

censornet.

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 |

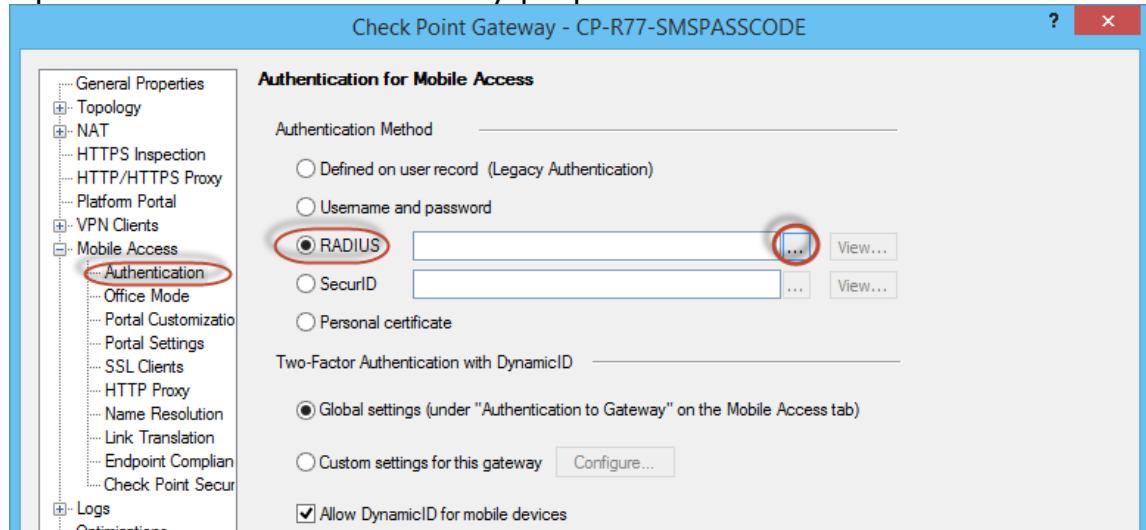


CheckPoint configuration for SMS PASSCODE®

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 certi

Two-Factor Authent: 0 object(s)

- Global setting
- Custom settings

Allow DynamicID for mobile devices

Fill out the Shared Secret and select PAP.

RADIUS Server Properties - RADIUS_Auth

| | |
|--|---|
| General | Accounting |
| Name: | <input type="text" value="RADIUS_Auth"/> |
| Comment: | <input type="text" value="RADIUS Authentication"/> |
| Color: | <input type="color" value="Orange"/> Orange |
| Host: | <input style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px; margin-right: 10px;" type="button" value="RADIUS-1"/> <input style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px;" type="button" value="New..."/> |
| Service: | <input style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px; margin-right: 10px;" type="button" value="UDP RADIUS"/> |
| Shared Secret: | <input type="text" value="*****"/> |
| Version: | <input style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px; margin-right: 10px;" type="button" value="RADIUS Ver. 2.0 Compatible"/> |
| Protocol: | <input style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px; margin-right: 10px;" type="button" value="PAP"/> |
| Priority: | 1 <input style="border: 1px solid #ccc; padding: 2px 5px; border-radius: 3px; margin-left: 10px;" type="button" value="▲"/> (1 is highest) |
| <input style="border: 1px solid #4db6ac; padding: 5px 10px; border-radius: 5px; background-color: #e0f2fd; color: #4db6ac; font-weight: bold; outline: none;" type="button" value="OK"/> <input style="border: 1px solid #ccc; padding: 5px 10px; border-radius: 5px; margin-left: 10px;" type="button" value="Cancel"/> | |



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

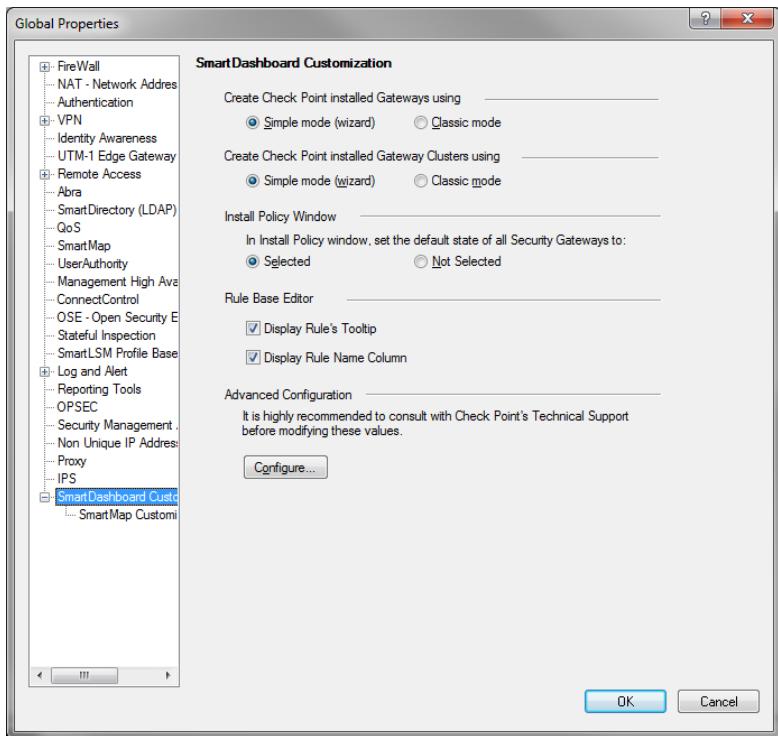
The screenshot shows the Censornet interface with two windows open:

- Users and Administrators** window:
 - Header: Users and Administrators
 - Show dropdown: External User Profiles
 - Content: A list box containing "generic*" with a user icon.
 - Buttons: New..., Remove, Edit... (highlighted), Close, Actions...
- External User Profile Properties** window:
 - Header: External User Profile Properties
 - Left sidebar (tree view): General Properties, Groups, **Authentication** (selected), Location, Time, Encryption.
 - Main content:
 - Authentication** section:
 - Authentication Scheme: RADIUS (selected)
 - Settings: A dropdown menu showing "RADIUS_Auth".
 - Select a RADIUS Server or Group of Servers: A dropdown menu showing "RADIUS_Auth".

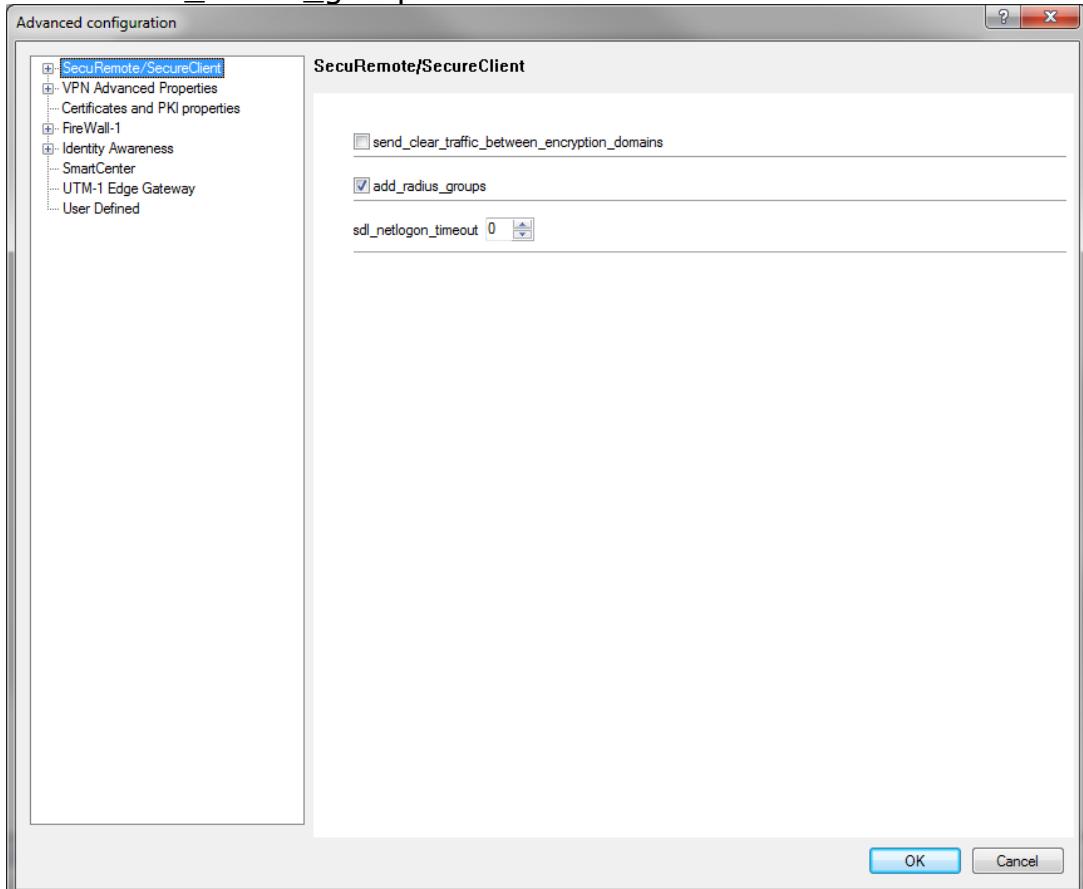
Authorization

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

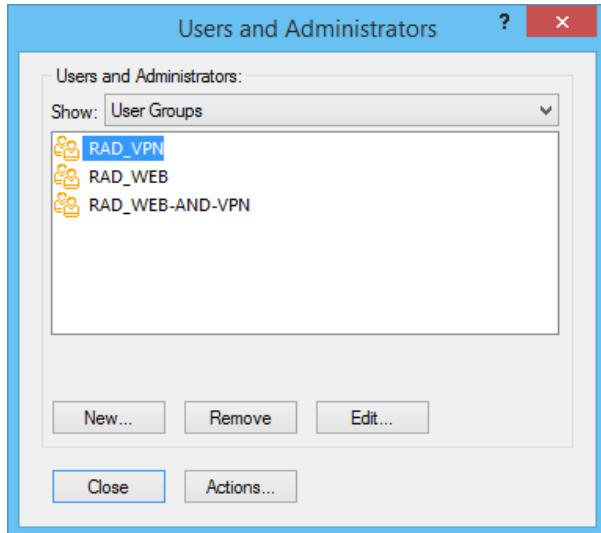
censornet.



Enable add_radius_groups



Make User groups beginning with RAD_



Use the user groups to allow access

| No. | Users | Applications | Install On |
|-----|----------------------------|--------------|------------|
| 1 | RAD_WEB RAD_WEB-AND-VPN | Any | Any |

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).

The screenshot shows two windows side-by-side. On the left is the 'SMS PASSCODE® - Configuration Tool' window, specifically the 'Connection Request Policy' tab. It lists four policies: 'CheckPoint' (checked), 'Netscaler NSProbeUser' (unchecked), 'Netscaler Users' (checked), and 'Use Windows authentication for all users' (checked). The 'Edit...' button for 'CheckPoint' is circled with a red number 1. The 'Edit default settings...' button at the bottom is circled with a red number 2. On the right is the 'RADIUS Settings for "CheckPoint"' window, showing the 'Authentication' tab. It has a dropdown menu under 'Side-by-side' set to 'Always'. A red arrow points from the 'Edit default settings...' button in the first window to this dropdown in the second window.

Create network policy

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

The screenshot shows the 'CP_VPN Properties' dialog box, specifically the 'Conditions' tab. It displays a table with one row: 'Condition' (Windows Groups) and 'Value' (SMSVPN). Below the table, a 'Condition description' section states: 'The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.' At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

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

