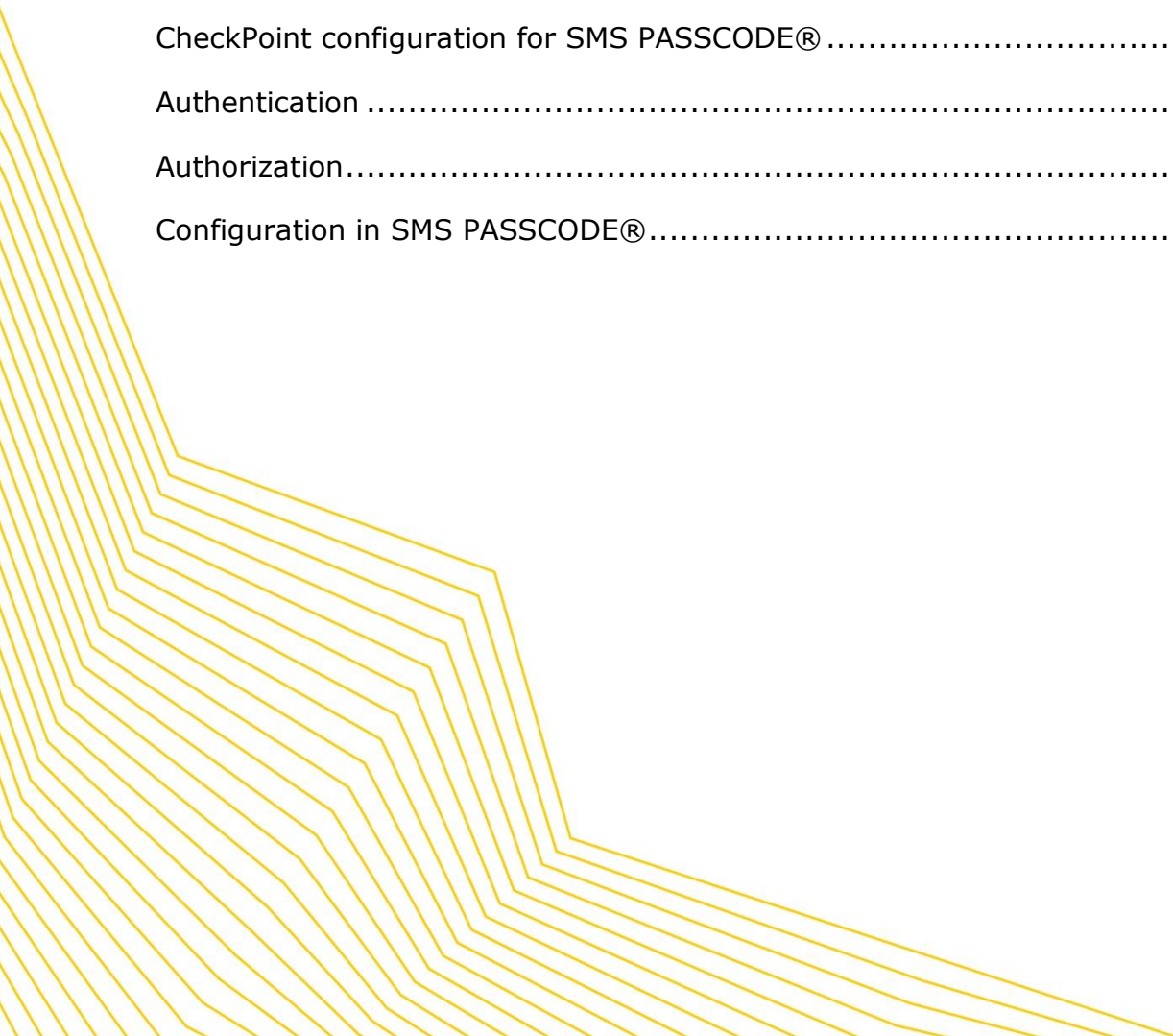




SMS PASSCODE CheckPoint R77 Configuration

Contents

- SMS PASSCODE CheckPoint R77 Configuration 0
- CheckPoint configuration for SMS PASSCODE® 1
- Authentication 1
- Authorization 3
- Configuration in SMS PASSCODE® 5



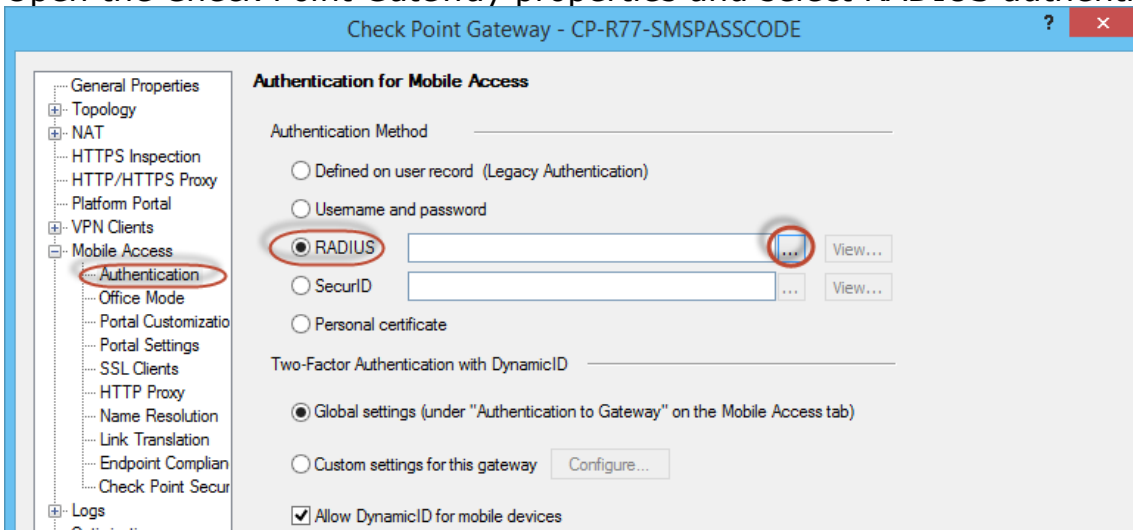


CheckPoint configuration for SMS PASSCODE®

This guide outlines the process of configuring a Check Point® for Authentication and Authorization with SMS PASSCODE®.

Authentication

Open the Check Point Gateway properties and select RADIUS authentication.



If not already created, create a RADIUS host or RADIUS group



Authentication Method

Defined on user record (Legacy Authentication)

Username and password

RADIUS

SecurID

Personal cert

Two-Factor Authentication: 0 object(s)

Global settings

Custom settings

Allow DynamicID for mobile devices

Name	Port	Comment

New...

RADIUS...

RADIUS Group...

Fill out the Shared Secret and select PAP.

RADIUS Server Properties - RADIUS_Auth

General Accounting

Name: RADIUS_Auth

Comment: RADIUS Authentication

Color: Orange

Host: RADIUS-1

Service: UDP RADIUS

Shared Secret: ●●●●

Version: RADIUS Ver. 2.0 Compatible

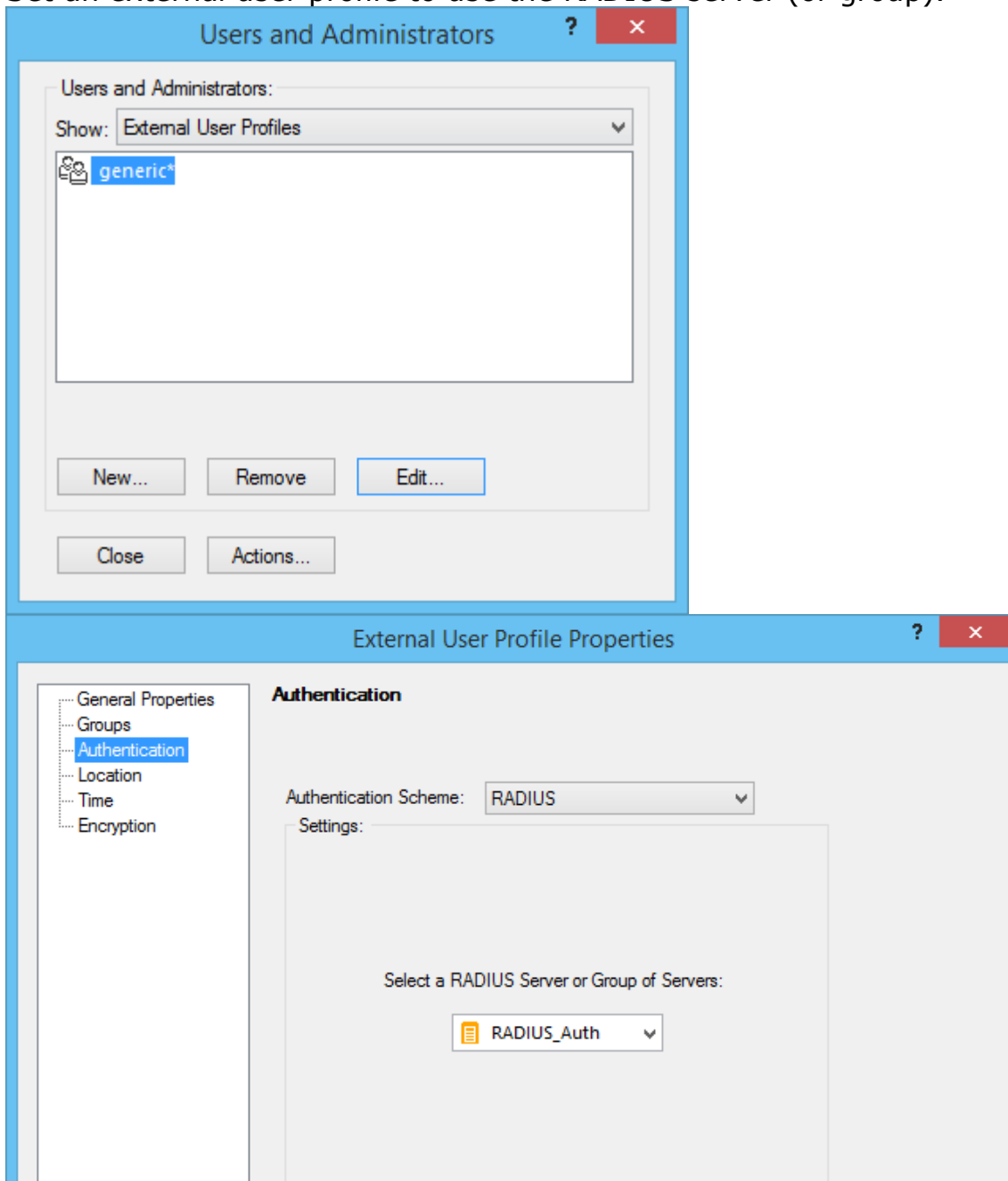
Protocol: PAP

Priority: 1 (1 is highest)

OK Cancel

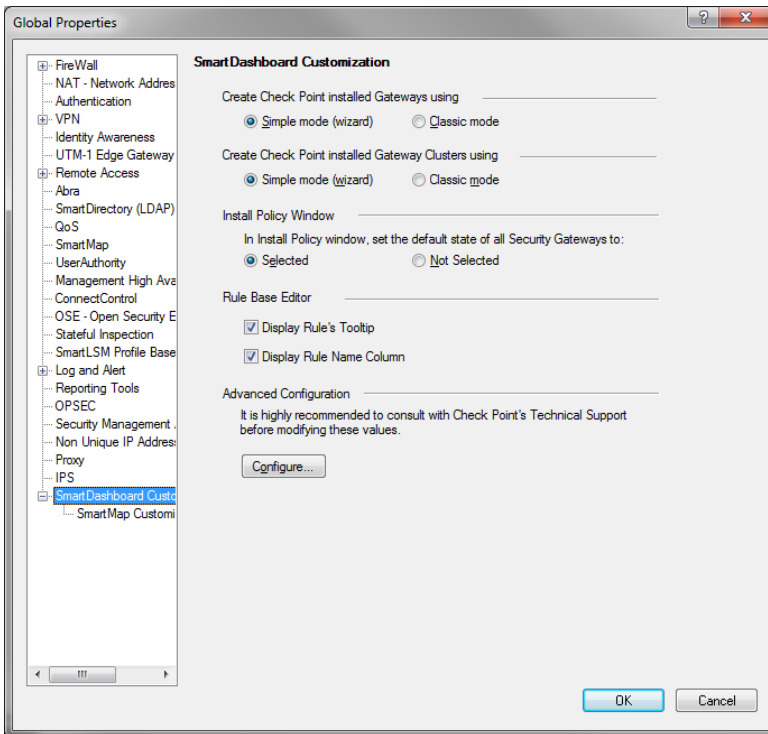


Set an external user profile to use the RADIUS server (or group).

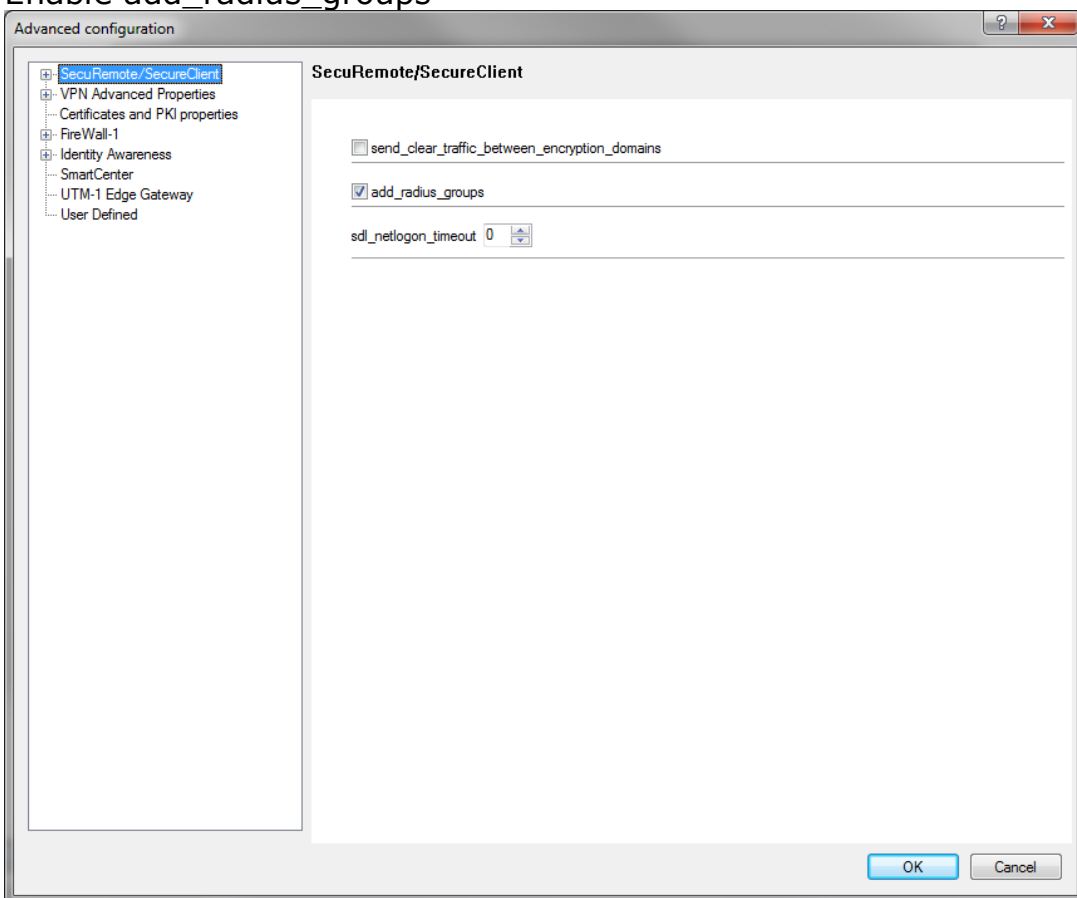


Authorization

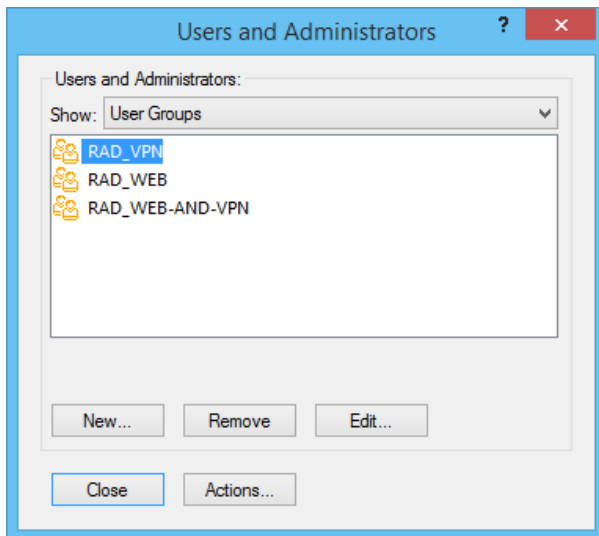
Navigate to Policy -> Global properties
Choose SmartDashboard Customization and press Configure.



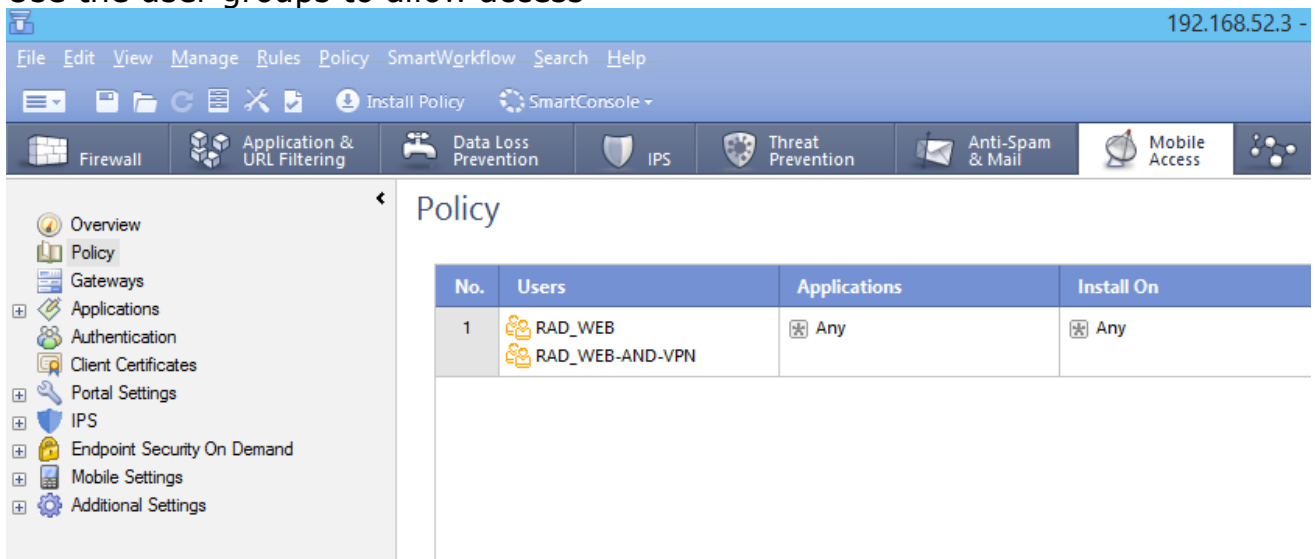
Enable add_radius_groups



Make User groups beginning with RAD_



Use the user groups to allow access



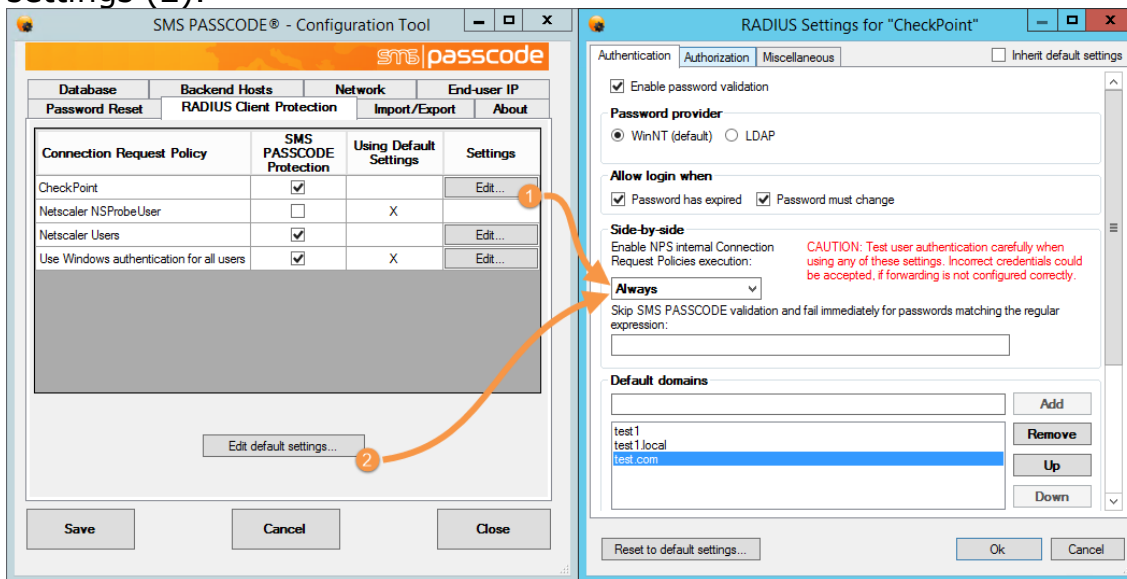
Configuration in SMS PASSCODE®

First, consult the SMS PASSCODE® Administrator Guide for configuration of the SMS PASSCODE Radius Client Protection.

Install the SMS PASSCODE radius protection and set side by side to Always in the SMS PASSCODE® configuration tool as illustrated below. You can configure

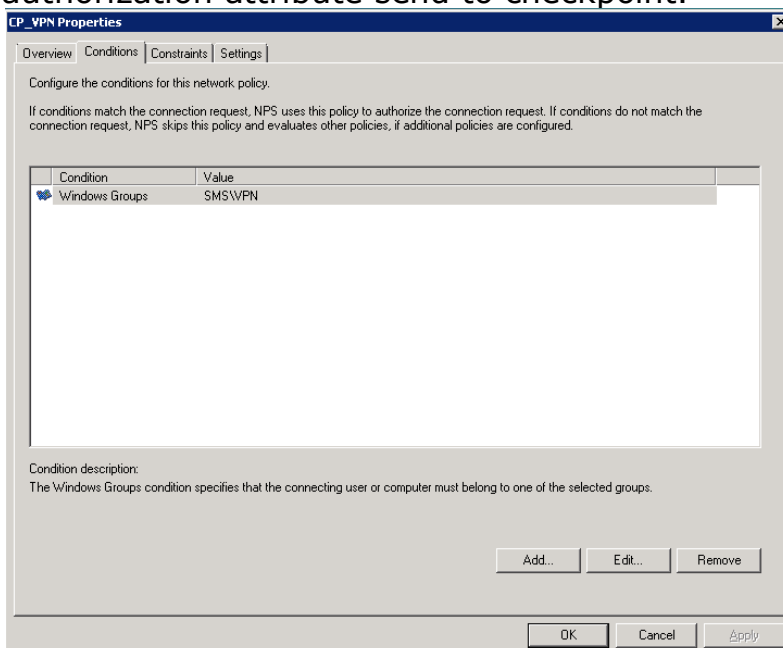


this in the individual Connection Request Policy settings (1) or in the default settings (2).



Create network policy

And choose the Windows group(s) where the user must be member to get the authorization attribute send to checkpoint.



The Class attribute can be used to send group name (without RAD_)



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
Class	VPN

Add... Edit... Remove

OK Cancel Apply