Cisco ASA configuration for SMS
PASSCODE

© SMS PASSCODE® 2014
Introduction

SMS PASSCODE® is widely used by Cisco customers extending the Cisco ASA VPN concentrators with both IPsec and SSL VPN extensions. This document provides a visual step-by-step guide for configuring the system to support SMS PASSCODE®.

Cisco Setup VPN group and radius client

1. Start ASDM and login to the Web interface.
2. Go to the wizards menu and select IPsec VPN Wizard or SSL VPN Wizard (the following is from IPsec wizard, but configuration is quite similar)
3. Select Remote Access and click next:

![VPN Wizard](image)

4. Select the Cisco VPN Client option and click next:
5. Click next once you have set the Pre-Shared Key parameter:

![VPN Wizard](image1)

6. Name the Server Group Name: SMS PASSCODE® and set the IP address and the Server Secret key and click ok:

![New Authentication Server Group](image2)

7. Select the AAA server option and select the SMSPasscode Group

![User Authentication](image3)
8. Select the SMS Pool Name from the pull-down menu and click next. If you do not have a pool defined, click New… and create the IP pool, select it and click next:

9. Set encryption to 3DES, Authentication to SHA and Diffie-Hellman Group to 2 and click next:

10. Verify “Enable Perfect Forwarding Secrecy (PFS) is checked and click next:
11. You have now set up the Cisco ASA for SMS PASSCODE® two-factor authentication.

Optional setup of the VPN concentrator using command line interface (CLI)

To use the command line interface, access the Cisco ASA VPN concentrator through the command line window and configure it as follows:

access-list inside_nat0_outbound line 4 extended permit ip any 10.255.253.0 255.255.255.240

aaa-server SMSPasscode protocol radius

aaa-server SMSPasscode (inside) host 10.10.10.10
timeout 5
key ********
tunnel-group GroupNameHasToMachOnVPNClient type remote-access
tunnel-group GroupNameHasToMachOnVPNClient general-attributes

authentication-server-group SMSPasscode

address-pool SMS
tunnel-group GroupNameHasToMachOnVPNClient ipsec-attributes

pre-shared-key ********
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs group1
Configuring SMS PASSCODE® authentication for radius

To set-up SMS PASSCODE® for RADIUS, please consult the SMS PASSCODE® Administrators Guide under the section “Configuring RADIUS Protection.”

Using MSCHAPv2 protocol

To use MSCHAPv2 protocol instead of PAP the ASA must have a bugfix for CSCtr85499 which should have been fixed in the following releases (please check cisco.com for CSCtr85499 for updated information):

- 8.4(4.2)
- 8.4(5)
- 8.6(1.4)
- 9.0(1)
- 9.1(1)
- 9.0(0.99)
- 100.8(0.133)M
- 100.8(33.4)M
- 100.7(13.75)M
- 100.8(11.21)M
- 100.7(6.79)M
- 100.9(2.1)M
- 100.8(27.7)M
- 100.9(0.1)M
- 8.4(4.99)
- 100.8(34.1)M

When creating the AAA radius server make sure to enable Microsoft CHAPv2 capable
And in the Connection Profile “Enable password management”

In SMS PASSCODE configuration tool you must make sure that Side-by-side to always

And that there is a Network Policy allowing the user to log in and change password via the MSCHAPv2 protocol.
Password change

A normal logon flow with password change through AnyConnect or Clientless SSLVPN would look like this:

Due to a bug in Cisco ASA password change is not possible via AnyConnect if the Anyconnect Client Software package is 3.0.x or 3.1.x but working with 2.5.x and below.
So if password change is needed please make sure that the image is not on 3.x

Logon and password change will work fine with 3.x AnyConnect, but if password change will fail with this error after reentering current password.
Authorization

SMS PASSCODE® support extension of a VPN connection with authorization detail. E.g. SMS PASSCODE® can read the individual users group memberships in Active Directory and if there are Dynamic Access Policies defined, SMS PASSCODE® can parse relevant membership attributes to the ASA Radius Client.

This can be defined in below window or via CLI:

![Image of ASDM interface showing Dynamic Access Policy configuration]

Command line interface commands

- access-list Auth_Test line 1 extended permit ip any any (change ip any any to the appropriate)
- dynamic-access-policy-record SMS_Authorization
- description "Authorization attributes from SMS Passcode Radius"
- network-acl Auth_Test
How to configure SMS PASSCODE® Authorization

Set up SMS PASSCODE® to use authorization with attribute number 25:

Please note that the separator is a semicolon.
Setup Group policies in ASA to match the groups

And set up the pool to use the wanted address pools:
Cisco ASA configuration for SMS PASSCODE

(Radius.25 must have a value matching the attribute value from the radius server to be aware that the value is case sensitive also for group name)

To avoid problems with upper/lower case groups – it is possible to specify ADGroupname;ASAgroupname

Note; Group name in attribute is always lower case.

Configure SMS PASSCODE® for co-existence with a token solution like RSA®

You can make SMS PASSCODE® to co-exist with radius based token solutions. It is a pre-requisite that the SMS PASSCODECE radius server is configured with radius forwarding to the token solution’s radius server.

The Cisco concentrator sends the requests for both SMS PASSCODE® and the Token solution to the SMS PASSCODE® radius server. The SMS PASSCODE® radius server will then forward the Token solution’s request to the token solutions radius server.
In the SMS PASSCODE® configuration tool you specify the side-by-side as “On failure only”. Optional you can in the SMS PASSCODE® configuration tool set a regular expression that denies the token code. This will save you from a request to the AD. In example this expression for numbers: ^\d*$

See screenshot for example.

To read more about the advanced Radius configurations in SMS PASSCODE please refer to SMS PASSCODE administrators guide.