



# FortiNAC - Microsoft Entra ID Authentication Cookbook

Version F 7.6.5

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)

July 10th, 2025

FortiNAC F 7.6.5 Microsoft Entra ID Authentication Cookbook

49-20-748677-20210922

# TABLE OF CONTENTS

<b>Overview</b> .....	<b>5</b>
<b>Requirements</b> .....	<b>6</b>
<b>Microsoft Entra ID Authentication using 802.1x with TTLS-PAP</b> .....	<b>7</b>
Prerequisite .....	7
1. Create and Register FortiNAC Application in Microsoft Entra ID .....	8
2. FortiGate Configuration .....	10
3. FortiNAC Configuration .....	12
Service Connectors Configuration .....	12
Microsoft Entra ID Mappings Configuration .....	13
FortiGate VDOM configuration .....	14
FortiSwitch Port Configuration .....	15
Generate Certificate for Microsoft Entra ID in FortiNAC Service Connector (Optional) .....	16
Step 1 - Generate new CSR on FortiNAC .....	16
Step 2 - Submit Certificate Request on Microsoft Active Directory .....	17
Step 3 - Upload the certificate onto FortiNAC .....	18
Step 4 - Upload the Certificate back to Microsoft Entra ID App Registration .....	19
4. Windows Client .....	19
<b>Microsoft Entra ID Authentication using Captive Portal</b> .....	<b>25</b>
1. Microsoft Entra ID, FortiGate, FortiNAC, and FortiSwitch Configuration .....	26
Step 1 - Microsoft Entra ID Configuration .....	26
Step 2 - FortiGate Configuration .....	26
Step 3 - FortiNAC configuration .....	27
Step 4 - FortiSwitch Port Configuration .....	28
Step 5 - Service Connectors Configuration .....	29
Step 7 - Portal Configuration .....	30
2. Windows Client Configuration .....	31
Step 1 - Disable dot1x on Host .....	31
Step 2 - Connect to the Network .....	31
<b>Microsoft Entra ID Authentication using TLS Certificate</b> .....	<b>35</b>
Overview .....	35
1. Generate TLS certificate for Microsoft Entra ID to do authentication .....	35
Method 1: .....	35
Method 2: .....	36
Result - TLS Certificate added in Client .....	41
2. FortiNAC Local RADIUS TLS Service Configuration .....	42
Step 1 - Generate Certificate Signing Request (CSR) .....	42
Step 2 - Submit Certificate Request on Microsoft Active Directory .....	43
Step 3 - Upload the certificate onto FortiNAC .....	44
Step 4 - Define Microsoft Entra ID Mappings and Authentication source in virtual server configuration .....	46
Step 5 - Define certificate attribute selection ranking in virtual server configuration .....	46
3. Configuration on Client Side .....	47
Step 1 - Export root CA from Active Directory Certificate Services .....	47
Step 2 - Import Root CA into Client Trust Root Certificates .....	50

---

Step 3 - Upload AD Root Certificate to FortiNAC .....	54
4. Use the TLS certificate to initiate authentication .....	55
5. Synchronize New attributes added in User/Host Profiles for Microsoft Entra ID .....	57
<b>Remote Group .....</b>	<b>58</b>
Overview .....	58
Configuration on FortiNAC through Service Connector .....	58
Remote Groups CLI Configuration .....	59
Example - Remote Group Use with User Host/Profile .....	60
Prerequisite .....	60
Steps on using 802.1X TLS Security Profile .....	61

## Overview

This document provides steps to configure the following features using Microsoft Entra ID. Note these features are independent of each other.

**Microsoft Entra ID Authentication using 802.1x with TTLS-PAP** - Enables FortiNAC to automatically register clients with a Microsoft Entra ID account based upon the RADIUS supplicant information.

**Microsoft Entra ID Authentication using Captive Portal** - Use Entra ID as the Authentication source for end users registering through the FortiNAC captive portal.

**Microsoft Entra ID Authentication using TLS Certificate** - Enables FortiNAC to automatically register clients with a Microsoft Entra ID account based upon the TLS certificate information.

**Remote Group**- Allows FortiNAC to sync groups of users from Microsoft Entra ID. These groups of users can constantly be polled and updated automatically or manually through FortiNAC service connector. Allows FortiNAC users to see the list of users authenticated by FortiNAC through Microsoft Entra ID authentication as a group in System > Groups > Remote Groups.

# Requirements

The requirement for conducting this use case is as the following:

Device	Version
FortiNAC	7.6.5 or later
FortiGate	
FortiSwitch	
FortiAP	
Windows Client	
Wireless adapter	

# Microsoft Entra ID Authentication using 802.1x with TTLS-PAP



Caution: EAP-TTLS PAP with Entra ID does NOT support MFA (Multi-Factor Authentication). See <https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth-ropc>

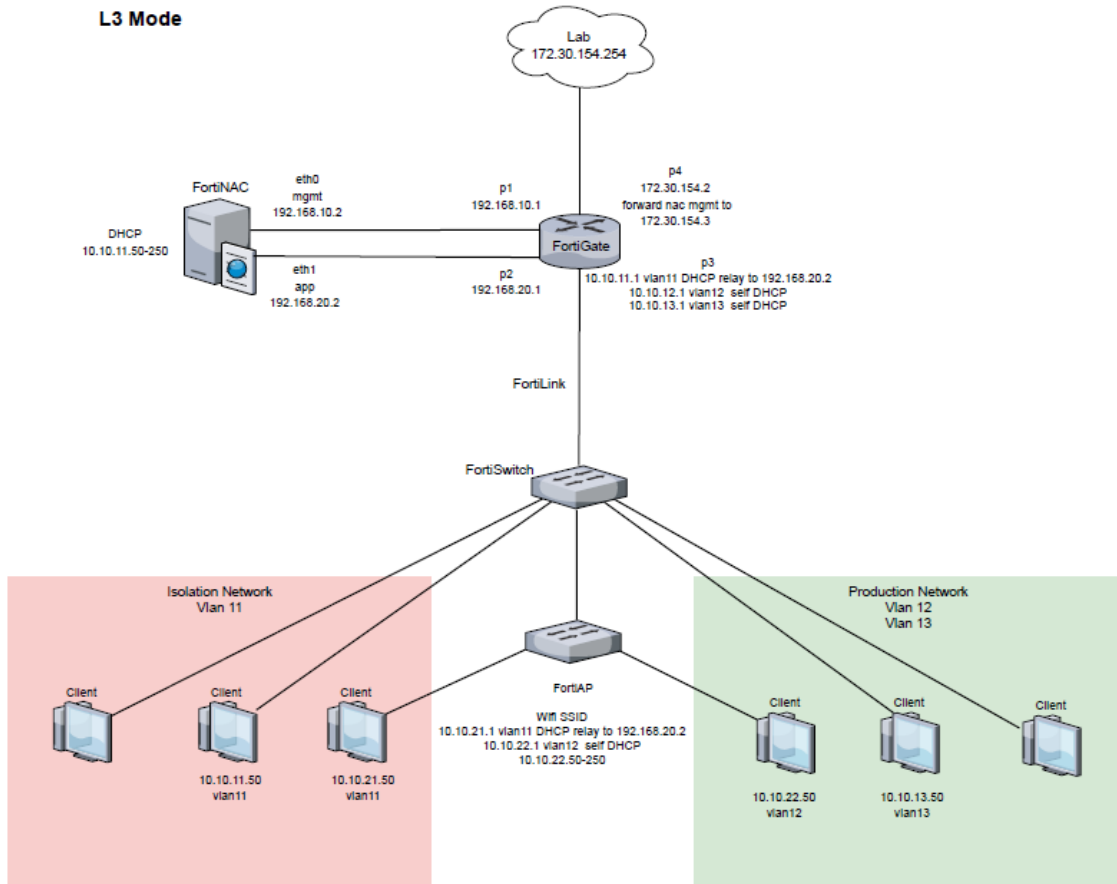
---

802.1X is a network authentication protocol that gives device access to the protected network after authentication. The verification is done through identifying the opened port through RADIUS server. Microsoft Entra ID Authentication intended to authenticate the 802.1X network protocol through the use of Microsoft Entra ID account.

## Prerequisite

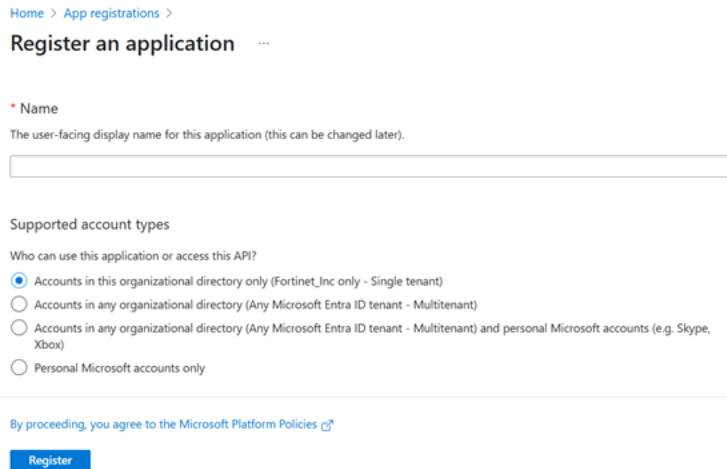
Before proceeding with Microsoft Entra ID Authentication, please configure TLS Service configuration in [2. FortiNAC Local RADIUS TLS Service Configuration on page 42](#).

Here is the use case diagram of the this authentication using 802.1x with TTLS-PAP:

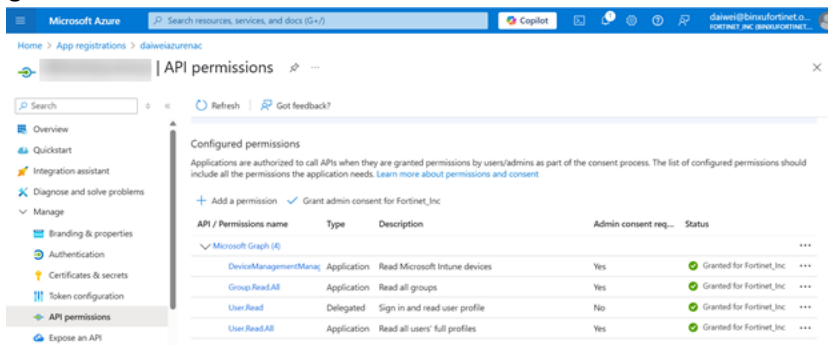


## 1. Create and Register FortiNAC Application in Microsoft Entra ID

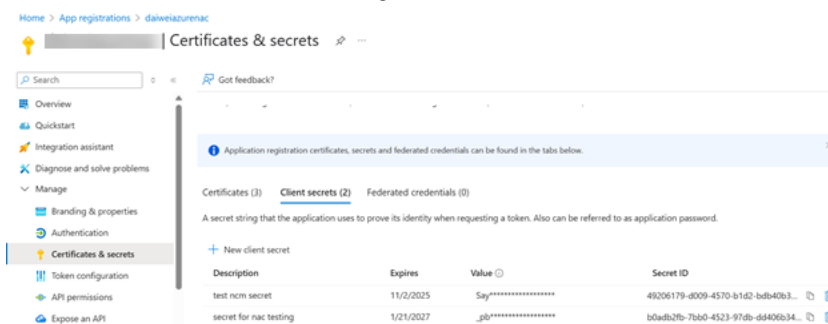
1. Log into Microsoft Entra ID, go to **App Registration**.
2. Fill in a name and choose a supported account types and click **Register**.



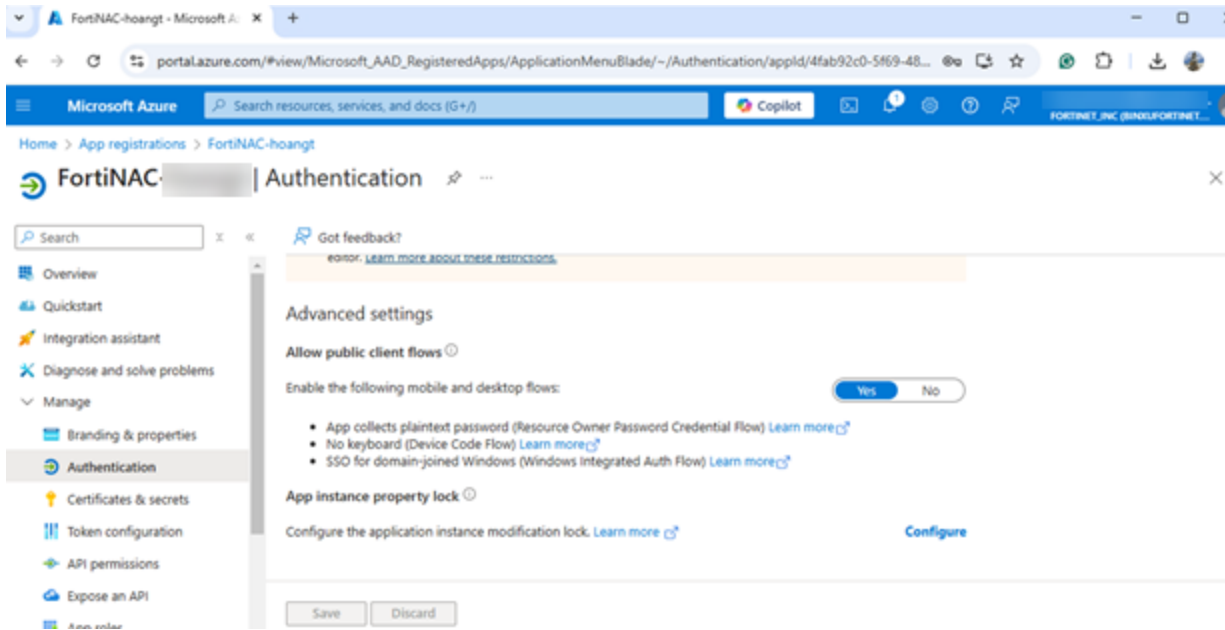
3. After the app is created, go to the app > Manage > API Permission.
4. Click +Add a Permission to grant permission of the following: (all types should be **Application**)
  - a. DeviceManagementManagedDevices.Read.All
  - b. Group.Read.All
  - c. User.Read.All
  - d. GroupMember.Read.All
  - e. Directory.Read.All
  - f. User.Read
  - g. User.Read.AI



5. Go to **Certificate \$ Secrets**, and generate Client Secrets or Certificate.



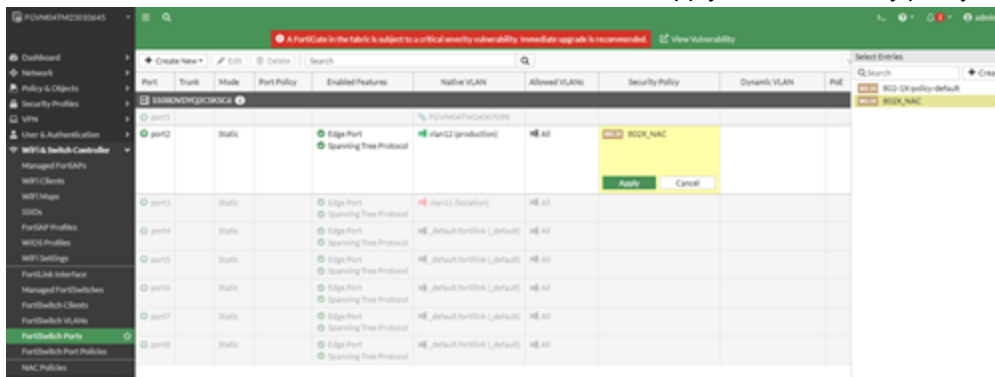
6. After the FortiNAC app is created. In the FortiNAC app, go to Manage > Authentication.
7. In the **Advanced Settings > Allow public client flows section**, click **Yes** to enable the following mobile and desktop flows.
8. Go to **Manage > Authentication**, click **Yes** to enable mobile and desktop flows in.



## 2. FortiGate Configuration

In order to prepare FortiGate for dot1x authentication, security policy needs to be configured on the FortiSwitch port (port 2) which 802.1x windows client is connected.

1. Go to **Wifi & Switch Controller > FortiSwitch Ports**, then apply 802.1.x security policy on port 2.



2. Here is an example of a 802.1x security policy:

**Edit FortiSwitch Security Policy**

Name: 802X\_NAC

Security mode: **Port-based** | MAC-based

User groups: RADIUS

Guest VLAN:

Guest authentication delay: 30 second(s)

Authentication fail VLAN:

MAC authentication bypass:

EAP pass-through:

Override RADIUS timeout:

**OK** | Cancel

- After the FortiSwitch configuration, Radius that connects to FortiNAC also needs to be configured. Go to **User & Authentication > RADIUS server**, select **PAP** method. Then click **Test Connectivity** to test the connectivity to the Radius Server. Make sure the Connection status is "Successful".

FGVM04TM23010645

**A FortiGate in the fabric is subject to a critical severity vulnerability. Immediate upgrade is recommended.**

**Edit RADIUS Server**

Name: FAC\_RADIUS

Authentication method: Default | **Specify**

NAS IP: [Redacted]

Include in every user group:

**Primary Server**

IP/Name: 192.168.2.2

Secret: [Redacted]

Connection status:  Successful

Test Connectivity

Test User Credentials

**Secondary Server**

IP/Name: [Redacted]

Secret: [Redacted]

Test Connectivity

Test User Credentials

**OK** | Cancel



Alternatively to fill in variables for Certificate type authentication, follow the steps in [Generate Certificate for Microsoft Entra ID in FortiNAC Service Connector \(Optional\)](#) on page 16. Only one authentication type is required.

## Microsoft Entra ID Mappings Configuration

1. Go to **Network > RADIUS > Virtual Servers**, then create a new Microsoft Entra ID Mapping which uses the Authentication Source named "FortiNAC-app" created above.

The screenshot shows the FortiNAC interface. The left sidebar is expanded to 'Network > RADIUS'. The main area displays 'Virtual Servers' with a table of configurations. Below this, there is a 'Domain Mappings' section with a table.

Name	TLS Service Configuration	EAP Types	Winbind Domains	Proxy Servers	Proxy Pool Type
DefaultConfig	RADIUS EAP	PEAP,MD5,GTC,MSCHAPv2	All	N/A	N/A
FNAC_App_Radius	FNAC_App_TLS	TLS,TTLS	None	N/A	N/A

Domain	Microsoft Entra ID Application
binuxfortinet.onmicrosoft.com	FortiNAC-app

2. Edit the RADIUS Servers Configuration Details and Authentication source of the virtual servers and enable TLS and TTLS in **Supported EAP Types**.

**RADIUS Server Configuration Details**

Name

Type

TLS Configuration

Supported EAP Types  TLS   
 TTLS   
 PEAP   
 TEAP   
 MD5   
 GTC   
 MSCHAPv2   
 FAST

Winbind Domain(s)  Allow Any   
 mylab   
 nacqa

OCSP Enabled

Authentication Source

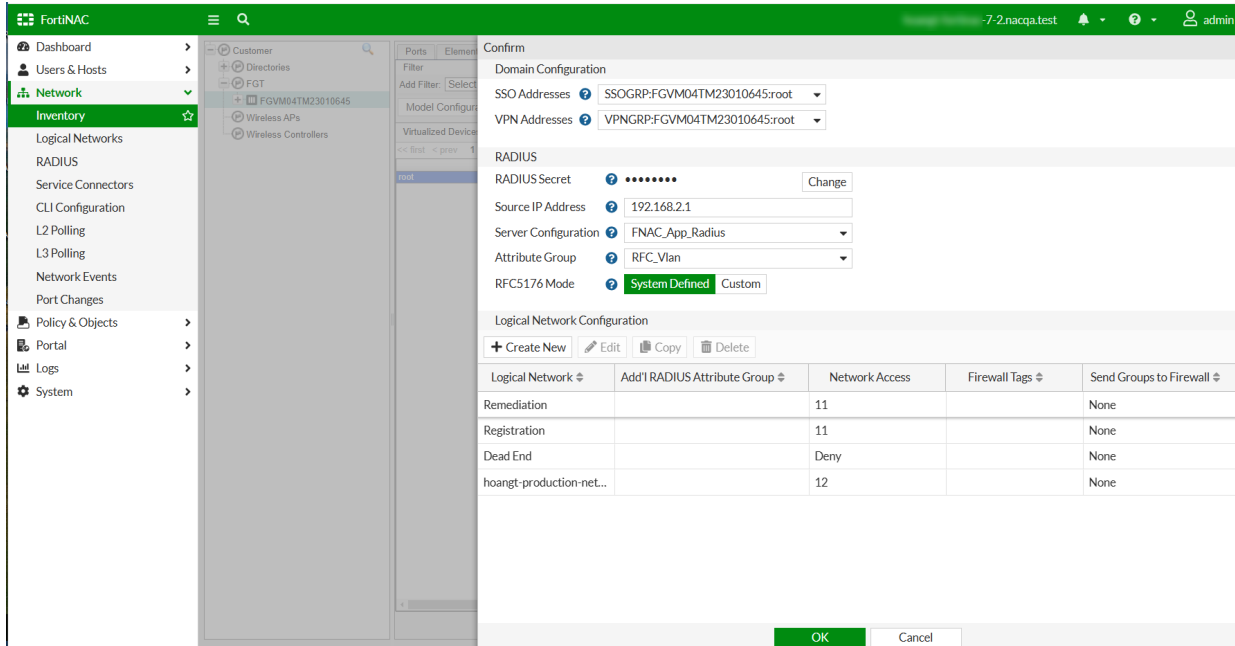
Client Certificate Attribute

Rank	Attribute
1	Common Name
2	SAN-UPN
3	SAN-DNS
4	SAN-EMAIL 4   Updated: 15:38:43 <input type="button" value="refresh"/>

3. Enable **Winbind Domains** by turning the toggle switch button "Allow Any".

## FortiGate VDOM configuration

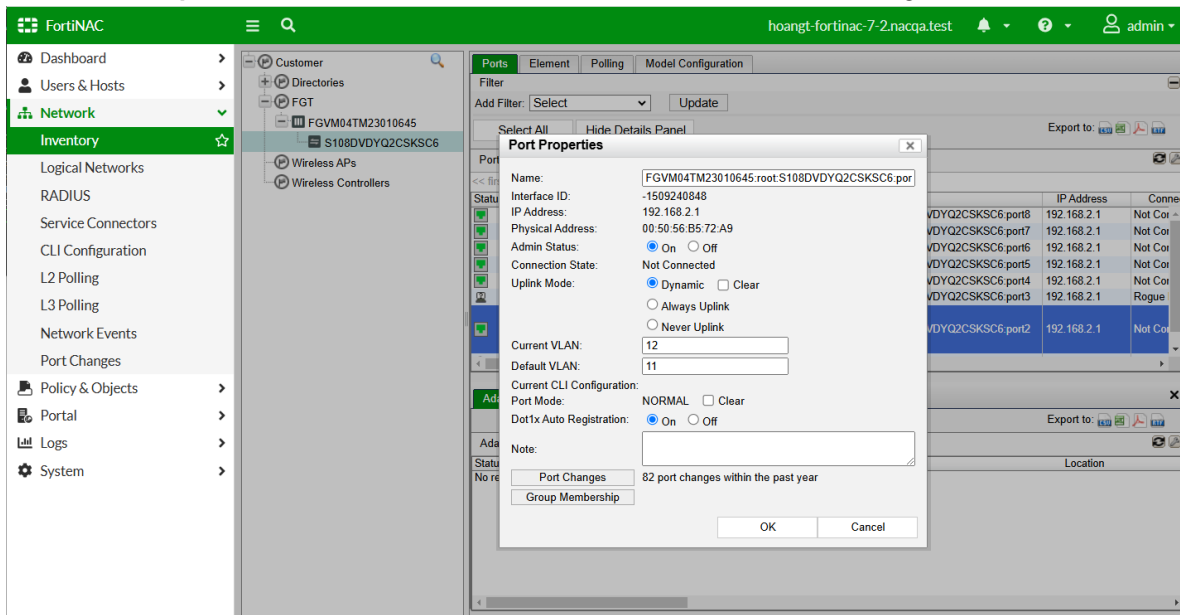
1. Go to **Network > Inventory > FGT > Virtualized Devices > root > Model Configuration** to configure the logical network configuration for Production networks.
2. Fill in IP address for the source IP address of the FortiGate interface for which FortiNAC is connected to. Make sure to test connectivity and credentials on the FortiGate and the result is successful.
3. Please make sure the correct RADIUS is used in the VDOM.
4. Configure Production VLAN is set to production vlan.



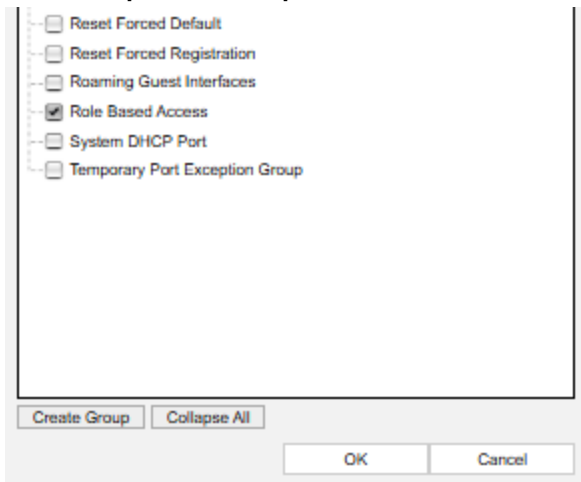
## FortiSwitch Port Configuration

Follow these steps to enable dot1x on port 2:

1. Go to **Network > Inventory > FortiSwitch port 2**
2. In the **Port Properties** window, click on **On** radio button to enable Dot1x Auto Registration.

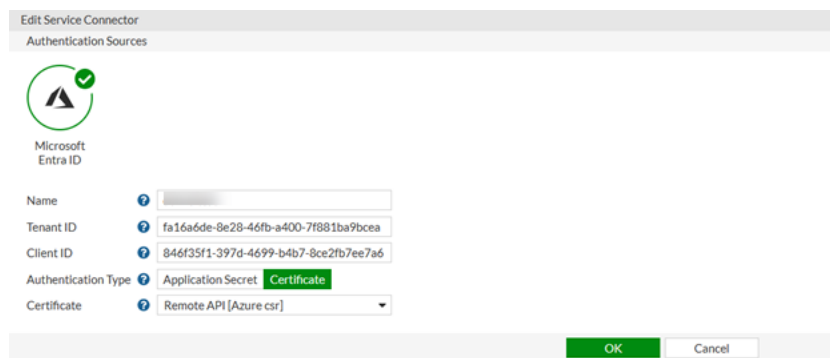


3. Click **Group Membership** button, and check **Role Based Access** button.



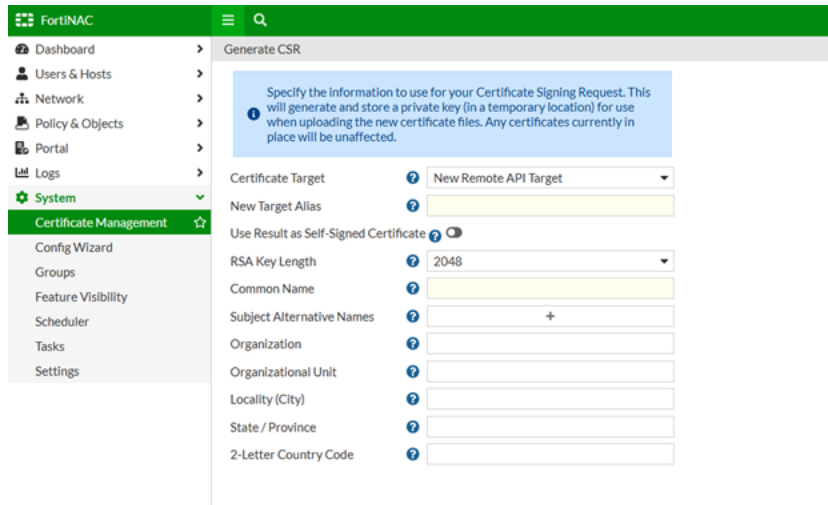
## Generate Certificate for Microsoft Entra ID in FortiNAC Service Connector (Optional)

This section will generate the certificate for Microsoft Entra ID in FortiNAC service Connector



### Step 1 - Generate new CSR on FortiNAC

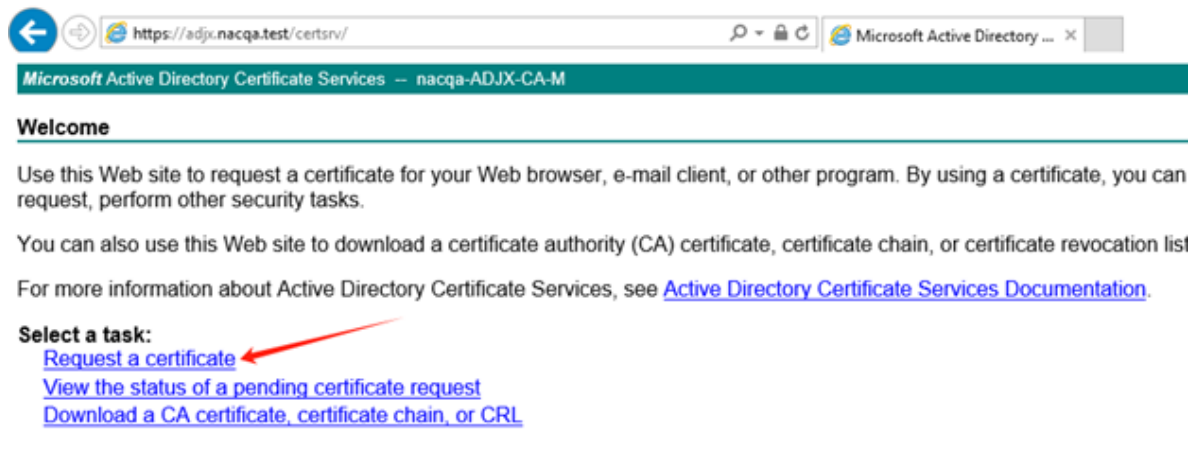
1. Go to **System > Certificate Management**, and generate a new CSR.
2. For **Certificate Target**, choose **New Remote Target**, and for **RSA key length**, fill in 2048.



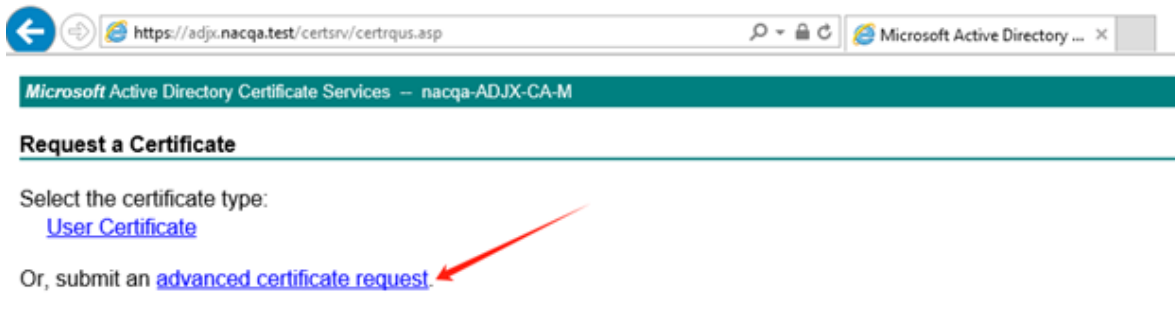
## Step 2 - Submit Certificate Request on Microsoft Active Directory

Use the CSR generated in Step 1 to submit a request for certificate in Microsoft Active Directory

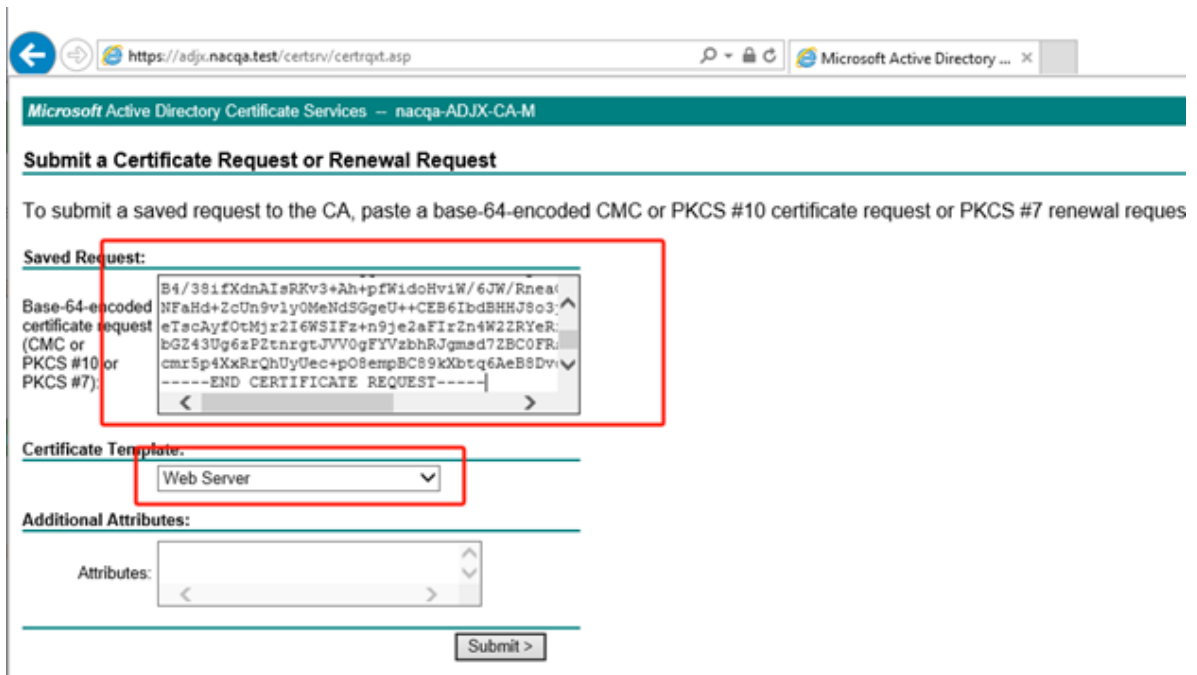
1. Open a browser to connect to Microsoft Active Directory Certificate Services, then click **Request a certificate**



2. In **Request a Certificate** page, click **advanced certificate request**.



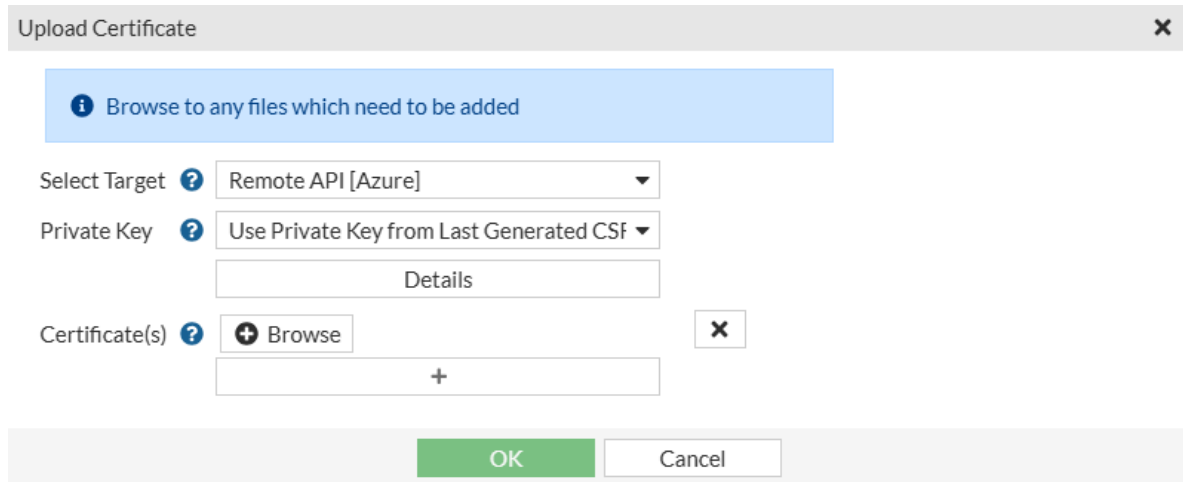
3. In **Advanced Certificate Request** page, click **Submit a certificate request by using a base 64 encoded CM**.
4. Paste the CSR generated from FortiNAC in **Base-64-encoded certificate**. In **Certificate Template**, select **Web Server**, and click **Submit**.



5. When the certificate is issued, download the certificate to the local machine.

### Step 3 - Upload the certificate onto FortiNAC

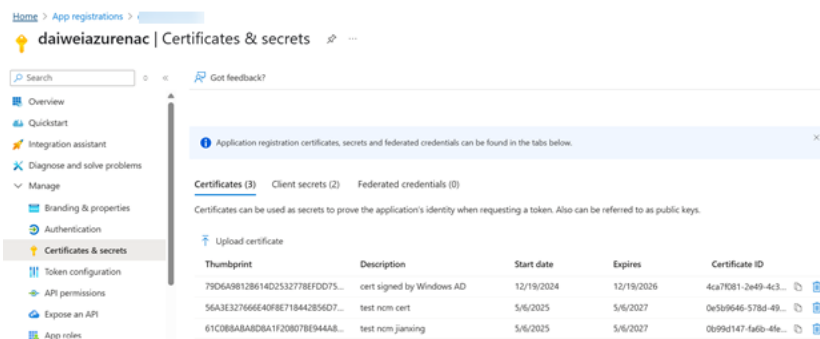
1. Log back onto FortiNAC, go to **System > Certificate Management**.
2. Click **Upload Certificate** and select "Remote API Target".
3. Browse and upload the certificate downloaded from Step 2, and click OK.



- Restart the service for the certificate to take into effect.

## Step 4 - Upload the Certificate back to Microsoft Entra ID App Registration

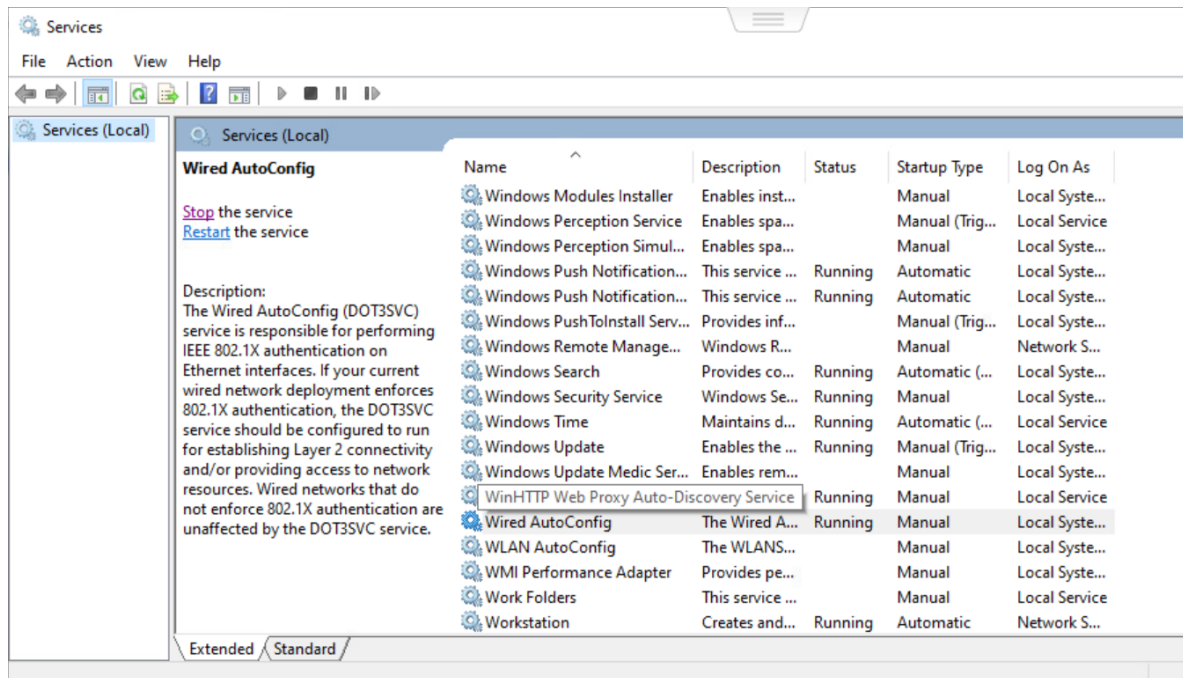
- Log into Microsoft Entra ID, and go to App Registration.



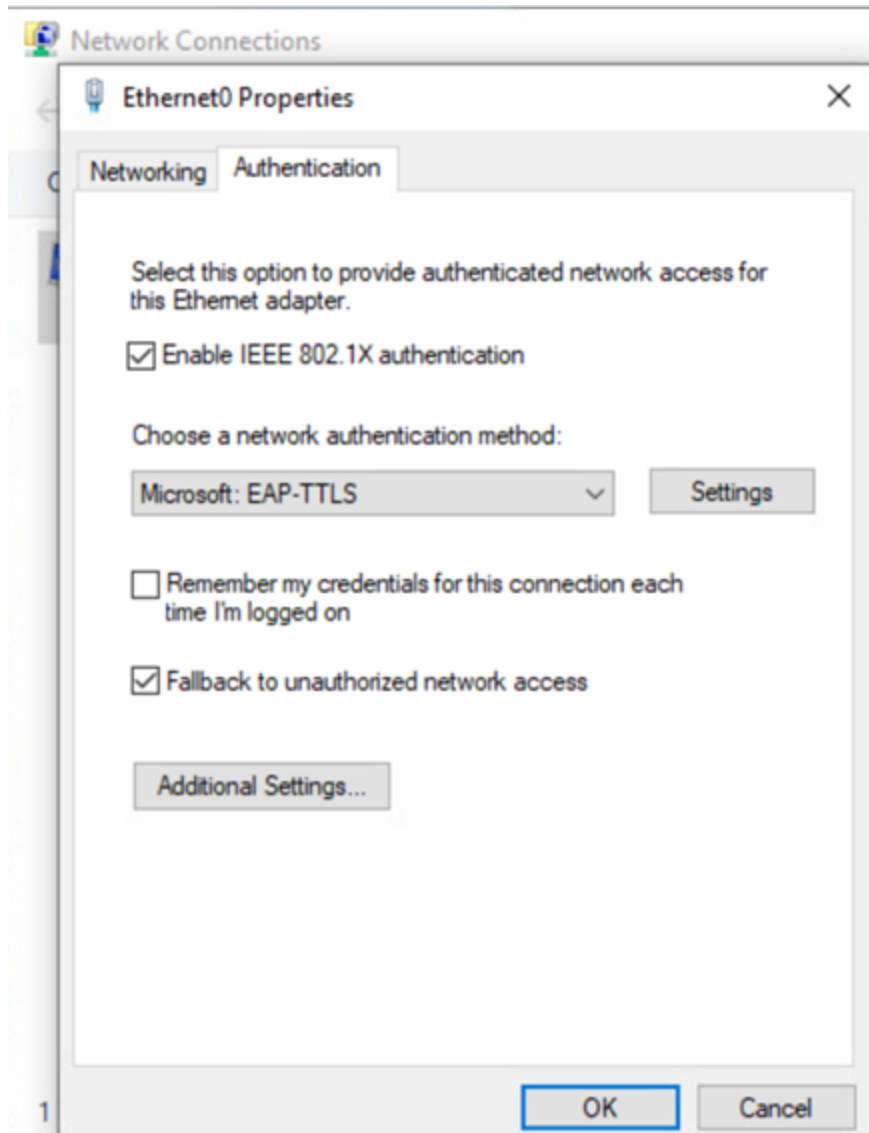
- Upload the Certificate to complete.

## 4. Windows Client

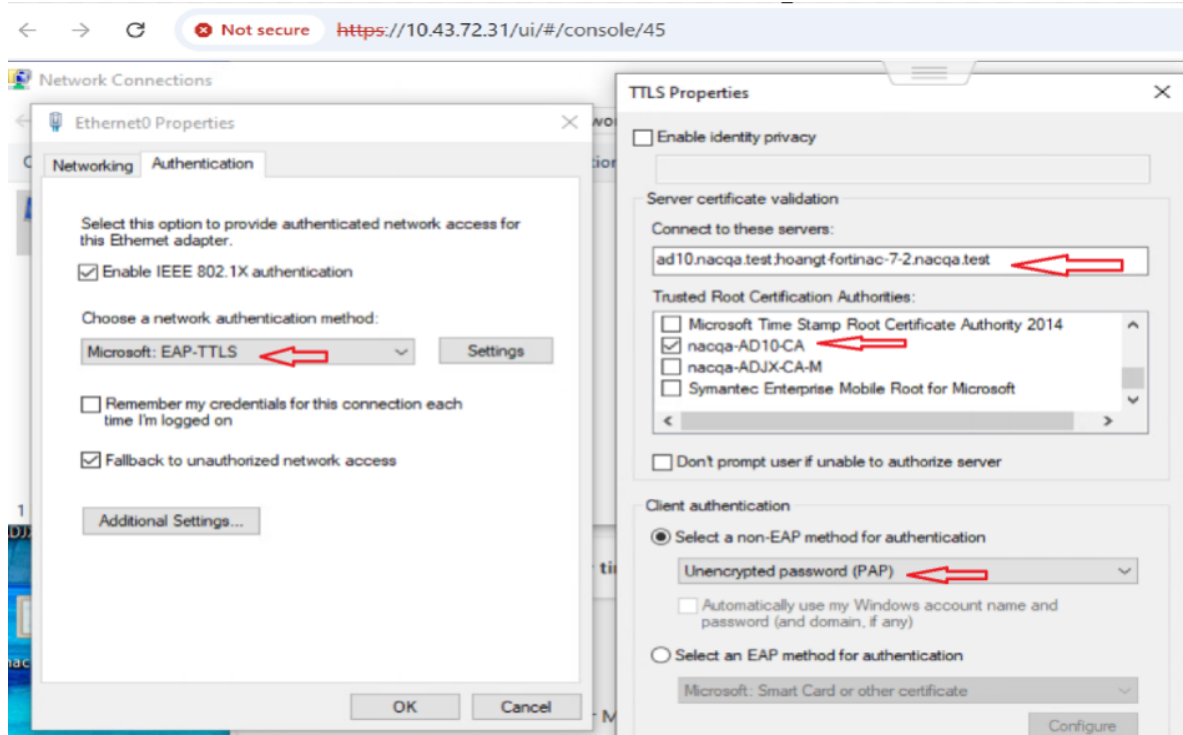
- Log into the Windows client host.
- Search for "Services", and go to Services client, and start the **Wired AutoConfig** service.



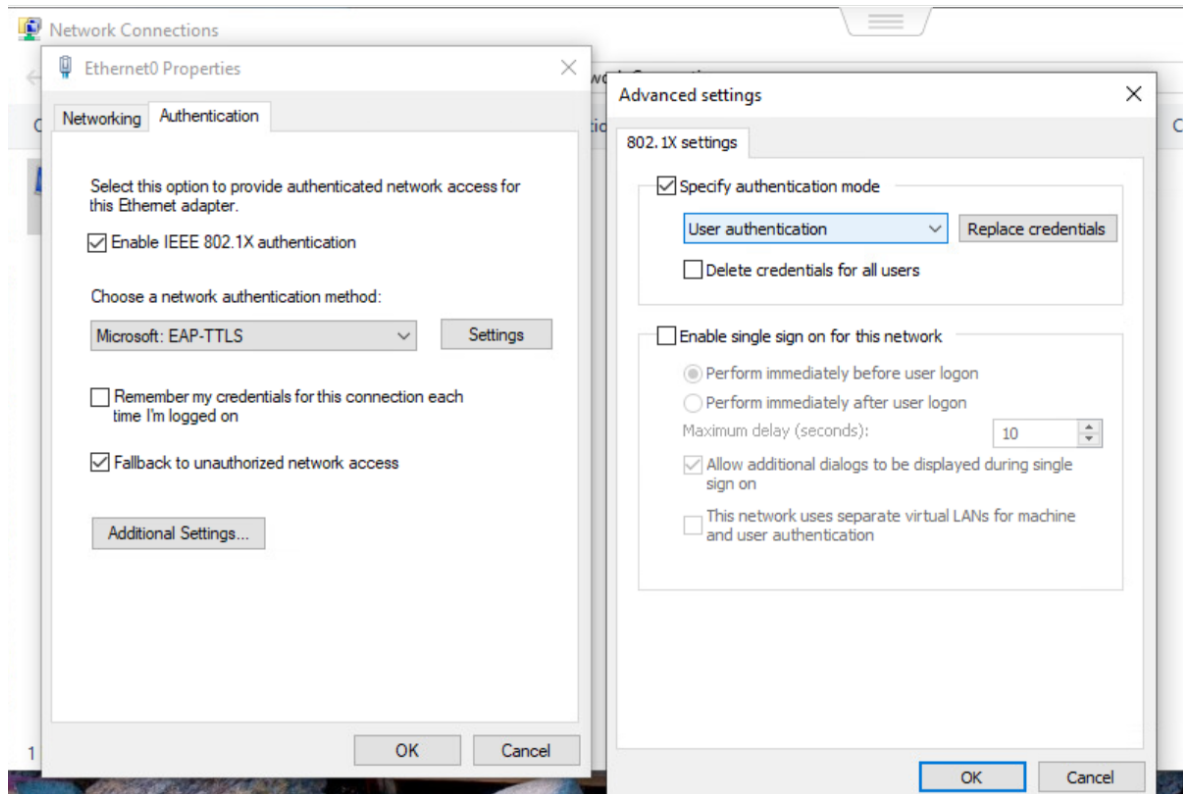
3. Open Network Connections and open the **Ethernet Properties > Authentication**.



4. Enable IEEE 802.1X authentication.
5. Click network authentication method drop down menu and choose Microsoft: EAP-TTLS, and click on Settings.
6. In the **TTLS Properties**, configure the AD and **Trusted Root Certification Authorities** for your environment. The image below is served as an example.



7. Go back to Authentication tab, click Additional Settings, click Specify authentication mode, and select User authentication.



8. On Windows Client, disable the Ethernet card and then enable it. The windows client adapter should now be authenticated and authorized.

- Open up Windows Command Line Prompt, and verify settings type: ipconfig/all

```
C:\Users\win10>ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-██████████-B5491D
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-50-56-B5-49-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::aecb:cbc0:f087:4a1f%13(Preferred)
IPv4 Address. . . . . : ██████████ (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, January 24, 2025 3:07:02 PM
Lease Expires . . . . . : Friday, January 31, 2025 3:07:03 PM
Default Gateway . . . . . : 10.10.12.1
DHCP Server . . . . . : 10.10.12.1
DHCPv6 IAID . . . . . : 100683862
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-15-73-47-00-50-56-B5-49-1D
DNS Servers . . . . . : 8.8.8.8
NetBIOS over Tcpi. . . . . : Enabled

C:\Users\win10>
```

- After the window client host is successfully authenticated, validate the client IP address is moved to production network. Open up Windows Command Line Prompt, and verify settings by typing: ipconfig/all
- In FortiNAC, the Windows machine should now appeared as one of the hosts in Hosts viewn with user registered to and logged on user attached.



Status	Host Name	Registered To	Logged On User	Host Role	Operating System	Criticality	Persistent Agent	Host Created
Registered	DESKTOP-SHARED-W...	██████████	██████████	NAC-Default	Windows 10	Low	⊗	2025/01/24 15:05:12
Registered		██████████	██████████			Low	⊗	2025/01/24 15:01:50
Registered						Low	⊗	2025/01/24 15:01:47
Registered						Low	⊗	2025/01/24 15:01:14
Registered						Low	⊗	2025/01/24 15:01:08
Registered						Low	⊗	2025/01/24 15:00:55
Registered						Low	⊗	2025/01/24 15:00:52
Registered						Low	⊗	2025/01/24 15:00:34

- From the inventory page. You can view the protocol detail. Inner EAP type is **None** is expected behavior since PAP is not an EAP type protocol.

# Microsoft Entra ID Authentication using 802.1x with TTLS-PAP

3	FGVM04TM25005006	port2	FGVM04TM25005006	root:S108DVZX-NT1WEAC:port2	10.15.35.151	User	11	12	On	Link Up	Role Based Access
5	FGVM04TM25005006	port1	FGVM04TM25005006	root:S108DVZX-NT1WEAC:port1	10.15.35.151	Learned Uplink	1	1	On	Link Up	Unenforced

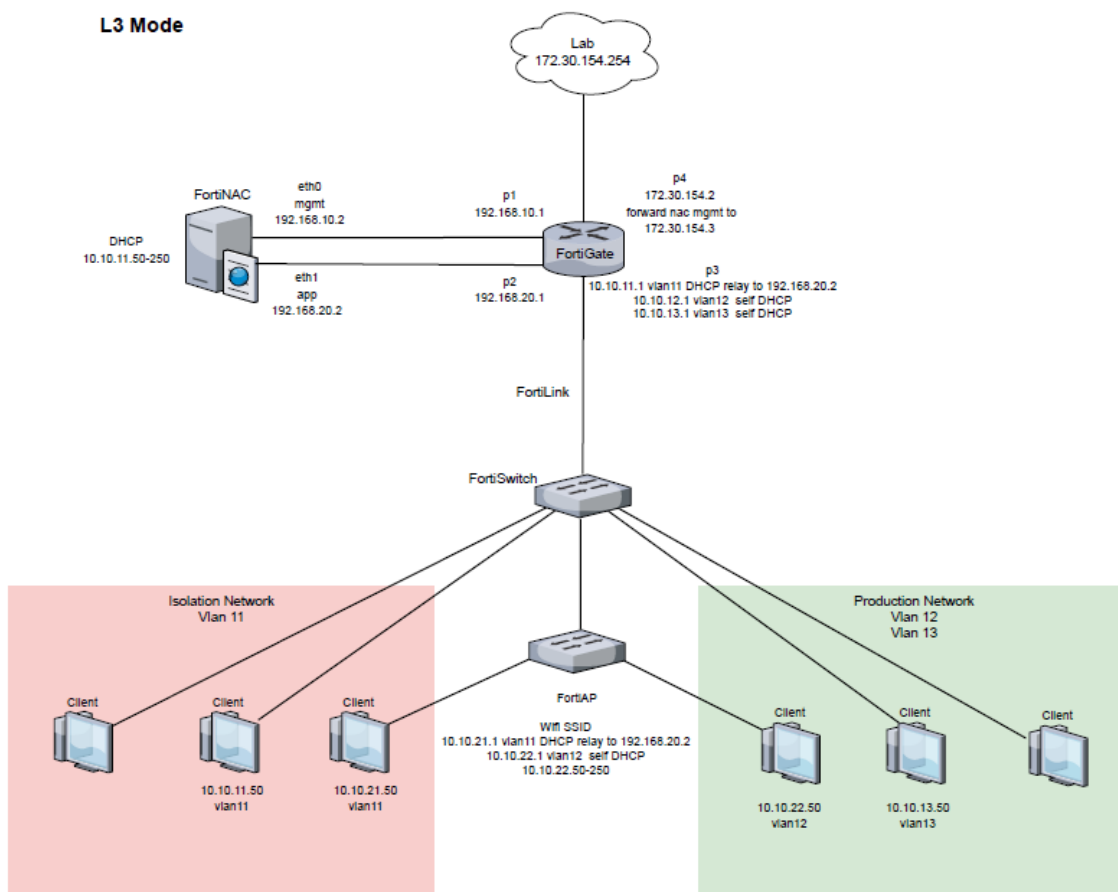
Adapters - Total: 1

Location	Connected Container	Rule Name	Media	RADIUS Auth Type	Outer EAP Type	Inner EAP Type	Access Value	Vendor Name	Machine Authentication	User Authentication
FGVM04TM25005006:root:S108DVZX-NT1WEAC:port2	dawei_fgf			802.1X	TTLS	NONE	12	VMware, Inc.		

# Microsoft Entra ID Authentication using Captive Portal

Captive Portal is FortiNAC's authentication protocol to grant device access to protected network. Microsoft Entra ID Authentication integrates the Captive Portal to streamline the authentication process. The Microsoft Entra ID users will be able to gain access promptly through the Microsoft Entra ID admin users when using Microsoft Entra ID Authentication with Captive Portal. This method is the quick and secure method to grant access to other device users within the protected network.

This is the use case diagram for the Microsoft Entra ID Authentication using Captive Portal:



# 1. Microsoft Entra ID, FortiGate, FortiNAC, and FortiSwitch Configuration

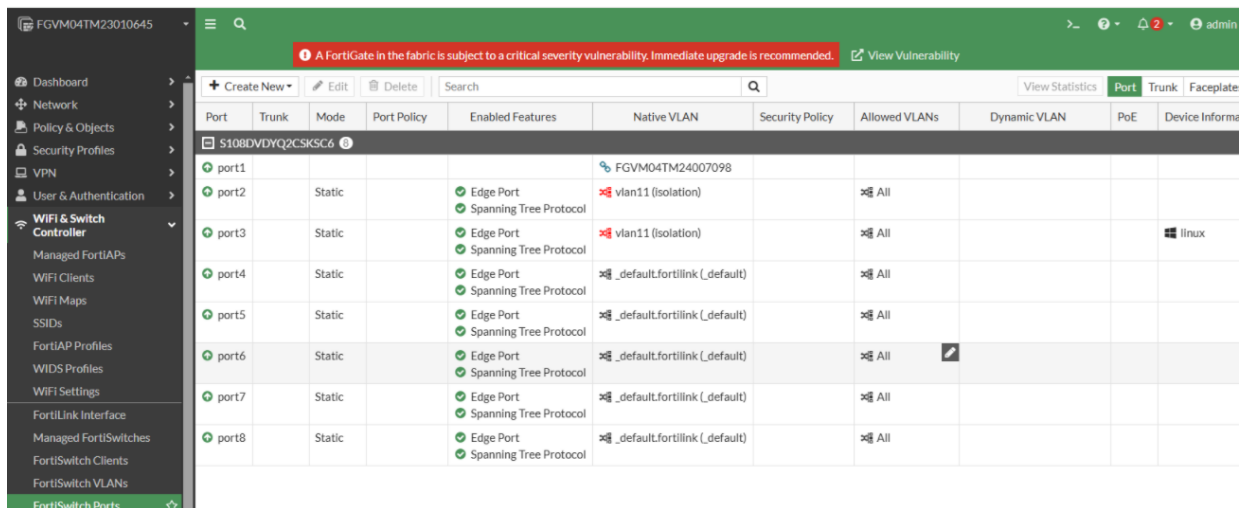
## Step 1 - Microsoft Entra ID Configuration

Follow the link to register FortiNAC application in [Microsoft Entra ID Configuration](#).

## Step 2 - FortiGate Configuration

Follow the link to configure FortiGate: [Firewall Configuration](#)

The FortiSwitch Port connecting to FortiNAC should not have security policy applied like 802.1.x.

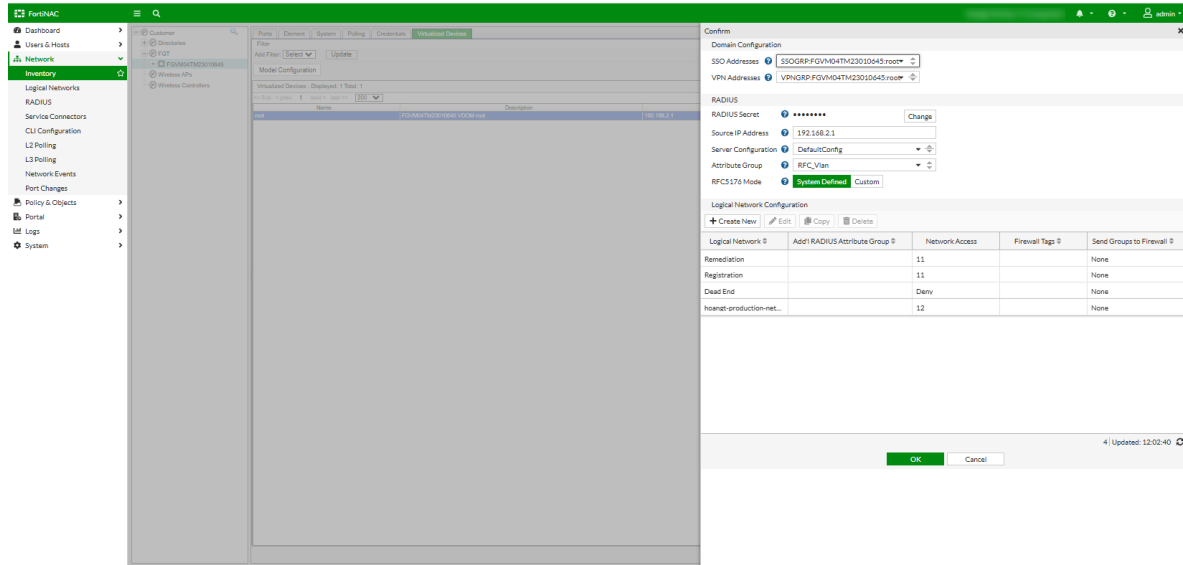


Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Security Policy	Allowed VLANs	Dynamic VLAN	PoE	Device Informa
port1				Edge Port Spanning Tree Protocol	FGVM04TM24007098		All			
port2		Static		Edge Port Spanning Tree Protocol	vlan11 (isolation)		All			
port3		Static		Edge Port Spanning Tree Protocol	vlan11 (isolation)		All			linux
port4		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)		All			
port5		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)		All			
port6		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)		All			
port7		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)		All			
port8		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)		All			

For Radius, make sure the test connectivity is successful. In the example below, 192.168.2.2 is the IP address of the interface on FortiNAC.

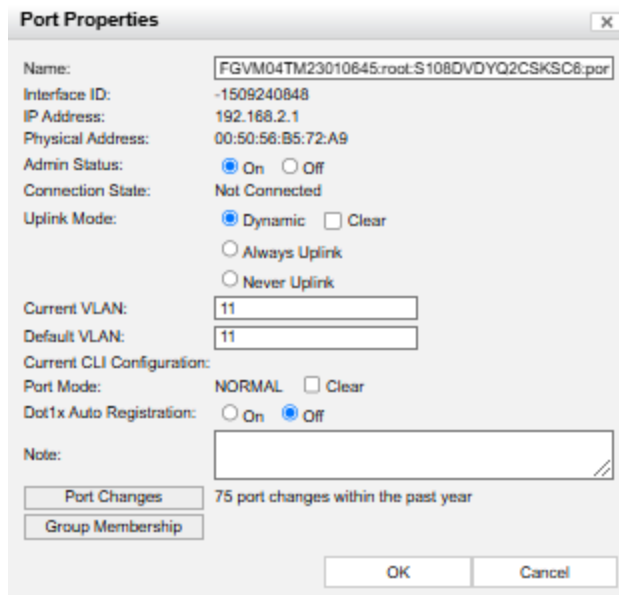


- For RADIUS configuration: go to Network > Inventory, in our example, make sure the connection to FortiGate is successful, and remediation/registration is set to enforce and vlan 11. Lastly, Production vlan is set to 12.

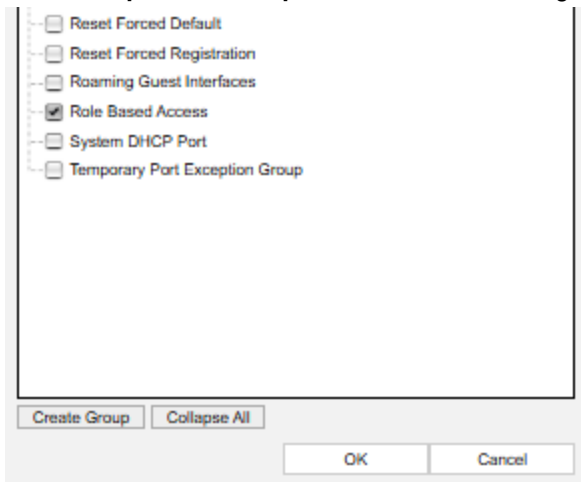


## Step 4 - FortiSwitch Port Configuration

- Go to **Network > Inventory > FortiSwitch port 2**.
- Click **Off** radio button to disable Dot1x Auto Registration.




3. Click **Group Membership**, and check the following in Group Membership.



## Step 5 - Service Connectors Configuration

1. Go to **Network > Service Connectors** and create a new Authentication Source. In this example, it will be called "portal"

Authentication Sources



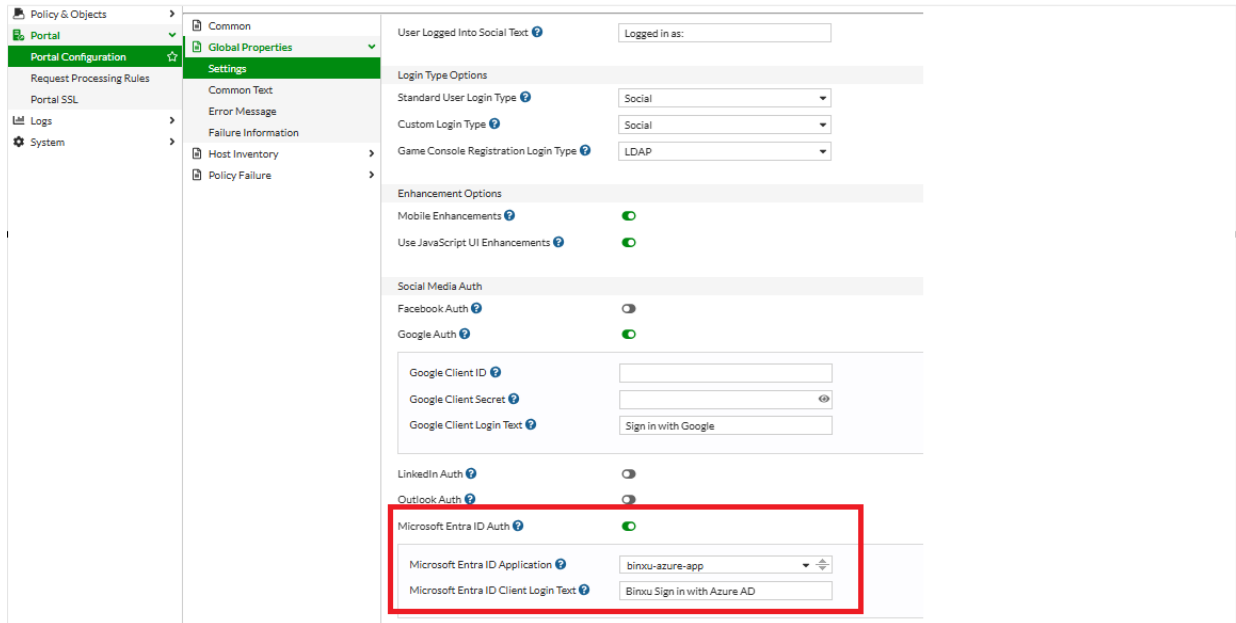
Microsoft  
Entra ID

Name	?	portal
Tenant ID	?	fa16a6de-8e28- <span style="background-color: #ccc; color: #888;">[REDACTED]</span>
Client ID	?	1c481e57-de19- <span style="background-color: #ccc; color: #888;">[REDACTED]</span>
Authentication Type	?	Application Secret <span style="background-color: #008000; color: white; padding: 2px 5px;">Certificate</span>
Certificate	?	Remote API [azurenew] <span style="font-size: 0.8em;">▼ ▲ ↻</span>
Import Groups From Microsoft Entra ID		<input type="checkbox"/>
Sync Groups Automatically		<input type="checkbox"/>
Delete Users No Longer Found on Sync	?	<input type="checkbox"/>

2. Fill in all the information of the Microsoft Entra ID environment: Microsoft Entra ID information and Application Secret.

## Step 7 - Portal Configuration

Go to **Portal > Portal Configuration > Configuration > Global > Global Properties > Settings**, and enable Microsoft Entra ID Auth and select the Microsoft Entra ID service connector created earlier, in this example, it will be "portal", and create a client Login text.



Continue to [2. Windows Client Configuration on page 31](#) to finish up with the rest of the configurations.

## 2. Windows Client Configuration

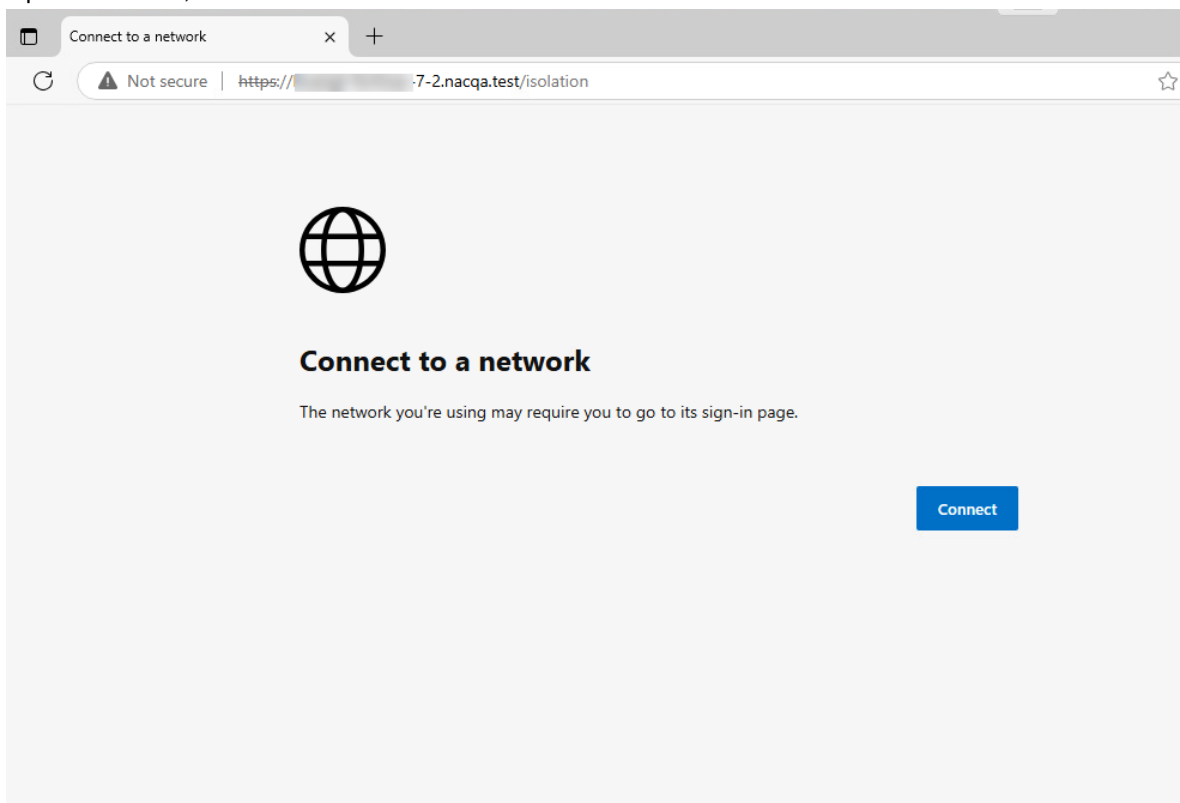
### Step 1 - Disable dot1x on Host

1. Log into the Windows client machine.
2. Go to **Network Connections** and open **Ethernet Properties > Authentication**.
3. Deselect **Enable IEEE 802.1X authentication** to disable dot1x on the host
4. Search for "Services", and go to **Services** client.
5. Stop the **Wired AutoConfig** service if it is running.

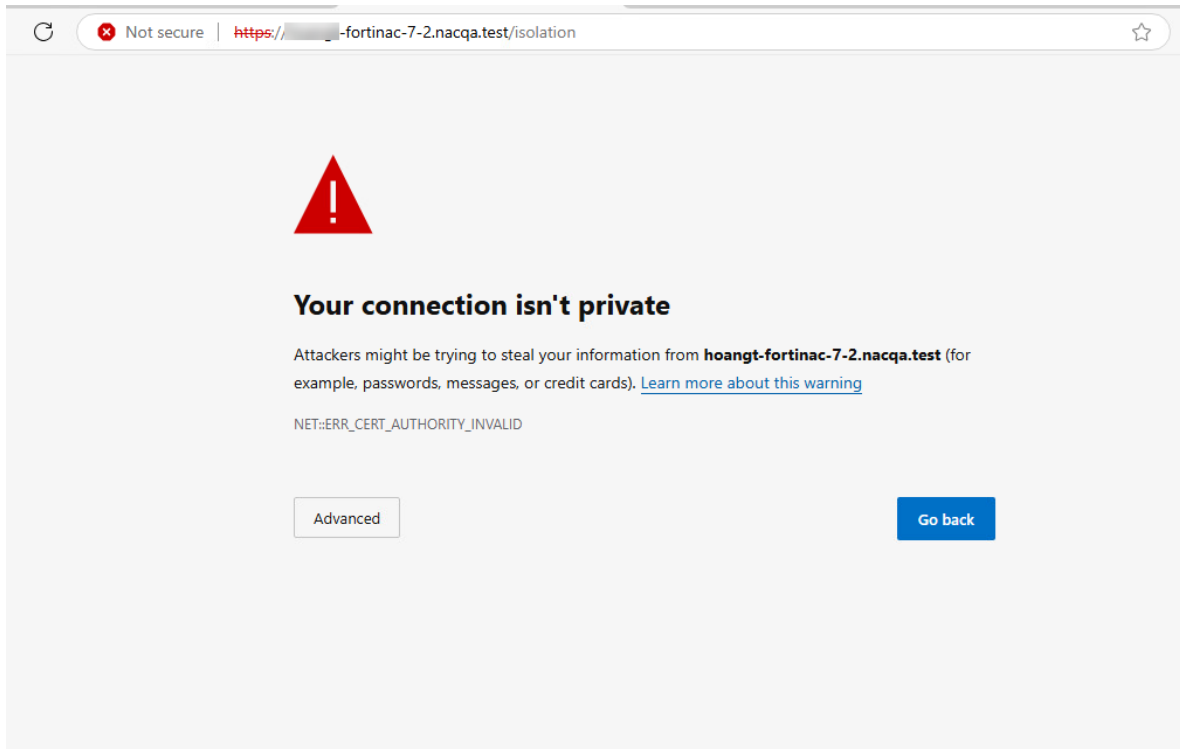
### Step 2 - Connect to the Network

Before configure windows on the client machine, delete all the cache and history to have a smooth test run.

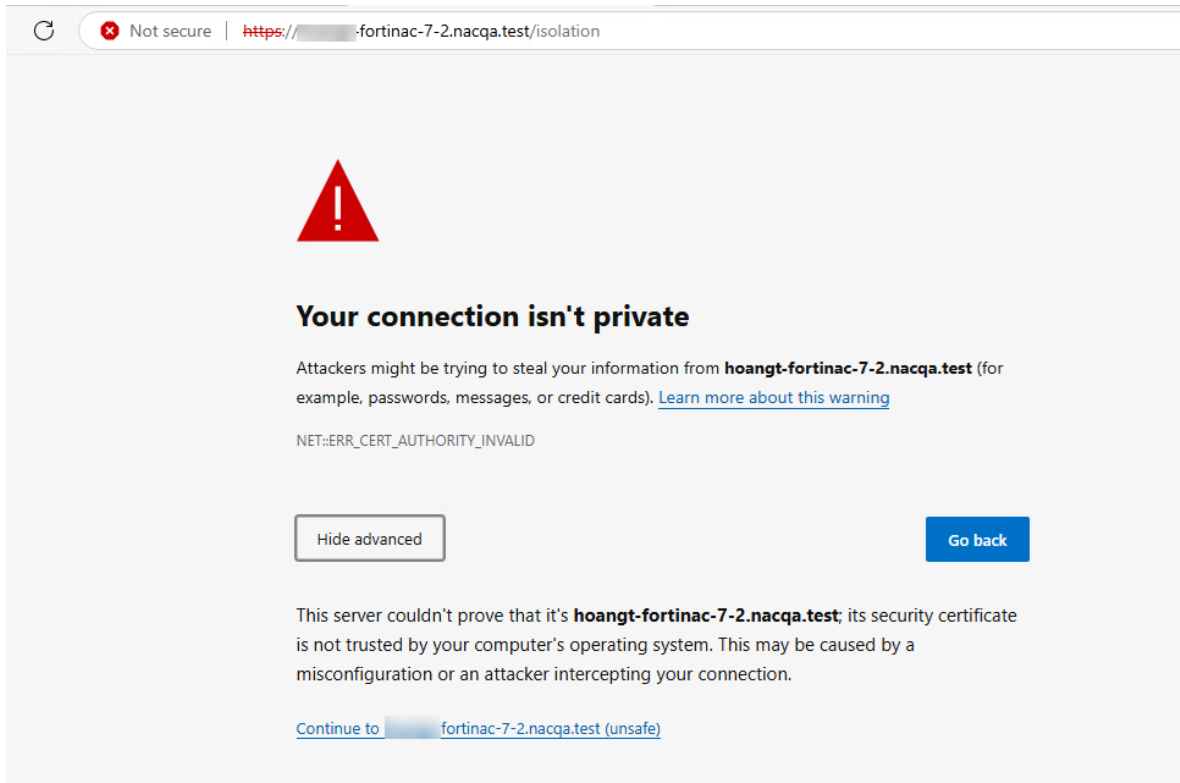
1. Go to **Network and Internet > Network and Sharing Center > View Network** and click on **Change adapter settings**.
2. Disable and enable the Ethernet card to trigger the authentication using Captive Portal.
3. Open a browser, and click **Connect**.



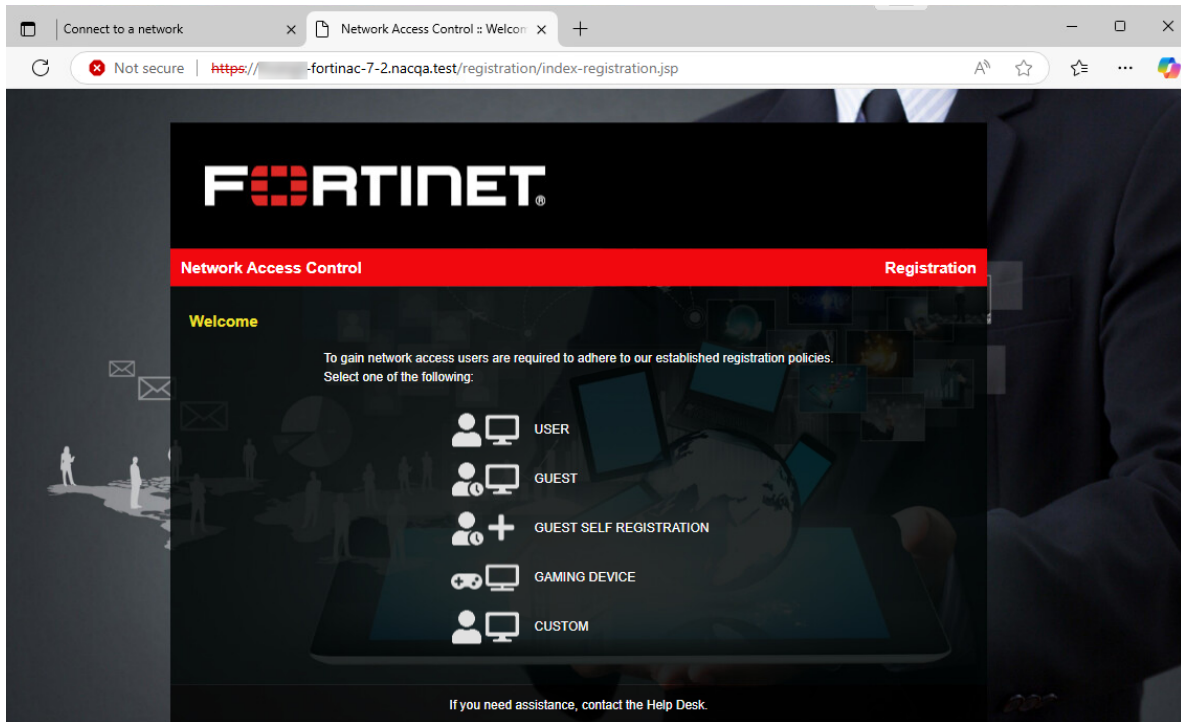
4. The browser would state the connection is not private, then click **Advanced**.



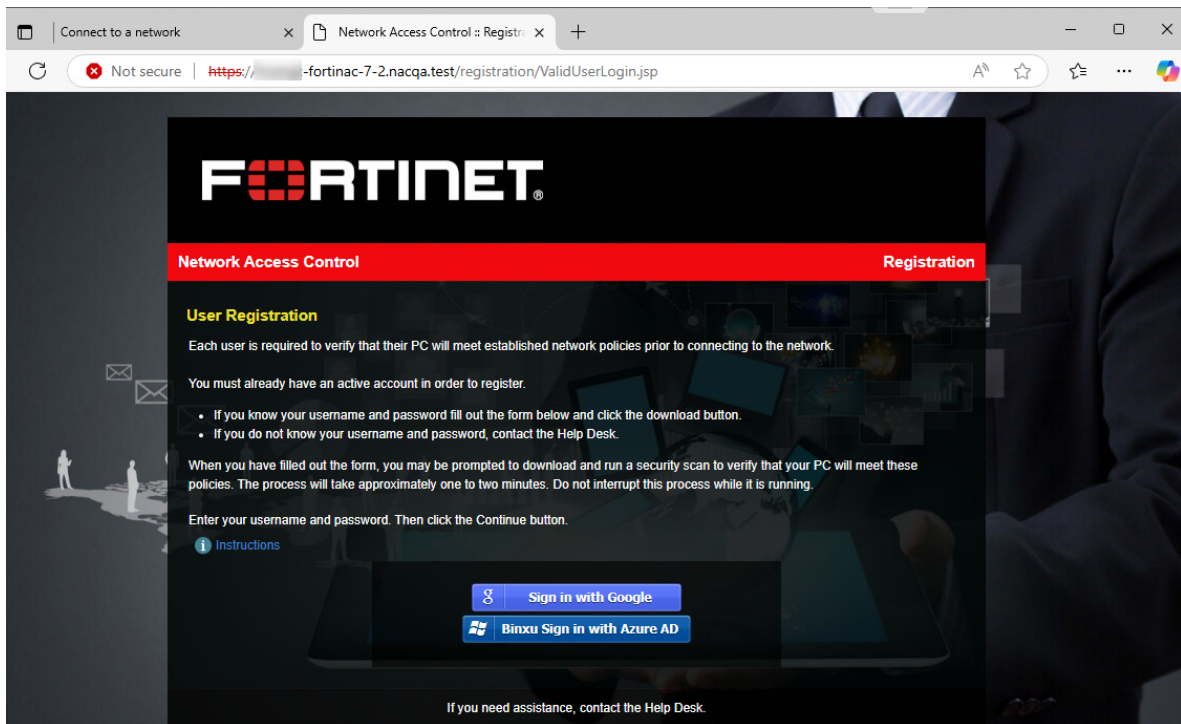
5. Then click the Continue link to trigger the Captive Portal.



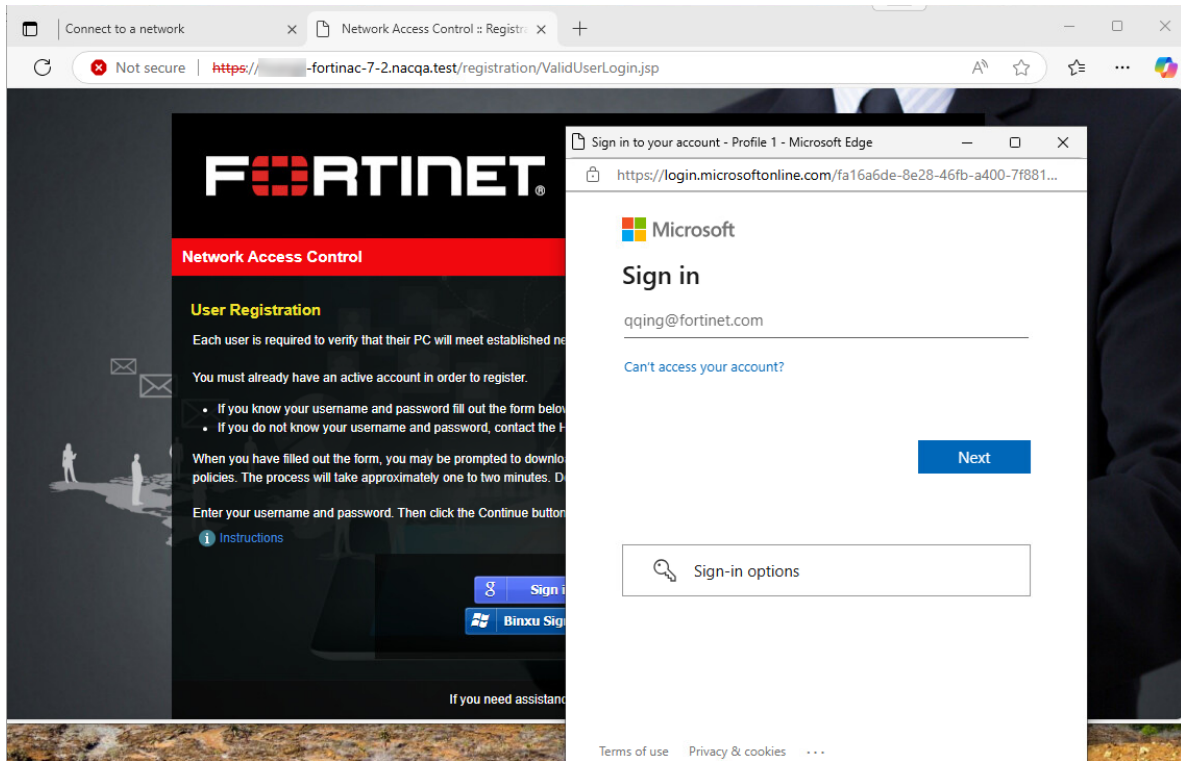
6. Wait until the Captive Portal show up, then click **User**.



7. Then click the Microsoft Entra ID signin button, in this example, customer can sing in with the Azure AD account.



8. A Login windows would popup, login with the Microsoft Entra ID account.



# Microsoft Entra ID Authentication using TLS Certificate

## Overview

Digital Certificate authentication ensure that only trusted devices and users can connect to their network as well as confirm the authenticity of a website to a web browser, also known as SSL certificate. Digital certificate requires a copy of a public key from the certificate holder, which needs to be matched the a corresponding private key to verify its identity. A public key certificate should be issued by the certificate authority(CA) to verify the identity.

## 1. Generate TLS certificate for Microsoft Entra ID to do authentication

There are multiple ways to generate TLS certificate for Microsoft Entra ID to do the authentication.

### Method 1:

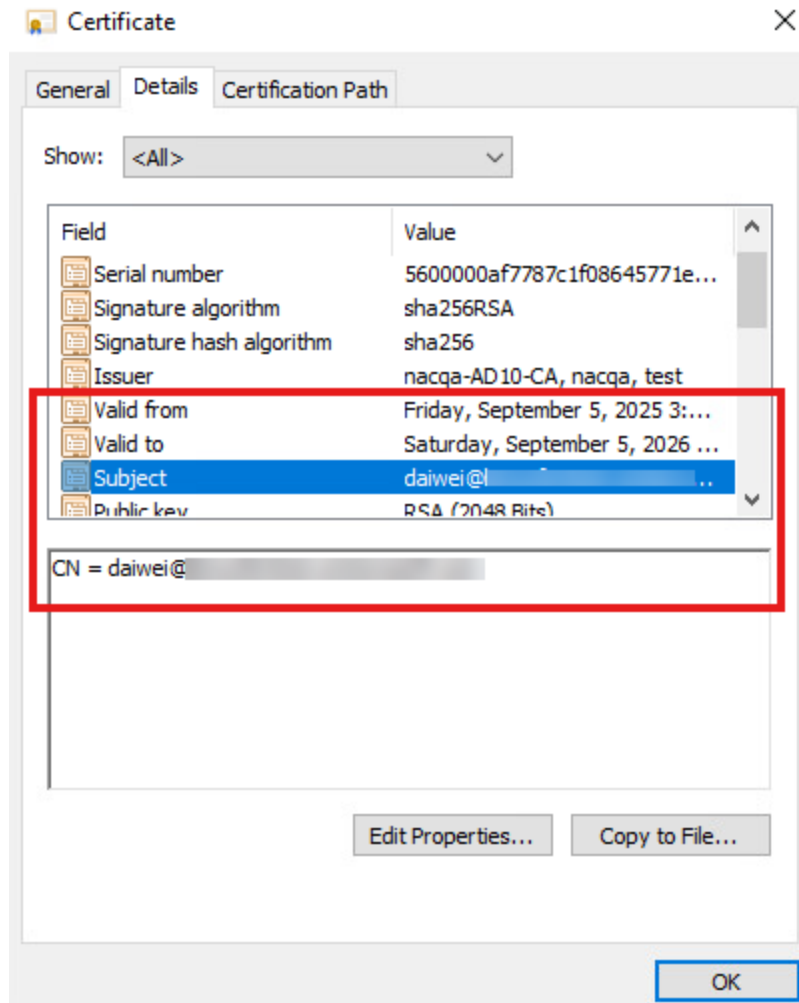
Users can generate the CSR by themselves and configure the value of CN/SAN-DNS/SAN-UPN/SAN-Email as the UPN(User Principal Name) of the Microsoft Entra ID user account.

Here is the UPN of the Microsoft Entra ID user account.

The screenshot shows the 'Overview' tab of a user profile in Microsoft Entra ID. The user's name is 'DZ' and their role is 'Member'. The 'User principal name' field is highlighted with a red box and contains the value 'daiwei@l...'. Other fields include Object ID, Created date time, User type, Identities, and Agent ID. On the right side, there are links for Group memberships (10), Applications (9), Assigned roles (3), and Assigned licenses (2).

Field	Value
User principal name	daiwei@l...
Object ID	9ca253a6-75f2-442b-ba66-e2cdb700b30e
Created date time	Aug 27, 2020, 4:20 PM
User type	Member
Identities	binxufortinet.onmicrosoft.com
Agent ID	

Group memberships	10
Applications	9
Assigned roles	3
Assigned licenses	2



## Method 2:

The second method is using Microsoft Intune to generate TLS certificate. Here are some reference links from Microsoft Official site:

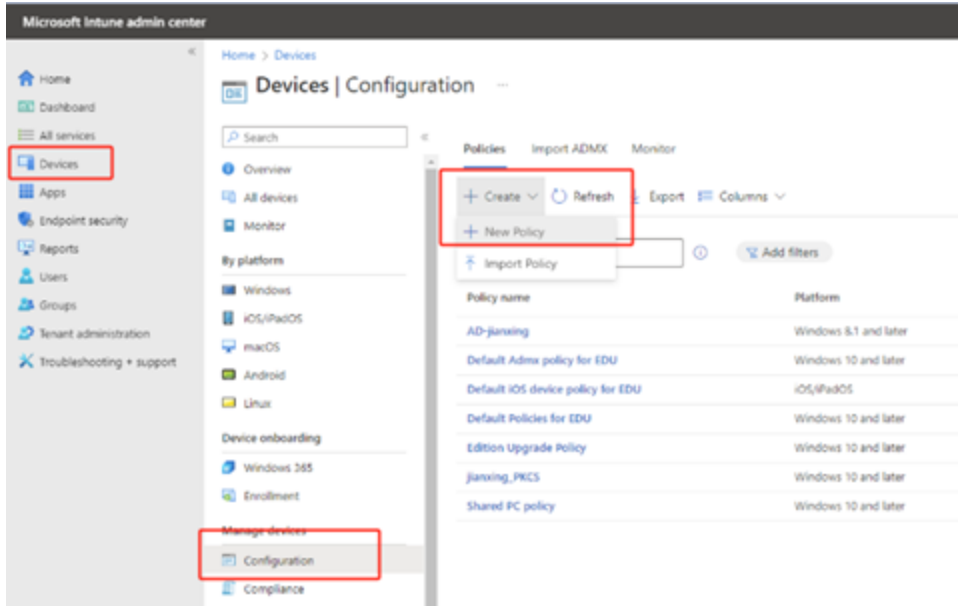
[Use a PKCS certificate profile to provision devices with certificates in Microsoft Intune](#)

[Install the Certificate Connector for Microsoft Intune](#)

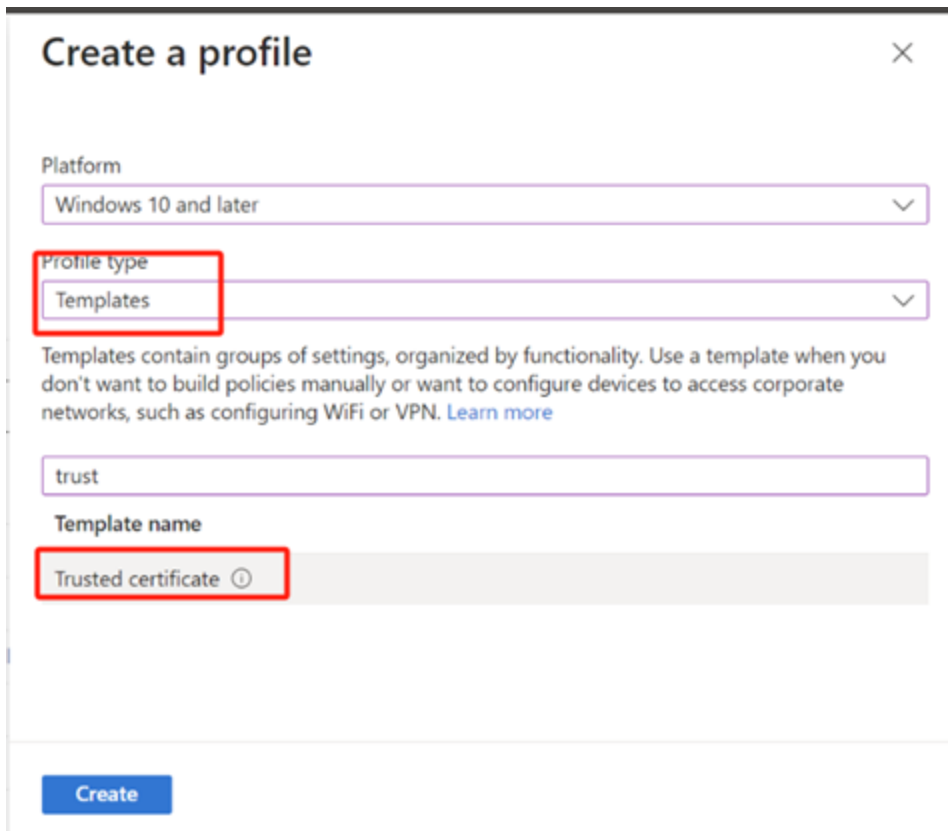
[Troubleshoot use of PKCS certificate profiles to provision certificates with Microsoft Intune](#)

### Step 1 - Configure Trust Certificate Profile

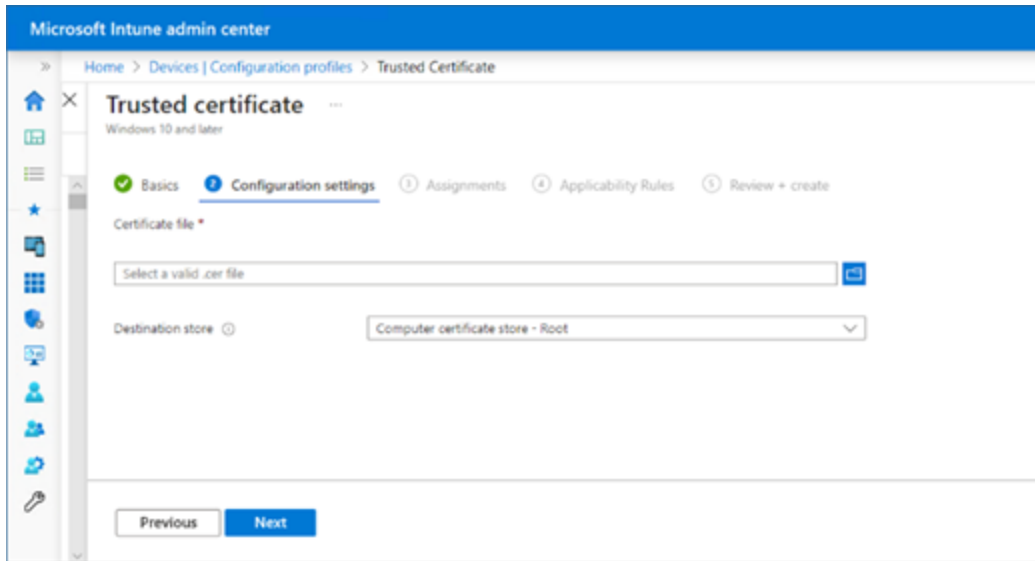
1. Go to [Microsoft Intune Admin Center](#)
2. Go to **Device > Configuration**
3. Under **Profile** tab, click **Create** and select **New Policy**.



4. Set **Platform** as “Windows 10 and later”, profile type as “Template”, and Template name as ” Trusted certificate”.



5. Select the root certificate you exported from CA.



## Step 2 - Configure PKCS certificate profile

1. In the **PKCS Certificate** profile, go to the **Basics** tab.

[Home](#) > [Devices | Configuration](#) > [Daiweitest](#) >

### PKCS certificate

Windows 10 and later

- 1 Basics**   2 Review + save

Name *	Daiweitest
Description	
Platform	Windows 10 and later
Profile type	PKCS certificate

2. In **Configuration settings**, set CN/SAN-DNS/SAN-Email/SAN-UPN format as `{{UserPrincipleName}}`

Home > Devices | Configuration > Daiweitest >

### PKCS certificate

Windows 10 and later

Configuration settings Review + save

Renewal threshold (%) \* 20

Certificate validity period \* Years 1

Key storage provider (KSP) \* Enroll to Trusted Platform Module (TPM) KSP if present, otherwise Software K...

Certification authority \*

Certification authority name \*

Certificate template name \* TESTPKCS

Certificate type \* User

Subject name format \* CN={{UserPrincipalName}}

Subject alternative name

Attribute	Value
URI	ID:Microsoft Endpoint ManagerGUID:{{DeviceId}}
DNS	{{DeviceId}}
User principal name (UPN)	{{UserPrincipalName}}
Email address	{{UserPrincipalName}}

Extended key usage

Name	Object Identifier	Predefined values
Client Authentication	1.3.6.1.5.5.7.3.2	Client Authentication (1.3.6.1.5.5.7.3.2) ...
Not configured	Not configured	Not configured

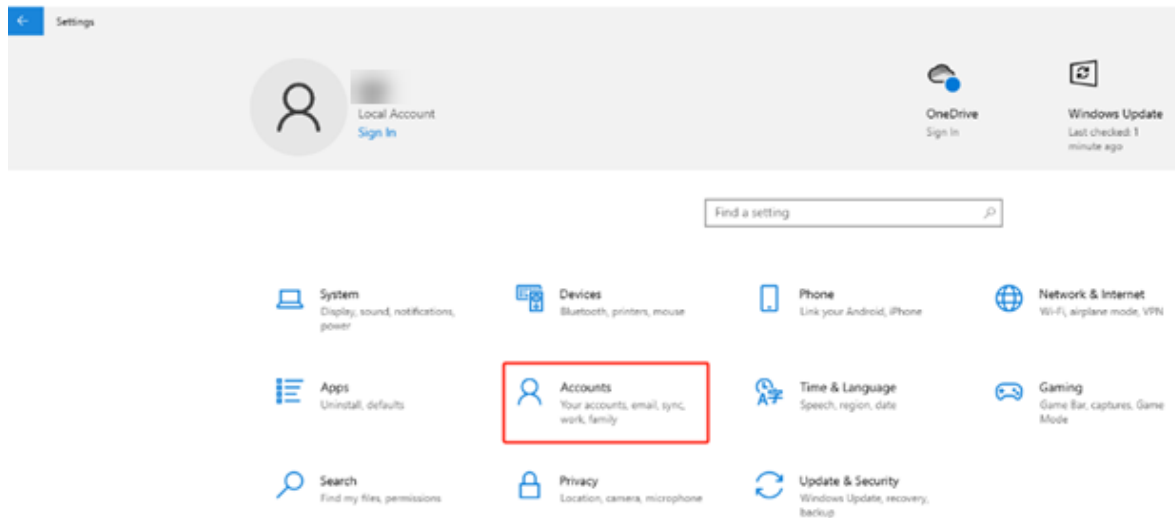
Review + save Cancel

### Step 3 - Install the Certificate Connector for Microsoft Intune

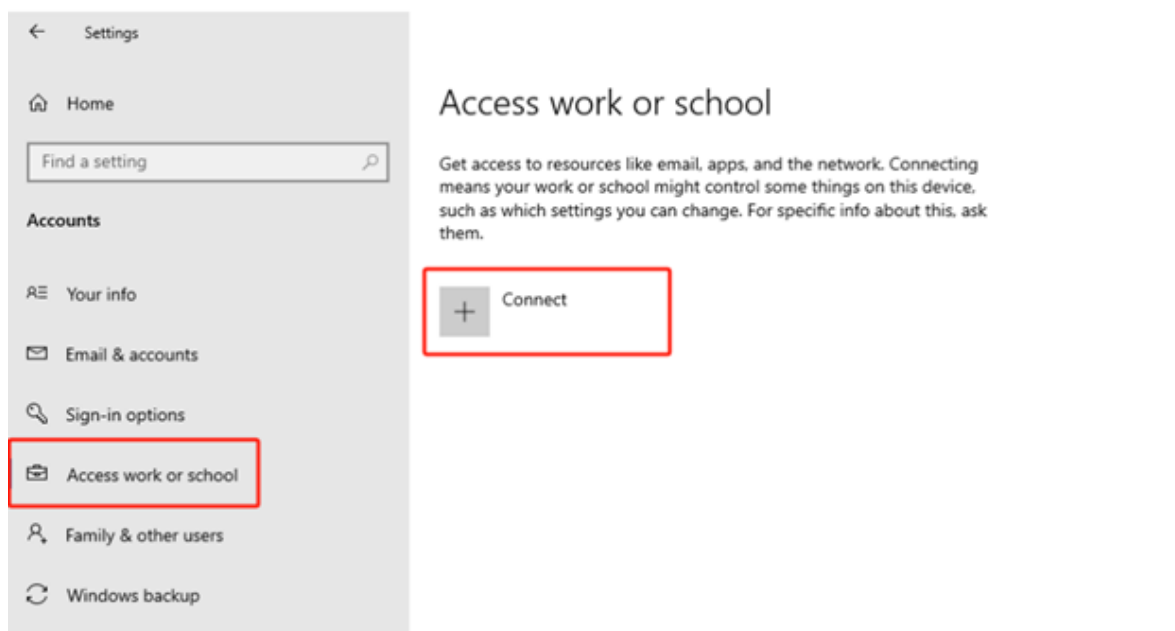
Please refer to tutorial from [Install the Certificate Connector for Microsoft Intune](#).

## Configuration on Windows Client Side

1. Login your Windows Client.
2. Open **Setting**, select **Accounts** and choose **Access Work or School**.

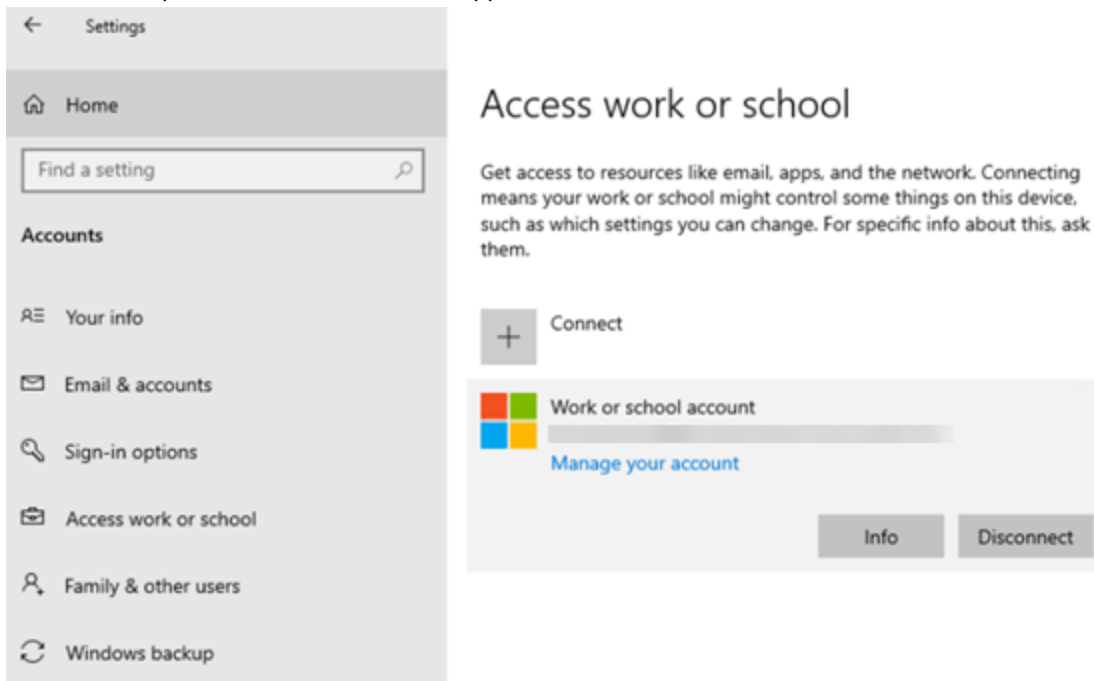


3. Click **Connect** to enter the account you used to login, make sure it has permissions in to allow users to enroll device.



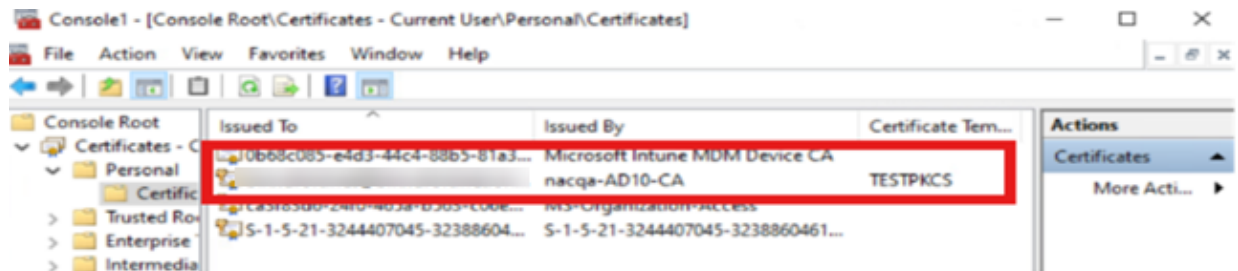
4. Enter the work or school account, and then click **Next**, sign in with your account password, then it will register the device with your organization.

5. Once it is completed, the account should appear as one of the access to work or school.



## Result - TLS Certificate added in Client

In Windows Client, go to **Current User > Personal > Certificates**, a user TLS certificate should now be added as a result.

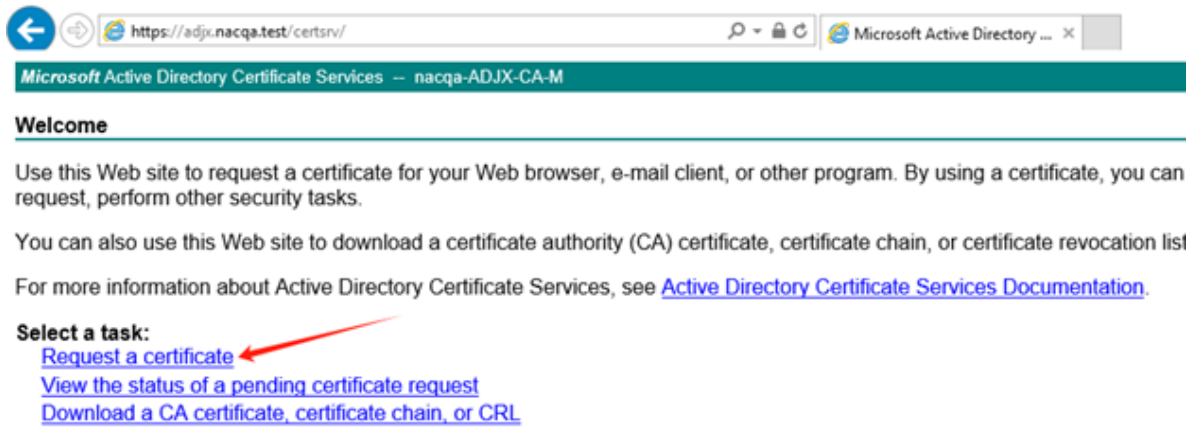




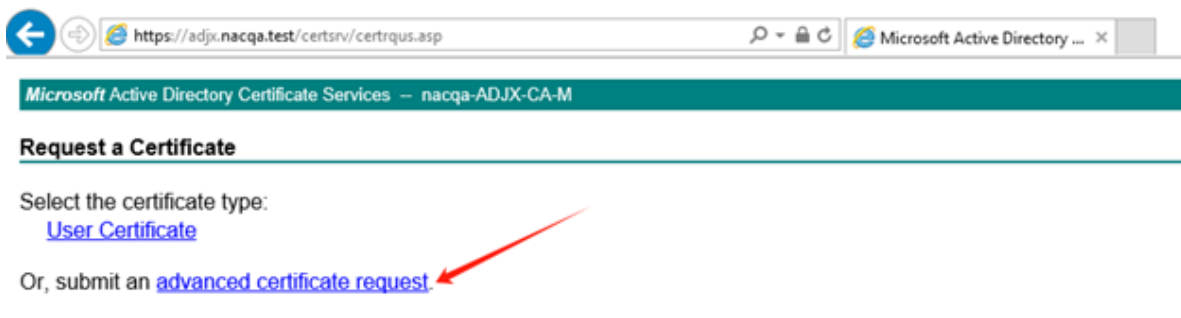
## Step 2 - Submit Certificate Request on Microsoft Active Directory

Use the CSR generated in Step 1 to submit a request for certificate in Microsoft Active Directory

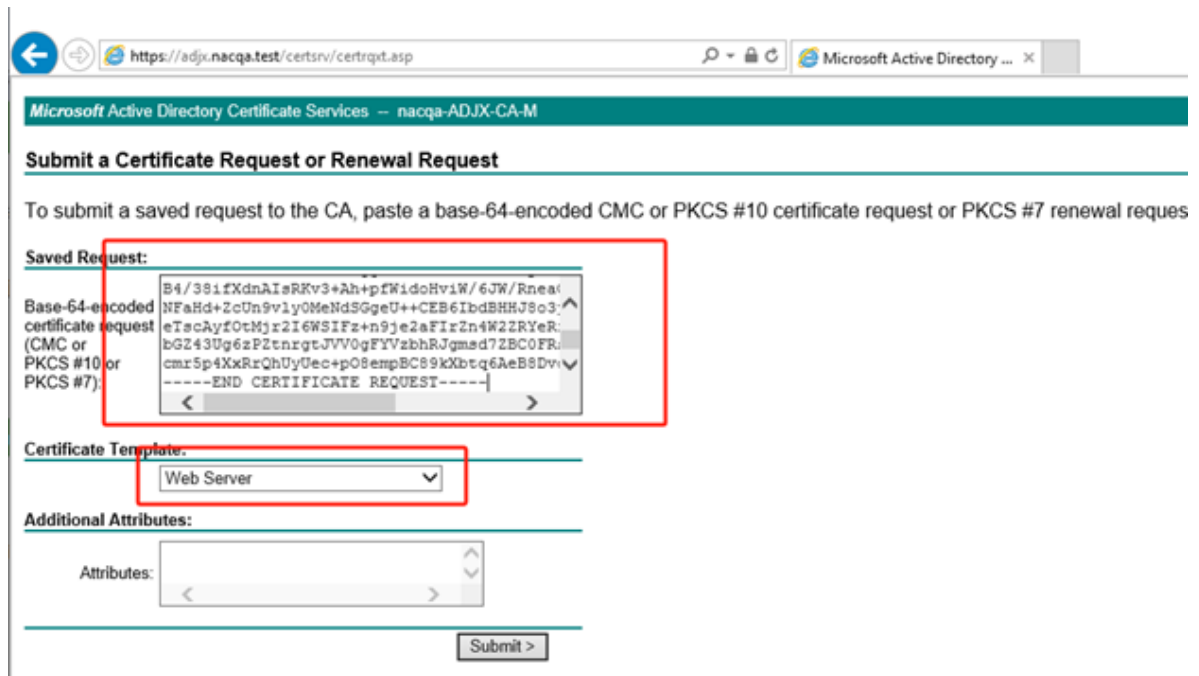
1. Open a browser to connect to Microsoft Active Directory Certificate Services, then click **Request a certificate**



2. In **Request a Certificate** page, click **advanced certificate request**.



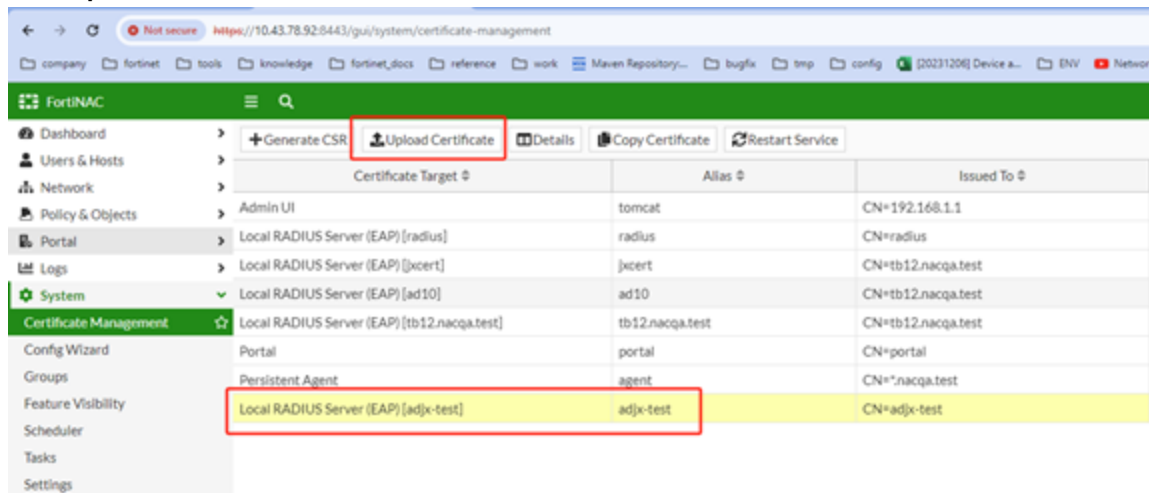
3. In **Advanced Certificate Request** page, click **Submit a certificate request by using a base 64 encoded CM..**
4. Paste the CSR generated from FortiNAC in **Base-64-encoded certificate**. In **Certificate Template**, select Web Server, and click **Submit**.



5. When the certificate is issued, download the certificate to the local machine.

### Step 3 - Upload the certificate on FortiNAC

1. Log back onto FortiNAC, go to **System > Certificate Management**.
2. Click **Upload Certificate**.

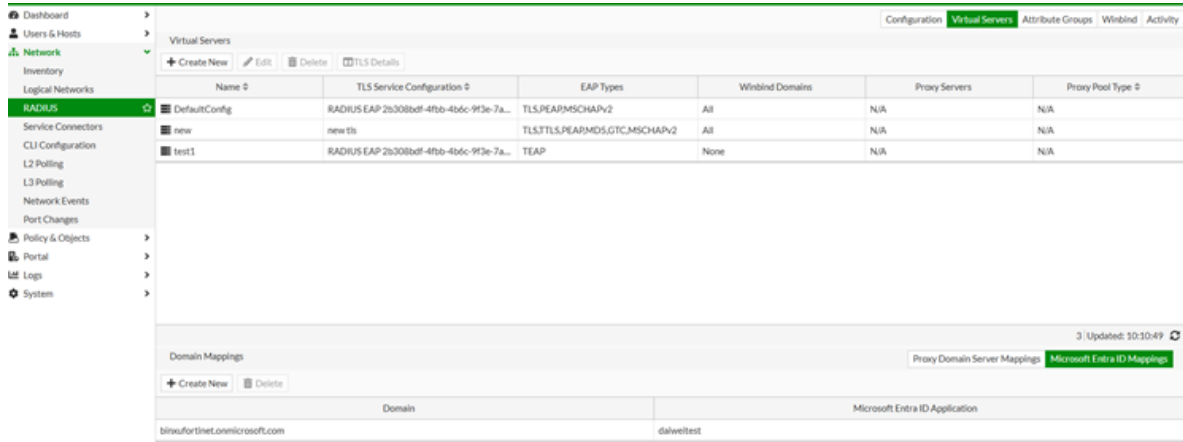


3. Click **Select Target**, and select "Local RADIUS Server (EAP)", then browse and upload the new RADIUS server EAP certificate downloaded from Step 2, and click **OK**.



## Step 4 - Define Microsoft Entra ID Mappings and Authentication source in virtual server configuration

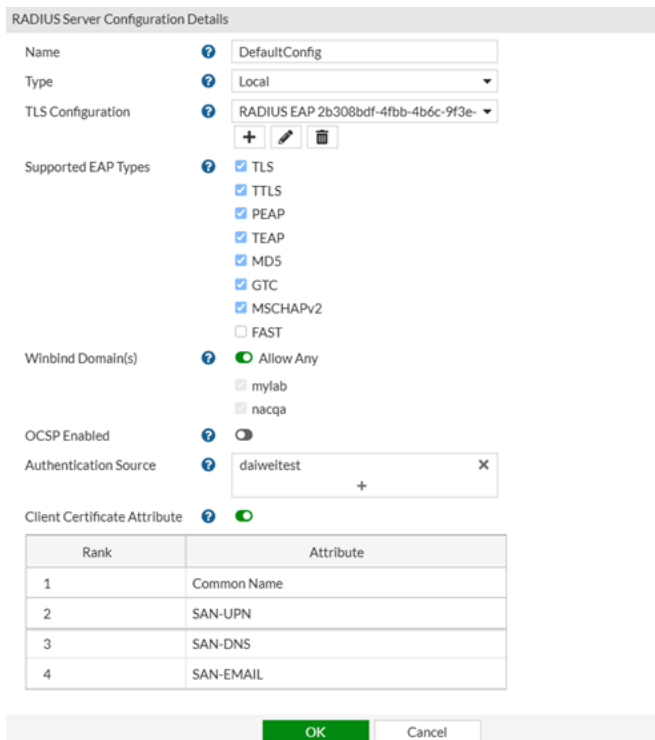
1. Under Domain Mappings, go to Microsoft Entra ID Mapping tab, add domain and Microsoft Entra ID Application.



2. Inside Virtual servers, for Authentication source, select the Microsoft Entra ID from the dropdown list.

## Step 5 - Define certificate attribute selection ranking in virtual server configuration

1. In FortiNAC, go to **Network > Radius > Virtual Server**, select one of the servers and double click that, a window will pop up.



1. In **Support EAP Types**, select **TLS** and **Client Certificate Attribute** will appear.
2. Enable the toggle switch button, and configure the ranking in which the attribute can be used to retrieve the username. Currently, 4 values are supported: **SAN-UPN, SAN-DNS, SAN-EMAIL, CN**.
3. FortiNAC will retrieve the username from these attributes according to the ranking configured.

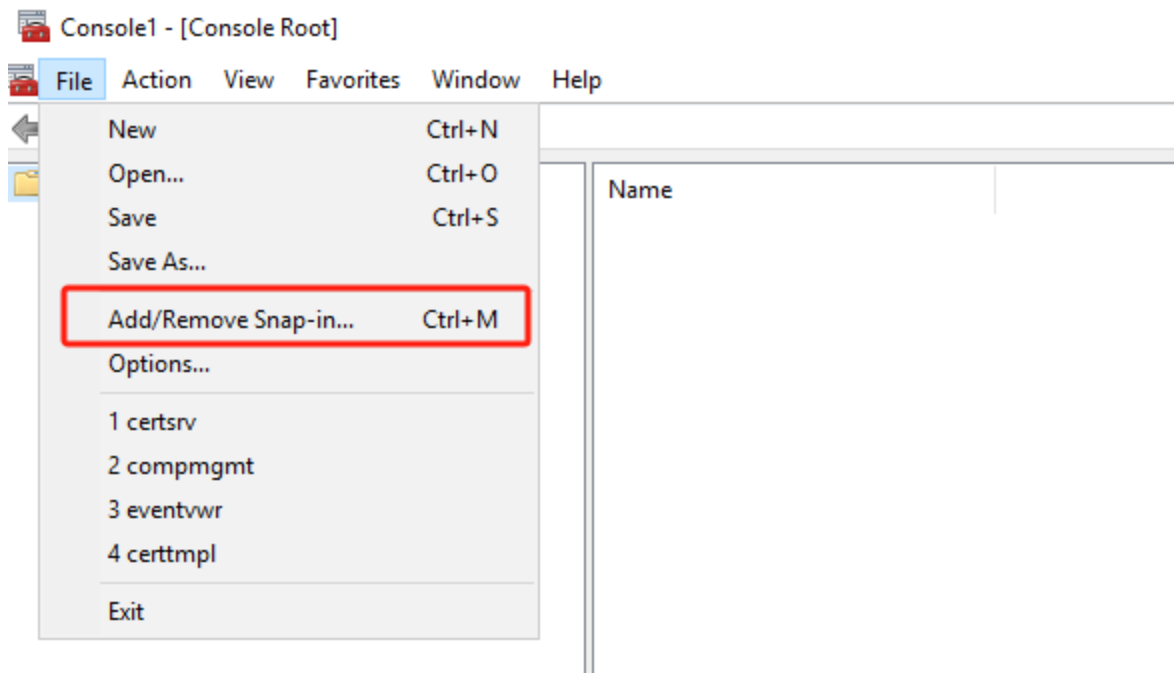
**For example**, in the screenshot above, FortiNAC will check if there is any common name existing in the certificate and the format is UPN, then the common name can be used to retrieve username and authentication is successful, then it will skip the rest of attributes. Otherwise, it will check **SAN-UPN** etc. If none of these attributes is existing in the certificate or username that retrieved from these attributes cannot finish authentication process, as a result authentication will failed.

### 3. Configuration on Client Side

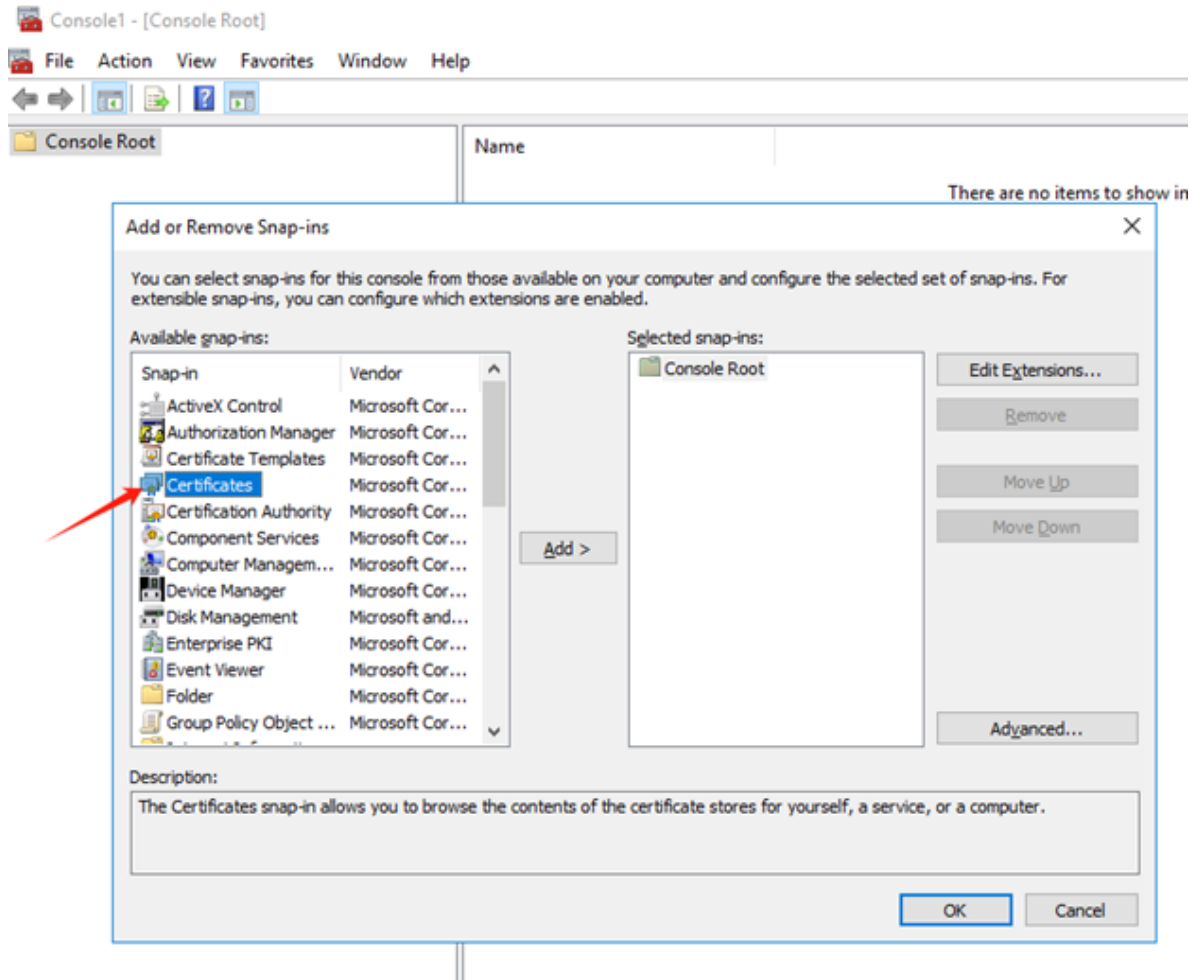
Follow these steps to configure Client Certificate:

#### Step 1 - Export root CA from Active Directory Certificate Services

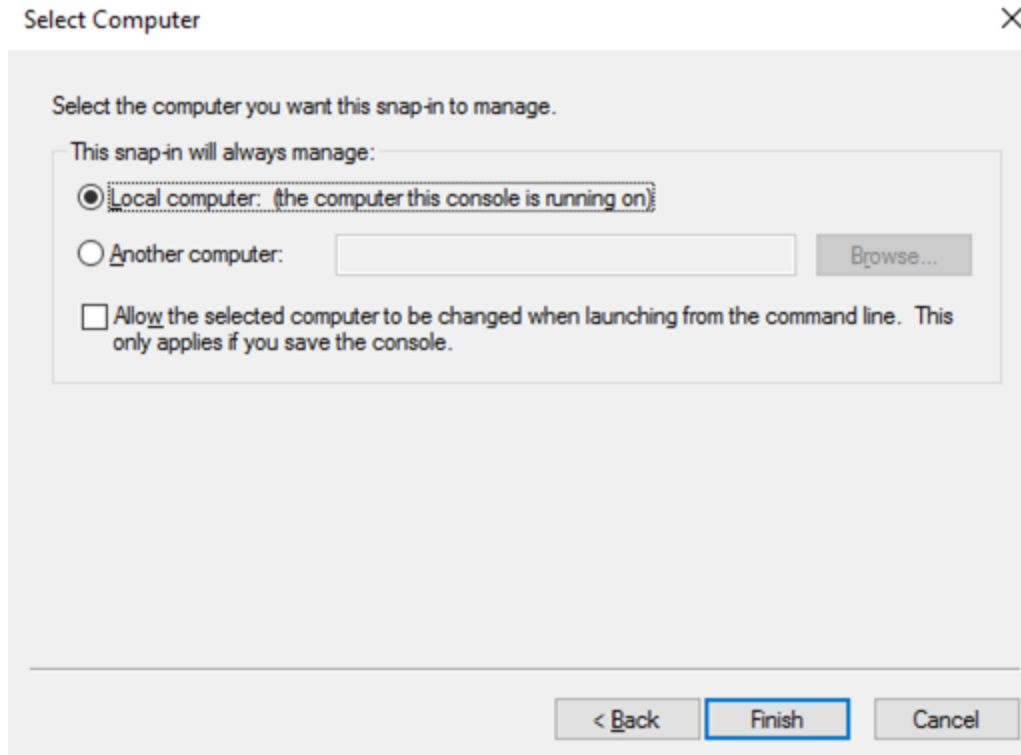
1. In root CA, click search and run on the command "mmc".
2. When the Console window opened, go to **File > Add/Remove Snap-in** from menu.



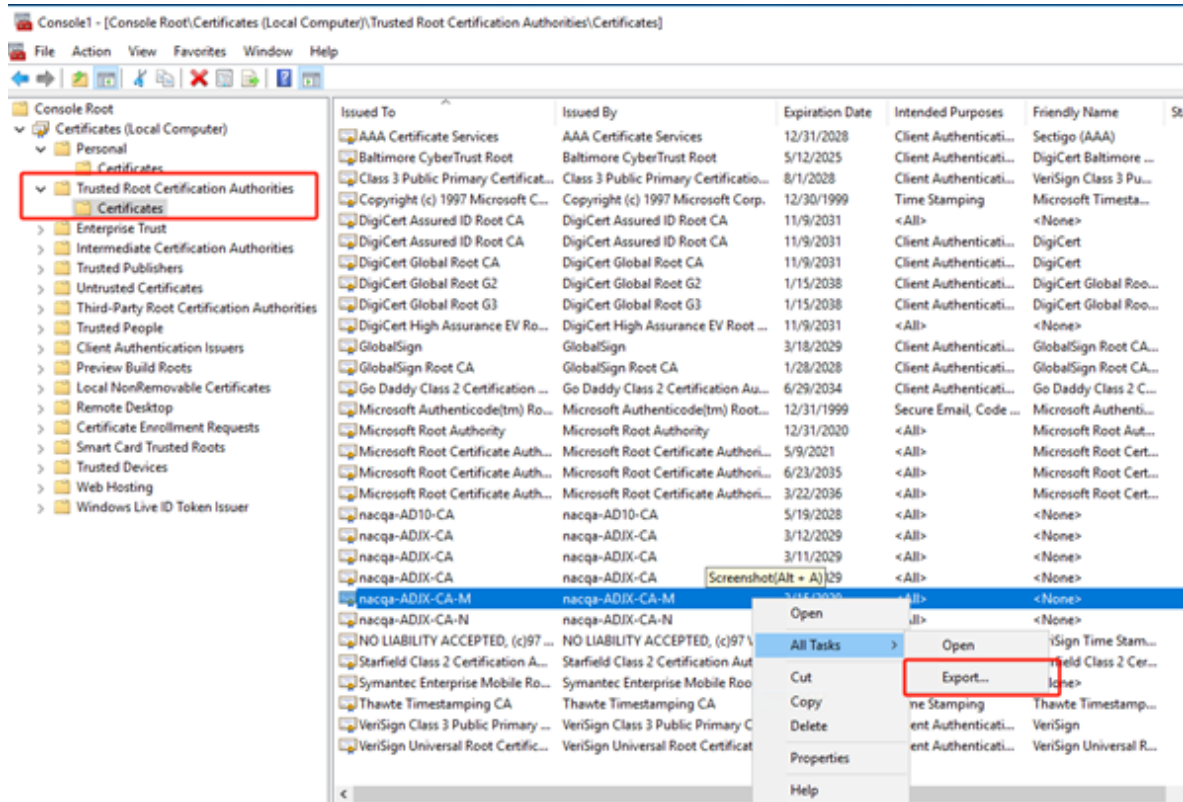
3. In available snap-ins, select Certificates to add, and click **Ok**.



4. In Certificate snap-in window, choose **Computer account**, and click **Next**.
5. Select **Local Computer** as where the snap-in will be managed, and click **Finish**.

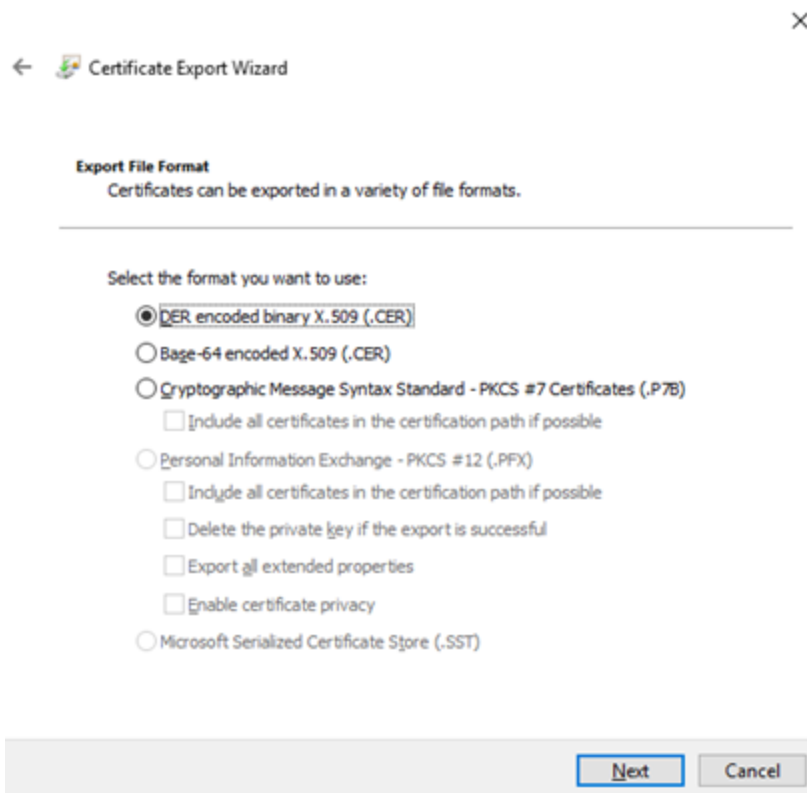


- Go back to Console, Go to **Trusted Root Certification Authorities > Certificates**, select **nacqa-ADJX-CA-M**, right click, click **All Tasks > Export**.



- In Certificate Export Wizard, click **Next** to continue.

- Click **DER encoded binary X.509 (.CER)** and click **Next**.



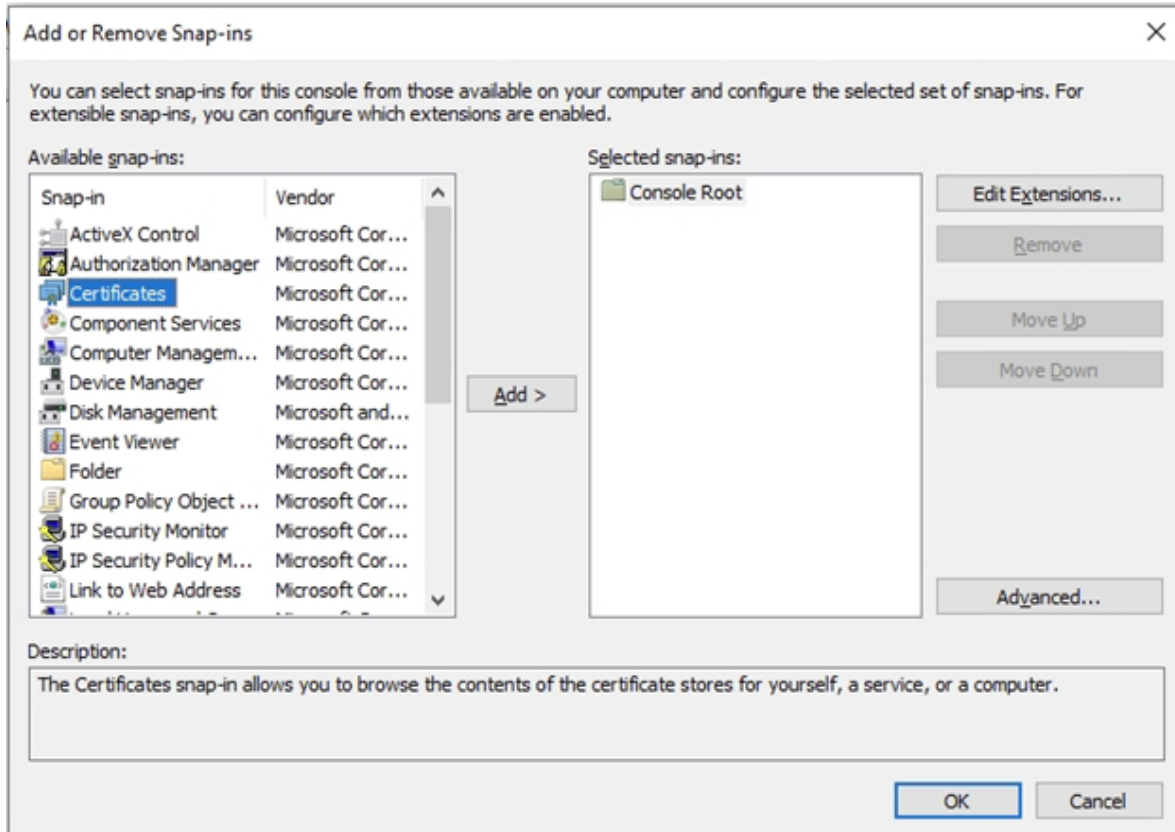
- Browse to the file you want to export, and click Finish to finish exporting the file.



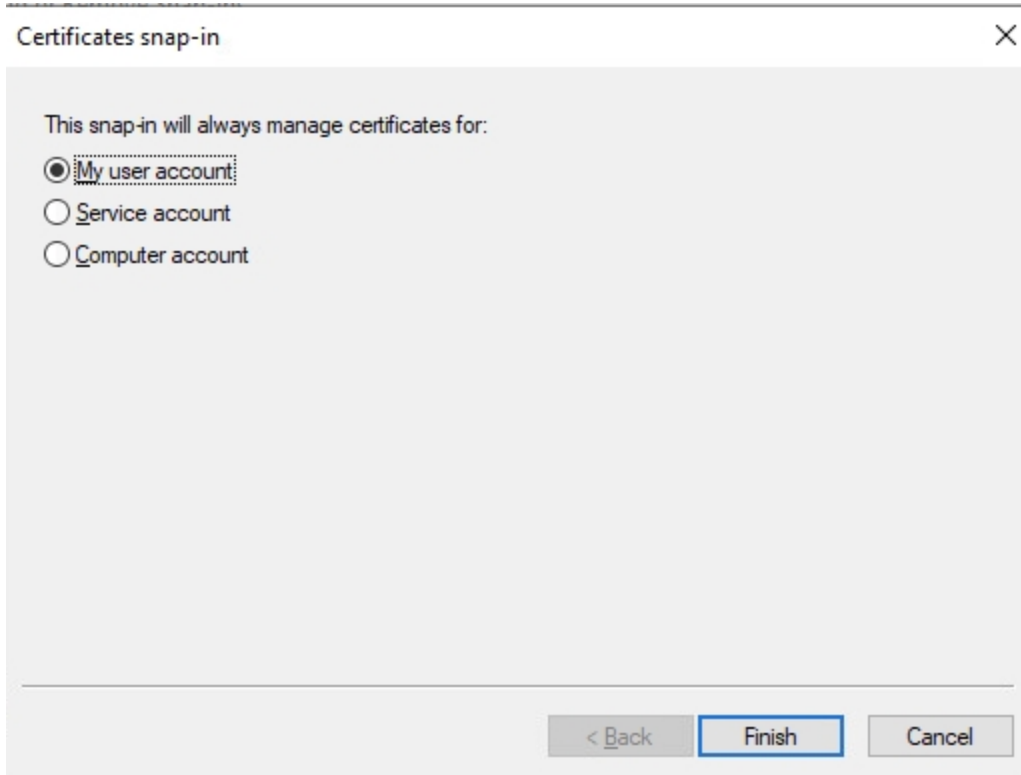
Before proceeding, generate a client certificate and place it in a personal folder under the Certificate's current user.

## Step 2 - Import Root CA into Client Trust Root Certificates

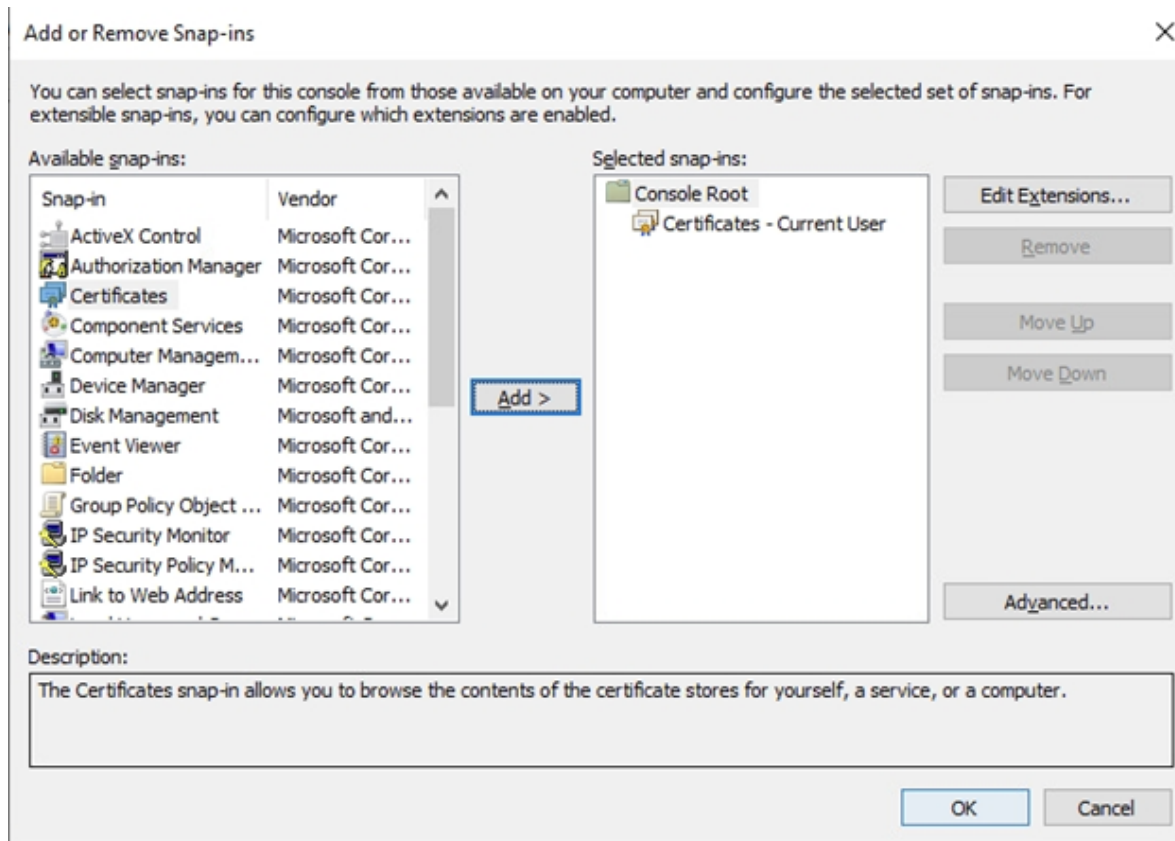
- In client machine, click search and run on the command "mmc".
- In **Add or Remove Snap-ins**, select **Certificates**.



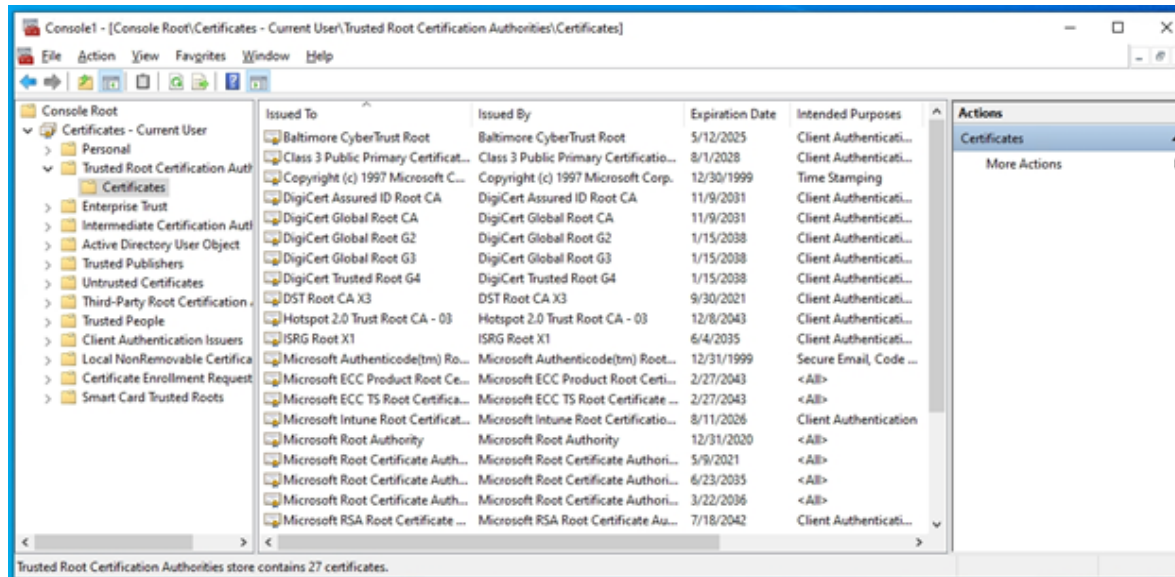
3. In **Certificates snap-in**, select **My user account**, and click **Finish**



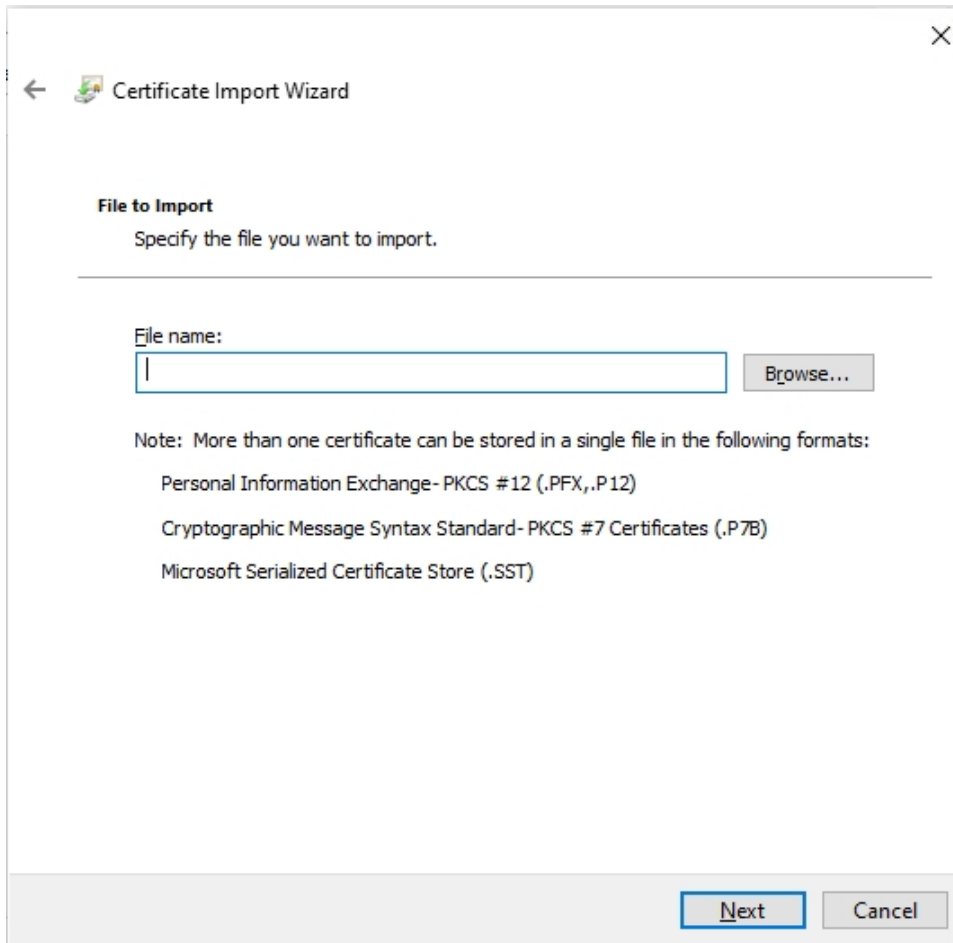
4. Right click on Trusted Root Certification Authorities, and select Certificates.



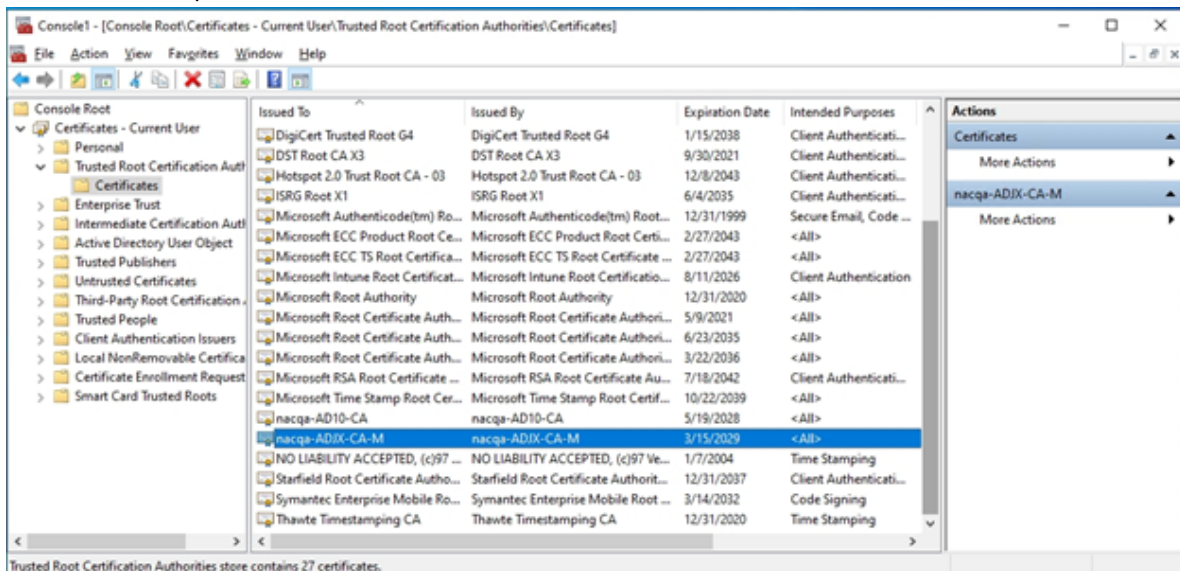
5. Select All Tasks > Import



6. Select Root CA file.

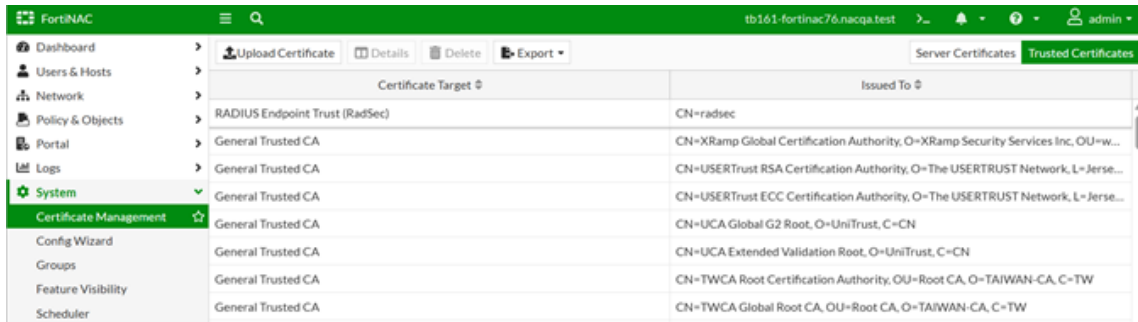


7. After the file is imported, the Root CA can be located in the list.

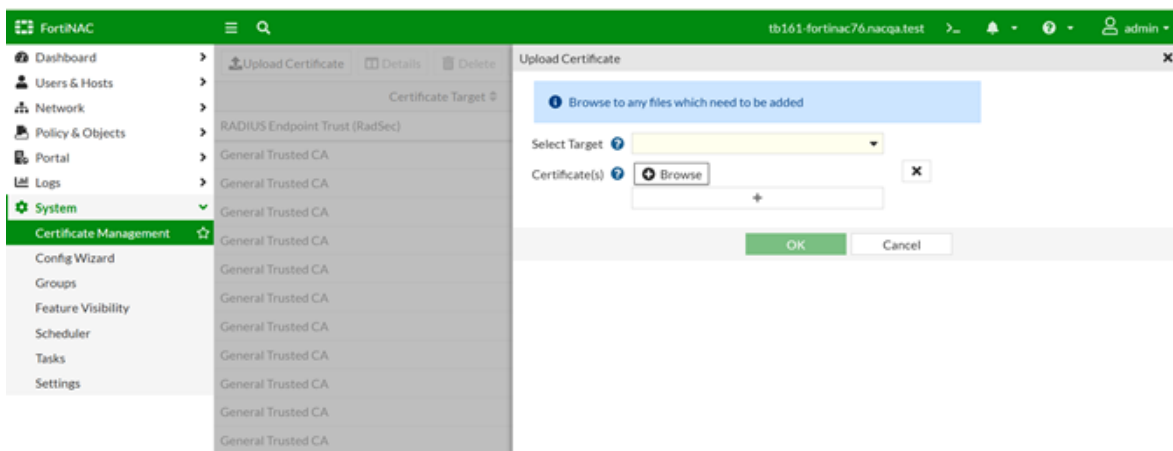


### Step 3 - Upload AD Root Certificate to FortiNAC

1. Log into FortiNAC, and go to **System > Certificate management**.
2. Select **Trusted Certificates** tab and click on **Upload Certificate**.

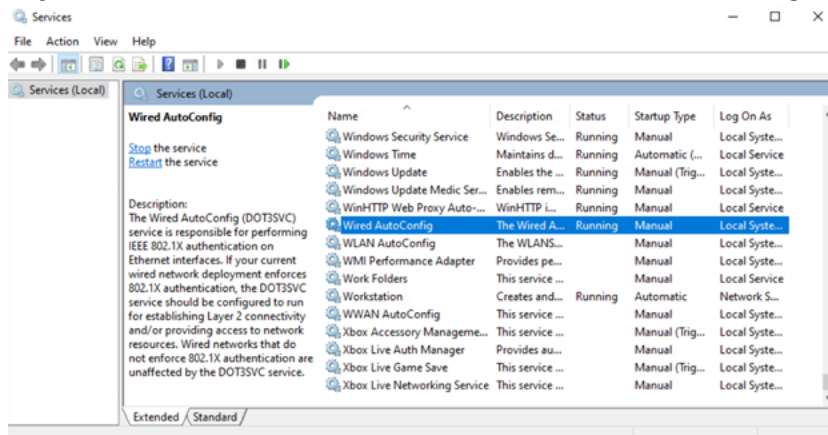


3. Click on **Browse** to add the AD root certificate to the FNAC

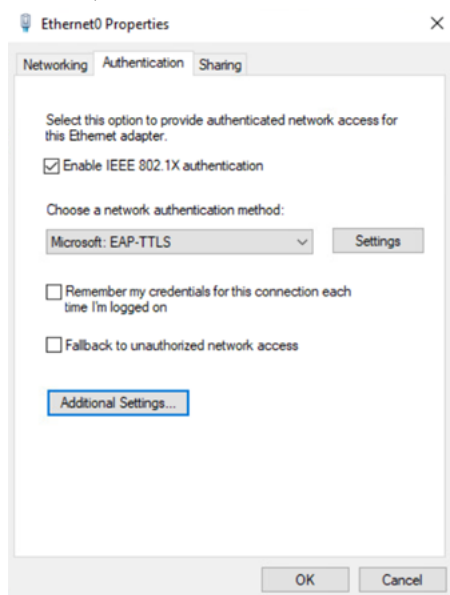


## 4. Use the TLS certificate to initiate authentication

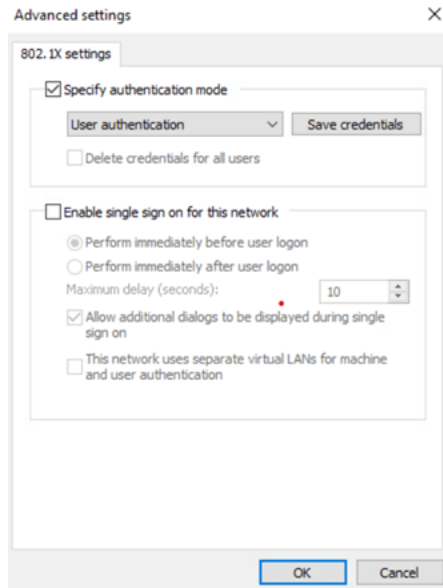
1. Log into the Windows host. Go to Services, and start **Wired Autoconfig** Service.



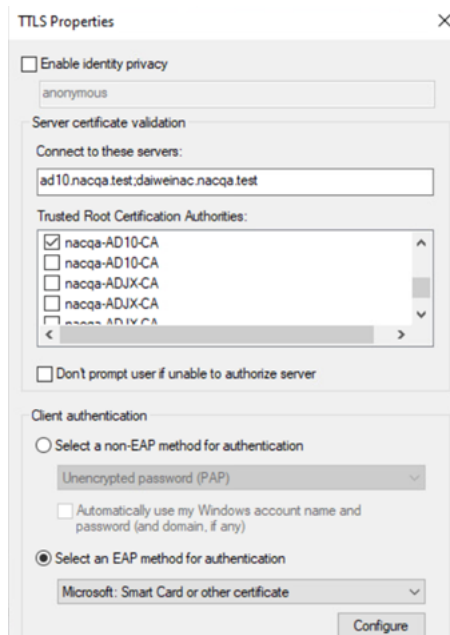
2. Go to **Control Panel > Network Connections**, right click on the network adapter, and click **Properties**.
3. Click on **Authentication** tab, and enable **IEEE 802.1X authentication**. For network authentication method, select **EAP-TTLS**.



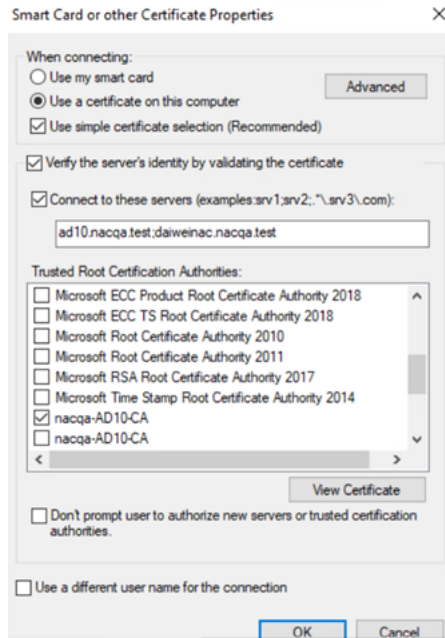
4. Click **Additional Settings > Specify authentication mode**, and choose **User authentication**.



5. Click on **Settings** next to **EAP-TLLS**
6. Uncheck **Enable Identity Privacy**.
7. For **Connect to these server**, input your CA address and FortiNAC address. Choose the **Trusted Root Certification Authorities**.
8. For **Client Authentication**, select an **EAP method for Authentication**. Choose **Smart Card** or other certificates.



9. Click **Configure** under Smart and certificates.

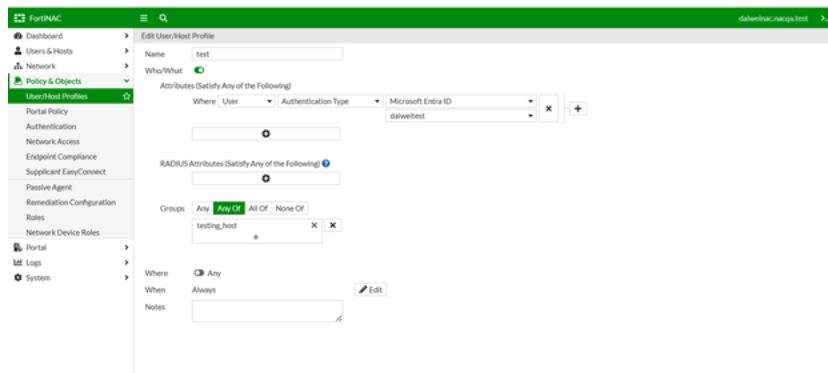


10. Enable **simple certificate selection**, **Verify the server's identity by validating the certificate**, **Connect to these servers** and input your CA and FortiNAC address.
11. Select the trusted root certification Authorities.

## 5. Synchronize New attributes added in User/Host Profiles for Microsoft Entra ID

The new Microsoft Entra ID service connector can be sourced and synchronize in User/Host profile .

1. Go to **Policy & Objects > User/Host Profiles > Who/What Attributes**.
2. In Where condition, set **User > Authentication Type** as Microsoft Entra ID, you can choose your service connector for Microsoft Entra ID.
3. If the user source is Microsoft Entra ID and authentication source matches the service connector configured for Microsoft Entra ID. The vlan will switch based on the matched policy.



# Remote Group

## Overview

Remote Group allows FortiNAC to sync groups of users from Microsoft Entra ID. These groups of users can constantly be polled and updated automatically or manually through FortiNAC service connector. Essentially, it allows FortiNAC users to see the list of users authenticated by FortiNAC through Microsoft Entra ID authentication as a group in **System > Groups > Remote Groups**.

These remote group can be also be used in User Host Profile (UHP).

FortiNAC checks the user group membership and then responds to RADIUS with a Production vlan in the scenario where access request are accepted according to network access policies.

## Configuration on FortiNAC through Service Connector

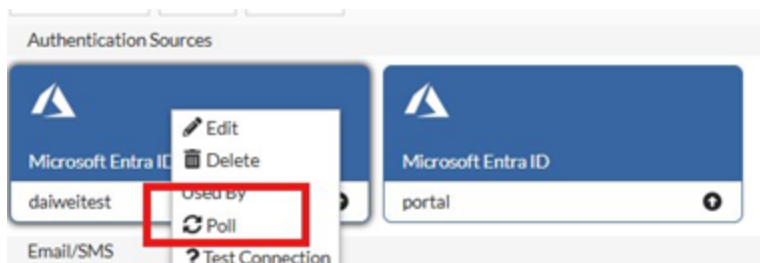
To import groups from Microsoft Entra ID, go to **Network > Service Connectors > Authentication Sources - > Microsoft Entra ID**.

1. Enable **Import Groups From Microsoft Entra ID**.

The screenshot shows the configuration interface for a Microsoft Entra ID authentication source. The 'Import Groups From Microsoft Entra ID' toggle is turned on. Below it, a list of groups to import is shown: 1231production, daiweigroup, Daiweiteamtest, and west. The 'Sync Groups Automatically' toggle is also turned on, and the 'Sync Every' interval is set to 1 Minute(s).

2. **Delete Users No Longer Found on Sync**
3. Select the groups to be imported from Microsoft Entra ID.
4. In **Sync Groups Automatically**, configure how often the groups to be synced in FortiNAC.
5. Enable **Delete Users No Longer Found on Sync** to automatically delete users no longer found from the group.

Alternatively, remote groups can also be pulled manually through right click on the service connector and select Poll.



The remote groups that are imported can now be viewed on FortiNAC at **System > Groups > Remote Groups**

Local Groups <span style="color: green;">Remote Groups</span>											
Name	Type	Used By	Members	Source Status	Owner	Group Source	Description	Last Modified By	Last Modified Time	Last Sync Time	
daiweigroup	Microsoft Entra ID	1	2	Synced	User	daiweittest		SYSTEM	2025/09/30 16:15:29	2025/09/30 16:15:29	
Daiweiteamtest	Microsoft Entra ID	1	1	Synced	User	daiweittest	Daiweiteamtest	SYSTEM	2025/09/30 16:15:29	2025/09/30 16:15:29	
1231productL...	Microsoft Entra ID	1	1	Synced	User	daiweittest		SYSTEM	2025/09/30 16:15:28	2025/09/30 16:15:28	
binxu	Microsoft Entra ID			Synced	User	portal	binxu	SYSTEM	2025/09/30 15:57:28	2025/09/30 15:57:28	
west	Microsoft Entra ID	1		Unavailable	User	daiweittest	west	SYSTEM	2025/09/29 12:04:09	2025/09/29 12:03:02	
duz_test	Microsoft Entra ID			Synced	User	portal		SYSTEM	2025/09/30 15:57:29	2025/09/30 15:57:29	

The **Source Status** is a reflection of the group status on Microsoft Entra ID:

1. Synced - connected and updated through Microsoft Entra ID.
2. Unavailable - the group is deleted from Microsoft Entra ID.
3. Disconnected - Service connector cannot reach the specific group.

## Remote Groups CLI Configuration

The following CLI commands can be used to display Microsoft Entra ID group details in FortiNAC CLI:

```
Diagnose system remote-group display all/id/name
```

CLI Com-mand	Description
<b>all</b>	Display all remote groups.
<b>id</b>	Display remote group information and/or members using ID.
<b>name</b>	Display remote group information and/or members by name

CLI Command example

```

Commands:
  all  Display all remote groups
  id   Display remote group information and/or members using ID
  name Display remote group information and/or members by name
daiweinac2 (Interim) # diagnose system remote-group display all
ID | Name | Type
-----|-----|-----
1373345314447362|daiweigroup|Microsoft Entra ID
1373345315557380|Daiweiteamtest|Microsoft Entra ID
1373346624471056|binxu|Microsoft Entra ID
1373382050545695|duz_test|Microsoft Entra ID
1375483748839431|1231production|Microsoft Entra ID
1377195803824152|west|Microsoft Entra ID
-----|-----|-----
daiweinac2 (Interim) #

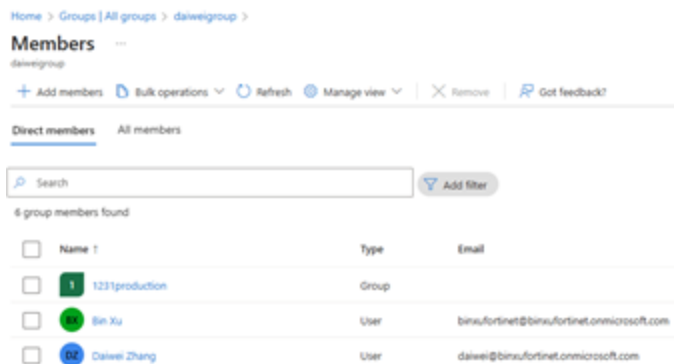
```

## Example - Remote Group Use with User Host/Profile

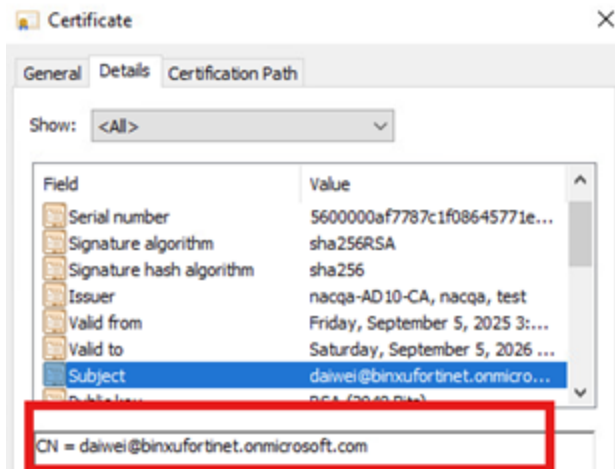
In this example, 802.1X TLS will be used in conjunction with Remote Group.

### Prerequisite

The user used to do the authentication is a member of remote group in Microsoft Entra ID.



The user has generated a TLS certificate that CN has the UPN format of username.



### Steps on using 802.1X TLS Security Profile

1. Add Microsoft Entra ID into FortiNAC network Service Connector.
2. Import remote group called "daiweigroup" and pull group.
3. Apply remote group "daiweigroup" in Network Access UHP.
4. Enable auto registration on switch port
5. Add 802.1X security profile from FortiGate switchport.
6. Add Authentication source and Microsoft Entra ID Mappings in radius configuration
7. Using TLS certificate which CN is "daiwei@binxufortinet.onmicrosoft.com" to do 802.1X authentication. Outer EAP method is TTLS, inner method is TLS.
8. After authentication is done, "daiwei@binxufortinet.onmicrosoft.com" is added into "daiweigroup" remote group automatically and host will move to production vlan

**Note:** Import UHP policy including remote group attribute from CA to NCM is not supported.

Result of the authentication

Status	First Name	Last Name	User ID	Number of Registered Hosts	Number of Logged in Hosts	Authentication Type	Authentication Name	Email	Phone
	Admin	admin	admin			Local			
	Daiwei	Zhang	zdaiwei			Other			
	Daiwei		daiwei			Other		daiwei@binxufortinet...	
	testfro000	zhang	zjianxing@binxufortine...			Microsoft Entra ID	daiweitest		
	DaiweiAzure	Zhang	daiwei@binxufortinet...			Microsoft Entra ID	daiweitest	daiwei@binxufortinet...	

Port	Port Name	Port Type	Port Mode	Port Speed	Port Duplex	Port Protocol	Port Status	Port Security	Port Access
2	port1	10.18.35.151	Learned	Uplink	1	1	On	Link Up	None/Normal Access
3	port1	10.18.35.151	Learned	Uplink	1	1	On	Link Up	Unrestricted

Adapters - Total: 1	Connected Container	Rule Name	Media	RADIUS Auth. Type	Outer EAP Type	Inner EAP Type	Access Value	Vendor Name	Machine Authentication	User Authentication	Host Name	Operating System
daiwei_lgt				802.1X	TTLS	TLS	92	VMware, Inc.				

## Remote Group

Local Groups		Remote Groups							View Members
Name	Type	Used By	Members	Source Status	Owner	Group Source	Description	Last M	
dalweigroup	Microsoft Entra ID	1	2	Synced	User	dalweitest		SYSTEM	
Dalweibeamtest	Microsoft Entra ID		1	Synced	User	dalweitest	Dalweibeamtest	SYSTEM	
1231producti...	Microsoft Entra ID		1	Synced	User	dalweitest		SYSTEM	
binou	Microsoft Entra ID			Synced	User	portal	binou	SYSTEM	
duz_test	Microsoft Entra ID			Synced	User	portal		SYSTEM	

Members

Search

- dalweigroup
- 1231production
- Zhang.DalweAzure



Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.