Cisco ASA configuration

Contents

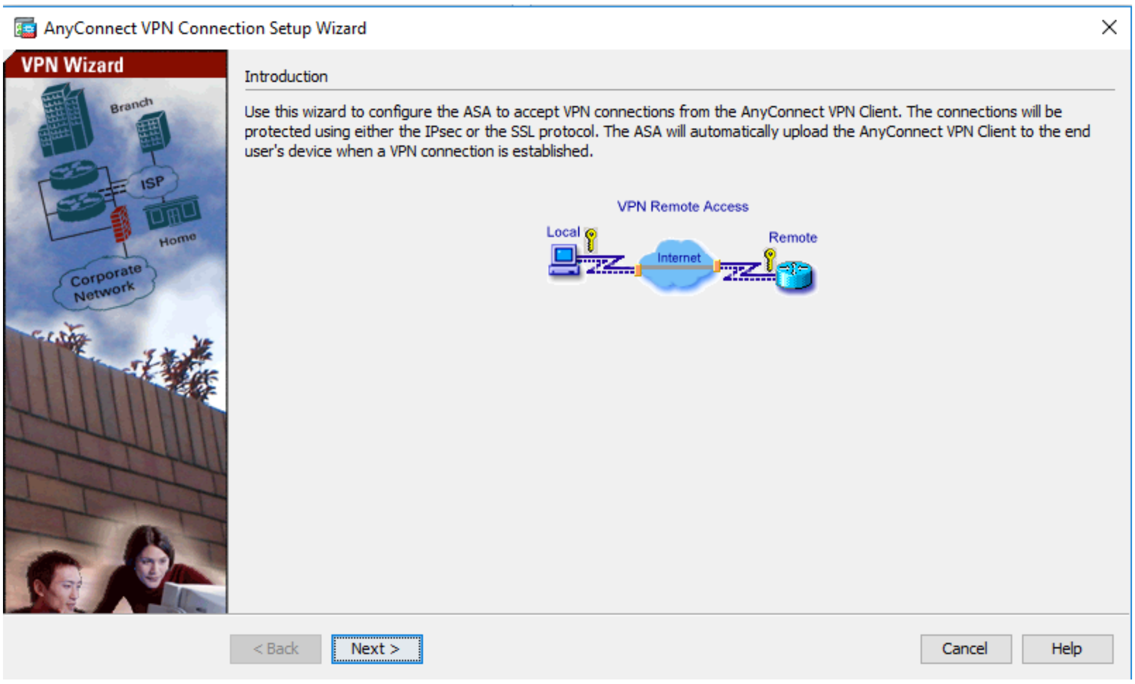
Cisco ASA configuration for SMS PASSCODE MFA

Introduction

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

Setup Cisco AnyConnect client

1. Start ASDM and login to the Web interface.
2. In the top tool bar select Wizards => VPN Wizards => AnyConnect VPN Wizard…

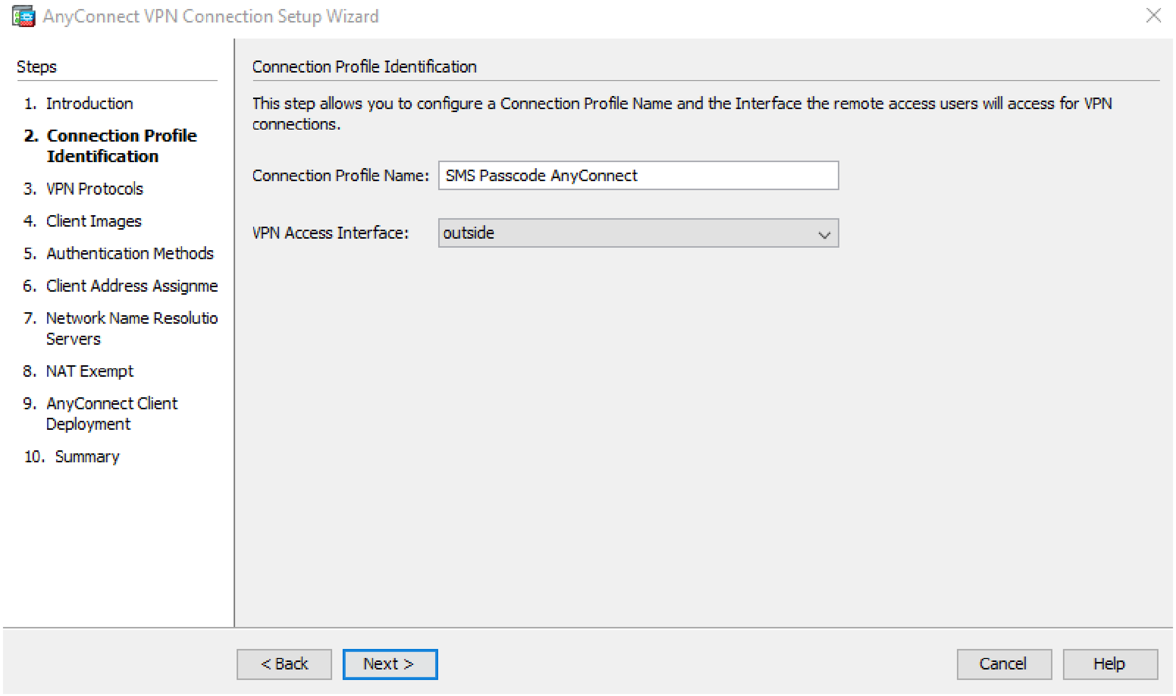


AnyConnect VPN Connection Setup Wizard

Introduction

Use this wizard to configure the ASA to accept VPN connections from the AnyConnect VPN Client. The connections will be protected using either the IPsec or the SSL protocol. The ASA will automatically upload the AnyConnect VPN Client to the end user's device when a VPN connection is established.

3. Click next and create Connection Profile Name for access to the outside interface (for this example the profile name is SMS Passcode AnyConnect):



AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. **Connection Profile Identification**
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

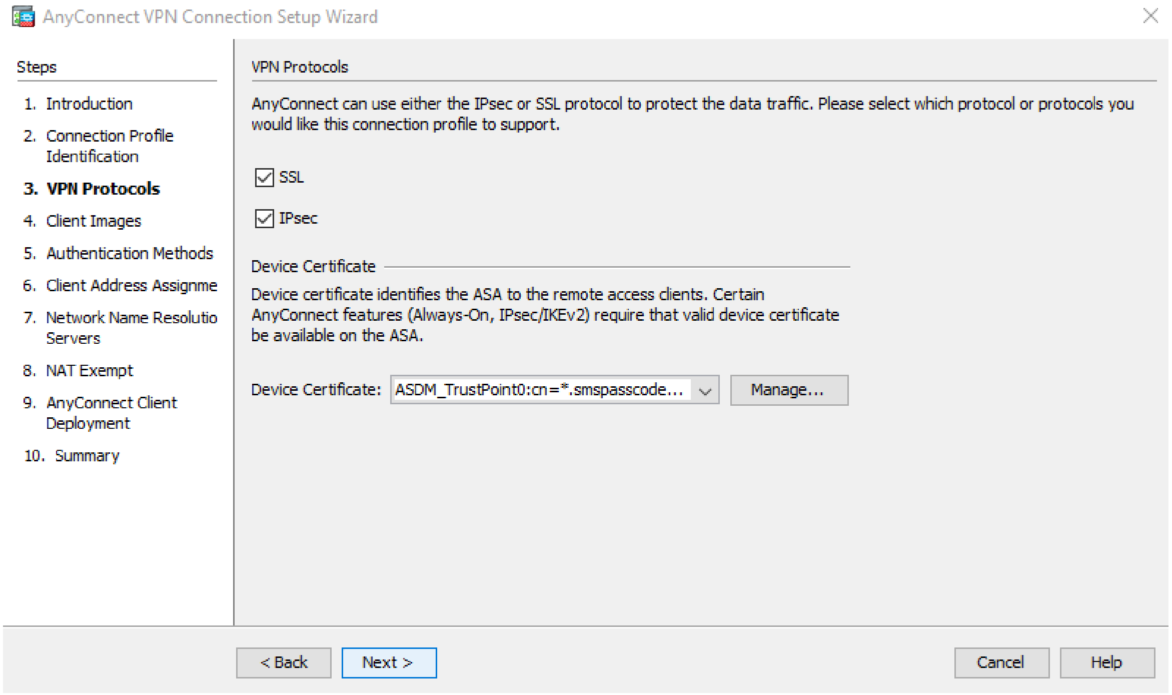
Connection Profile Identification

This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections.

Connection Profile Name: SMS Passcode AnyConnect

VPN Access Interface: outside

4. Click Next and select the VPN Protocols. You will want to select both SSL and IPsec as well as assigning a Device certificate:



AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. **VPN Protocols**
4. Client Images
5. Authentication Methods
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

VPN Protocols

AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.

☑ SSL

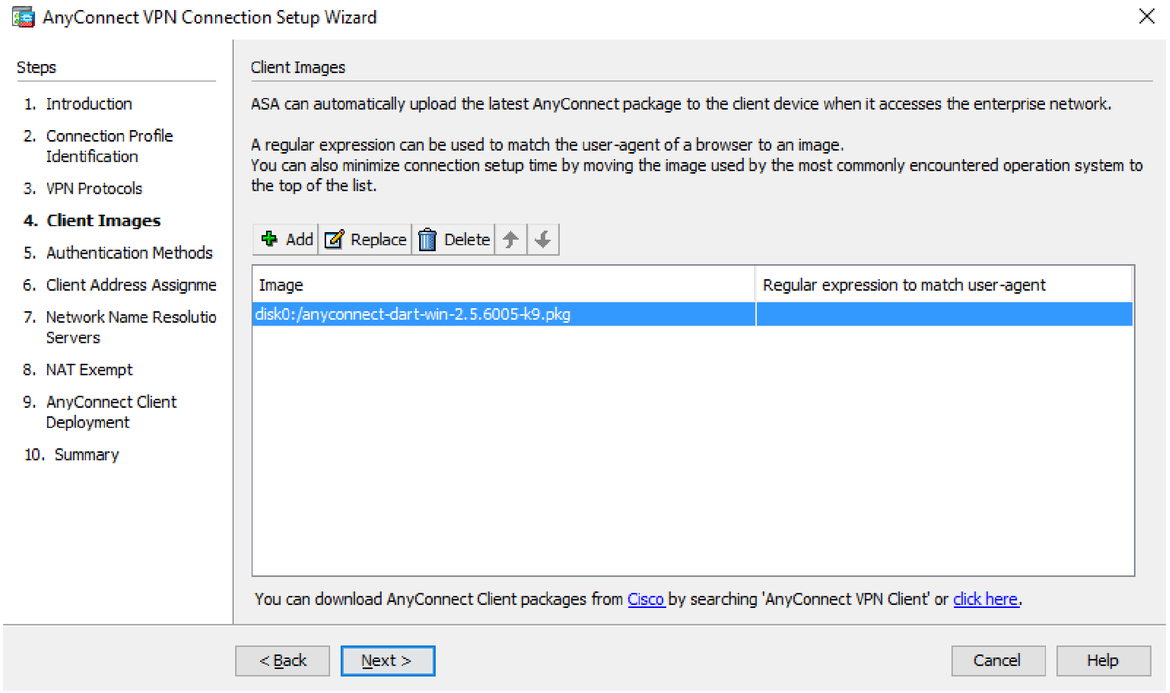
☑ IPsec

Device Certificate

Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.

Device Certificate: ASDM_TrustPoint0:cn=*.smspasscode...

5. Click next and you can choose whether or not to make the AnyConnect software available from the ASA:



AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. **Client Images**
5. Authentication Methods
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Client Images

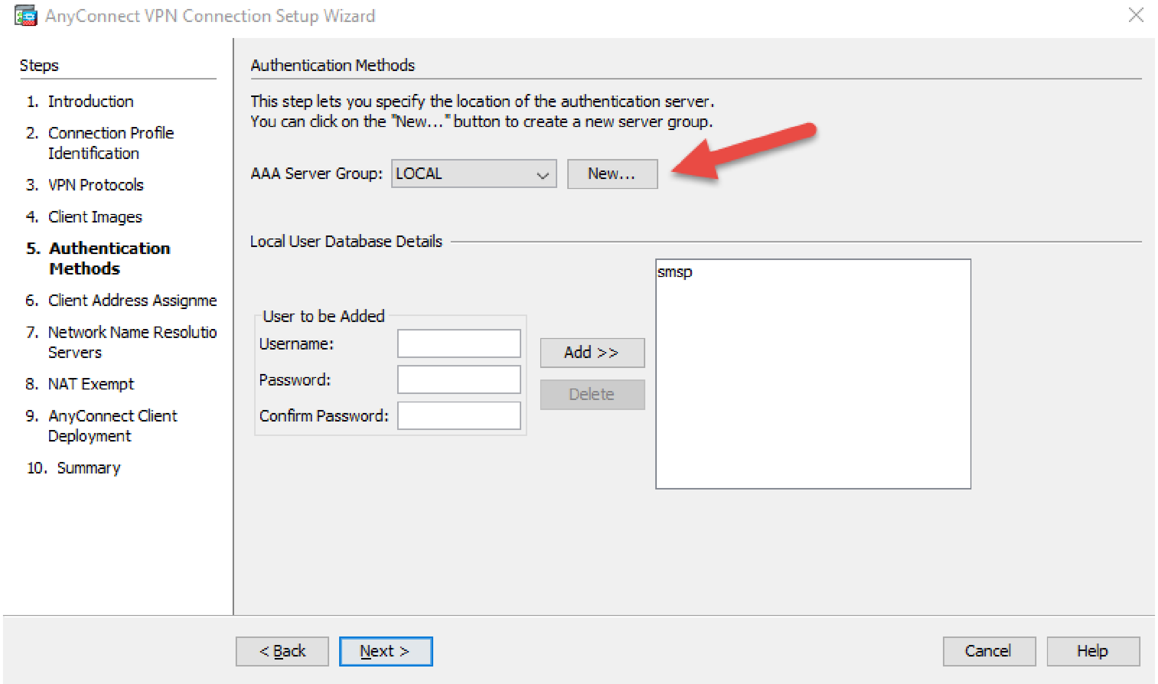
ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network.

A regular expression can be used to match the user-agent of a browser to an image.
You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.

Image	Regular expression to match user-agent
disk0:/anyconnect-dart-win-2.5.6005-k9.pkg	

You can download AnyConnect Client packages from Cisco by searching 'AnyConnect VPN Client' or click here.

6. Click Next and Create the Authentication Method. Make new AAA server group (refers to the Windows NPS/Radius server):



AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. **Authentication Methods**
6. Client Address Assignme
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Authentication Methods

This step lets you specify the location of the authentication server.
You can click on the "New..." button to create a new server group.

AAA Server Group: LOCAL

Local User Database Details

User to be Added

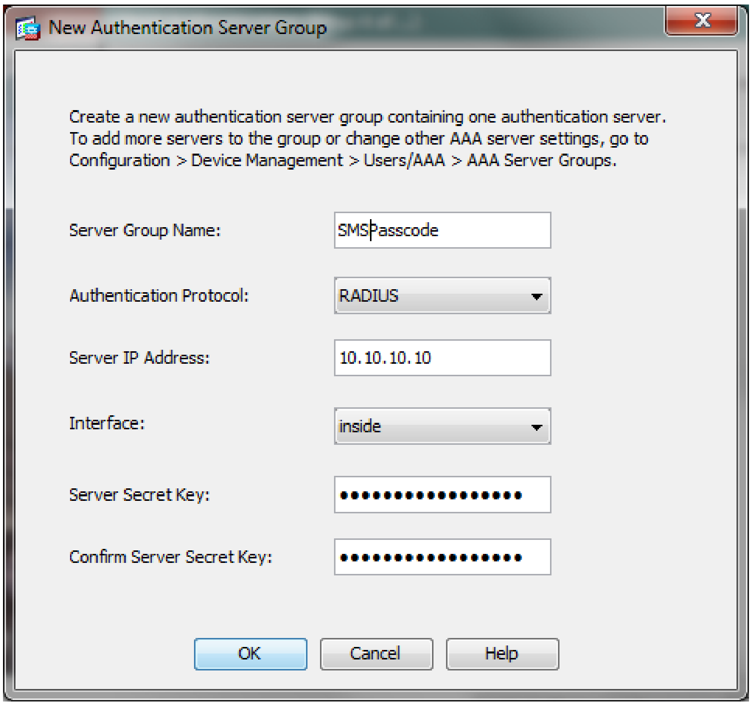
Username:

Password:

Confirm Password:

smsp

7. We named our group SMSPasscode on the inside interface. The Server Secret key is the same key you configure when creating your Radius Client on the NPS server:



New Authentication Server Group

Create a new authentication server group containing one authentication server.
To add more servers to the group or change other AAA server settings, go to Configuration > Device Management > Users/AAA > AAA Server Groups.

Server Group Name: SMSPasscode

Authentication Protocol: RADIUS

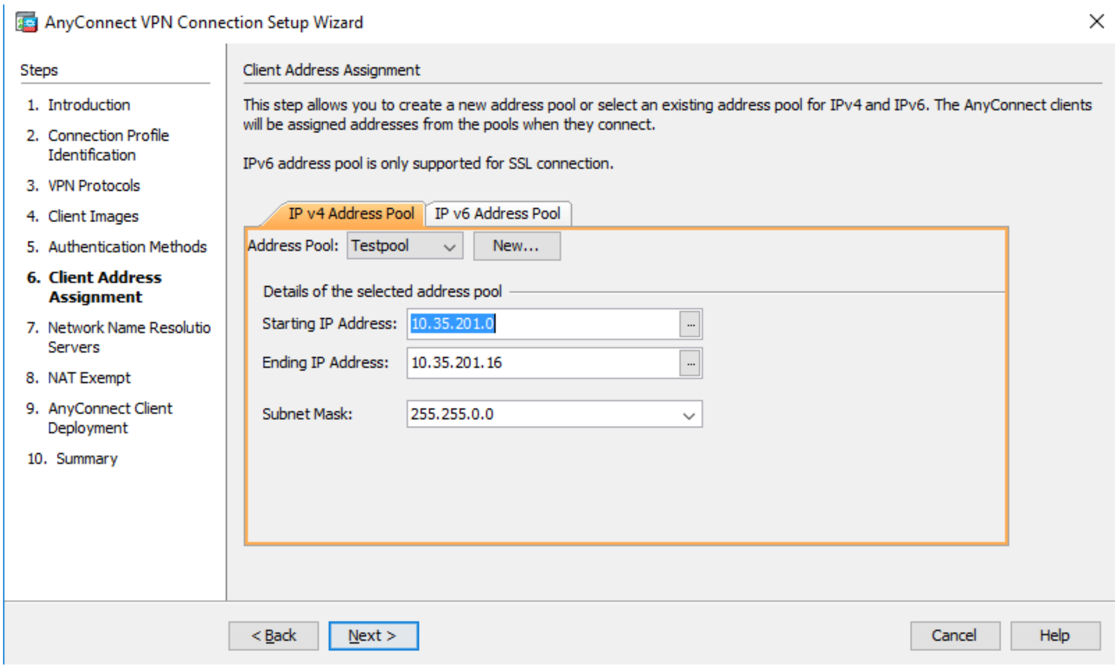
Server IP Address: 10.10.10.10

Interface: inside

Server Secret Key: •••••••••••••••••

Confirm Server Secret Key: •••••••••••••••••

8. Click Ok then Next. You will now be prompted to supply your address pool. Please be sure to make the pool large enough to allow for all of your potential users.



AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. **Client Address Assignment**
7. Network Name Resolutio Servers
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Client Address Assignment

This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients will be assigned addresses from the pools when they connect.

IPv6 address pool is only supported for SSL connection.

Address Pool: Testpool

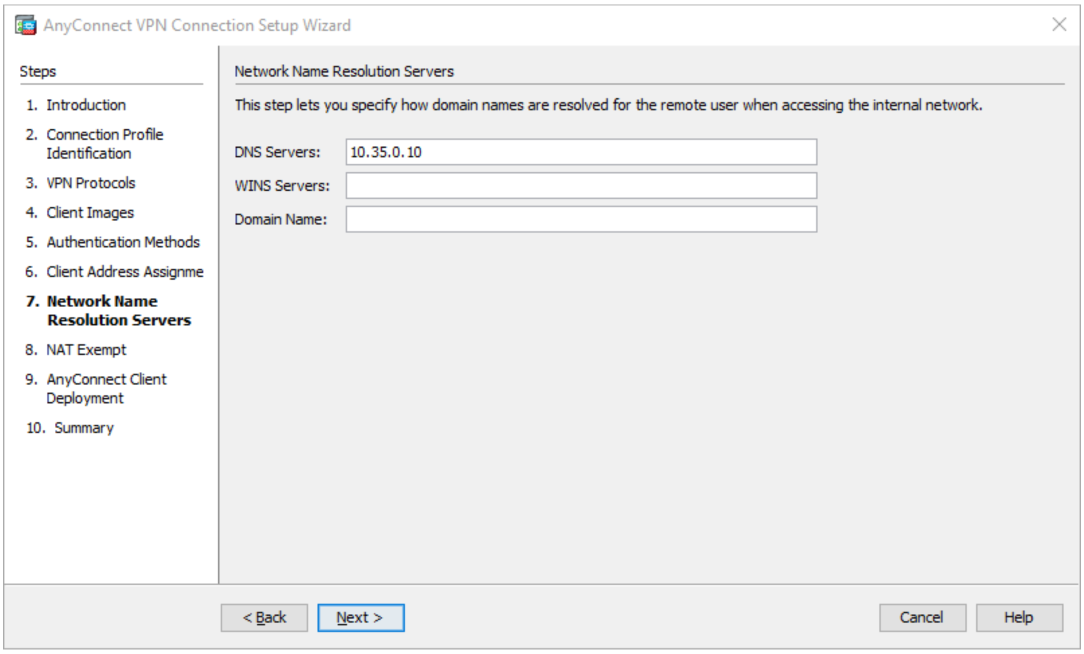
Details of the selected address pool

Starting IP Address: 10.35.201.0

Ending IP Address: 10.35.201.16

Subnet Mask: 255.255.0.0

9. Assign DNS/WINS/Domain Name, WINS and Domain Name are optional:



AnyConnect VPN Connection Setup Wizard

Steps

1. Introduction
2. Connection Profile Identification
3. VPN Protocols
4. Client Images
5. Authentication Methods
6. Client Address Assignme
7. **Network Name Resolution Servers**
8. NAT Exempt
9. AnyConnect Client Deployment
10. Summary

Network Name Resolution Servers

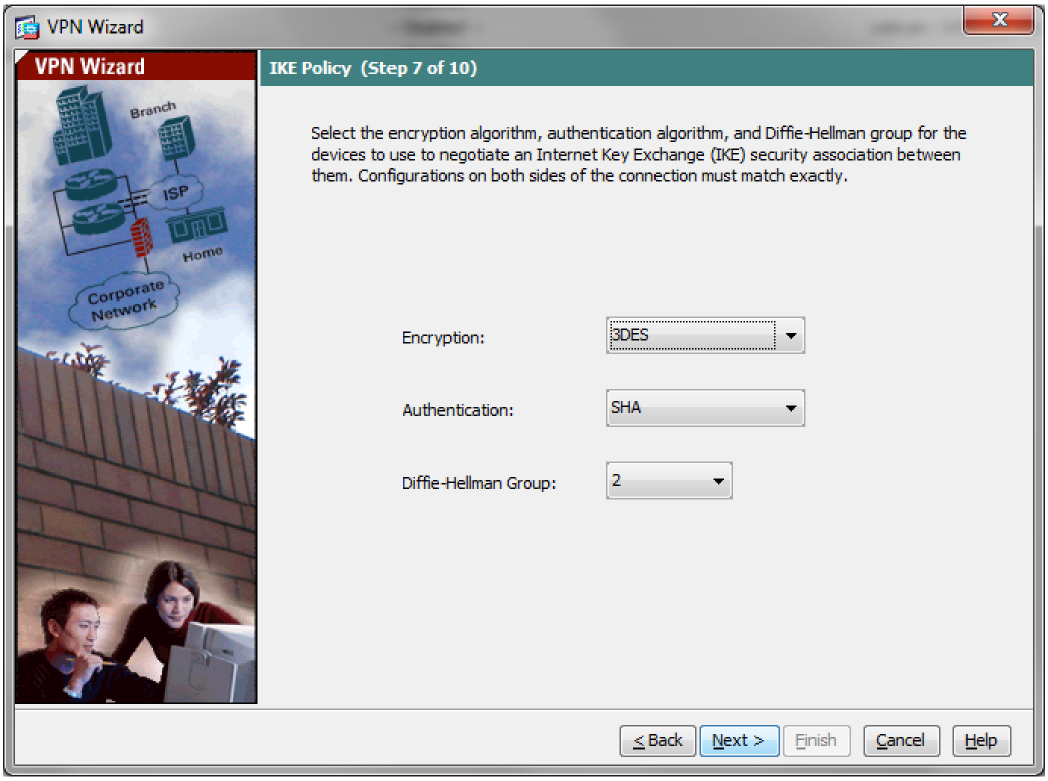
This step lets you specify how domain names are resolved for the remote user when accessing the internal network.

DNS Servers: 10.35.0.10

WINS Servers:

Domain Name:

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



IKE Policy (Step 7 of 10)

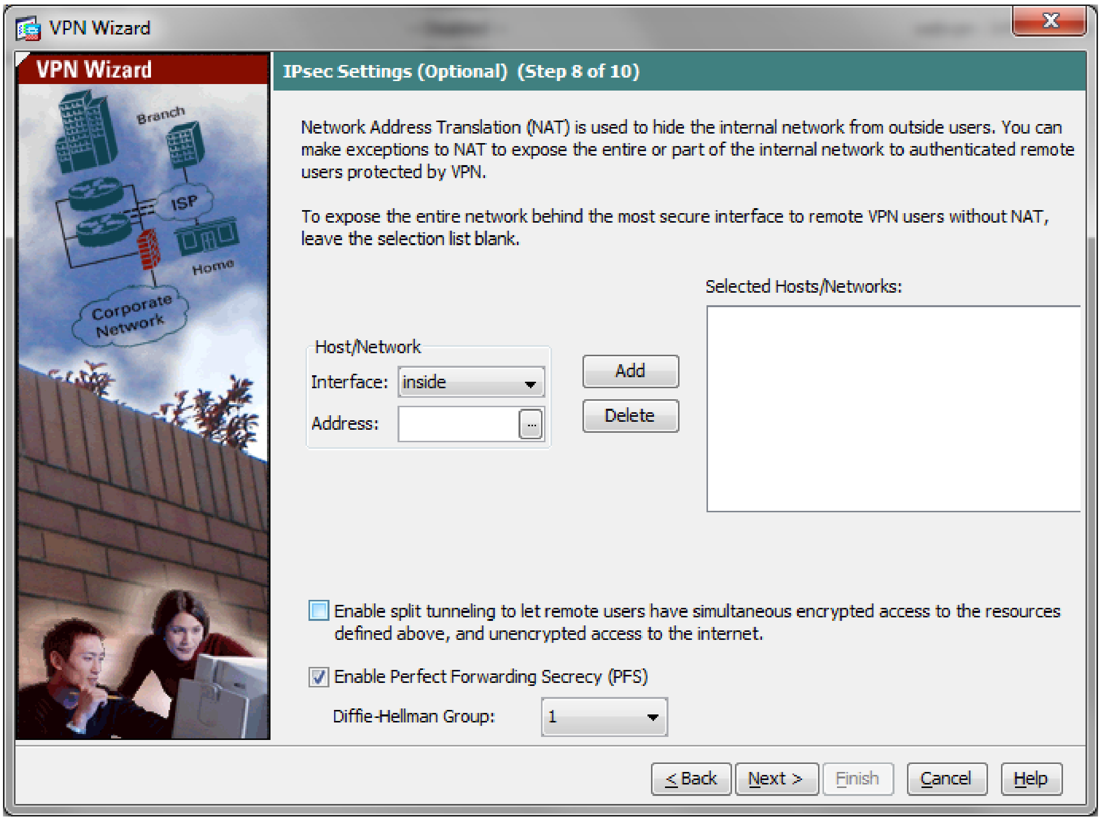
Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.

Encryption: 3DES

Authentication: SHA

Diffie-Hellman Group: 2

11. Verify "Enable Perfect Forwarding Secrecy (PFS) is checked and click next:



IPsec Settings (Optional) (Step 8 of 10)

Network Address Translation (NAT) is used to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN.

To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the selection list blank.

Host/Network

Interface: inside

Address:

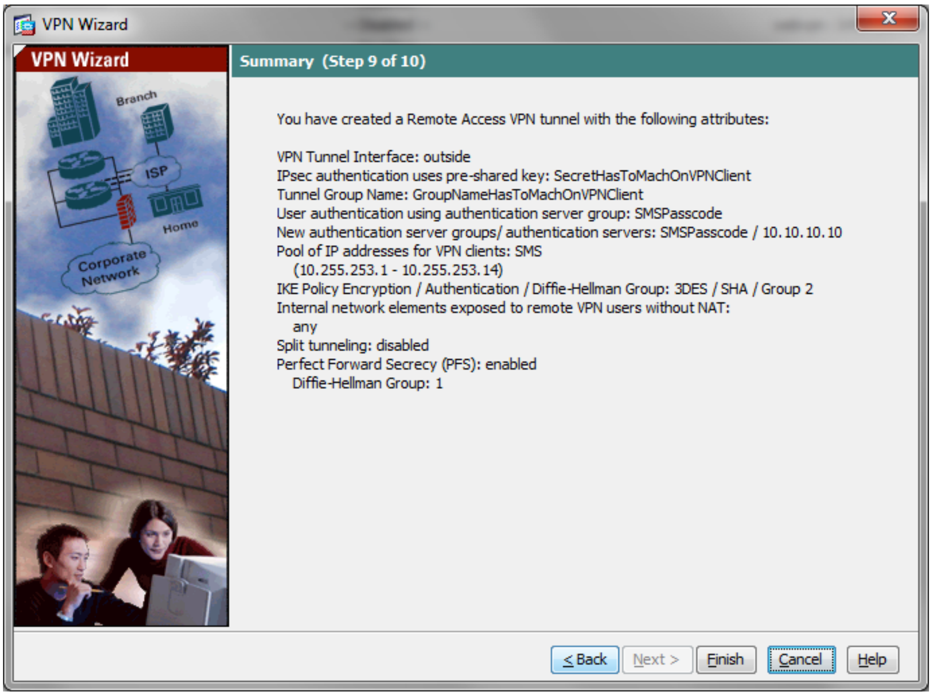
Selected Hosts/Networks:

☐ Enable split tunneling to let remote users have simultaneous encrypted access to the resources defined above, and unencrypted access to the internet.

☑ Enable Perfect Forwarding Secrecy (PFS)

Diffie-Hellman Group: 1

12. You have now set up the Cisco ASA for SMS PASSCODE® Multi-Factor authentication.



Summary (Step 9 of 10)

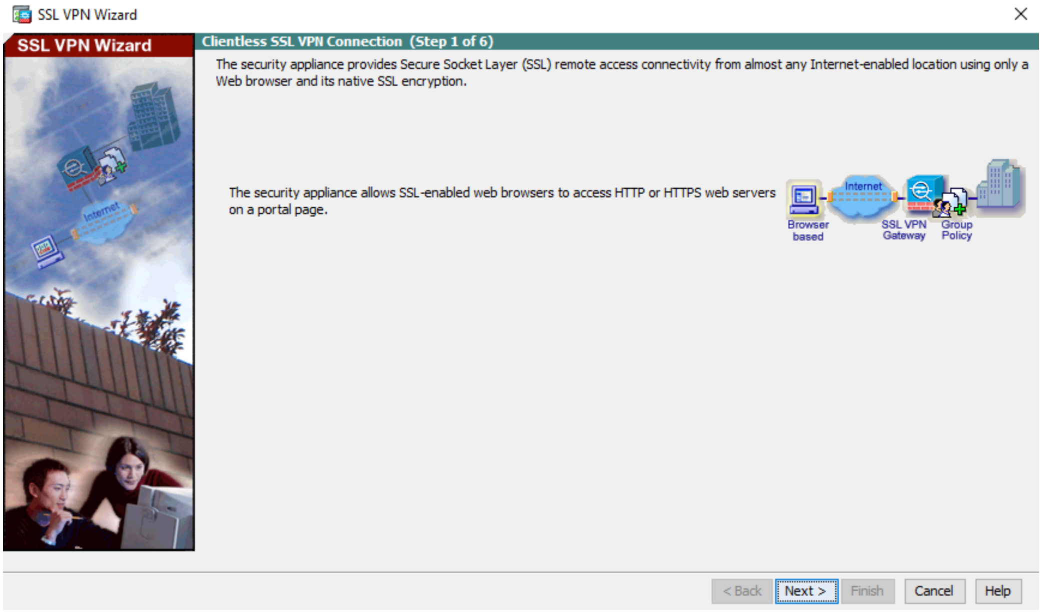
```
You have created a Remote Access VPN tunnel with the following attributes:

VPN Tunnel Interface: outside
IPsec authentication uses pre-shared key: SecretHasToMachOnVPNClient
Tunnel Group Name: GroupNameHasToMachOnVPNClient
User authentication using authentication server group: SMSPasscode
New authentication server groups/ authentication servers: SMSPasscode / 10.10.10.10
Pool of IP addresses for VPN clients: SMS
   (10.255.253.1 - 10.255.253.14)
IKE Policy Encryption / Authentication / Diffie-Hellman Group: 3DES / SHA / Group 2
Internal network elements exposed to remote VPN users without NAT:
   any
Split tunneling: disabled
Perfect Forward Secrecy (PFS): enabled
   Diffie-Hellman Group: 1
```

Setup Cisco Clientless SSL VPN

Please note that for the clientless VPN access we are assuming that DNS has already been configured and you are aware of how to associate bookmarks with your group policies.

1. Start ASDM and login to the Web interface.
2. In the top tool bar select Wizards => VPN Wizards => Clientless SSL VPN Wizard…



SSL VPN Wizard

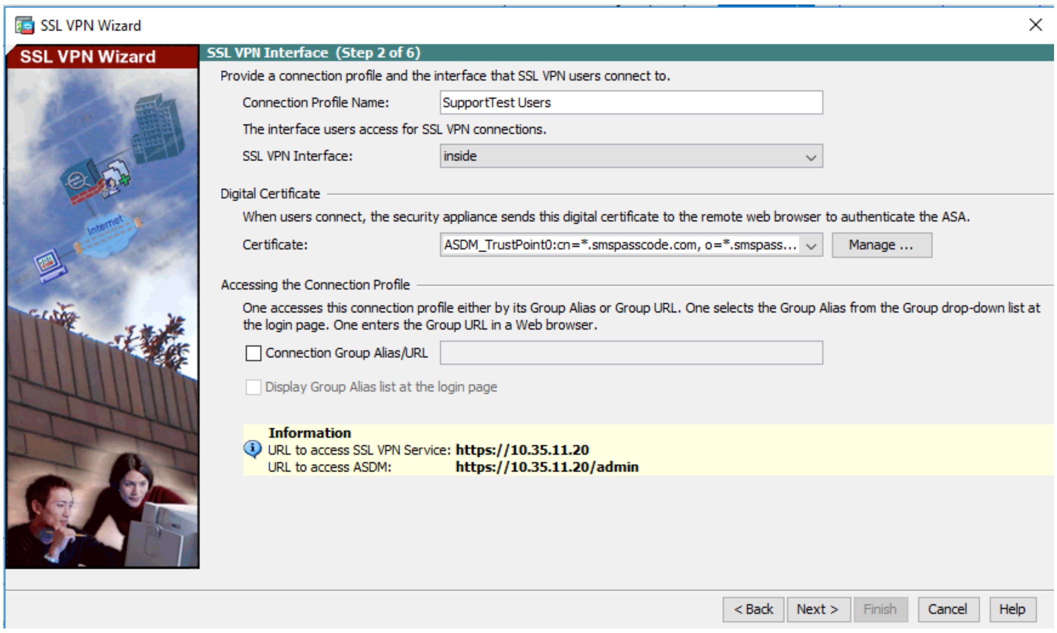
SSL VPN Wizard

Clientless SSL VPN Connection (Step 1 of 6)

The security appliance provides Secure Socket Layer (SSL) remote access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption.

The security appliance allows SSL-enabled web browsers to access HTTP or HTTPS web servers on a portal page.

3. You will then create your Connection Profile Name, choose the interface from where the users will connect, assign the Digital Certificate and you will also see the URL the users will need to access the clientless webpage. (As my example is from a test environment I will use the inside interface. Most will probably post to the outside interface).



SSL VPN Wizard

SSL VPN Wizard

SSL VPN Interface (Step 2 of 6)

Provide a connection profile and the interface that SSL VPN users connect to.

Connection Profile Name: SupportTest Users

The interface users access for SSL VPN connections.

SSL VPN Interface: inside

Digital Certificate

When users connect, the security appliance sends this digital certificate to the remote web browser to authenticate the ASA.

Certificate: ASDM_TrustPoint0:cn=*.smspasscode.com, o=*.smspass...

Accessing the Connection Profile

One accesses this connection profile either by its Group Alias or Group URL. One selects the Group Alias from the Group drop-down list at the login page. One enters the Group URL in a Web browser.

□ Connection Group Alias/URL

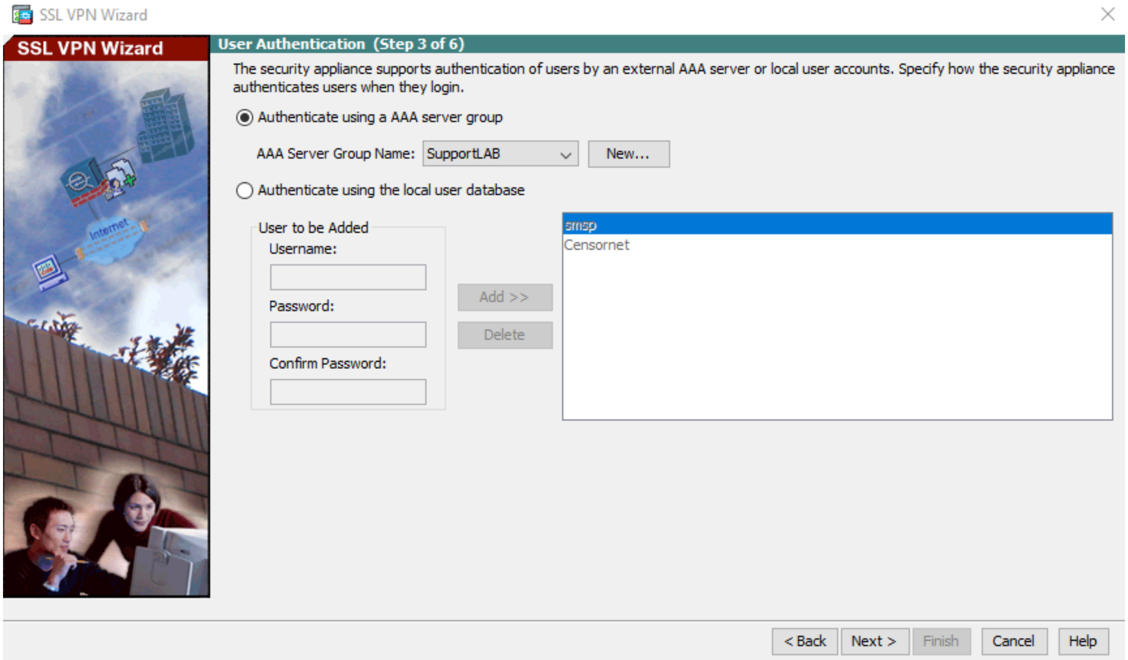
□ Display Group Alias list at the login page

Information

URL to access SSL VPN Service: **https://10.35.11.20**

URL to access ASDM: **https://10.35.11.20/admin**

4. Next you will assign your AAA Server Group (AKA your RADIUS server). My Group is call SupportLAB. The Wizard creates the server group (SupportLAB) and server in one configuration. Please note the AAA Server Group can have multiple Radius servers.



SSL VPN Wizard

User Authentication (Step 3 of 6)

The security appliance supports authentication of users by an external AAA server or local user accounts. Specify how the security appliance authenticates users when they login.

● Authenticate using a AAA server group

AAA Server Group Name: SupportLAB

○ Authenticate using the local user database

User to be Added

Username:

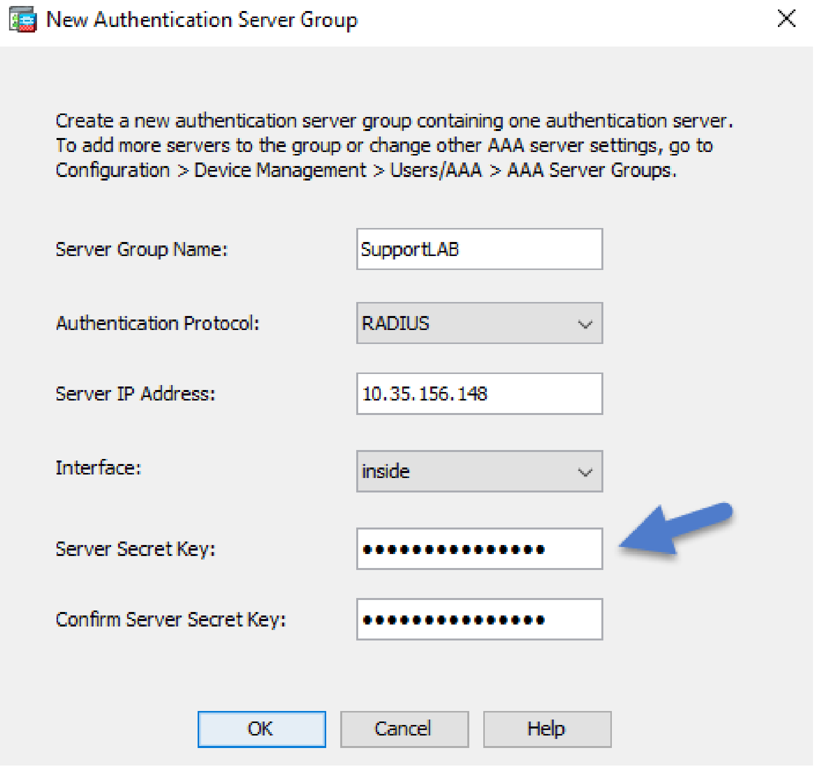
Password:

Confirm Password:

smsp

Censornet

The Server Secret key will be the key you use on the NPS RADIUS server. This should not be confused with the shared secret used for the Configuration Tool in SMS PASSCODE.



New Authentication Server Group

Create a new authentication server group containing one authentication server. To add more servers to the group or change other AAA server settings, go to Configuration > Device Management > Users/AAA > AAA Server Groups.

Server Group Name: SupportLAB

Authentication Protocol: RADIUS

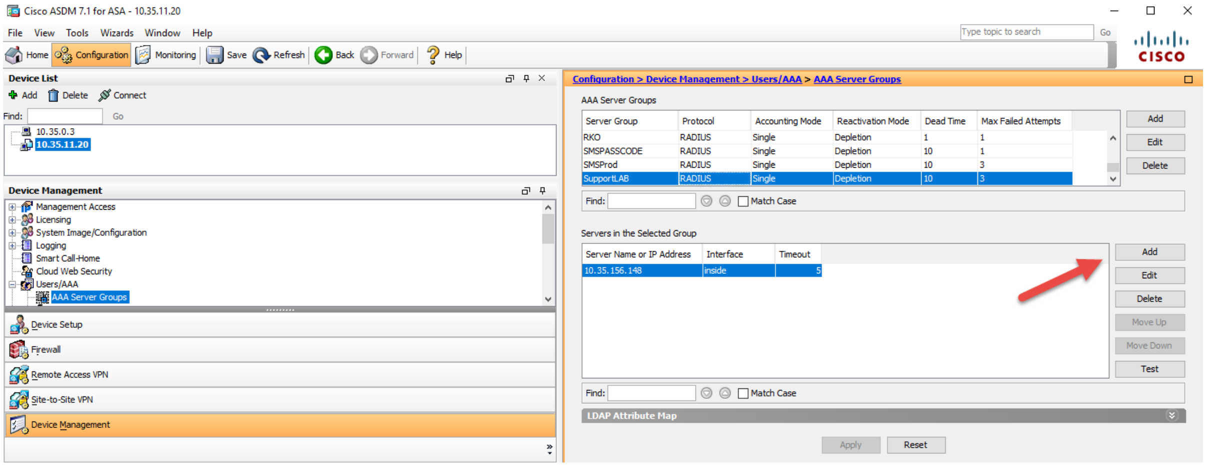
Server IP Address: 10.35.156.148

Interface: inside

Server Secret Key: ••••••••••••••••

Confirm Server Secret Key: ••••••••••••••••

You can add more RADIUS servers in the device manager as shown below.



Configuration > Device Management > Users/AAA > AAA Server Groups

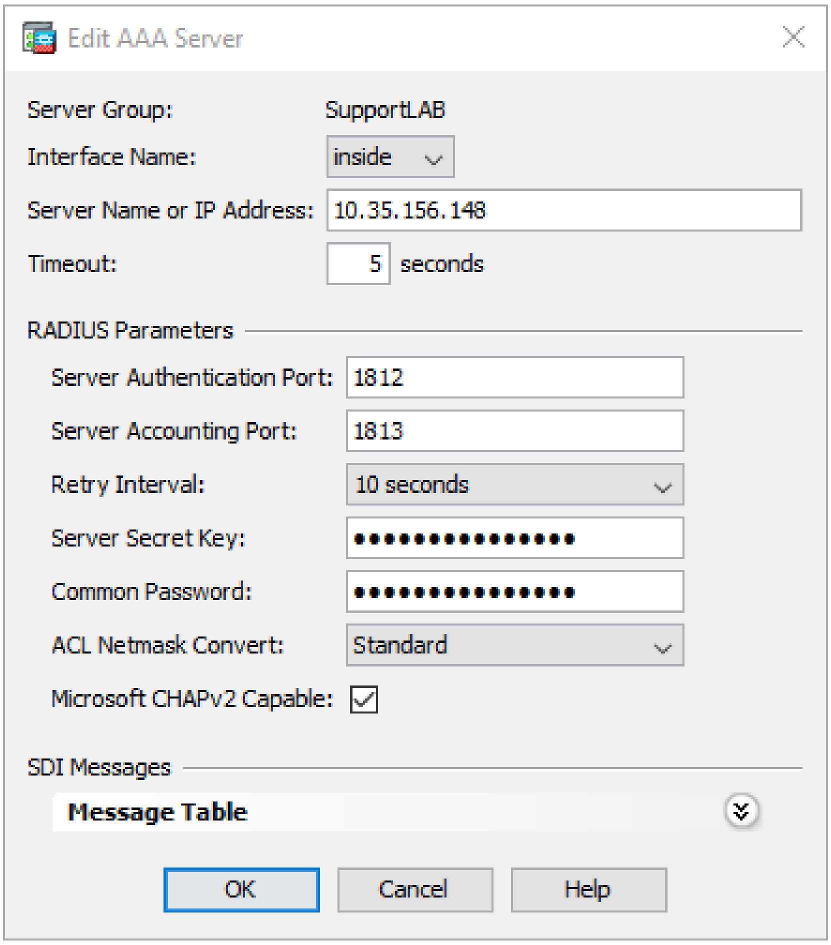
AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
RKO	RADIUS	Single	Depletion	1	1
SMSPASSCODE	RADIUS	Single	Depletion	10	1
SMSProd	RADIUS	Single	Depletion	10	3
SupportLAB	RADIUS	Single	Depletion	10	3

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
10.35.156.148	inside	5

Please also take note of the RADIUS ports that are configured on the RADIUS server. You should be using ports 1812/1813


Edit AAA Server

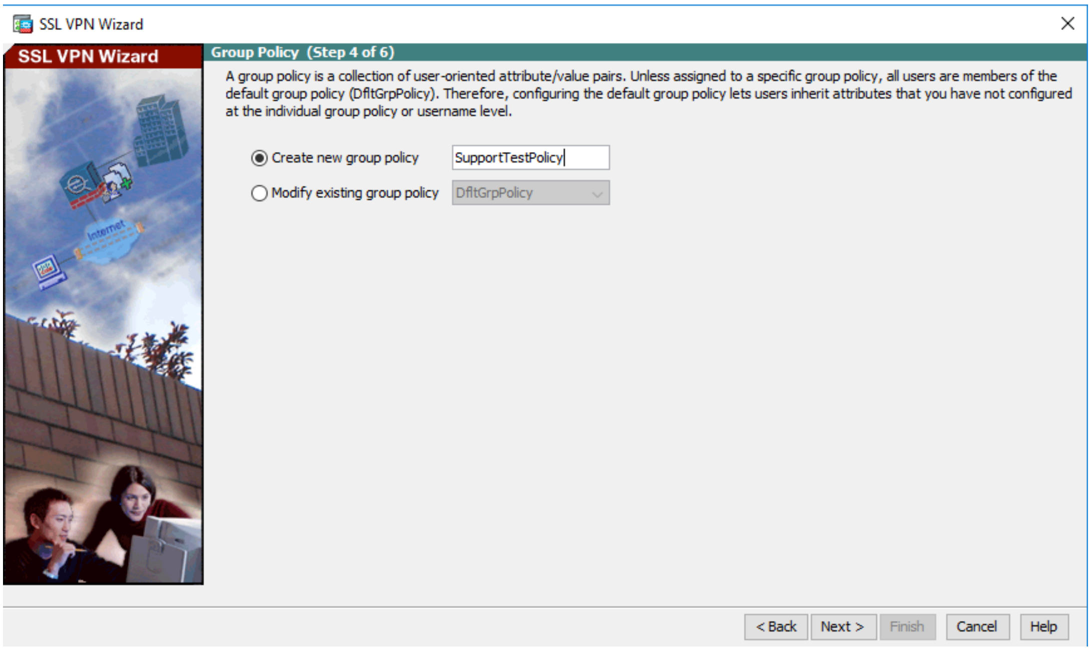
Server Group:	SupportLAB
Interface Name:	inside
Server Name or IP Address:	10.35.156.148
Timeout:	5 seconds

RADIUS Parameters

Server Authentication Port:	1812
Server Accounting Port:	1813
Retry Interval:	10 seconds
Server Secret Key:	•••••••••••••••
Common Password:	•••••••••••••••
ACL Netmask Convert:	Standard
Microsoft CHAPv2 Capable:	☑

SDI Messages

5. Create and/or assign your group policy.



SSL VPN Wizard

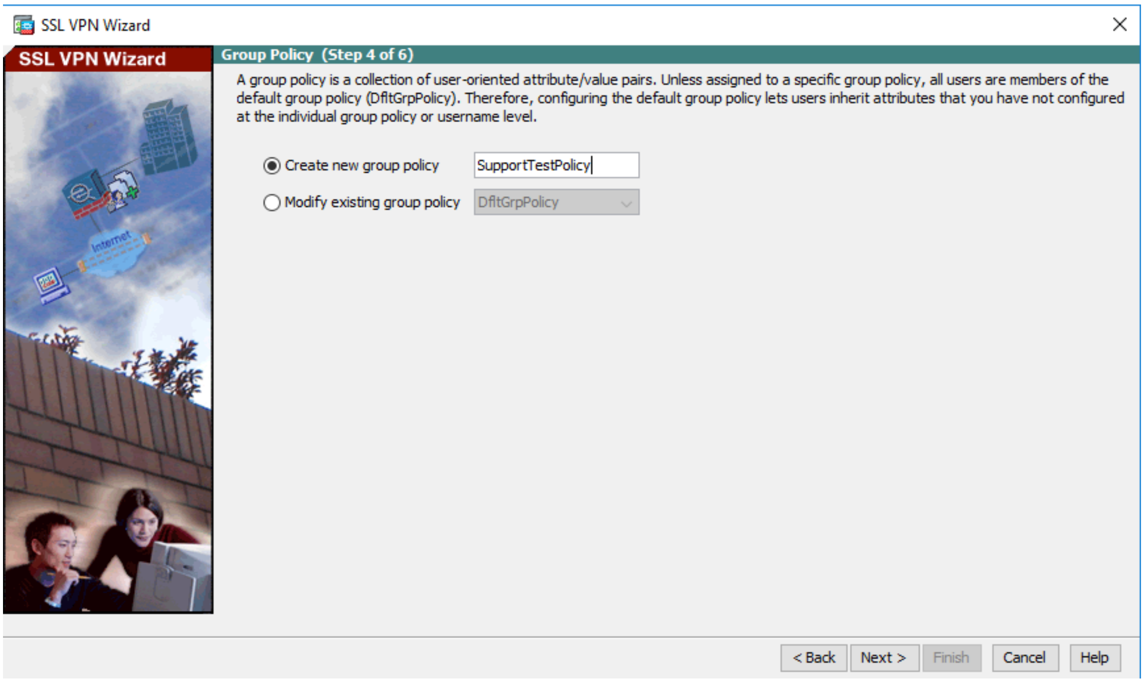
Group Policy (Step 4 of 6)

A group policy is a collection of user-oriented attribute/value pairs. Unless assigned to a specific group policy, all users are members of the default group policy (DfltGrpPolicy). Therefore, configuring the default group policy lets users inherit attributes that you have not configured at the individual group policy or username level.

● Create new group policy: SupportTestPolicy

○ Modify existing group policy: DfltGrpPolicy

6. Configure your Bookmark page. This will be the list of Applications and websites that will be available via the Cisco SSL VPN connection.



SSL VPN Wizard

Group Policy (Step 4 of 6)

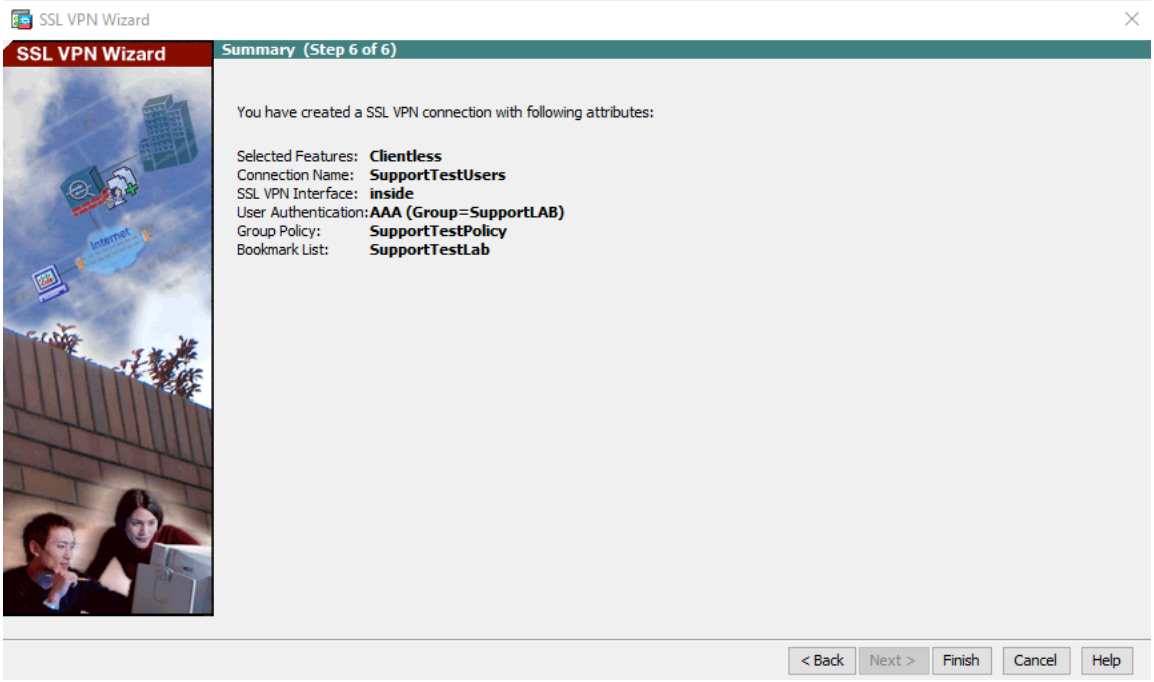
A group policy is a collection of user-oriented attribute/value pairs. Unless assigned to a specific group policy, all users are members of the default group policy (DfltGrpPolicy). Therefore, configuring the default group policy lets users inherit attributes that you have not configured at the individual group policy or username level.

● Create new group policy: SupportTestPolicy

○ Modify existing group policy: DfltGrpPolicy

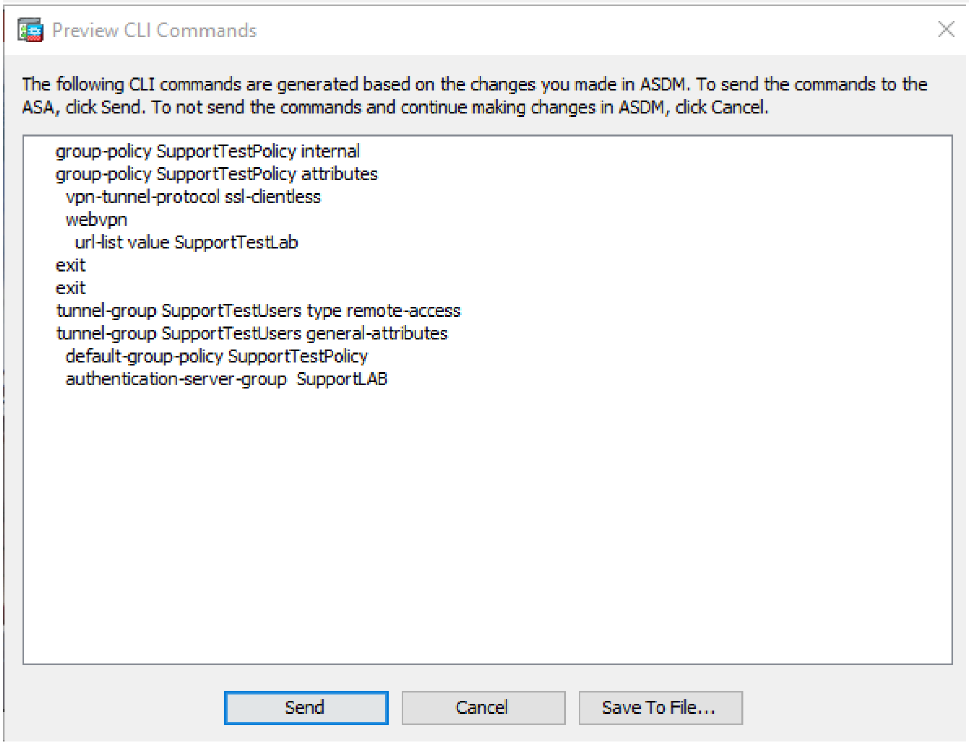
7. Then make a note of your connection parameters if you are going to need to troubleshoot later, you will know which parameters are associated to your

configuration. Also note the CLI commands forwarded if you wish to troubleshoot via the CLI.



You have created a SSL VPN connection with following attributes:

Selected Features:	**Clientless**
Connection Name:	**SupportTestUsers**
SSL VPN Interface:	**inside**
User Authentication:	**AAA (Group=SupportLAB)**
Group Policy:	**SupportTestPolicy**
Bookmark List:	**SupportTestLab**



The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the ASA, click Send. To not send the commands and continue making changes in ASDM, click Cancel.

```
group-policy SupportTestPolicy internal
group-policy SupportTestPolicy attributes
 vpn-tunnel-protocol ssl-clientless
 webvpn
  url-list value SupportTestLab
exit
exit
tunnel-group SupportTestUsers type remote-access
tunnel-group SupportTestUsers general-attributes
 default-group-policy SupportTestPolicy
 authentication-server-group  SupportLAB
```

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 GroupNameHasToMatchOnVPNClient type remote-access
tunnel-group GroupNameHasToMatchOnVPNClient general-attributes
  authentication-server-group  SMSPasscode
  address-pool  SMS
tunnel-group GroupNameHasToMatchOnVPNClient 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

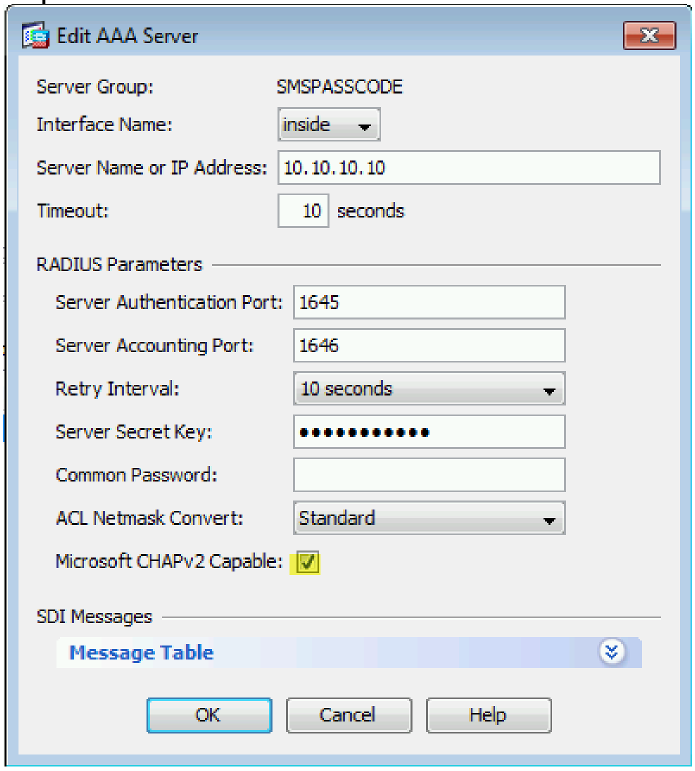
To set-up SMS PASSCODE® for RADIUS, please consult the SMS PASSCODE® Administrators Guide under the section “Configuring RADIUS Protection.”

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



Edit AAA Server

Server Group: SMSPASSCODE

Interface Name: inside

Server Name or IP Address: 10.10.10.10

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key: ●●●●●●●●●●●

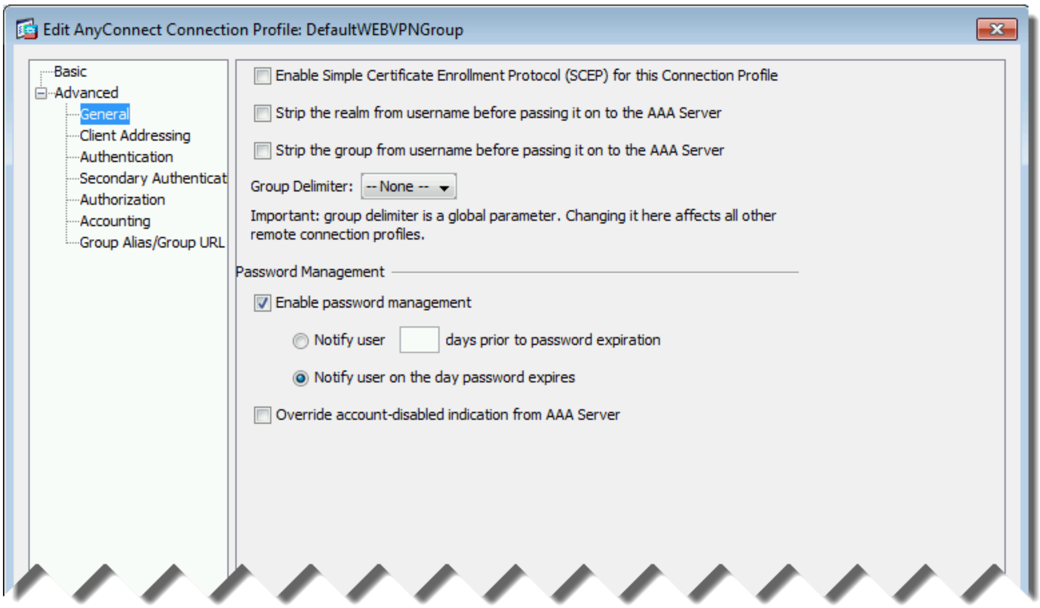
Common Password:

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable: ☑

SDI Messages

And in the Connection Profile “Enable password management”



Edit AnyConnect Connection Profile: DefaultWEBVPNGroup

☐ Enable Simple Certificate Enrollment Protocol (SCEP) for this Connection Profile

☐ Strip the realm from username before passing it on to the AAA Server

☐ Strip the group from username before passing it on to the AAA Server

Group Delimiter: -- None --

Important: group delimiter is a global parameter. Changing it here affects all other remote connection profiles.

Password Management

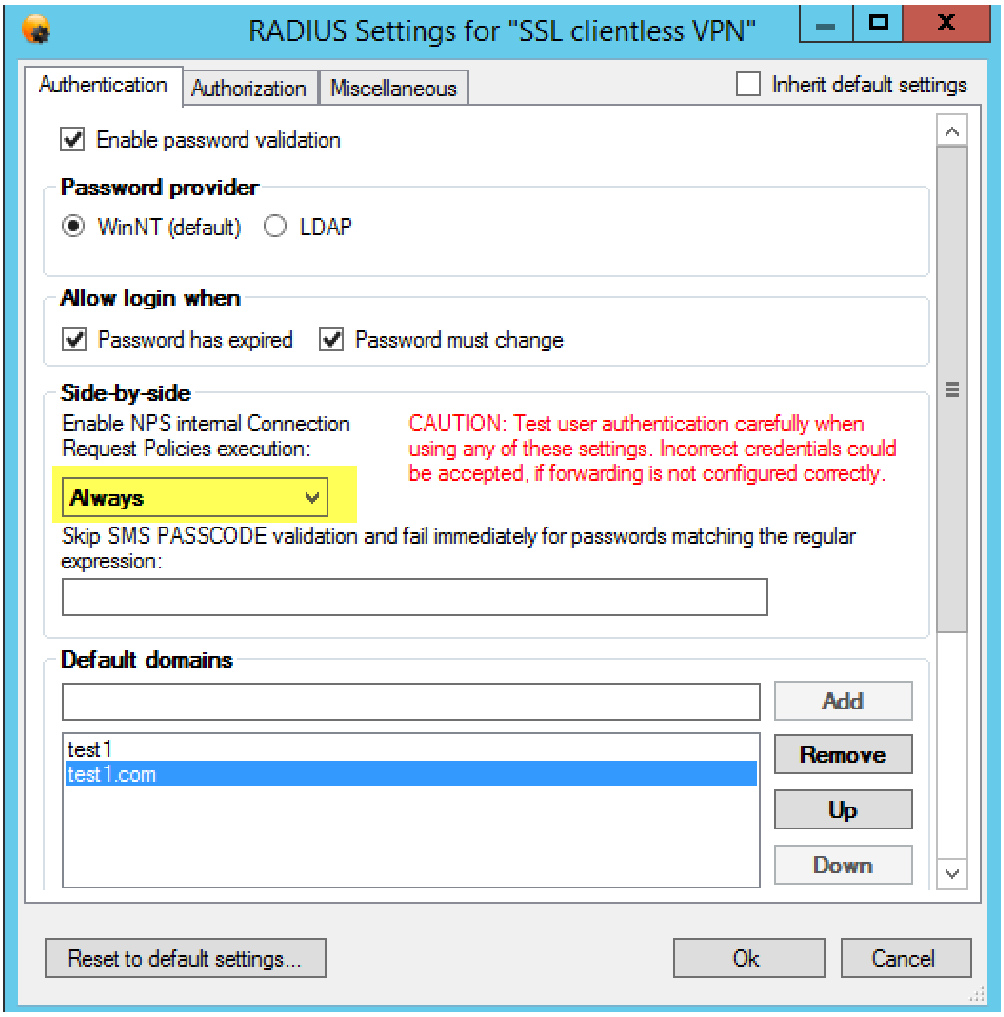
☑ Enable password management

○ Notify user days prior to password expiration

● Notify user on the day password expires

☐ Override account-disabled indication from AAA Server

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



RADIUS Settings for "SSL clientless VPN"

□ Inherit default settings

☑ Enable password validation

Password provider

● WinNT (default) ○ LDAP

Allow login when

☑ Password has expired ☑ Password must change

Side-by-side

Enable NPS internal Connection Request Policies execution: **Always**

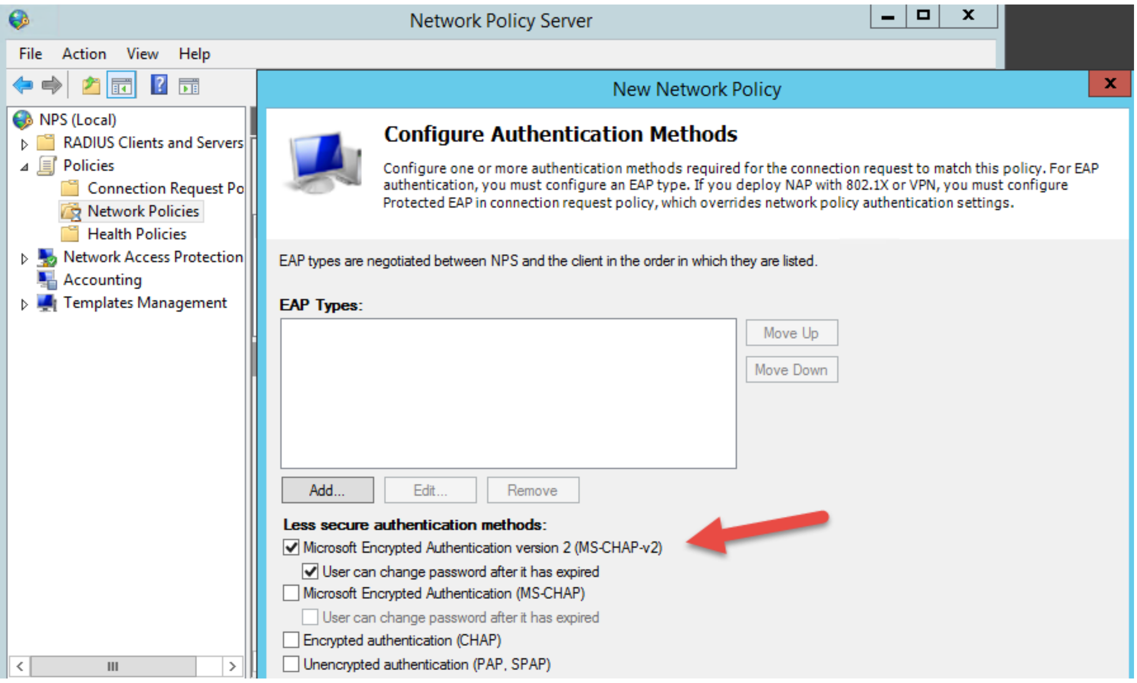
CAUTION: Test user authentication carefully when using any of these settings. Incorrect credentials could be accepted, if forwarding is not configured correctly.

Skip SMS PASSCODE validation and fail immediately for passwords matching the regular expression:

Default domains

test1
test1.com

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



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

☑ User can change password after it has expired

☐ Microsoft Encrypted Authentication (MS-CHAP)

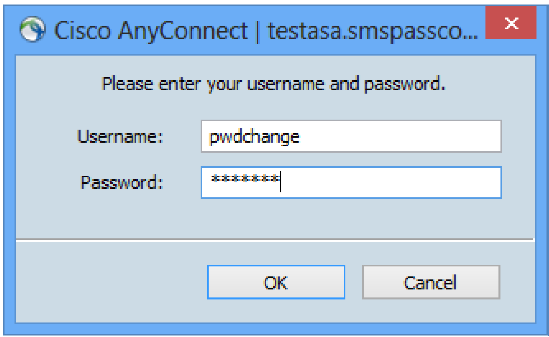
☐ User can change password after it has expired

☐ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

Password change

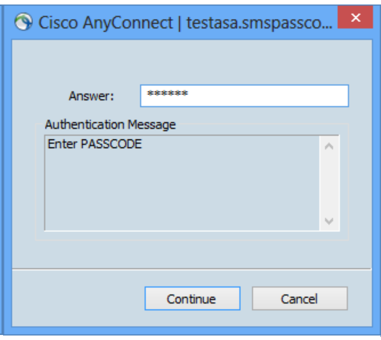
A normal logon flow with password change through AnyConnect or Clientless SSLVPN would look like this


Cisco AnyConnect | testasa.smspassco...

Please enter your username and password.

Username: pwdchange

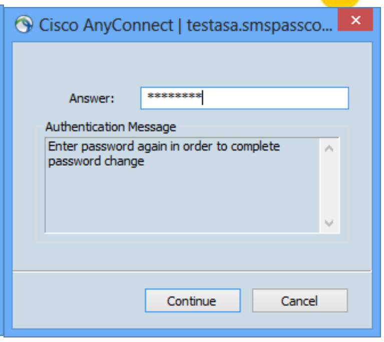
Password: ********


Cisco AnyConnect | testasa.smspassco...

Answer: ******

Authentication Message

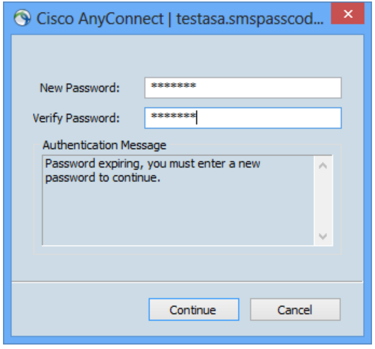
Enter PASSCODE


Cisco AnyConnect | testasa.smspassco...

Answer: ********

Authentication Message

Enter password again in order to complete password change


Cisco AnyConnect | testasa.smspasscod...

New Password: *******

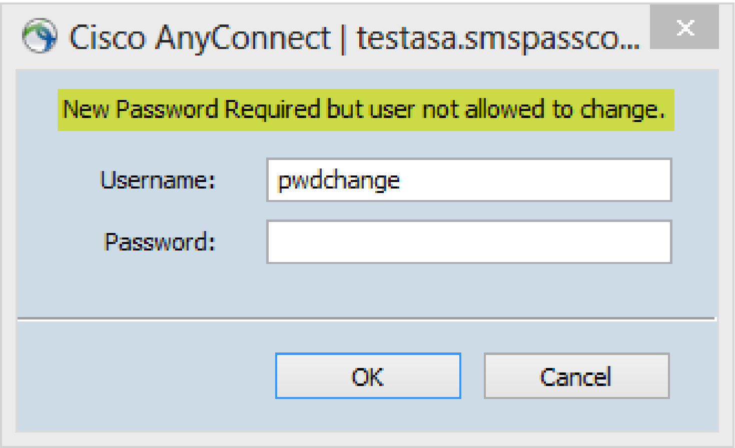
Verify Password: *******

Authentication Message

Password expiring, you must enter a new password to continue.

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 b

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 password change will fail with this error after reentering current password.


Cisco AnyConnect | testasa.smspassco...

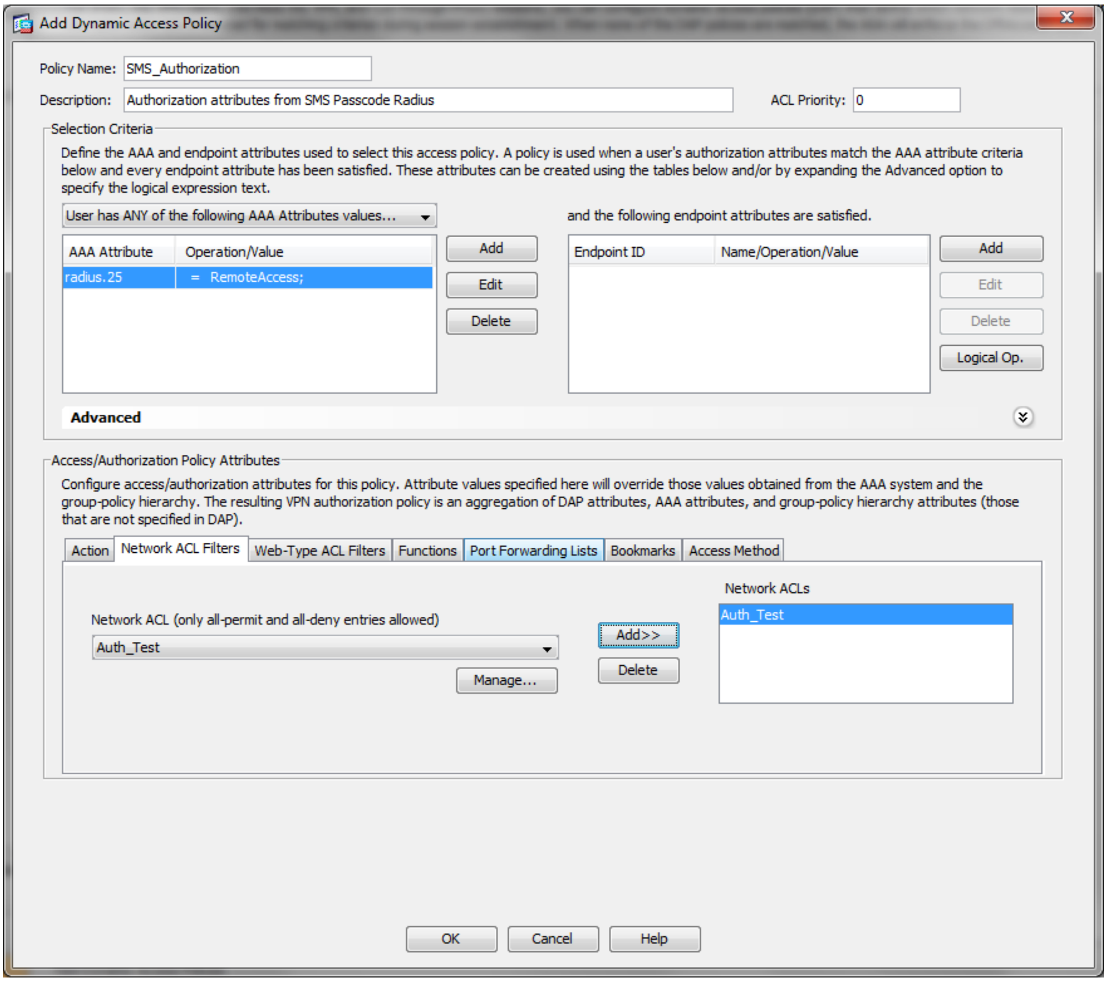
New Password Required but user not allowed to change.

Username: pwdchange

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:



Policy Name: SMS_Authorization

Description: Authorization attributes from SMS Passcode Radius

ACL Priority: 0

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values...

AAA Attribute	Operation/Value
radius.25	= RemoteAccess;

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value

Access/Authorization Policy Attributes

Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Network ACL (only all-permit and all-deny entries allowed): Auth_Test

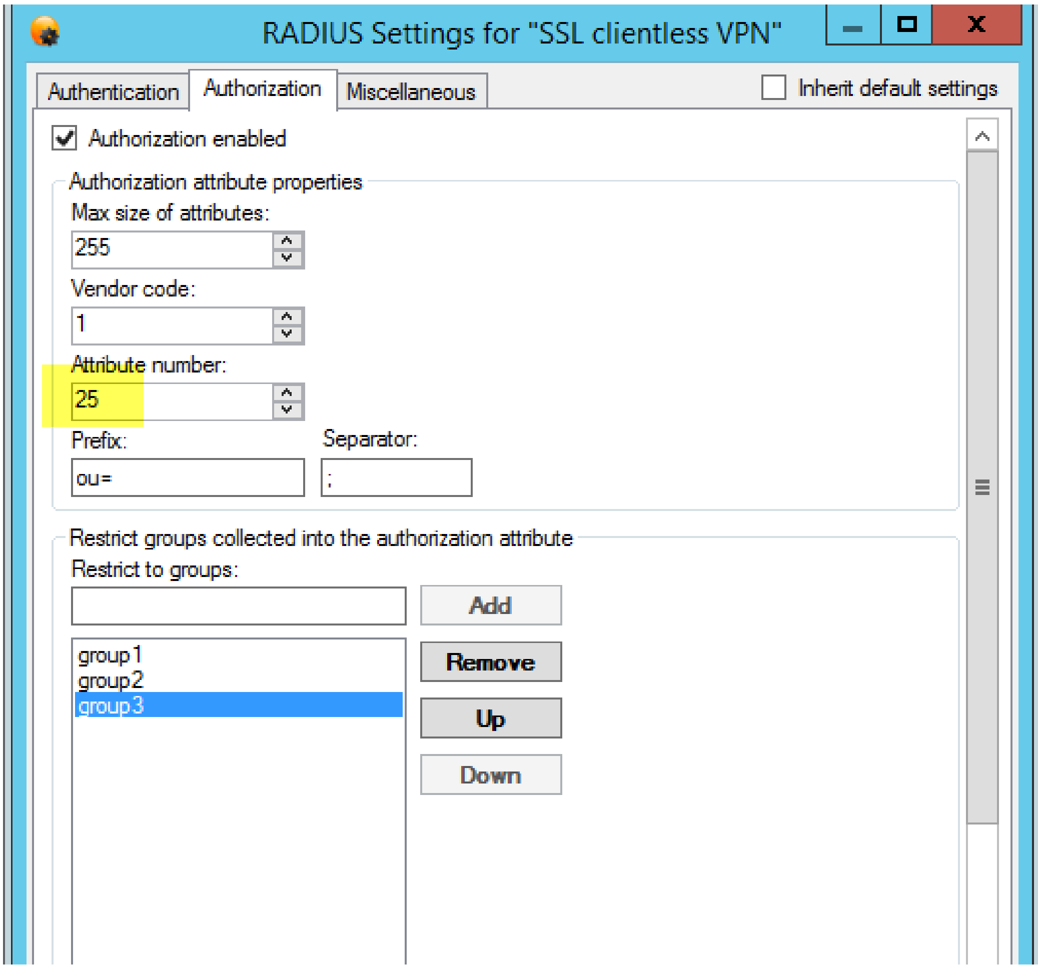
Network ACLs: Auth_Test

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**



RADIUS Settings for "SSL clientless VPN"

☑ Authorization enabled

Authorization attribute properties

Max size of attributes: 255

Vendor code: 1

Attribute number: 25

Prefix: ou=

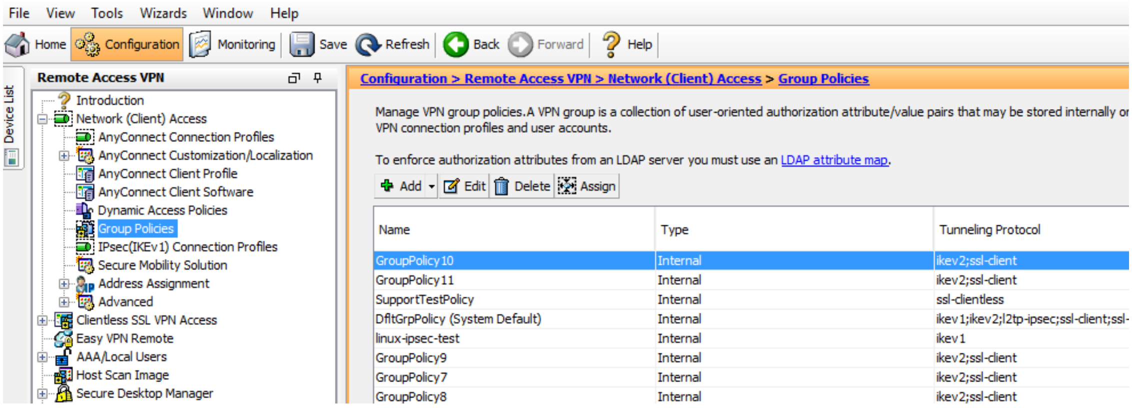
Separator: ;

Restrict groups collected into the authorization attribute

Restrict to groups:

group1
group2
group3

Setup Group policies in ASA to match the groups



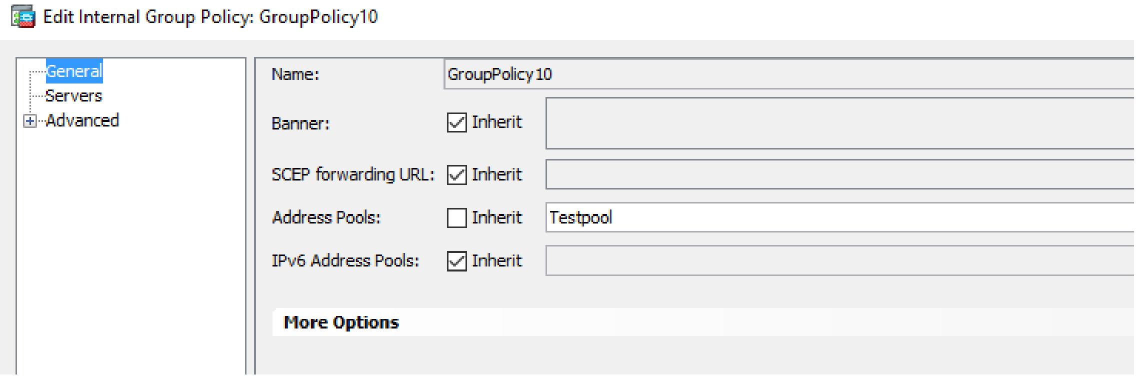
Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies.A VPN group is a collection of user-oriented authorization attribute/value pairs that may be stored internally or VPN connection profiles and user accounts.

To enforce authorization attributes from an LDAP server you must use an LDAP attribute map.

Name	Type	Tunneling Protocol
GroupPolicy10	Internal	ikev2;ssl-client
GroupPolicy11	Internal	ikev2;ssl-client
SupportTestPolicy	Internal	ssl-clientless
DfltGrpPolicy (System Default)	Internal	ikev1;ikev2;l2tp-ipsec;ssl-client;ssl-
linux-ipsec-test	Internal	ikev1
GroupPolicy9	Internal	ikev2;ssl-client
GroupPolicy7	Internal	ikev2;ssl-client
GroupPolicy8	Internal	ikev2;ssl-client

And set up the pool to use the wanted address pools:



Edit Internal Group Policy: GroupPolicy10

Name: GroupPolicy10

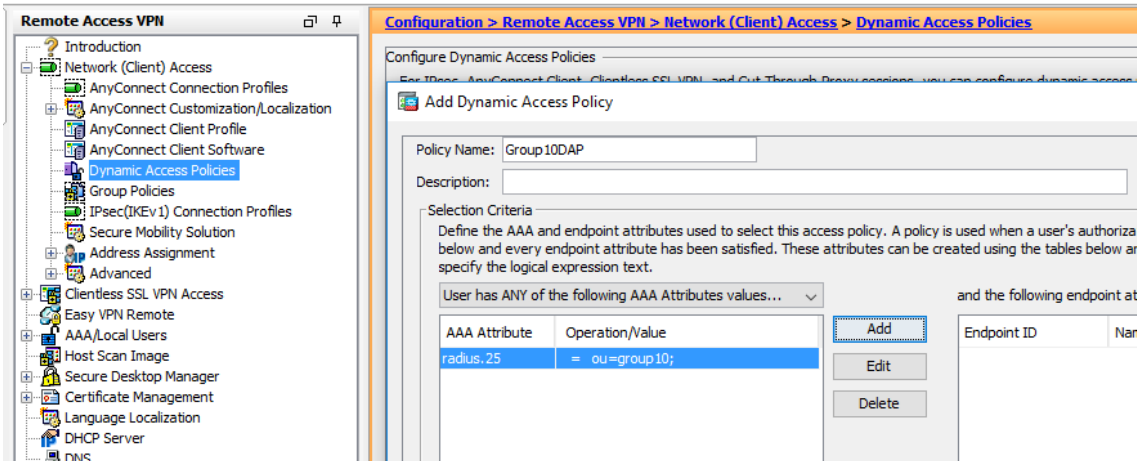
Banner: ☑ Inherit

SCEP forwarding URL: ☑ Inherit

Address Pools: □ Inherit Testpool

IPv6 Address Pools: ☑ Inherit

More Options



Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies

Configure Dynamic Access Policies

Add Dynamic Access Policy

Policy Name: Group10DAP

Description:

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authoriza below and every endpoint attribute has been satisfied. These attributes can be created using the tables below ar specify the logical expression text.

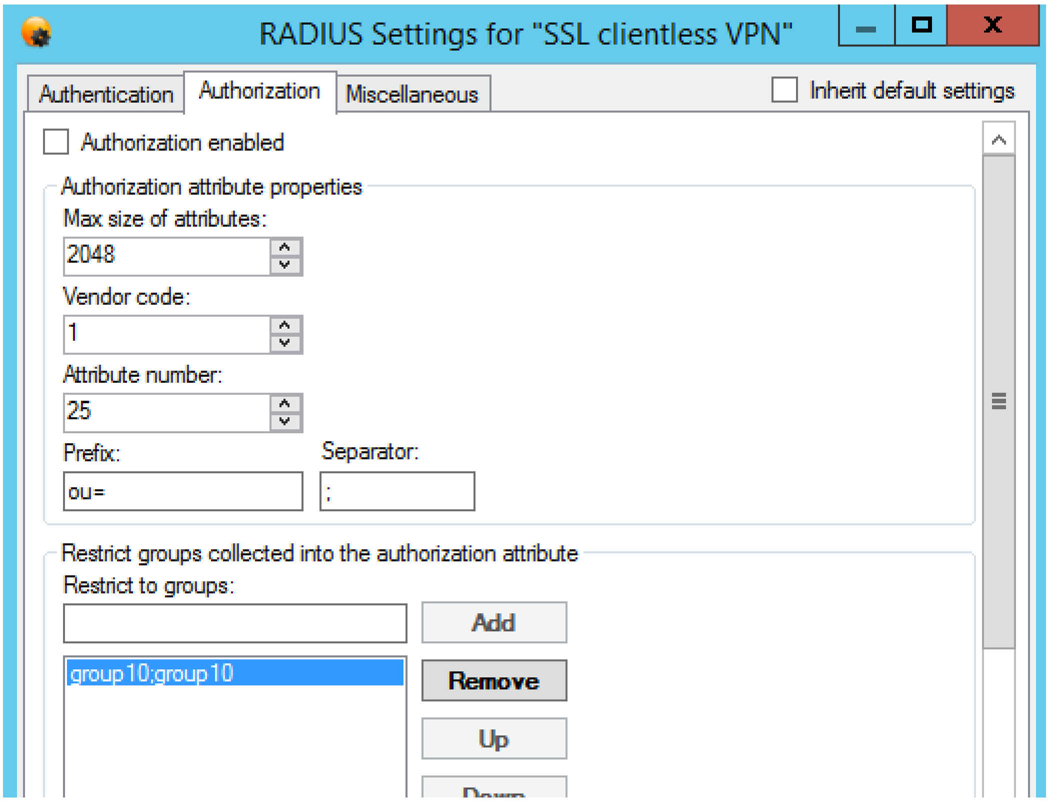
User has ANY of the following AAA Attributes values...

and the following endpoint at

AAA Attribute	Operation/Value
radius.25	= ou=group10;

(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



RADIUS Settings for "SSL clientless VPN"

□ Inherit default settings

□ Authorization enabled

Authorization attribute properties

Max size of attributes: 2048

Vendor code: 1

Attribute number: 25

Prefix: ou=

Separator: ;

Restrict groups collected into the authorization attribute

Restrict to groups:

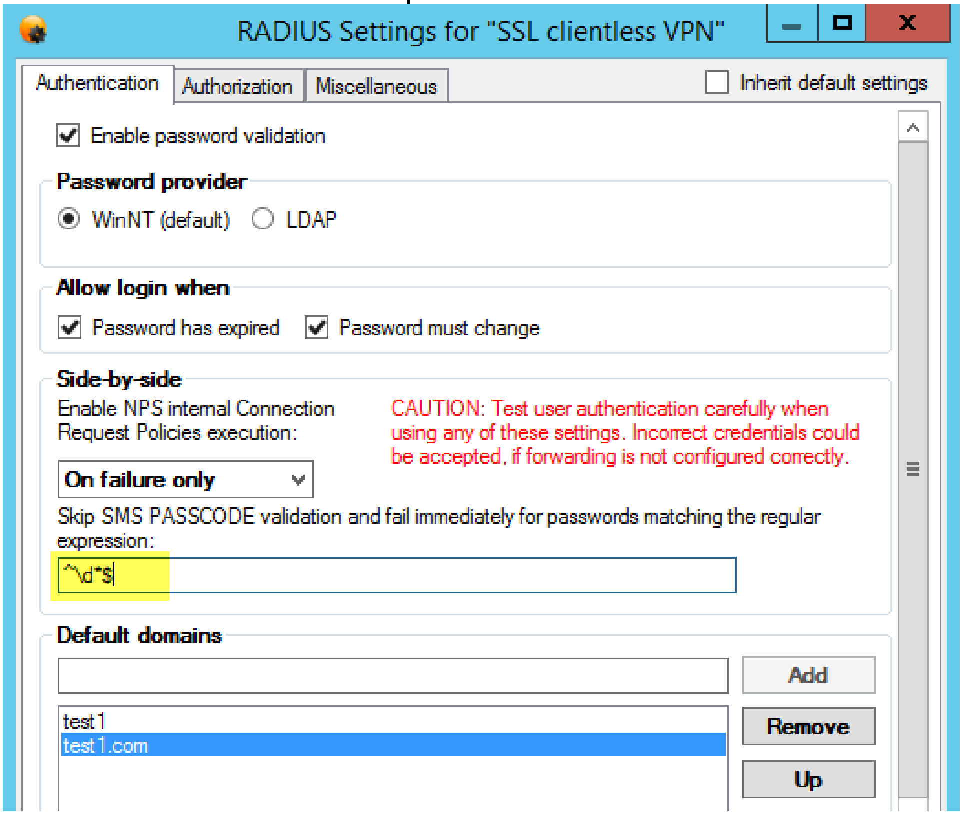
group10;group10

Note; Group name in attribute is always lower case.

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

You can make SMS PASSCODE® to co-exist with radius based token solutions. It is a pre-requisite that the SMS PASSCODCE 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.



RADIUS Settings for "SSL clientless VPN"

□ Inherit default settings

☑ Enable password validation

Password provider

● WinNT (default) ○ LDAP

Allow login when

☑ Password has expired ☑ Password must change

Side-by-side

Enable NPS internal Connection Request Policies execution: On failure only

CAUTION: Test user authentication carefully when using any of these settings. Incorrect credentials could be accepted, if forwarding is not configured correctly.

Skip SMS PASSCODE validation and fail immediately for passwords matching the regular expression: ^\d*$

Default domains

test1
test1.com

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