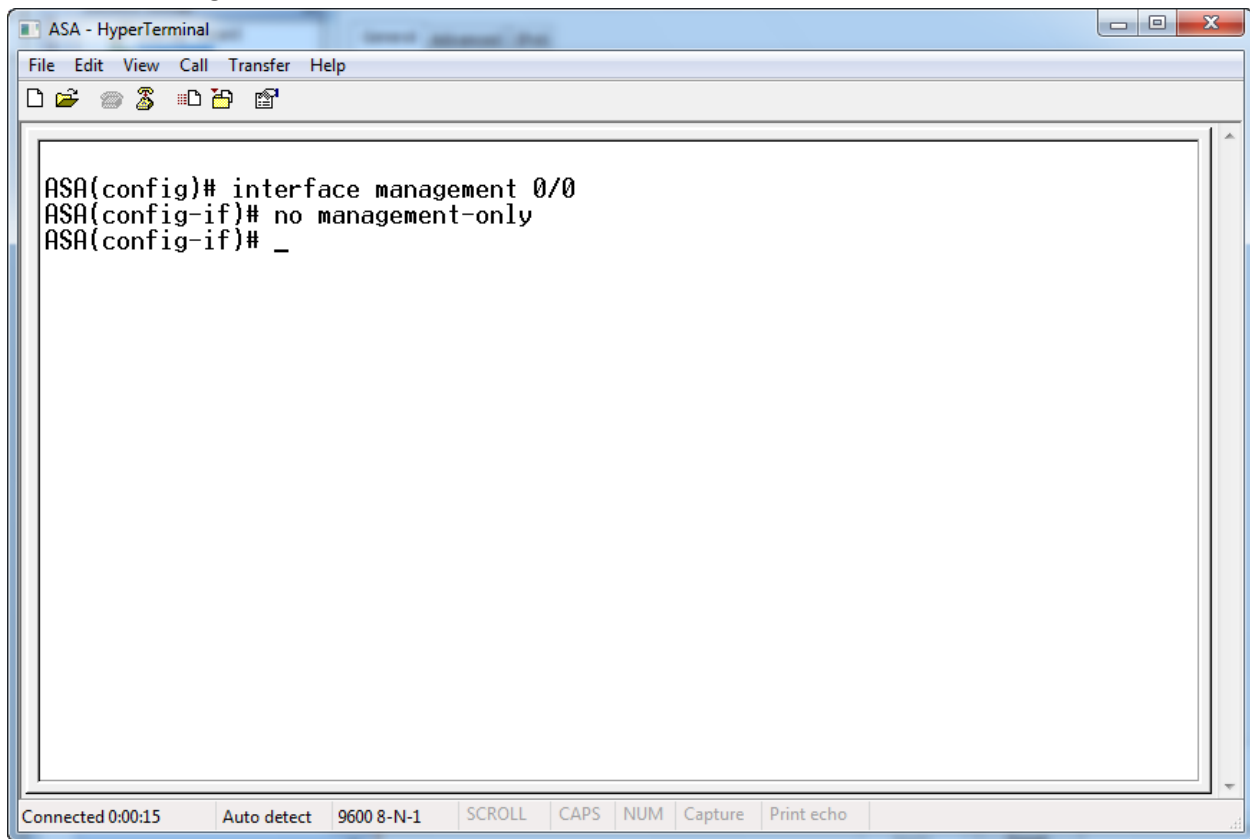
Description:

OK Cancel Help

Apply Reset

<admin> 15 1/1/03 2:03:04 AM UTC

Cấu hình với dòng lệnh



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window contains a terminal session with the following commands and output:

```
ASA(config)# interface management 0/0
ASA(config-if)# no management-only
ASA(config-if)# _
```

The status bar at the bottom of the window displays: "Connected 0:00:15", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Cấu hình cho phép telnet

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH". The left sidebar shows the "Device Management" tree with "ASDM/HTTPS/Telnet/SSH" selected. The main content area shows a table of access configurations:

Type	Interface	IP Address	Mask/Prefix Length
ASDM/HTTPS	management	192.168.1.0	255.255.255.0

An "Edit Device Access Configuration" dialog box is open, showing the configuration for the selected entry:

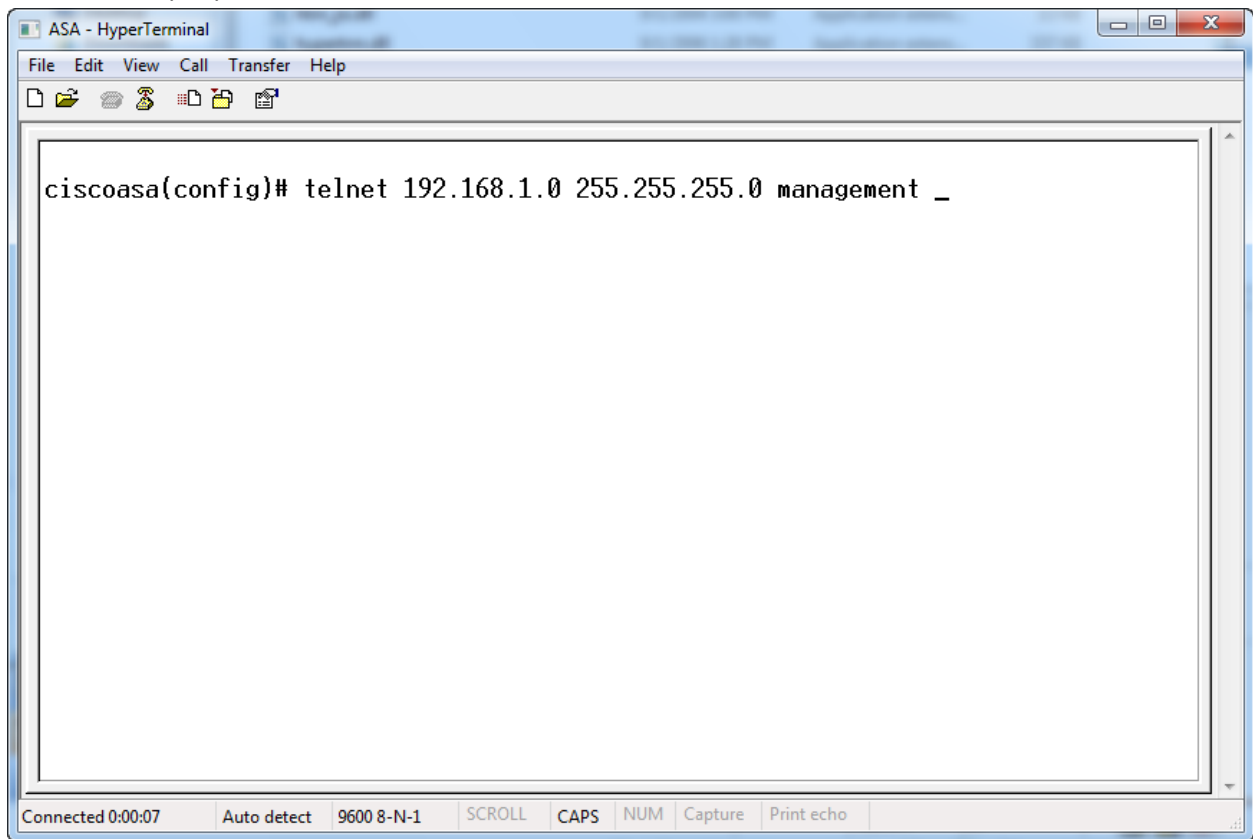
- Access Type: ASDM/HTTPS Telnet SSH
- Interface Name: management
- IP Address: 192.168.1.0
- Mask: 255.255.255.0

Below the dialog, the main configuration page shows various settings:

- Http Settings: Enable HTTP Service
- Port Number: (empty)
- Idle Timeout: (empty)
- Session Timeout:
- Require client certificate to access ASDM on the following interfaces: Interfaces: (empty)
- Telnet Settings: Telnet Timeout: 5 minutes
- SSH Settings: Allowed SSH Version(s): 1 & 2, SSH Timeout: 5 minutes

Buttons for "Apply" and "Reset" are visible at the bottom of the configuration page. The status bar at the bottom shows "<admin> 15" and the date/time "1/1/03 2:09:41 AM UTC".

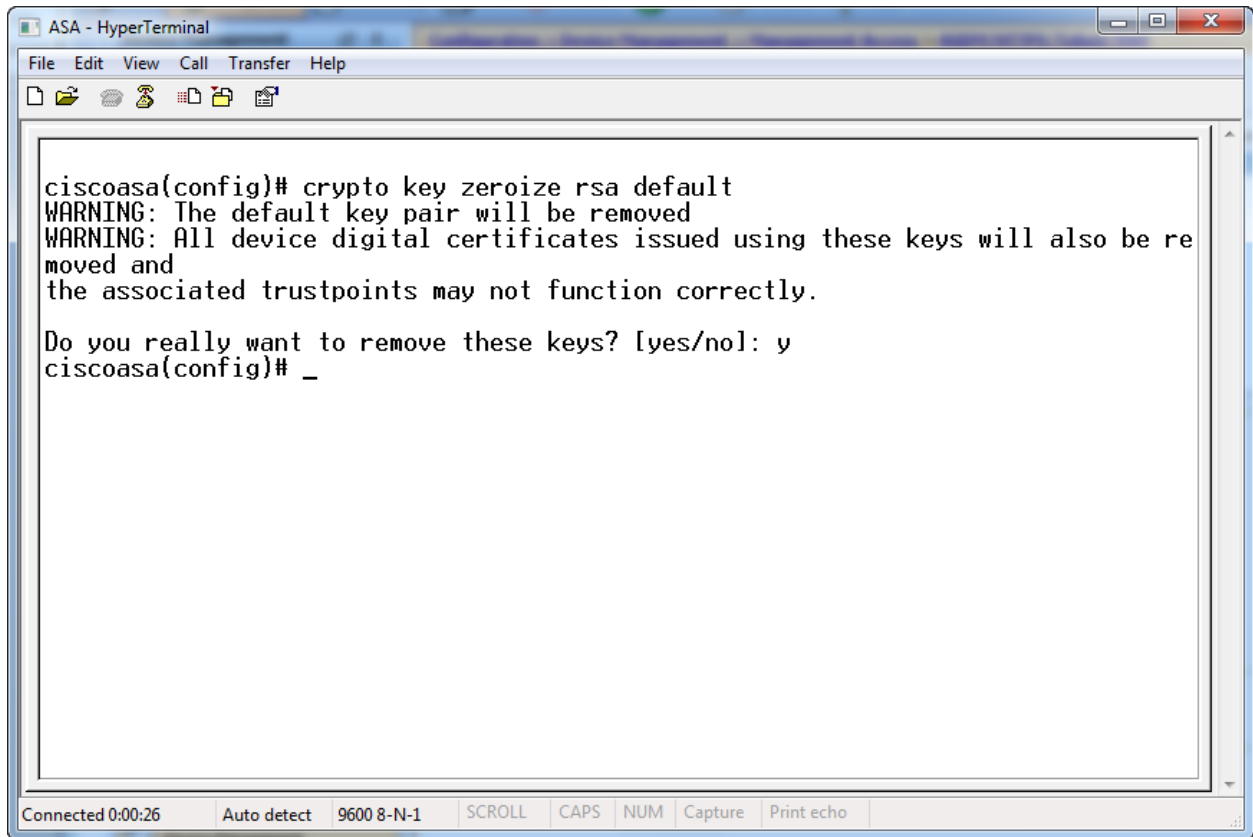
Cấu hình cho phép telnet với CLI



The image shows a HyperTerminal window titled "ASA - HyperTerminal". The window has a menu bar with "File", "Edit", "View", "Call", "Transfer", and "Help". Below the menu bar is a toolbar with icons for file operations. The main area of the window displays a command prompt for a Cisco ASA in configuration mode: "ciscoasa(config)# telnet 192.168.1.0 255.255.255.0 management _". The status bar at the bottom of the window shows "Connected 0:00:07", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

```
ciscoasa(config)# telnet 192.168.1.0 255.255.255.0 management _
```

Xoá key RSA mặc định



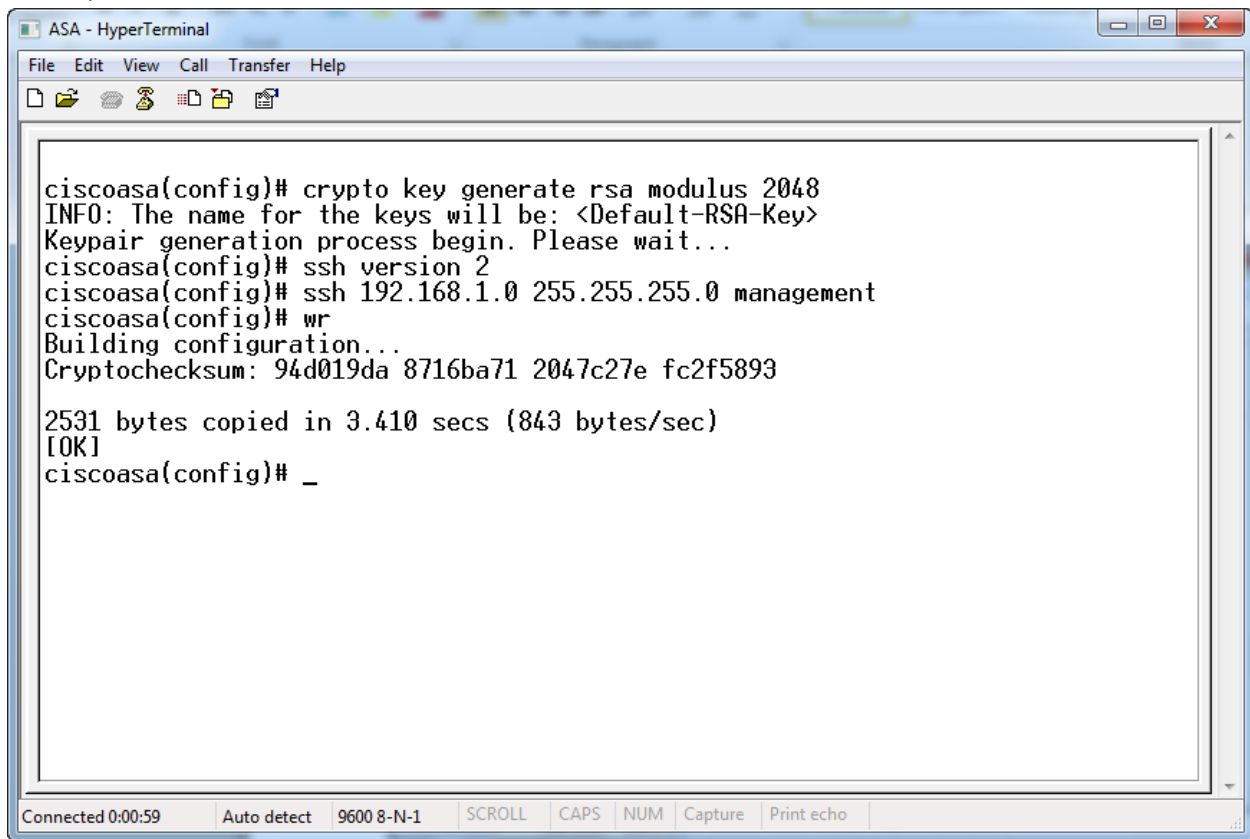
```
ASA - HyperTerminal
File Edit View Call Transfer Help
[Icons]

ciscoasa(config)# crypto key zeroize rsa default
WARNING: The default key pair will be removed
WARNING: All device digital certificates issued using these keys will also be removed and
the associated trustpoints may not function correctly.

Do you really want to remove these keys? [yes/no]: y
ciscoasa(config)# _

Connected 0:00:26  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

Tạo key rsa mới



```
ASA - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# crypto key generate rsa modulus 2048
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh 192.168.1.0 255.255.255.0 management
ciscoasa(config)# wr
Building configuration...
Cryptochecksum: 94d019da 8716ba71 2047c27e fc2f5893

2531 bytes copied in 3.410 secs (843 bytes/sec)
[OK]
ciscoasa(config)# _

Connected 0:00:59  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

Kích hoạt ssh

The screenshot shows the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH". The left sidebar shows the "Device Management" tree with "ASDM/HTTPS/Telnet/SSH" selected. The main content area displays a table of access configurations and various settings.

Type	Interface	IP Address	Mask/Prefix Length
ASDM/HTTPS	management	192.168.1.0	255.255.255.0

An "Edit Device Access Configuration" dialog box is open, showing the following settings:

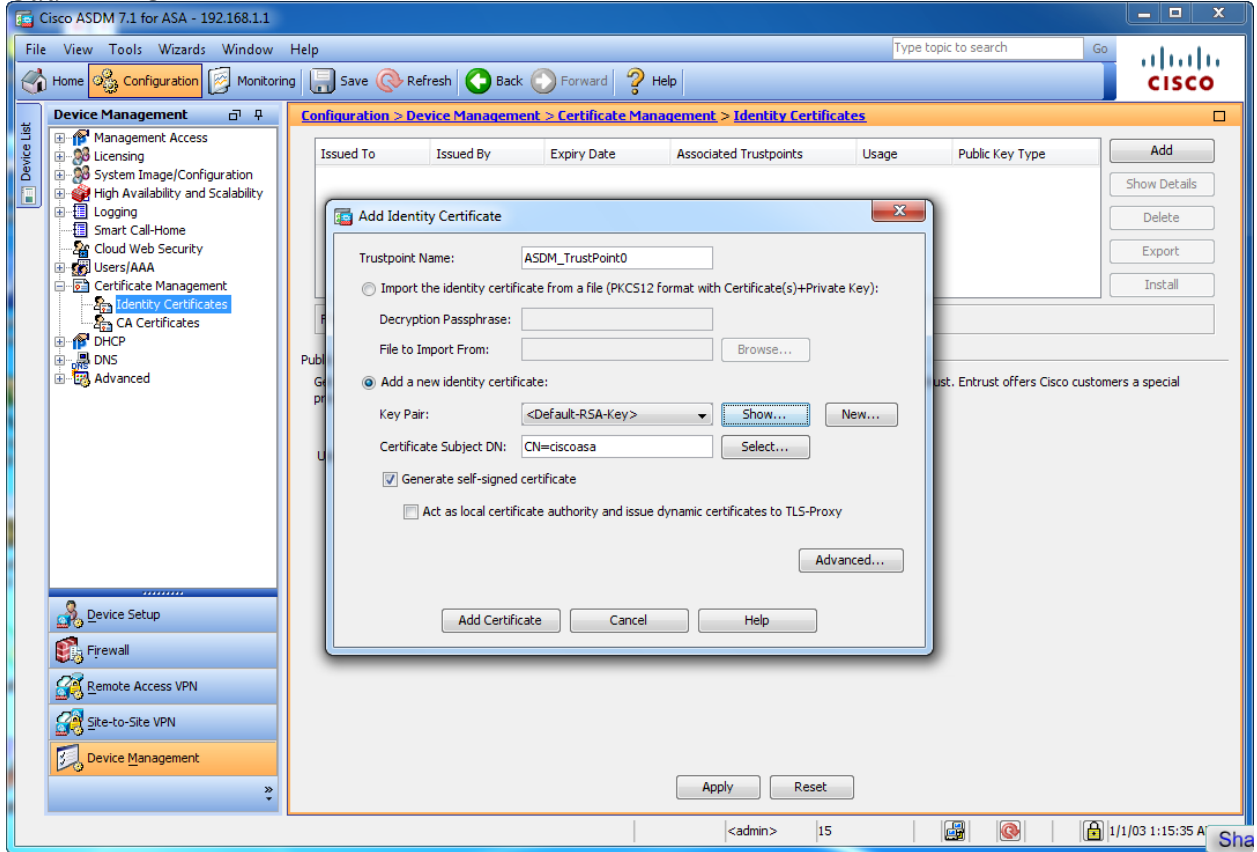
- Access Type: ASDM/HTTPS Telnet SSH
- Interface Name: management
- IP Address: 192.168.1.0
- Mask: 255.255.255.0

Other settings in the main window include:

- Http Settings: Enable HTTP Service
- Port Number: (empty)
- Idle Timeout: (empty)
- Session Timeout:
- Require client certificate to access ASDM on the following interfaces: Interfaces: (empty)
- Telnet Settings: Telnet Timeout: 5 minutes
- SSH Settings: Allowed SSH Version(s): 1 & 2; SSH Timeout: 5 minutes

Buttons for "Apply" and "Reset" are visible at the bottom of the configuration area. The status bar at the bottom shows "<admin> 15" and the date/time "1/1/03 2:17:51 AM UTC".

Cấu hình CA



Tạo CA thành công

The screenshot displays the Cisco ASDM 7.1 for ASA - 192.168.1.1 interface. The main window is titled "Configuration > Device Management > Certificate Management > Identity Certificates". A table with columns "Issued To", "Issued By", "Expiry Date", "Associated Trustpoints", "Usage", and "Public Key Type" is visible. An "Add Identity Certificate" dialog box is open, showing "Trustpoint Name: ASDM_TrustPoint1" and the "Add a new identity" option selected. An "Enrollment Status" dialog box is overlaid on top, displaying "Enrollment succeeded." with an "OK" button. The bottom status bar shows "Configuration changes saved successfully." and the user is logged in as "<admin>".

Kiểm tra CA sau khi được tạo

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

Configuration > Device Management > Certificate Management > Identity Certificates

Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type
hostname=cisco...	hostname=cisco...	01:19:17 UTC Dec ...	ASDM_TrustPoint1	General Purp...	RSA (2048 bits)

Find: Match Case

Public CA Enrollment

Get your Cisco ASA security appliance up and running quickly with an SSL Advantage digital certificate from Entrust. Entrust offers Cisco customers a special promotional price for certificates and trial certificates for testing.

[Enroll ASA SSL certificate with Entrust](#)

Using a previously saved certificate signing request, [enroll with Entrust](#).

Apply Reset

Configuration changes saved successfully. <admin> 15 1/1/03 1:19:35 A Sha

Tùy chọn thuật toán mã hóa trong SSL

Cisco ASDM 7.1 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Configuration > Device Management > Advanced > SSL Settings

Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.

The SSL version for the security appliance to negotiate as a "server": Any

The SSL version for the security appliance to negotiate as a "client": Any

Encryption

Available Algorithms

- RC4-SHA1
- RC4-MD5
- DES-SHA1
- DHE-AES128-SHA1
- DHE-AES256-SHA1
- NULL-SHA1

Active Algorithms

- AES256-SHA1
- 3DES-SHA1
- AES128-SHA1

Certificates

Specify which certificates, if any, should be used for SSL authentication on each interface. The fallback certificate will be used on interfaces not associated with a certificate of their own.

Interface	Trustpoint	Load Balancing Trustpoint	Edit
dmz			
inside			
management	ASDM_TrustPoint5:hostname=ciscoasa,...	ASDM_TrustPoint5:hostname=ciscoasa, cn=ciscoasa:h...	

Fallback Certificate: -- None --

Apply Reset

Configuration changes saved successfully.

<admin> 15 1/1/03 1:35:18 A Sha

Khai báo CA sẽ được sử dụng

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window is titled "Cisco ASDM 7.1 for ASA - 192.168.1.1". The navigation pane on the left shows the "Device Management" tree, with "SSL Settings" selected under the "Advanced" category. The main content area is titled "Configuration > Device Management > Advanced > SSL Settings". It contains the following configuration options:

- Configure SSL parameters. These parameters affect both ASDM and SSL VPN access.
- The SSL version for the security appliance to negotiate as a "server": Any
- The SSL version for the security appliance to negotiate as a "client": Any
- Encryption section with "Available Algorithms" and "Active Algorithms" lists.
- Certificate Management section with "Interface" set to "management".
- "Primary Enrolled Certificate" and "Load Balancing Enrolled Certificate" dropdown menus, both showing "ASDM_TrustPoint5:hostname=ciscoasa, cn=ciscoasa:ho...".
- "Fallback Certificate" dropdown menu set to "-- None --".

A "Select SSL Certificate" dialog box is open in the foreground, containing the following text:

Specify enrolled trustpoints to be used for SSL authentication and VPN load balancing on the management interface. To enroll a trustpoint, go to Device Management > Certificate Management > Identity Certificates.

The dialog box has "OK", "Cancel", and "Help" buttons. In the background, the "Active Algorithms" list includes "256-SHA1", "85-SHA1", and "128-SHA1".

At the bottom of the interface, a status bar shows "Configuration changes saved successfully.", the user is logged in as "<admin>", and the system time is "1/1/03 1:35:28 A".

Tạo username và password để truy cập ASA

Cisco ASDM 7.1 for ASA - 192.168.1.1

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Configuration > Device Management > Users/AAA > User Accounts

Add User Account

Identity

VPN Policy

Username: lucandat

Password: *****

Confirm Password: *****

User authenticated using MSCHAP

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.

Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)

Privilege level is used with command authorization.

Privilege Level: 15

CLI login prompt for SSH, Telnet and console (no ASDM access)

This setting is effective only if "aaa authentication http console LOCAL" command is configured.

No ASDM, SSH, Telnet or Console access

This setting is effective only if "aaa authentication http console LOCAL" and "aaa authorization exec" commands are configured.

Find: Next Previous

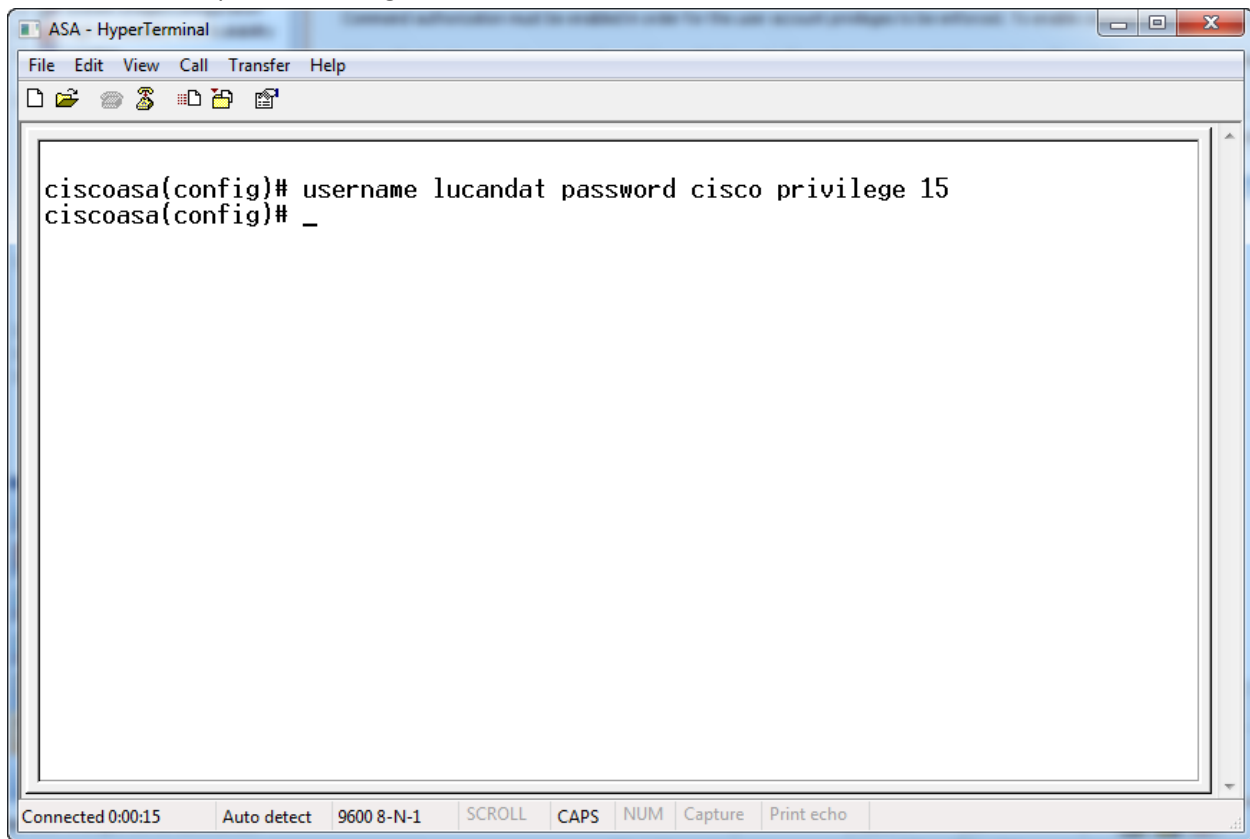
OK Cancel Help

Apply Reset

Configuration changes saved successfully.

<admin> 15 1/1/03 1:39:28 A Sha

Tạo username và password bằng CLI



```
ASA - HyperTerminal
File Edit View Call Transfer Help
ciscoasa(config)# username lucandat password cisco privilege 15
ciscoasa(config)# _
Connected 0:00:15 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Tạo AAA server group

The screenshot shows the Cisco ASDM 7.1 for ASA interface. The main window displays the configuration for AAA Server Groups. A dialog box titled "Add AAA Server Group" is open, allowing the user to configure a new server group. The configuration details are as follows:

AAA Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				3

The "Add AAA Server Group" dialog box contains the following fields and options:

- AAA Server Group: tac
- Protocol: TACACS+
- Accounting Mode: Simultaneous Single
- Reactivation Mode: Depletion Timed
- Dead Time: 10 minutes
- Max Failed Attempts: 3

Buttons: OK, Cancel, Help

At the bottom of the main window, there are buttons for "Apply" and "Reset". The status bar at the bottom indicates "Configuration changes saved successfully." and shows the user as "<admin>" with a session ID of "15". The system time is "1/1/03 1:41:18 A".

Cấu hình AAA server trên cổng management

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window shows the configuration path: Configuration > Device Management > Users/AAA > AAA Server Groups. A table lists the configured AAA Server Groups:

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				3
tac	TACACS+	Single	Depletion	10	3

An "Edit AAA Server" dialog box is open, showing the configuration for the "tac" server group:

- Server Group: tac
- Interface Name: management
- Server Name or IP Address: 192.168.1.1
- Timeout: 10 seconds
- TACACS+ Parameters:
 - Server Port: 49
 - Server Secret Key: [masked]
- SDI Messages: Message Table

The status bar at the bottom indicates "Configuration changes saved successfully." and shows the user as <admin> with 15 sessions. The system time is 1/1/03 1:41:58 A.

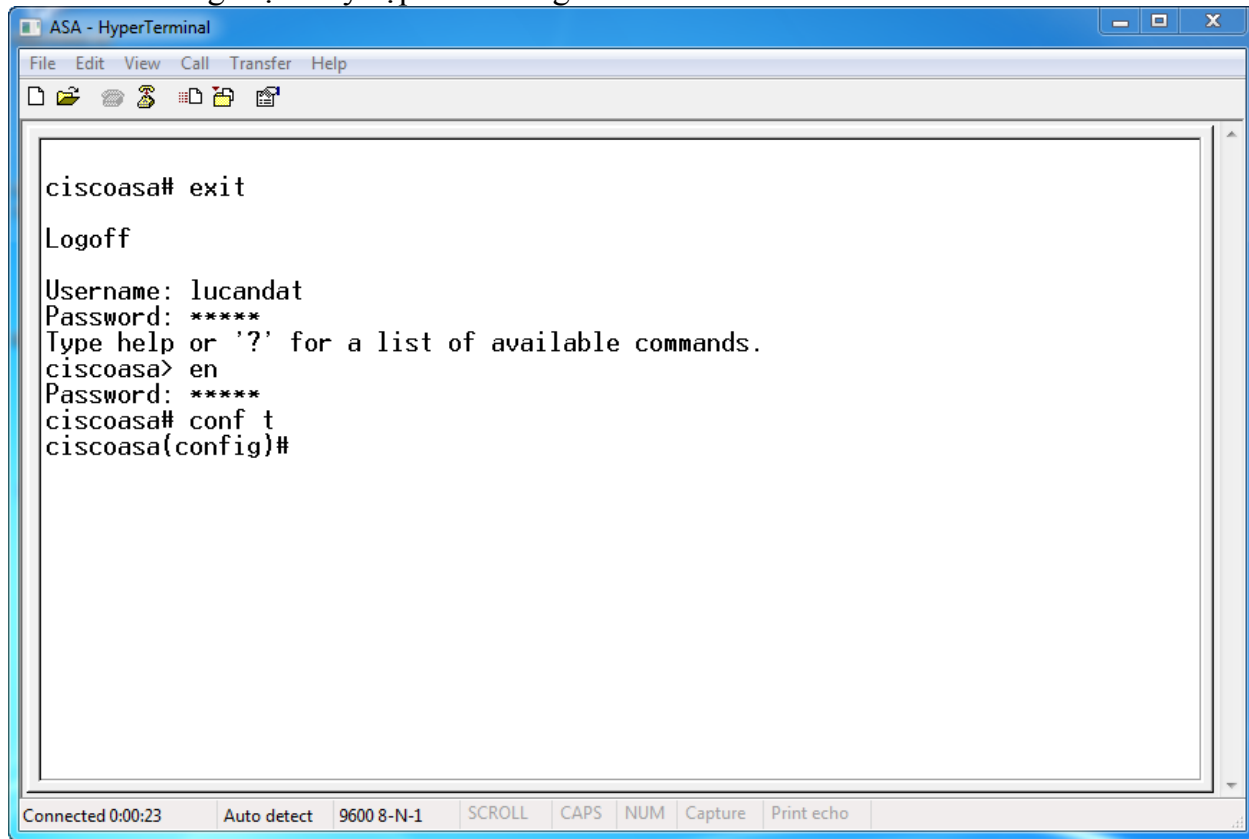
Cấu hình chứng thực AAA access

The screenshot shows the Cisco ASDM 7.1 for ASA configuration interface. The breadcrumb path is Configuration > Device Management > Users/AAA > AAA Access > Authentication. The left sidebar shows the configuration tree with 'AAA Access' selected. The main pane displays the 'Authentication' tab with the following configuration:

- Enable authentication for administrator access to the ASA.
- Require authentication to allow use of privileged mode commands: Enable, Server Group: tac, Use LOCAL when server group fails
- Require authentication for the following types of connections:
 - HTTP/ASDM, Server Group: tac, Use LOCAL when server group fails
 - Serial, Server Group: tac, Use LOCAL when server group fails
 - SSH, Server Group: tac, Use LOCAL when server group fails
 - Telnet, Server Group: tac, Use LOCAL when server group fails

Buttons for 'Apply' and 'Reset' are visible at the bottom of the configuration pane. A status bar at the bottom left indicates 'Configuration changes saved successfully.' and the bottom right shows the user '<admin>' and the time '1/1/03 1:42:38 A'.

Kiểm tra chứng thực truy cập ASA bằng CLI



```
ASA - HyperTerminal
File Edit View Call Transfer Help
ciscoasa# exit
Logoff
Username: lucandat
Password: *****
Type help or '?' for a list of available commands.
ciscoasa> en
Password: *****
ciscoasa# conf t
ciscoasa(config)#
```

Connected 0:00:23 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo


Firefox

Đang kết nối...

https://192.168.1.1/admin/public/index.html

Google

Cisco ASDM 7.1(4)



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 bảo: "Authentication"

Tên đăng nhập:

Mật khẩu:

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.

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

Home Configuration Monitoring Save Refresh Back Forward Help

Configuration > Device Management > Users/AAA > AAA Access > Authorization

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
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

Apply Reset

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

Home Configuration Monitoring Save Refresh Back Forward Help

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
auth-prompt	configure	cmd	15

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

Home Configuration Monitoring Save Refresh Back Forward Help

Type topic to search Go

CISCO

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 Server Group: tac

SSH Server Group: tac

Telnet Server Group: tac

Require command accounting for ASA

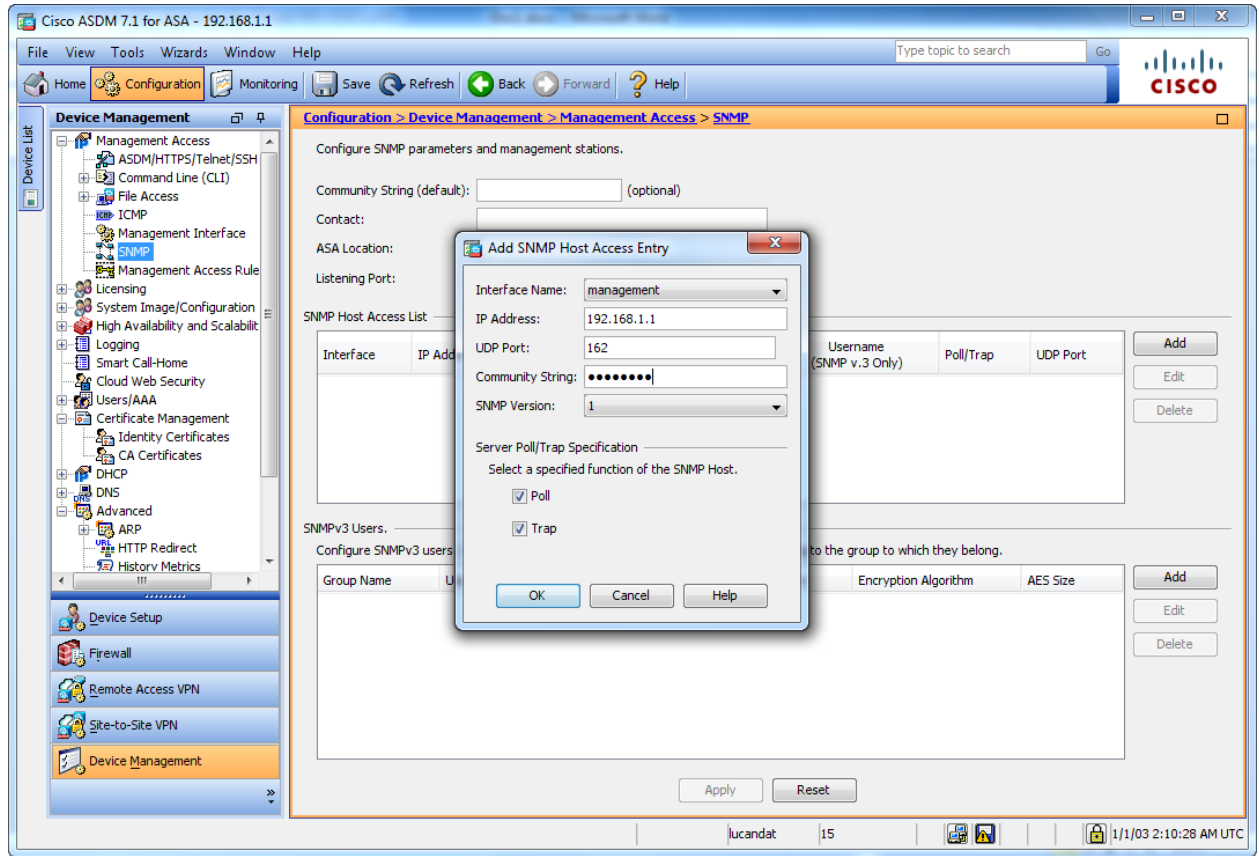
Enable Server Group: tac

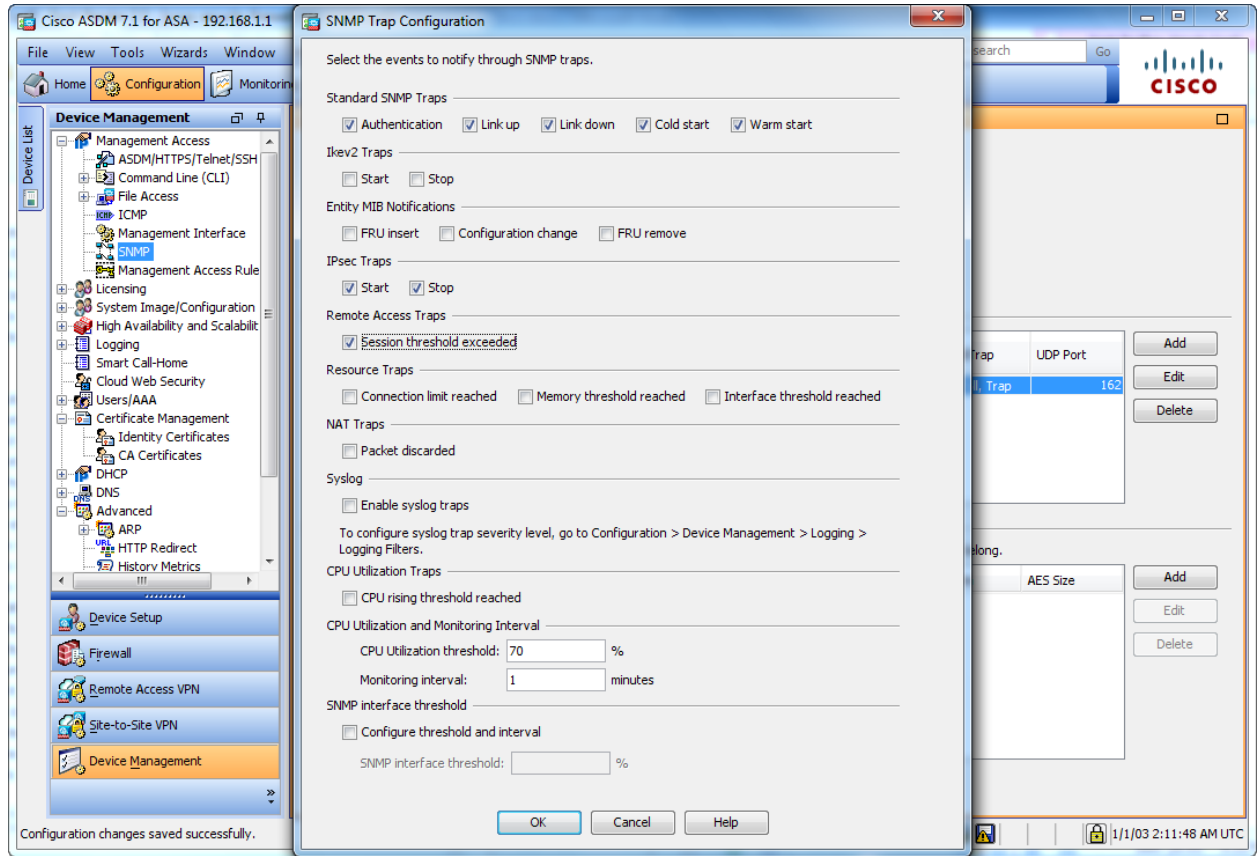
Privilege level: 15

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

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
poll, Trap	162

Trap	AES Size
------	----------

Apply Reset

Configuration changes saved successfully.

lucandat 15 1/1/03 2:13:58 AM UTC

Tạo AAA Server GROUP

The screenshot displays the Cisco ASDM 7.1 for ASA configuration interface. The main window shows the configuration path: Configuration > Device Management > Users/AAA > AAA Server Groups. A table lists the existing AAA Server Groups:

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				1

An "Add AAA Server Group" dialog box is open, with the following configuration:

- AAA Server Group: Tacacs
- Protocol: TACACS+
- Accounting Mode: Simultaneous Single
- Reactivation Mode: Depletion Timed
- Dead Time: 10 minutes
- Max Failed Attempts: 3

The dialog box has "OK", "Cancel", and "Help" buttons. The main window also shows a "Find:" search bar and a "Match Case" checkbox. The status bar at the bottom indicates "Device configuration loaded successfully." and shows the user as "<admin>" with a session ID of "15". The system time is "1/1/03 2:32:31 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

Configuration > Device Management > Users/AAA > AAA Access > Authentication

Device List

- 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

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 Server Group: Tacacs Use LOCAL when server group fails

Serial Server Group: Tacacs Use LOCAL when server group fails

SSH Server Group: Tacacs Use LOCAL when server group fails

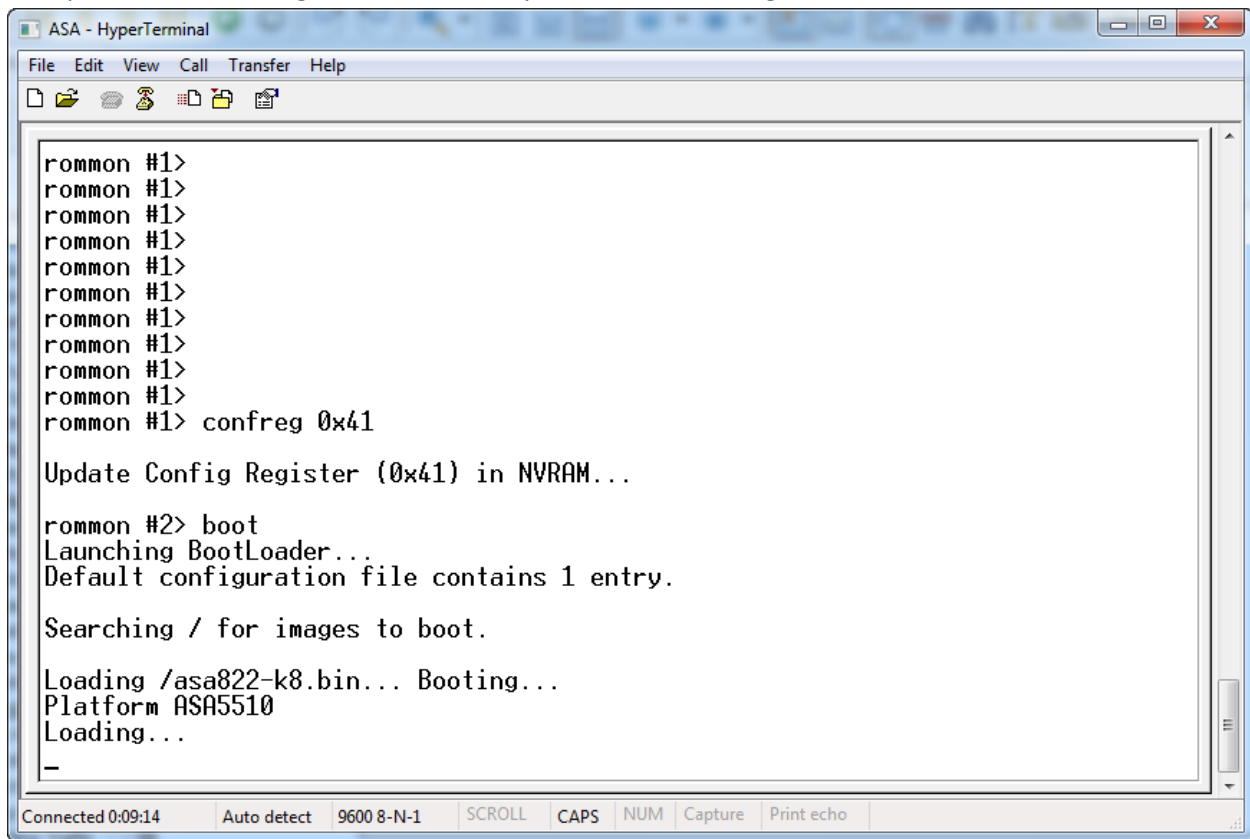
Telnet Server Group: Tacacs Use LOCAL when server group fails

Apply Reset

Configuration changes saved successfully.

<admin> 15 1/1/03 2:33:01 AM UTC

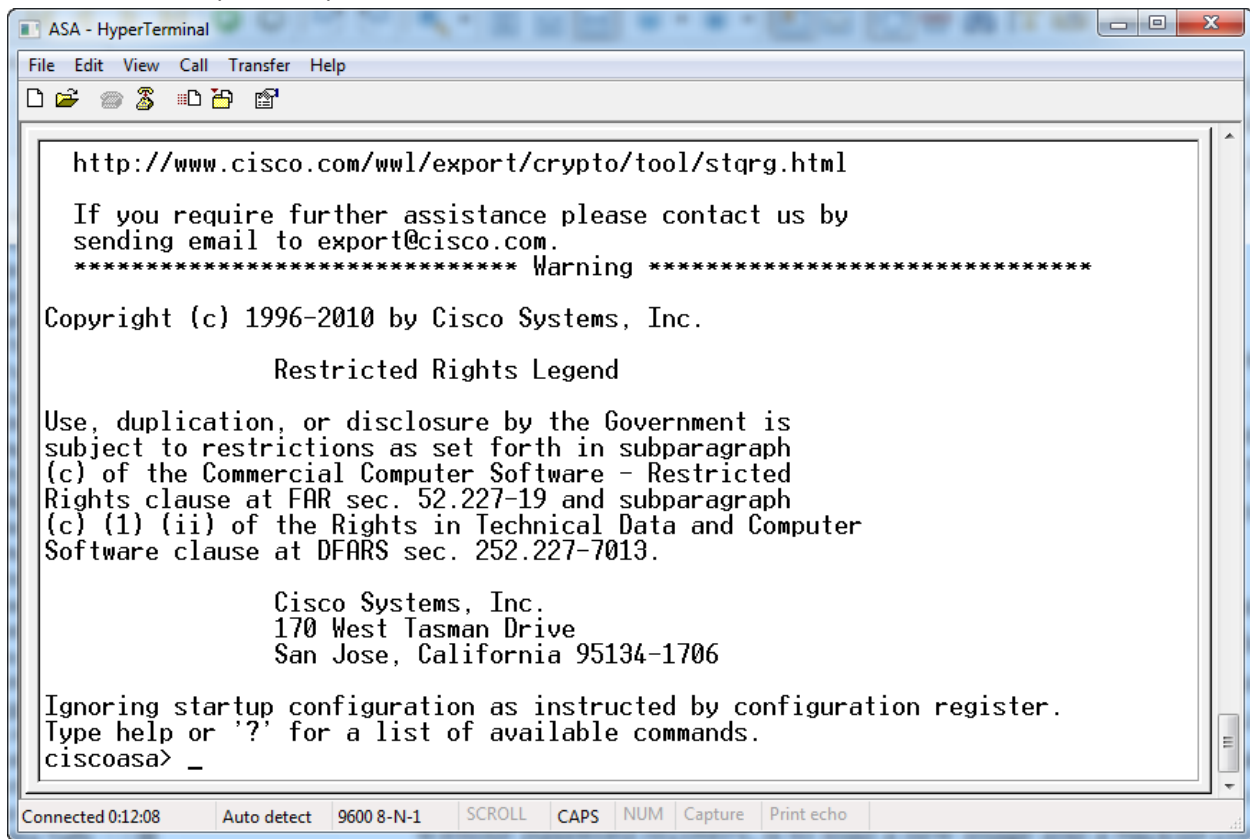
Khôi phục mật khẩu bằng cách nhấn ESC hay Break khi khởi động ASA



```
ASA - HyperTerminal
File Edit View Call Transfer Help
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1>
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
rommon #2> boot
Launching BootLoader...
Default configuration file contains 1 entry.
Searching / for images to boot.
Loading /asa822-k8.bin... Booting...
Platform ASA5510
Loading...
-
```

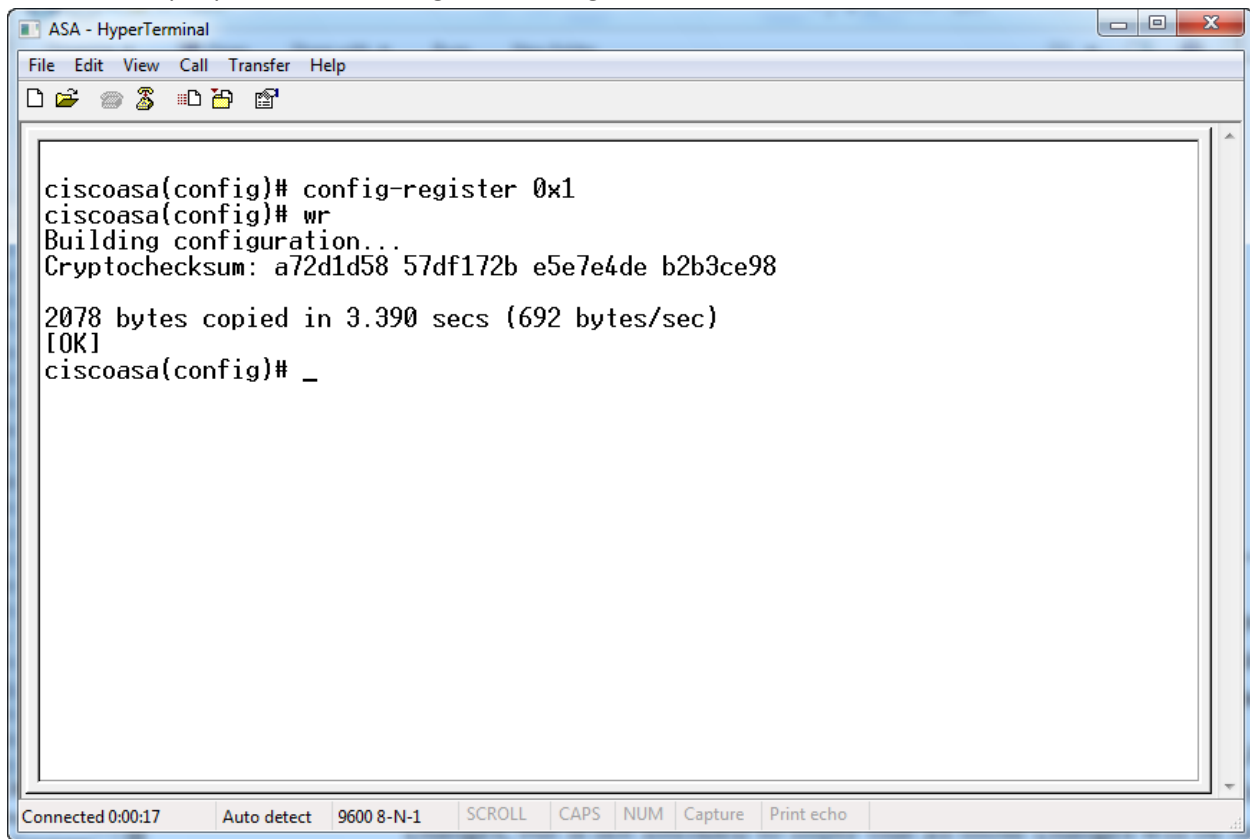
Connected 0:09:14 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Giao diện sau khi phục hồi password



```
ASA - HyperTerminal
File Edit View Call Transfer Help
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by
sending email to export@cisco.com.
***** Warning *****
Copyright (c) 1996-2010 by Cisco Systems, Inc.
Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Ignoring startup configuration as instructed by configuration register.
Type help or '?' for a list of available commands.
ciscoasa> _
Connected 0:12:08 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Cấu hình cho phép lần sau khởi động bình thường



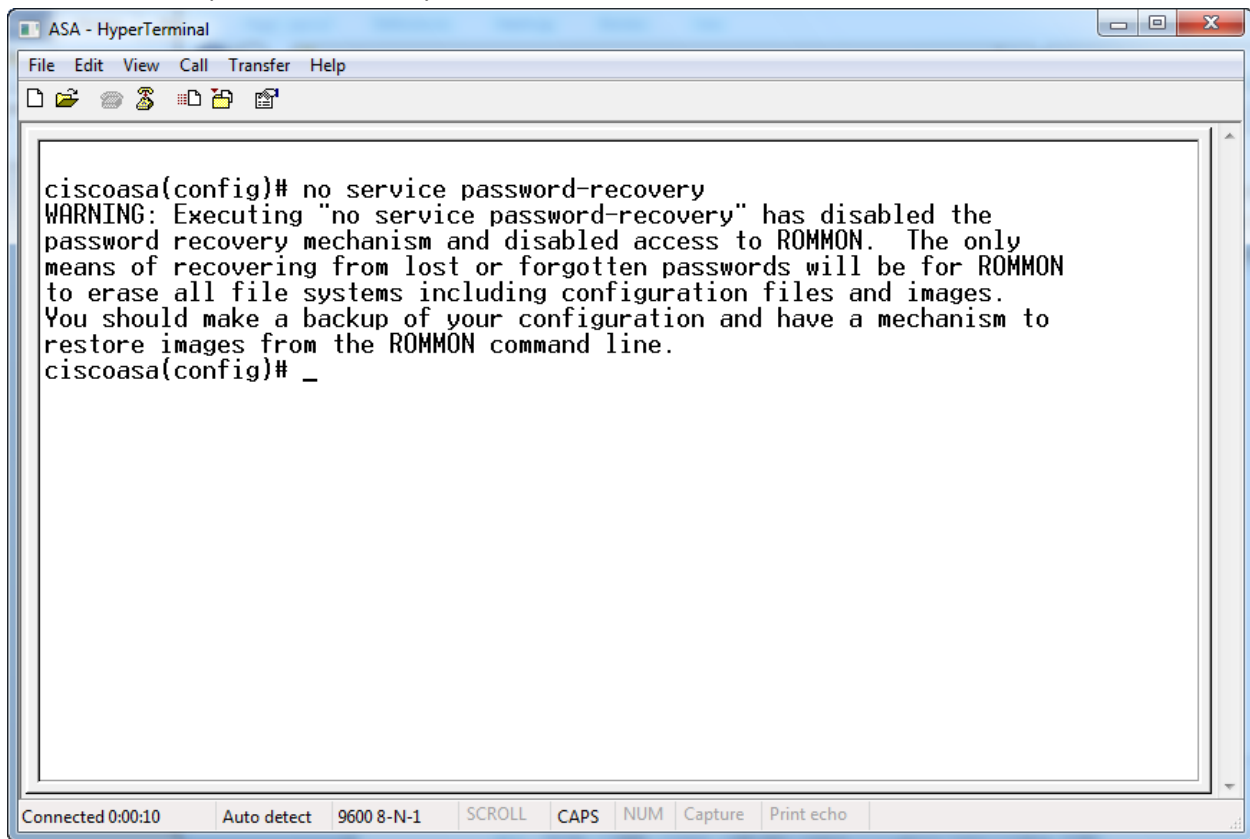
```
ASA - HyperTerminal
File Edit View Call Transfer Help
[Icons]

ciscoasa(config)# config-register 0x1
ciscoasa(config)# wr
Building configuration...
Cryptochecksum: a72d1d58 57df172b e5e7e4de b2b3ce98

2078 bytes copied in 3.390 secs (692 bytes/sec)
[OK]
ciscoasa(config)# _

Connected 0:00:17  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

Cấu hình service password-recovery

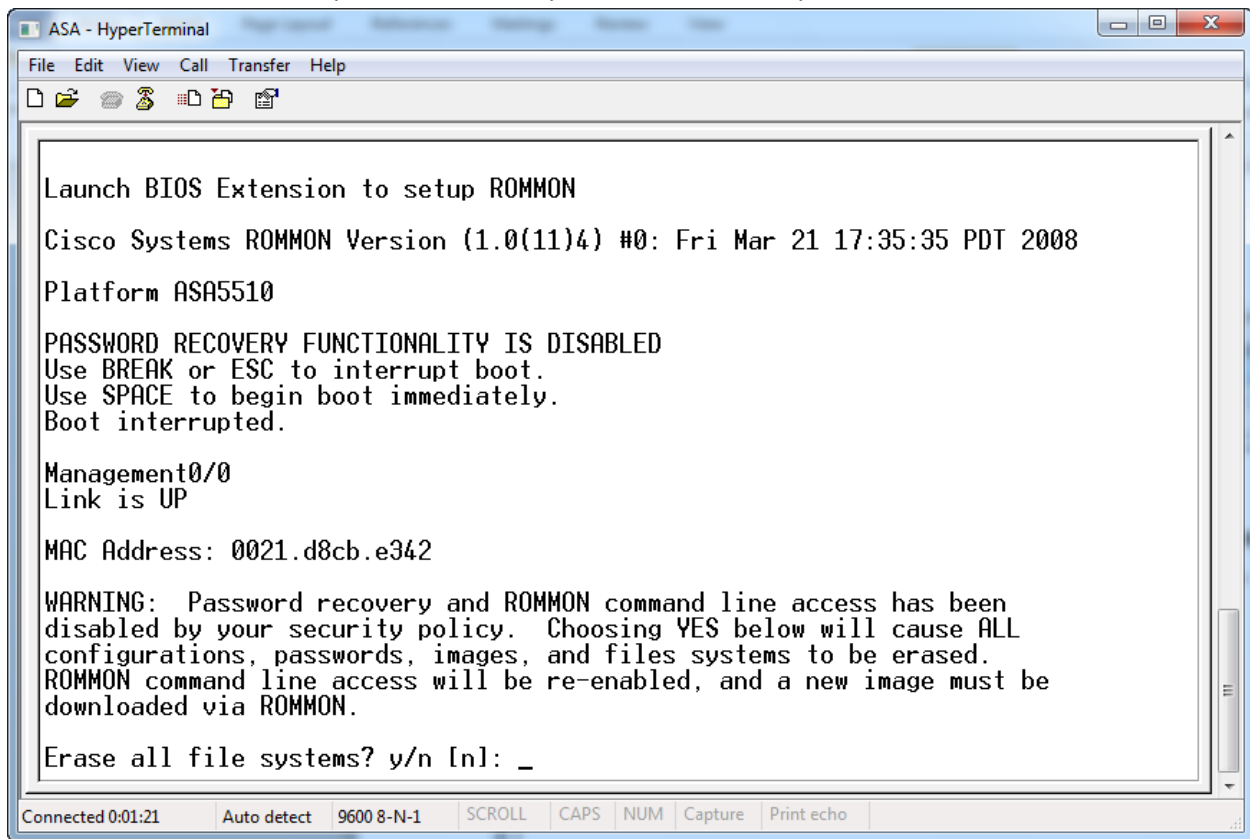


```
ASA - HyperTerminal
File Edit View Call Transfer Help
[Icons]

ciscoasa(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the
password recovery mechanism and disabled access to ROMMON. The only
means of recovering from lost or forgotten passwords will be for ROMMON
to erase all file systems including configuration files and images.
You should make a backup of your configuration and have a mechanism to
restore images from the ROMMON command line.
ciscoasa(config)# _

Connected 0:00:10  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

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



```
ASA - HyperTerminal
File Edit View Call Transfer Help
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(11)4) #0: Fri Mar 21 17:35:35 PDT 2008
Platform ASA5510
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

Management0/0
Link is UP

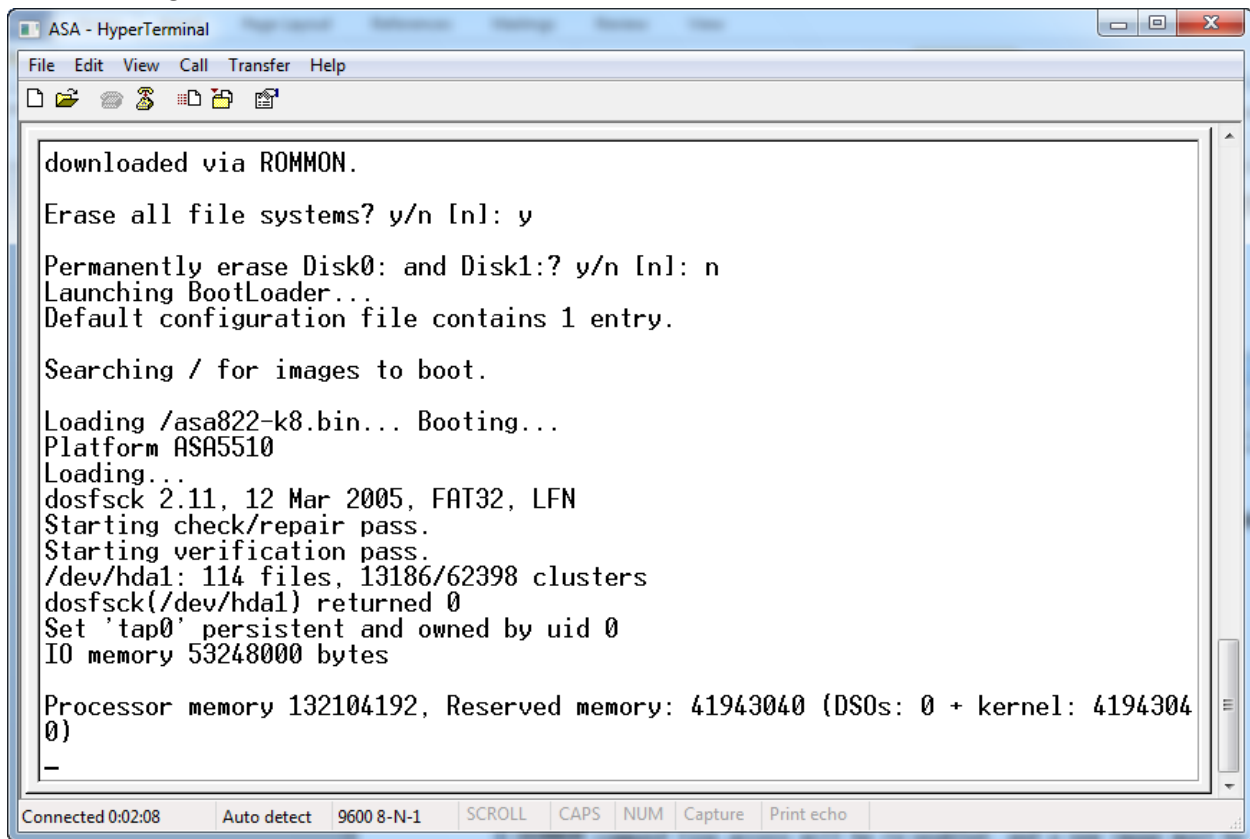
MAC Address: 0021.d8cb.e342

WARNING: Password recovery and ROMMON command line access has been
disabled by your security policy. Choosing YES below will cause ALL
configurations, passwords, images, and files systems to be erased.
ROMMON command line access will be re-enabled, and a new image must be
downloaded via ROMMON.

Erase all file systems? y/n [n]: _
```

Connected 0:01:21 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

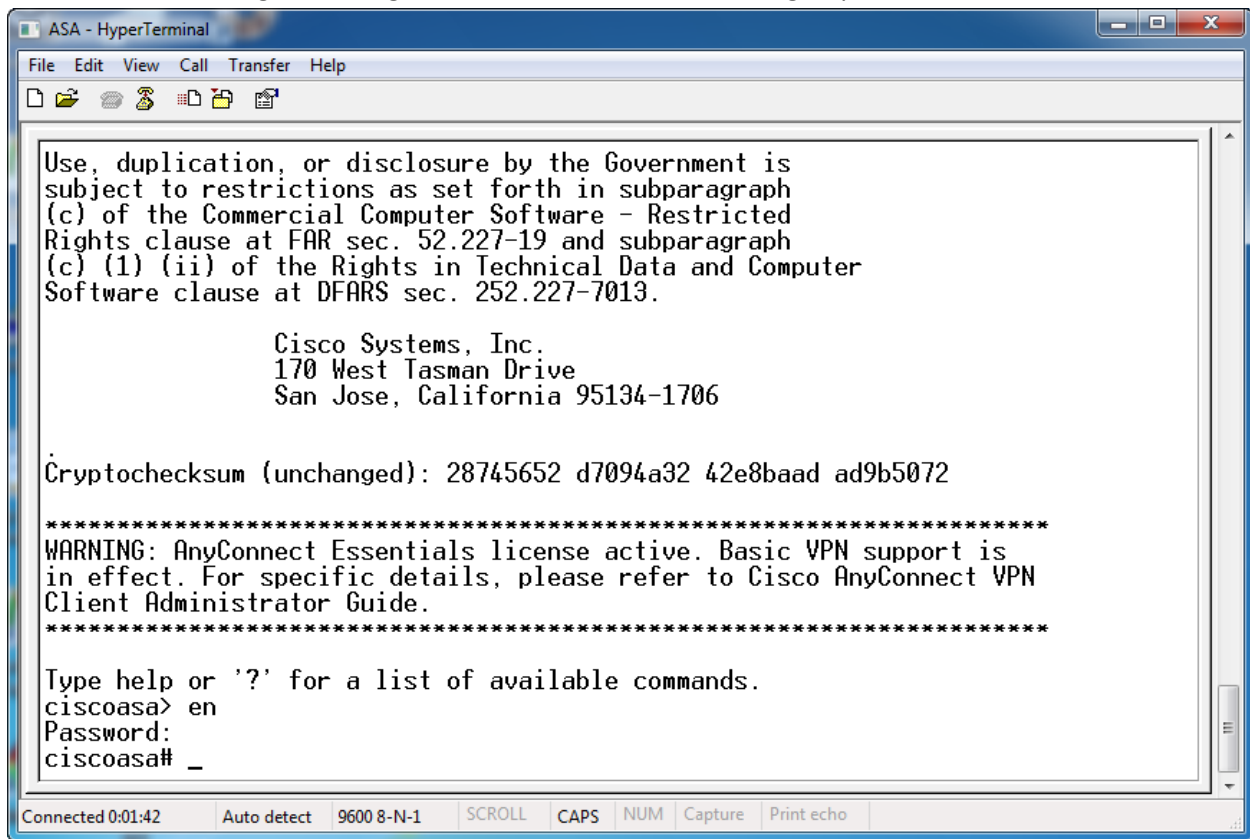
ASA khởi động lại

A screenshot of a HyperTerminal window titled "ASA - HyperTerminal". The window shows the boot process of an ASA device. The text displayed is as follows:

```
downloaded via ROMMON.  
Erase all file systems? y/n [n]: y  
Permanently erase Disk0: and Disk1:? y/n [n]: n  
Launching BootLoader...  
Default configuration file contains 1 entry.  
Searching / for images to boot.  
Loading /asa822-k8.bin... Booting...  
Platform ASA5510  
Loading...  
dosfsck 2.11, 12 Mar 2005, FAT32, LFN  
Starting check/repair pass.  
Starting verification pass.  
/dev/hda1: 114 files, 13186/62398 clusters  
dosfsck(/dev/hda1) returned 0  
Set 'tap0' persistent and owned by uid 0  
IO memory 53248000 bytes  
  
Processor memory 132104192, Reserved memory: 41943040 (DSOs: 0 + kernel: 41943040)  
-
```

The status bar at the bottom of the window shows "Connected 0:02:08", "Auto detect", "9600 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

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



```
ASA - HyperTerminal
File Edit View Call Transfer Help
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cryptochecksum (unchanged): 28745652 d7094a32 42e8baad ad9b5072

*****
WARNING: AnyConnect Essentials license active. Basic VPN support is
in effect. For specific details, please refer to Cisco AnyConnect VPN
Client Administrator Guide.
*****

Type help or '?' for a list of available commands.
ciscoasa> en
Password:
ciscoasa# _

Connected 0:01:42 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

