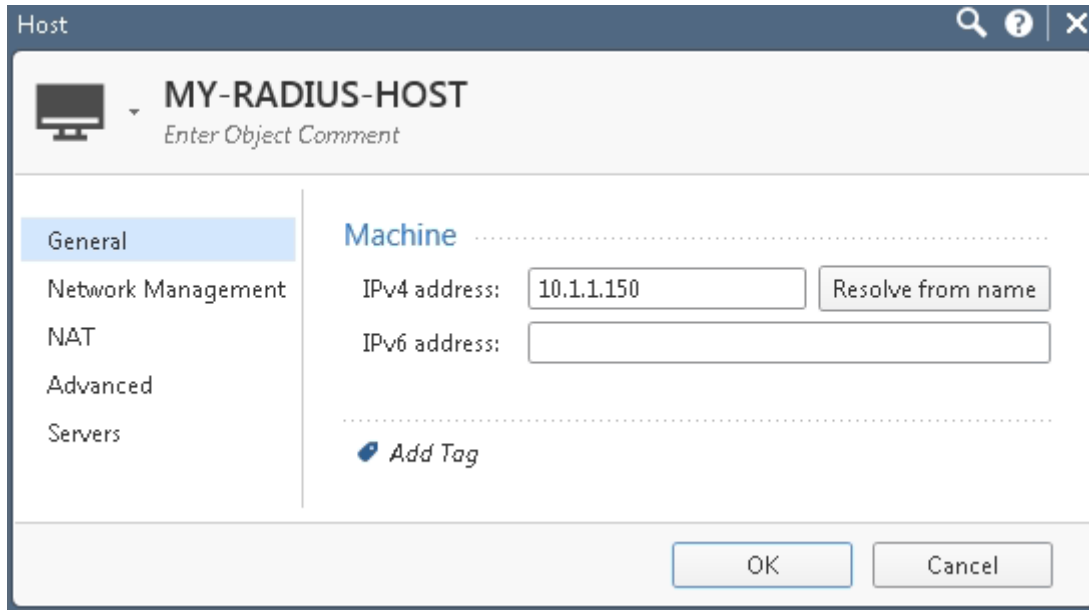
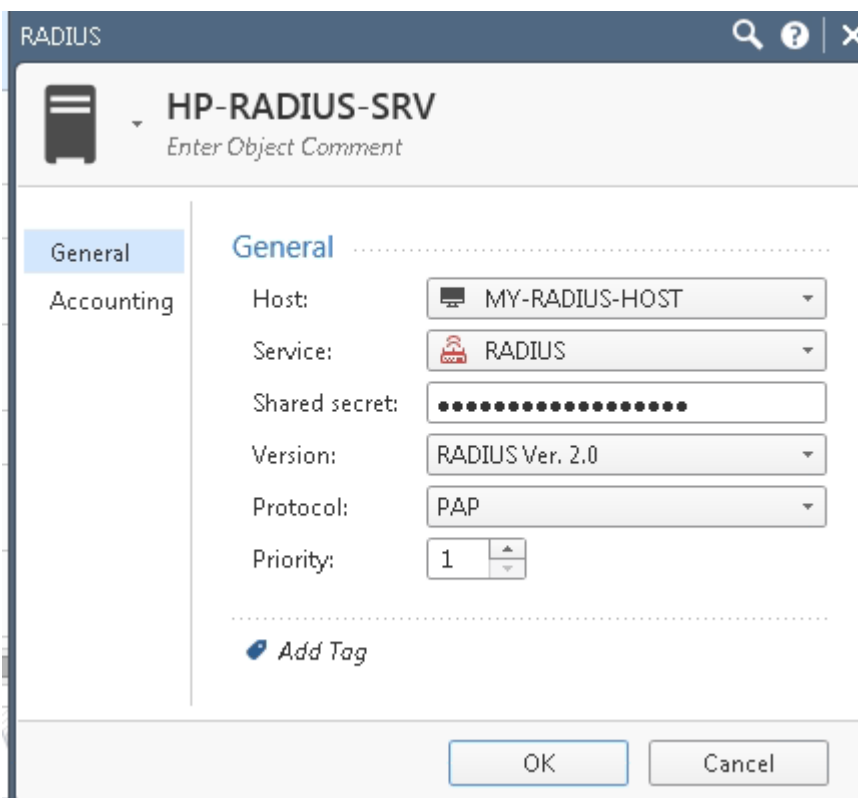


Remote access VPN Granting User Access Using RADIUS Server Groups

1. Create a Radius Server object and Host object




The screenshot shows the 'Host' configuration window for an object named 'MY-RADIUS-HOST'. The window has a title bar with search, help, and close icons. Below the title bar is a header area with the object name and a prompt to 'Enter Object Comment'. A left sidebar contains menu items: 'General' (selected), 'Network Management', 'NAT', 'Advanced', and 'Servers'. The main area is titled 'Machine' and contains the following fields: 'IPv4 address' with the value '10.1.1.150' and a 'Resolve from name' button; 'IPv6 address' with an empty text box; and an 'Add Tag' button. At the bottom are 'OK' and 'Cancel' buttons.



The screenshot shows the 'RADIUS' configuration window for an object named 'HP-RADIUS-SRV'. The window has a title bar with search, help, and close icons. Below the title bar is a header area with the object name and a prompt to 'Enter Object Comment'. A left sidebar contains menu items: 'General' (selected) and 'Accounting'. The main area is titled 'General' and contains the following fields: 'Host' with a dropdown menu showing 'MY-RADIUS-HOST'; 'Service' with a dropdown menu showing 'RADIUS'; 'Shared secret' with a masked text box (dots); 'Version' with a dropdown menu showing 'RADIUS Ver. 2.0'; 'Protocol' with a dropdown menu showing 'PAP'; and 'Priority' with a spinner box showing '1'. There is also an 'Add Tag' button. At the bottom are 'OK' and 'Cancel' buttons.

2. Create Empty group


User Group

 **RAD_project2**
Enter Object Comment

Mailing List Address:


+ | ×

| Name | Comments |
|-----------------------|----------|
| <i>No items found</i> | |

 Add Tag

OK Cancel


User Group

 **RAD_project1**
Enter Object Comment

Mailing List Address:

+ | ×

| Name | Comments |
|-----------------------|----------|
| <i>No items found</i> | |

 Add Tag

OK Cancel

3. Made the below changes via GUIDBEDIT

The screenshot shows the GUIBEDIT application interface. On the left is a tree view of the configuration hierarchy, with 'properties' selected. The main window displays a table of objects and a detailed field configuration table.

| Object Name | Class Name | Last Modify Time |
|-----------------------------|-----------------------------|--------------------------|
| firewall_properties | firewall_properties | Mon Apr 23 14:45:33 2018 |
| span_port_configuration | span_port_properties | Mon Apr 16 14:59:22 2018 |
| drop_down_mapping_container | drop_down_mapping_container | Mon Apr 16 14:59:22 2018 |

| Field Name | Type | Value | Valid Values | Default Value | Field description |
|------------------------------|--------------|---------|--------------|---------------|--|
| r_access_enable_p | string | first | first | first | r_access_enable_p |
| raccessenable | boolean | true | | true | Accept Remote Access control connections |
| radius_connect_timeout | unumber | 120 | 0~uint_max | 120 | radius_connect_timeout |
| radius_groups_sttr | number | 26 | 0~255 | 25 | radius_groups_sttr |
| radius_ignore | container | | 0~255 | | radius_ignore |
| radius_retrant_num | unumber | 2 | 0~uint_max | 2 | radius_retrant_num |
| radius_retrant_timeout | unumber | 5 | 0~uint_max | 5 | radius_retrant_timeout |
| radius_send_framed | boolean | false | | | radius_send_framed |
| radius_user_timeout | unumber | 600 | 0~uint_max | 600 | radius_user_timeout |
| rate_limit_sampling_interval | number | 1 | 1~600 | 1 | rate_limit_sampling_interval |
| registration | owned object | hotspot | hotspot | | registration |

The screenshot shows the GUIBEDIT application interface. On the left is a tree view of the configuration hierarchy, with 'properties' selected. The main window displays a table of objects and a detailed field configuration table.

| Object Name | Class Name | Last Modify Time |
|-----------------------------|-----------------------------|--------------------------|
| firewall_properties | firewall_properties | Mon Apr 23 14:45:33 2018 |
| span_port_configuration | span_port_properties | Mon Apr 16 14:59:22 2018 |
| drop_down_mapping_container | drop_down_mapping_container | Mon Apr 16 14:59:22 2018 |

| Field Name | Type | Value | Valid Values | Default Value | Field description |
|---------------------------------|--------------|------------------------------|-------------------------------------|---------------|--|
| accept_rip | boolean | false | | | accept_rip |
| acceptdecrypt | boolean | true | | true | Enable Accept on Decrypt for Gateway to G... |
| actions_limit_on | boolean | false | | | If true, the actions limit will be applied |
| active_resolver | boolean | true | true | true | active_resolver |
| add_ip_alt_name_for_ICA_certs | boolean | true | | true | add_ip_alt_name_for_ICA_certs |
| add_ip_alt_name_for_opsec_certs | boolean | false | | | add_ip_alt_name_for_opsec_certs |
| add_nt_groups | boolean | false | | | add_nt_groups |
| add_radius_groups | boolean | true | | | add_radius_groups |
| adresstrans | boolean | false | | | adresstrans |
| admin_expiration_global_data | owned object | admin_expiration_global_data | [admin_expiration_global_data,NULL] | | admin_expiration_global_data |
| expiration_date | string | 31-dec-2030 | | 31-dec-2030 | expiration_date |

Ready 192.168.10.5 Read/Write NUM

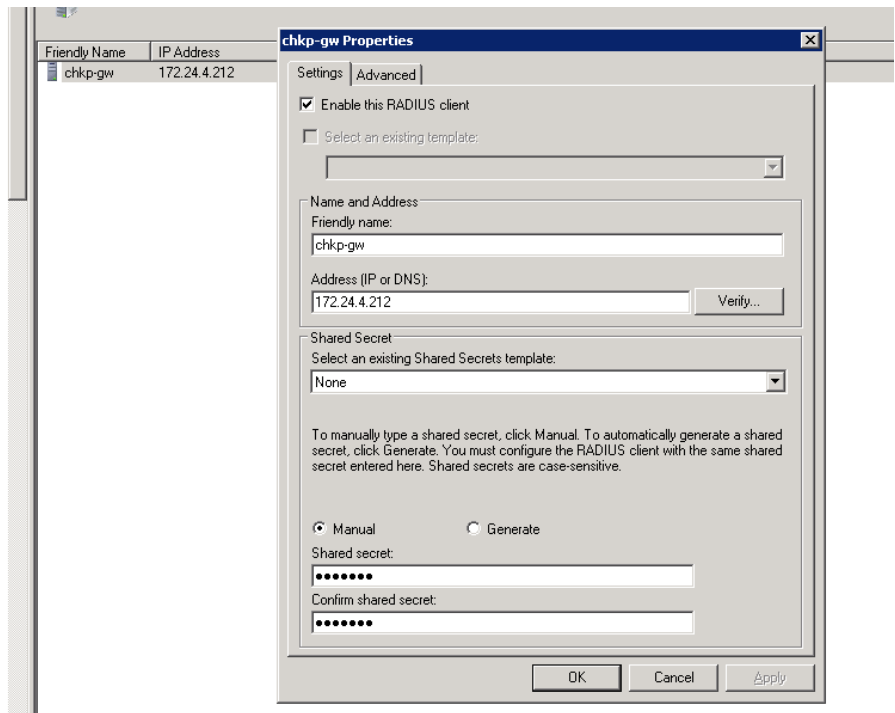
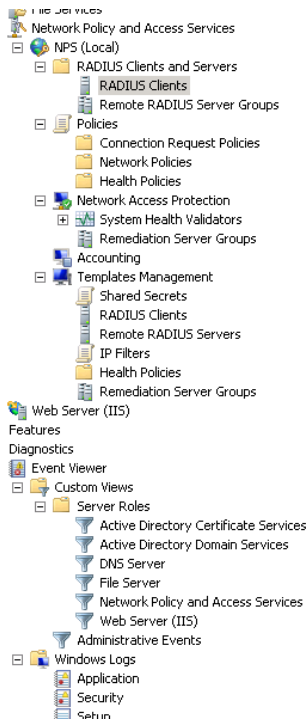
4. External profile Configuration

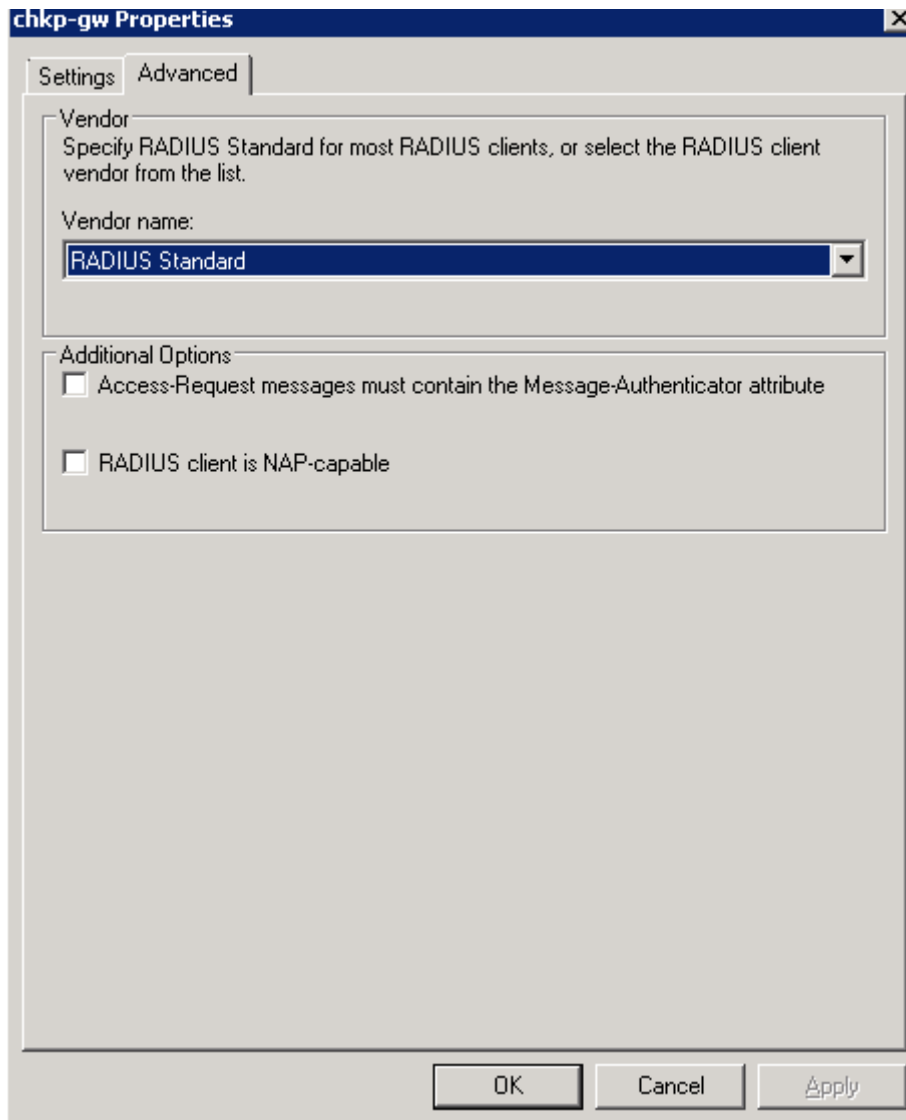
The screenshot shows the 'External User Profile Properties' dialog box. The 'General Properties' tab is active. The 'External User Profile name' is 'MFAUser'. The 'Expiration Date' is '12/31/2030'. Under 'Domain Name matching definitions', the 'Free format' option is selected, with 'Domain Name' set to 'chkpdemo.com' and 'Separator' set to '@'. The 'Outcome' is 'User_Name@chkpdemo.com'. The 'Omit Domain Name when authenticating users' checkbox is unchecked.

5. Access Rule using Empty group

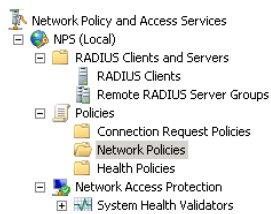
| | | | | | | | | |
|---|-----------|------------------|--------------|--------------|-------|--------|-------------------|------------------|
| 5 | Project 1 | RAD_project1@Any | STU13-MGMT01 | RemoteAccess | * Any | Accept | Log Accounting | * Policy Targets |
| 6 | Project 2 | RAD_project2@Any | ADMIN-PC | RemoteAccess | * Any | Accept | Log Accounting | * Policy Targets |

6. Radius Configuration





7. Network Policy :



| Policy Name | Status | Processing Order | Access Type | Source |
|---|---------|------------------|--------------|-------------|
| Connections to Microsoft Routing and Remote Access server | Enabled | 1 | Deny Access | Unspecified |
| Project1 | Enabled | 2 | Grant Access | Unspecified |
| Project2 | Enabled | 3 | Grant Access | Unspecified |

8. Network Policy For Project 1 :

Project1 Properties [X]

Overview | Conditions | Constraints | Settings

Policy name:

Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

Policy enabled

Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

Grant access. Grant access if the connection request matches this policy.

Deny access. Deny access if the connection request matches this policy.

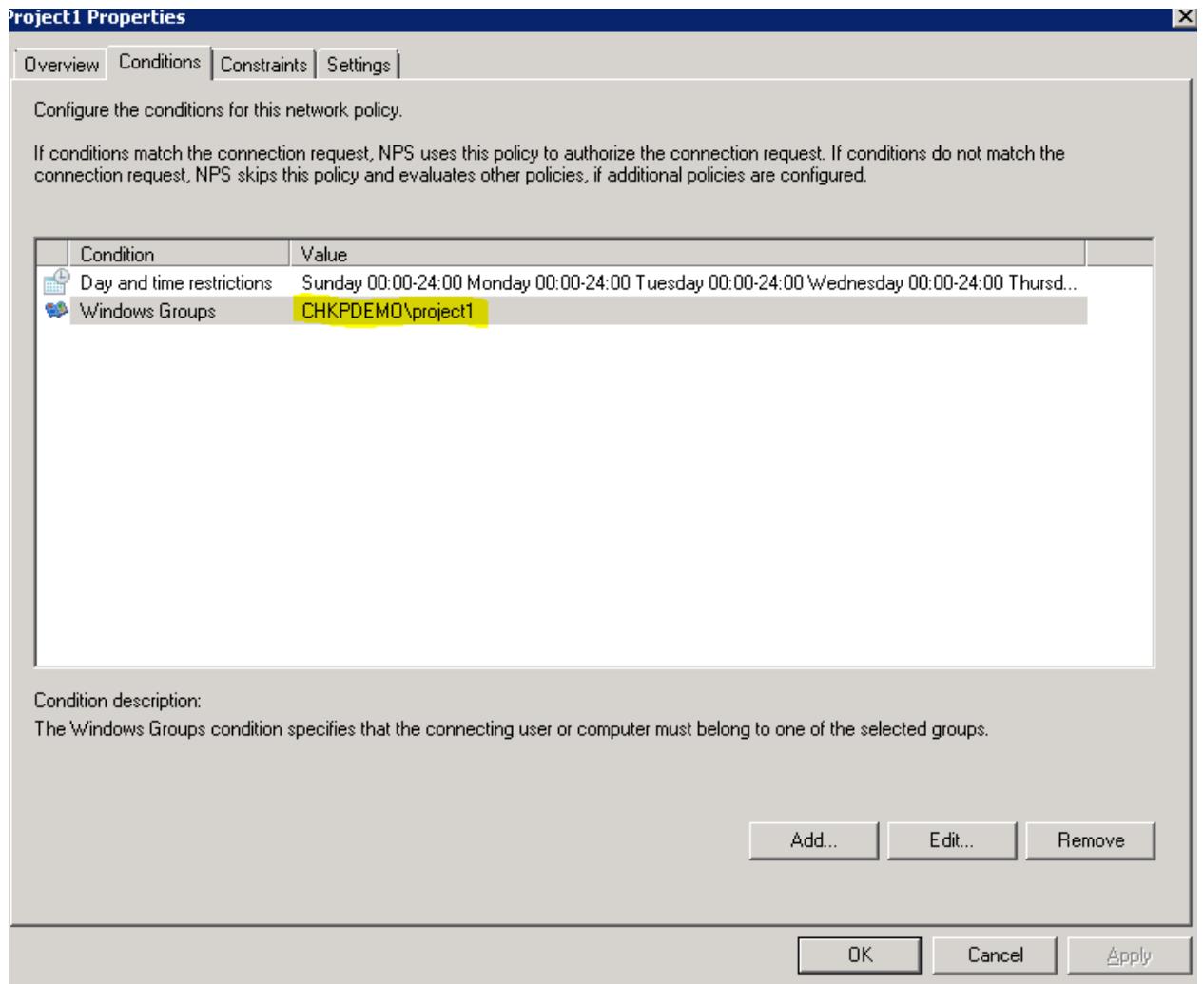
Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .

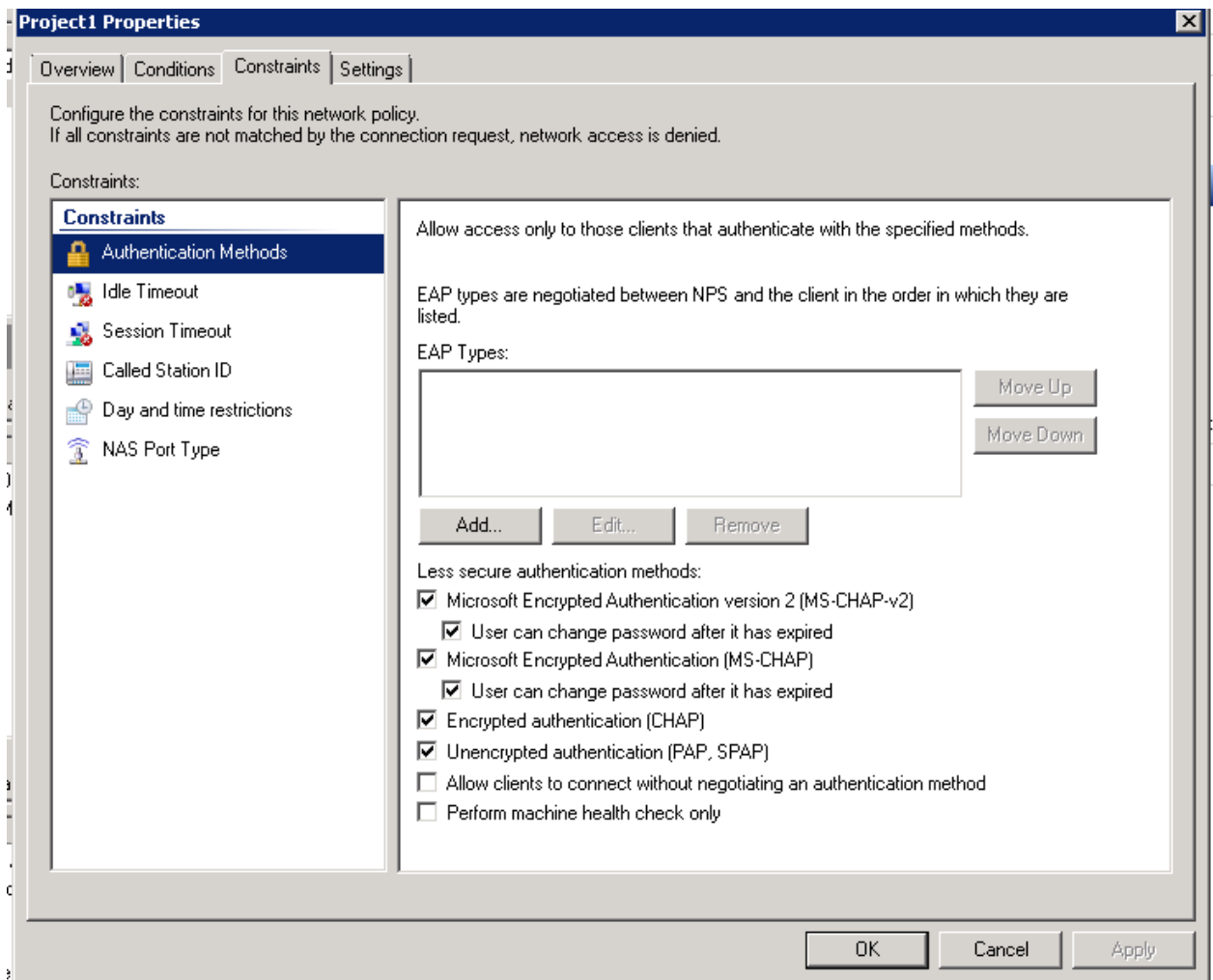
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

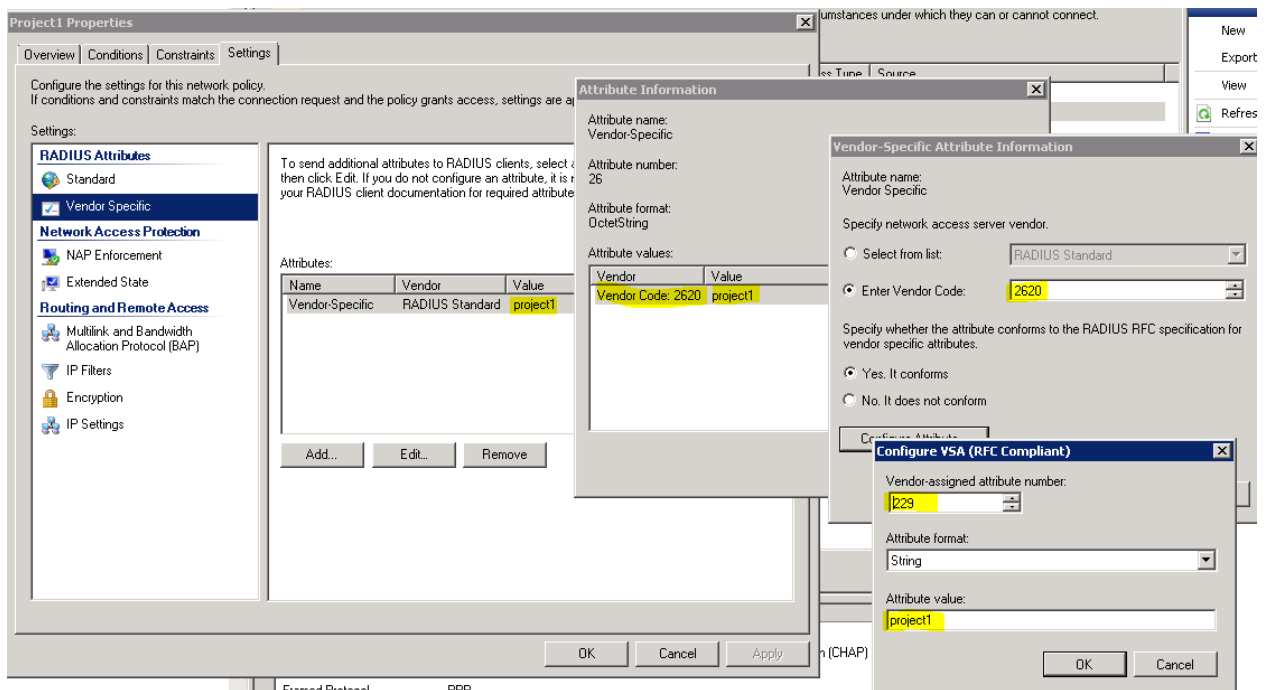
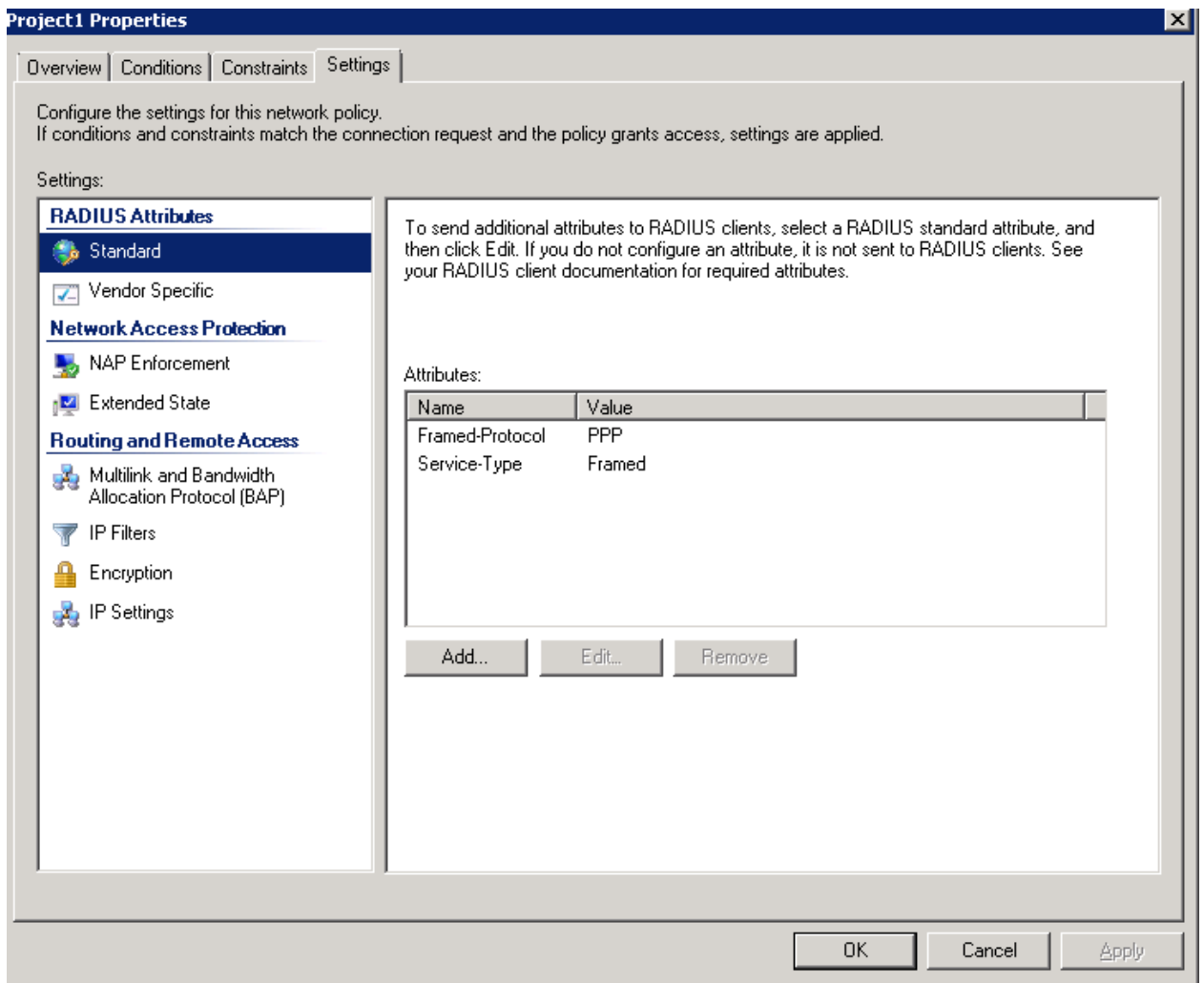
Type of network access server:

Vendor specific:

OK Cancel Apply







project 2

Project2 Properties

Overview | Conditions | Constraints | Settings

Policy name:

Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

Policy enabled

Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

Grant access. Grant access if the connection request matches this policy.
 Deny access. Deny access if the connection request matches this policy.
 Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:

Vendor specific:

OK Cancel Apply

