

## How to Configure VPN Authentication for SMS PASSCODE

<https://campus.barracuda.com/doc/96026122/>

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 **Basic** section, click **+** to add a RADIUS Server. The **Basic** configuration window opens.
6. 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 (#).
7. Click **OK**.
8. Select **Login-LAT-Group** from the **Group Attribute** drop-down list.
9. Next to the **Group Attribute Delimiter** field, select the **Other** check box.
10. Enter **;** as the the **Group Attribute Delimiter**.
11. From the **Group Attribute Usage** list, select **All**.

**RADIUS Authentication Settings**

Activate Scheme: Yes

Method: RADIUS

Basic

| Radius Server A... | Radius Server P... | Radius Server Key | NAS-ID |
|--------------------|--------------------|-------------------|--------|
| 10.10.10.10        | 1812               | *****             |        |

Group Attribute: Login-LAT-Group

Group Attribute Delimiter: :  Other

Group Attribute Usage: All

User Info Helper Scheme:

OTP Preserves State: No

Number of Processes: 5

*This scheme is referred to as radius/RADIUS in this and other configuration parts.*

12. Click **Send Changes** and **Activate**.

## Step 2. Configure the Client-to-Site VPN

1. Go to **CONFIGURATION > Configuration Tree > Box > 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. The **Group VPN Settings** window opens.
4. When using user/password authentication, select the **External Authentication** check box.
5. From the **Default Authentication Scheme** list, select **radius**.

Group VPN Settings

**X509 Client Security**

Mandatory Client Credentials  X509 Certificate  
 External Authentication  
 IPsec needs Xauth

Certificate Login Matching  Login must match AltName in Certificate

---

**Server**

Primary Authentication Scheme: Default Authentication Schi

Default Authentication Scheme: **radius**

Secondary Authentication Scheme: -NONE-  
 Ras Login permission required

**X509 Certificate**  
Client certificate authentication mandatory.

**External Authentication**  
User password authentication mandatory.

**IPsec needs Xauth**  
IPsec clients must support Xauth to connect.

**Certificate Login Matching**  
The user name part of the subjectAltName in the certificate must match the login name.

---

**Primary Authentication Scheme**  
Select a single authentication scheme, or extract from username (user@<auth. scheme name>) to use multiple authentication schemes. The default scheme is used as the fallback.

**Default Authentication Scheme**  
The default or fallback authentication scheme used to authenticate VPN clients.

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. (For detailed information on how to create group policies, see **Step 4** in [How to Configure a Client-to-Site VPN Group Policy.](#))

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

### Group Policy Setup

**Common Settings** TEST  Disabled

Statistic Name: TESTGP

**Network** TestNetwork 10.30.50.0

DNS IPv4: 10.5.0.6

DNS IPv6:

WINS:

Network Routes: Network Routes  
10.6.0.0/32

Access Control List (ACL): Access Control List

**Barracuda - Settings:** TEST

- Enforce Windows Security Settings (Vista and newer on...)
- VPN Client Network
 

|                    |    |
|--------------------|----|
| DNS Suffix for VPN |    |
| ENA                | No |
| Always On          | No |
- Firewall Rules
 

|                    |        |
|--------------------|--------|
| VPN Client NAC     | Ignore |
| VPN                |        |
| Offline            |        |
| Firewall Always ON | No     |
- Login Message
 

|         |  |
|---------|--|
| Message |  |
| Bitmap  |  |
- Encryption Algorithms

**Enforce Windows Security Settings (Vista and newer only)**  
Enforce MS Windows security features for NG Network Access Clients to allow VPN connections. Requires MS Windows Vista or later.

**Group Policy Condition**

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

Export to file ... OK Cancel

### Group Condition Setup

Group Policy Condition

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

Use One-Time Password

X509 Certificate Conditions

Subject

Certificate Policy  (OID: 2.5.29.32)

Generic v3 OID

Content

Client Condition

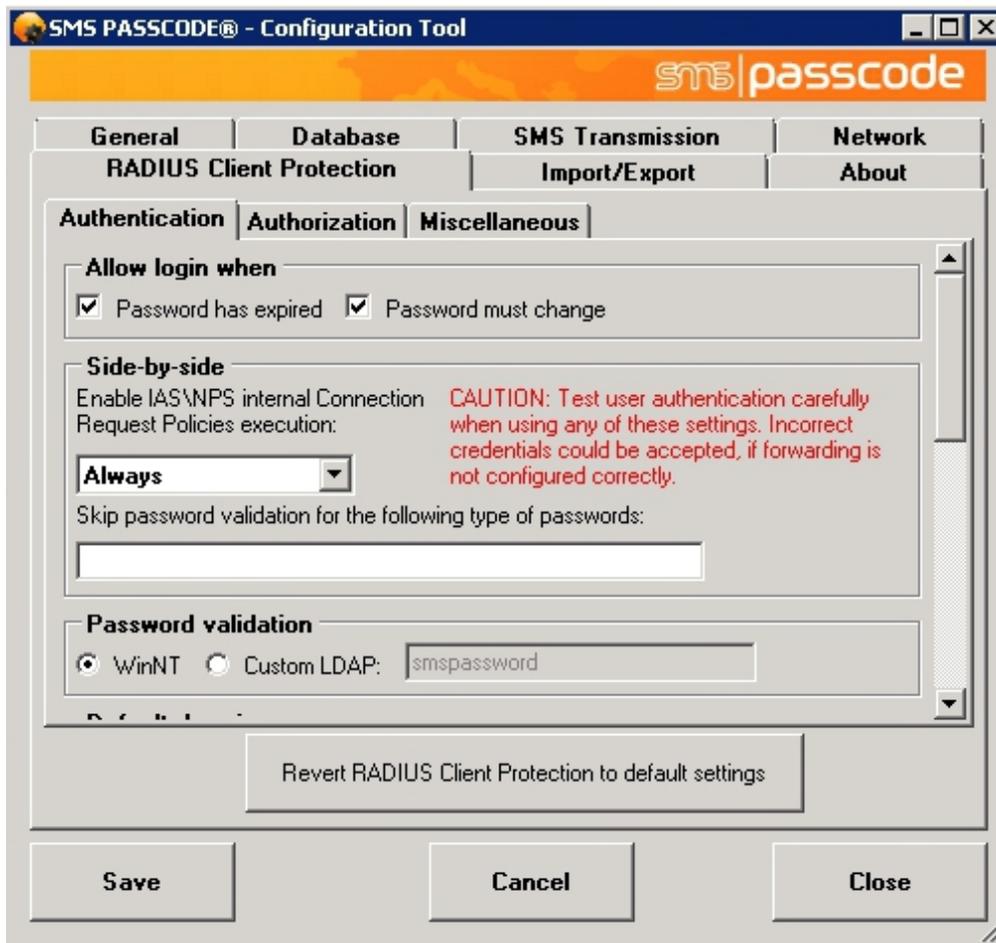
Barracuda Client  IPsec Client

Peer Address/Network

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

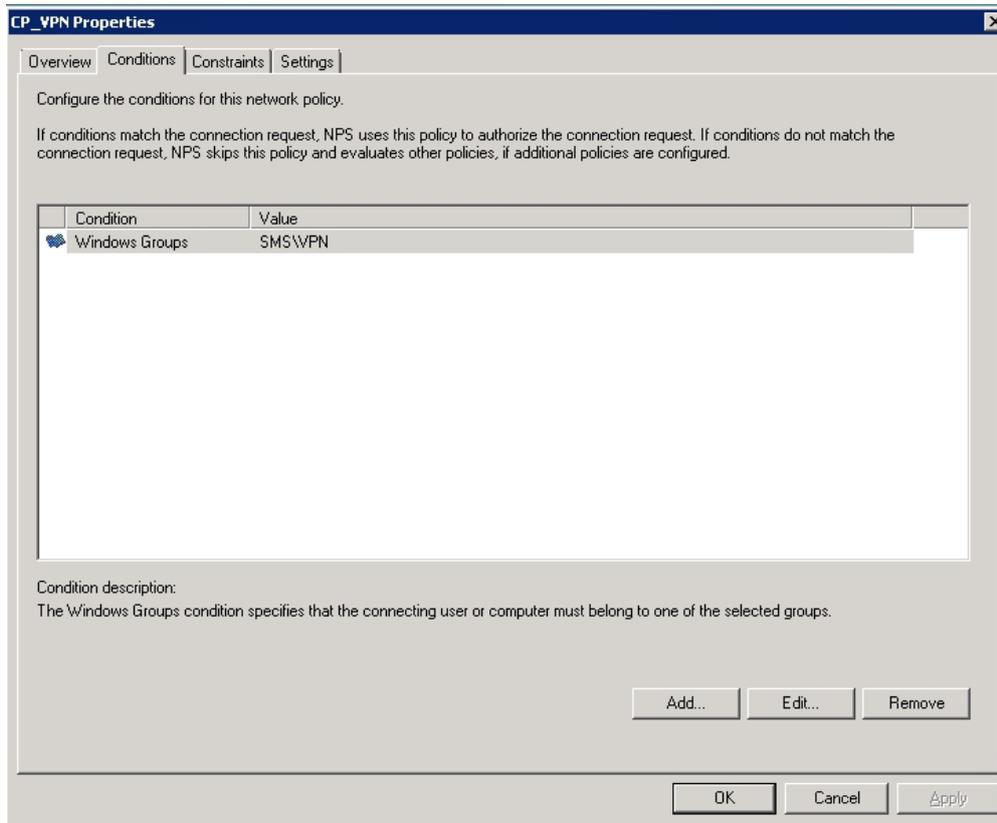
## Step 4. Configure SMS PASSCODE

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:

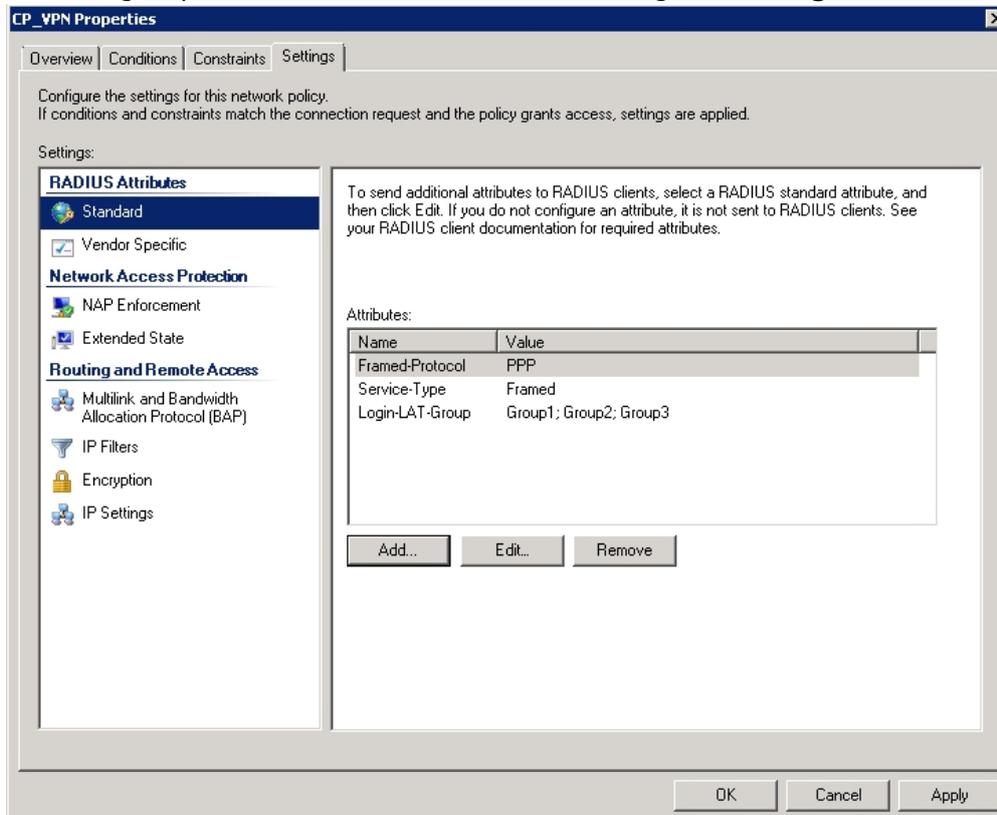


3. Open the Microsoft Windows Network Policy Server (IAS/NPS) and create a network policy. Open the policy and choose the Windows groups containing the users.

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.



## Figures

1. sms\_p01.png
2. sms\_p02.png
3. gr\_policy.png
4. pol\_cond.png
5. sms\_pass.jpg
6. pass\_admin.jpg
7. lat\_login.jpg

© Barracuda Networks Inc., 2024 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.