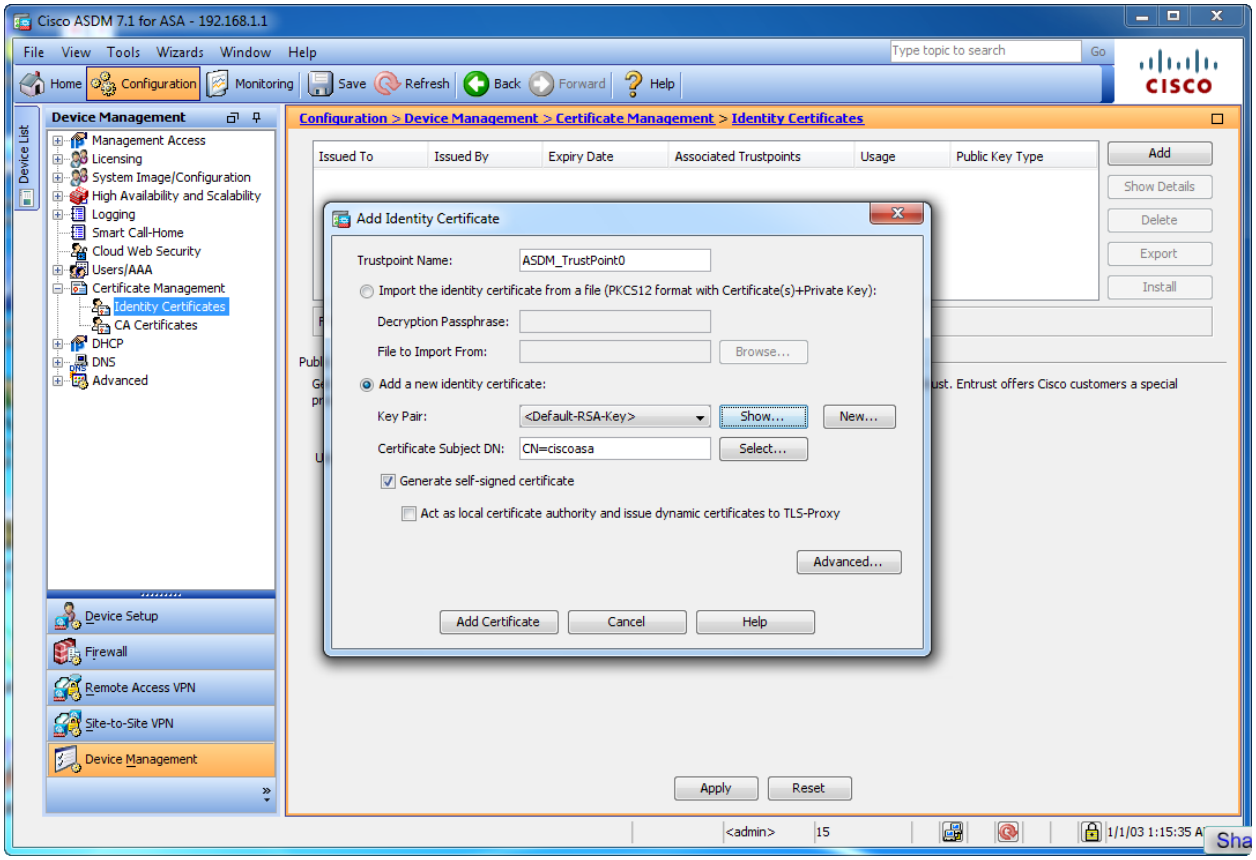
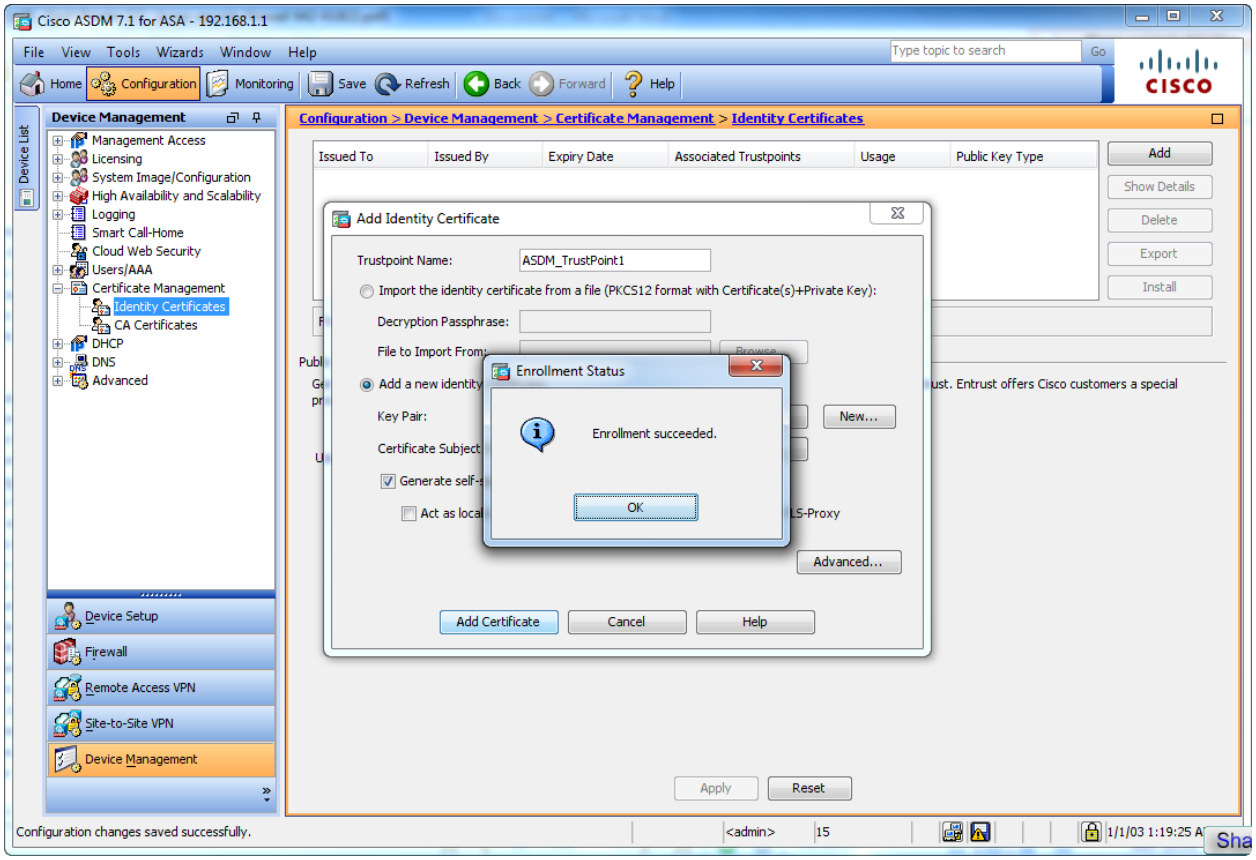
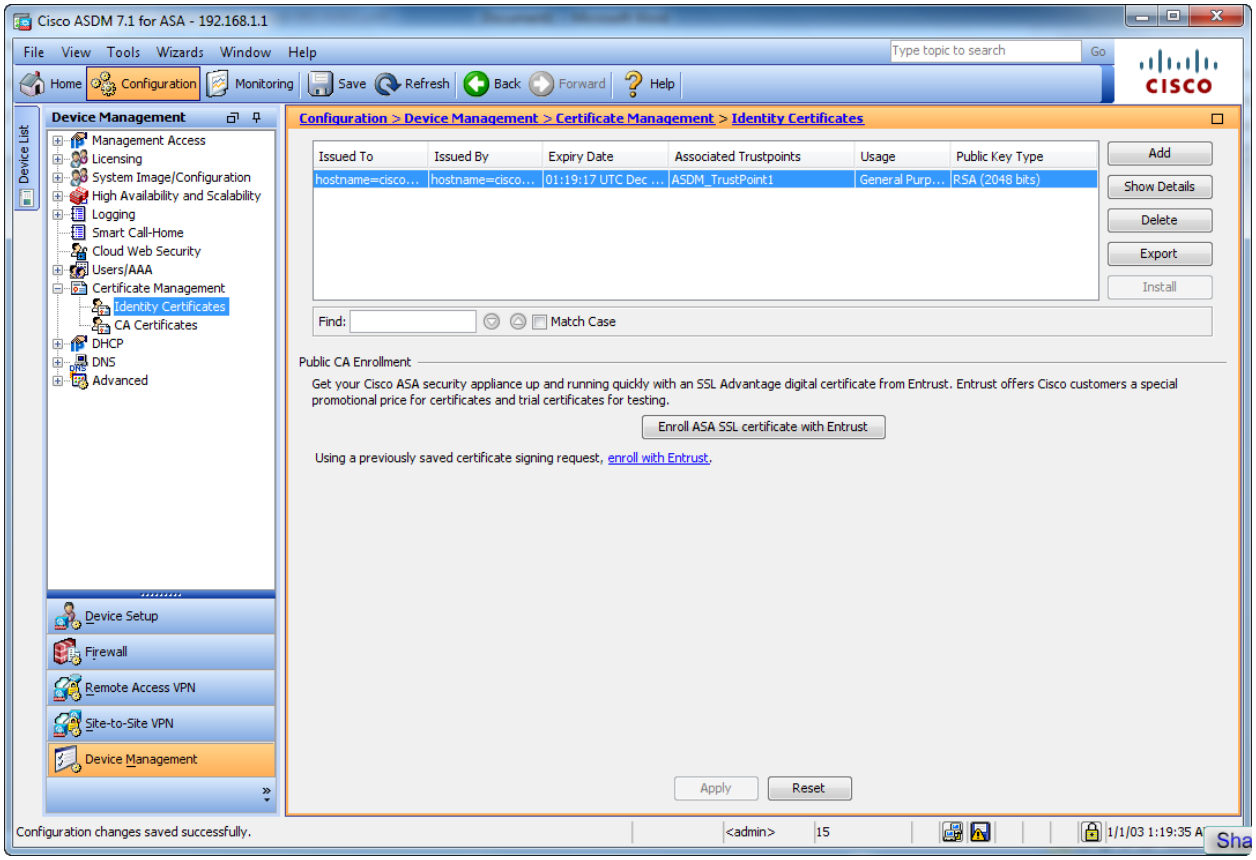
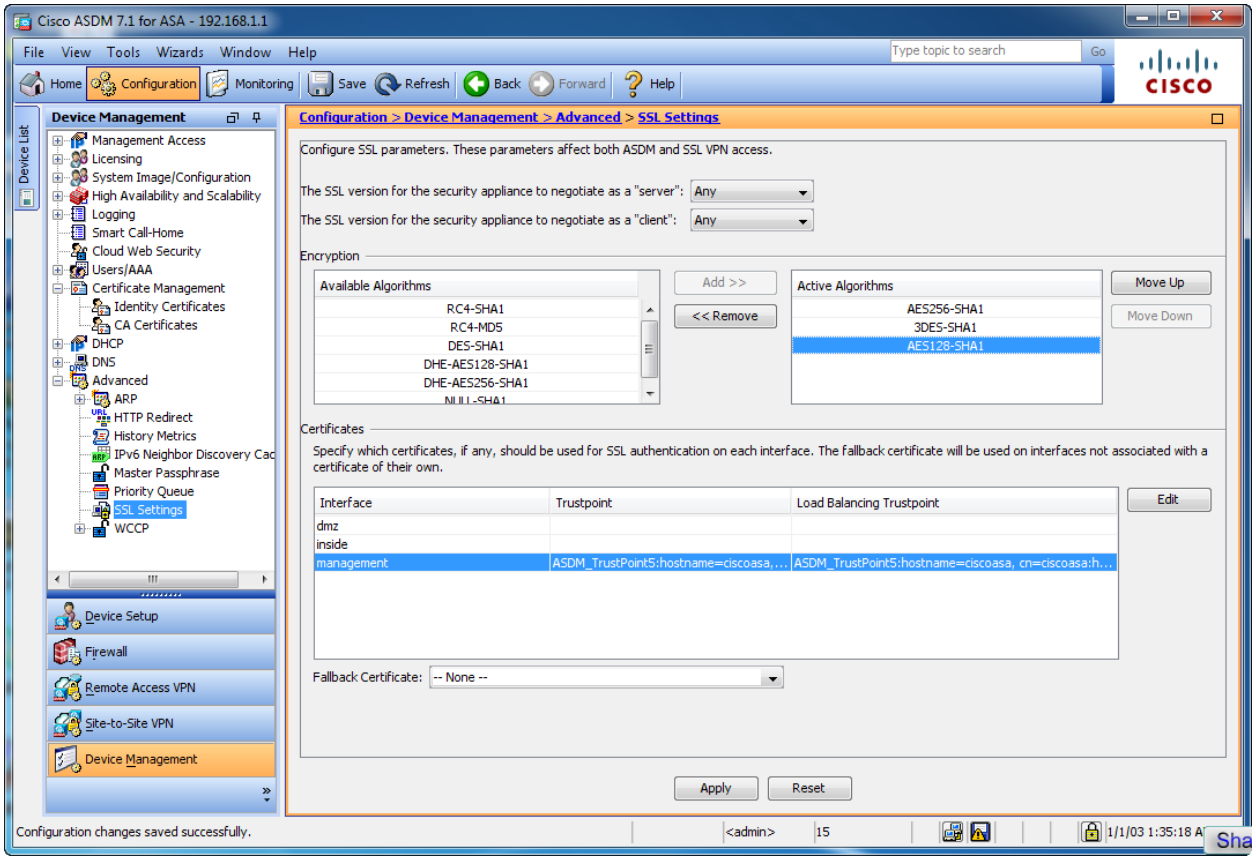
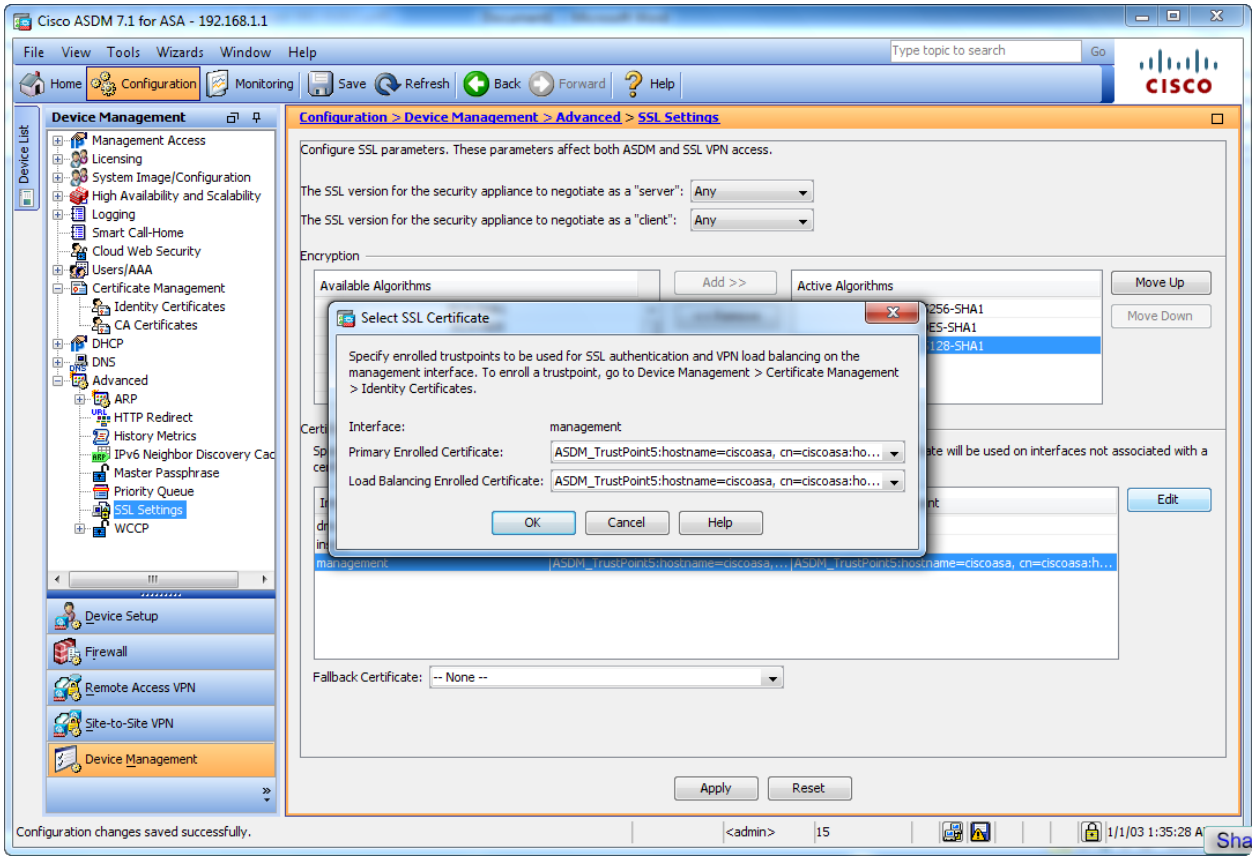
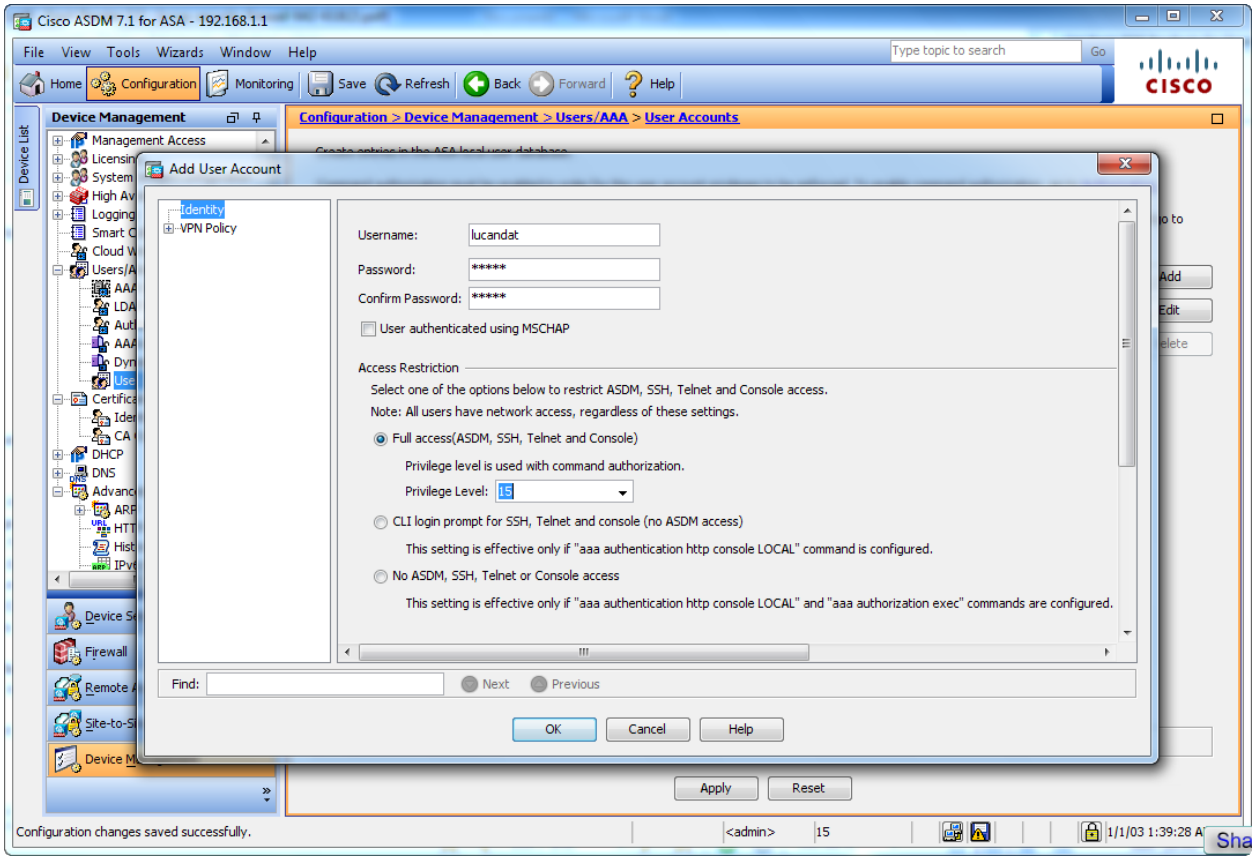

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalability
Logging
Smart Call-Home
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
1/1/03 1:15:35 A

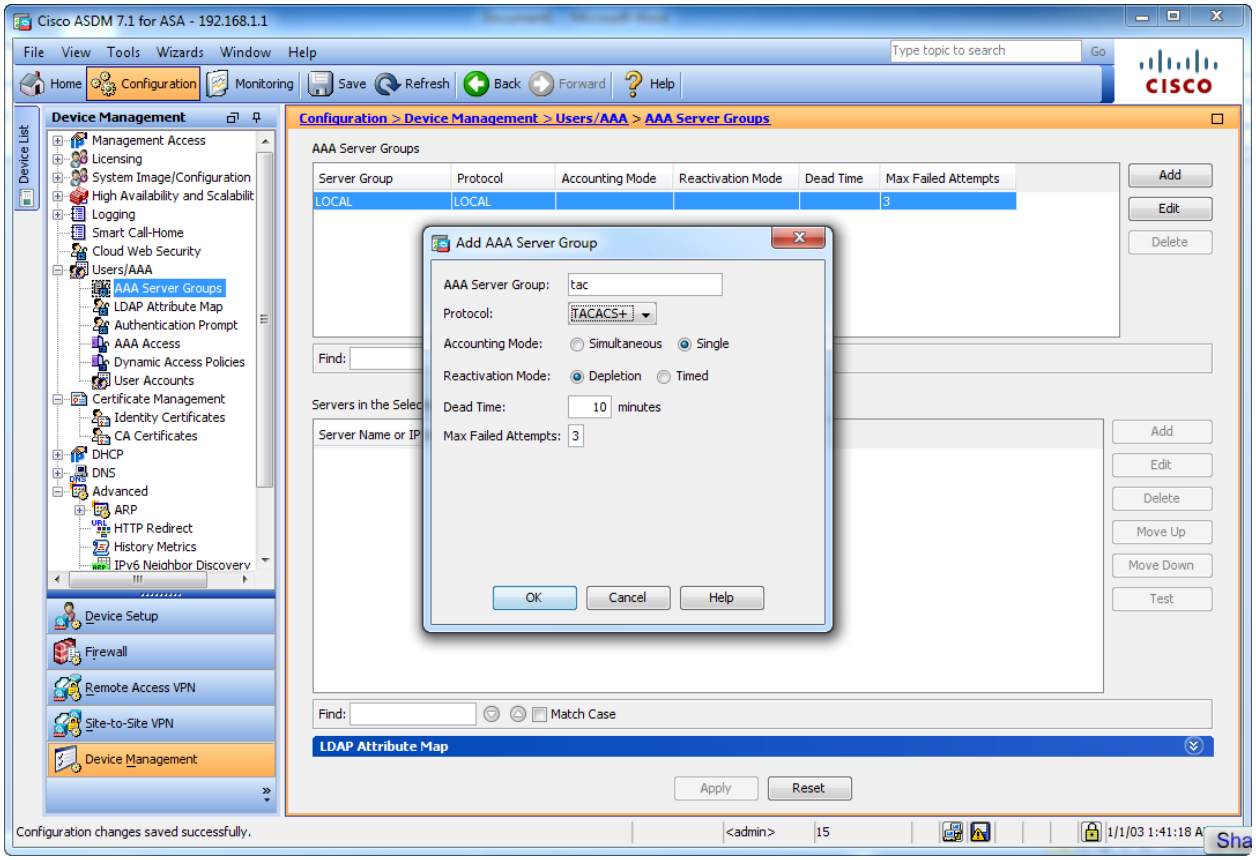

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalability
Logging
Smart Call-Home
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_TrustPoint1
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
Key Pair:
New...
Certificate Subject
Generate self-
Act as loca
LS-Proxy
Advanced...
Add Certificate
Cancel
Help
Enrollment Status
Enrollment succeeded.
OK
ust. Entrust offers Cisco customers a special
Apply
Reset
Configuration changes saved successfully.
<admin>
15
1/1/03 1:19:25 A
Sha

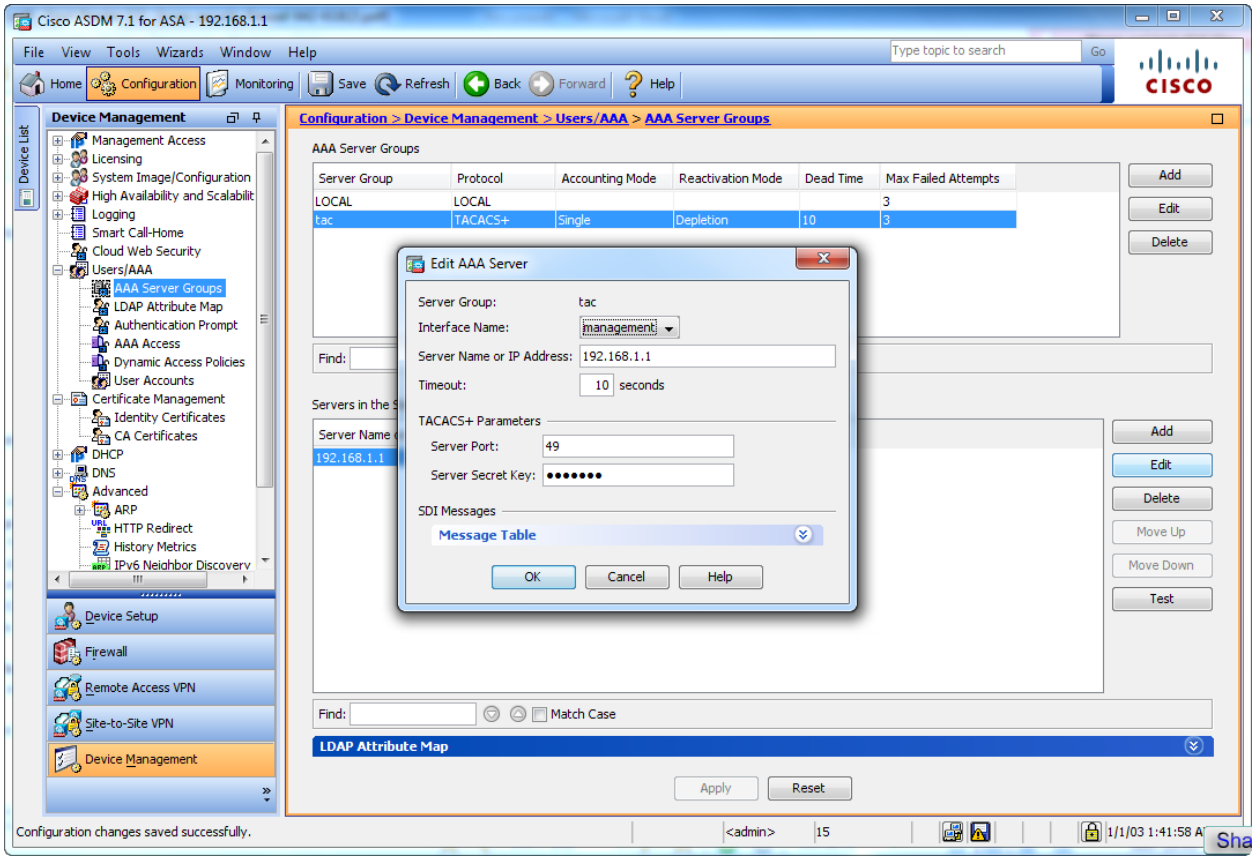

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalability
Logging
Smart Call-Home
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
hostname=cisco...
hostname=cisco...
01:19:17 UTC Dec ...
ASDM_TrustPoint1
General Purp...
RSA (2048 bits)
Add
Show Details
Delete
Export
Install
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

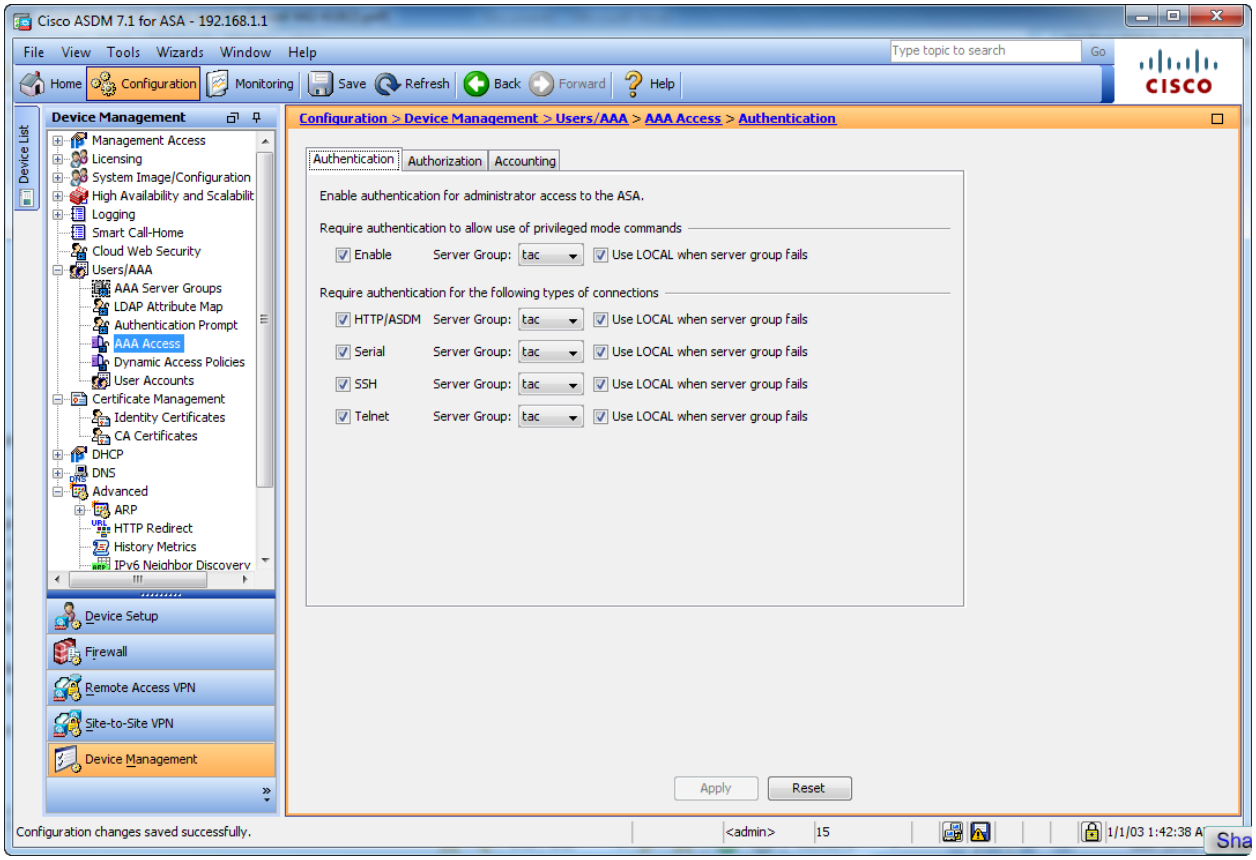

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalability
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
Certificate Management
Identity Certificates
CA Certificates
DHCP
DNS
Advanced
ARP
HTTP Redirect
History Metrics
IPv6 Neighbor Discovery Cac
Master Passphrase
Priority Queue
SSL Settings
WCCP
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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
Add >>
<< Remove
Active Algorithms
AES256-SHA1
3DES-SHA1
AES128-SHA1
Move Up
Move Down
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

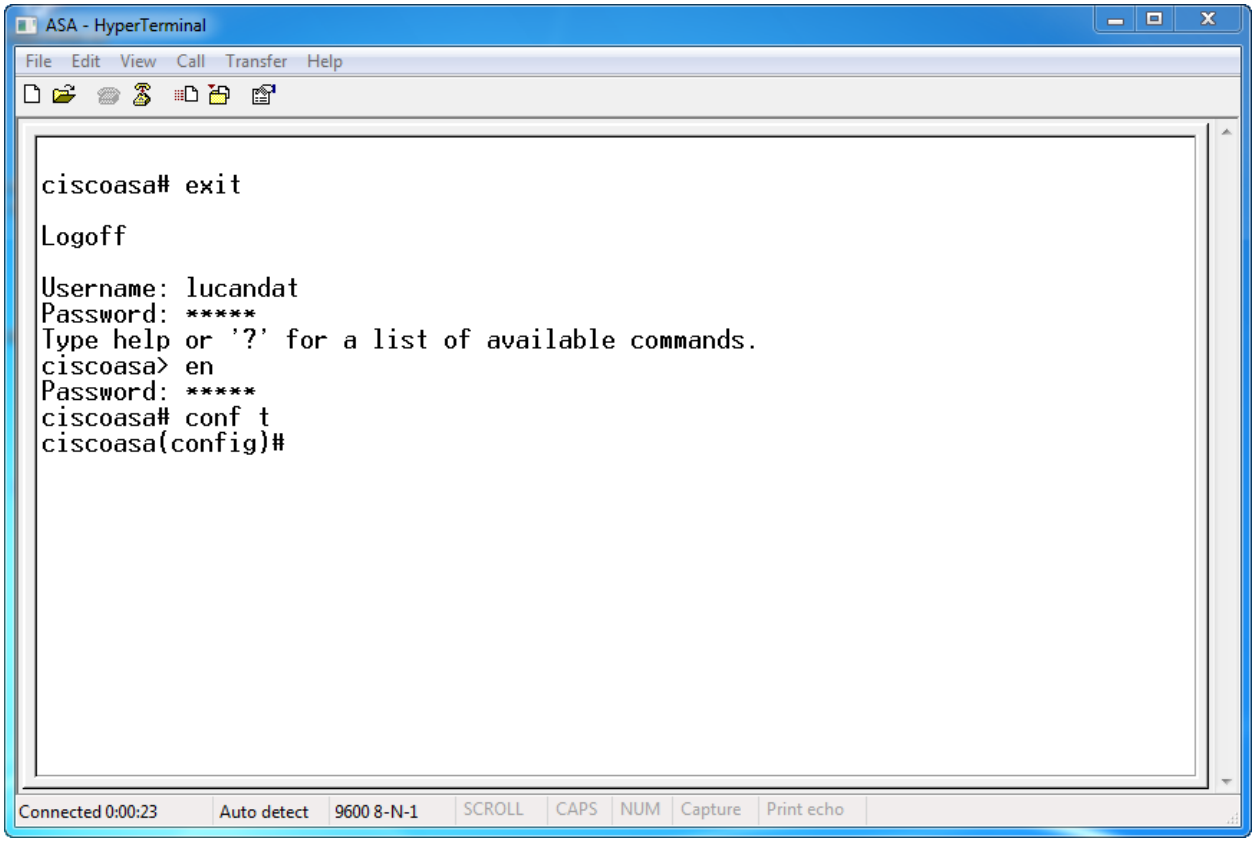

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalability
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
Certificate Management
Identity Certificates
CA Certificates
DHCP
DNS
Advanced
ARP
HTTP Redirect
History Metrics
IPv6 Neighbor Discovery Cac
Master Passphrase
Priority Queue
SSL Settings
WCCP
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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
Add >>
Active Algorithms
Move Up
Move Down
256-SHA1
ES-SHA1
128-SHA1
Select SSL Certificate
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.
Interface: management
Primary Enrolled Certificate: ASDM_TrustPoint5:hostname=ciscoasa, cn=ciscoasa:ho...
Load Balancing Enrolled Certificate: ASDM_TrustPoint5:hostname=ciscoasa, cn=ciscoasa:ho...
OK
Cancel
Help
te will be used on interfaces not associated with a
Edit
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 1:35:28 A
Sha

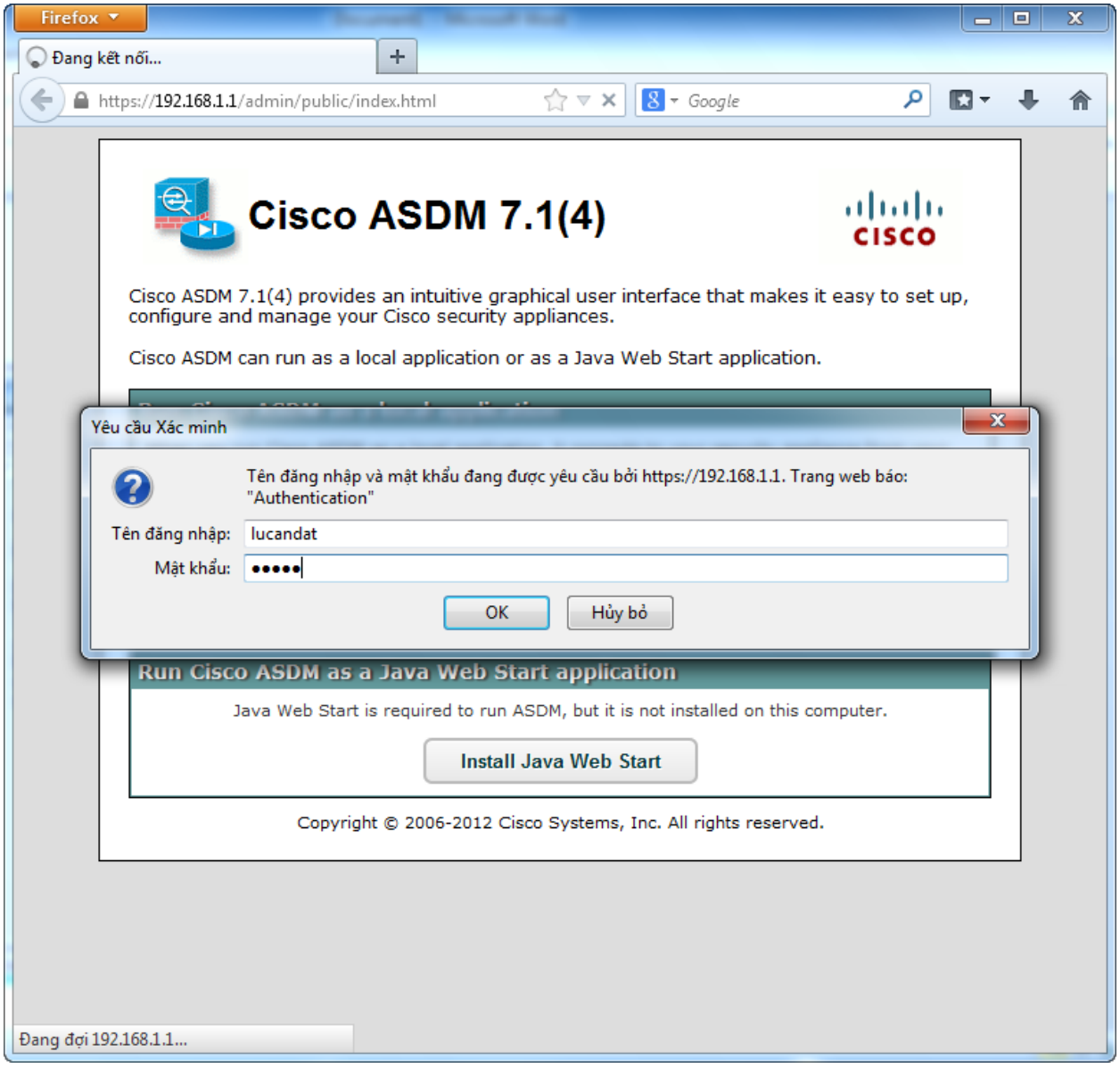

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
Licensing
System
High Av
Logging
Smart C
Cloud W
Users/A
AAA
LDA
Auth
AAA
Dyn
Use
Certifica
Ide
CA
DHCP
DNS
Advanc
ARP
HTT
Hist
IPv
Device Se
Firewall
Remote A
Site-to-Si
Device M
Configuration > Device Management > Users/AAA > User Accounts
Add
Edit
elete
Apply
Reset
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
Configuration changes saved successfully.
<admin>
15
1/1/03 1:39:28 A
Sha

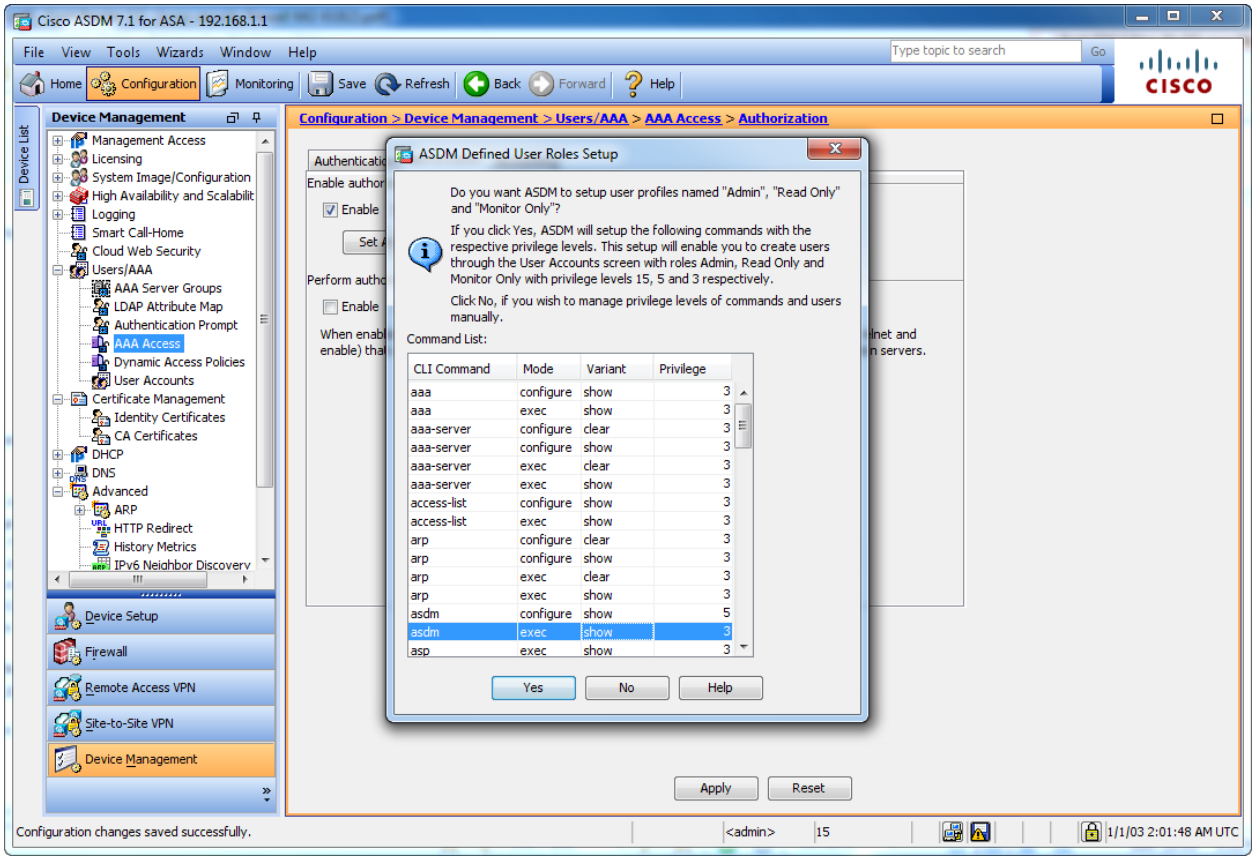

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
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 Discovery
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Management > Users/AAA > AAA Server Groups
AAA Server Groups
Server Group
Protocol
Accounting Mode
Reactivation Mode
Dead Time
Max Failed Attempts
LOCAL
LOCAL
3
Add
Edit
Delete
Find:
Servers in the Selec
Server Name or IP
Add
Edit
Delete
Move Up
Move Down
Test
Find:
Match Case
LDAP Attribute Map
Apply
Reset
Add AAA Server Group
AAA Server Group:
tac
Protocol:
TACACS+
Accounting Mode:
Simultaneous
Single
Reactivation Mode:
Depletion
Timed
Dead Time:
10
minutes
Max Failed Attempts:
3
OK
Cancel
Help
Configuration changes saved successfully.
<admin>
15
1/1/03 1:41:18 A
Sha

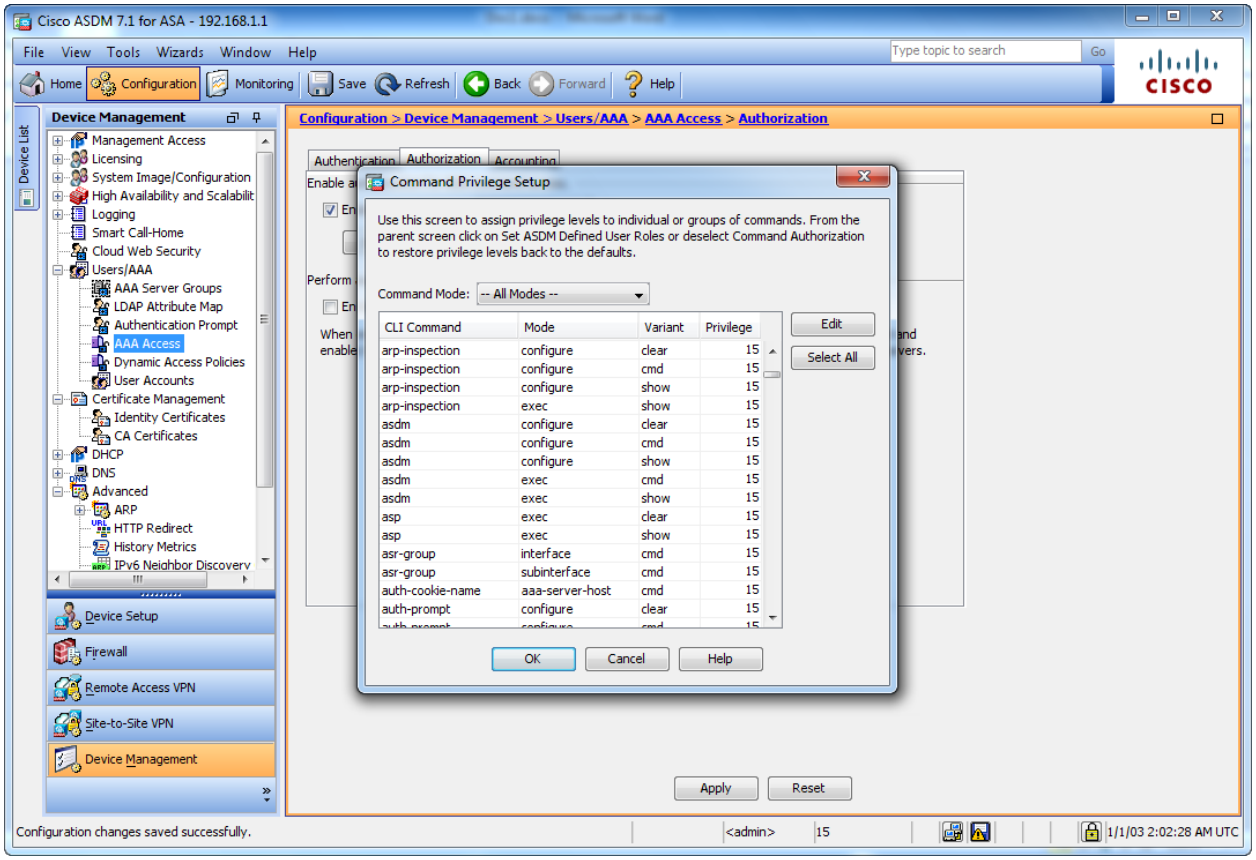

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Go
Home Configuration Monitoring Save Refresh Back Forward Help
CISCO
Device List
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
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 Discovery
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Device Management > Users/AAA > AAA Server Groups
AAA Server Groups
Server Group
Protocol
Accounting Mode
Reactivation Mode
Dead Time
Max Failed Attempts
LOCAL
LOCAL
3
tac
TACACS+
Single
Depletion
10
3
Add
Edit
Delete
Find:
Servers in the S
Server Name
192.168.1.1
Add
Edit
Delete
Move Up
Move Down
Test
Find:
Match Case
LDAP Attribute Map
Apply
Reset
Edit AAA Server
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: •••••••
SDI Messages
Message Table
OK
Cancel
Help
Configuration changes saved successfully.
<admin>
15
1/1/03 1:41:58 A
Sha

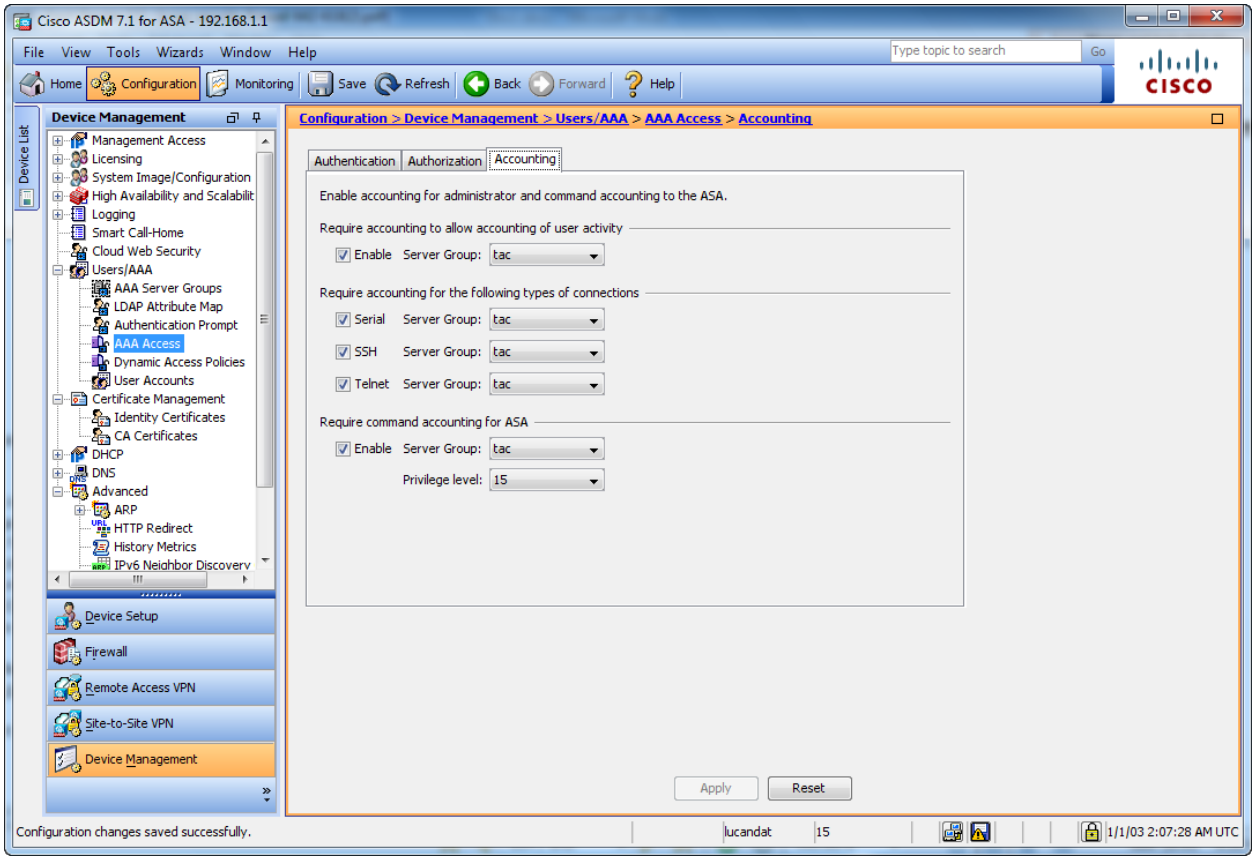

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Type topic to search
Home Configuration Monitoring Save Refresh Back Forward Help
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
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 Discovery
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
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: 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
Apply Reset
Configuration changes saved successfully.
<admin> 15

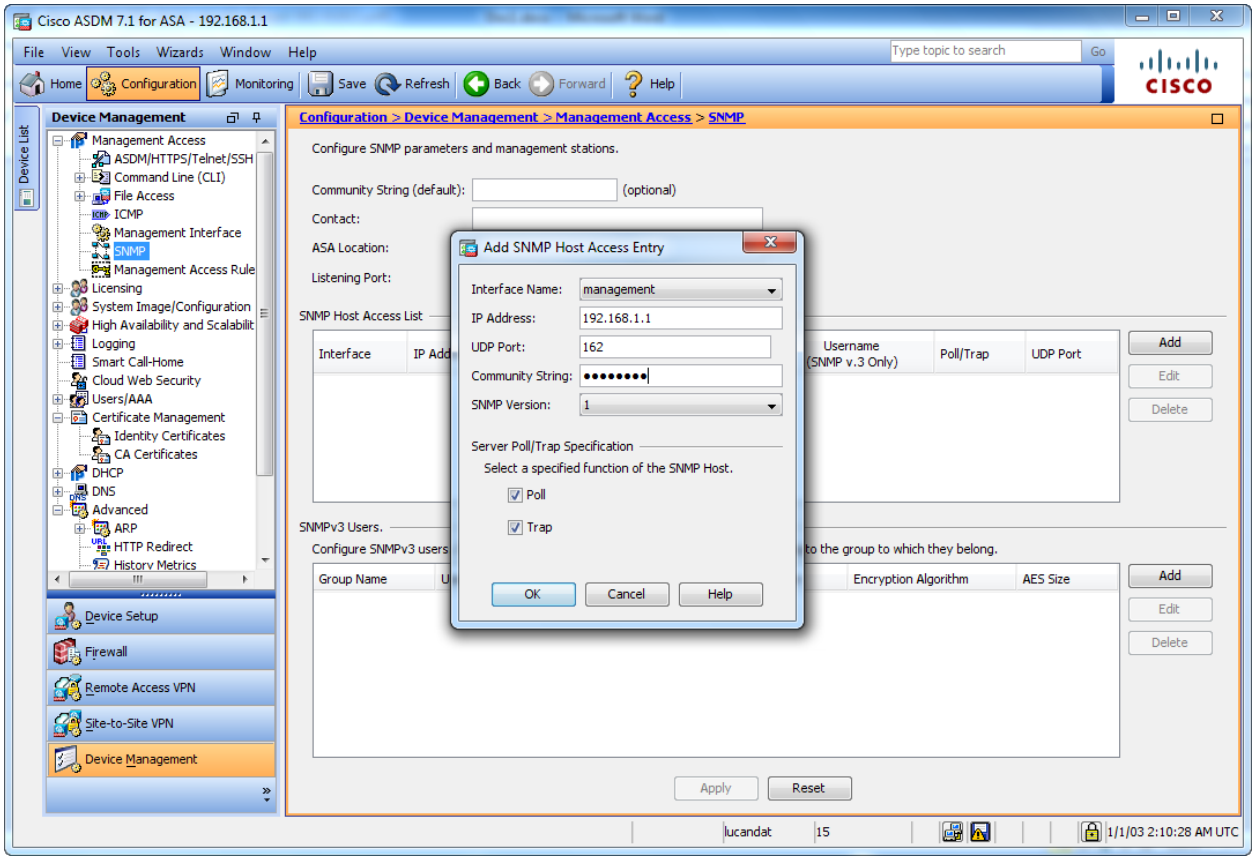

ASA - HyperTerminal
File Edit View Call Transfer Help
ciscoasa# exit
Logoff
Username: lucandat
Password: *****
Type help or '?' for a list of available commands.
ciscoasa> en
Password: *****
ciscoasa# conf t
ciscoasa(config)#
Connected 0:00:23 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

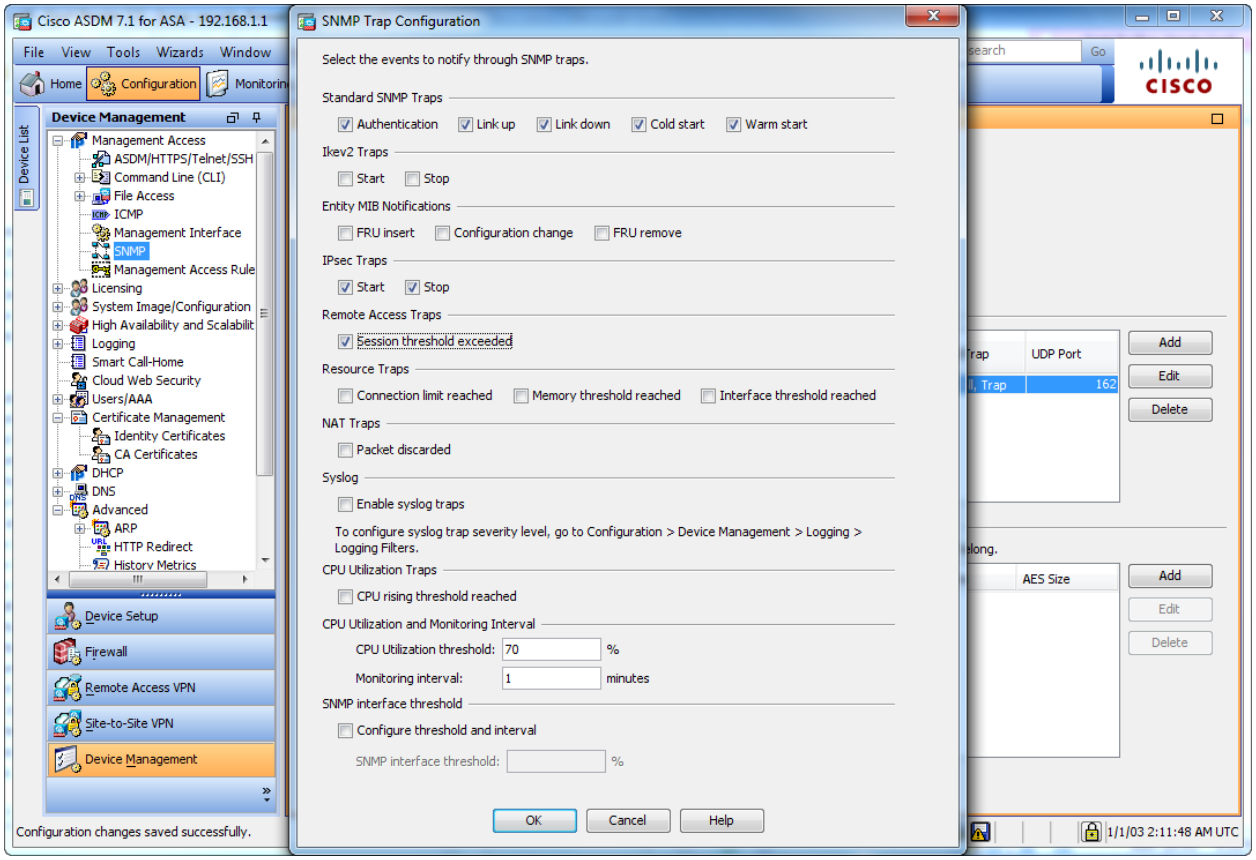

Firefox
Đang kết nối...
https://192.168.1.1/admin/public/index.html
Google
Cisco ASDM 7.1(4)
cisco
Cisco ASDM 7.1(4) provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco security appliances.
Cisco ASDM can run as a local application or as a Java 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...

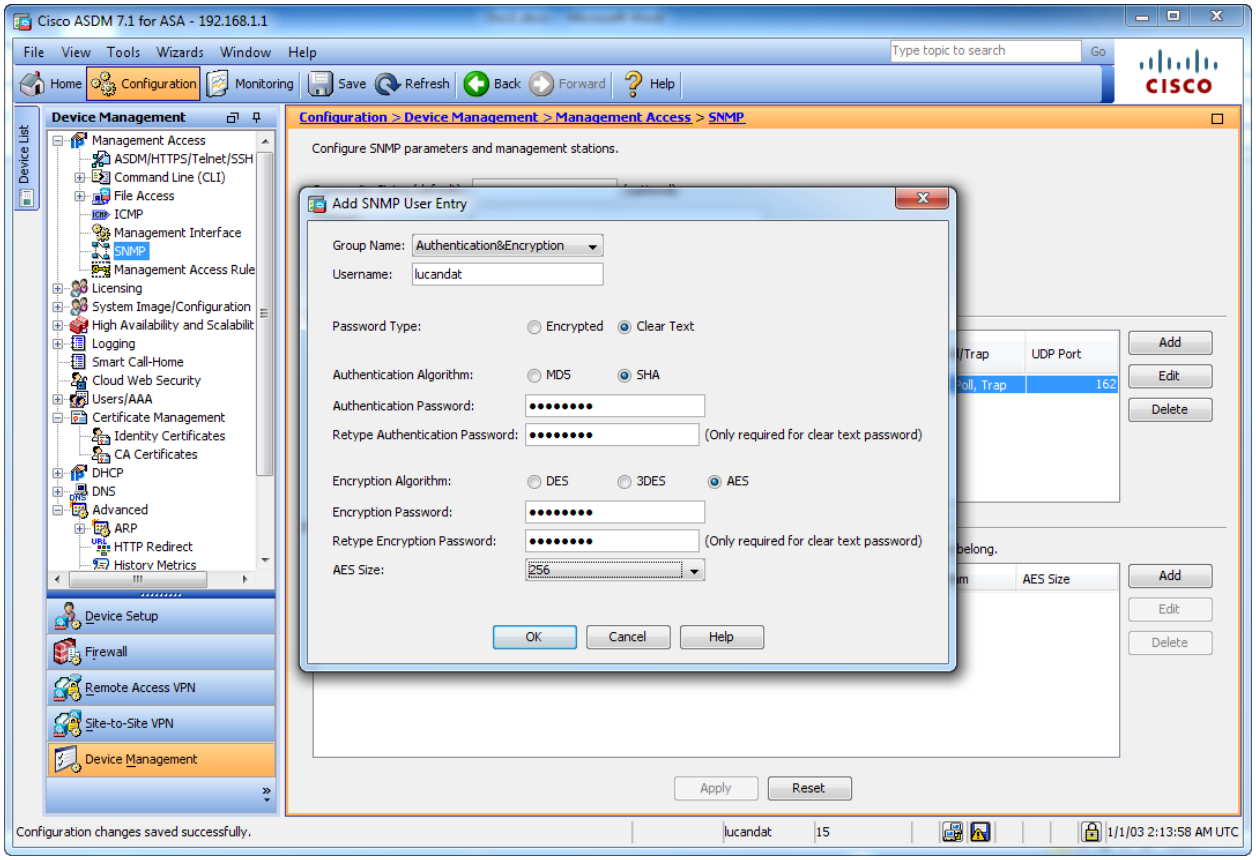

Cisco ASDM 7.1 for ASA - 192.168.1.1
File View Tools Wizards Window Help
Home Configuration Monitoring Save Refresh Back Forward Help
Device Management
Management Access
Licensing
System Image/Configuration
High Availability and Scalabilit
Logging
Smart Call-Home
Cloud Web Security
Users/AAA
AAA Server 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 Discovery
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
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
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
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 Discovery
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 Discovery
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 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
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.
Community String (default):
(optional)
Contact:
ASA Location:
Listening Port:
SNMP Host Access List
Interface
IP Add
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 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 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
UDP Port
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
Poll, 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