The Queen’s College
IT Open Morning

Microsoft Network Policy Server + VLANs/ACLs

What does it do?

- Network Policy Server
    - Authenticates devices based on
        - 802.1x Credentials
            - Username/Password
            - Certificate
        - MAC Address
    - Places the client in the correct VLAN + send other RADIUS Attributes

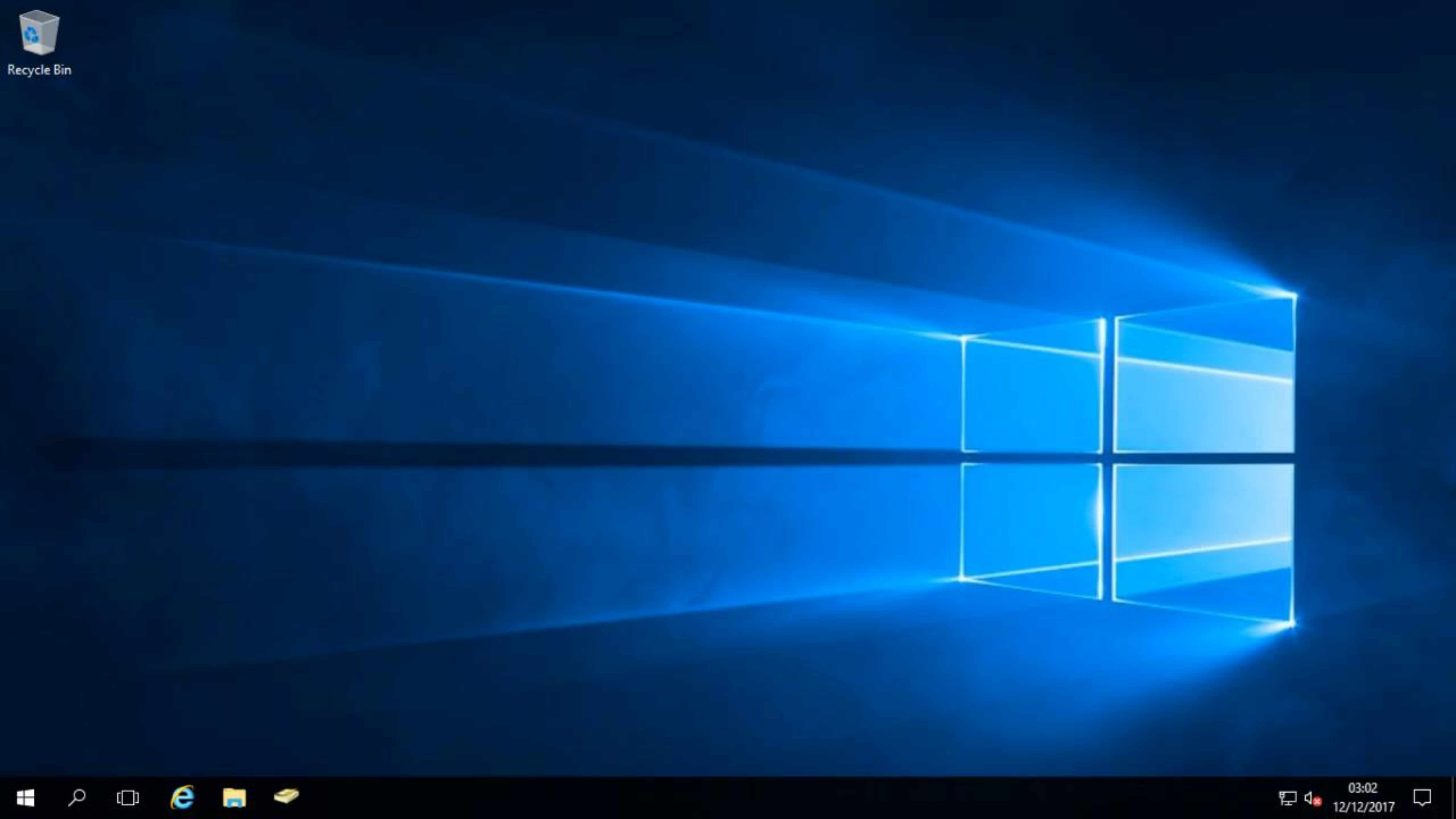
Alternatives…

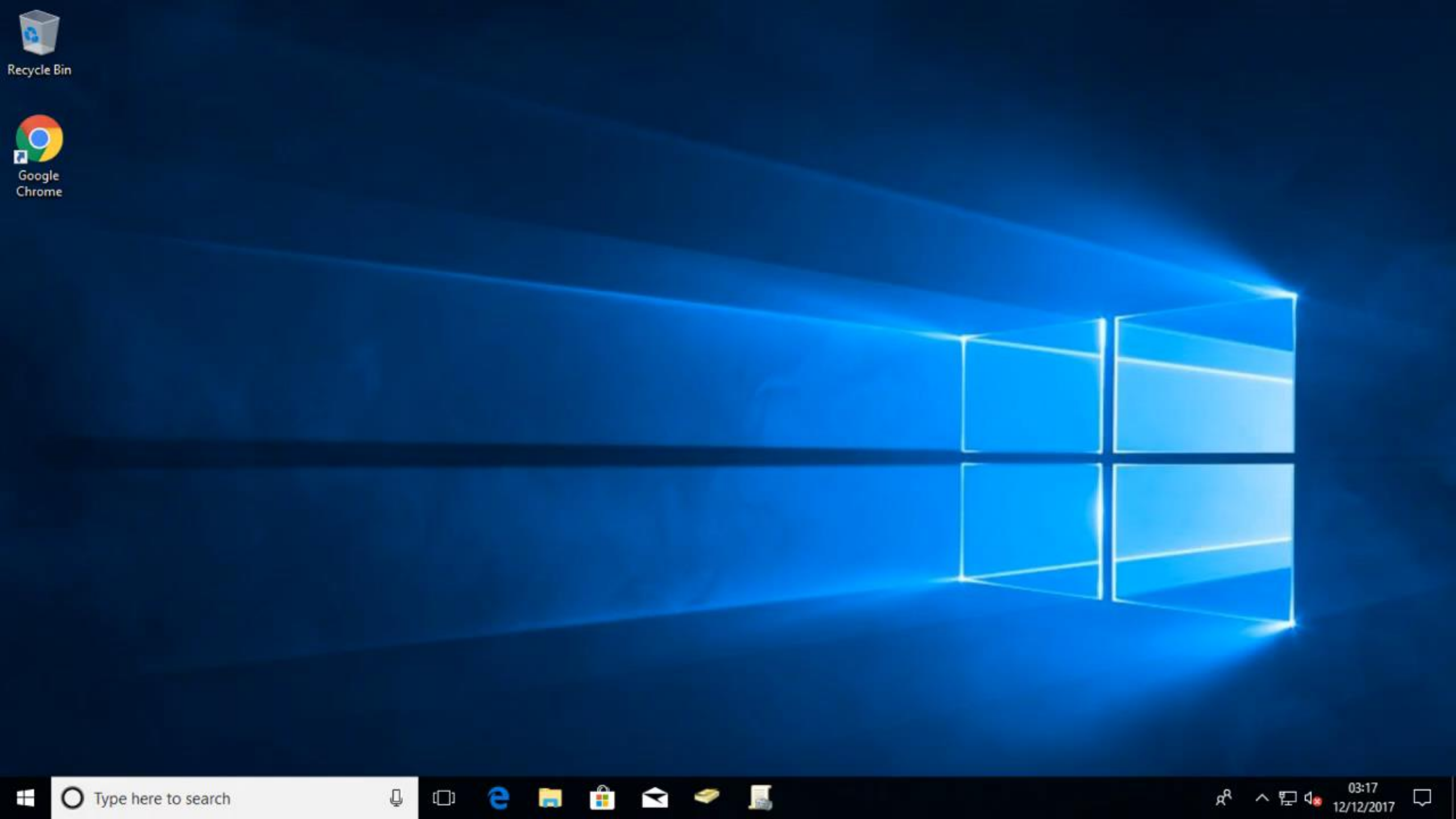
- Bradford Network Sentry
- Aruba Clear Pass
- PacketFence

Network Switch Config

```
radius-server host 172.16.0.2 key <key!!>
radius-server dead-time 1
radius-server timeout 3
radius-server retransmit 2
aaa authentication login privilege-mode
aaa authentication ssh login radius local
aaa authentication ssh enable radius local
aaa port-access mac-based addr-format no-delimiter
```

```
aaa port-access gvrp-vlans
aaa authentication port-access eap-radius
aaa port-access authenticator 1-8
aaa port-access authenticator 1-8 quiet-period 30
aaa port-access authenticator 1-8 tx-period 2
aaa port-access authenticator 1-8 supplicant-timeout 2
aaa port-access authenticator 1-8 server-timeout 10
aaa port-access authenticator 1-8 max-requests 3
aaa port-access authenticator 1-8 reauth-period 600
aaa port-access authenticator 1-8 auth-vid 1
aaa port-access authenticator 1-8 client-limit 3
aaa port-access authenticator active
aaa port-access mac-based 1-8
aaa port-access mac-based 1-8 logoff-period 862400
aaa port-access mac-based 1-8 quiet-period 30
aaa port-access mac-based 1-8 server-timeout 10
aaa port-access mac-based 1-8 reauth-period 600
aaa port-access mac-based 1-8 unauth-vid 97
aaa port-access mac-based 1-8 addr-limit 3
aaa port-access 1-8 controlled-direction in
```


Recycle Bin
03:02
12/12/2017


Recycle Bin
Google Chrome
Type here to search
03:17
12/12/2017

certsrv - [Certification Authority (KC-DC01.kings.ox.ac.uk)\kings-KC-DC01-CA\Certificate Templates]

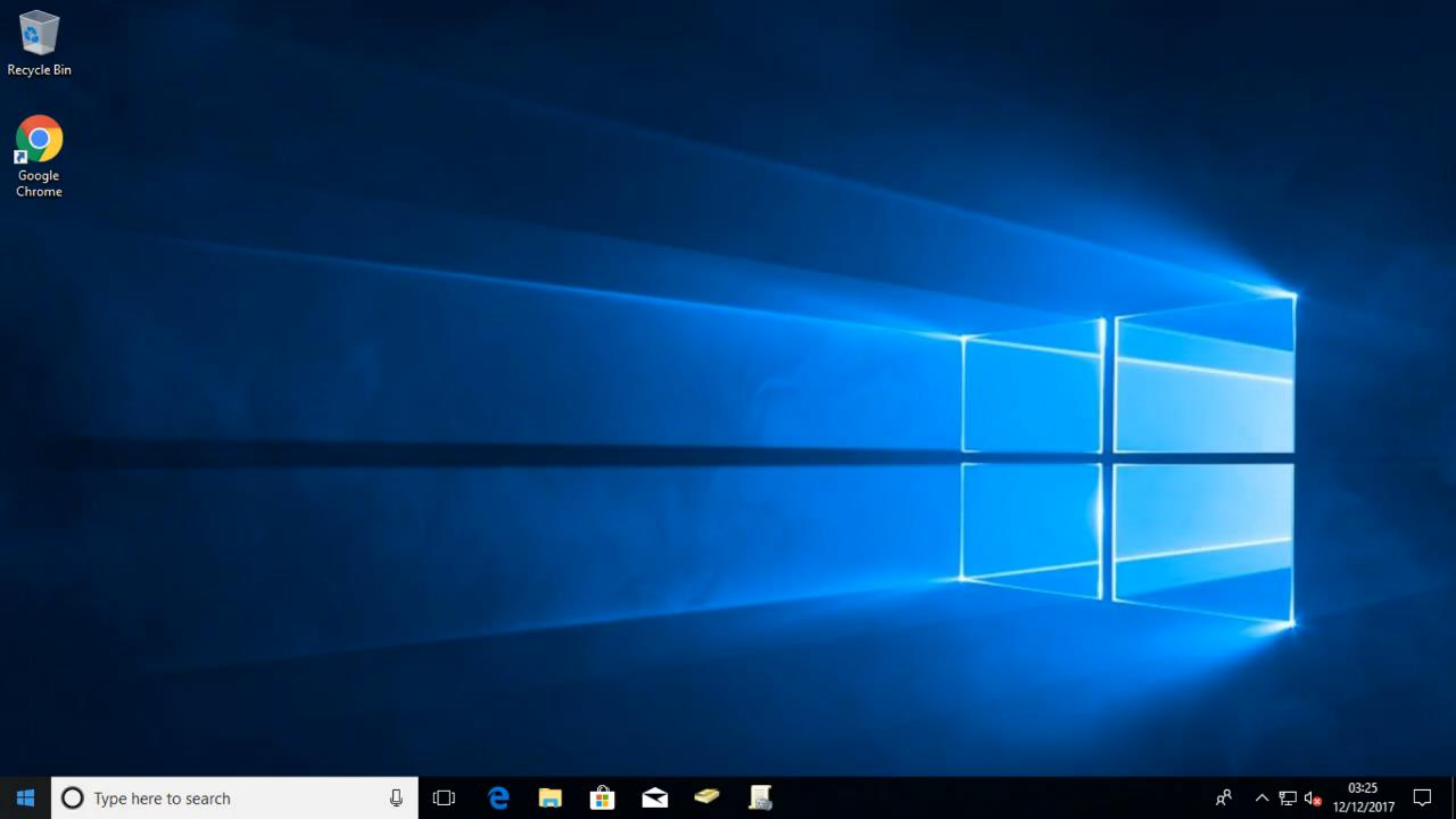
File Action View Help

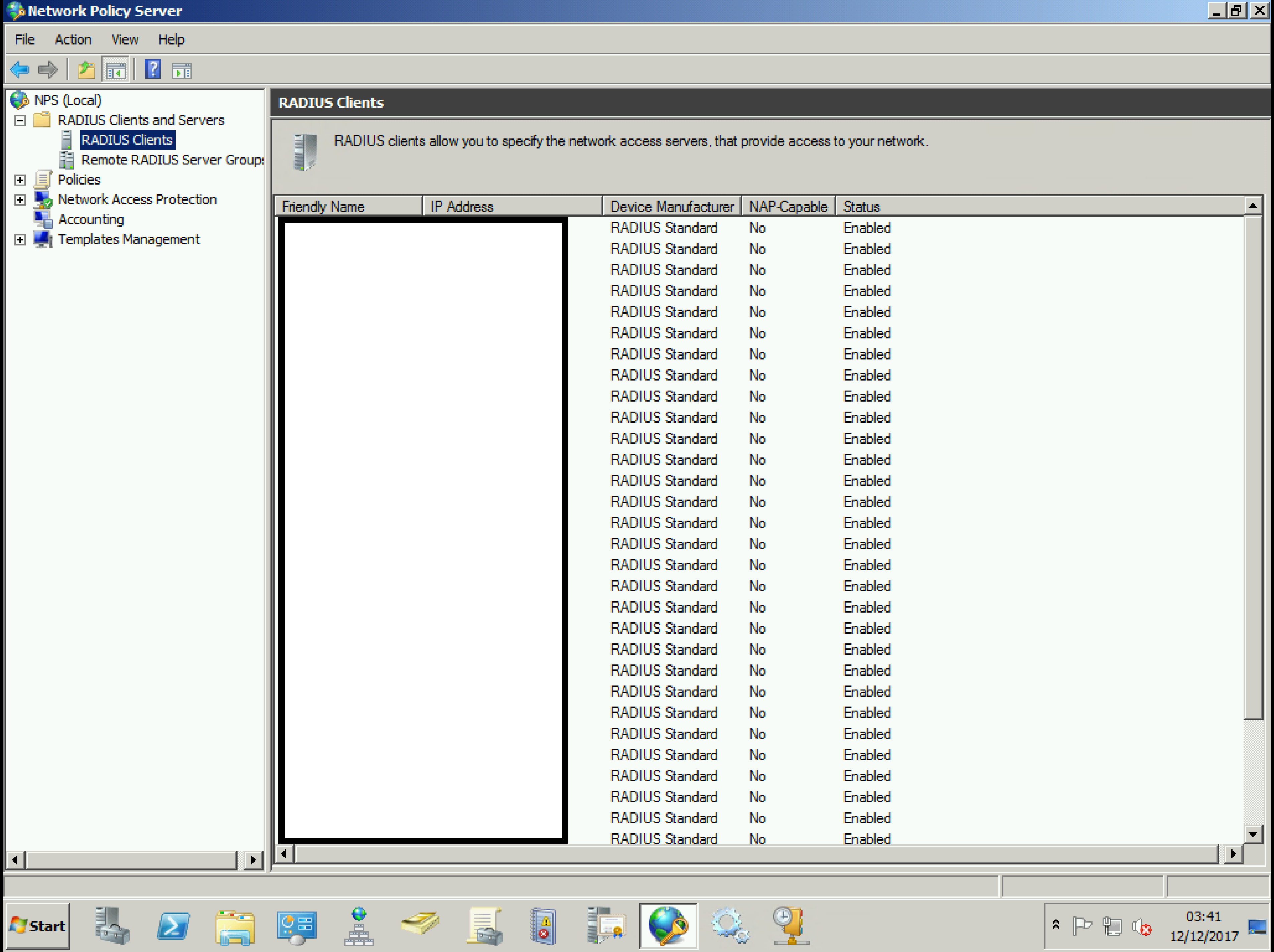
- Certification Authority (KC-DC01.
  - kings-KC-DC01-CA
    - Revoked Certificates
    - Issued Certificates
    - Pending Requests
    - Failed Requests
    - Certificate Templates

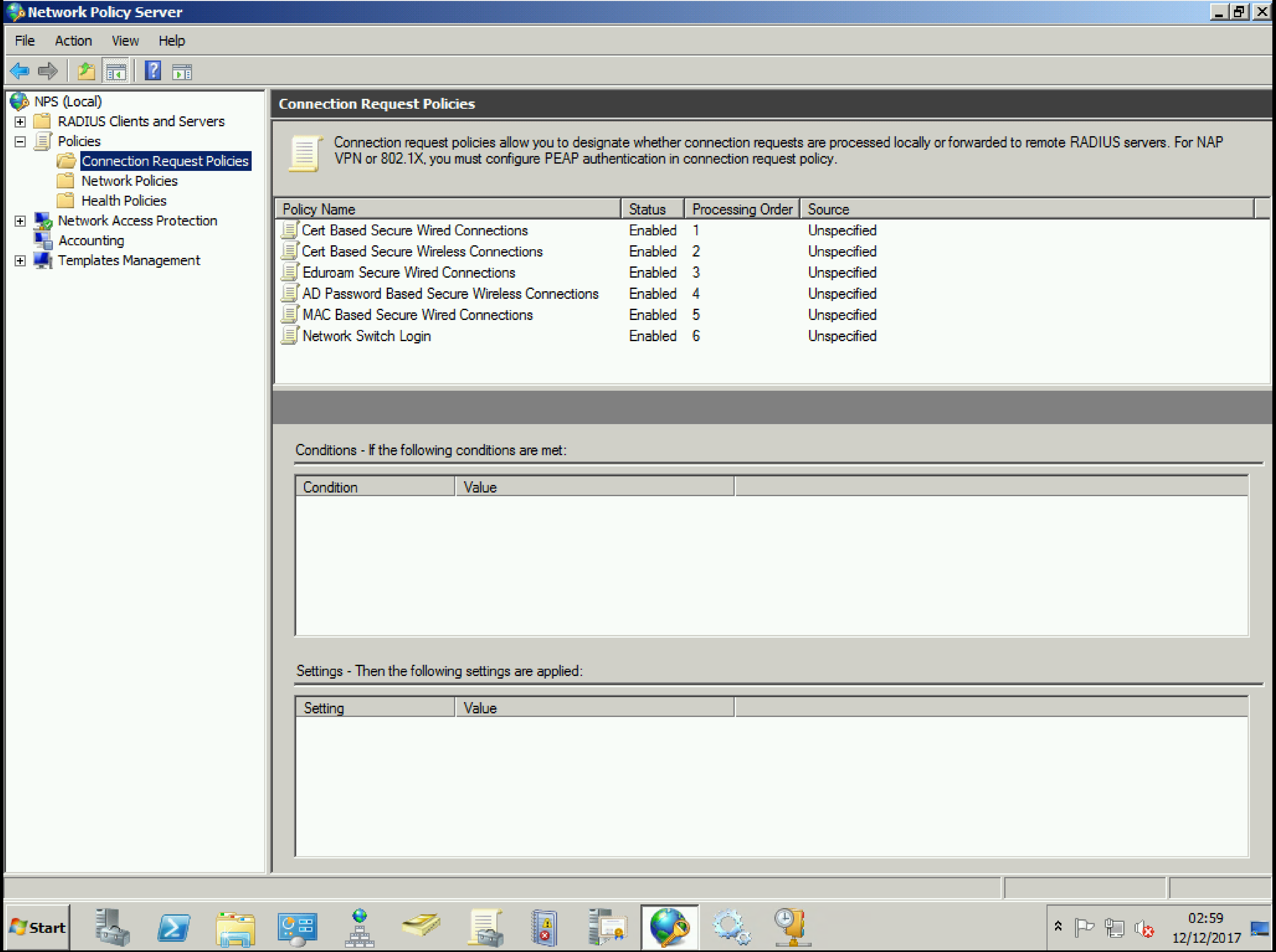
Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...

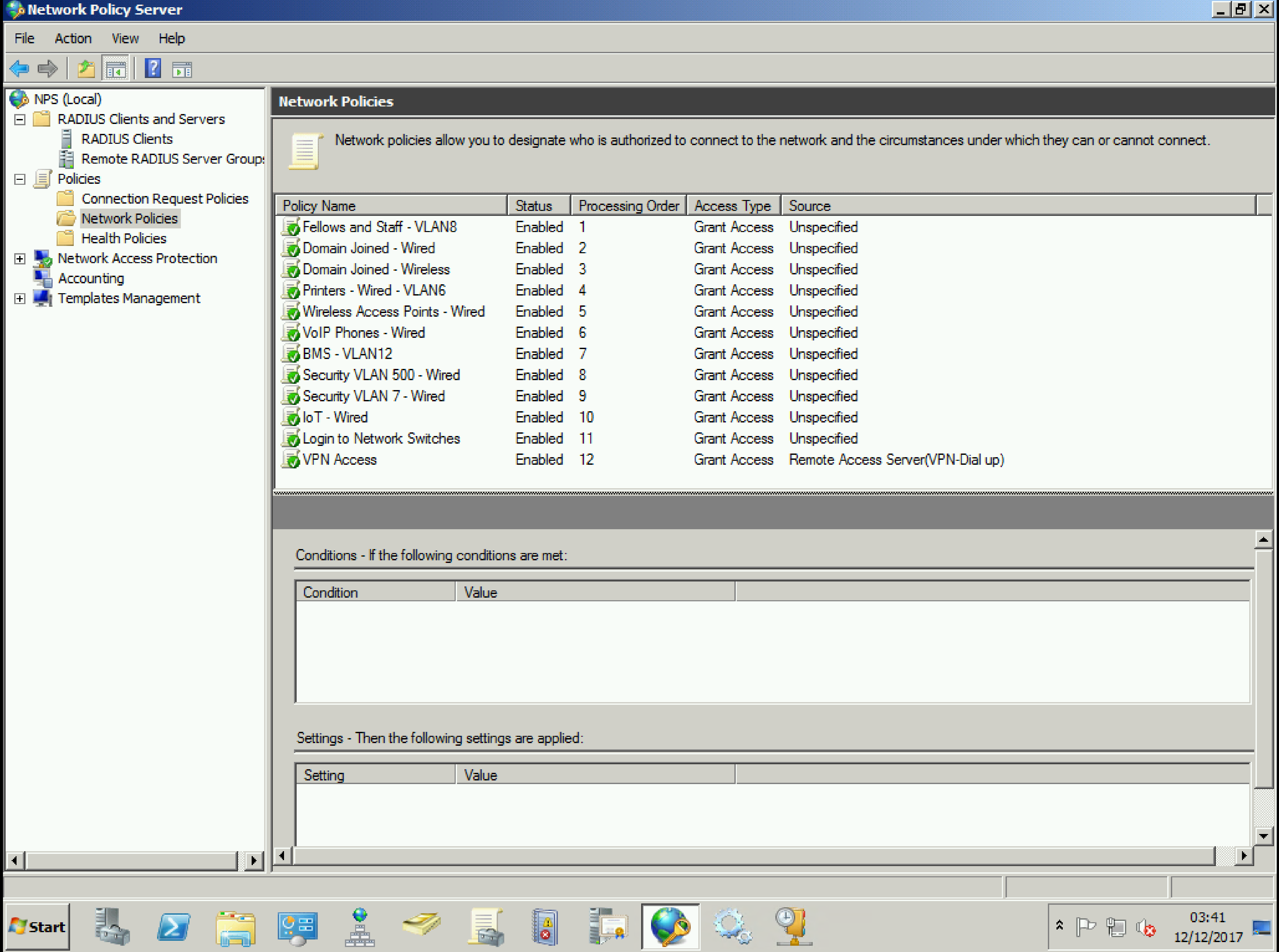
Type here to search

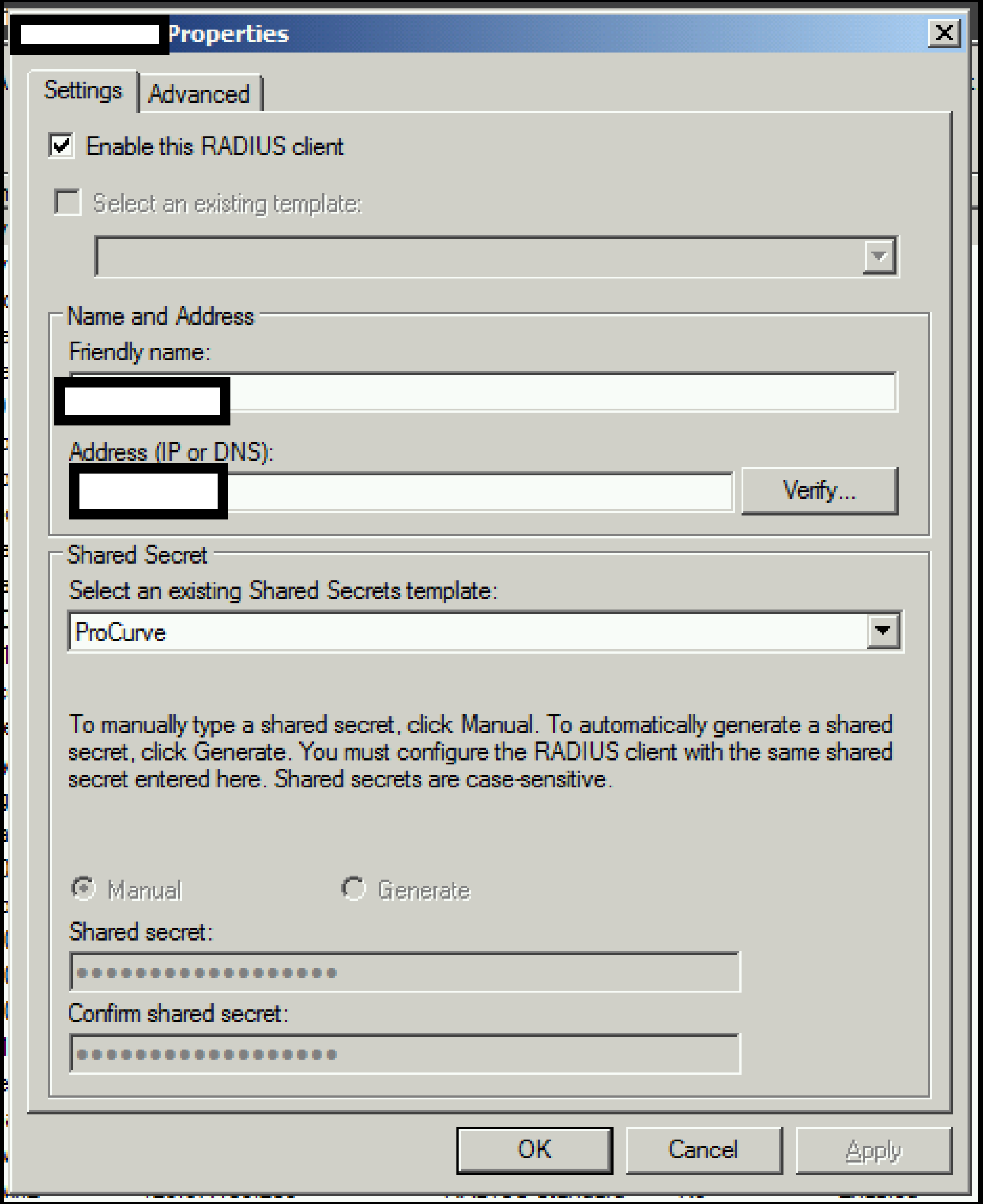
03:20
12/12/2017

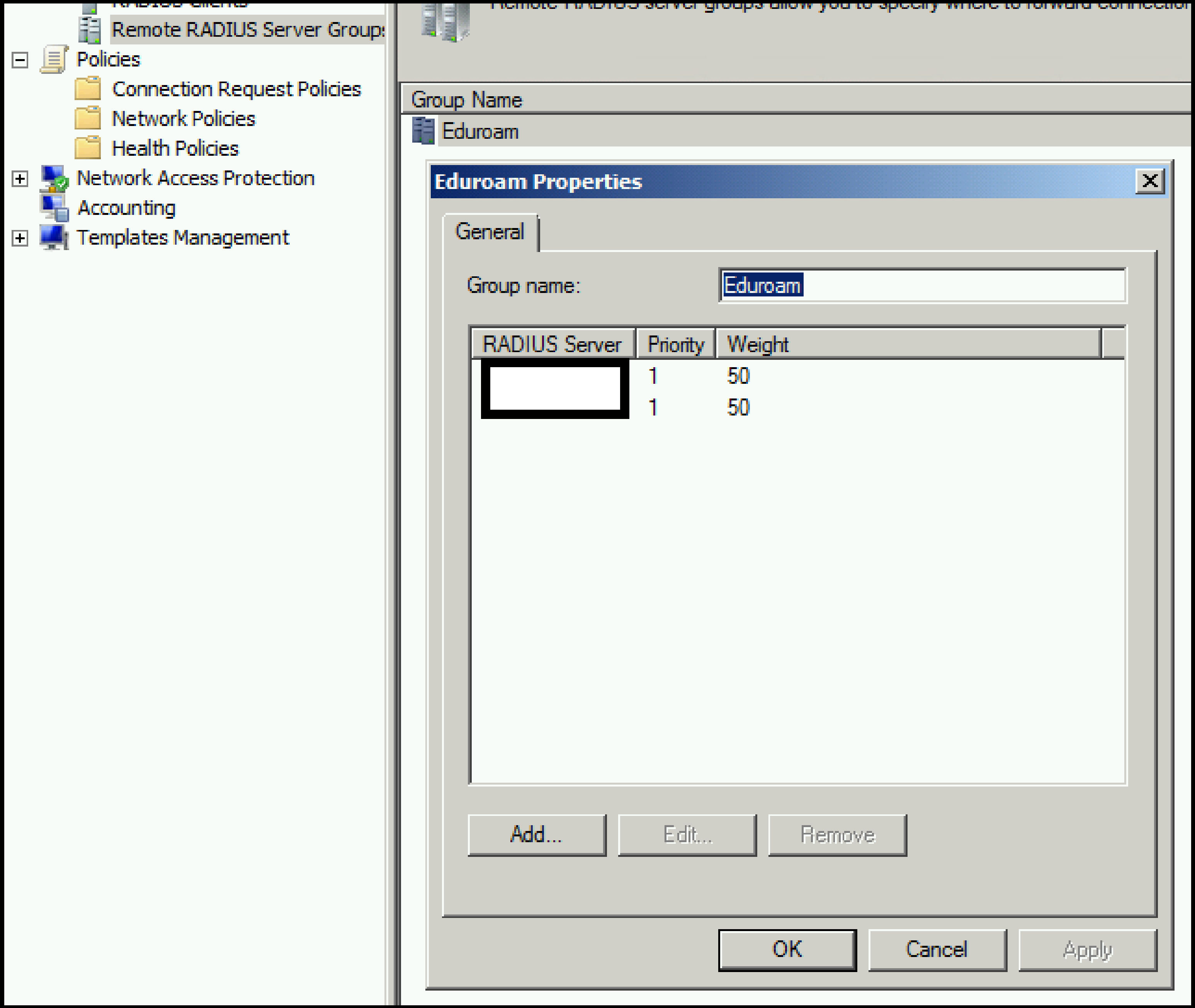

Recycle Bin
Google Chrome
Type here to search
03:25
12/12/2017

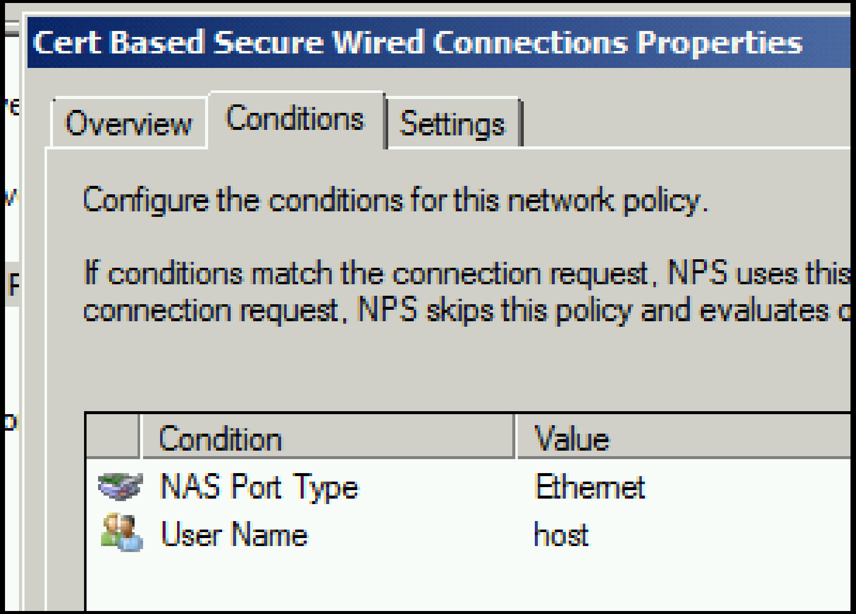

Network Policy Server
File
Action
View
Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Network Access Protection
Accounting
Templates Management
RADIUS Clients
RADIUS clients allow you to specify the network access servers, that provide access to your network.
Friendly Name
IP Address
Device Manufacturer
NAP-Capable
Status
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
RADIUS Standard No Enabled
Start
03:41
12/12/2017

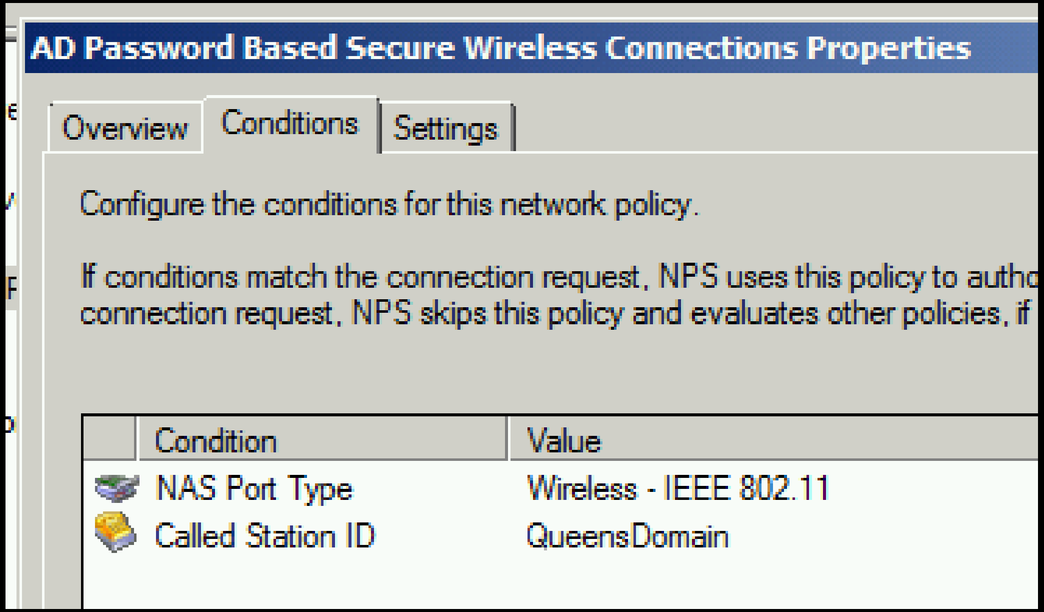

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Templates Management
Connection Request Policies
Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.
Policy Name
Status
Processing Order
Source
Cert Based Secure Wired Connections Enabled 1 Unspecified
Cert Based Secure Wireless Connections Enabled 2 Unspecified
Eduroam Secure Wired Connections Enabled 3 Unspecified
AD Password Based Secure Wireless Connections Enabled 4 Unspecified
MAC Based Secure Wired Connections Enabled 5 Unspecified
Network Switch Login Enabled 6 Unspecified
Conditions - If the following conditions are met:
Condition
Value
Settings - Then the following settings are applied:
Setting
Value
Start
02:59
12/12/2017

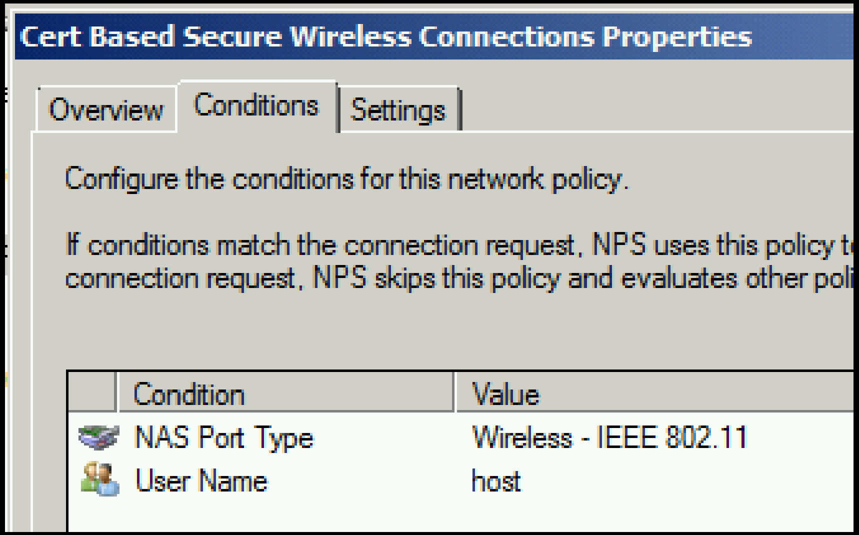

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Group:
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Templates Management
Network Policies
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
Policy Name Status Processing Order Access Type Source
Fellows and Staff - VLAN8 Enabled 1 Grant Access Unspecified
Domain Joined - Wired Enabled 2 Grant Access Unspecified
Domain Joined - Wireless Enabled 3 Grant Access Unspecified
Printers - Wired - VLAN6 Enabled 4 Grant Access Unspecified
Wireless Access Points - Wired Enabled 5 Grant Access Unspecified
VoIP Phones - Wired Enabled 6 Grant Access Unspecified
BMS - VLAN12 Enabled 7 Grant Access Unspecified
Security VLAN 500 - Wired Enabled 8 Grant Access Unspecified
Security VLAN 7 - Wired Enabled 9 Grant Access Unspecified
IoT - Wired Enabled 10 Grant Access Unspecified
Login to Network Switches Enabled 11 Grant Access Unspecified
VPN Access Enabled 12 Grant Access Remote Access Server(VPN-Dial up)
Conditions - If the following conditions are met:
Condition Value
Settings - Then the following settings are applied:
Setting Value
Start
03:41
12/12/2017

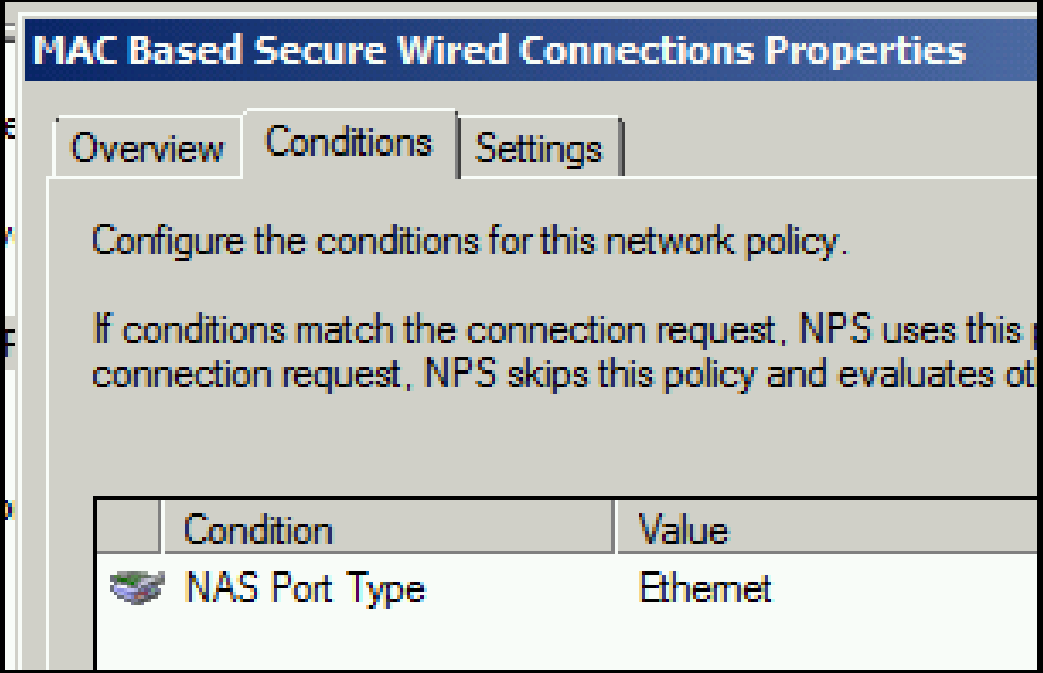

[redacted] Properties
Settings
Advanced
Enable this RADIUS client
Select an existing template:
Name and Address
Friendly name:
[redacted]
Address (IP or DNS):
[redacted]
Verify...
Shared Secret
Select an existing Shared Secrets template:
ProCurve
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
Manual
Generate
Shared secret:
Confirm shared secret:
OK
Cancel
Apply

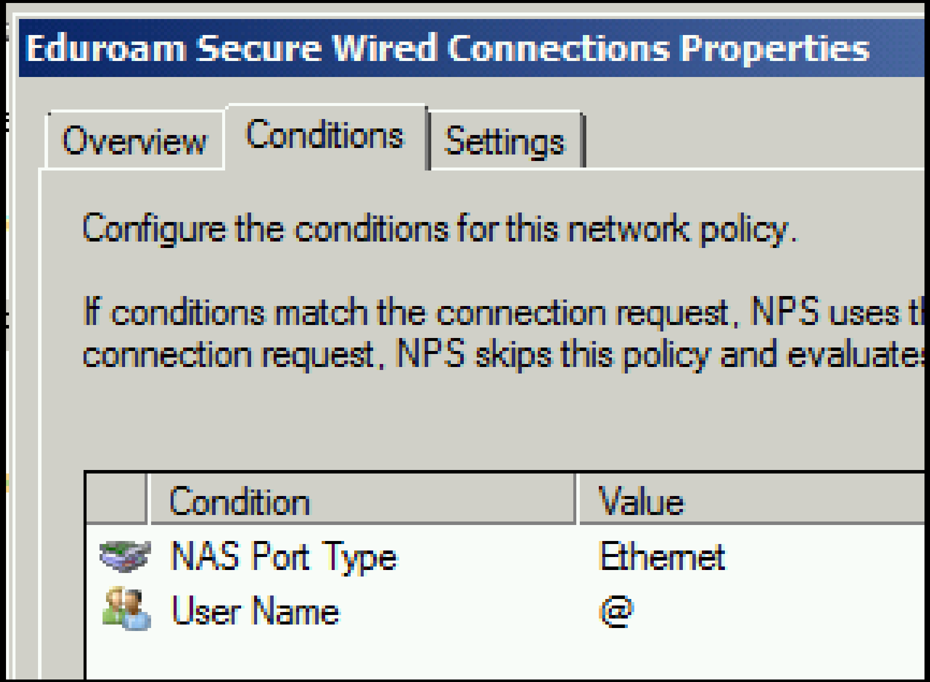

Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Network Access Protection
Accounting
Templates Management
Group Name
Eduroam
Eduroam Properties
General
Group name:
Eduroam
RADIUS Server
Priority
Weight
1
50
1
50
Add...
Edit...
Remove
OK
Cancel
Apply

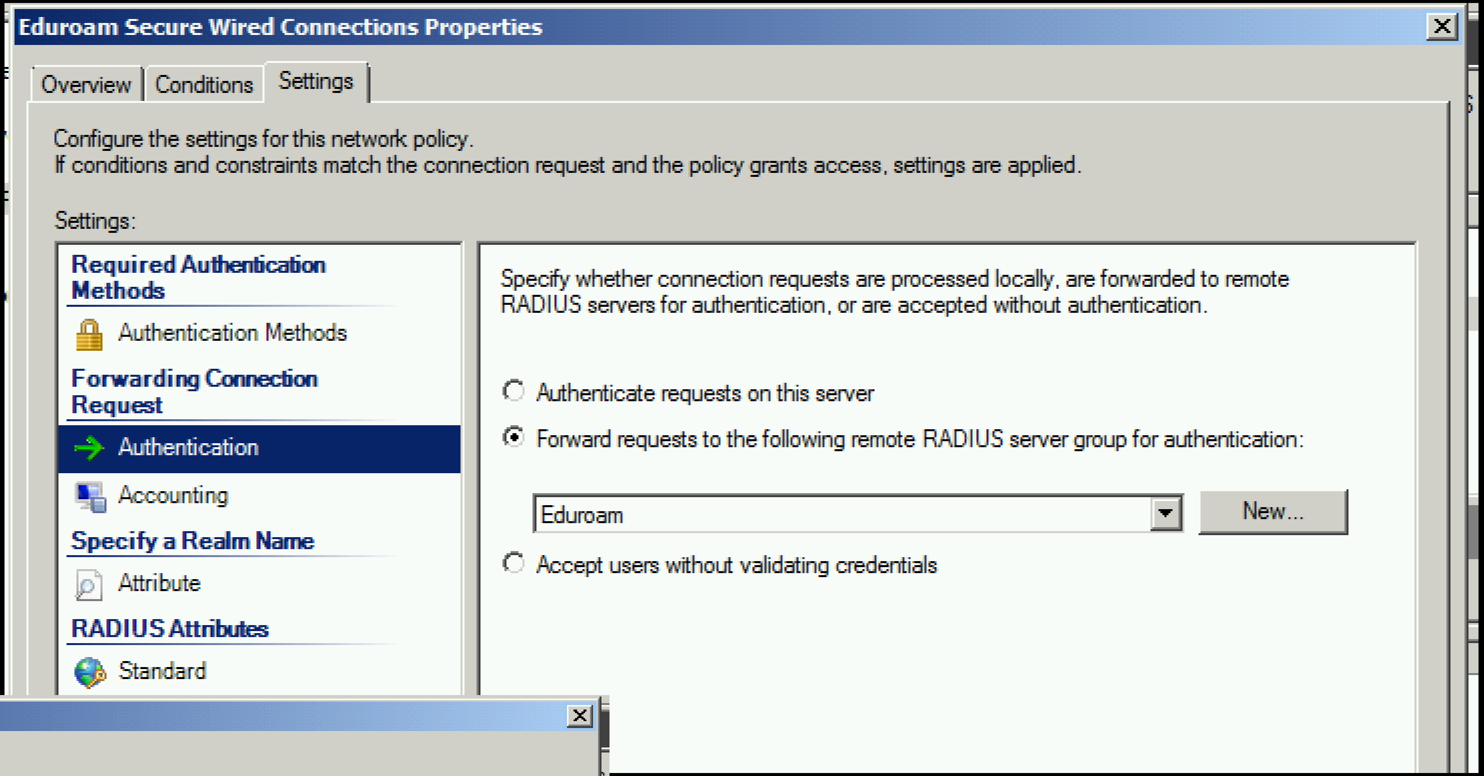

Cert Based Secure Wired Connections Properties
Overview
Conditions
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this
connection request, NPS skips this policy and evaluates
Condition
Value
NAS Port Type
Ethernet
User Name
host

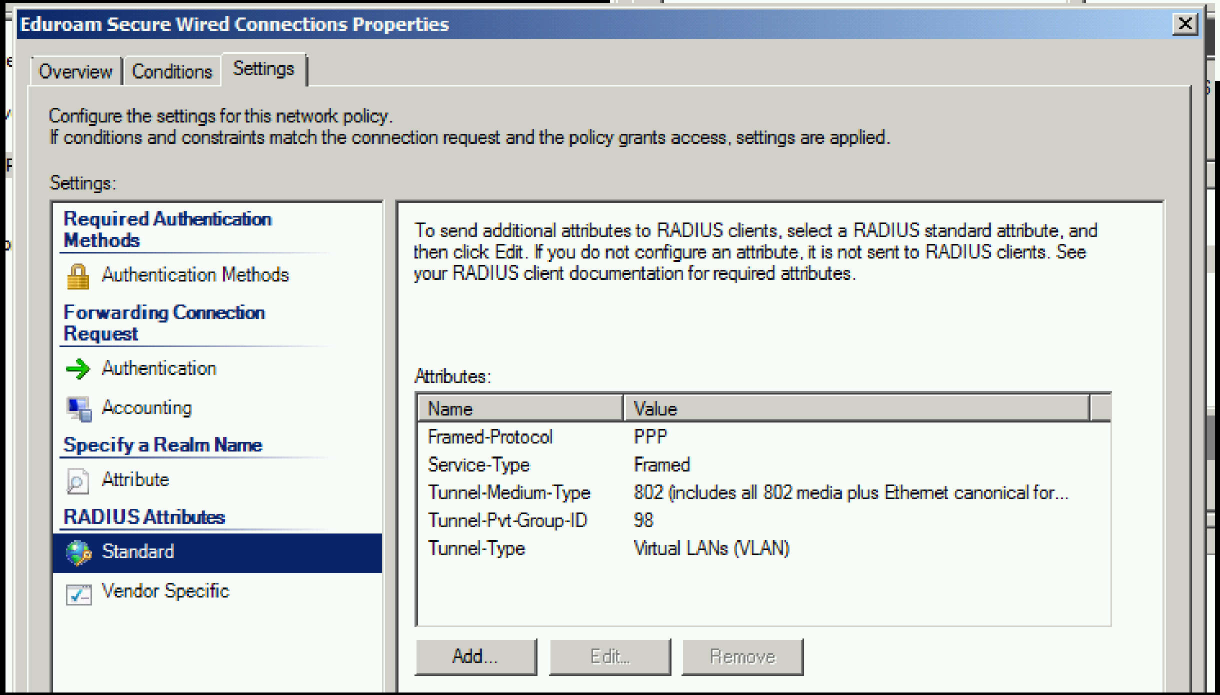

AD Password Based Secure Wireless Connections Properties
Overview
Conditions
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to auth
connection request, NPS skips this policy and evaluates other policies, if
Condition
Value
NAS Port Type
Wireless - IEEE 802.11
Called Station ID
QueensDomain

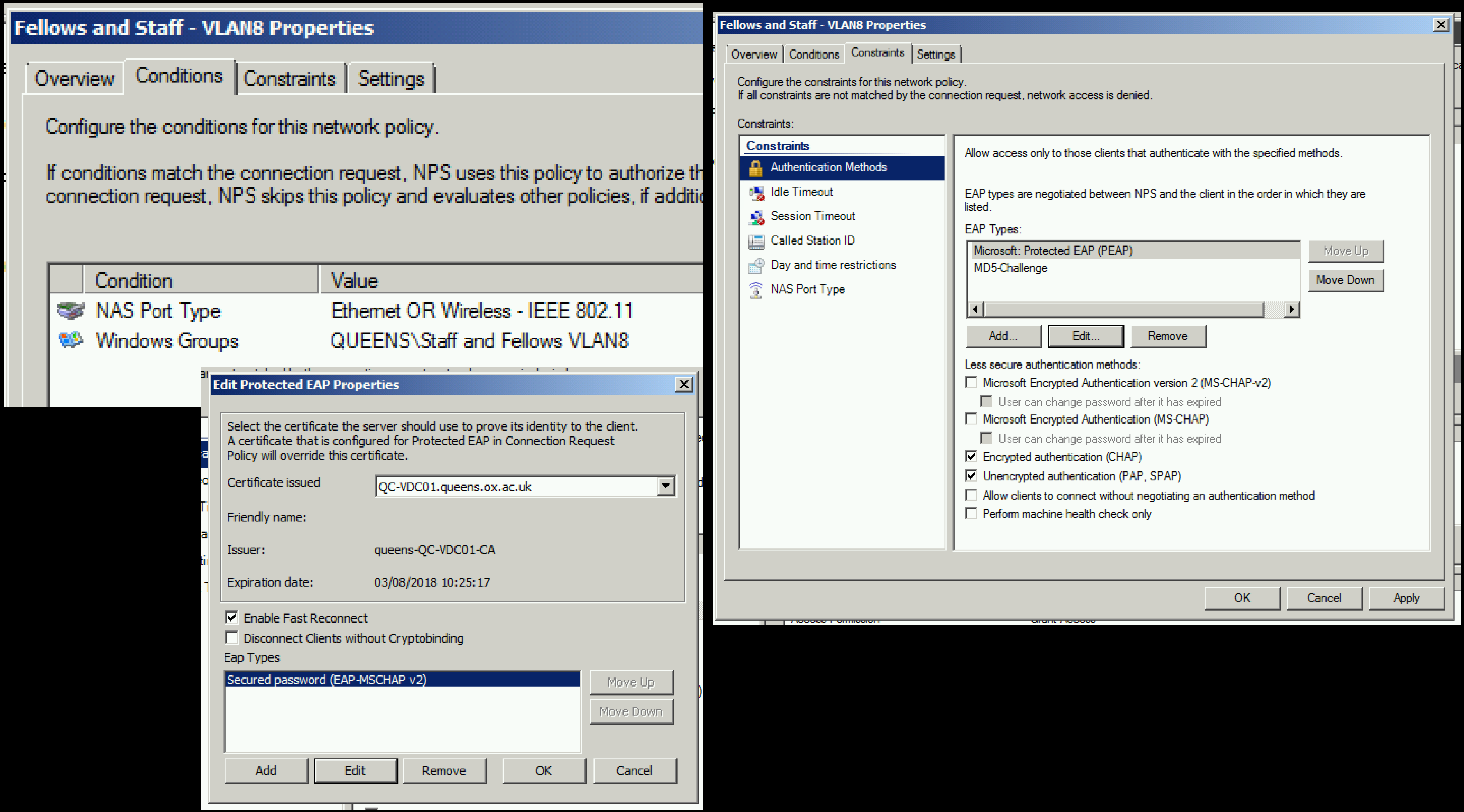

Cert Based Secure Wireless Connections Properties
Overview
Conditions
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy
connection request, NPS skips this policy and evaluates other pol
Condition
Value
NAS Port Type
Wireless - IEEE 802.11
User Name
host

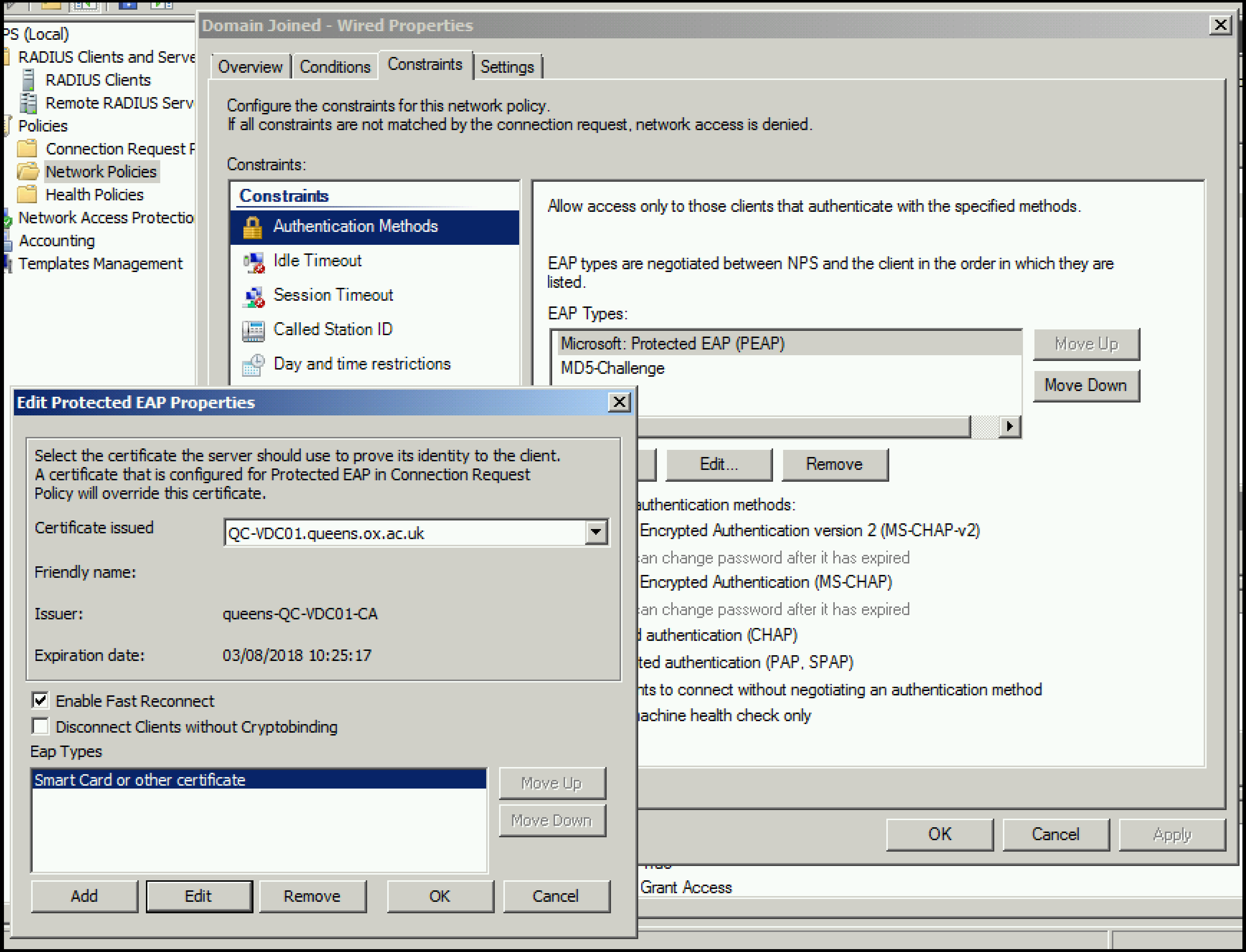

MAC Based Secure Wired Connections Properties
Overview
Conditions
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this
connection request, NPS skips this policy and evaluates
Condition
Value
NAS Port Type
Ethernet


Eduroam Secure Wired Connections Properties
Overview
Conditions
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses t
connection request, NPS skips this policy and evaluate
Condition
Value
NAS Port Type
Ethernet
User Name
@

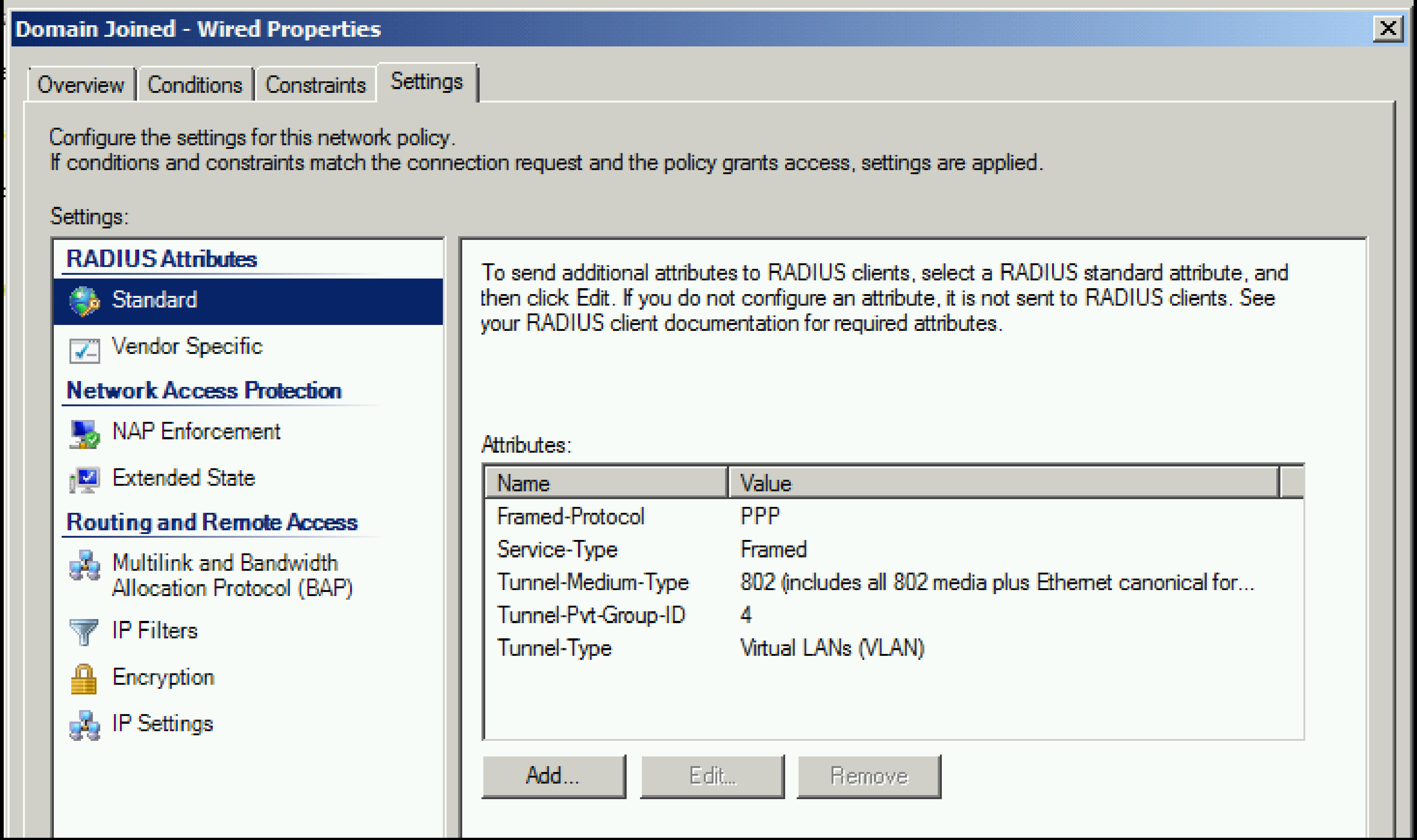

Eduroam Secure Wired Connections Properties
Overview
Conditions
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
Required Authentication Methods
Authentication Methods
Forwarding Connection Request
Authentication
Accounting
Specify a Realm Name
Attribute
RADIUS Attributes
Standard
Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.
Authenticate requests on this server
Forward requests to the following remote RADIUS server group for authentication:
Eduroam
New...
Accept users without validating credentials

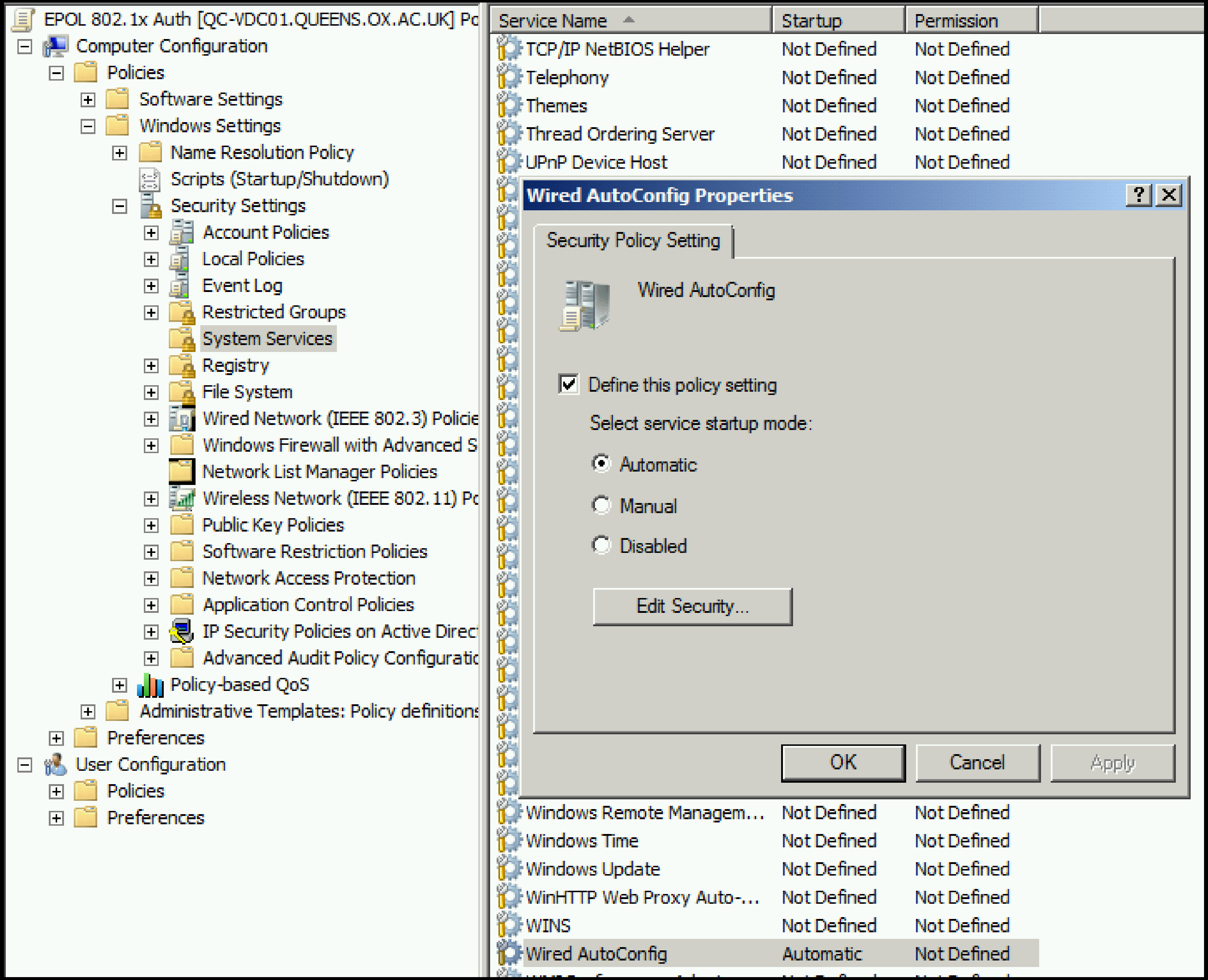

Eduroam Secure Wired Connections Properties
Overview
Conditions
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
Required Authentication Methods
Authentication Methods
Forwarding Connection Request
Authentication
Accounting
Specify a Realm Name
Attribute
RADIUS Attributes
Standard
Vendor Specific
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
98
Tunnel-Type
Virtual LANs (VLAN)
Add...
Edit...
Remove

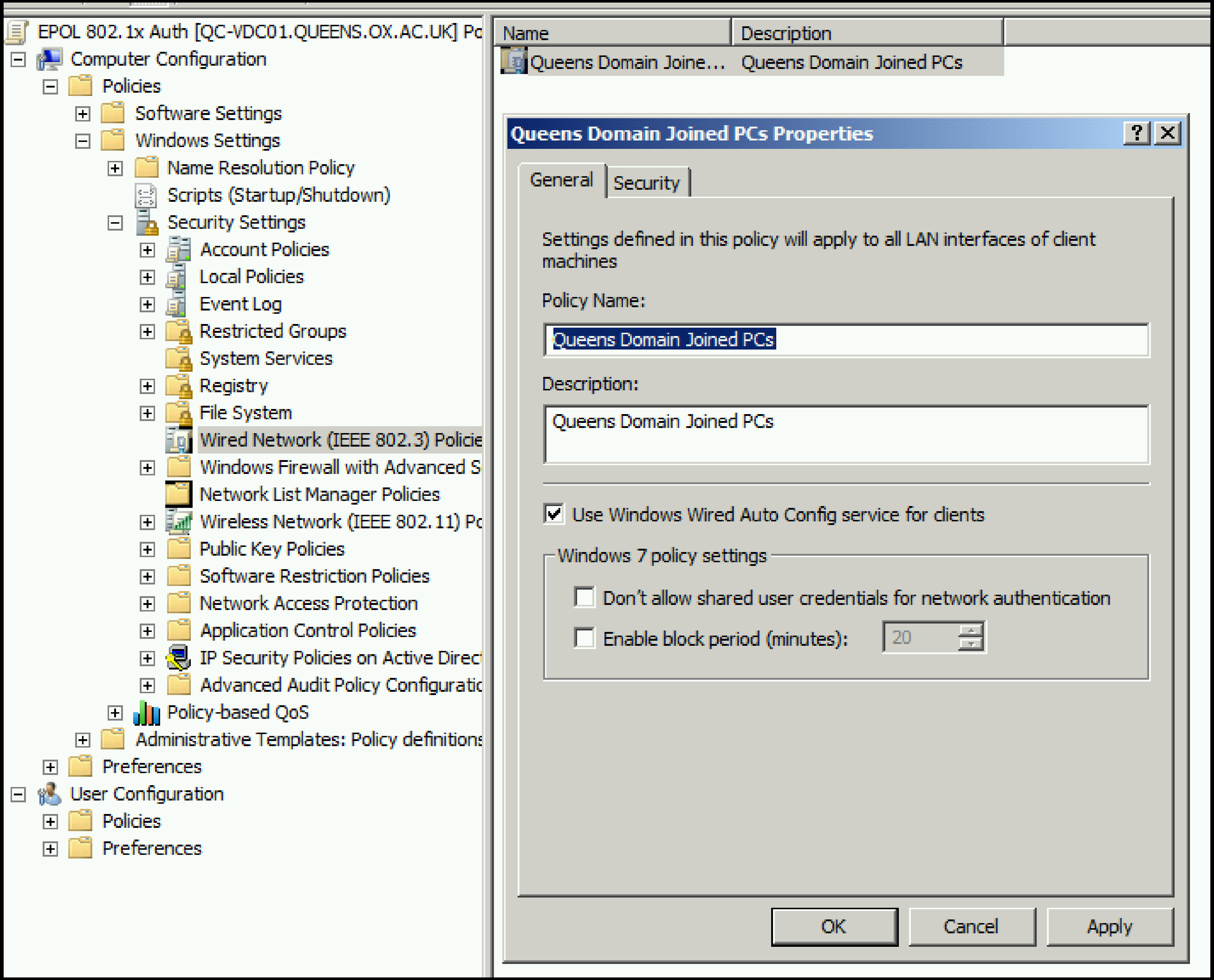

Fellows and Staff - VLAN8 Properties
Overview
Conditions
Constraints
Settings
Configure the conditions for this network policy.
If conditions match the connection request, NPS uses this policy to authorize th
connection request, NPS skips this policy and evaluates other policies, if additi
Condition
Value
NAS Port Type
Ethernet OR Wireless - IEEE 802.11
Windows Groups
QUEENS\Staff and Fellows VLAN8
Edit Protected EAP Properties
Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate.
Certificate issued
QC-VDC01.queens.ox.ac.uk
Friendly name:
Issuer:
queens-QC-VDC01-CA
Expiration date:
03/08/2018 10:25:17
Enable Fast Reconnect
Disconnect Clients without Cryptobinding
Eap Types
Secured password (EAP-MSCHAP v2)
Move Up
Move Down
Add
Edit
Remove
OK
Cancel
Fellows and Staff - VLAN8 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: Protected EAP (PEAP)
MD5-Challenge
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
Perform machine health check only
OK
Cancel
Apply

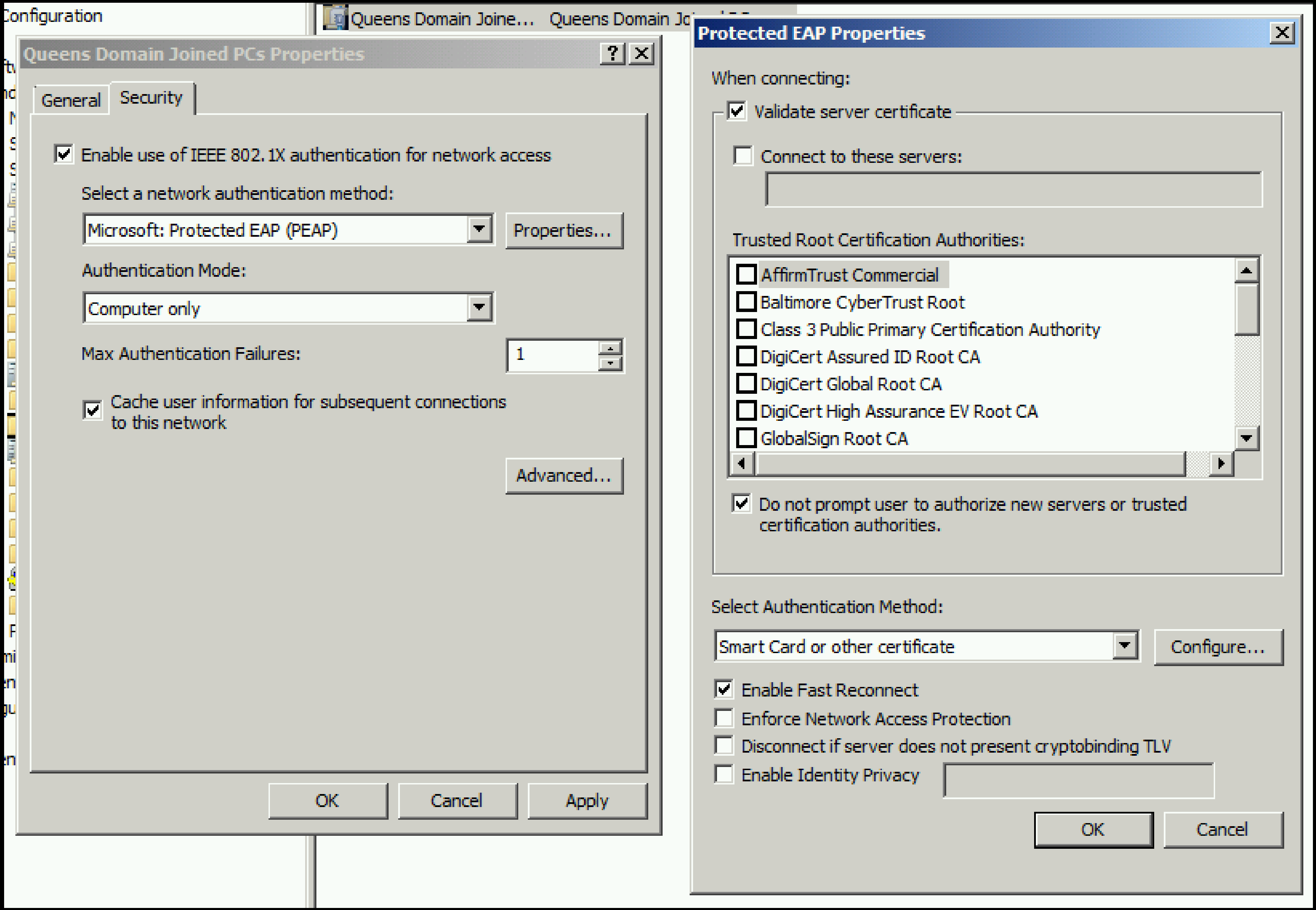


PS (Local)
RADIUS Clients and Serve
RADIUS Clients
Remote RADIUS Serv
Policies
Connection Request F
Network Policies
Health Policies
Network Access Protectio
Accounting
Templates Management
Domain Joined - Wired Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network 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
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: Protected EAP (PEAP)
MD5-Challenge
Move Up
Move Down
Edit...
Remove
authentication methods:
Encrypted Authentication version 2 (MS-CHAP-v2)
an change password after it has expired
Encrypted Authentication (MS-CHAP)
an change password after it has expired
authentication (CHAP)
ted authentication (PAP, SPAP)
nts to connect without negotiating an authentication method
achine health check only
OK
Cancel
Apply
Grant Access
Edit Protected EAP Properties
Select the certificate the server should use to prove its identity to the client.
A certificate that is configured for Protected EAP in Connection Request
Policy will override this certificate.
Certificate issued
QC-VDC01.queens.ox.ac.uk
Friendly name:
Issuer:
queens-QC-VDC01-CA
Expiration date:
03/08/2018 10:25:17
Enable Fast Reconnect
Disconnect Clients without Cryptobinding
Eap Types
Smart Card or other certificate
Move Up
Move Down
Add
Edit
Remove
OK
Cancel


Domain Joined - Wired 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
Tunnel-Medium-Type
802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID
4
Tunnel-Type
Virtual LANs (VLAN)
Add...
Edit...
Remove


EPOL 802.1x Auth [QC-VDC01.QUEENS.OX.AC.UK] Po
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policie
Windows Firewall with Advanced S
Network List Manager Policies
Wireless Network (IEEE 802.11) Po
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Direct
Advanced Audit Policy Configuratio
Policy-based QoS
Administrative Templates: Policy definitions
Preferences
User Configuration
Policies
Preferences
Service Name
Startup
Permission
TCP/IP NetBIOS Helper
Not Defined
Not Defined
Telephony
Not Defined
Not Defined
Themes
Not Defined
Not Defined
Thread Ordering Server
Not Defined
Not Defined
UPnP Device Host
Not Defined
Not Defined
Wired AutoConfig Properties
Security Policy Setting
Wired AutoConfig
Define this policy setting
Select service startup mode:
Automatic
Manual
Disabled
Edit Security...
OK
Cancel
Apply
Windows Remote Managem...
Not Defined
Not Defined
Windows Time
Not Defined
Not Defined
Windows Update
Not Defined
Not Defined
WinHTTP Web Proxy Auto-...
Not Defined
Not Defined
WINS
Not Defined
Not Defined
Wired AutoConfig
Automatic
Not Defined


EPOL 802.1x Auth [QC-VDC01.QUEENS.OX.AC.UK] Pc
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policie
Windows Firewall with Advanced S
Network List Manager Policies
Wireless Network (IEEE 802.11) Pc
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Direc
Advanced Audit Policy Configuratic
Policy-based QoS
Administrative Templates: Policy definitions
Preferences
User Configuration
Policies
Preferences
Name
Description
Queens Domain Joine…
Queens Domain Joined PCs
Queens Domain Joined PCs Properties
General
Security
Settings defined in this policy will apply to all LAN interfaces of client machines
Policy Name:
Queens Domain Joined PCs
Description:
Queens Domain Joined PCs
Use Windows Wired Auto Config service for clients
Windows 7 policy settings
Don't allow shared user credentials for network authentication
Enable block period (minutes):
20
OK
Cancel
Apply


Configuration
Queens Domain Joine...
Queens Domain Joined PCs Properties
General
Security
Enable use of IEEE 802.1X authentication for network access
Select a network authentication method:
Microsoft: Protected EAP (PEAP)
Properties...
Authentication Mode:
Computer only
Max Authentication Failures:
1
Cache user information for subsequent connections to this network
Advanced...
OK
Cancel
Apply
Protected EAP Properties
When connecting:
Validate server certificate
Connect to these servers:
Trusted Root Certification Authorities:
AffirmTrust Commercial
Baltimore CyberTrust Root
Class 3 Public Primary Certification Authority
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert High Assurance EV Root CA
GlobalSign Root CA
Do not prompt user to authorize new servers or trusted certification authorities.
Select Authentication Method:
Smart Card or other certificate
Configure...
Enable Fast Reconnect
Enforce Network Access Protection
Disconnect if server does not present cryptobinding TLV
Enable Identity Privacy
OK
Cancel

Correct as of 24/07/2017

VLAN	ID	Address Range	Default Gateway	Network Zone	Authentication Method
Public Range	1	129.67.180.0/22	129.67.180.6 (Core)	External - Untrusted (for Layer 3)	802.1x Certificate or MAC
Wired Infrastructure	2	10.128.0.0/21	10.128.0.1 (Core)	Internal - Trusted	None
Servers	3	10.128.8.0/21	10.128.8.1 (Core)	Internal - Trusted	None
Wired Clients	4	10.128.16.0/21	10.128.16.1 (Core)	Internal - Trusted	802.1x Certificate or MAC
Wireless Clients	5	10.128.24.0/21	10.128.24.1 (Core)	Internal - Trusted	802.1x Certificate
Printers	6	10.128.32.0/21	10.128.32.1 (Core)	Internal - Trusted	802.1x MAC
Security	7	10.128.40.0/21	10.128.40.1 (Core)	Internal - Trusted	802.1x MAC
Fellows and Staff	8	10.128.48.0/21	10.128.48.1 (PaloAlto)	Internal - Untrusted	802.1x AD Creds or MAC
Wireless Infrastructure	9	10.128.56.0/21	10.128.56.1 (Core)	Internal - Trusted	802.1x MAC
Eduroam (ox.ac.uk)	10	10.128.64.0/21	10.128.64.1 (PaloAlto)	Internal - Untrusted	802.1x Remote Access Creds
IoT	11	10.128.72.0/21	10.128.72.1 (PaloAlto)	Internal - Untrusted	802.1x MAC
Building Management System	12	10.128.80.0/21	10.128.80.1 (Core)	Internal - Trusted	802.1x MAC
Out of Band	13	10.128.88.0/21	10.128.88.1 (Core)	Internal - Trusted	None
IT Office	14	10.128.96.0/21	10.128.96.1 (Core)	Internal - Trusted	802.1x Certificate
SOUP	15	10.128.104.0/21	10.128.104.1 (PaloAlto)	Internal - Untrusted	None – Single port in IT Office
OWL	97	N/A	N/A	External - IT Services	Captive Web Portal (ITS Hosted)
Eduroam	98	N/A	N/A	External - IT Services	802.1x Remote Access Creds
VoIP	99	N/A	N/A	External - IT Services	802.1x MAC
Security (legacy)	500	10.0.1.0/16	N/A	Internal - Trusted	802.1x MAC
Wireless (legacy)	555	10.0.0.0/22	10.0.0.1 (Core)	Internal - Trusted	802.1x MAC

[redacted].queens.ox.ac.uk - PuTTY

```
SW-ITOFFICE01# show port-access clients

 Port Access Client Status

  Port  Client Name   MAC Address   IP Address       User Role         Type  VLAN
  ----- ------------- ------------- ---------------- ----------------- ----- ----
  2     00[redacted]  001a[redacted] n/a                               MAC   99
  7     00[redacted]  0000[redacted] n/a                               MAC   12
  8     00[redacted]  0000[redacted] n/a                               MAC   12
  9     e8[redacted]  e803[redacted] n/a                               MAC   4
  10    bc[redacted]  bc30[redacted] n/a                               MAC   12
  12    ho[redacted]  0050[redacted] n/a                               8021X 4
  12    00[redacted]  001a[redacted] n/a                               MAC   99
  14    00[redacted]  001e[redacted] n/a                               MAC   6
  15    ho[redacted]  6400[redacted] n/a                               8021X 4
  15    00[redacted]  001a[redacted] n/a                               MAC   99
  17    00[redacted]  001a[redacted] n/a                               MAC   99
  22    00[redacted]  0011[redacted] n/a                               MAC   6

[redacted]
```

ACLS Slide

Further Reading

- Lynda.com https://www.lynda.com/Windows-Server-tutorials/Overview-Network-Policy-Server-NPS/459490/505660-4.html