

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:

付 VPN Wizard	-	×
VPN Wizard	VPN Tunnel Type (Step 1 of)	
Branch Br	Use this wizard to configure new tunnel between two devices is ca established by calls from remote This wizard creates basic tunnel (site-to-site VPN tunnels or new remote access VPN tunnels. A illed a site-to-site tunnel and is bidirectional. A tunnel users such as telecommuters is called remote access tunnel. configurations that you can edit later using the ASDM.
Corporate Network	VPN Tunnel Type:	Site-to-Site VPN
	🔘 Site-to-Site	
	Remote Access	Local Contraction Contractication Contracticatii Contractication Contracti
	VPN Tunnel Interface:	utside 👻
	Enable inbound IPsec session authorization access lists still	ns to bypass interface access lists. Group policy and per-user apply to the traffic.
		≤Back <u>Next</u> > Einish <u>Cancel H</u> elp

4. Select the Cisco VPN Client option and click next:





5. Click next once you have set the Pre-Shared Key parameter:

		_
VPN Wizard	/PN Client Authentication Method and Tunnel Group Name (Step 3 of)	
Branch	The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the subsequent screens. Configure authentication method and turnel group for this remote connection. Use the same tunnel group name for the device and the remote client.	
	Dra shared low	
Home	O Pre-shared key	
Corporate	Pre-Shared Key: SecretHasToMachOnVPNClient	
Nu	O Certificate	
1	Certificate Signing Algorithm: rsa-sig	
	Certificate Name: ASDM_TrustPoint1 v	
THUM	Challenge/response authentication (CRACK)	
THE	Tunnel Group	
The	Tunnel Group Name: GroupNameHasToMachOnVPNClient	
	SBack Next > Einish Gancel Help]

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

New Authentication Server Gro	pup
Create a new authentication se To add more servers to the gro Configuration > Device Manage	erver group containing one authentication server. up or change other AAA server settings, go to ement > Users/AAA > AAA Server Groups.
Server Group Name:	SMSÞasscode
Authentication Protocol:	RADIUS
Server IP Address:	10. 10. 10. 10
Interface:	inside 🔻
Server Secret Key:	•••••
Confirm Server Secret Key:	•••••
ОК	Cancel Help

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





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:

🔯 VPN Wizard	
VPN Wizard	IKE Policy (Step 7 of 10)
Brondt Brondt	Select the encryption algorithm, authentication algorithm, and Diffe_Helman group for the devices to use to negotiate an Internet Key Exchange (IXE) security association between them. Configurations on both sales of the connection must match exactly.
Corporate Natwork	Encryption: DDES Authentication: SHA
	Diffe-Helman Group: 2

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

VPN Wizard	IPsec Settings (Optional) (Step 8 of 10)
Branch	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.
I Month	Selected Hosts/Networks:
Consume Consume	Host/Network Interface: inade Add Delete
-	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-Helman Group: 1
	<u>≤Back</u> <u>Next</u> > Enish <u>Cancel</u> <u>Help</u>



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 10.255.253.0 255.255.240

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

🚰 Edit AAA Server	X
Server Group: SI	MSPASSCODE
Interface Name: ii	nside 👻
Server Name or IP Address: 1	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	
Message Table	*
ОК	Cancel Help



And in the Connection Profile "Enable password management"

🖆 Edit AnyConnect Connecti	on Profile: DefaultWEBVPNGroup	X
Baic Advanced Generic Clent Addressing Clent Addressing Scondary Authenticat Authentication Secondary Authenticat Authorization Accounting Group Alias/Group URL	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:	
	Notify user days prior to password expiration Notify user on the day password expires Override account-disabled indication from AAA Server	
\sim		

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

MS PASSEDDE® - C	onfiguration T	ool	378	passo	ode
Database Password Reset	Transmissi RADIUS CE	on Network	ork Import/	End-use Export /	r IP About
Allow login when	pired 🗖 Paco	word must change			÷
Fastword has en Side-by-side Enable IAS WPS inte	epied M Pass	CAUTION: Test u	ler authentic	ation carefully	Ŧ
Request Policies eve	cution:	when using any of	these setting	gr. Inconect	1.00
Always		not configured con	rectly.	, a roowarding s	•

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

	🔊 Cisco AnyCo	nnect testasa	.smspassco 💌
-	Answer:	*****	
S Cisco AnyConnect testasa.smspassco	Authentication M	lessage	
Please enter your username and password.	Enter PASSCOD	E	^
Username: pwdchange			
Password ******			~
OK Cancel		Continue	Cancel
🛇 Cisco AnyConnect testasa.smspassco 🗙			
Answer:			
Authentication Message Enter password again in order to complete			
password change			
U			
Continue Cancel			
S Cisco AnyConnect I testasa.smspasscod ×			
New Password:			
Verify Password:			
Authentication Message			
password expiring, you must enter a new A			
Continue Cancel			

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.



📴 Cisco ASDM 6.4 for ASA - 10.35.11.	20		- 2
File View Tools Wizards Wind	low Help	Look For:	©
Home 🔏 Configuration 🔯 Mor	nitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦻 Help		CISCO
Device List 🗗 🕂 🗡	Configuration > Remote Access VPN > Network (Client) Access > Any	Connect Client Software	
Add Delete Sonnect Find: Go 10.055.11.20 Go moxa2.smspasscode.net	AnyConnect Client Images Clack AnyConnect Client packages can be downloaded from the Clack Web usin browser to an initiate connection setup time by moving the image used by the n Φ Add $[\underline{c}]$ Replace $[\underline{b}]$ Delete $\frac{1}{2} \neq \frac{1}{2}$	g the search string 'AnyConnect VPN Clent'. The regular expression is nost commonly encountered operation system to the top of the list.	used to match the user-agent of a
Remote Access VIII (3) (3) AnyConnect Clent Porfie (3) (3) AnyConnect Clent Porfie (3) (3) Dynamc Access Poldes (3) (3) Breec(DicV) (3) (3) (3) Dynamc Access Poldes (4) (4) (4) Dy	Inge dido/myonnett-dertein-2.5.600540 pkg	Regular expression to match user-agent	

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.

S Cisco AnyConnect testasa.smspassco	×
New Password Required but user not allowed to change	<u>.</u>
Username: pwdchange	
Password:	
OK Cancel	



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:

olicy Name: SMS_A	uthorization				
escription: Author	ization attributes from SMS Passcode Radius			ACL Priority: 0	
Selection Criteria Define the AAA a below and every specify the logica	nd endpoint attributes used to select this acc endpoint attribute has been satisfied. These l expression text.	ess policy. A policy attributes can be c	is used when a user's reated using the table	authorization attributes match the Ai s below and/or by expanding the Adv	AA attribute criteria vanced option to
User has ANY of	the following AAA Attributes values 👻		and the following e	ndpoint attributes are satisfied.	
AAA Attribute	Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
180/05.25	- RenoteAccess,	Edit			Edit
		Delete			Delete
					Logical Op.
Advanced Access/Authorizatio Configure access, group-policy hiera	on Policy Attributes /authorization attributes for this policy. Attrib rdhy. The resulting VPN authorization policy i field in DAP)	ute values specifie s an aggregation o	d here will override th f DAP attributes, AAA	ose values obtained from the AAA sys attributes, and group-policy hierarch	stem and the y attributes (those
Advanced Access/Authorization Configure access, group-policy hiera that are not spect Action Network	on Policy Attributes //authorization attributes for this policy. Attrib rchy. The resulting VPN authorization policy i field in DAP). k ACL Filters Web-Type ACL Filters Functi	ute values specifie s an aggregation o ons Port Forward	d here will override thi f DAP attributes, AAA ng Lists Bookmarks	ose values obtained from the AAA sys attributes, and group-policy hierarch Access Method	stem and the y attributes (those
Advanced Access/Authorizatic Configure access, group-policy hiera that are not spec Action Networ	on Policy Attributes Authorization attributes for this policy. Attrib rchy, The resulting VPN authorization policy i field in DAP). k ACL Filters Web-Type ACL Filters Functi	ute values specifie s an aggregation o ons Port Forward	d here wil override th FDAP attributes, AAA ng Lists Bookmarks	ose values obtained from the AAA sys attributes, and group-policy hierarch Access Method Network ACLs	stem and the y attributes (those
Advanced Access/Authorizatio Configure access, group-policy hiere that are not spec Action Network Network ACL	an Policy Attributes fourthinization attributes for this policy. Attrib field in DAP). K ACL Filters Web-Type ACL Filters Functi (only all-permit and all-deny entries allowed)	ute values specifie s an aggregation o ons Port Forward	d here will override th FDAP attributes, AAA ng Lists Bookmarks	ose values obtained from the AAA sys attributes, and group-policy hierarch Access Method Network ACLs Auth_Test	stem and the y attributes (those
Advanced Access/Authorizatic Configure access, group-policy hiere that are not spec Action Network Network ACL Auth_Test	an Policy Attributes deuthorization attributes for this policy. Attrib field in DAP). K AQL Filters Web-Type AQL Filters Functi Web-Type AQL Filters Function (only all-permit and all-deny entries allowed)	ute values specifie s an aggregation o ons Port Forward	d here will override th FDAP attributes, AAA ng Lists Bookmarks Add>>	ose values obtained from the AAA sys attributes, and group-policy hierarch Access Method Network ACLs Auth_Test	stem and the y attributes (those
Advanced Access/Authorizatic Configure access group-policy hiere that are not spect Action Network Network ACL Auth_Test	on Policy Attributes Authorization attributes for this policy. Attrib field in DAP). K ACL Filters Web-Type ACL Filters Functb (only all-permit and all-deny entries allowed)	ute values specifie s an aggregation o ons Port Forward	d here will override th f DAP attributes, AAA ng Lists Bookmarks Add>>> Delete	ose values obtained from the AAA sys attributes, and group-policy hierarch Access Method Network ACLs Auth_Test	stem and the y attributes (those
Advanced Access/Authorizatic Configure access group-policy hiers that are not spec Action Network Network ACI Auth_Test	on Policy Attributes Authorization attributes for this policy. Attrib field in DAP). K. ACL. Filters Web-Type ACL Filters Functs (only all-permit and all-deny entries allowed)	ute values specifie s an aggregation o ons Port Forward	d here wil override the DAP attributes, AAA ng Lists Bookmarks Add>> Delete	ose values obtained from the AAA sys attributes, and group-policy hierarch Access Method Network ACLs Auth_Text	Stem and the y attributes (those
Advanced Access/Authorizatic Configure access group-policy hiers that are not spect Action Network Network ACI Auth_Test	on Policy Attributes (authorization attributes for this policy. Attrib fact in DAP). Red in DAP). KACL Filters Web-Type ACL Filters Funct KACL Filters Web-Type ACL Filters Funct	ute values specifier s an aggregation o ons Port Forward	d here will override th f DAP attributes, AAA ng Lists Bookmarks Add>> Delete	ose values obtained from the AAA sys attributes, and group-policy hierarch Access Method Network ACLs Auth_Text	Stem and the y attributes (those
Advanced Access/Authorizatic Configure access proup-policy hier that are not spec Action Network ACI Auth_Test	an Policy Attributes for this policy. Attrib feel in DAP). K ACL Filters Web-Type ACL Filters Function (only all-permit and all-deny entries allowed)	ute values specifie s an aggregation o ons Port Forward	d here will override th FDAP attributes, AAA ng Lists Bookmarks Add>> Delete	ose values obtained from the AAA sys attributes, and group-policy hierarch Access Method Network ACLs Auth_Test	stem and the y attributes (those
Advanced Access/Authorizabic Configure access, group-policy hier that are not spec Action Network ACI Auth_Test	an Policy Attributes fourthorized no attributes for this policy. Attrib field in DAP). K ACL Filters Web-Type ACL Filters Functi (only all-permit and all-deny entries allowed)	ute values specifie s an aggregation o ons Port Forward) Manage	d here will override th F DAP attributes, AAA ng Lists Bookmarks Add>> Delete	ose values obtained from the AAA sys attributes, and group-policy hierarch Access Method Network ACLs Auth_Test	stem and the y attributes (those
Advanced Access/Authorizatic Configure access proup-policy hier that are not spec Action Network ACL Auth_Test	an Policy Attributes Authorization attributes for this policy. Attrib field in DAP). K ACL Filters Web-Type ACL Filters Function K ACL Filters Web-Type ACL Filters Function (only all-permit and all-deny entries allowed)	ute values specifie an aggregation o ons Port Forward	d here wil override th FDAP attributes, AAA ng Lists Bookmarks Add>> Delete	ose values obtained from the AAA sys attributes, and group-policy hierarch Access Method Network ACLs Auth_Test	Stem and the y attributes (those
Advanced Access/Authorizatic Configure access, group-policy hitter that are not spec- that are not spec- lead and the special special special Network ACL Auth_Test	an Policy Attributes (withinvasion attributes for this policy. Attrib (roly, The reading VPN authorization policy (red in DAP). ACL Filters Web-Type ACL Filters Funct (only all-permit and all-deny entries allowed)	ute values specifie s an aggregation o ons Port Forward) Manage	d here will override thi DAP attributes, AAA ng Lists Bookmarks Add>> Delete	ose values obtained from the AAA sys attributes, and group-policy hierarch Access Method Network ACLs Auth_Text	stem and the y attributes (those

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:

TIADIOS Client	Database Protection	SMS Transmission	Network About
uthentication Au	uthorization Mis	cellaneous	
Authorization enal	bled		
Authorization att	ribute properties		
Max size of attribute	-		
Vendor code:			
1	-		
Attribute number:			
25	-		
Prefix	Separator:		
ou=	1		
Restrict groups Restrict to groups:	collected into the	authorization attribute	Add
group1			Remove
group2 group3			lle
			Down
Conly collect first	matching group		

Please note that the separator is a semikolon



Setup Group policies in ASA to match the groups

1	Cisco ASDM 6.2 for ASA - 10.6.0.19	178 m	Statement of the local division in which the local division in the	
Fil	e View Tools Wizards Window Help			
	Home Configuration Monitoring	Save 🔇 Refresh 🔇 Back 💭 Forward	2 Help	
	Remote Access VPN a P ×	Configuration > Remote Access VPN > Netwo	ork (Client) Access > Group Policies	
Device U	Introduction Network (Client) Access AnyConnect Connection Profiles IPsec Connection Profiles Croup Policies Dynamic Access Policies	Manage VPN group policies. A VPN group is a coll VPN connection profiles and user accounts. To enforce authorization attributes from an LDA Add • 2 Edit 1 Delete	ection of user-oriented authorization attribute/value pai P server you must use an <u>LDAP attribute map</u> .	rs that may be stored internally on the d
	Address Assignment	Name	Туре	Tunneling Protocol
	Advanced	MSVPN	Internal	LZTP-IPSec
	E Clentless SSL VPN Access	Test	Internal	IPSec,webvpn
	Easy VPN Remote	SMS	Internal	IPSec,webvpn,svc
	😑 🚮 AAA/Local Users	DfitGrpPolicy (System Default)	Internal	IPSec,L2TP-IPSec
	AAA Server Groups	group1	Internal	- Inherited -
	LUAP Attribute Map	group2	Internal	- Inherited -
	Secure Desktop Manager	group3	Internal	Inherited

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

General	Name:	group1			
B Advanced	Banner:	V Inherit			
	Address Pools:	Inherit	SMS		Select
	IPv6 Address Pools:	💟 Inherit			Select
	More Ontions				(*)
	more options				
	Prore options				
	Hore options				
	Hore options				
	The options				
	THE OPLINES				
	Hore options				



Selection Crit Define the	eria AAA and endpoint attributes used to selec	t this access policy. A polic	y is used when a user's	authorization attributes match the A	AA attribute criteria
specify the	logical expression text.	 These attributes can be 	created using the table	es below and/or by expanding the Adv	vanced option to
User has A	NY of the following AAA Attributes values	•• •	and the following e	ndpoint attributes are satisfied.	
AAA Attra	oute Operation/Value	Add	Endpoint ID	Name/Operation/Value	Add
radius.25	= ou=group1;	Edit			Edit
		Delete			Delete
			5		
					copia op.
Advance	d				
Access/Auth Configure a group-polic that are no Action	orization Policy Attributes access/authorization attributes for this policy hierarchy. The resulting VPN authorization t specified in DAP). letwork ACL Filters Web-Type ACL Filters	cy. Attribute values specifi in policy is an aggregation Functions Port Forwar	ed here will override th of DAP attributes, AAA ding Lists Bookmarks	ose values obtained from the AAA sy attributes, and group-policy hierarch Access Method	stem and the ny attributes (those
Access/Auth Configure a group-polic that are no Action	orization Policy Attributes cccess/authorization attributes for this poli- y hierarchy. The resulting VPN authorization t specified in DAP). letwork ACL Filters Web-Type ACL Filters Continue Terminate 0	cy. Attribute values specifi n policy is an aggregation	ed here wil override th of DAP attributes, AAA ding Lists Bookmarks	ose values obtained from the AAA sy attributes, and group-policy hierarch Access Method	stem and the ny attributes (those
Access/Auth Configure a group-polic that are no Action Action Specify	orization Policy Attributes iccess/authorization attributes for this poli- typerarchy. The resulting VPN authorization typeofied in DAP). ietwork ACL Filters Web-Type ACL Filters Continue Terminate Continues the message that will be displayed when the	cy. Attribute values specifi n policy is an aggregation Functions Port Forwar is record is selected.	ed here will override th of DAP attributes, AAA ding Lists Bookmarks	ose values obtained from the AAA sy attributes, and group-policy hierarch Access Method	stem and the ny attributes (those
Access/Auth Configure a group-polic that are no Action Action: Specify 1 User Me	orization Policy Attributes iccess/authorization attributes for this policy is peofied in DAP). ietwork ACL Filters Web-Type ACL Filters Continue Terminate Continue the message that will be displayed when the issage:	cy. Attribute values specifi n policy is an aggregation Functions Port Forwar is record is selected.	ed here wil override th of DAP attributes, AAA ding Lists Bookmarks	ose values obtained from the AAA sy attributes, and group-policy hierarch Access Method	stem and the ny attributes (those



(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

MS PASSCODE® - Configuration Tool	ginel	Dasscor		
General Database RADIUS Client Protection	SMS Transmission Net Import/Export Ab			
Authentication Authorization Miscel	llaneous			
Authorization enabled				
Authorization attribute properties Max size of attribute:				
4 🗄				
Vendor code:				
1 🔅				
Attribute number:				
25				
Prefix Separator:				
ou=				
Active directory resolve provider				
G Global catalon C LDAP				
Restrict groups collected into the ar Restrict to groups:	uthorization attribute			
1		Add		
group1;group1		Remove		
group2;group2		TICHIOTE		

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 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: \wedge d*\$

See screenshot for example.

5MS PASSCODE®	- Configuratio	1 Tool		_	
				sna passco	Je
ieneral Databa	ise SMS Tran	smission Network	RADIUS Client Protect	ion Import/Export About	
Authentication	Authorization	Miscellaneous			4
Allow login w	hen				-
Password ha	s expired 🔽 Pa	assword must change			
Request Policies	execution:	Incorrect credentia	ls could be accepted, if forw	arding is not configured correctly.	
Skip password va	alidation for the fol	owing type of password	ls:		
^\d*\$ 🔶		_			
Password val	idation				_
• WinNT O	Custom LDAP:	smspassword			
	- V - when				

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

About SMS PASSCODE®

SMS PASSCODE is the leading technology in two- and multi-factor authentication using your mobile phone. To protect against the rise in internet based identity theft hitting both consumers and corporate employees, SMS PASSCODE offers a stronger authentication via the mobile phone SMS service compared to traditional alternatives. SMS PASSCODE installs in minutes and is much easier to implement and administer with the added benefit that users find it an intuitively smart way to gain better protection. The solution offers out-of-the-box protection of standard login systems such as Citrix, Cisco, Microsoft, VMware View, Juniper and other IPsec and SSL VPN systems as well as web sites. Installed at thousands of sites, this is a proven patent pending technology. In the last years, SMS PASSCODE has been named to the Gartner Group Magic Quadrant on User Authentication, awarded twice to the prestigious Red Herring 100 most interesting tech companies list, a Secure Computing Magazine Top 5 Security Innovator, InfoSecurity Guide Best two-factor authentication, a Citrix Solution of the Year Finalist, White Bull top 30 EMEA companies, a Gazelle 2010, 2011, 2012 and 2013 Fast Growth firm and a ComOn most promising IT company Award. For more information visit: www.smspasscode.com or our blog at blog.smspasscode.com.