
How to Configure VPN Authentication for SMS PASSCODE

<https://campus.barracuda.com/doc/53248376/>

SMS PASSCODE offers strong authentication via SMS messaging on mobile phones. It provides out-of-the-box protection of standard login systems such as Citrix, Cisco, Microsoft, other IPsec and SSL VPN systems as well as websites. Follow the steps in this article to configure VPN authentication for SMS PASSCODE.

Step 1. Enable RADIUS Authentication

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. In the left menu, select **RADIUS Authentication**.
3. Click **Lock**.
4. From the **Activate Scheme** field, select **Yes**.
5. In the **Radius Server Address** field, enter the IP address of the IAS/NPS server as the SMS PASSCODE RADIUS authentication client.

The **Radius Server Key** must match the **Shared Secret** on the server. The shared secret can consist of small and capital characters, numbers, and non alpha-numeric symbols, except the hash sign (#).

6. Click **Send Changes** and **Activate**.

Step 2. Configure the Client-to-Site VPN

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > Client to Site**.
2. Click **Lock**.
3. Click the **External CA** tab and then click the **Click here for options** link.
4. In the **Group VPN Settings** window, select the **External Authentication** check box.
5. From the **Authentication Scheme** list, select **radius**.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 3. Create a Group Policy

Create a **Group Policy** with the corresponding **Group Policy Condition** to allow access from the client.

It is possible to limit to **Group Pattern** (groups sent in the **Login-LAT-Group** attribute).

Group Policy Setup

Edit Group Policy
X

Name Disabled

Common Settings TEST

Statistic Name

Network TestNetwork 10.30.50.0

DNS

WINS

Network Routes
10.6.0.0/32

Access Control List (ACL)

Access Control List

Barracuda | IPSec

Barracuda - Settings: TEST

Enable VPN Client NAC

ENA Split Tunnel ON

Domain

Firewall Rules

VPN Offline

Message Bitmap

Registry Firewall Always ON

Key **Tunnel**

Time Limit Probing

Traffic Limit Timeout

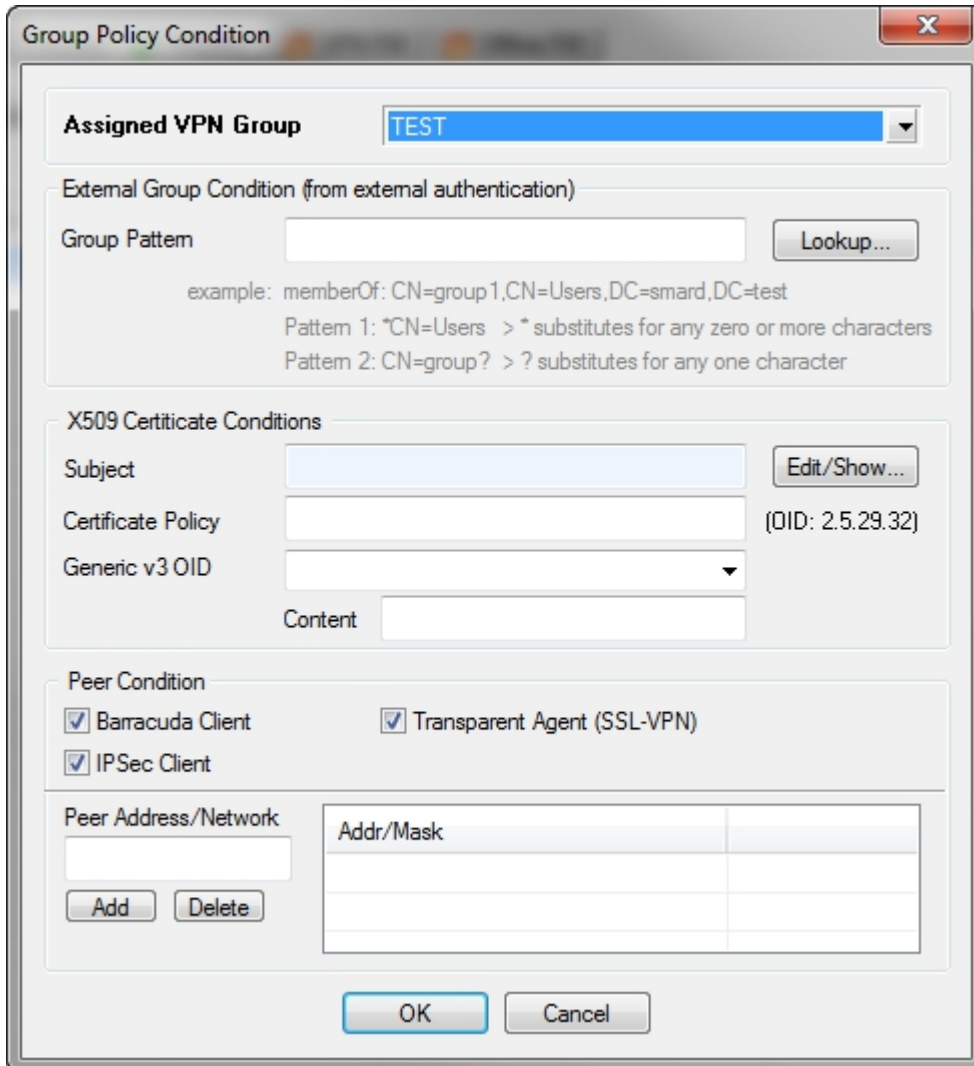
Accepted Ciphers: AES 256 CAST 3DES Null

AES Blowfish DES

Group Policy Condition

External Group	Client	X509 Subject	Cert Policy / OID	Peer
	Barracuda , IPSec , Tr. Agent		/ =	

Group Condition Setup



Assigned VPN Group TEST

External Group Condition (from external authentication)

Group Pattern

example: memberOf: CN=group1,CN=Users,DC=smard,DC=test
Pattern 1: *CN=Users > * substitutes for any zero or more characters
Pattern 2: CN=group? > ? substitutes for any one character

X509 Certificate Conditions

Subject

Certificate Policy (OID: 2.5.29.32)

Generic v3 OID

Content

Peer Condition

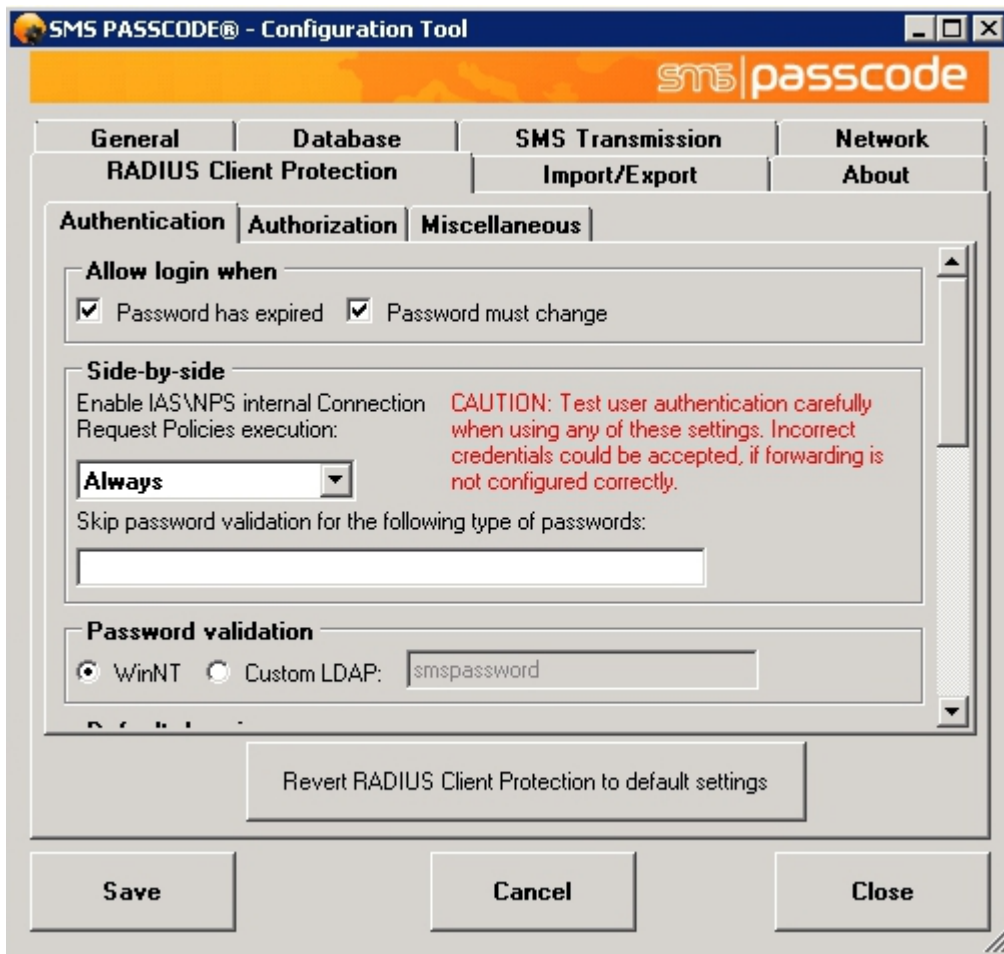
Barracuda Client Transparent Agent (SSL-VPN)
 IPSec Client

Peer Address/Network

Addr/Mask	
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

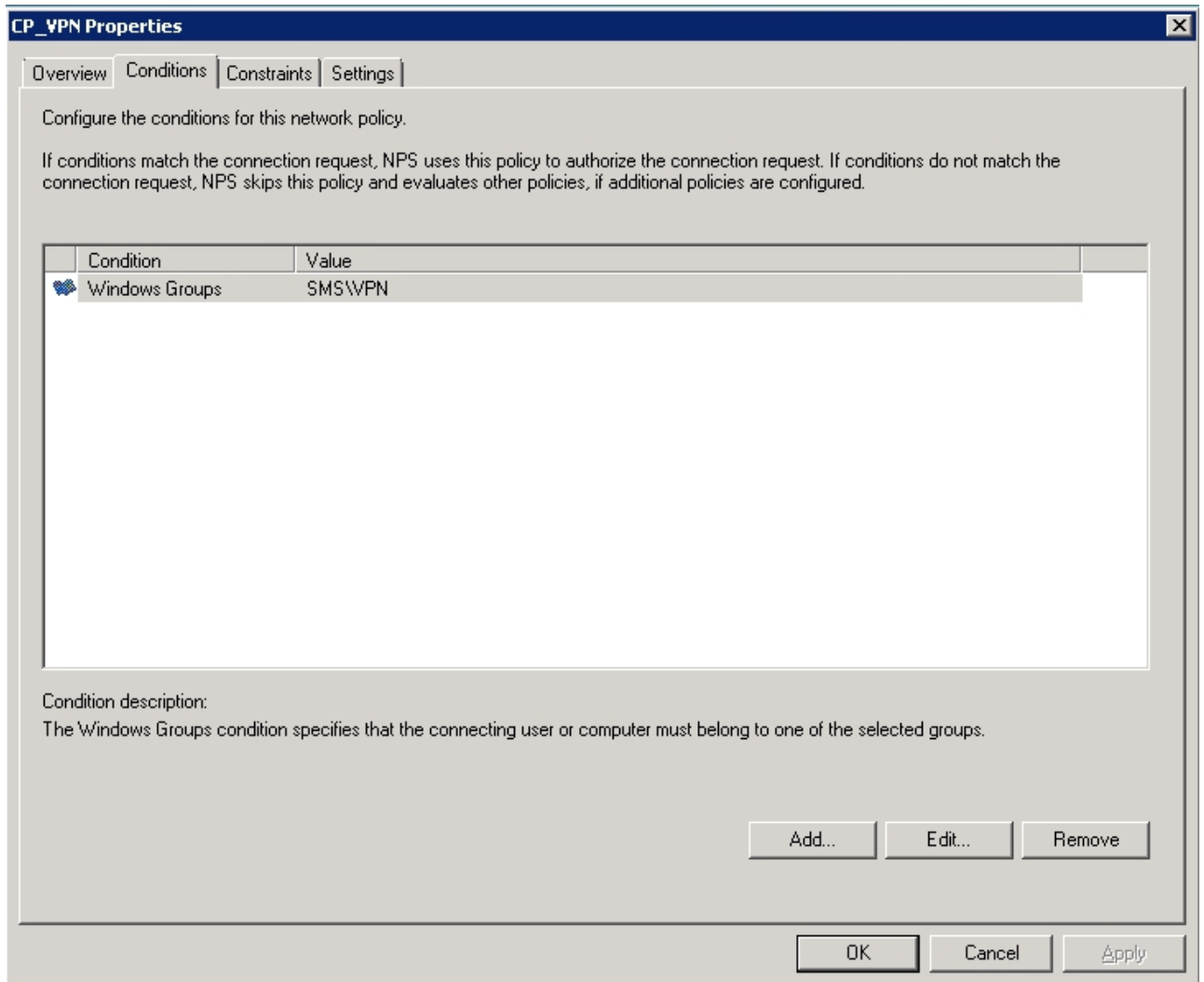
Step 4. Configure SMS PASSCODE

1. Install and configure the RADIUS client according to the "SMS PASSCODE Administrator's Guide."
2. From the **Authentication** tab in the **SMS PASSCODE - Configuration Tool** window, select **Always** from the **Request Policies execution** list in the **Side-by-side** section.
See the following figure:



3. Open the Microsoft Windows Network Policy Server (IAS/NPS) and create a network policy. Open the policy and choose the Windows groups containing the users.

The user must be a member of the group. For more details, see the "SMS PASSCODE Administrator's Guide."



4. To send group names to the RADIUS client, configure the **Login-LAT-Group** attribute.

CP_VPN Properties

Overview | Conditions | Constraints | **Settings**

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

- Standard
- Vendor Specific

Network Access Protection

- NAP Enforcement
- Extended State

Routing and Remote Access

- Multilink and Bandwidth Allocation Protocol (BAP)
- IP Filters
- Encryption
- IP Settings

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed
Login-LAT-Group	Group1; Group2; Group3

Figures

1. gr_policy.jpg
2. pol_cond.jpg
3. sms_pass.jpg
4. pass_admin.jpg
5. lat_login.jpg

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.