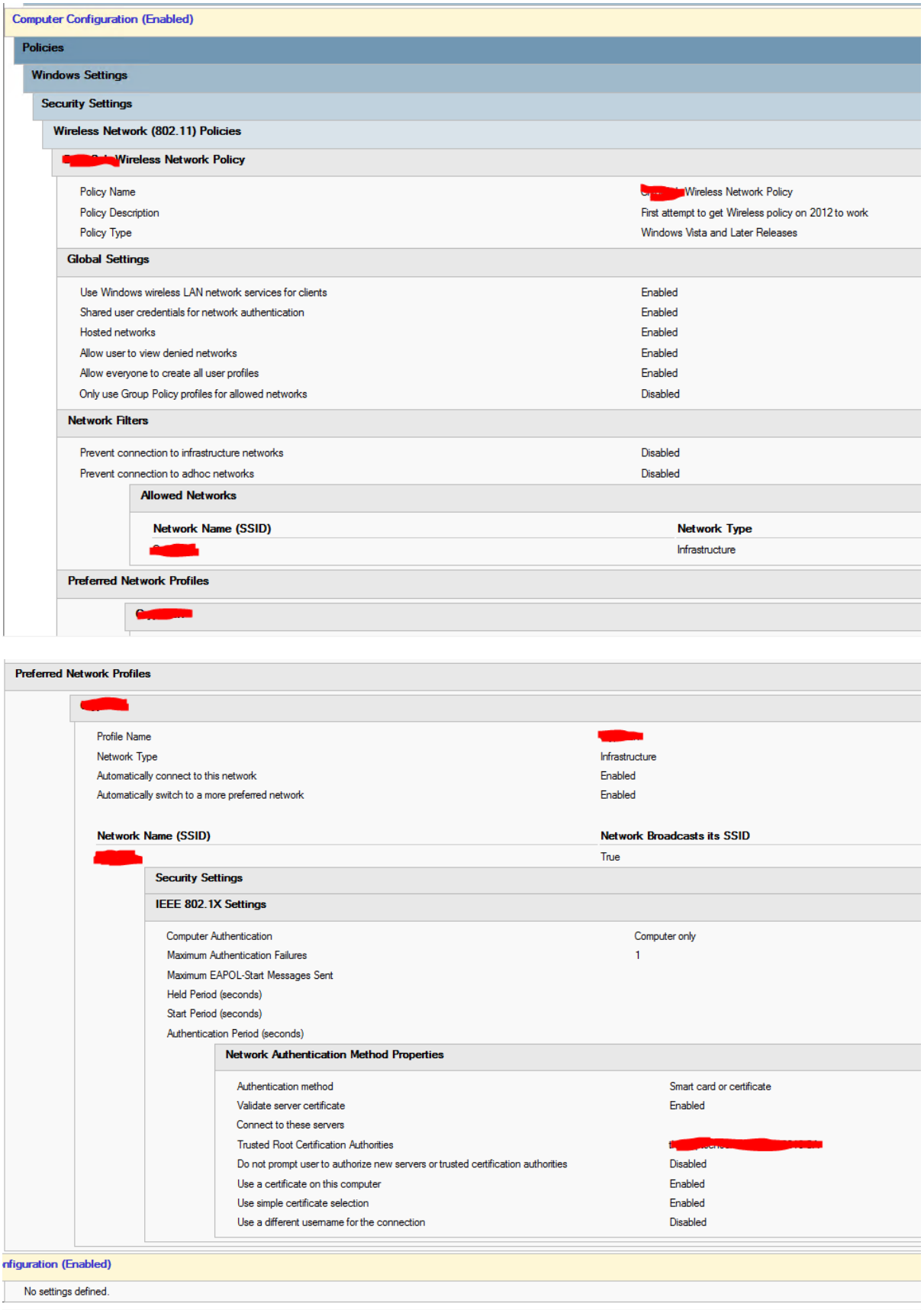
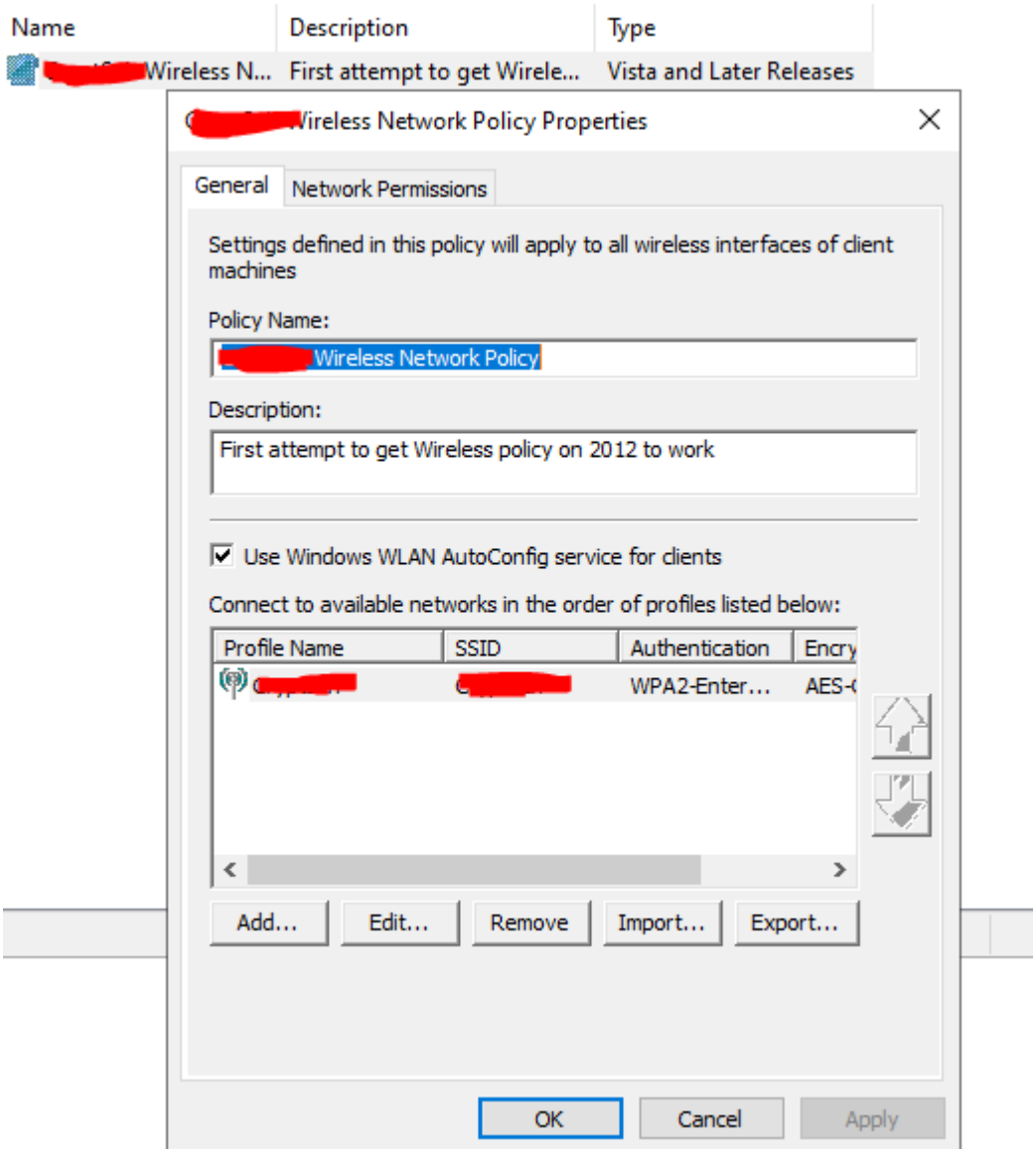
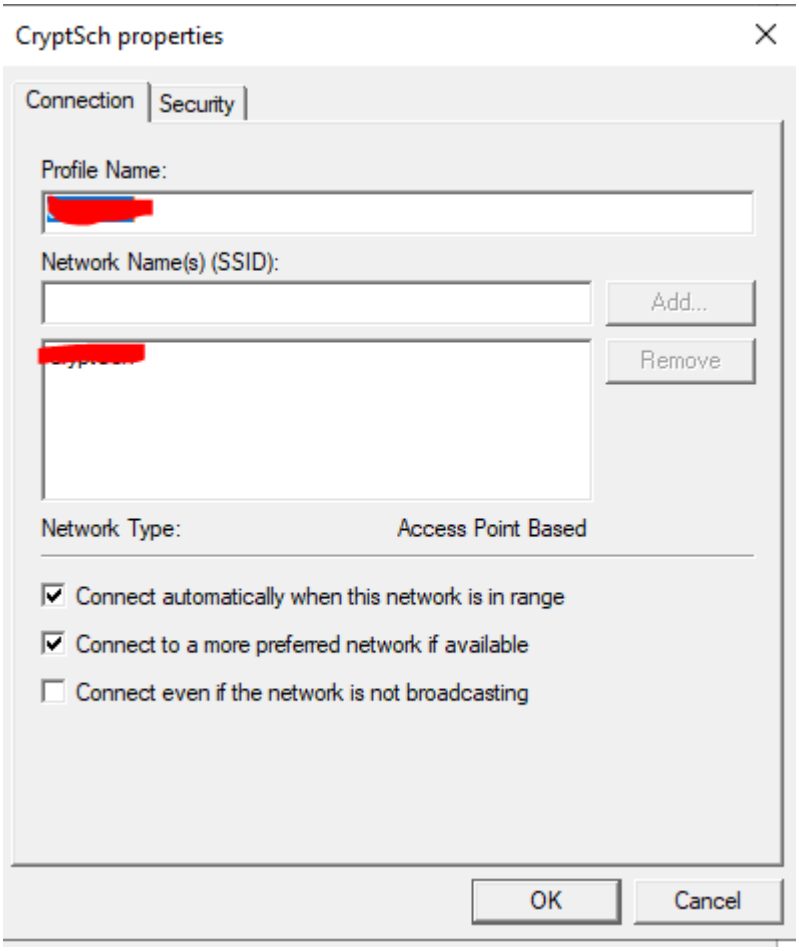
WiFi GPO

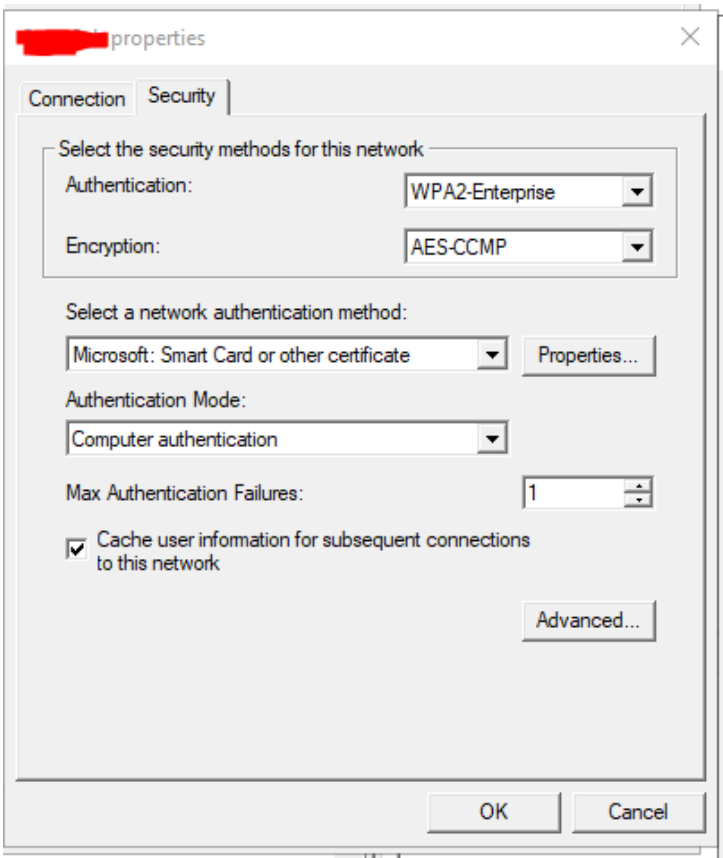


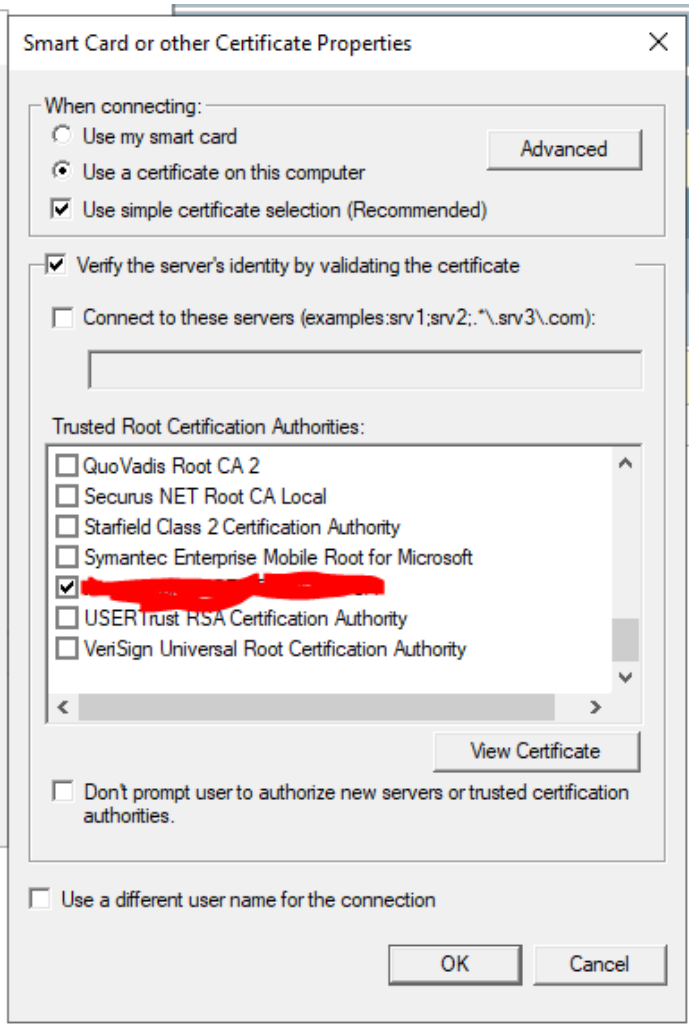
Trusted root certificate authority – the name of the internal CA server that issues the computer certs.

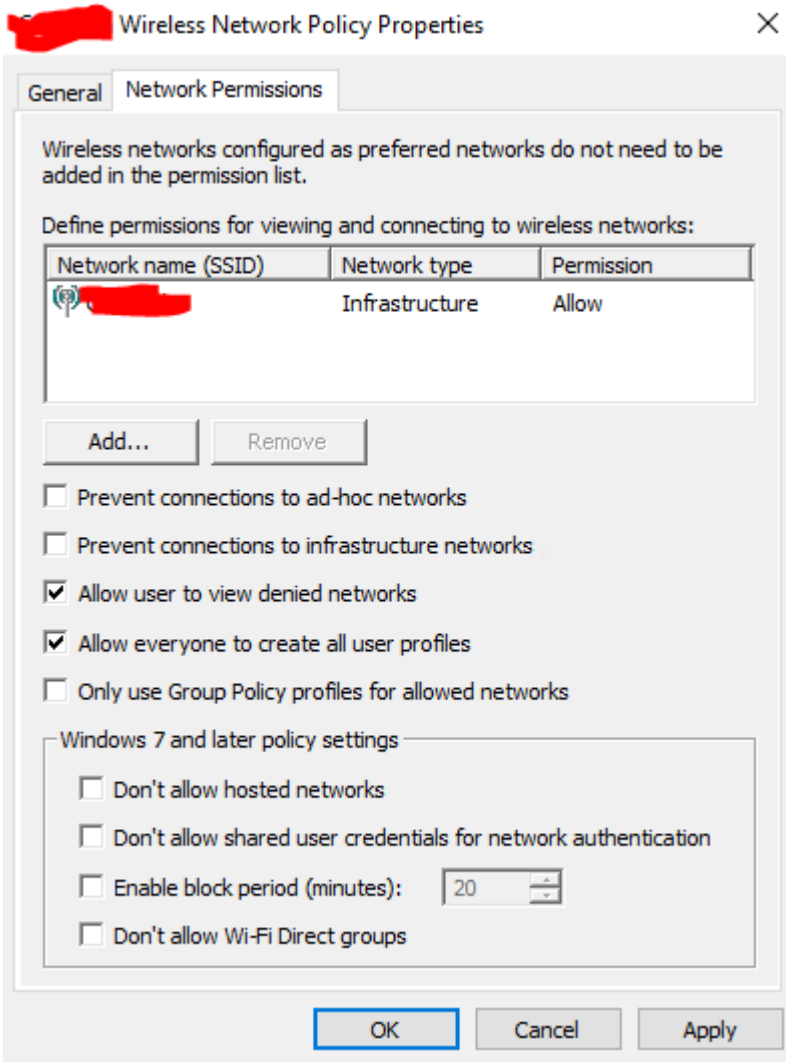


Clicking edit on the profile


CryptSch properties
Connection
Security
Profile Name:
[redacted]
Network Name(s) (SSID):
Add...
Remove
[redacted]
Network Type: Access Point Based
Connect automatically when this network is in range
Connect to a more preferred network if available
Connect even if the network is not broadcasting
OK
Cancel


[redacted] properties
Connection
Security
Select the security methods for this network
Authentication:
WPA2-Enterprise
Encryption:
AES-CCMP
Select a network authentication method:
Microsoft: Smart Card or other certificate
Properties...
Authentication Mode:
Computer authentication
Max Authentication Failures:
1
Cache user information for subsequent connections to this network
Advanced...
OK
Cancel

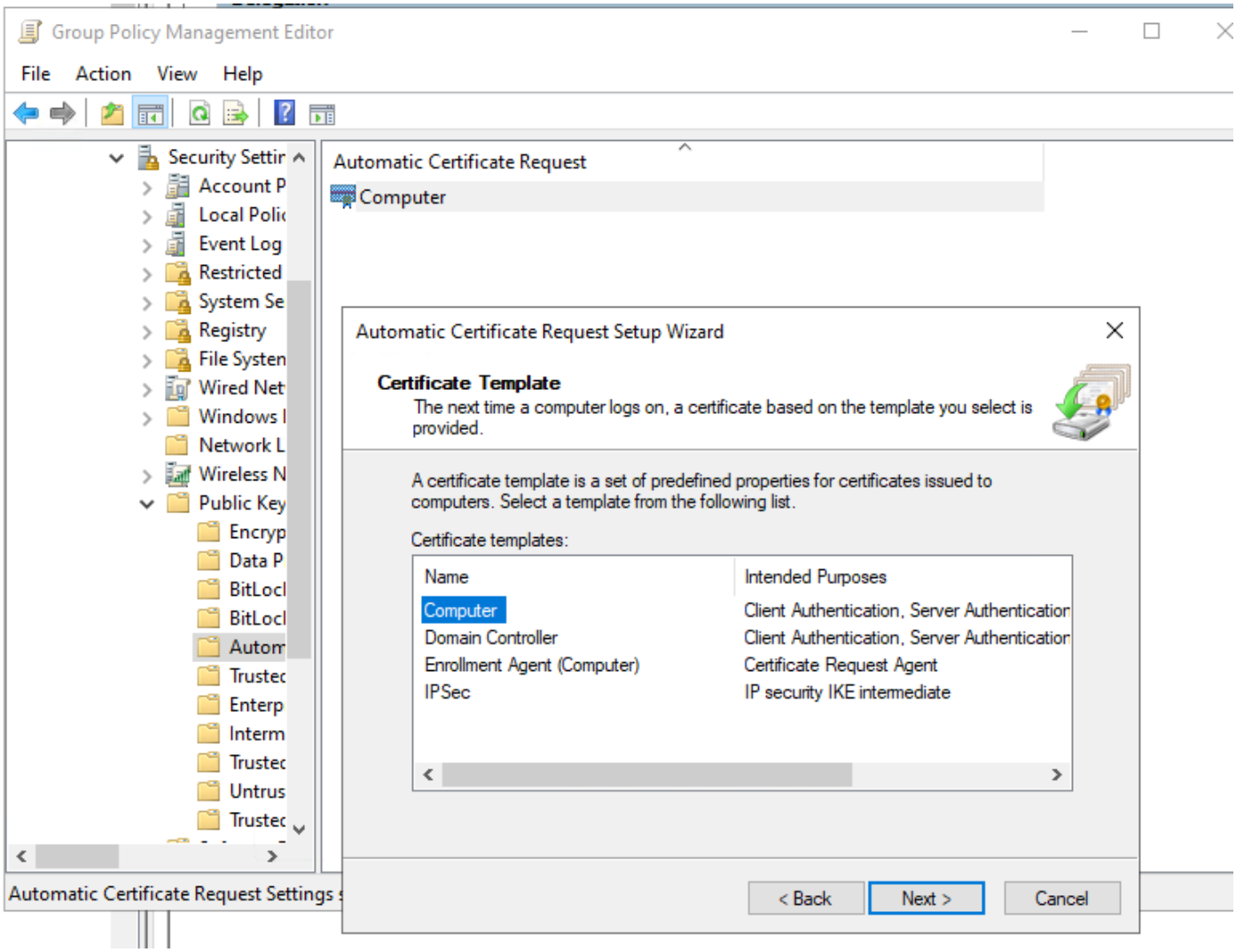

Smart Card or other Certificate Properties
When connecting:
Use my smart card
Use a certificate on this computer
Advanced
Use simple certificate selection (Recommended)
Verify the server's identity by validating the certificate
Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):
Trusted Root Certification Authorities:
QuoVadis Root CA 2
Securus NET Root CA Local
Starfield Class 2 Certification Authority
Symantec Enterprise Mobile Root for Microsoft
[redacted]
USERTrust RSA Certification Authority
VeriSign Universal Root Certification Authority
View Certificate
Don't prompt user to authorize new servers or trusted certification authorities.
Use a different user name for the connection
OK
Cancel


[redacted] Wireless Network Policy Properties
General
Network Permissions
Wireless networks configured as preferred networks do not need to be added in the permission list.
Define permissions for viewing and connecting to wireless networks:
Network name (SSID)
Network type
Permission
[redacted]
Infrastructure
Allow
Add...
Remove
Prevent connections to ad-hoc networks
Prevent connections to infrastructure networks
Allow user to view denied networks
Allow everyone to create all user profiles
Only use Group Policy profiles for allowed networks
Windows 7 and later policy settings
Don't allow hosted networks
Don't allow shared user credentials for network authentication
Enable block period (minutes):
20
Don't allow Wi-Fi Direct groups
OK
Cancel
Apply

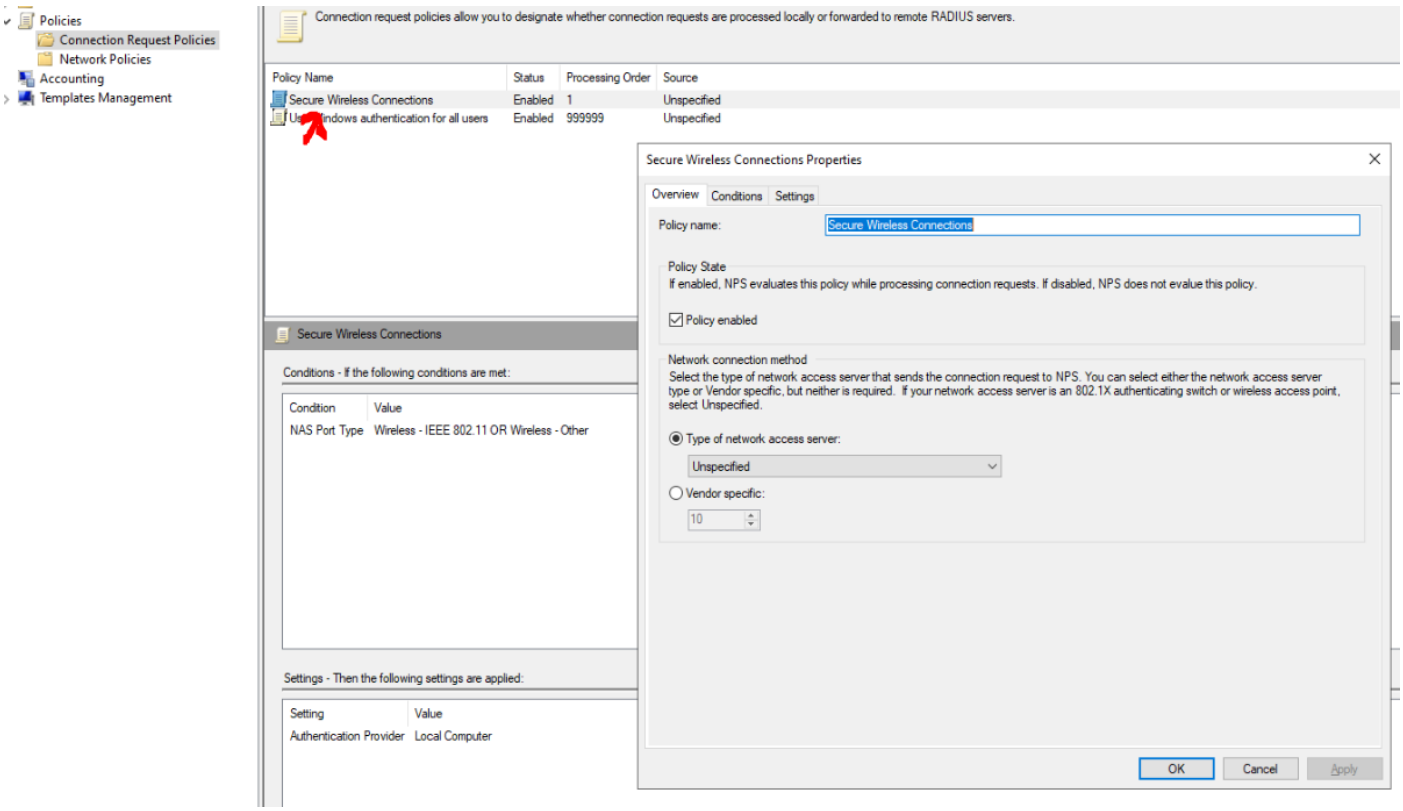
Certificate policy

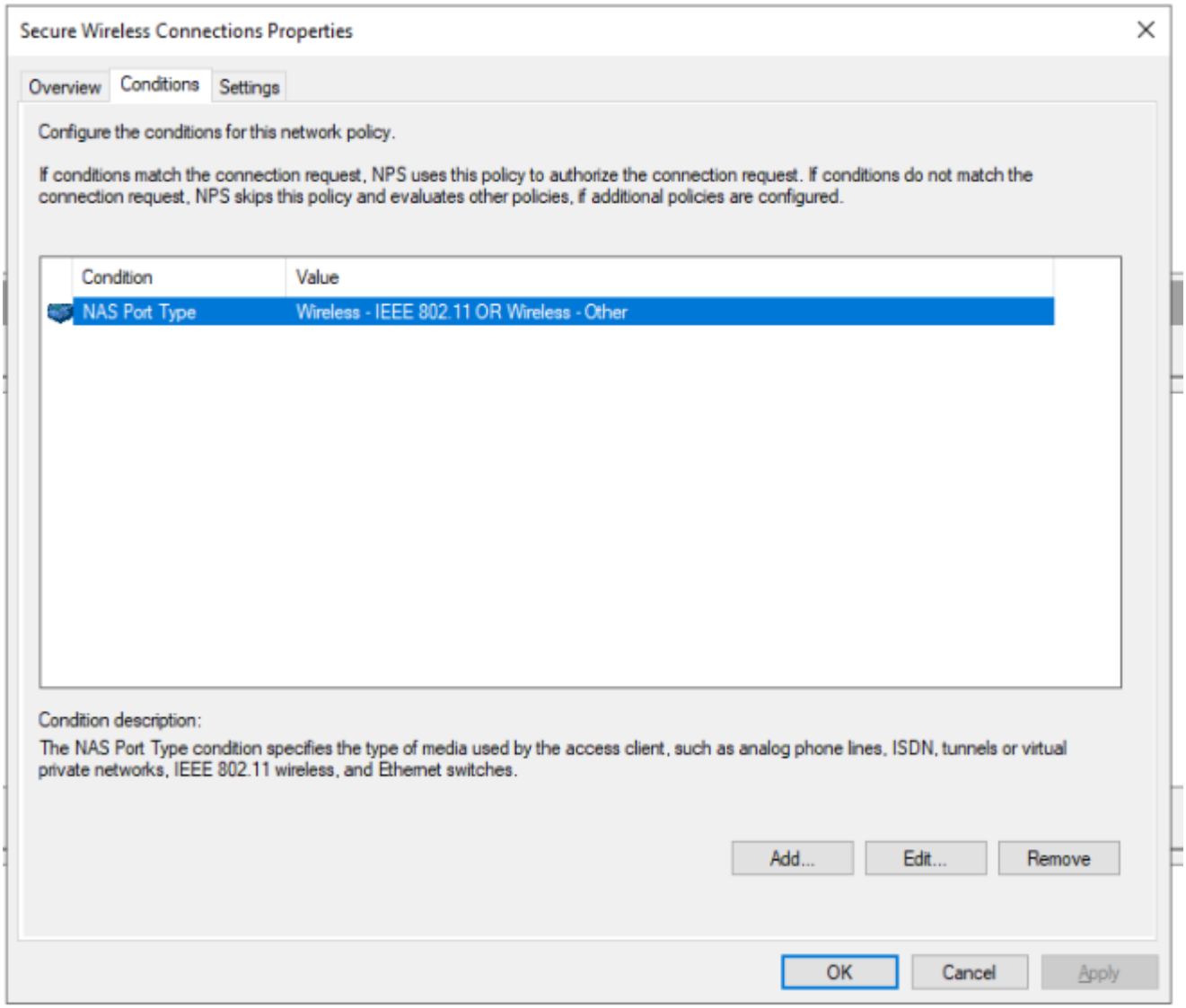
Certificate Policy
Data collected on: 16/12/2024 11:34:15 show all

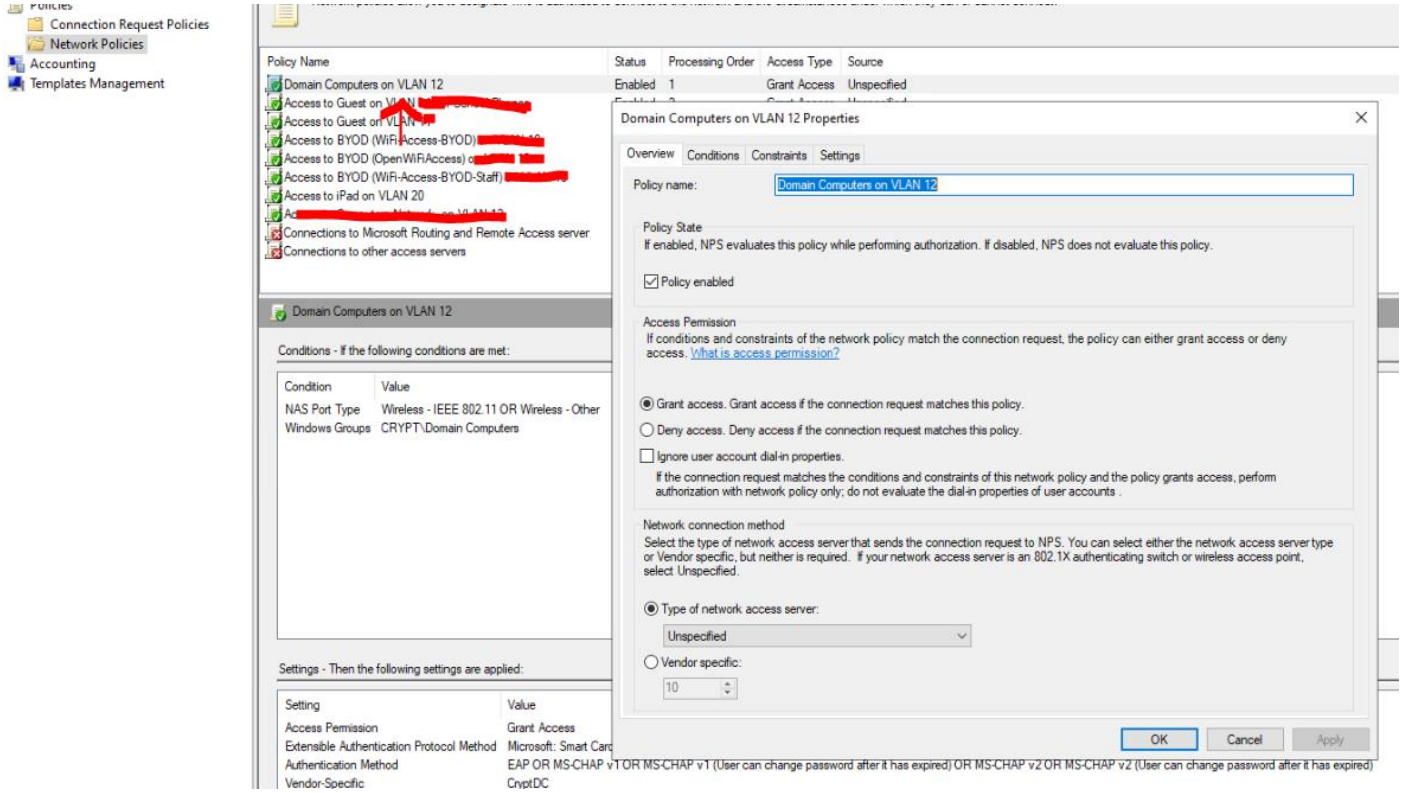
General hide
Details show
Links show
Security Filtering show
Delegation show
Computer Configuration (Enabled) hide
Policies hide
Windows Settings hide
Security Settings hide
Public Key Policies/Encrypting File System show
Public Key Policies/Automatic Certificate Request Settings hide
Automatic Certificate Request
Computer
For additional information about individual settings, launch the Local Group Policy Object Editor.
User Configuration (Enabled) hide
No settings defined.

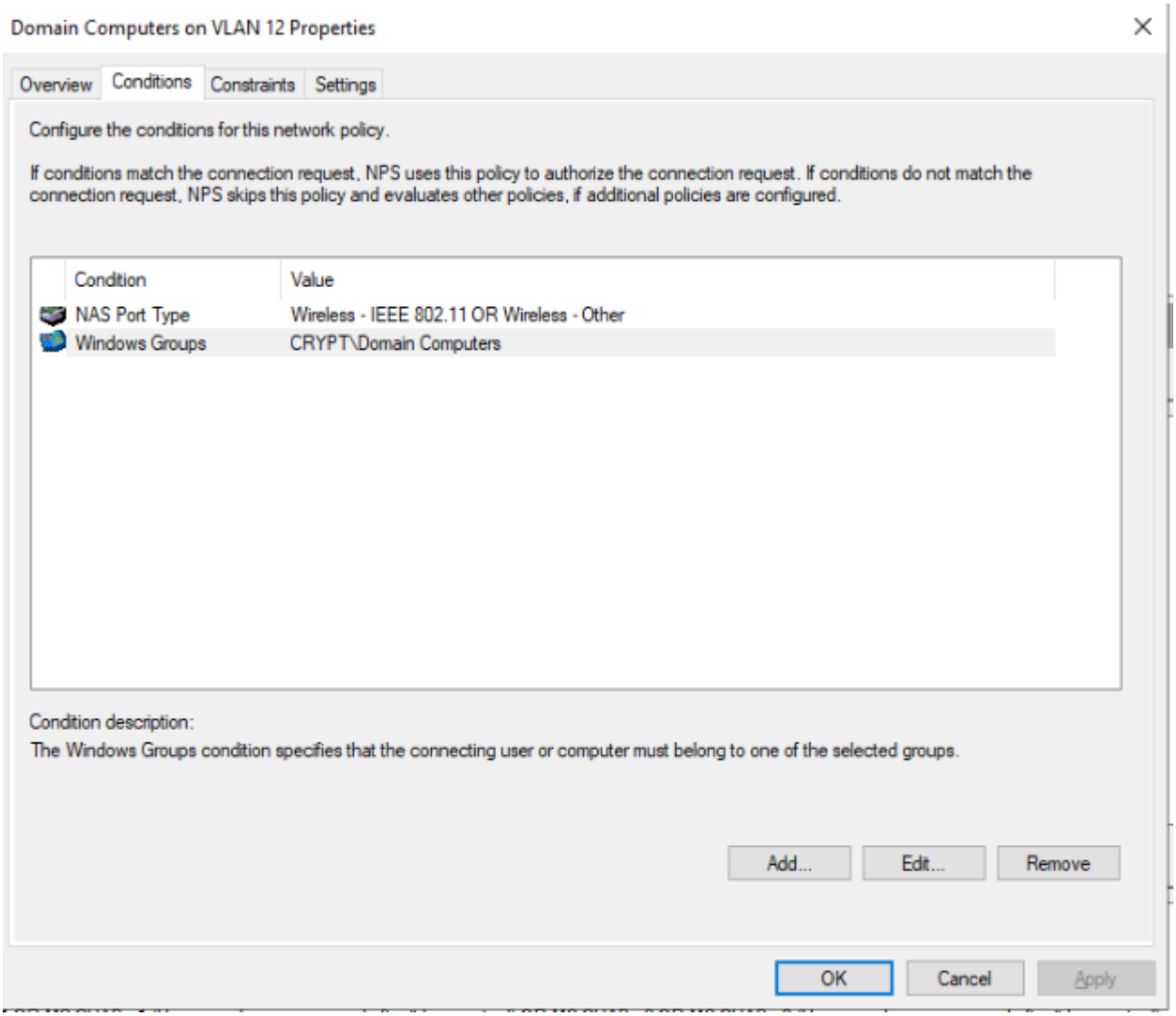


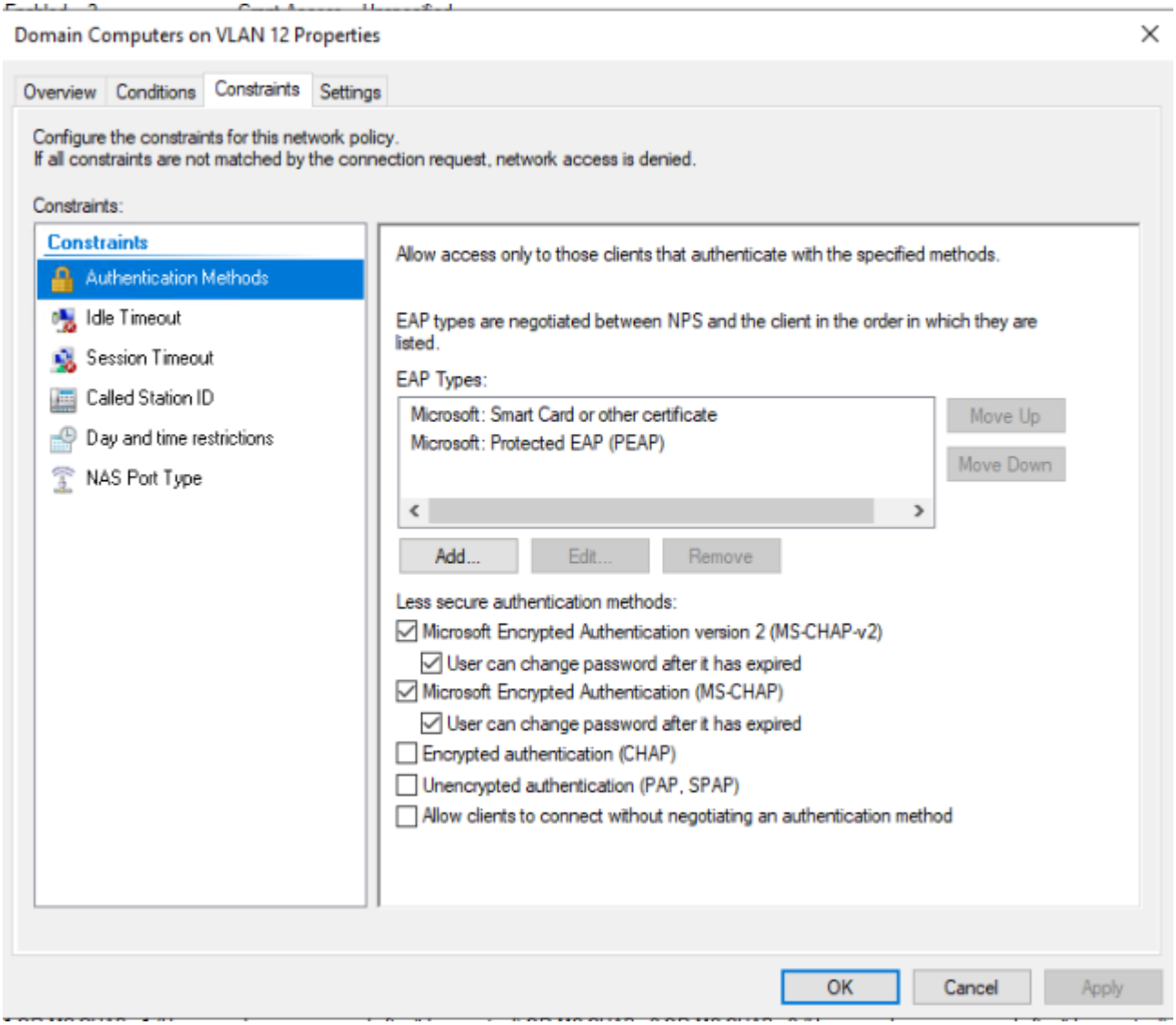
NPS

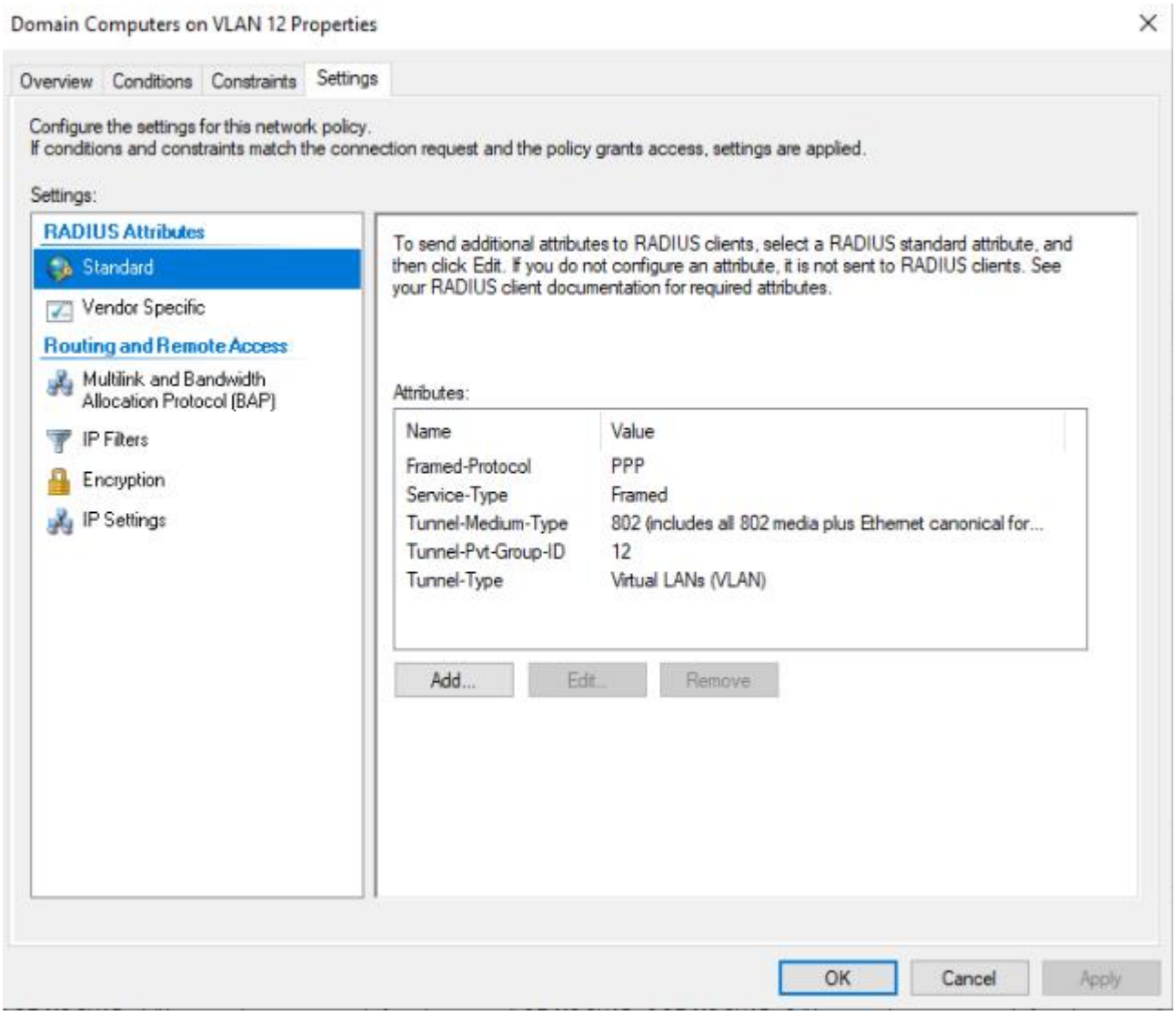

Policies
Connection Request Policies
Network Policies
Accounting
Templates Management
Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.
Policy Name
Status
Processing Order
Source
Secure Wireless Connections
Enabled
1
Unspecified
Enabled
999999
Unspecified
Secure Wireless Connections Properties
Overview
Conditions
Settings
Policy name:
Secure Wireless Connections
Policy State
If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy.
Policy enabled
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:
Unspecified
Vendor specific:
10
Secure Wireless Connections
Conditions - If the following conditions are met:
Condition
Value
NAS Port Type
Wireless - IEEE 802.11 OR Wireless - Other
Settings - Then the following settings are applied:
Setting
Value
Authentication Provider
Local Computer
OK
Cancel
Apply

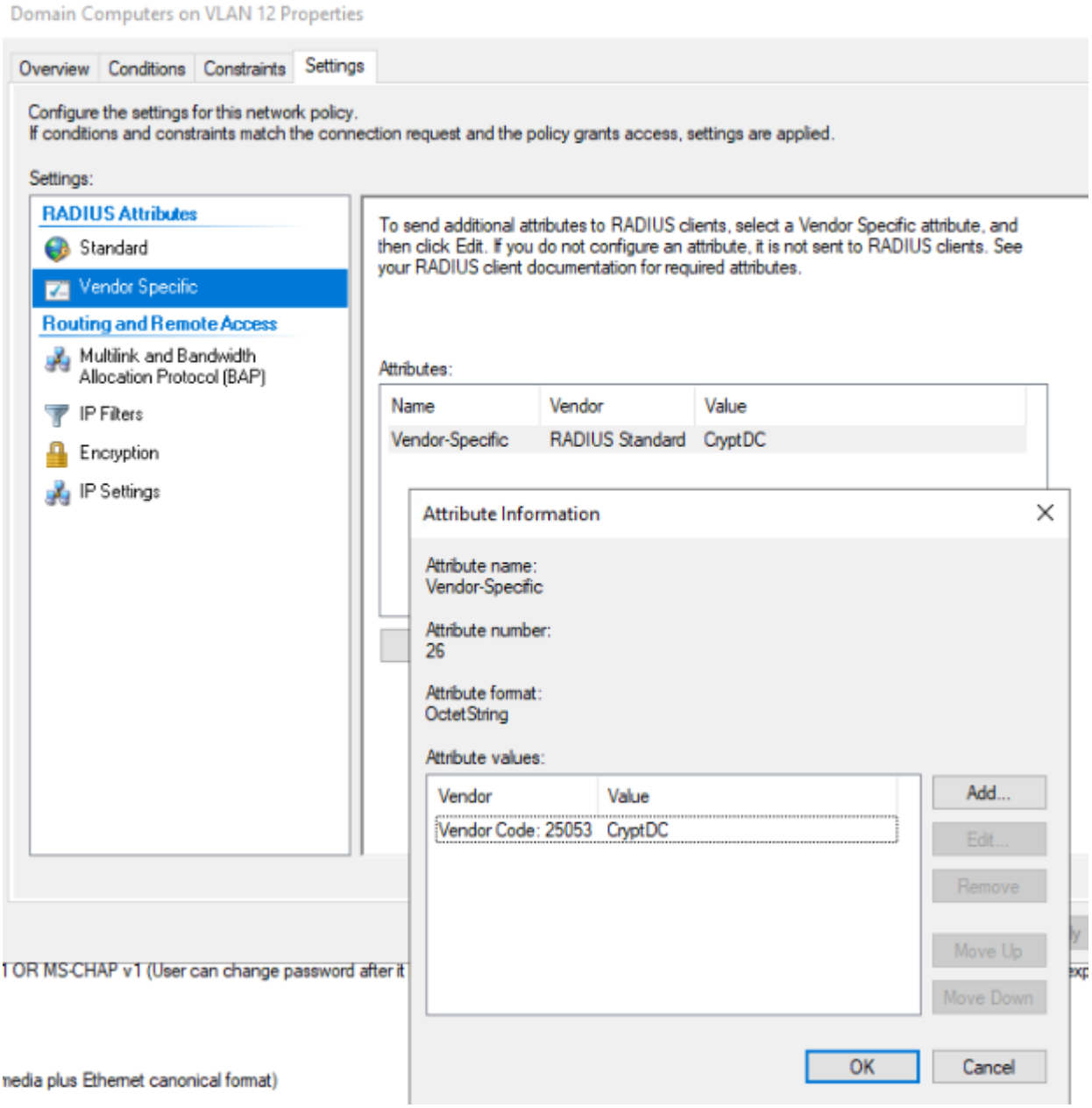

Secure Wireless Connections Properties
Overview
Conditions
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
NAS Port Type
Wireless - IEEE 802.11 OR Wireless - Other
Condition description:
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.
Add...
Edit...
Remove
OK
Cancel
Apply


Connection Request Policies
Network Policies
Accounting
Templates Management
Policy Name
Status
Processing Order
Access Type
Source
Domain Computers on VLAN 12
Enabled
1
Grant Access
Unspecified
Access to Guest on VLAN
Access to Guest on VLAN
Access to BYOD (WiFi-Access-BYOD)
Access to BYOD (OpenWiFiAccess)
Access to BYOD (WiFi-Access-BYOD-Staff)
Access to iPad on VLAN 20
Connections to Microsoft Routing and Remote Access server
Connections to other access servers
Domain Computers on VLAN 12
Conditions - If the following conditions are met:
Condition
Value
NAS Port Type
Wireless - IEEE 802.11 OR Wireless - Other
Windows Groups
CRYPT\Domain Computers
Settings - Then the following settings are applied:
Setting
Value
Access Permission
Grant Access
Extensible Authentication Protocol Method
Microsoft: Smart Card
Authentication Method
EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 OR MS-CHAP v2 (User can change password after it has expired)
Vendor-Specific
CryptDC
Domain Computers on VLAN 12 Properties
Overview
Conditions
Constraints
Settings
Policy name:
Domain Computers on VLAN 12
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:
Unspecified
Vendor specific:
10
OK
Cancel
Apply


Domain Computers on VLAN 12 Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.
Condition
Value
NAS Port Type
Wireless - IEEE 802.11 OR Wireless - Other
Windows Groups
CRYPT\Domain Computers
Condition description:
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.
Add...
Edit...
Remove
OK
Cancel
Apply


Domain Computers on VLAN 12 Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Constraints
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only to those clients that authenticate with the specified methods.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Microsoft: Smart Card or other certificate
Microsoft: Protected EAP (PEAP)
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method
OK
Cancel
Apply


Domain Computers on VLAN 12 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
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
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID
12
Tunnel-Type
Virtual LANs (VLAN)
Add...
Edit...
Remove
OK
Cancel
Apply



This is for Ruckus to pass the group info across