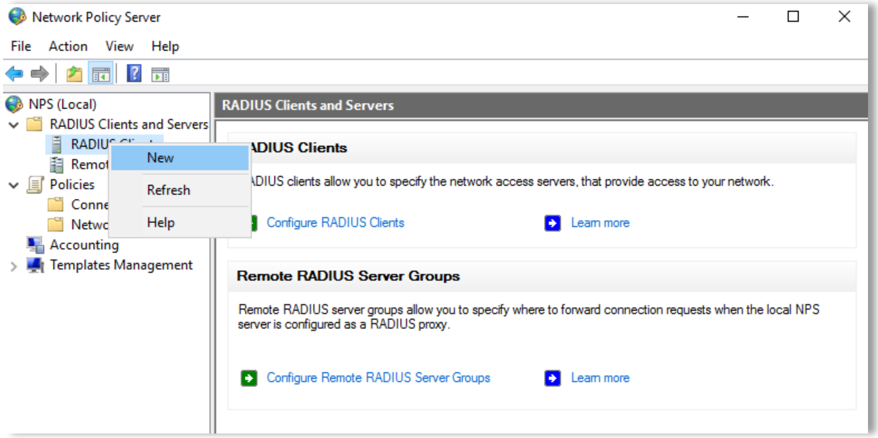
How to enable users to change expired Passwords on SonicWall UTM Appliances using SSLVPN.

- This document is created based on 6.5 firmware but the procedures are the same with previous versions of SonicOS.
- To enable password changes the SonicWall and the Server need to use MSCHAPv2.
- It is recommended to use LDAPS 636 for the communication between the SonicWall and the AD Server(s).
- Check also if any other Application is using the default RADIUS ports on the server by doing a netstat -ab from the command prompt, if UDP 1812 and 1813 are already listed you will need to change on the NPS Radius Client Advanced settings and the SonicWall RADIUS Settings.
- This document presumes you have already set up the LDAP(S) connection between the SonicWall and the Server. If not refer to this document on the link below first
- https://www.sonicwall.com/en-us/support/knowledge-base/170707170351983

Setting up the Server(s)

1. We will need to Install NPS if not already installed, to do this go to **Server Manager**, select **Add Roles and Features** and Select **Network Policy and Access Services,** continue with the Wizard only selecting Network Policy And Access Services.
2. Run the NPS by going to either Server Manager / Tools / Network Policy Server or by selecting from the Start Menu / Windows Administrative Tools / Network Policy Server.
3. To start we set up the Radius Client, in our case the connecting IP address which will be the SonicWall LAN IP, right click on RADIUS Clients and select new, give it a name, enter your required IP and a Shared Secret of your choice.

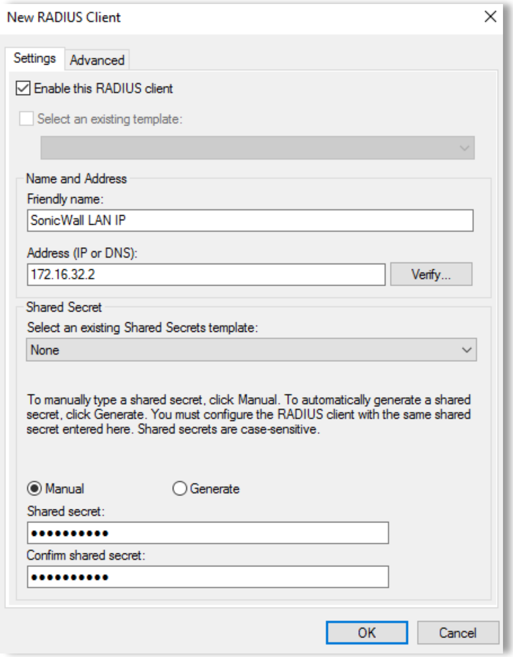


ADIUS Clients

ADIUS clients allow you to specify the network access servers, that provide access to your network.

Remote RADIUS Server Groups

Remote RADIUS server groups allow you to specify where to forward connection requests when the local NPS server is configured as a RADIUS proxy.



☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: SonicWall LAN IP

Address (IP or DNS): 172.16.32.2

Shared Secret

Select an existing Shared Secrets template: None

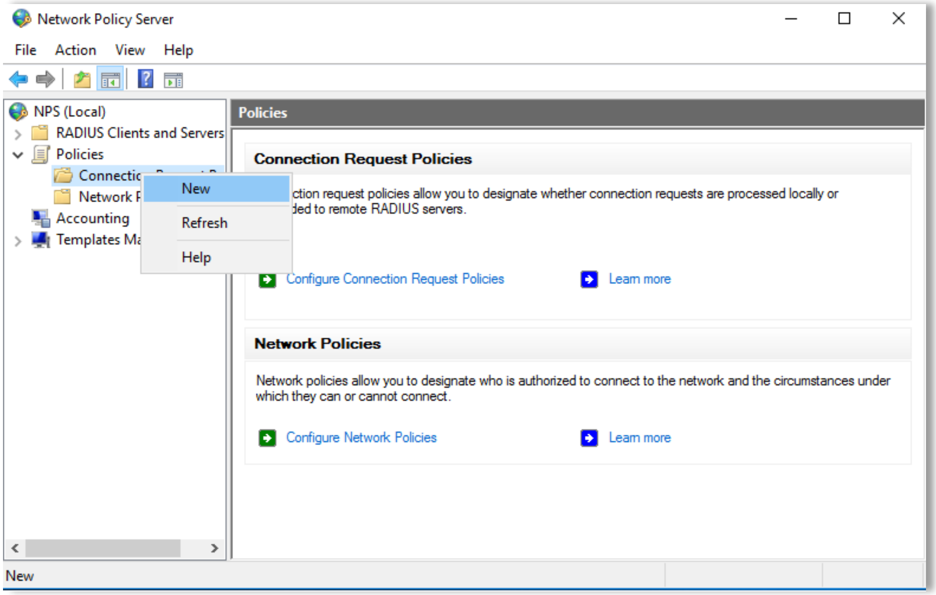
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••••

Confirm shared secret: ••••••••••

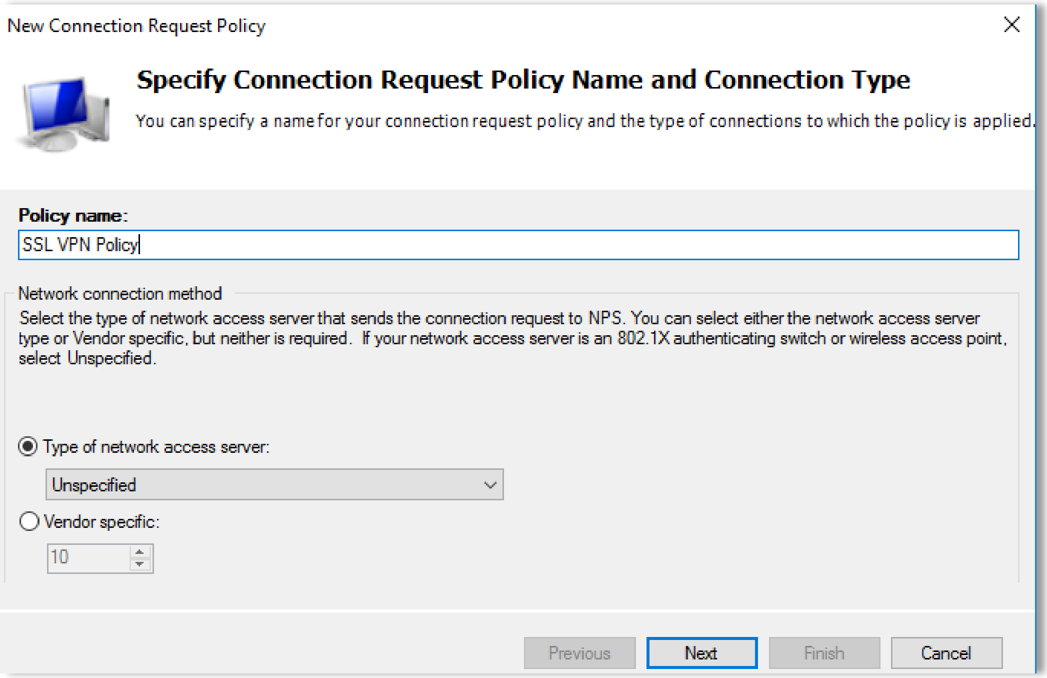
4. Once loaded we need to create the Connection Policy and the Network Policy, right click on the Connection Policies in the Policies section and select New.



ction request policies allow you to designate whether connection requests are processed locally or ded to remote RADIUS servers.

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

5. Give the Connection Policy a name.



Specify Connection Request Policy Name and Connection Type

You can specify a name for your connection request policy and the type of connections to which the policy is applied.

Policy name: SSL VPN Policy

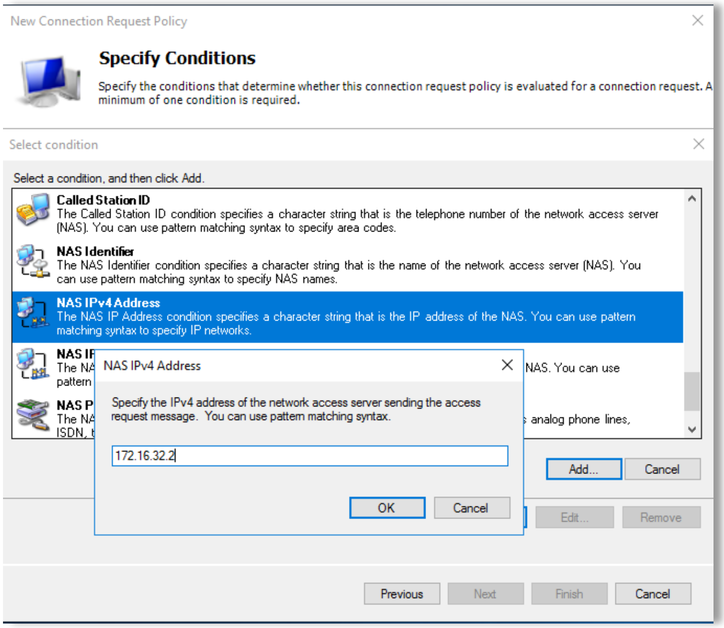
Network connection method

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

6. Specify the conditions to connect, in this case we chose the NAS IPv4 Address and enter the IP address of the SonicWall LAN IP which is on the same subnet as the server.



New Connection Request Policy

Specify Conditions

Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Select condition

Select a condition, and then click Add.

Called Station ID
The Called Station ID condition specifies a character string that is the telephone number of the network access server (NAS). You can use pattern matching syntax to specify area codes.

NAS Identifier
The NAS Identifier condition specifies a character string that is the name of the network access server (NAS). You can use pattern matching syntax to specify NAS names.

NAS IPv4 Address
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.

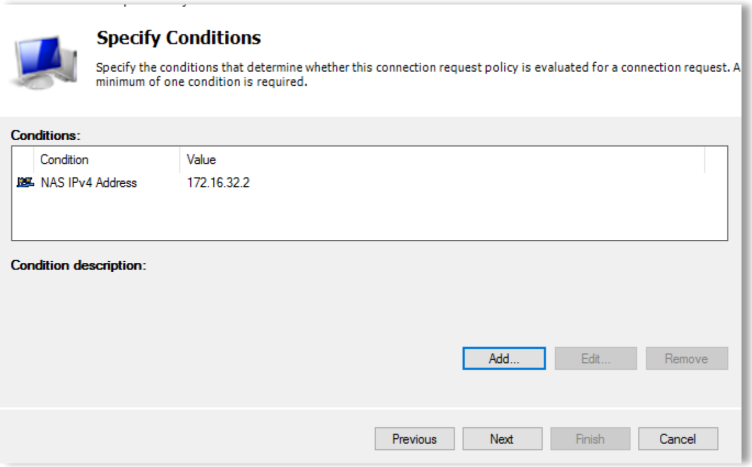
NAS IF
The NA NAS. You can use
pattern

NAS P
The NA analog phone lines,
ISDN,

NAS IPv4 Address

Specify the IPv4 address of the network access server sending the access request message. You can use pattern matching syntax.

172.16.32.2



Specify Conditions

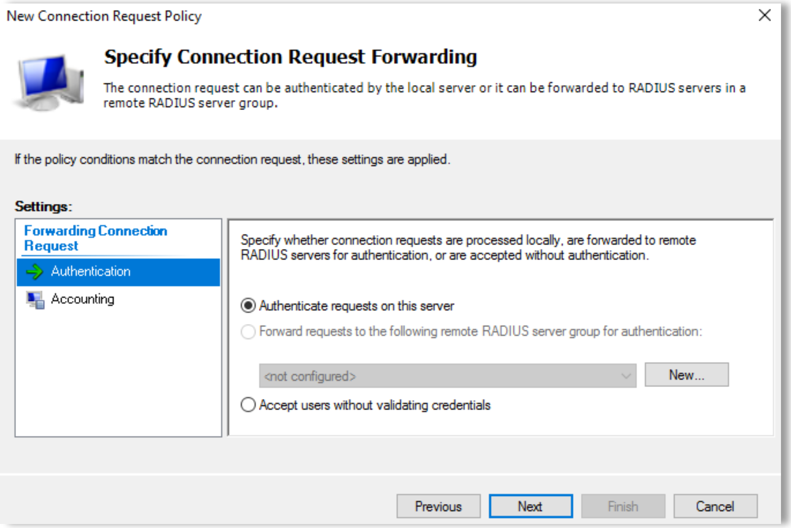
Specify the conditions that determine whether this connection request policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

Condition	Value
NAS IPv4 Address	172.16.32.2

Condition description:

7. Leave the Authentication settings and Methods as Default.



New Connection Request Policy

Specify Connection Request Forwarding

The connection request can be authenticated by the local server or it can be forwarded to RADIUS servers in a remote RADIUS server group.

If the policy conditions match the connection request, these settings are applied.

Settings:

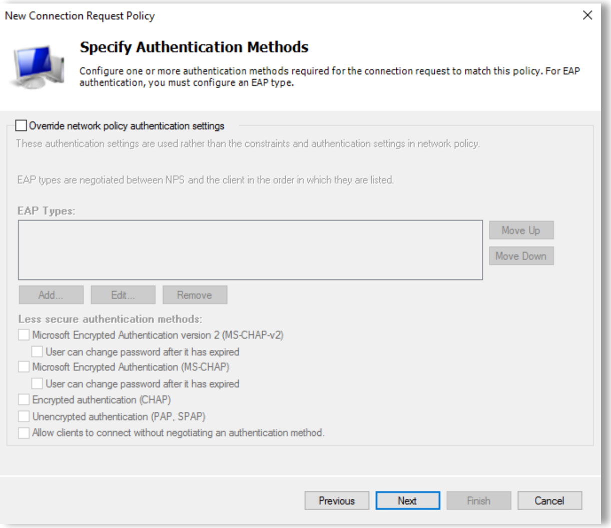
Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

● Authenticate requests on this server

○ Forward requests to the following remote RADIUS server group for authentication:

<not configured>

○ Accept users without validating credentials



New Connection Request Policy

Specify Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

□ Override network policy authentication settings

These authentication settings are used rather than the constraints and authentication settings in network policy.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

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)

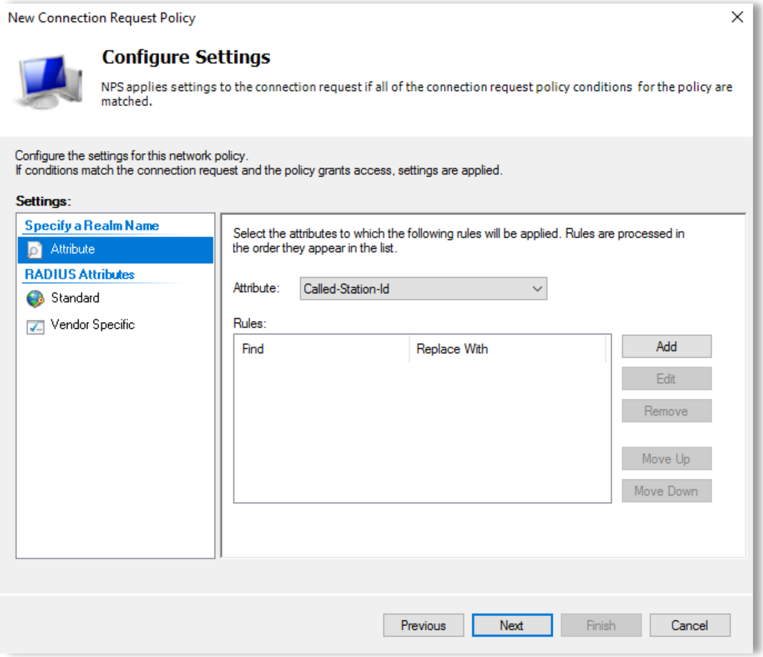
□ User can change password after it has expired

□ Encrypted authentication (CHAP)

□ Unencrypted authentication (PAP, SPAP)

□ Allow clients to connect without negotiating an authentication method.

8. You don't need to add any Attributes just select next and finish.



Configure Settings

NPS applies settings to the connection request if all of the connection request policy conditions for the policy are matched.

Configure the settings for this network policy.
If conditions match the connection request and the policy grants access, settings are applied.

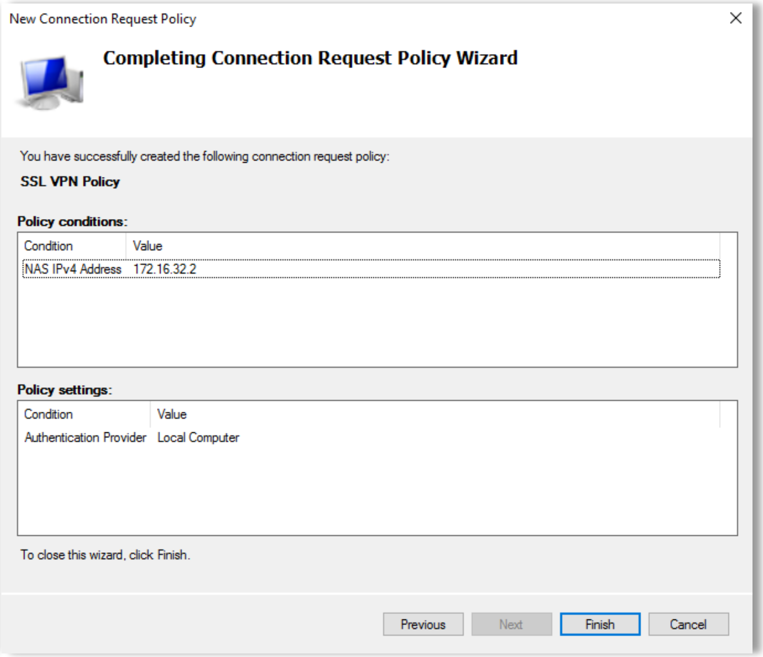
Settings:

Select the attributes to which the following rules will be applied. Rules are processed in the order they appear in the list.

Attribute: Called-Station-Id

Rules:

Find	Replace With



Completing Connection Request Policy Wizard

You have successfully created the following connection request policy:

SSL VPN Policy

Policy conditions:

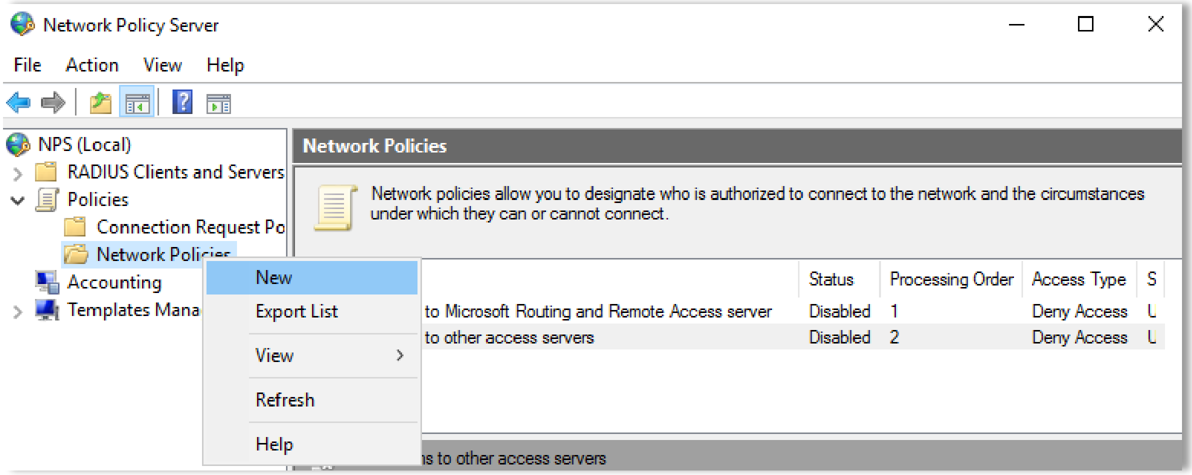
Condition	Value
NAS IPv4 Address	172.16.32.2

Policy settings:

Condition	Value
Authentication Provider	Local Computer

To close this wizard, click Finish.

9. Next, we need to set up the Network Policy like the previous one right click and select New.



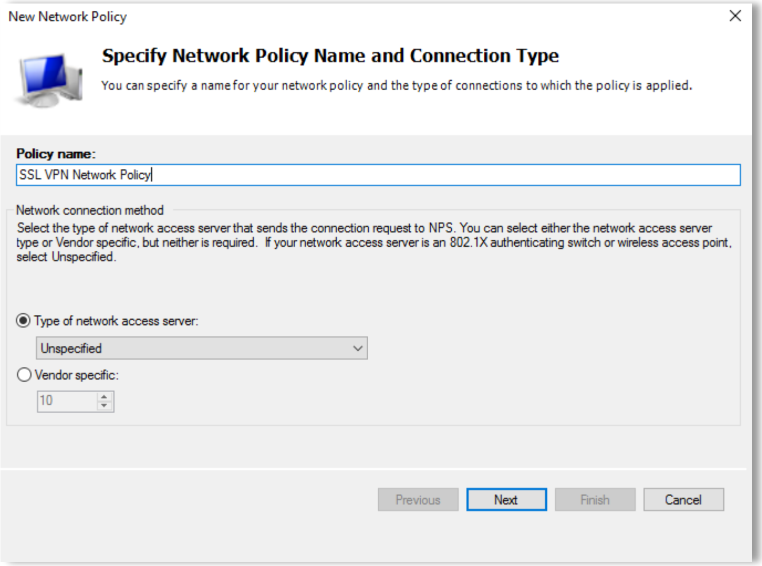
Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

	Status	Processing Order	Access Type	S
to Microsoft Routing and Remote Access server	Disabled	1	Deny Access	L
to other access servers	Disabled	2	Deny Access	L

s to other access servers

10. This time under the condition we select User Groups.



New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

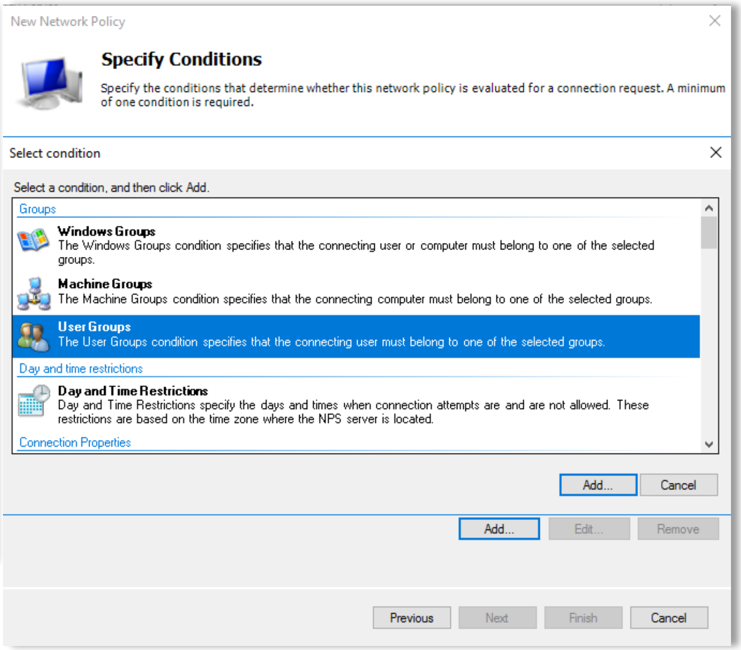
Policy name: SSL VPN Network Policy

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



New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Select condition

Select a condition, and then click Add.

Groups

Windows Groups The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

Machine Groups The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.

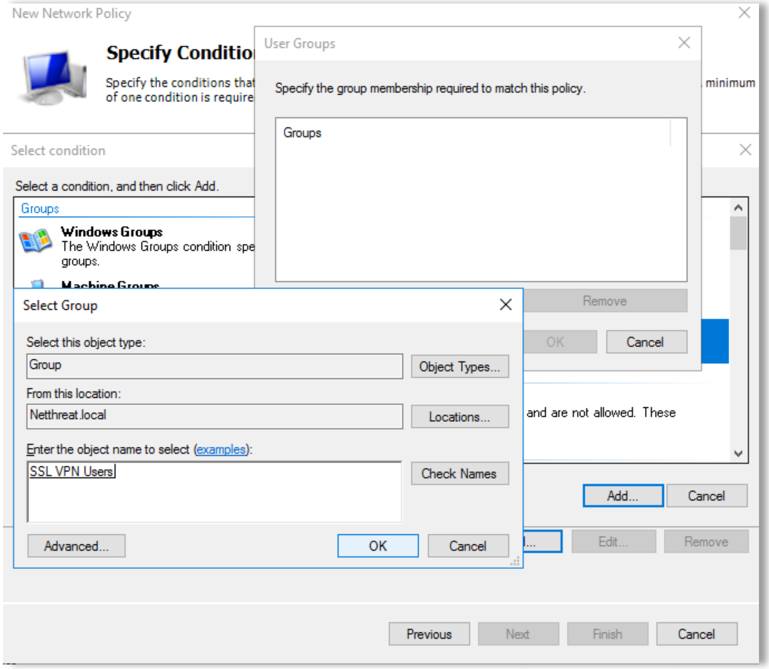
User Groups The User Groups condition specifies that the connecting user must belong to one of the selected groups.

Day and time restrictions

Day and Time Restrictions Day and Time Restrictions specify the days and times when connection attempts are and are not allowed. These restrictions are based on the time zone where the NPS server is located.

Connection Properties

11. We choose the group which has all our SSL VPN users in.



User Groups

Specify the group membership required to match this policy.

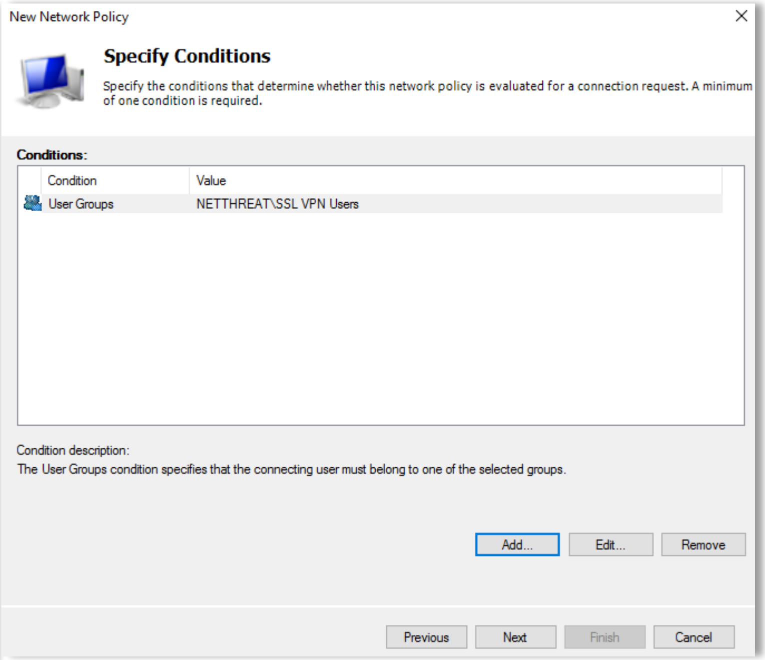
Groups

Select Group

Select this object type: Group

From this location: Netthreat.local

Enter the object name to select (examples): SSL VPN Users



New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

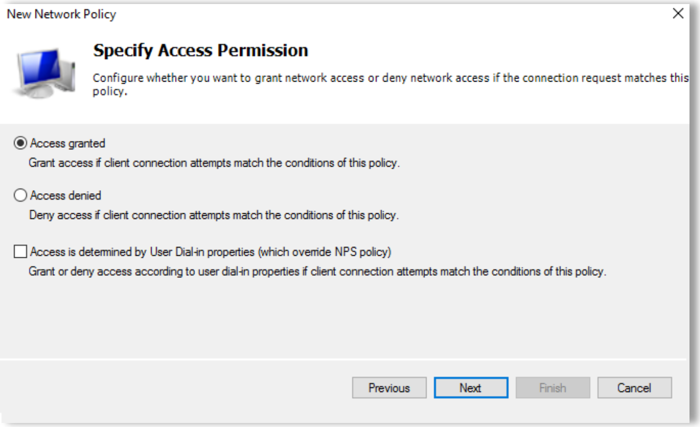
Conditions:

Condition	Value
User Groups	NETTHREAT\SSL VPN Users

Condition description:
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

netthreat
thinking security

12. Select Access Granted and select the Authentication Methods as below MSCHAP and MSCHAPv2.



New Network Policy

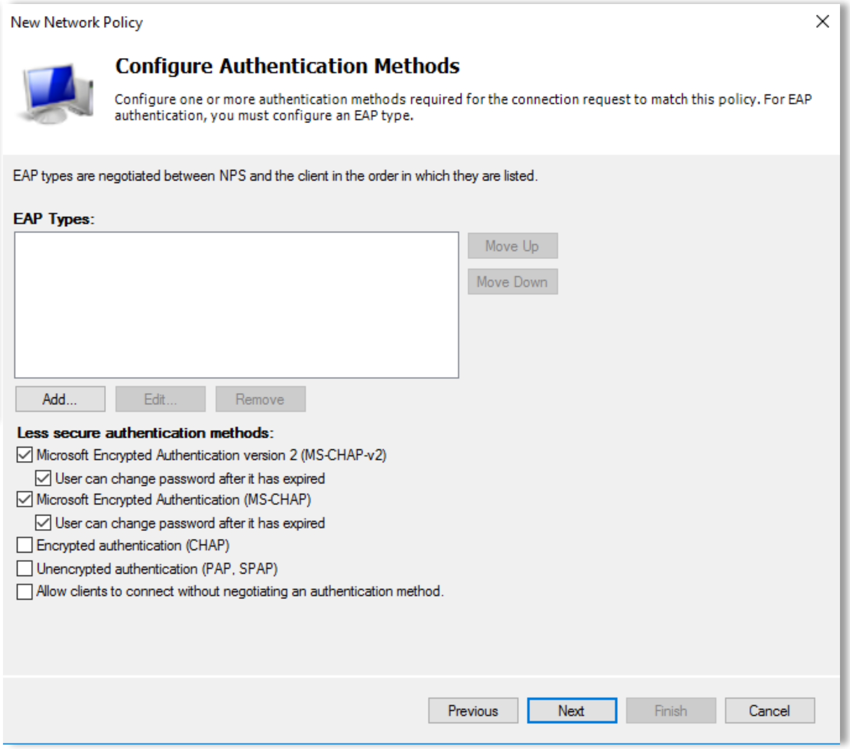
Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

● Access granted
Grant access if client connection attempts match the conditions of this policy.

○ Access denied
Deny access if client connection attempts match the conditions of this policy.

□ Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

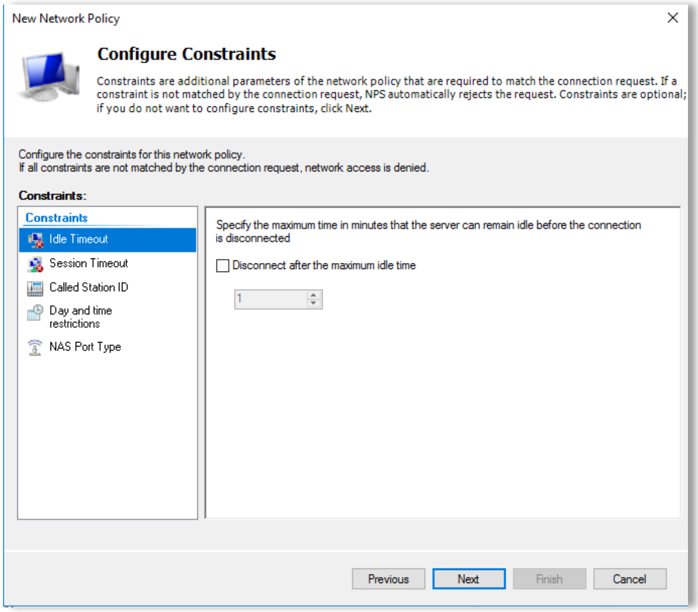
EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

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.

13. On configure Constraints and Configure Settings leave as default.



New Network Policy

Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

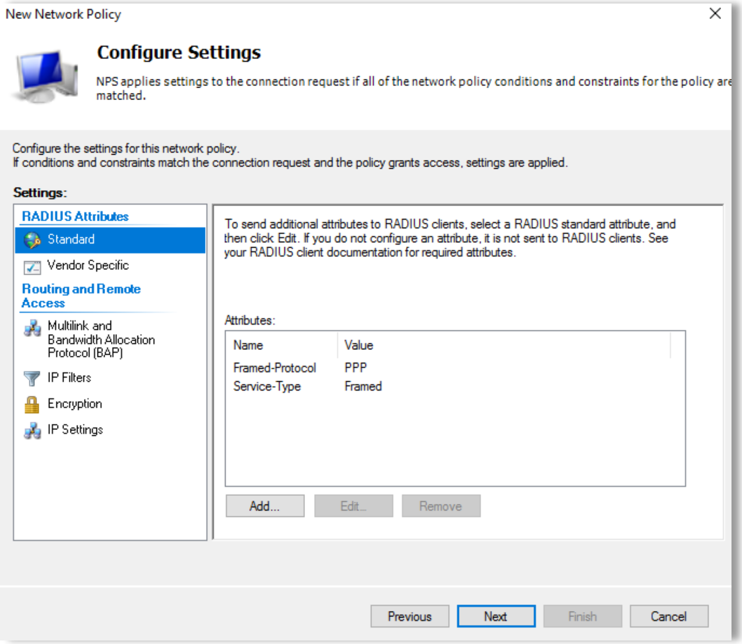
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

□ Disconnect after the maximum idle time

1



New Network Policy

Configure Settings

NPS applies settings to the connection request if all of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

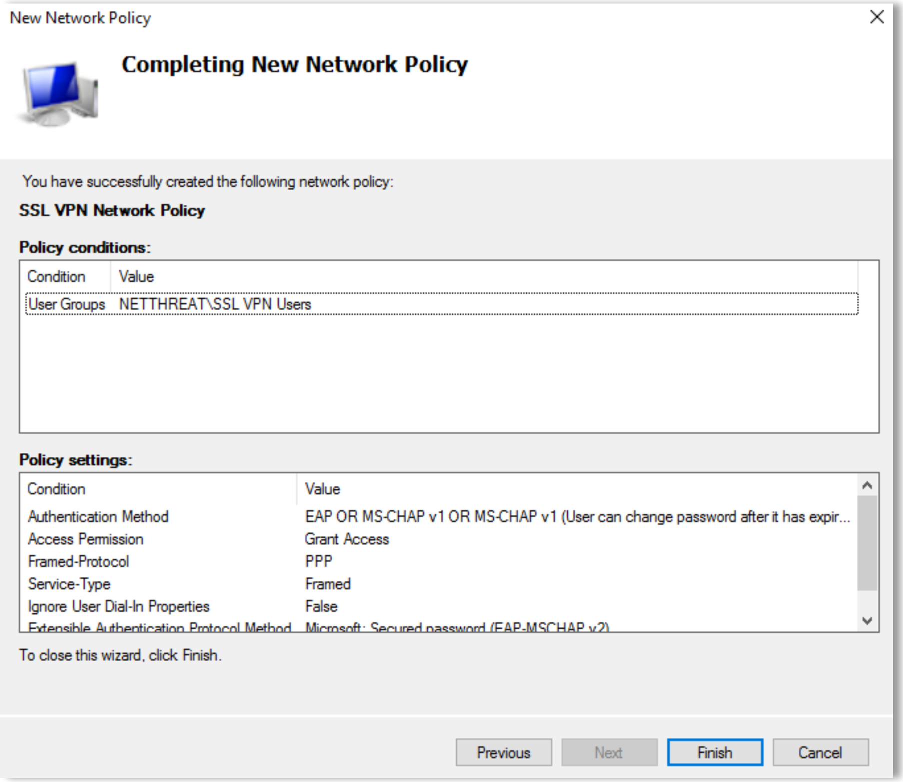
RADIUS Attributes
Standard
Vendor Specific
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings

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

14. Next Check the Settings are correct and the Finish.



New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

SSL VPN Network Policy

Policy conditions:

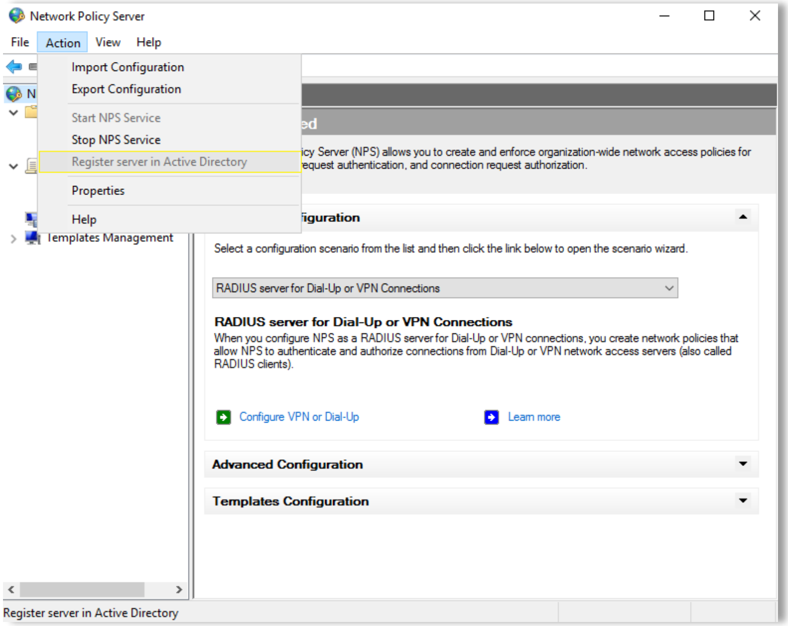
Condition	Value
User Groups	NETTHREAT\SSL VPN Users

Policy settings:

Condition	Value
Authentication Method	EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expir...
Access Permission	Grant Access
Framed-Protocol	PPP
Service-Type	Framed
Ignore User Dial-In Properties	False
Extensible Authentication Protocol Method	Microsoft: Secured password (EAP-MSCHAP v2)

To close this wizard, click Finish.

15. We need to register NPS in Active Directory, Select Action from the top menu and then Register server in Active Directory.



Network Policy Server

icy Server (NPS) allows you to create and enforce organization-wide network access policies for
equest authentication, and connection request authorization.

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

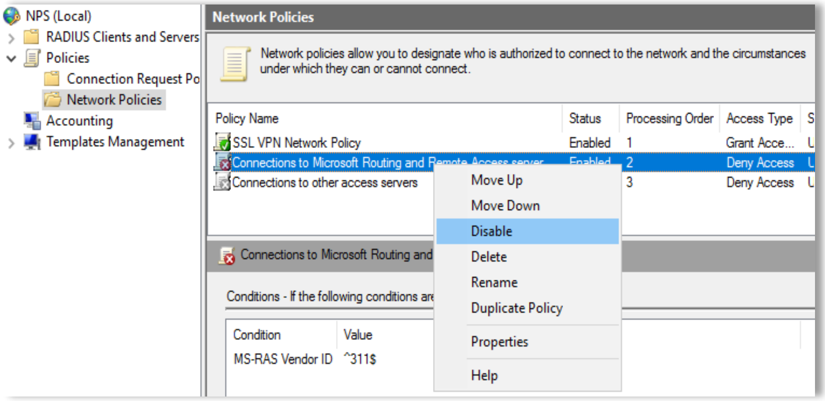
RADIUS server for Dial-Up or VPN Connections

RADIUS server for Dial-Up or VPN Connections

When you configure NPS as a RADIUS server for Dial-Up or VPN connections, you create network policies that allow NPS to authenticate and authorize connections from Dial-Up or VPN network access servers (also called RADIUS clients).

Register server in Active Directory

16. Next, we need to disable the Default Policy Profiles, it is the same procedure for the Connection and the both the default Network Policies, right click on the policies and select Disable.



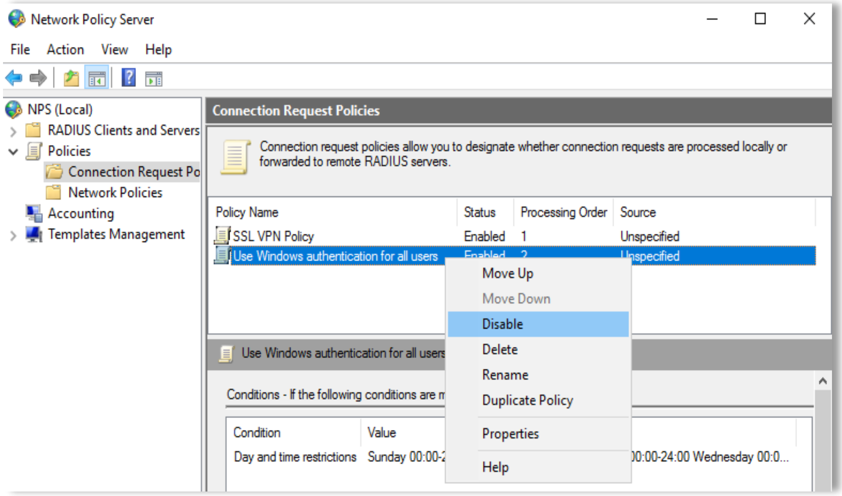
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	S
SSL VPN Network Policy	Enabled	1	Grant Acce...	U
Connections to Microsoft Routing and Remote Access server	Enabled	2	Deny Access	U
Connections to other access servers		3	Deny Access	U

Connections to Microsoft Routing and

Conditions - If the following conditions are

Condition	Value
MS-RAS Vendor ID	^311$



Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

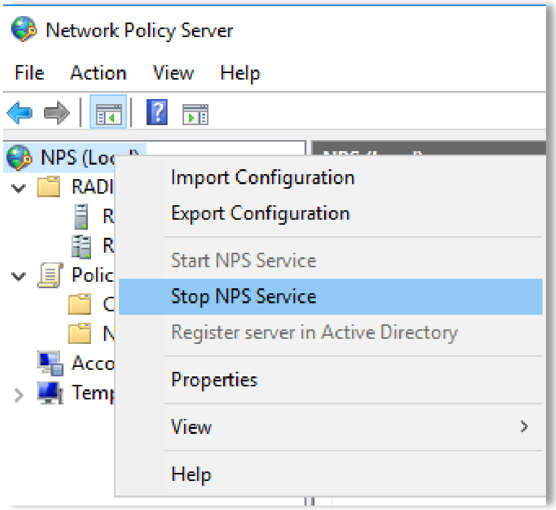
Policy Name	Status	Processing Order	Source
SSL VPN Policy	Enabled	1	Unspecified
Use Windows authentication for all users	Enabled	2	Unspecified

Use Windows authentication for all users

Conditions - If the following conditions are m

Condition	Value
Day and time restrictions	Sunday 00:00-2 ... 00:00-24:00 Wednesday 00:0...

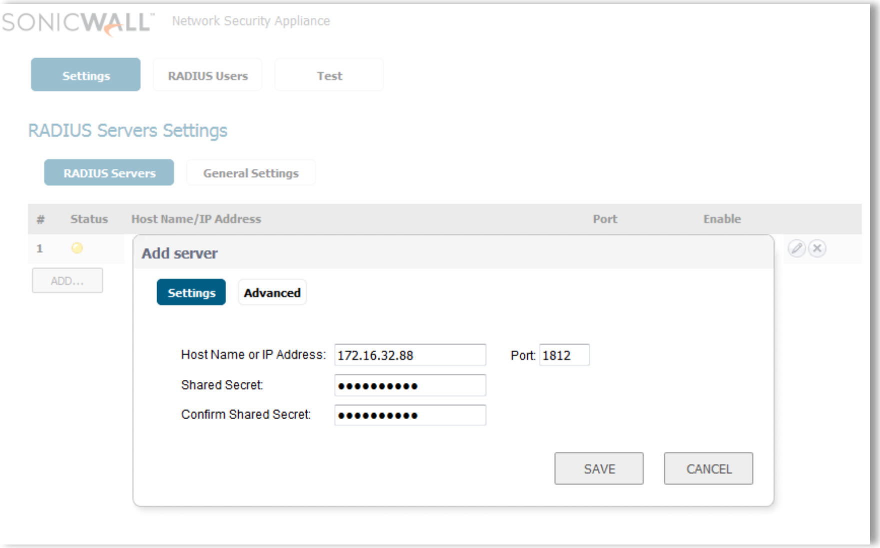
17. Once you have configured everything, I would recommend restarting the NPS Service after any changes, you can do this by right clicking on the main NPS icon and selecting Stop NPS Service, wait a few seconds for it to refresh then select Start NPS Service.



18. That's the Server side set up, you can repeat on a backup server if needed.

Setting up the SonicWall

1. To Set up the SonicWall to enable Password changes we first need to go (in Classic Navigation Mode) **Users / Settings** / **Authentication** and Select Configure RADIUS, then ADD, enter your Servers IP address and the Shared Secret chosen to match the one entered on the NPS RADIUS Client.



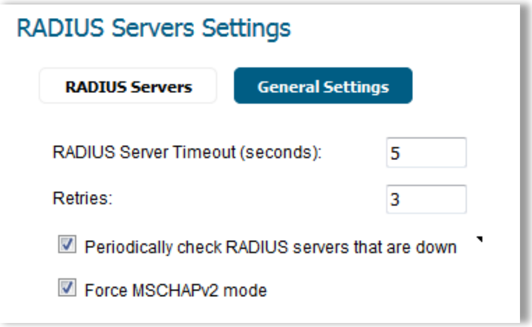
RADIUS Servers Settings

Add server

Host Name or IP Address: 172.16.32.88 Port: 1812

Shared Secret: ••••••••••

Confirm Shared Secret: ••••••••••



RADIUS Servers Settings

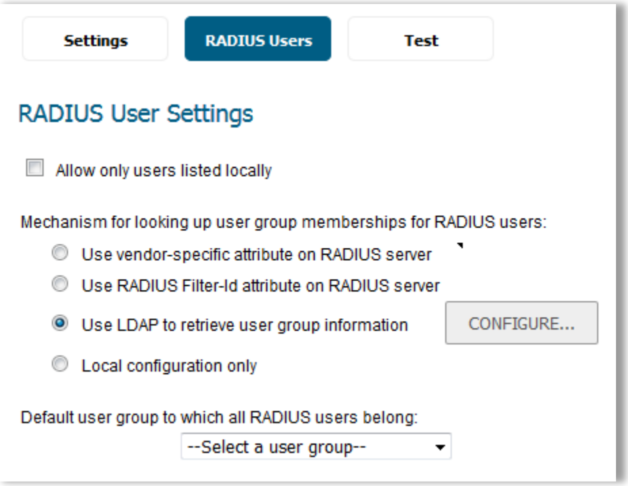
RADIUS Server Timeout (seconds): 5

Retries: 3

☑ Periodically check RADIUS servers that are down

☑ Force MSCHAPv2 mode

2. Next select RADIUS Users and set to Use LDAP to Retrieve User Names, to test go to Test and check the connectivity and authentication, if you have any errors check the Firewall on the Server and the User is in the relevant Group under the Local User and Groups / Local Groups / SSL VPN Services / Members.



RADIUS User Settings

□ Allow only users listed locally

Mechanism for looking up user group memberships for RADIUS users:

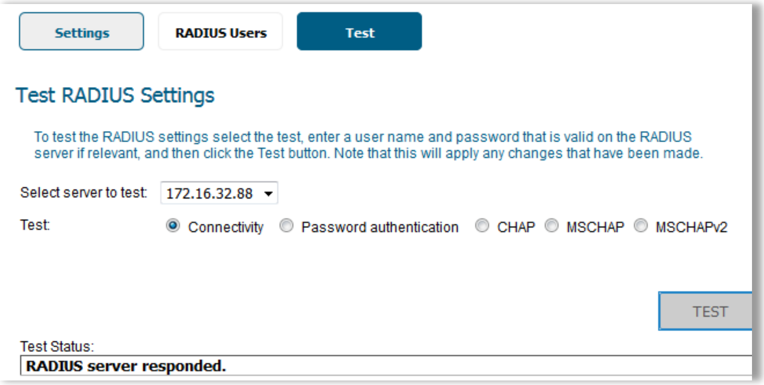
○ Use vendor-specific attribute on RADIUS server

○ Use RADIUS Filter-Id attribute on RADIUS server

● Use LDAP to retrieve user group information

○ Local configuration only

Default user group to which all RADIUS users belong: --Select a user group--



Test RADIUS Settings

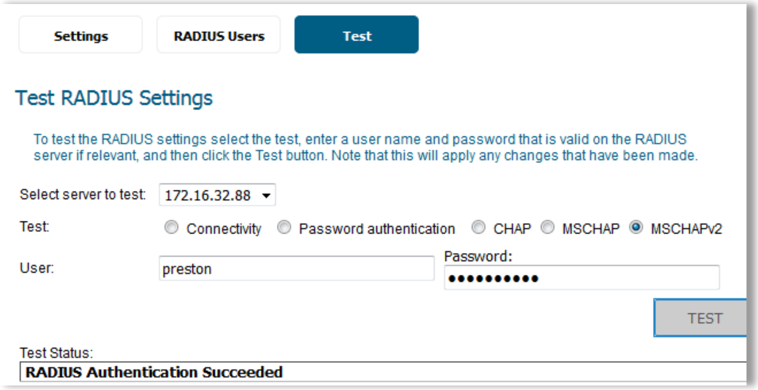
To test the RADIUS settings select the test, enter a user name and password that is valid on the RADIUS server if relevant, and then click the Test button. Note that this will apply any changes that have been made.

Select server to test: 172.16.32.88

Test: ● Connectivity ○ Password authentication ○ CHAP ○ MSCHAP ○ MSCHAPv2

Test Status:

RADIUS server responded.



Test RADIUS Settings

To test the RADIUS settings select the test, enter a user name and password that is valid on the RADIUS server if relevant, and then click the Test button. Note that this will apply any changes that have been made.

Select server to test: 172.16.32.88

Test: ○ Connectivity ○ Password authentication ○ CHAP ○ MSCHAP ● MSCHAPv2

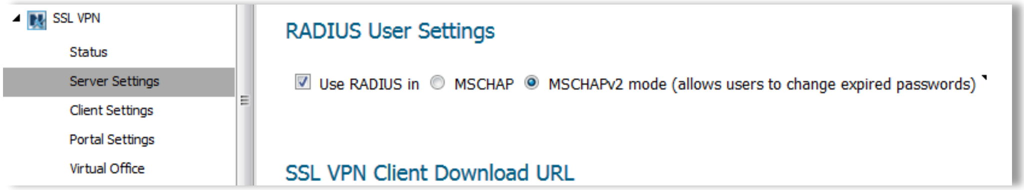
User: preston

Password: ••••••••••

Test Status:

RADIUS Authentication Succeeded

3. The last thing you need to do is under the SSL VPN Server settings is to change the RADIUS User Settings to use RADIUS with MSCHAPv2 this is in case you already have users connected to the SSL VPN it may force them to reconnect.



RADIUS User Settings

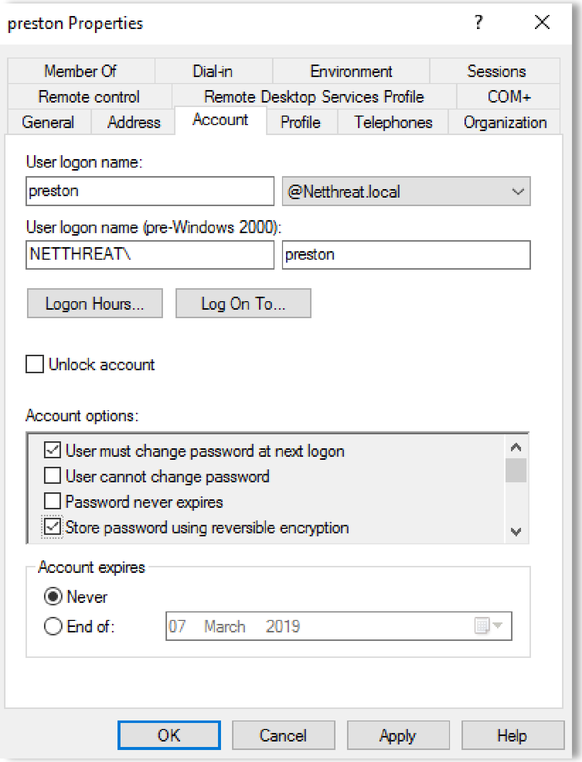
☑ Use RADIUS in ○ MSCHAP ● MSCHAPv2 mode (allows users to change expired passwords)

SSL VPN Client Download URL

4. Now that all the settings are in and working, we can now check the Changing of expired Passwords will work.

5. First check that you can connect and authenticate as expected using SonicWall Netextender or mobile connect.

6. Now go in to AD Users and Computers and set the Users password to expire on next logon like below



User logon name: preston @Netthreat.local

User logon name (pre-Windows 2000): NETTHREAT\ preston

□ Unlock account

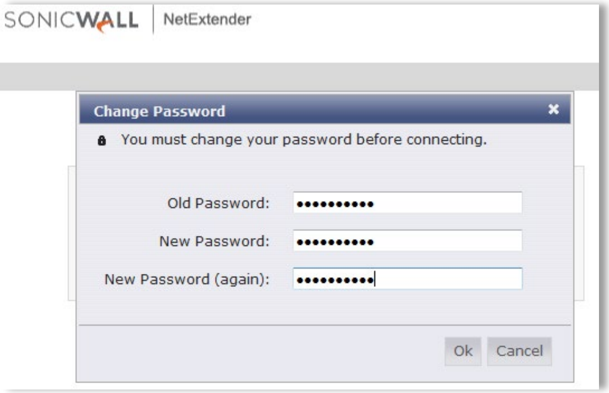
Account options:

☑ User must change password at next logon
□ User cannot change password
□ Password never expires
☑ Store password using reversible encryption

Account expires

● Never
○ End of: 07 March 2019

7. When you login again with Netextender with your password you will be prompted with the Change Password popup



SONICWALL | NetExtender

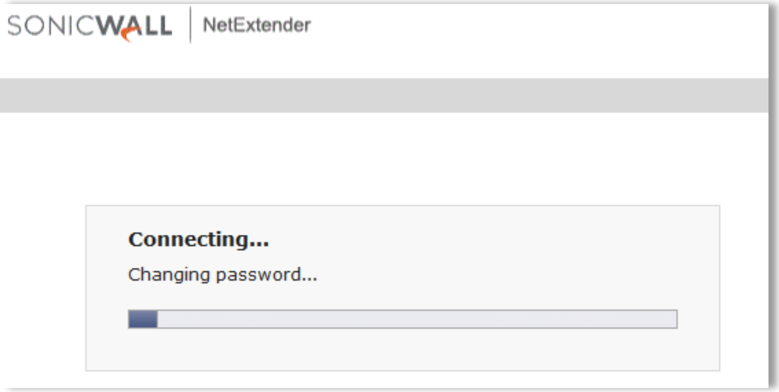
Change Password

You must change your password before connecting.

Old Password: ••••••••••

New Password: ••••••••••

New Password (again): ••••••••••

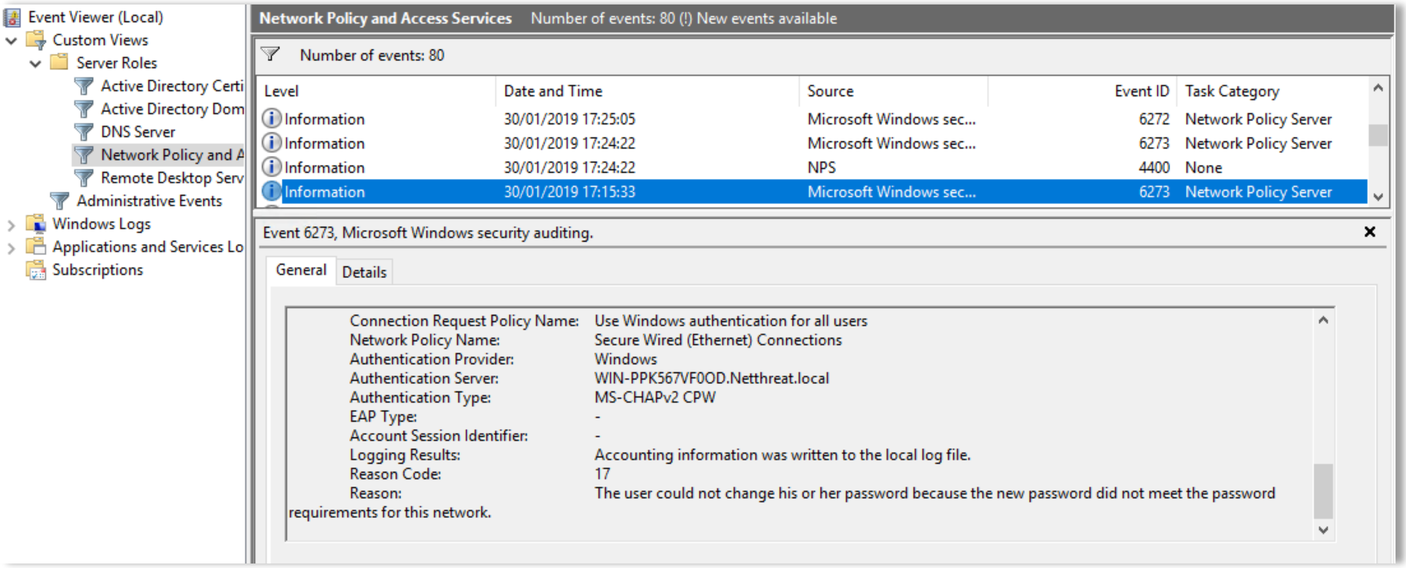


SONICWALL | NetExtender

Connecting...

Changing password...

8. You should now be connected, if you have any issues connecting, the best place to look is on the Server on the Event Viewer under Server Roles / Network and Access Policies, it could be to do with your Domain Password polices especially if you are trying to use a previously used password.



Network Policy and Access Services   Number of events: 80 (!) New events available

Number of events: 80

Level	Date and Time	Source	Event ID	Task Category
Information	30/01/2019 17:25:05	Microsoft Windows sec...	6272	Network Policy Server
Information	30/01/2019 17:24:22	Microsoft Windows sec...	6273	Network Policy Server
Information	30/01/2019 17:24:22	NPS	4400	None
Information	30/01/2019 17:15:33	Microsoft Windows sec...	6273	Network Policy Server

Event 6273, Microsoft Windows security auditing.

```
        Connection Request Policy Name:   Use Windows authentication for all users
        Network Policy Name:              Secure Wired (Ethernet) Connections
        Authentication Provider:          Windows
        Authentication Server:            WIN-PPK567VF0OD.Netthreat.local
        Authentication Type:              MS-CHAPv2 CPW
        EAP Type:                         -
        Account Session Identifier:       -
        Logging Results:                  Accounting information was written to the local log file.
        Reason Code:                      17
        Reason:                           The user could not change his or her password because the new password did not meet the password
requirements for this network.
```