



# **How to Configure 802.1x**

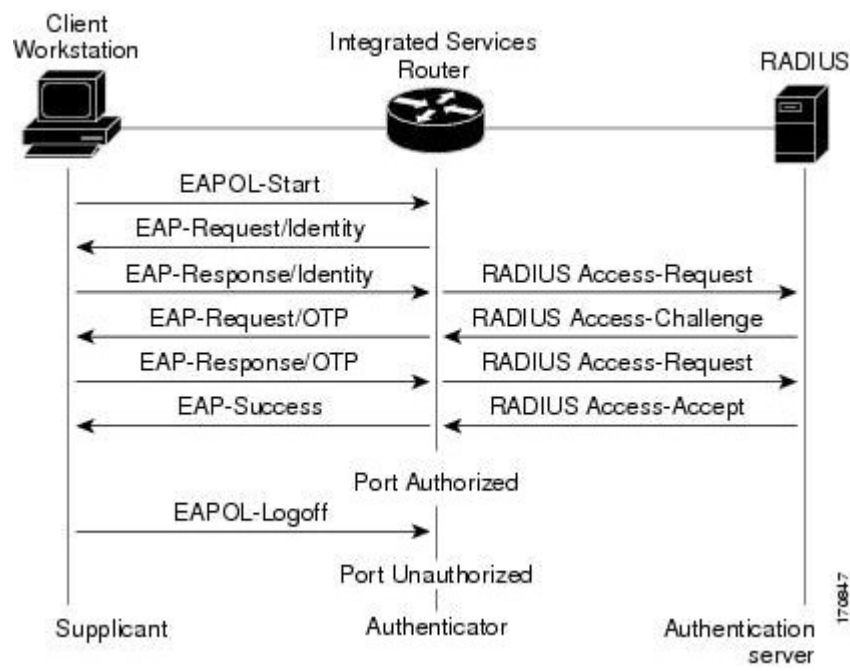
For Windows Server

## Contents

Switch Configuration .....	3
EAP Message Exchange .....	3
Configure 802.1x Port-Based Authentication .....	3
802.1x Global commands .....	3
802.1x Port Configuration .....	3
Radius Global commands .....	4
Windows Server Configuration .....	4
Install Network Policy and Access Services Role .....	4
Add the Radius Client .....	5
Windows Client Configuration .....	7
Turn on Wired Service .....	7
Enable 802.1x .....	7
Certificate Authority Configuration .....	10

# Switch Configuration

## EAP Message Exchange



## Configure 802.1x Port-Based Authentication

### 802.1x Global commands

1. Enable
2. Configure Terminal
3. Aaa new-model
4. Aaa authentication dot1x default group radius
5. Dot1x system-auth-control
6. End
7. Write memory

### 802.1x Port Configuration

1. Enable
2. Configure Terminal
3. Interface gi1/0/1
4. Dot1x port-control auto
5. Dot1x pae authenticator
6. End
7. Write memory

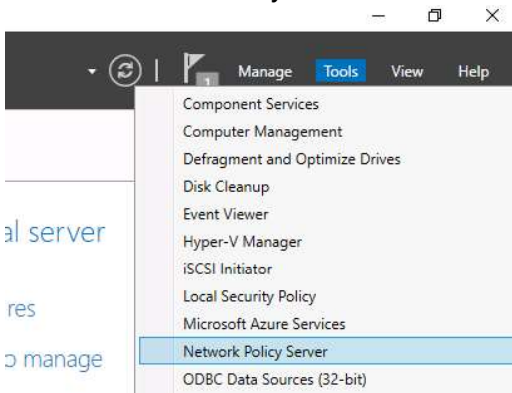
## Radius Global commands

1. Enable
2. Configure Terminal
3. Radius-server host XXX.XXX.XXX.XXX auth-port 1812 key XXXXXXXXXXXX
4. Radius-server host XXX.XXX.XXX.XXX acct-port 1813 key XXXXXXXXXXXX
5. End
6. Write memory

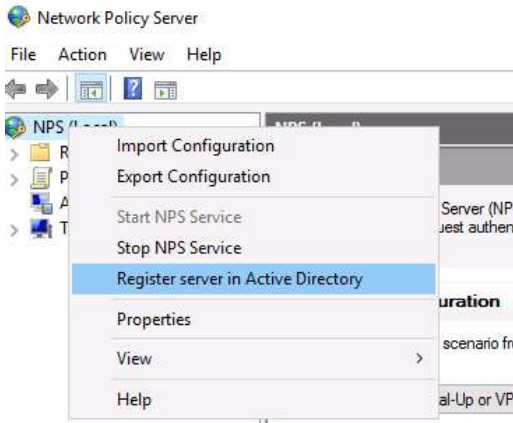
# Windows Server Configuration

## Install Network Policy and Access Services Role

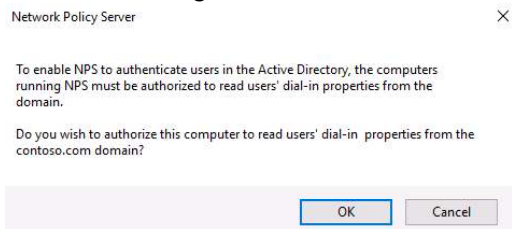
1. Install Network Policy and Access Services Role to Server (NPS)



2. Register NPS in Active Directory



3. Confirm the registration



# Add the Radius Client

4. Expand the Radius Clients and Servers section in the NPS console tree and select New on the Radius Clients item



5. On the Settings tab, create a Friendly Name, client address (IP or DNS) and Shared Secret (the password you used in the Switch configuration - See Radius Global Command numbers 3 and 4 on page 4)

New RADIUS Client

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:  
Cisco\_3360

Address (IP or DNS):  
192.168.0.1 Verify...

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.

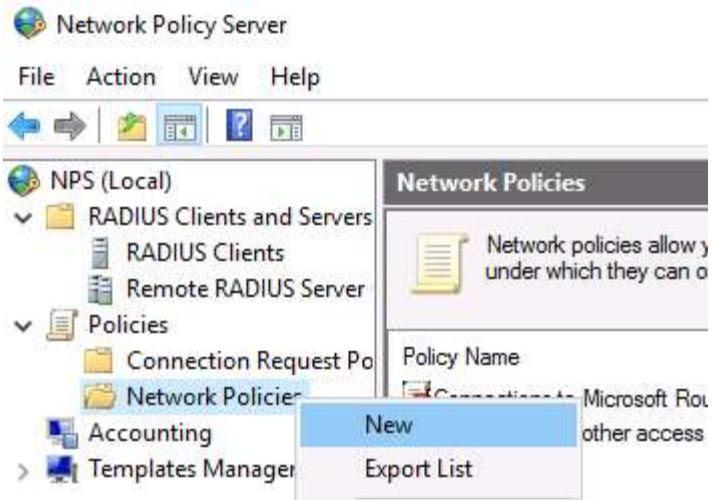
☒ Manual ☐ Generate

Shared secret:  
.....

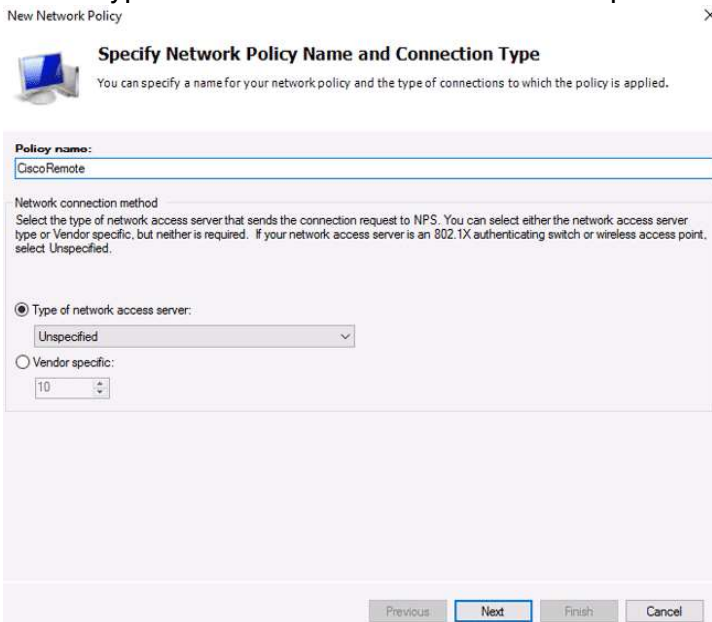
Confirm shared secret:  
.....

OK Cancel

6. Configure NPS Policies on the Radius Server by expanding the Policies>Network Policies branch and Select New

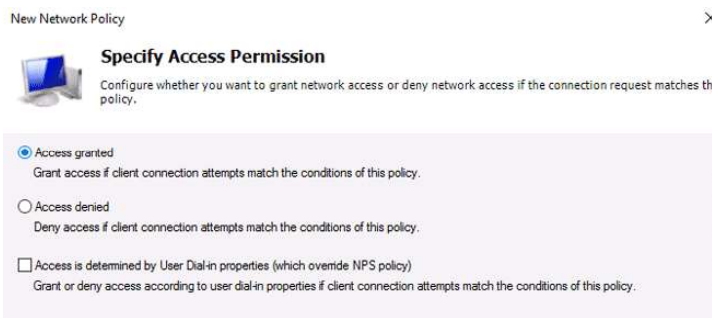


7. Leave Type of Network Access Server as “Unspecified”



8. Specify Conditions by adding Windows Groups Domain Users and Domain Computers from Active Directory

9. On the next screen select Access Granted



## 10. Check MS-CHAP-v2, MS-CHAP and add EAP (in the EAP Type box)

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:**

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.

Previous Next Finish Cancel

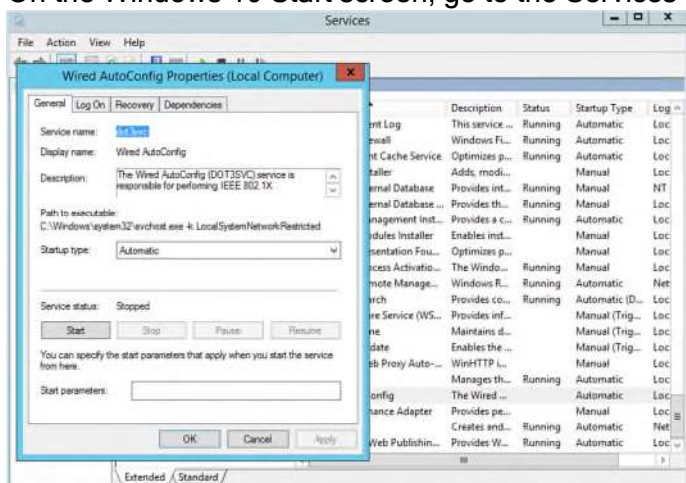
## 11. From the EAP Types, ensure that you add Certificate Authority from the dropdown

## 12. Ensure that you add the Radius certificate to the Trust Certificates on the Server

# Windows Client Configuration

## Turn on Wired Service

## 13. On the Windows 10 Start screen, go to the Services and find Wired AutoConfig and turn it on to Automatic.

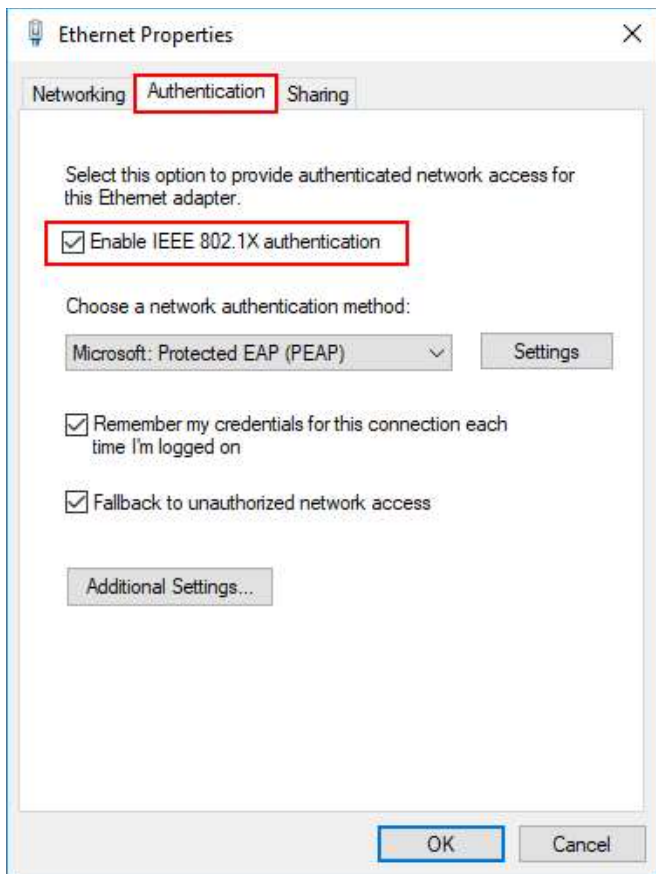


## Enable 802.1x

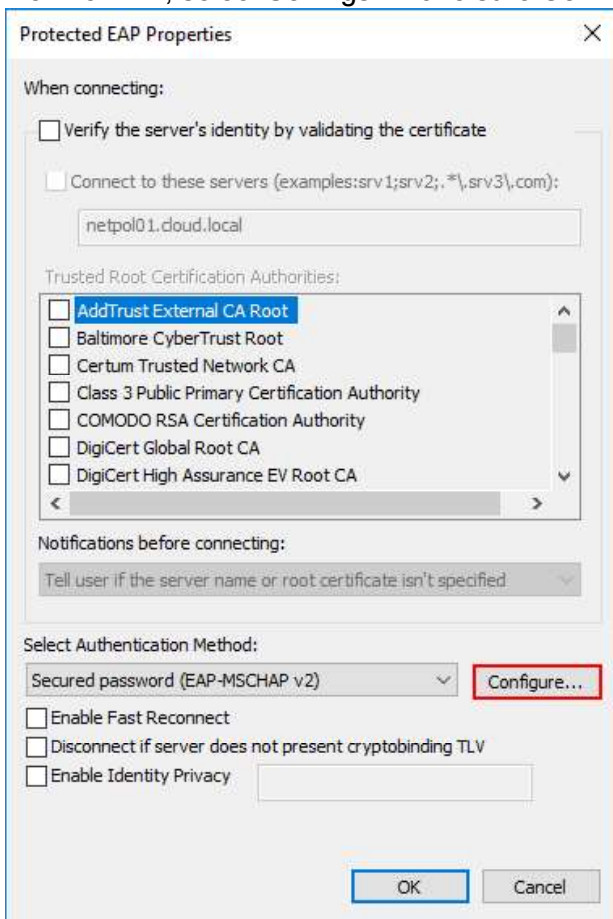
## 14. Go to the Ethernet properties adapter settings and go to the Authentication tab (added by turning on Wired AutoConfig service)

## 15. Select the Enable IEEE 802.1x authentication box and ensure Protected EAP is selected (also make sure Fallback to unauthorized network access is selected).



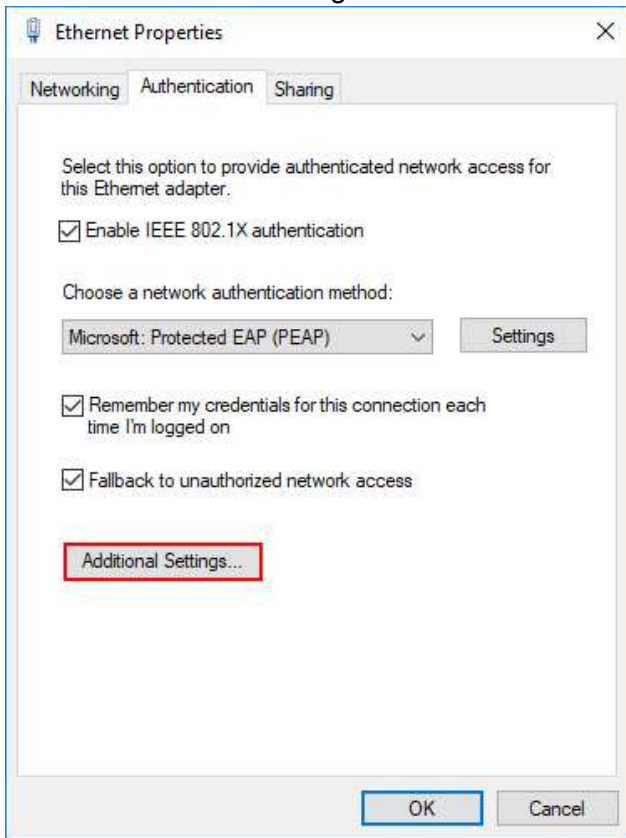


16. Next to EAP, select Settings. Make sure Certificate Authority and Radius certificates are selected

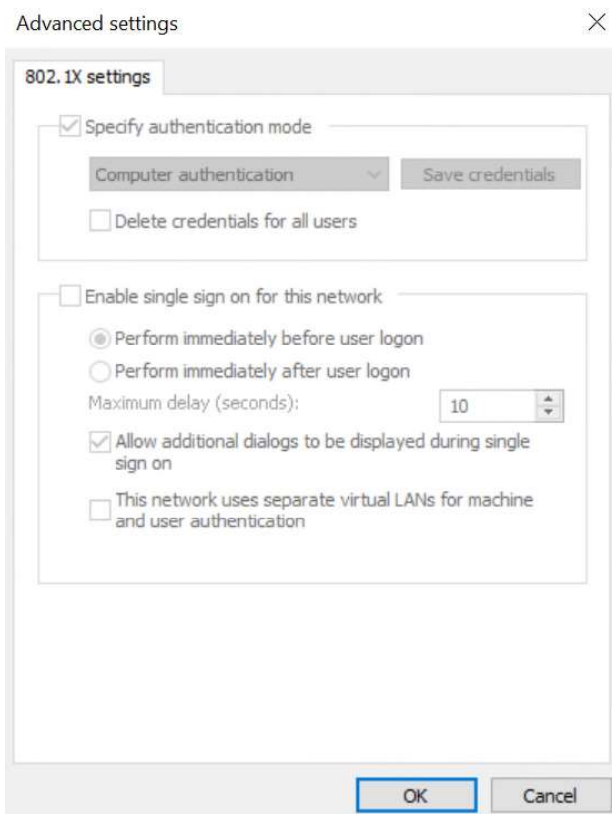




## 17. Click on Additional Settings



## 18. Select Computer Authentication



## 19. Install the Radius certificate under your Trusted certificates for the machine.

# Certificate Authority Configuration

20. Log into the Certificate Authority Server
21. Create a new certificate for your Radius server
22. Create a GPO to push out Radius server certificate on all your Windows Machines so that it trusts the Radius server for 802.1x authentication

