FortiNAC - Microsoft Entra ID Authentication Guide

Version F 7.6.3

July 10th, 2025
FortiNAC F 7.6.3 Microsoft Entra ID Authentication Guide
49-20-748677-20210922

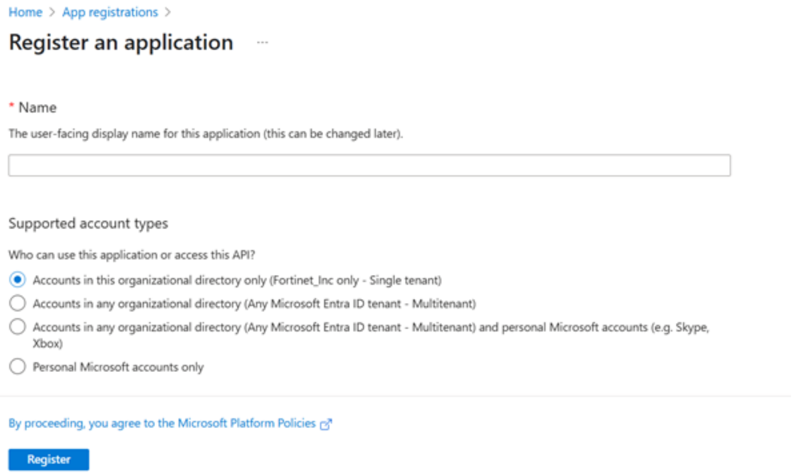
TABLE OF CONTENTS

Overview

Microsoft Entra ID can provide convenience for enterprises to use Microsoft Entra ID as authentication source to grant network connection. This document provides configurations using Microsoft Entra ID AD as native authentication source.

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**.



* Name

The user-facing display name for this application (this can be changed later).

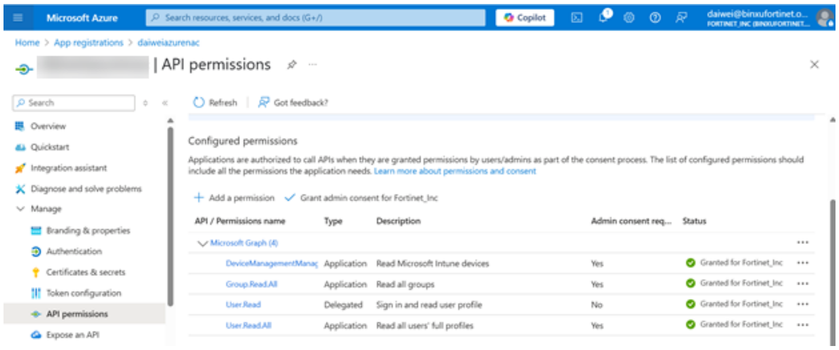
Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Fortinet_Inc only - Single tenant)
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

By proceeding, you agree to the Microsoft Platform Policies

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



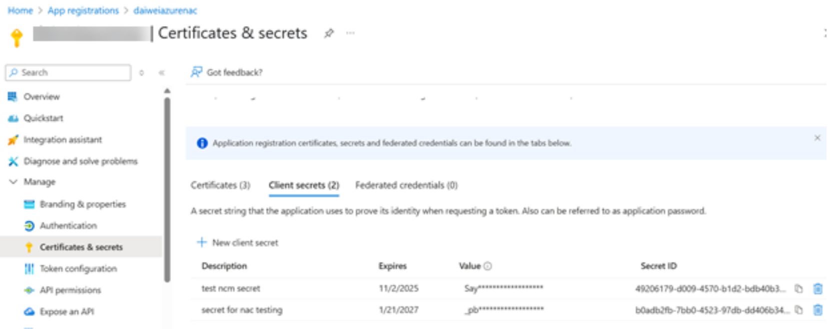
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
daiwei@binxufortinet.o...
FORTINET_INC (BINXUFORTINET...
Home > App registrations > daiweiazurenac
[redacted] | API permissions
Search
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
Refresh
Got feedback?
+ Add a permission
✓ Grant admin consent for Fortinet_Inc

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (4)				
DeviceManagementManag	Application	Read Microsoft Intune devices	Yes	✓ Granted for Fortinet_Inc
Group.Read.All	Application	Read all groups	Yes	✓ Granted for Fortinet_Inc
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for Fortinet_Inc
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for Fortinet_Inc

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



Home > App registrations > daiweiazurenac

[redacted] | Certificates & secrets

Application registration certificates, secrets and federated credentials can be found in the tabs below.

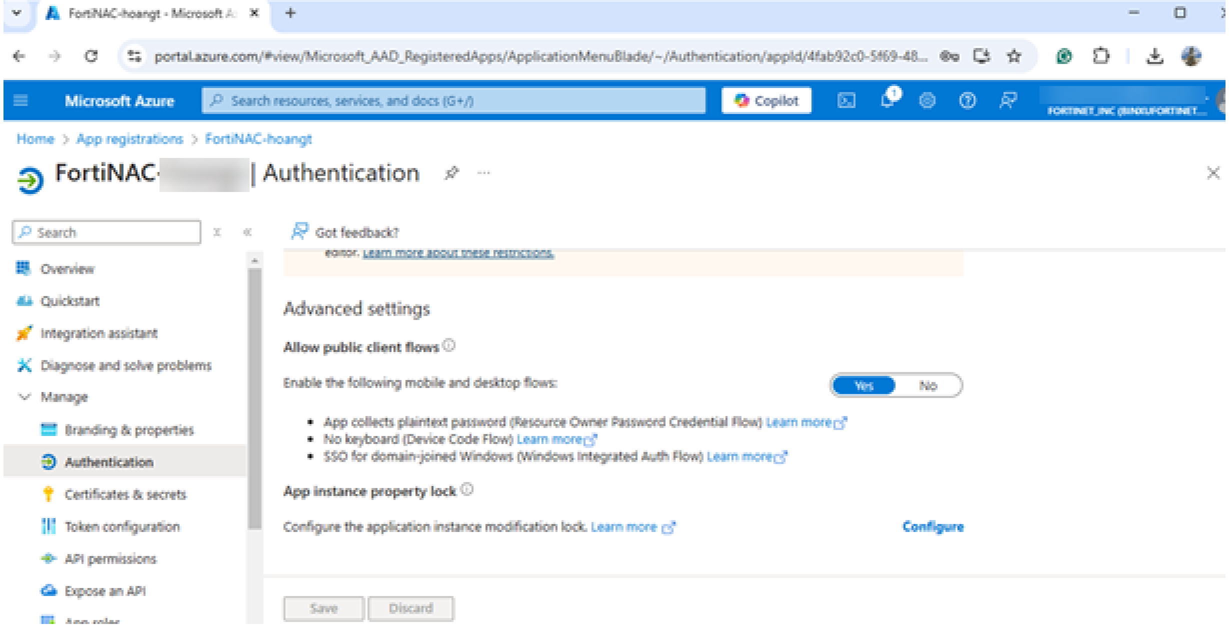
Certificates (3) | Client secrets (2) | Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
test ncm secret	11/2/2025	Say******************	49206179-d009-4570-b1d2-bdb40b3...
secret for nac testing	1/21/2027	_pb******************	b0adb2fb-7bb0-4523-97db-dd406b34...

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.



portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Authentication/appId/4fab92c0-5f69-48...

Home > App registrations > FortiNAC-hoangt

FortiNAC-[redacted] | Authentication

Advanced settings

Allow public client flows

Enable the following mobile and desktop flows: [✓ Yes] No

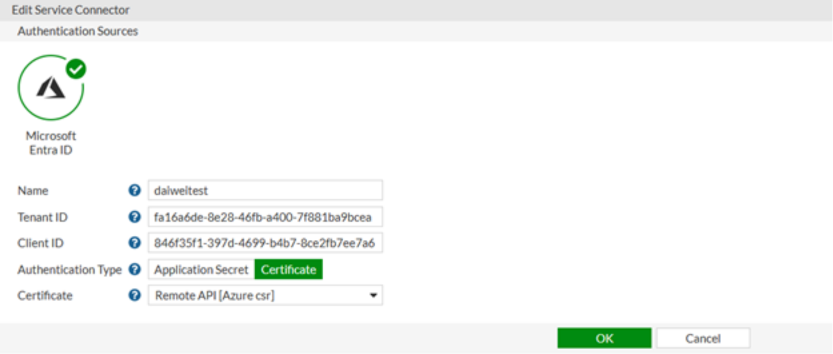
- App collects plaintext password (Resource Owner Password Credential Flow) Learn more
- No keyboard (Device Code Flow) Learn more
- SSO for domain-joined Windows (Windows Integrated Auth Flow) Learn more

App instance property lock

Configure the application instance modification lock. Learn more — Configure

Generate Certificate for Microsoft Entra ID in FortiNAC Service Connector

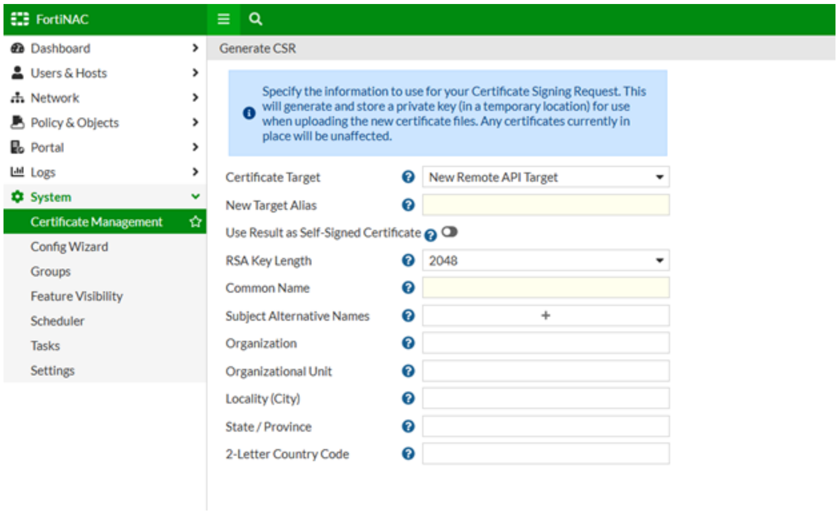
This section will generate the certificate for Microsoft Entra ID in FortiNAC service Connector



Name	dalweltest
Tenant ID	fa16a6de-8e28-46fb-a400-7f881ba9bcea
Client ID	846f35f1-397d-4699-b4b7-8ce2fb7ee7a6
Authentication Type	Application Secret / Certificate
Certificate	Remote API [Azure csr]

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.



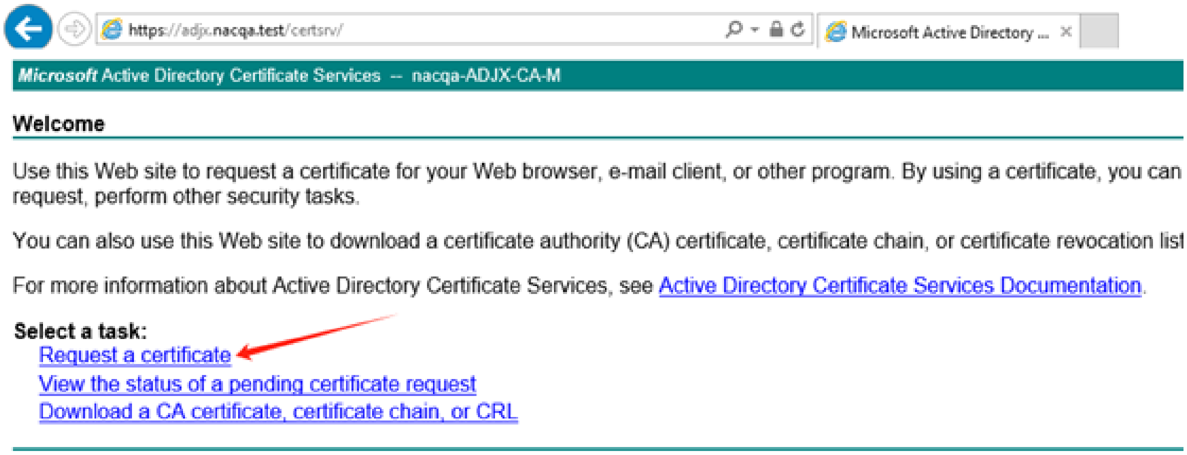
Specify the information to use for your Certificate Signing Request. This will generate and store a private key (in a temporary location) for use when uploading the new certificate files. Any certificates currently in place will be unaffected.

Certificate Target	New Remote API Target
New Target Alias	
Use Result as Self-Signed Certificate	
RSA Key Length	2048
Common Name	
Subject Alternative Names	+
Organization	
Organizational Unit	
Locality (City)	
State / Province	
2-Letter Country Code	

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**



https://adjx.nacqa.test/certsrv/
Microsoft Active Directory ...

Microsoft Active Directory Certificate Services -- nacqa-ADJX-CA-M

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can request, perform other security tasks.

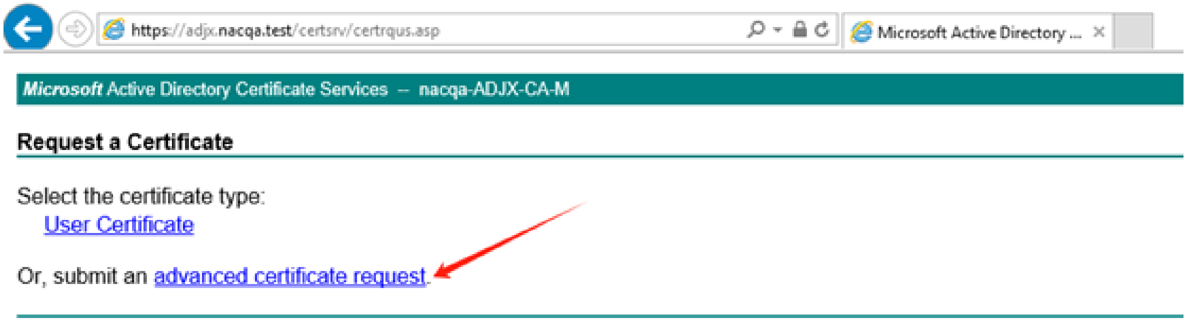
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

.

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



https://adjx.nacqa.test/certsrv/certrqus.asp
Microsoft Active Directory ...

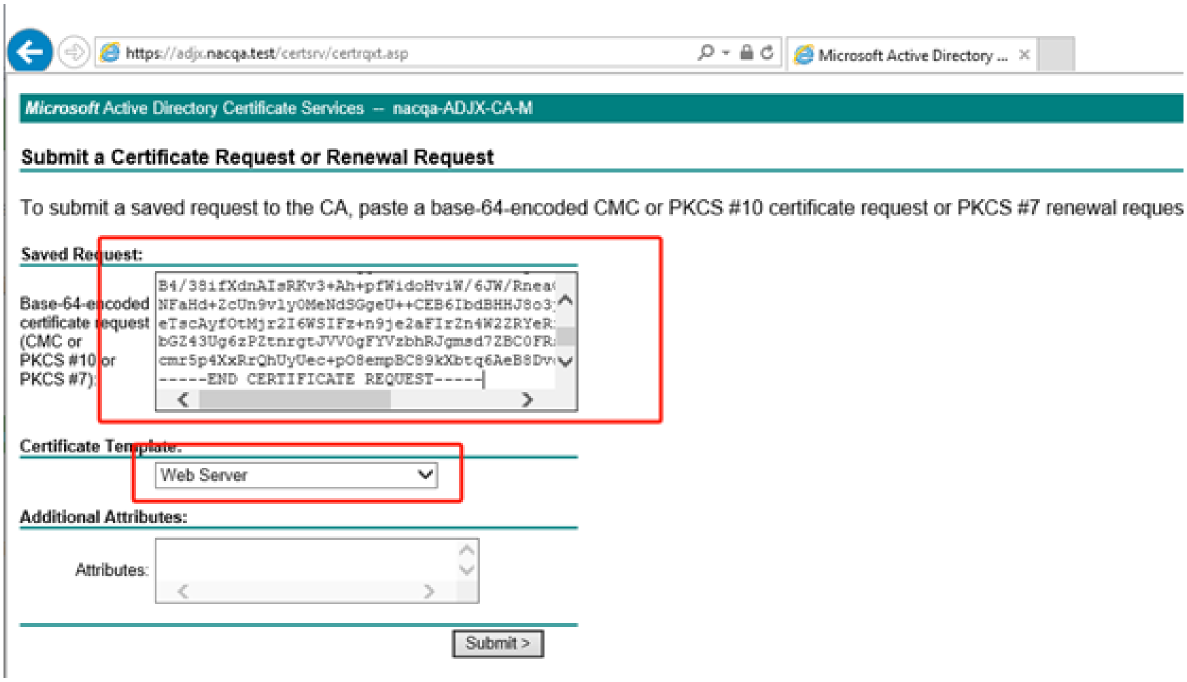
Microsoft Active Directory Certificate Services -- nacqa-ADJX-CA-M

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an 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**.



https://adjx.nacqa.test/certsrv/certrqxt.asp
Microsoft Active Directory ...

Microsoft Active Directory Certificate Services -- nacqa-ADJX-CA-M

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal reques

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
B4/38ifXdnAIsRKv3+Ah+pfWidoHviW/6JW/Rnea
NFaHd+ZcUn9vly0MeNdSGgeU++CEB6IbdBHHJ8o3
eTscAyfOtMjr2I6WSIFz+n9je2aFIrZn4W2ZRYeR
bGZ43Ug6zPZtnrgtJVV0gFYVzbhRJgmsd7ZBC0FR
cmr5p4XxRrQhUyUec+pO8empBC89kXbtq6AeB8Dv
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

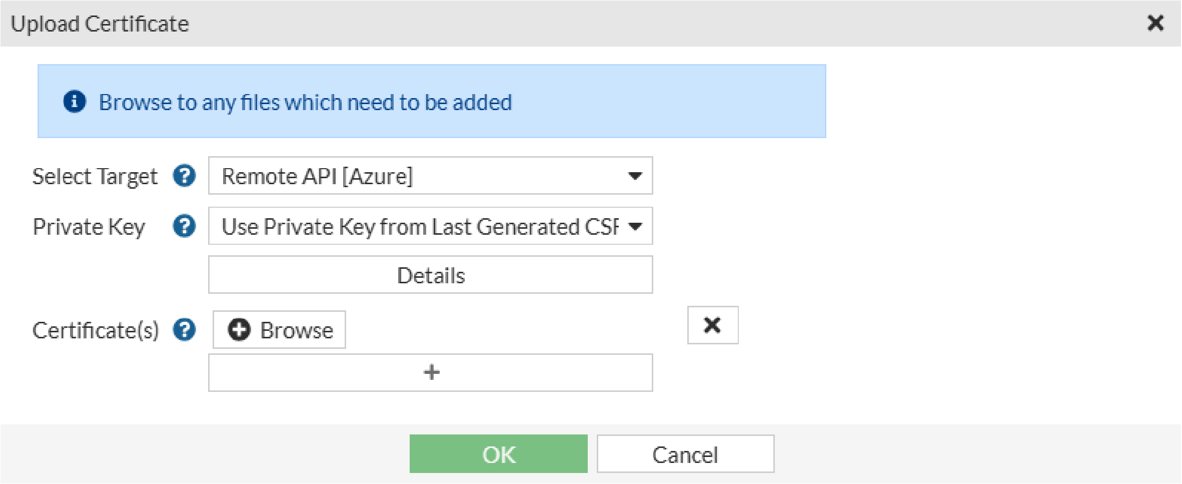
Additional Attributes:

Attributes:

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 Mangement**.
2. Click **Upload Certificate** and select "Remote API Target".
3. Browse and upload the certificate downloaded from Step 2, and click OK.



Upload Certificate

Browse to any files which need to be added

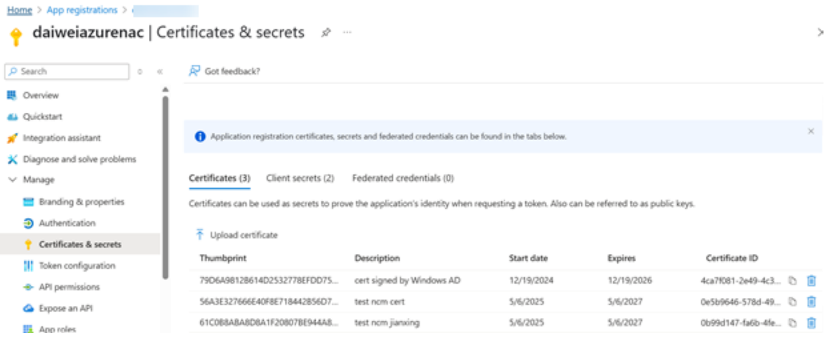
Select Target: Remote API [Azure]

Private Key: Use Private Key from Last Generated CSF

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

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

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



daiweiazurenac | Certificates & secrets

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (3) Client secrets (2) Federated credentials (0)

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

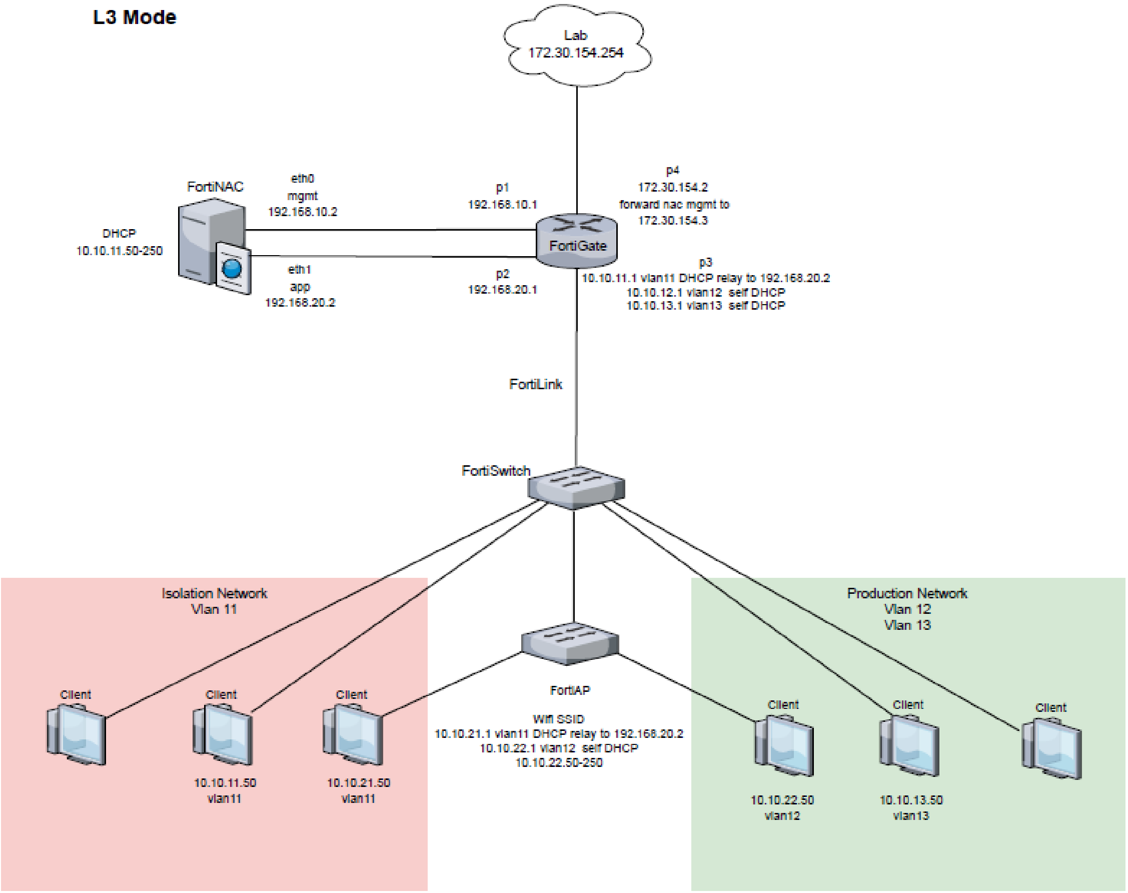
Thumbprint	Description	Start date	Expires	Certificate ID
79D6A98128614D2532778EFDD75...	cert signed by Windows AD	12/19/2024	12/19/2026	4ca7f081-2e49-4c3...
56A3E327666E40F8E718442856D7...	test ncm cert	5/6/2025	5/6/2027	0e5b9646-578d-49...
61C088ABA8D8A1F20807BE944A8...	test ncm jianxing	5/6/2025	5/6/2027	0b99d147-fa6b-4fe...

2. Upload the Certificate to complete.

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:



Step 1-6 Microsoft Entra ID, FortiGate, FortiNAC, and FortiSwitch Configuration

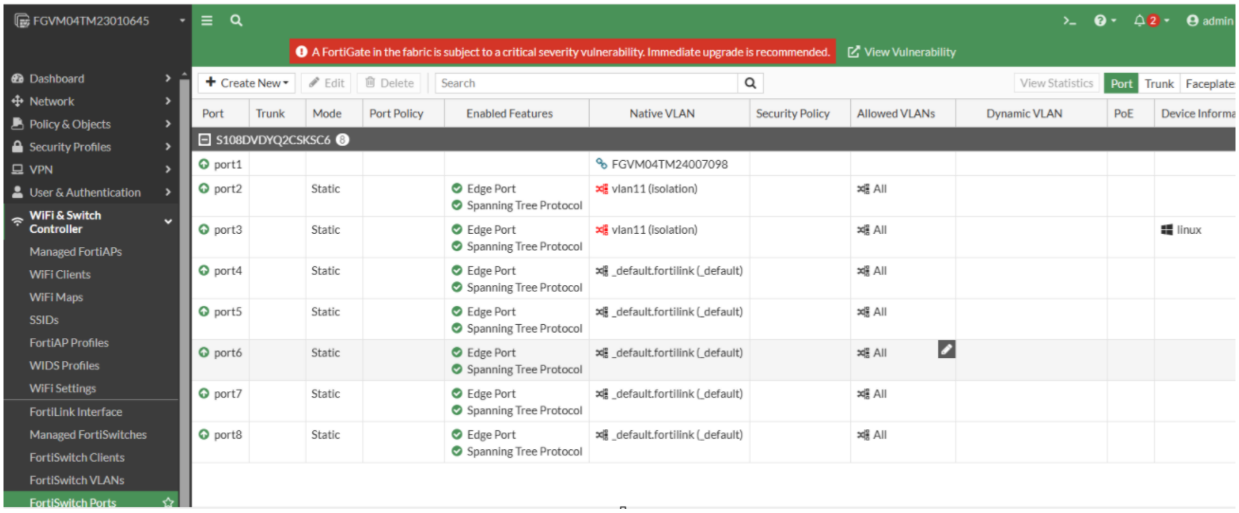
Step 1 - Microsoft Entra ID Configuration

Follow the link to register FortiNAC application in Microsoft Microsoft Entra ID: Microsoft Entra ID OAuth 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.

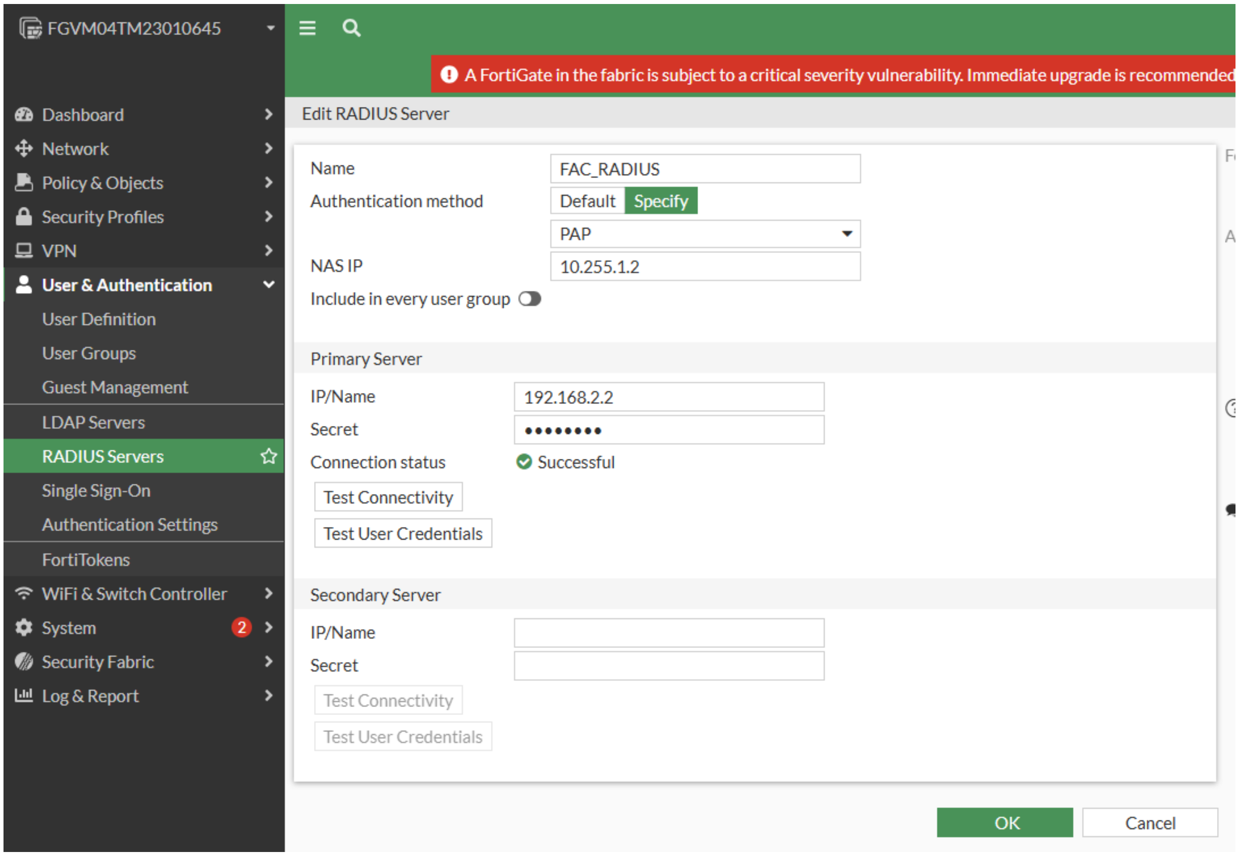


A FortiGate in the fabric is subject to a critical severity vulnerability. Immediate upgrade is recommended. View Vulnerability

S108DVDYQ2CSKSC6 8

Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Security Policy	Allowed VLANs	Dynamic VLAN	PoE	Device Informa
port1					FGVM04TM24007098					
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.



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]
	PAP
NAS IP	10.255.1.2
Include in every user group	○

Primary Server

IP/Name	192.168.2.2
Secret	••••••••
Connection status	✓ Successful

Test Connectivity

Test User Credentials

Secondary Server

IP/Name	
Secret	

Test Connectivity

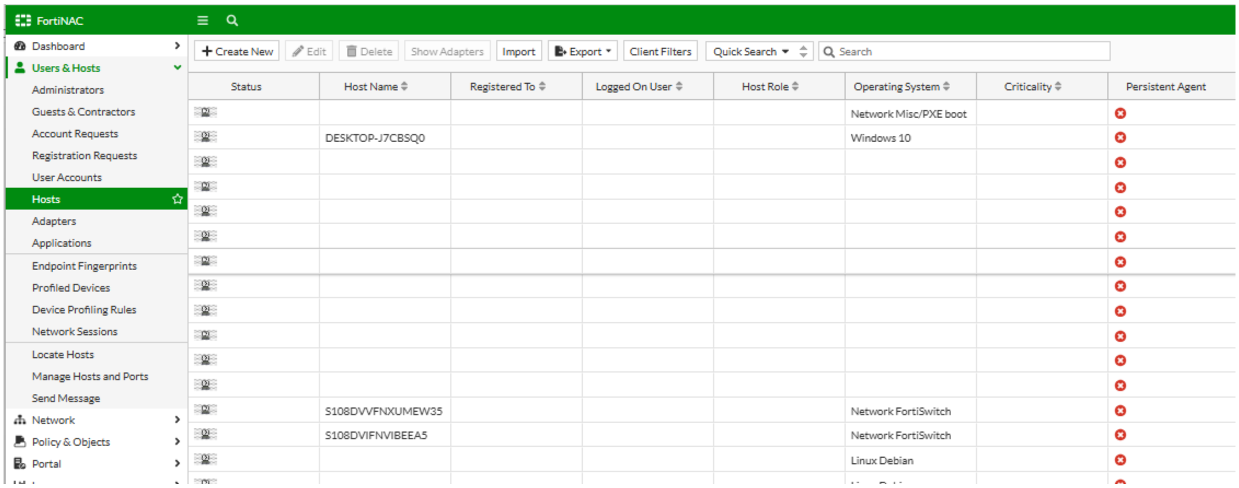
Test User Credentials

OK Cancel

Step 3 - FortiNAC configuration

Follow the link below to configure FortiNAC overall configuration: FortiNAC Configuration

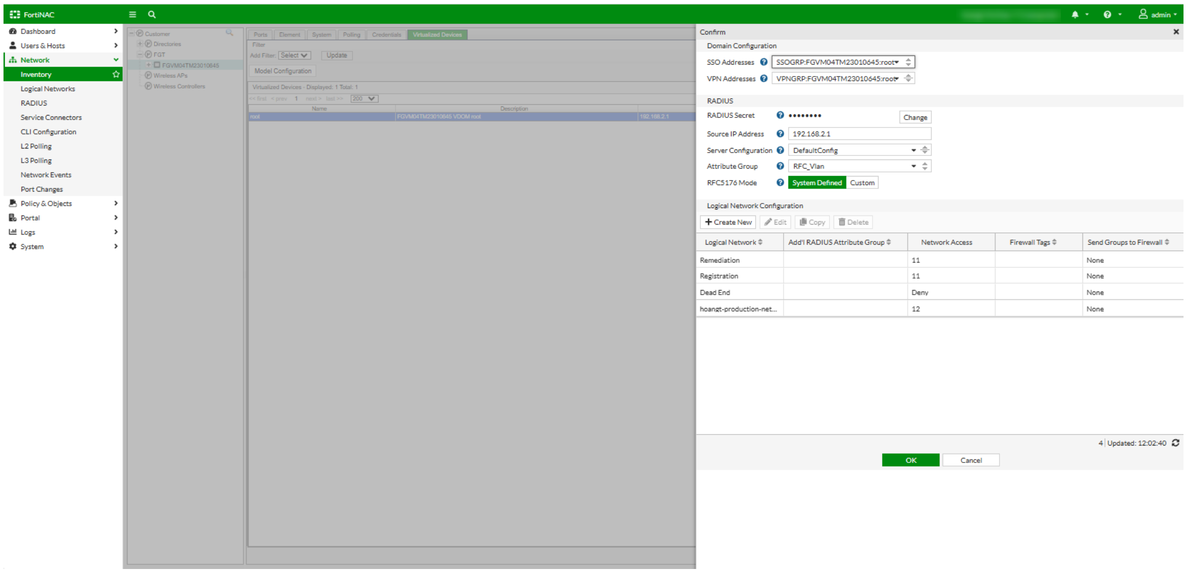
Note: Delete the client host under test in **Users & Hostst > Hosts** to have successful test run.



Status	Host Name	Registered To	Logged On User	Host Role	Operating System	Criticality	Persistent Agent
					Network Misc/PXE boot		⊗
	DESKTOP-J7CBSQ0				Windows 10		⊗
							⊗
							⊗
							⊗
							⊗
							⊗
							⊗
							⊗
							⊗
							⊗
							⊗
	S108DVVFNXUMEW35				Network FortiSwitch		⊗
	S108DVIFNVIBEEA5				Network FortiSwitch		⊗
					Linux Debian		⊗

1. Go to **Policy & Objects > Authentications**, enable **Enable Authentication** but don’t enable Authentication Method.

2. 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.



Confirm

Domain Configuration

SSO Addresses: SSOGRP:FGVM04TM23010645:root

VPN Addresses: VPNGRP:FGVM04TM23010645:root

RADIUS

RADIUS Secret: ••••••••

Source IP Address: 192.168.2.1

Server Configuration: DefaultConfig

Attribute Group: RFC_Vlan

RFC5176 Mode: [✓ System Defined] Custom

Logical Network Configuration

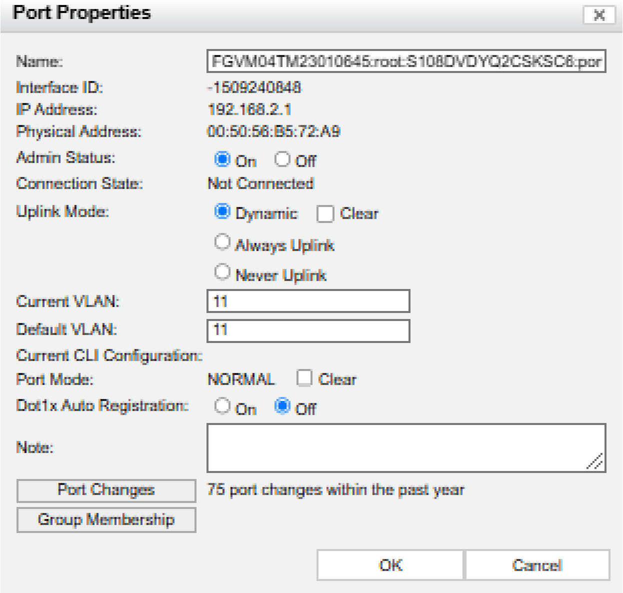
Logical Network	Add'l RADIUS Attribute Group	Network Access	Firewall Tags	Send Groups to Firewall
Remediation		11		None
Registration		11		None
Dead End		Deny		None
hoangt-production-net...		12		None

4 | Updated: 12:02:40

OK Cancel

Step 4 - FortiSwitch Port Configuration

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

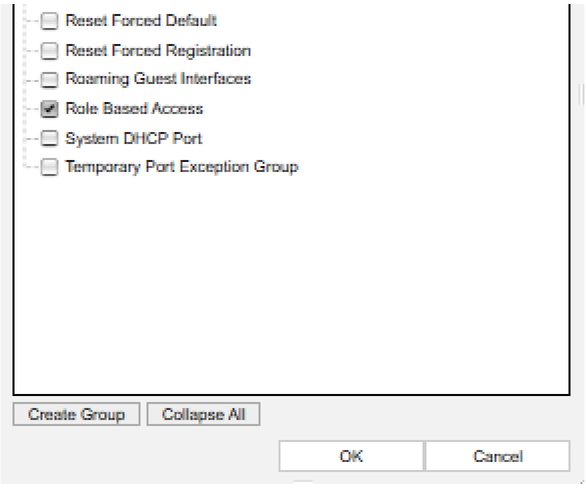


Port Properties

Name:	FGVM04TM23010645:root:S108DVDYQ2CSKSC8:por
Interface ID:	-1509240848
IP Address:	192.168.2.1
Physical Address:	00:50:56:B5:72:A9
Admin Status:	● On ○ Off
Connection State:	Not Connected
Uplink Mode:	● Dynamic □ Clear ○ Always Uplink ○ Never Uplink
Current VLAN:	11
Default VLAN:	11
Current CLI Configuration:	
Port Mode:	NORMAL □ Clear
Dot1x Auto Registration:	○ On ● Off
Note:	
Port Changes	75 port changes within the past year
Group Membership	

OK Cancel

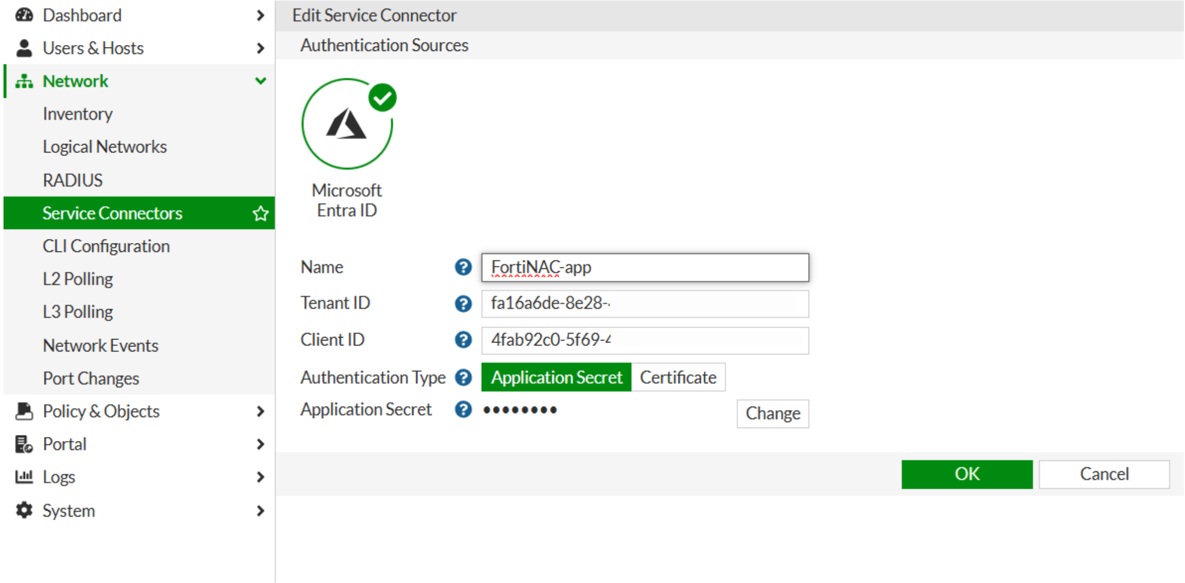
3. Click **Group Membership**, and check the following in Group Membership.



- □ Reset Forced Default
- □ Reset Forced Registration
- □ Roaming Guest Interfaces
- ☑ Role Based Access
- □ System DHCP Port
- □ Temporary Port Exception Group

Step 4 - Service Connectors Configuration

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



Name: FortiNAC-app

Tenant ID: fa16a6de-8e28-

Client ID: 4fab92c0-5f69-4

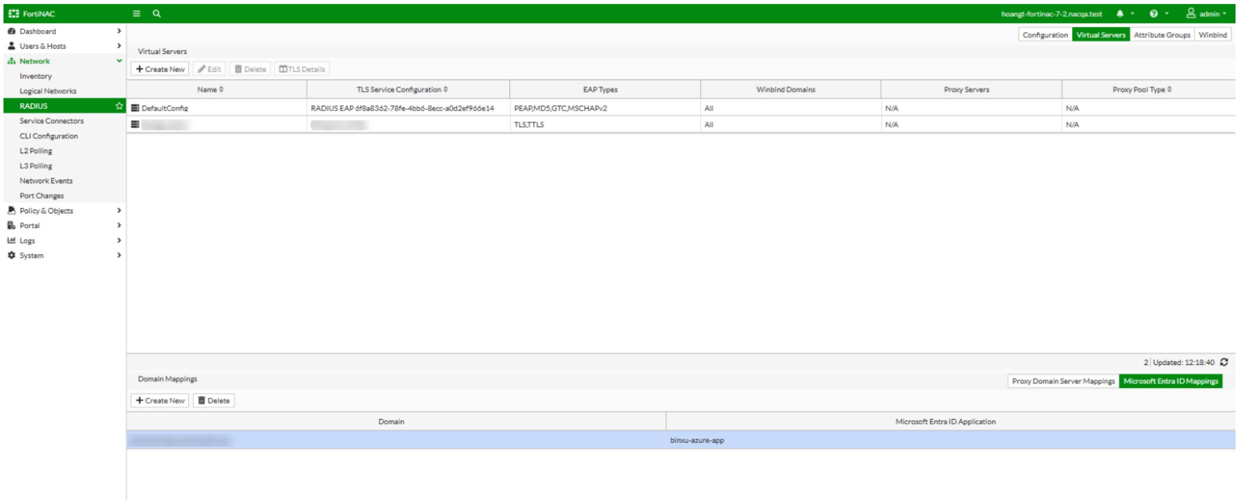
Authentication Type: Application Secret | Certificate

Application Secret: ••••••••

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

Step 5 - Microsoft Entra ID Mappings

Go to **Network > RADIUS > Virtual Servers** and create a new Microsoft Entra ID Mapping which uses the authentication source created earlier in Service Connectors, in this example, will be "binxu-azure-app".



Virtual Servers

Name	TLS Service Configuration	EAP Types	Winbind Domains	Proxy Servers	Proxy Pool Type
DefaultConfig	RADIUS EAP 6f8a8362-78fe-4bb6-8ecc-a0d2ef966e14	PEAP,MD5,GTC,MSCHAPv2	All	N/A	N/A
[redacted]	[redacted]	TLS,TTLS	All	N/A	N/A

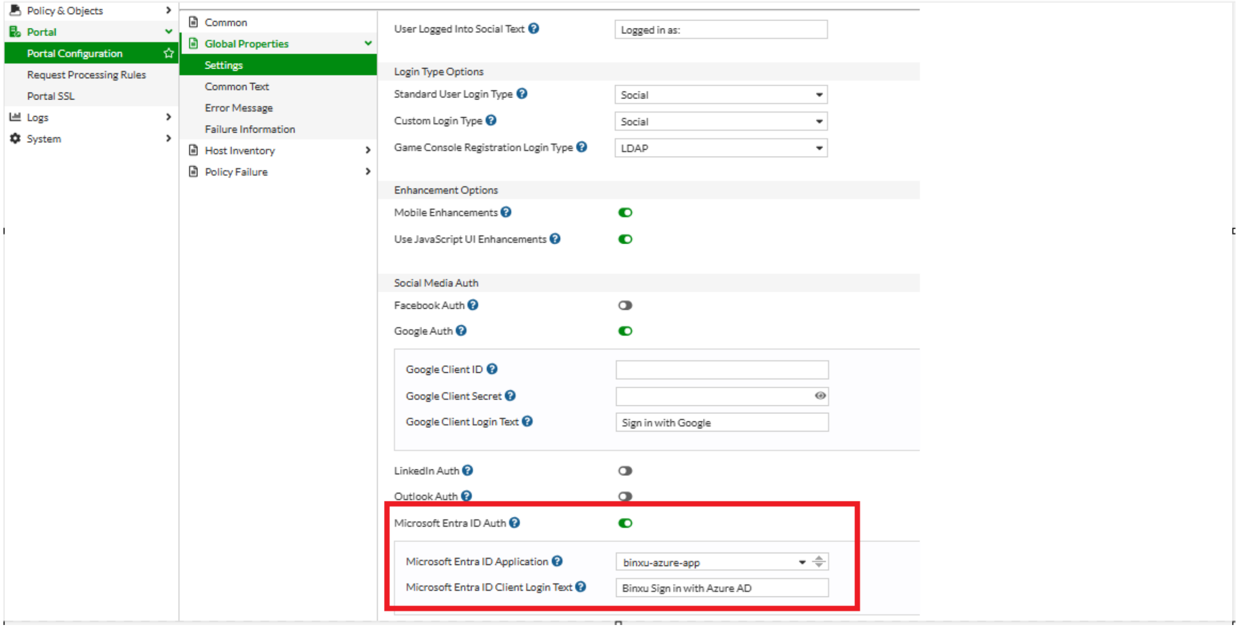
2 | Updated: 12:18:40

Domain Mappings

Domain	Microsoft Entra ID Application
[redacted]	binxu-azure-app

Step 6 - 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 "binxu-azure-app", and create a client Login text.



User Logged Into Social Text: Logged in as:

Login Type Options

- Standard User Login Type: Social
- Custom Login Type: Social
- Game Console Registration Login Type: LDAP

Enhancement Options

- Mobile Enhancements: ●
- Use JavaScript UI Enhancements: ●

Social Media Auth

- Facebook Auth: ○
- Google Auth: ●
  - Google Client ID:
  - Google Client Secret:
  - Google Client Login Text: Sign in with Google
- LinkedIn Auth: ○
- Outlook Auth: ○
- Microsoft Entra ID Auth: ●
  - Microsoft Entra ID Application: binxu-azure-app
  - Microsoft Entra ID Client Login Text: Binxu Sign in with Azure AD

Continue to Step 7 - Windows Client Configuration on page 18 to finish up with the rest of the configurations.

Step 7 - Windows Client Configuration

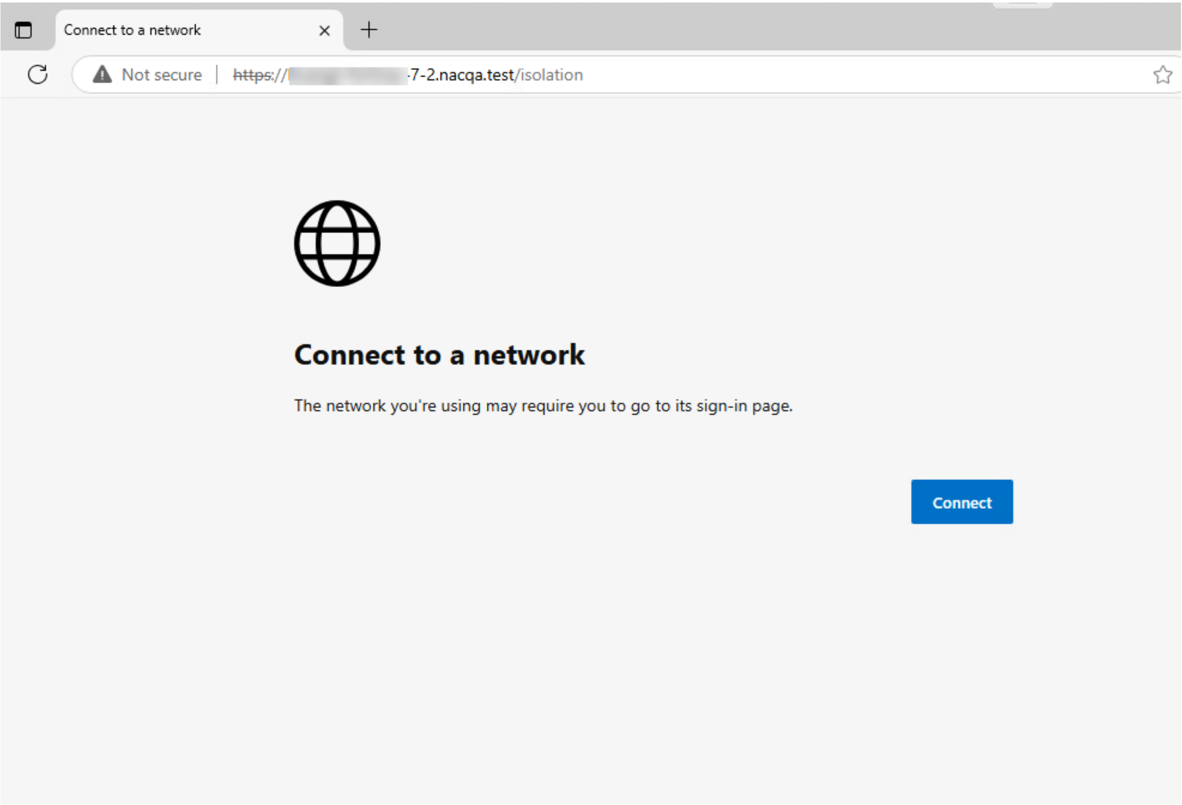
Part 1 - Disable dot1x on Host

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.

Part 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**.

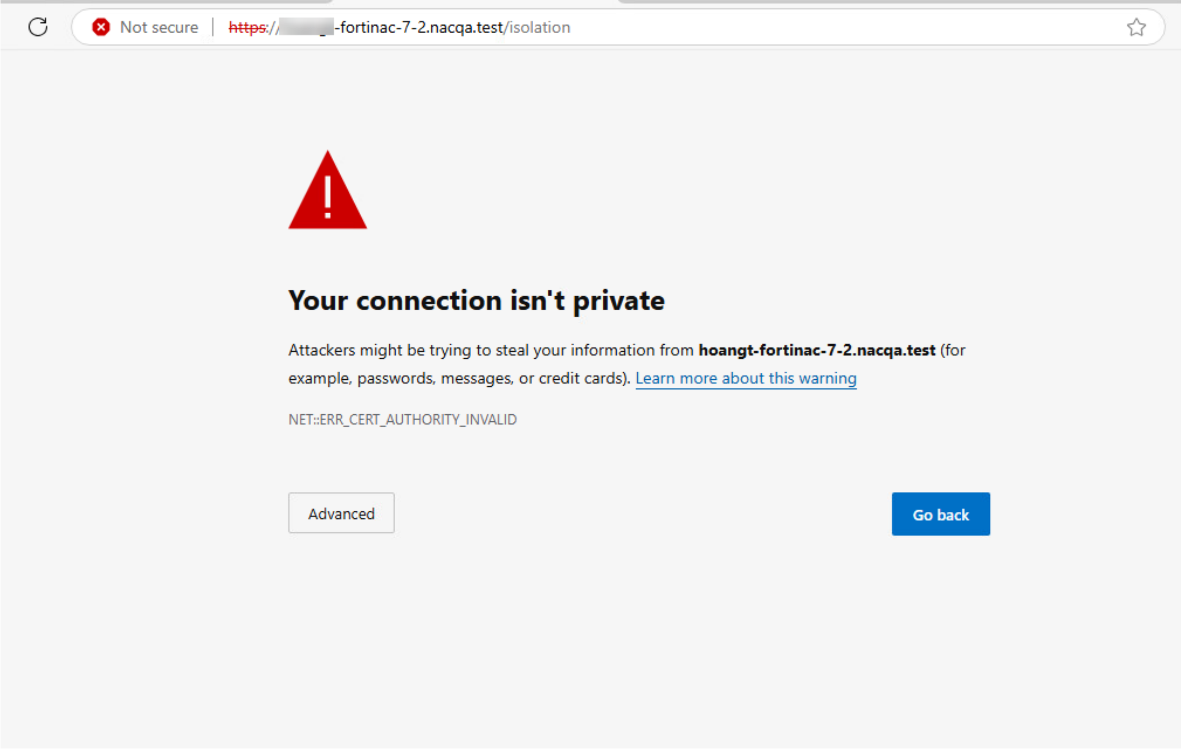


~~https~~://[redacted]7-2.nacqa.test/isolation

Connect to a network

The network you're using may require you to go to its sign-in page.

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

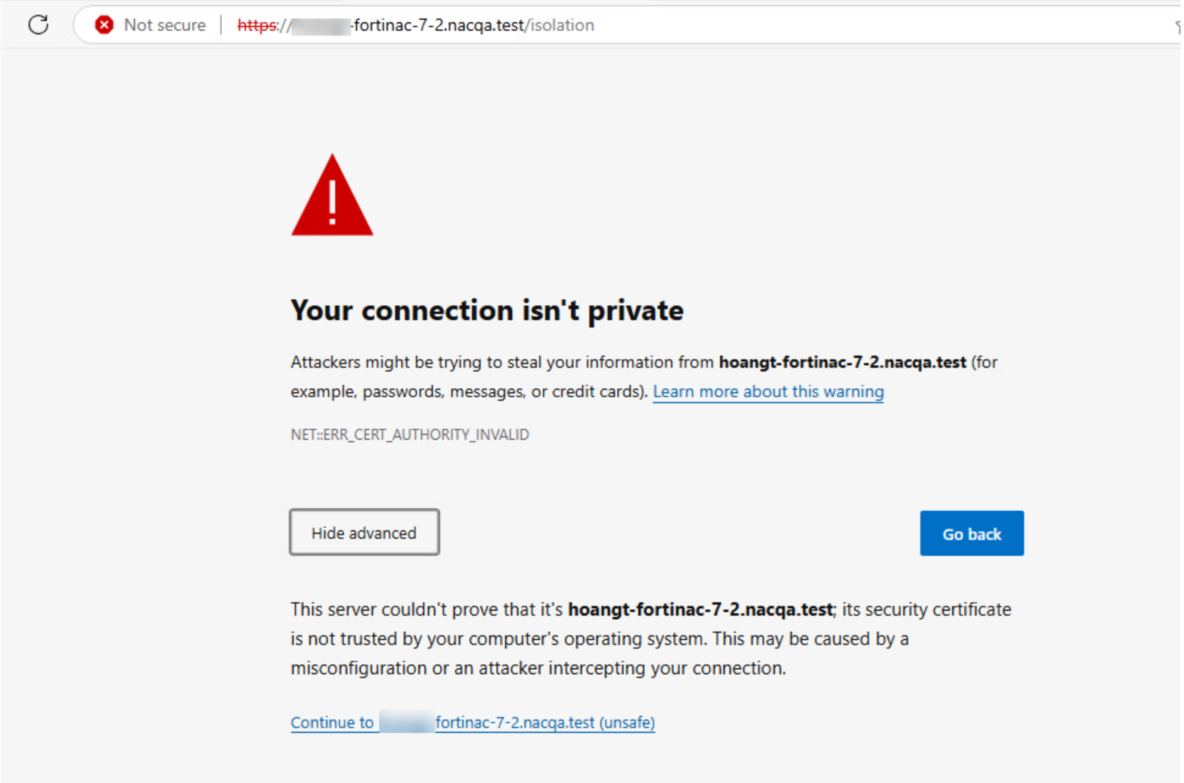


Your connection isn't private

Attackers might be trying to steal your information from **hoangt-fortinac-7-2.nacqa.test** (for example, passwords, messages, or credit cards). Learn more about this warning

NET::ERR_CERT_AUTHORITY_INVALID

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



Your connection isn't private

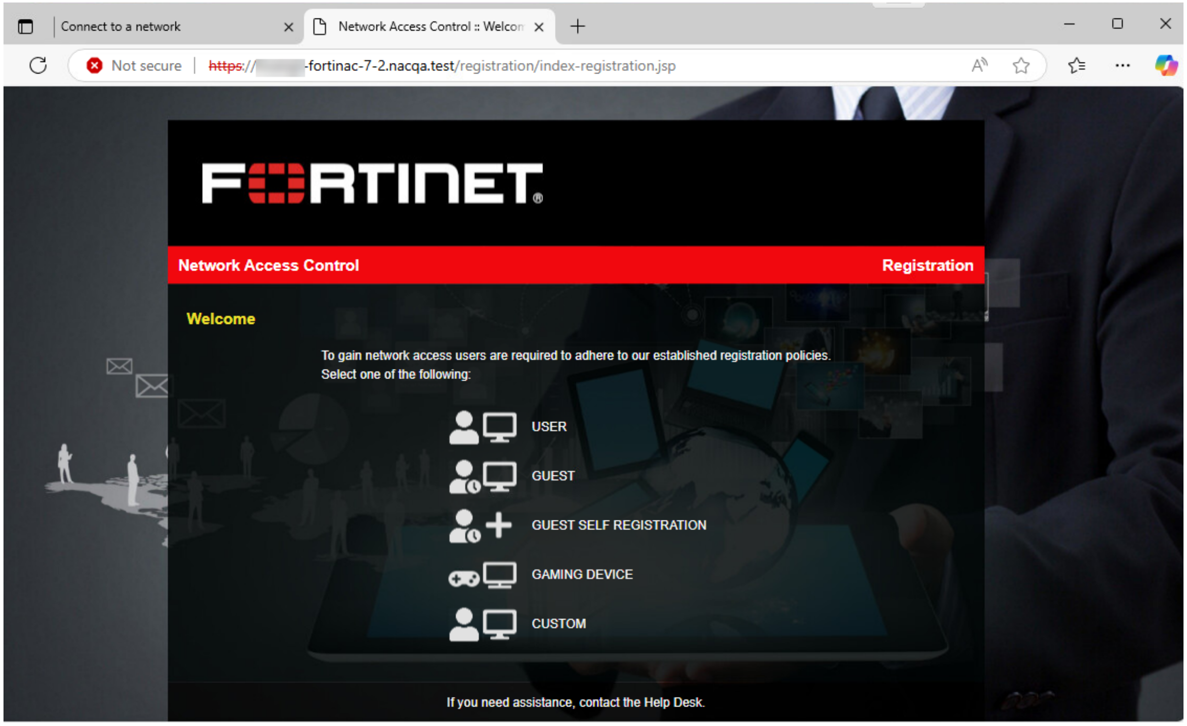
Attackers might be trying to steal your information from **hoangt-fortinac-7-2.nacqa.test** (for example, passwords, messages, or credit cards). Learn more about this warning

NET::ERR_CERT_AUTHORITY_INVALID

This server couldn't prove that it's **hoangt-fortinac-7-2.nacqa.test**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Continue to [redacted]fortinac-7-2.nacqa.test (unsafe)

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


Connect to a network
Network Access Control :: Welcon
Not secure
https://[redacted]-fortinac-7-2.nacqa.test/registration/index-registration.jsp
FORTINET

Network Access Control

Registration

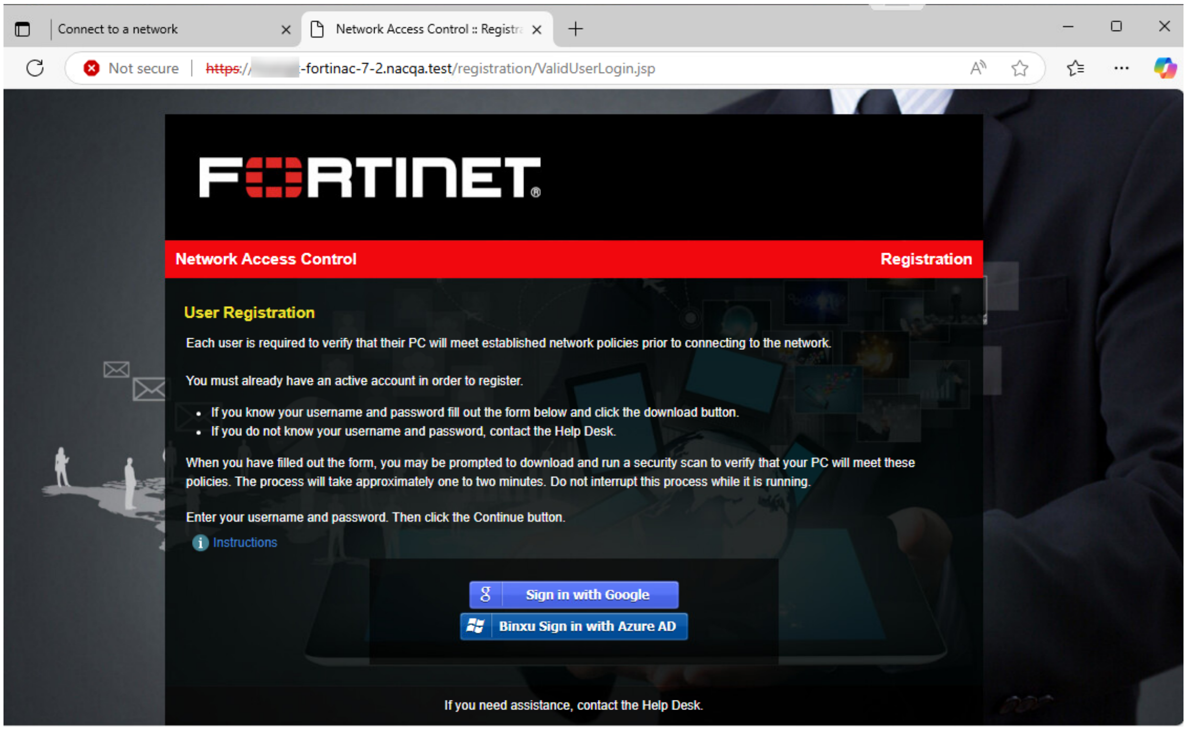
Welcome

To gain network access users are required to adhere to our established registration policies.
Select one of the following:

- USER
- GUEST
- GUEST SELF REGISTRATION
- GAMING DEVICE
- CUSTOM

If you need assistance, contact the Help Desk.

7. Then click the Microsoft Entra ID signin button, in this example, it will be Benxu Sign in with Microsoft Entra ID.


Connect to a network
Network Access Control :: Registr
Not secure
https://[redacted]-fortinac-7-2.nacqa.test/registration/ValidUserLogin.jsp
FORTINET

Network Access Control

Registration

User Registration

Each user is required to verify that their PC will meet established network policies prior to connecting to the network.

You must already have an active account in order to register.

- If you know your username and password fill out the form below and click the download button.
- If you do not know your username and password, contact the Help Desk.

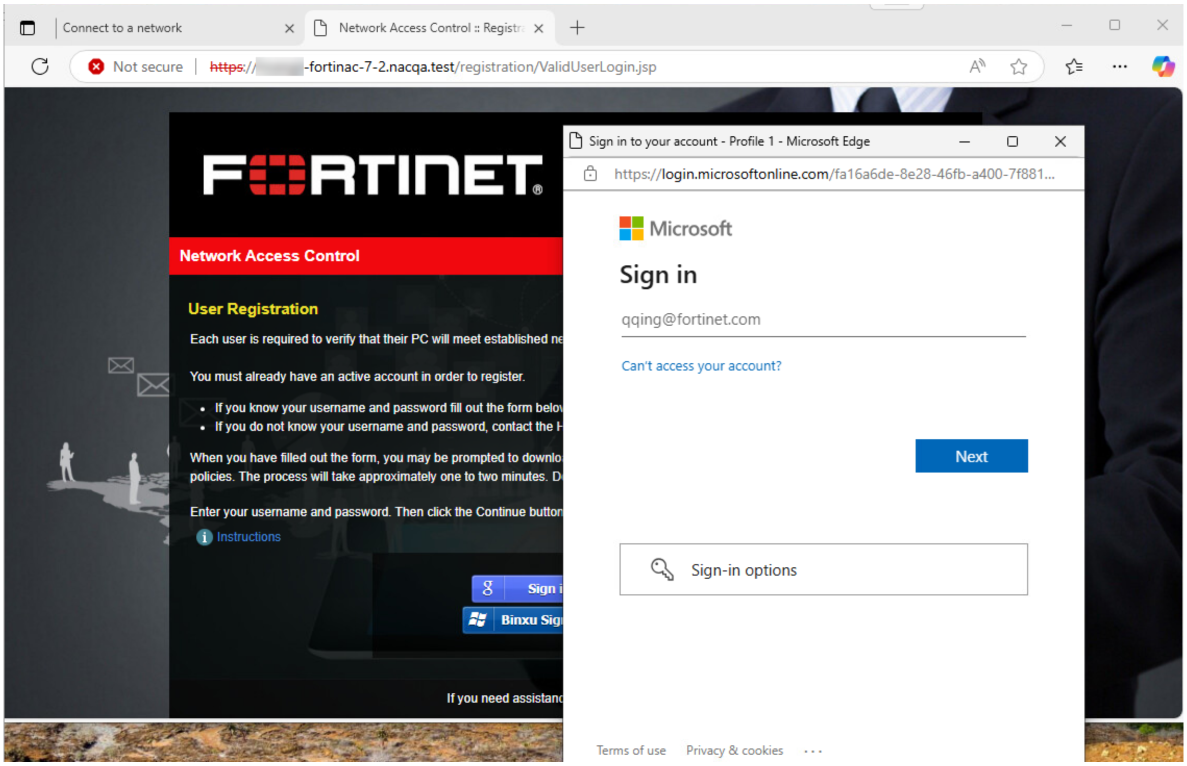
When you have filled out the form, you may be prompted to download and run a security scan to verify that your PC will meet these policies. The process will take approximately one to two minutes. Do not interrupt this process while it is running.

Enter your username and password. Then click the Continue button.

Instructions

If you need assistance, contact the Help Desk.

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



Connect to a network
Network Access Control :: Registr
Not secure
https://[redacted]-fortinac-7-2.nacqa.test/registration/ValidUserLogin.jsp
FORTINET
Sign in to your account - Profile 1 - Microsoft Edge
https://login.microsoftonline.com/fa16a6de-8e28-46fb-a400-7f881...
Microsoft

Network Access Control

User Registration

Each user is required to verify that their PC will meet established ne

You must already have an active account in order to register.

- If you know your username and password fill out the form belov
- If you do not know your username and password, contact the H

When you have filled out the form, you may be prompted to downlo policies. The process will take approximately one to two minutes. D

Enter your username and password. Then click the Continue button

Instructions

If you need assistanc

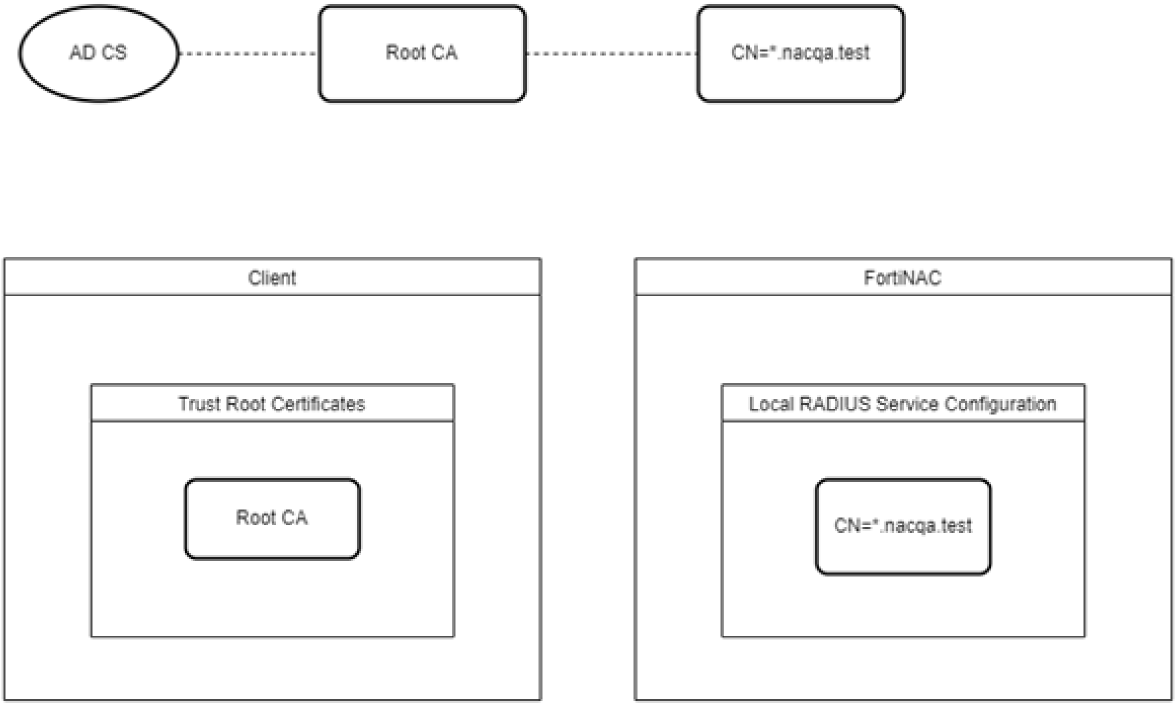
Sign in

qqing@fortinet.com

Microsoft Entra ID Authentication using Certificate

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.

Here is the topology of certificate configuration, the client needs to acquire server certificate from FortNAC.

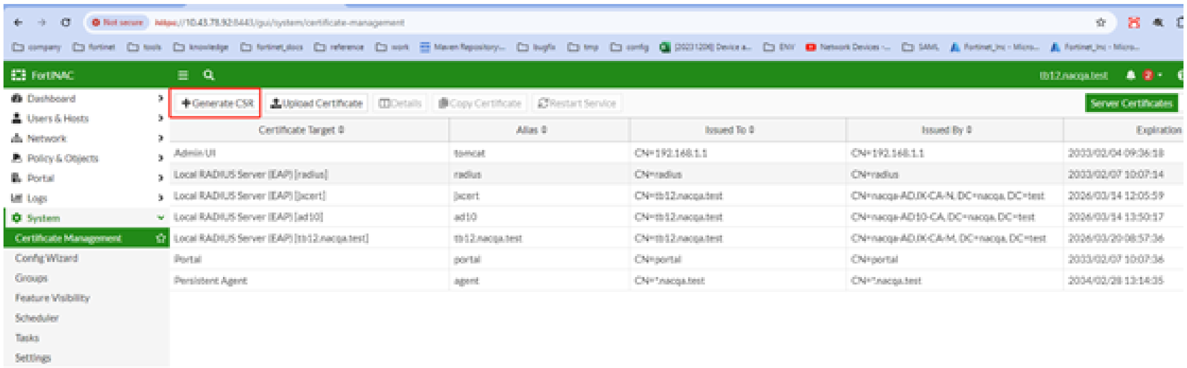


Step 1 - Configure Local RADIUS TLS Service Configuration

Step 1 - Generate Certificate Signing Request (CSR)

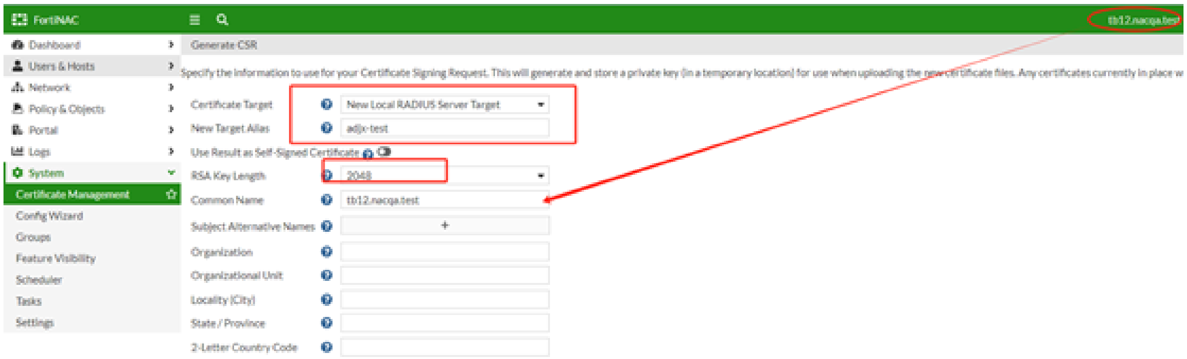
Certificate Signing Request (CSR) is an encoded file that contains the public key for requesting certificate from Certificate Authority(CA).

1. Go to Certificate Management, click **+ Generate CSR**.



Certificate Target	Alias	Issued To	Issued By	Expiration
Admin UI	tomcat	CN=192.168.1.1	CN=192.168.1.1	2033/02/04 09:36:18
Local RADIUS Server (EAP) [radius]	radius	CN=radius	CN=radius	2033/02/07 10:07:34
Local RADIUS Server (EAP) [jxcert]	jxcert	CN=tb12.nacqa.test	CN=nacqa-AD.IX-CA-N, DC=nacqa, DC=test	2026/03/14 12:05:59
Local RADIUS Server (EAP) [ad10]	ad10	CN=tb12.nacqa.test	CN=nacqa-AD10-CA, DC=nacqa, DC=test	2026/03/14 13:50:17
Local RADIUS Server (EAP) [tb12.nacqa.test]	tb12.nacqa.test	CN=tb12.nacqa.test	CN=nacqa-AD.IX-CA-M, DC=nacqa, DC=test	2026/03/20 08:57:36
Portal	portal	CN=portal	CN=portal	2033/02/07 10:07:36
Persistent Agent	agent	CN=*.nacqa.test	CN=*.nacqa.test	2034/02/28 13:14:35

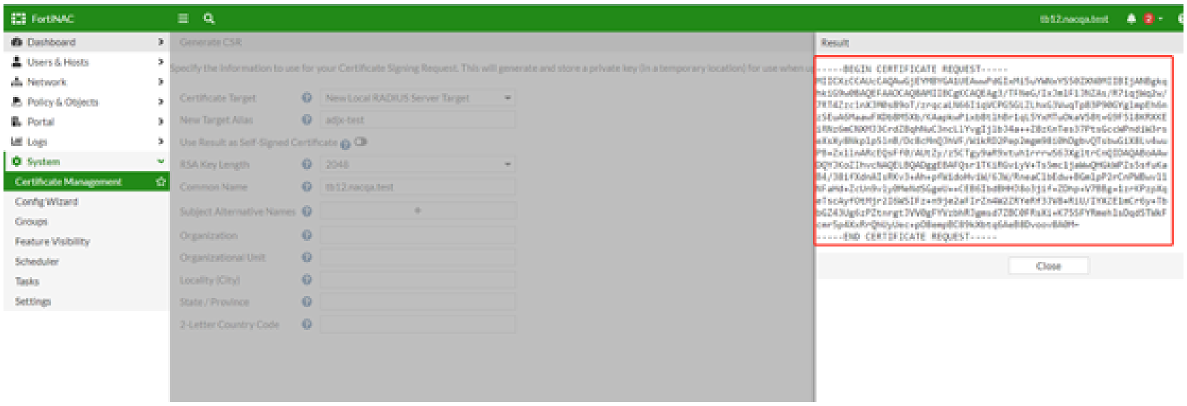
2. Fill in the Certificate Target or the new local radius server target (EAP), new Target Alias, RSA Key Length, and Common name information.



Specify the information to use for your Certificate Signing Request. This will generate and store a private key (in a temporary location) for use when uploading the new certificate files. Any certificates currently in place w

Certificate Target: New Local RADIUS Server Target
New Target Alias: adjx-test
Use Result as Self-Signed Certificate
RSA Key Length: 2048
Common Name: tb12.nacqa.test
Subject Alternative Names: +
Organization:
Organizational Unit:
Locality (City):
State / Province:
2-Letter Country Code:

3. Once the CSR is generated, copy in entire key.



Specify the information to use for your Certificate Signing Request. This will generate and store a private key (in a temporary location) for use when u

Certificate Target: New Local RADIUS Server Target

New Target Alias: adjx-test

Use Result as Self-Signed Certificate

RSA Key Length: 2048

Common Name: tb12.nacqa.test

Subject Alternative Names

Organization

Organizational Unit

Locality (City)

State / Province

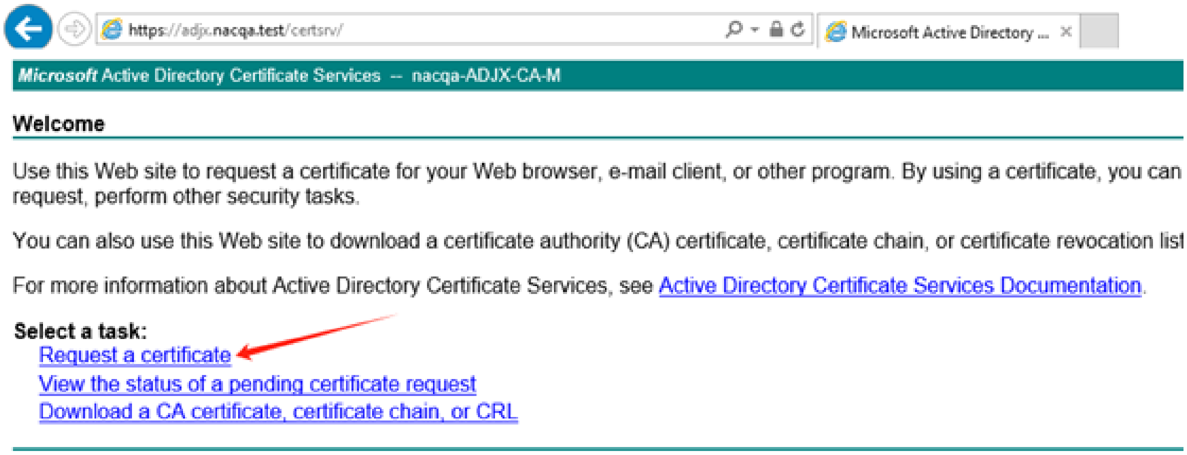
2-Letter Country Code

```
-----BEGIN CERTIFICATE REQUEST-----
[illegible]
-----END CERTIFICATE REQUEST-----
```

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**


https://adjx.nacqa.test/certsrv/
Microsoft Active Directory ...

Microsoft Active Directory Certificate Services -- nacqa-ADJX-CA-M

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

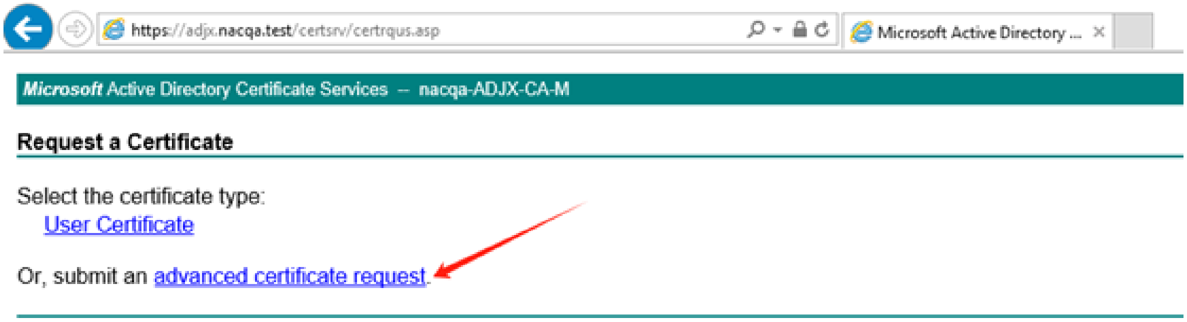
Request a certificate

View the status of a pending certificate request

Download a CA certificate, certificate chain, or CRL

.

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


https://adjx.nacqa.test/certsrv/certrqus.asp
Microsoft Active Directory ...

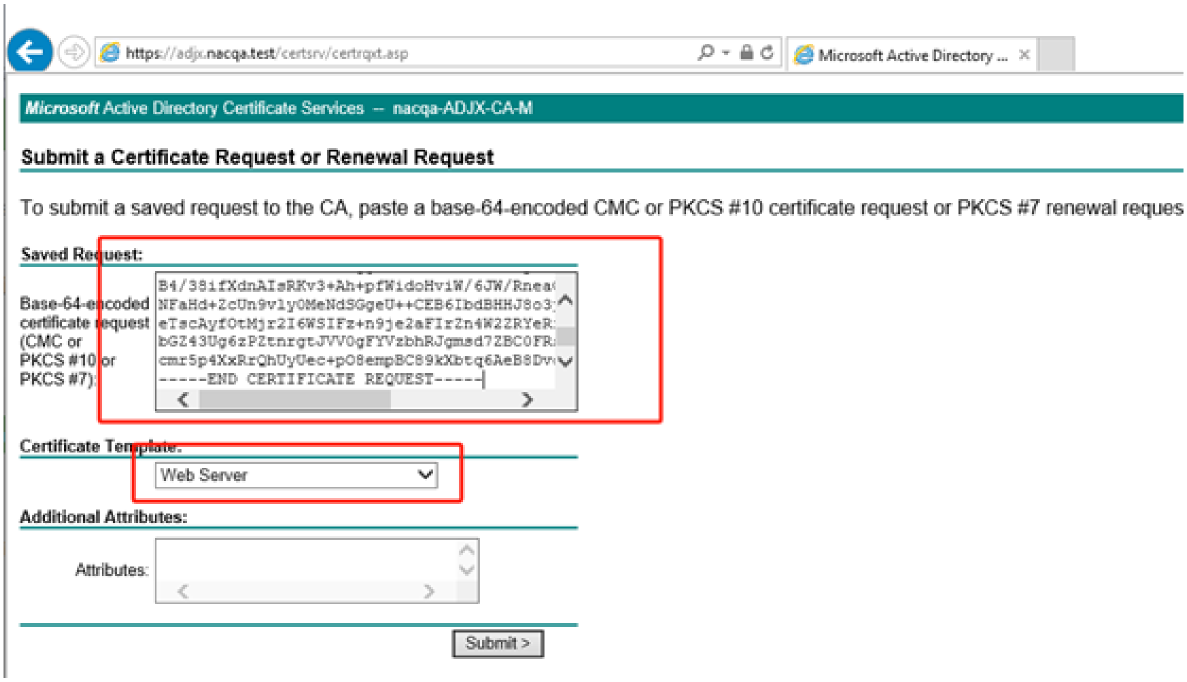
Microsoft Active Directory Certificate Services -- nacqa-ADJX-CA-M

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an 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**.


https://adjx.nacqa.test/certsrv/certrqxt.asp
Microsoft Active Directory ...

Microsoft Active Directory Certificate Services -- nacqa-ADJX-CA-M

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal reques

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
B4/38ifXdnAIsRKv3+Ah+pfWidoHviW/6JW/Rnea
NFaHd+ZcUn9vly0MeNdSGgeU++CEB6IbdBHHJ8o3
eTscAyfOtMjr2I6WSIFz+n9je2aFIrZn4W2ZRYeR
bGZ43Ug6zPZtnrgtJVV0gFYVzbhRJgmsd7ZBC0FR
cmr5p4XxRrQhUyUec+pO8empBC89kXbtq6AeB8Dv
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

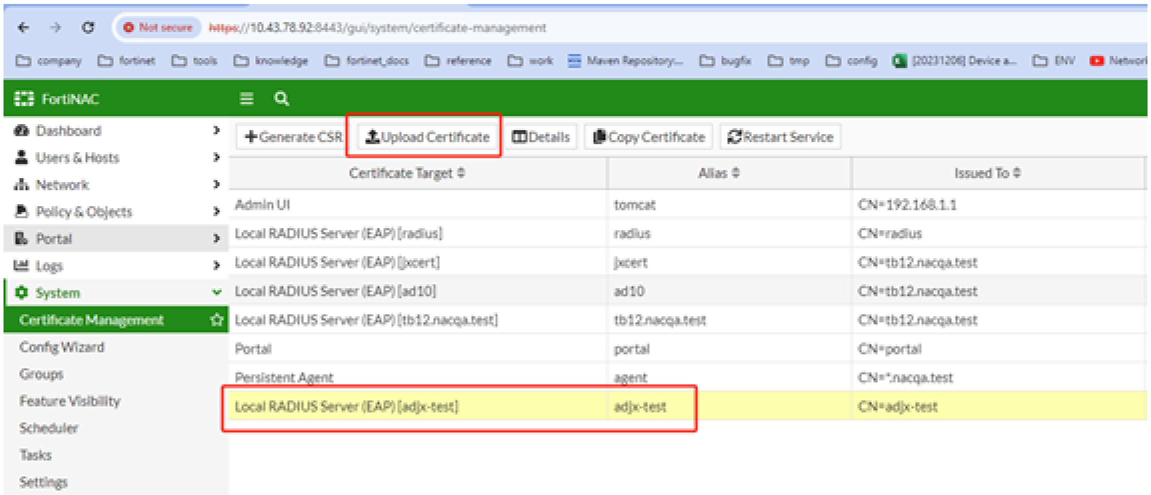
Additional Attributes:

Attributes:

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

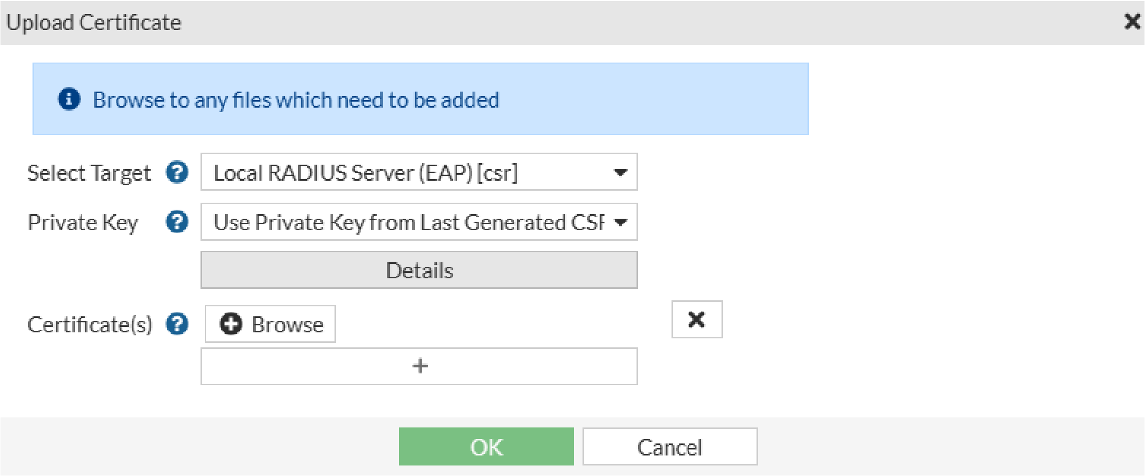
Step 3 - Upload the certificate onto FortiNAC

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



Certificate Target	Alias	Issued To
Admin UI	tomcat	CN=192.168.1.1
Local RADIUS Server (EAP) [radius]	radius	CN=radius
Local RADIUS Server (EAP) [jxcert]	jxcert	CN=tb12.nacqa.test
Local RADIUS Server (EAP) [ad10]	ad10	CN=tb12.nacqa.test
Local RADIUS Server (EAP) [tb12.nacqa.test]	tb12.nacqa.test	CN=tb12.nacqa.test
Portal	portal	CN=portal
Persistent Agent	agent	CN=*.nacqa.test
Local RADIUS Server (EAP) [adjx-test]	adjx-test	CN=adjx-test

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**.

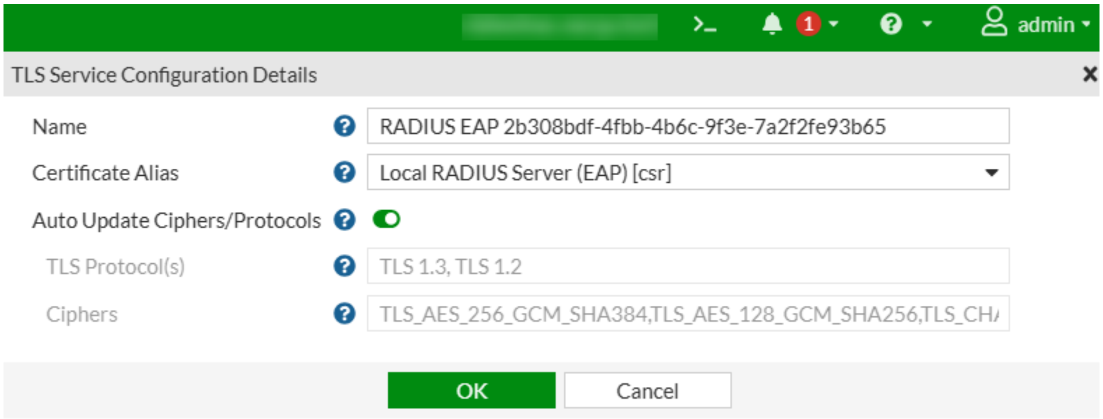

Upload Certificate

Browse to any files which need to be added

Select Target: Local RADIUS Server (EAP) [csr]

Private Key: Use Private Key from Last Generated CSR

4. Restart the service for the certificate to take into effect.
5. Go to **Network > RADIUS**, click **DefaultConfig** and select **Edit**, configure the **TLS configuration Details** by selecting "LOCAL RADIUS Server (EAP) [csr]" as the **Certificate Alias**, and click **OK**.

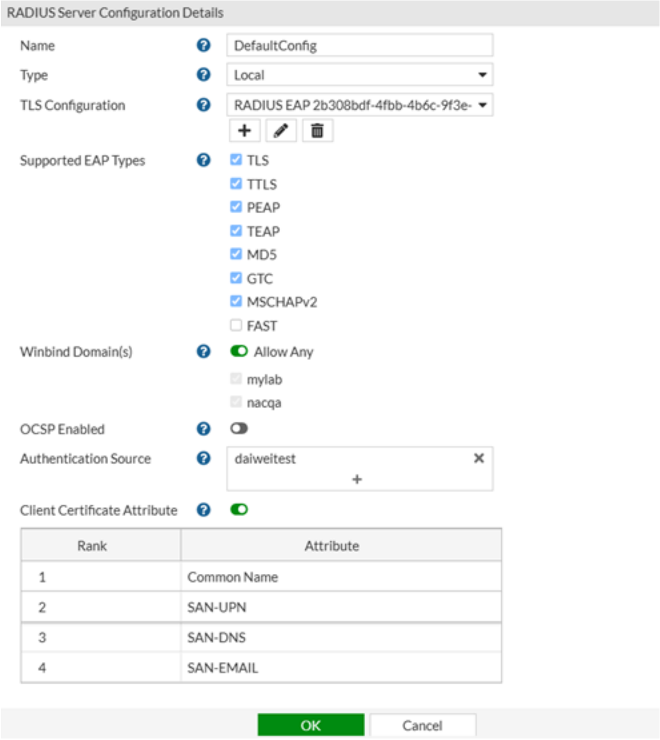


TLS Service Configuration Details

Name	RADIUS EAP 2b308bdf-4fbb-4b6c-9f3e-7a2f2fe93b65
Certificate Alias	Local RADIUS Server (EAP) [csr]
Auto Update Ciphers/Protocols	●
TLS Protocol(s)	TLS 1.3, TLS 1.2
Ciphers	TLS_AES_256_GCM_SHA384,TLS_AES_128_GCM_SHA256,TLS_CH/

Step 4 - 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.



RADIUS Server Configuration Details

Name: DefaultConfig

Type: Local

TLS Configuration: RADIUS EAP 2b308bdf-4fbb-4b6c-9f3e-

Supported EAP Types:
☑ TLS
☑ TTLS
☑ PEAP
☑ TEAP
☑ MD5
☑ GTC
☑ MSCHAPv2
☐ FAST

Winbind Domain(s): ● Allow Any
☐ mylab
☐ nacqa

OCSP Enabled: ○

Authentication Source: daiweitest

Client Certificate Attribute: ●

Rank	Attribute
1	Common Name
2	SAN-UPN
3	SAN-DNS
4	SAN-EMAIL

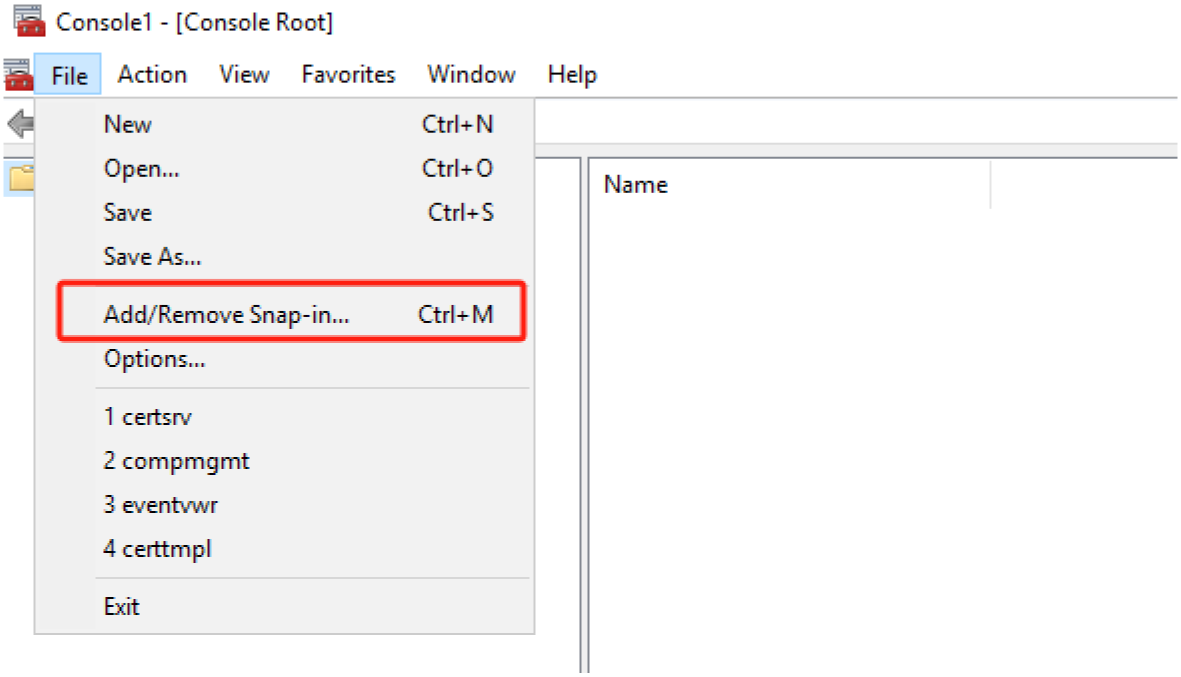
1. In **Support EAP Types**, select **TLS** and **Client Certificate Attribute** will appear.
2. Enable the toggle switch button, and configure the ranking in which the attribute can be used to retrieve the username. Currently, 4 values are supported: **SAN-UPN,SAN-DNS,SAN-EMAIL, CN**.
3. FortiNAC will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

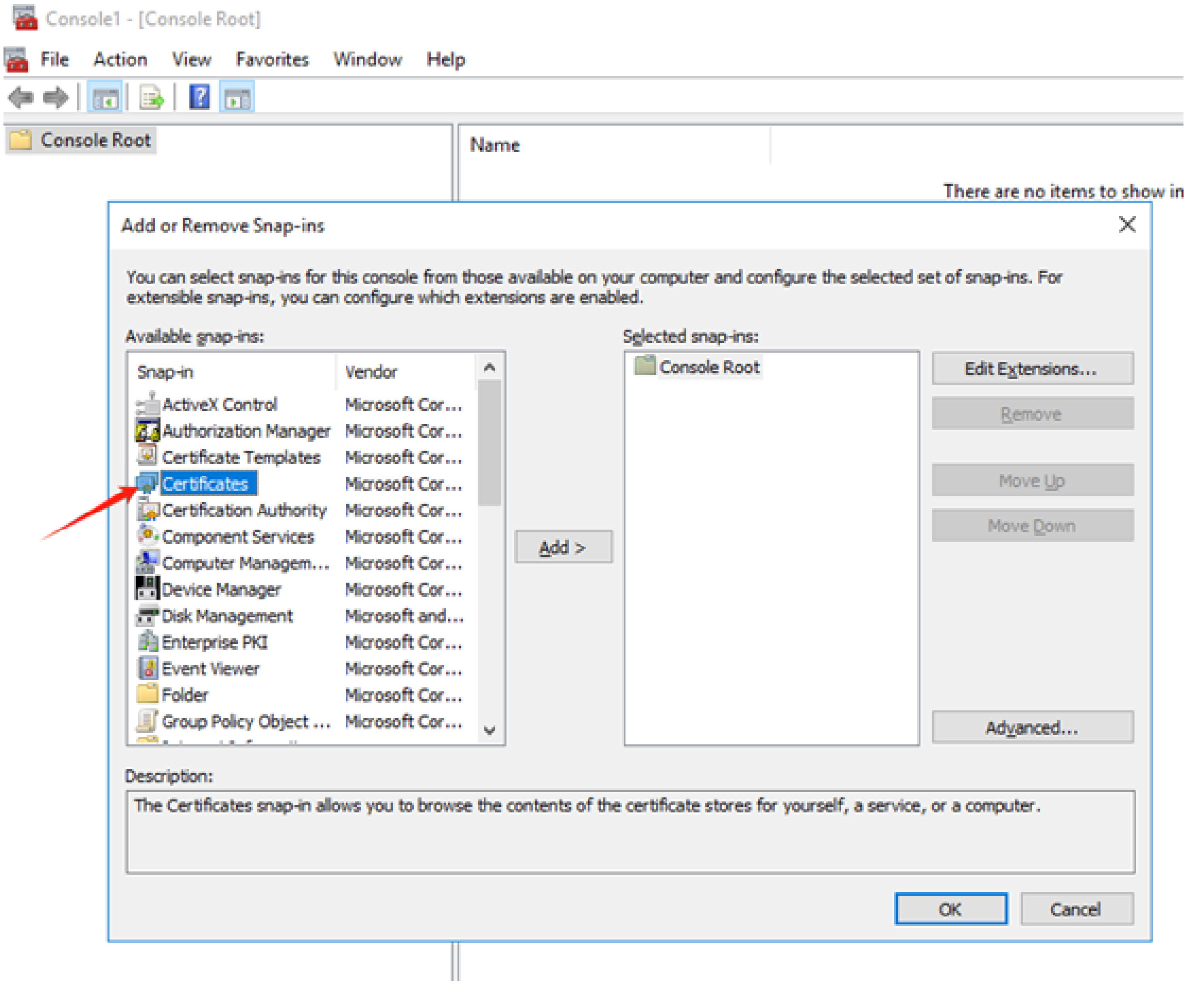
Step 2 - Configure Client Certificate

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**.

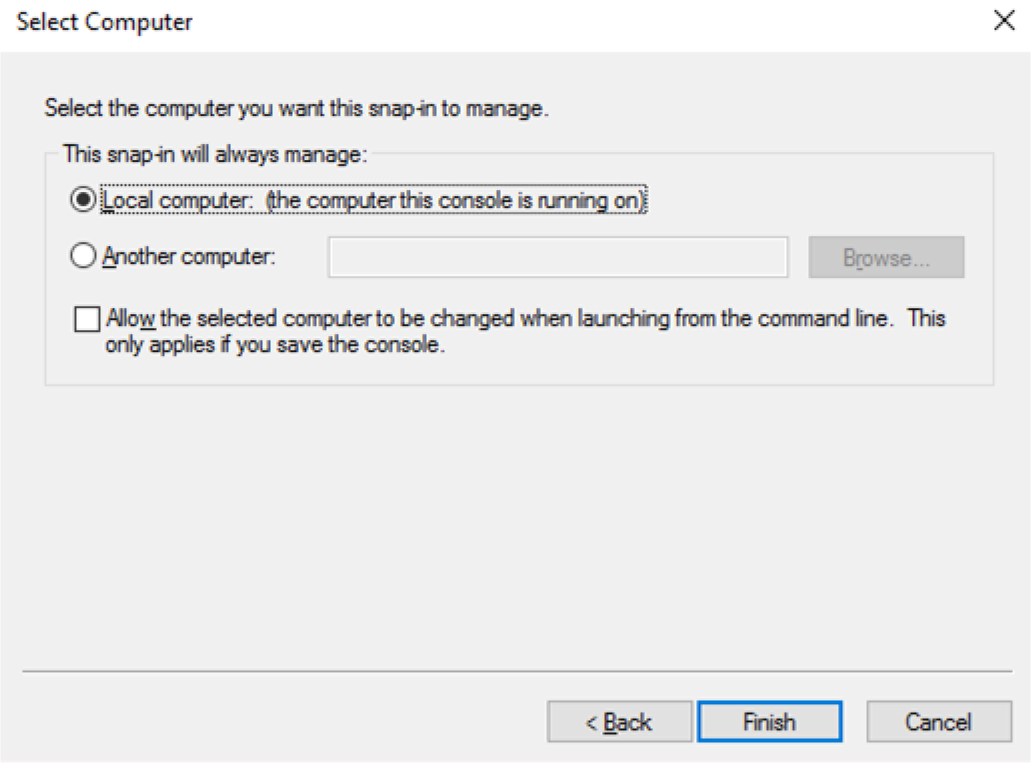


You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Enterprise PKI	Microsoft Cor...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

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**.



Select Computer

Select the computer you want this snap-in to manage.

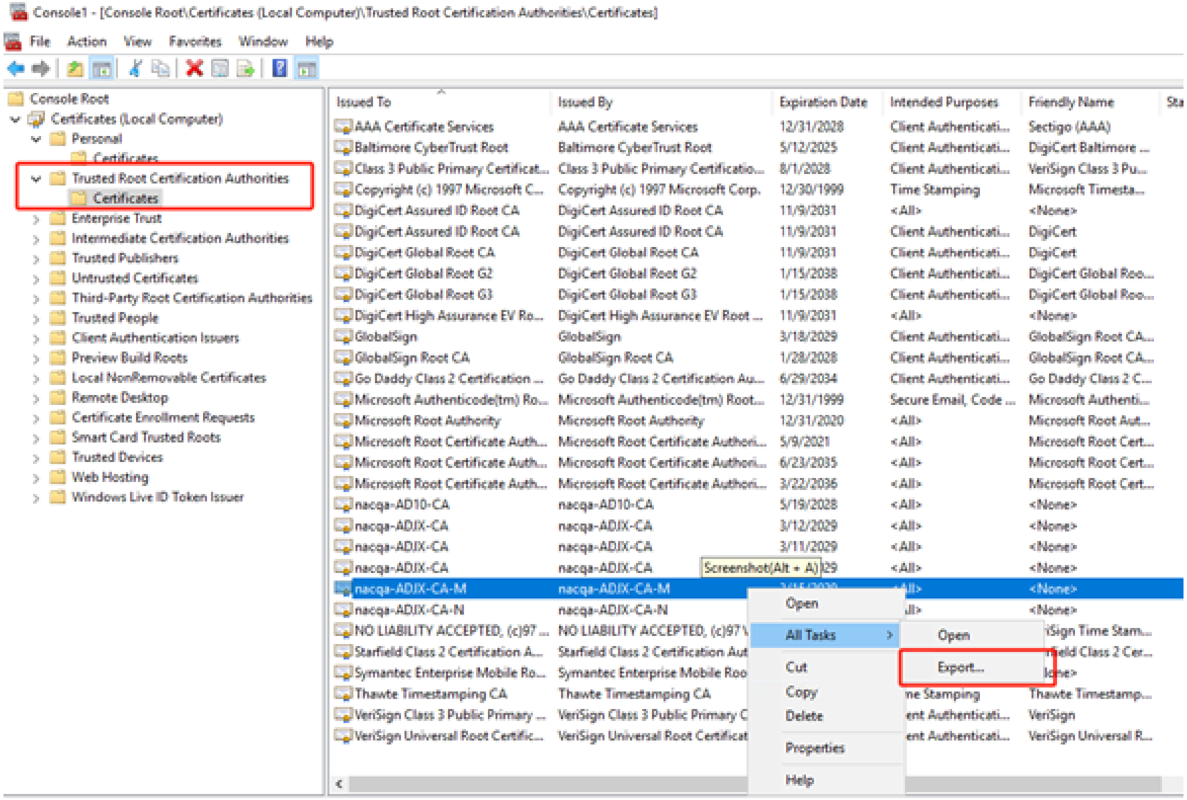
This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer: Browse...

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

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



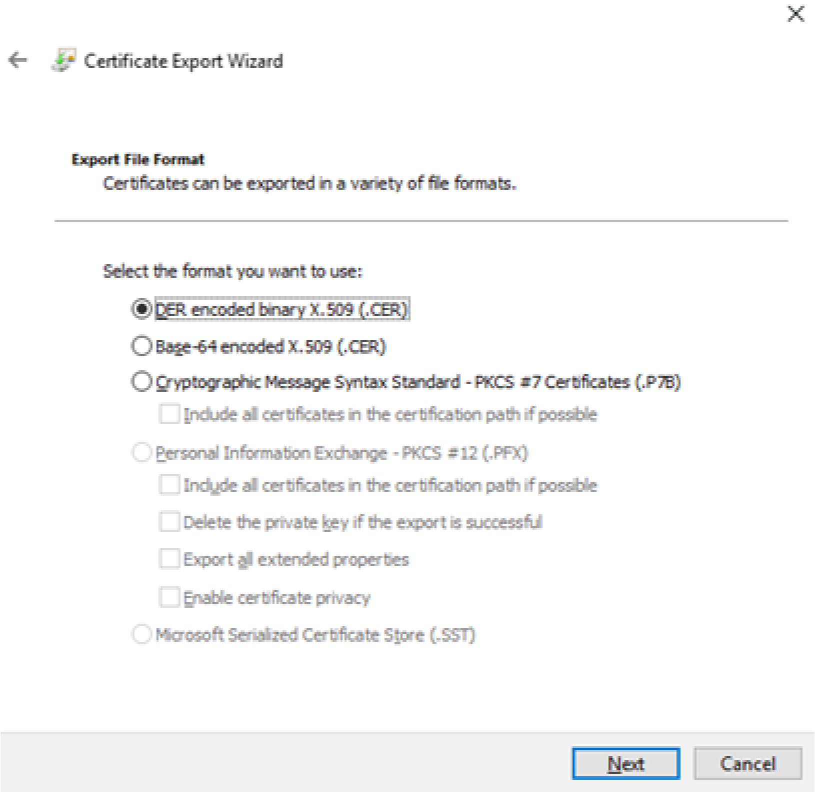
Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\Certificates]

- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - Preview Build Roots
    - Local NonRemovable Certificates
    - Remote Desktop
    - Certificate Enrollment Requests
    - Smart Card Trusted Roots
    - Trusted Devices
    - Web Hosting
    - Windows Live ID Token Issuer

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Sta
AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authenticati...	Sectigo (AAA)	
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati...	DigiCert Baltimore ...	
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Client Authenticati...	VeriSign Class 3 Pu...	
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...	
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	<All>	<None>	
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authenticati...	DigiCert	
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati...	DigiCert	
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati...	DigiCert Global Roo...	
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authenticati...	DigiCert Global Roo...	
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	<All>	<None>	
GlobalSign	GlobalSign	3/18/2029	Client Authenticati...	GlobalSign Root CA...	
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Client Authenticati...	GlobalSign Root CA...	
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	6/29/2034	Client Authenticati...	Go Daddy Class 2 C...	
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...	
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>	Microsoft Root Cert...	
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>	Microsoft Root Cert...	
nacqa-AD10-CA	nacqa-AD10-CA	5/19/2028	<All>	<None>	
nacqa-ADJX-CA	nacqa-ADJX-CA	3/12/2029	<All>	<None>	
nacqa-ADJX-CA	nacqa-ADJX-CA	3/11/2029	<All>	<None>	
nacqa-ADJX-CA	nacqa-ADJX-CA	29	<All>	<None>	
nacqa-ADJX-CA-M	nacqa-ADJX-CA-M	[illegible]	ll>	<None>	
nacqa-ADJX-CA-N	nacqa-ADJX-CA-N		ll>	<None>	
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V			iSign Time Stam...	
Starfield Class 2 Certification A...	Starfield Class 2 Certification Aut			ield Class 2 Cer...	
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Roo			lone>	
Thawte Timestamping CA	Thawte Timestamping CA		ne Stamping	Thawte Timestamp...	
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary C		ent Authenticati...	VeriSign	
VeriSign Universal Root Certific...	VeriSign Universal Root Certificat		ent Authenticati...	VeriSign Universal R...	

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

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



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

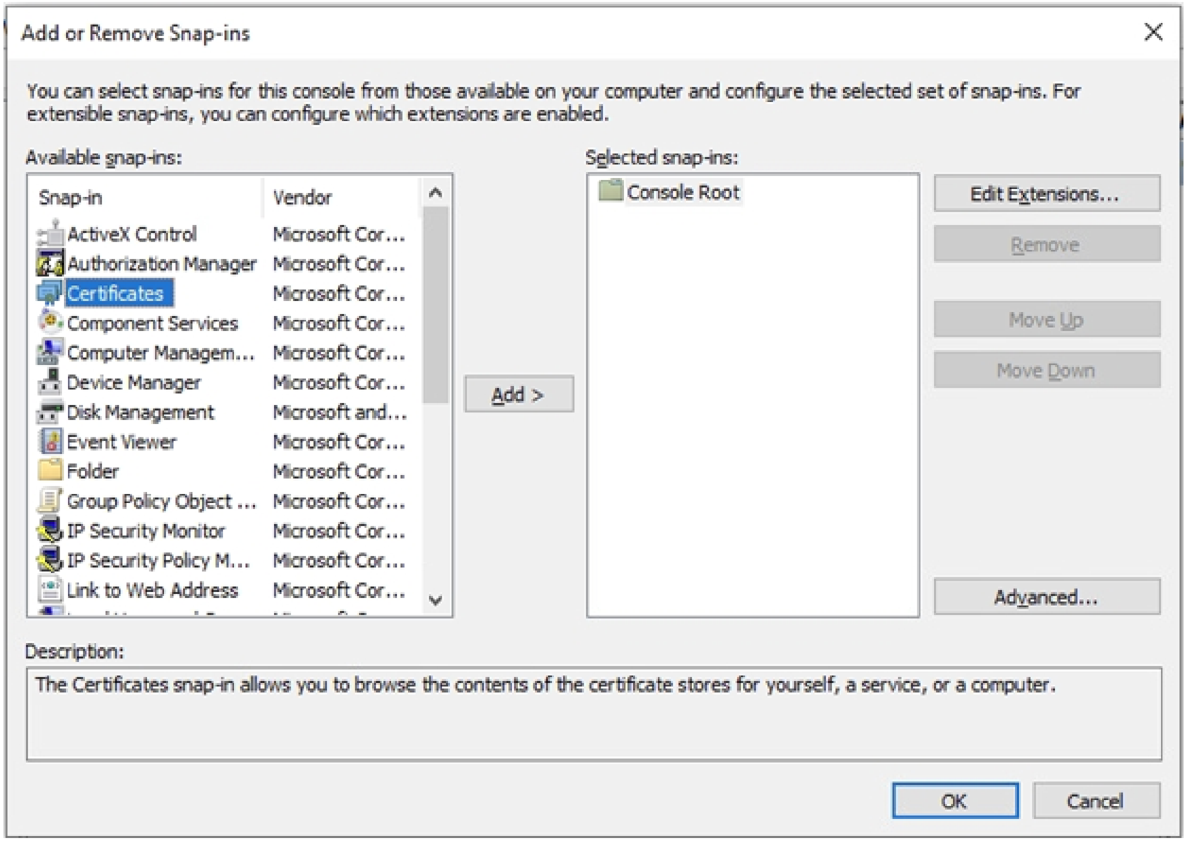
● DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
□ Enable certificate privacy
○ Microsoft Serialized Certificate Store (.SST)

9. 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 folder to be imported.

Import Root CA into Client Trust Root Certificates

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



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

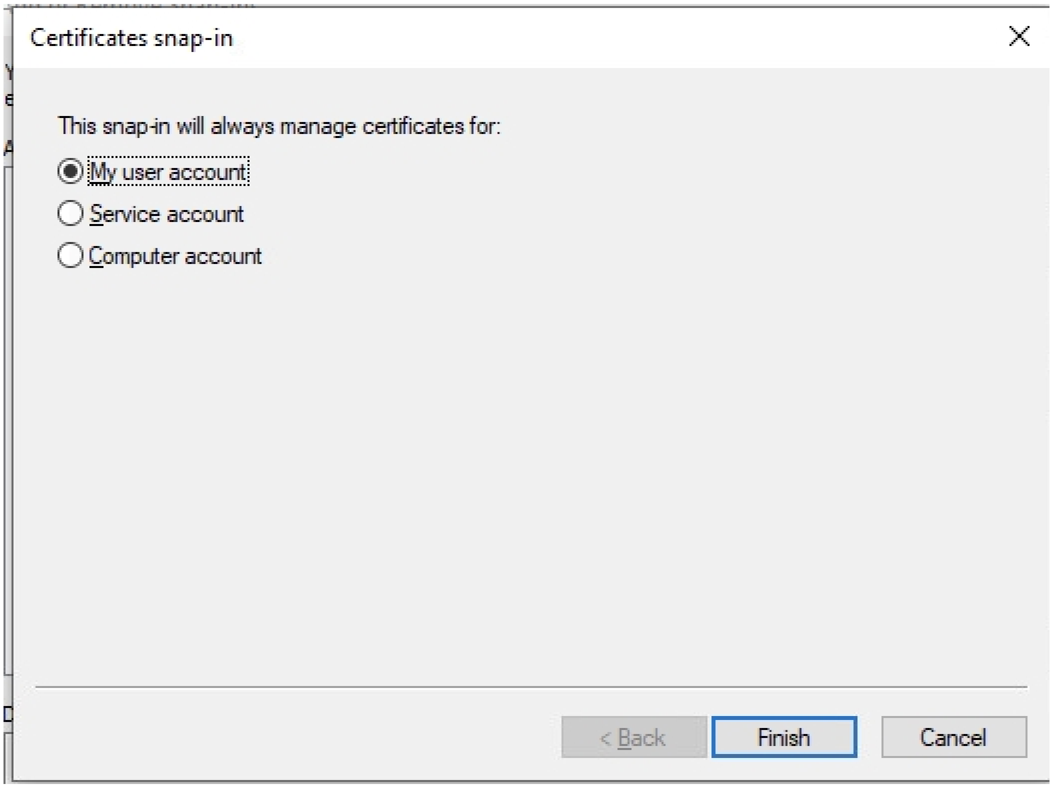
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

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



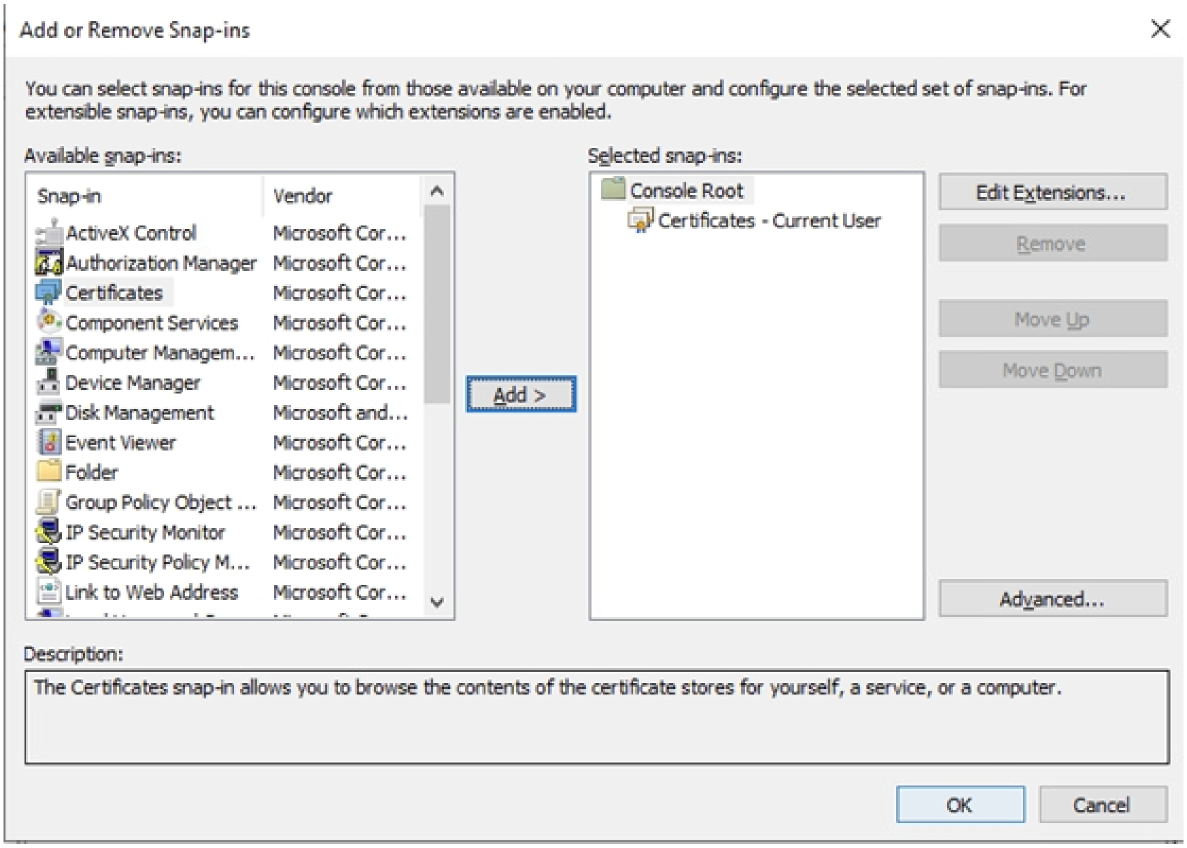
This snap-in will always manage certificates for:

● My user account

○ Service account

○ Computer account

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



Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

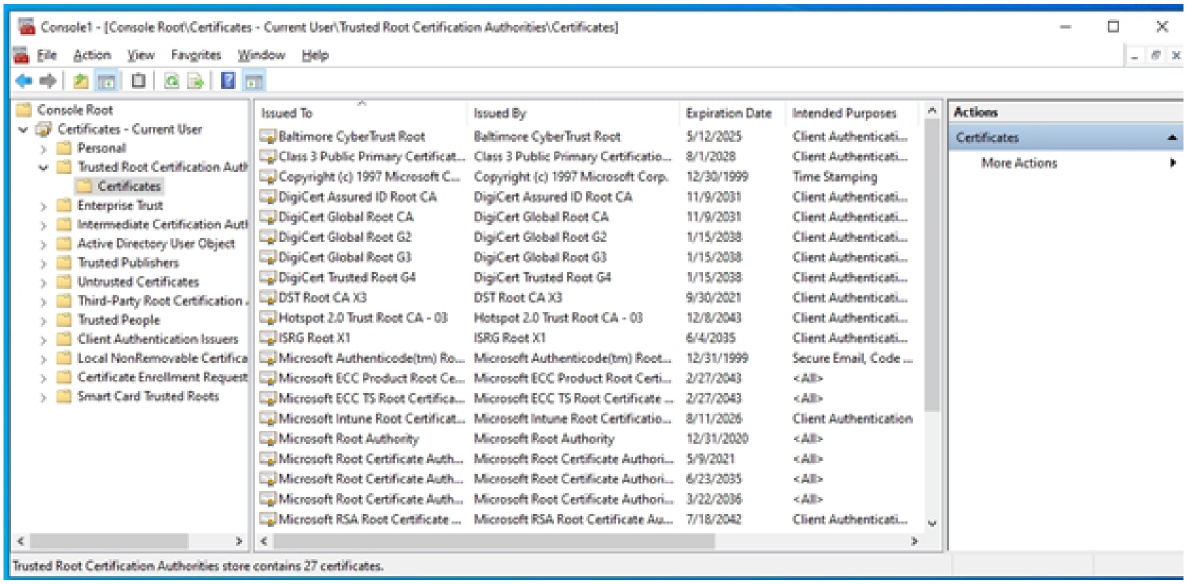
Selected snap-ins:

Console Root
Certificates - Current User

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

5. Select All Tasks > Import



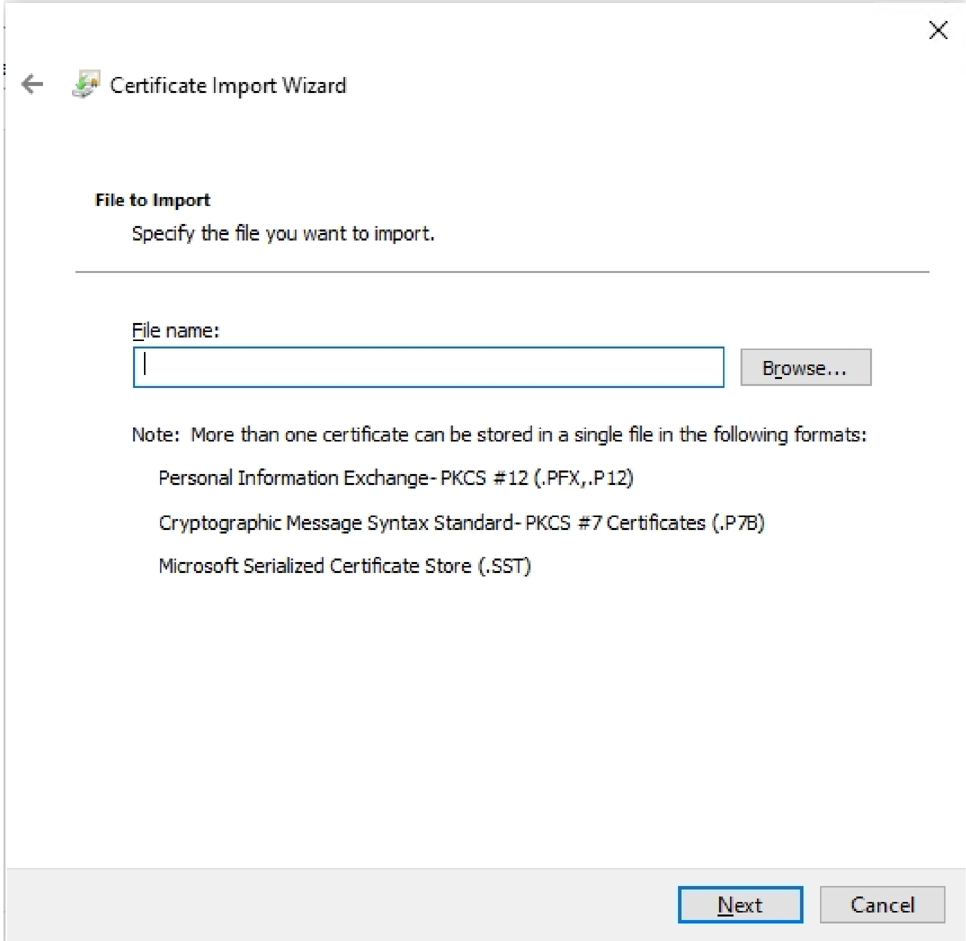
Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification Auth
Certificates
Enterprise Trust
Intermediate Certification Auth
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Client Authentication Issuers
Local NonRemovable Certifica
Certificate Enrollment Request
Smart Card Trusted Roots
Actions
Certificates
More Actions

Issued To	Issued By	Expiration Date	Intended Purposes
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authenticati...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Client Authenticati...
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authenticati...
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authenticati...
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authenticati...
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authenticati...
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati...
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticati...
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Client Authenticati...
ISRG Root X1	ISRG Root X1	6/4/2035	Client Authenticati...
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	2/27/2043	<All>
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>
Microsoft Intune Root Certificat...	Microsoft Intune Root Certificatio...	8/11/2026	Client Authentication
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>
Microsoft RSA Root Certificate ...	Microsoft RSA Root Certificate Au...	7/18/2042	Client Authenticati...

Trusted Root Certification Authorities store contains 27 certificates.

6. Select Root CA file.



File to Import

Specify the file you want to import.

File name:

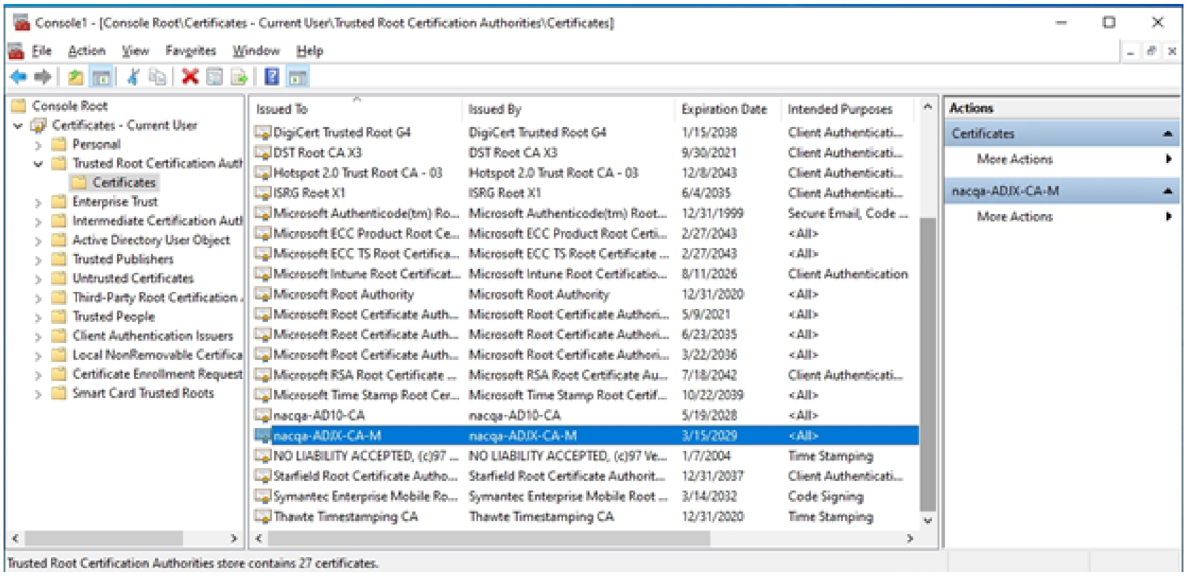
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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



Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification Auth
Certificates
Enterprise Trust
Intermediate Certification Auth
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Client Authentication Issuers
Local NonRemovable Certifica
Certificate Enrollment Request
Smart Card Trusted Roots
Actions
Certificates
More Actions
nacqa-ADJX-CA-M
More Actions

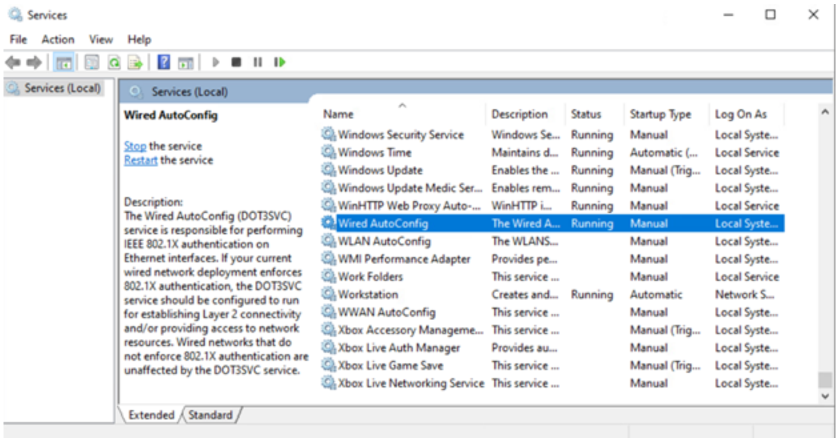
Issued To	Issued By	Expiration Date	Intended Purposes
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authenticati...
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authenticati...
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Client Authenticati...
ISRG Root X1	ISRG Root X1	6/4/2035	Client Authenticati...
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...
Microsoft ECC Product Root Ce...	Microsoft ECC Product Root Certi...	2/27/2043	<All>
Microsoft ECC TS Root Certifica...	Microsoft ECC TS Root Certificate ...	2/27/2043	<All>
Microsoft Intune Root Certificat...	Microsoft Intune Root Certificatio...	8/11/2026	Client Authentication
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	6/23/2035	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	3/22/2036	<All>
Microsoft RSA Root Certificate ...	Microsoft RSA Root Certificate Au...	7/18/2042	Client Authenticati...
Microsoft Time Stamp Root Cer...	Microsoft Time Stamp Root Certif...	10/22/2039	<All>
nacqa-AD10-CA	nacqa-AD10-CA	5/19/2028	<All>
nacqa-ADJX-CA-M	nacqa-ADJX-CA-M	3/15/2029	<All>
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 Ve...	1/7/2004	Time Stamping
Starfield Root Certificate Autho...	Starfield Root Certificate Authorit...	12/31/2037	Client Authenticati...
Symantec Enterprise Mobile Ro...	Symantec Enterprise Mobile Root ...	3/14/2032	Code Signing
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping

Trusted Root Certification Authorities store contains 27 certificates.

Note: After the root certificate is exported, it also need to be uploaded on FortiNAC as well.

Step 3 - Client Configuration

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



Services (Local)

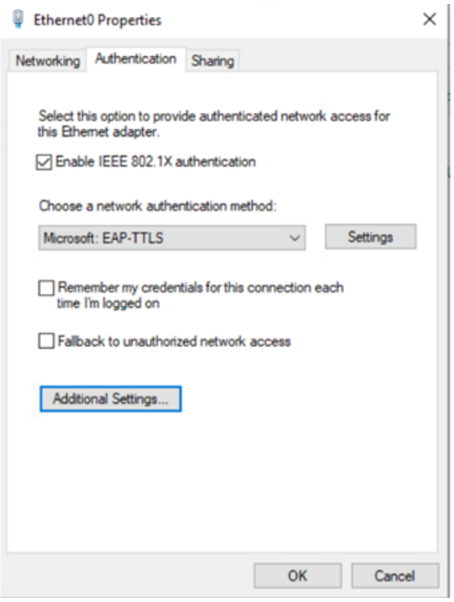
Wired AutoConfig

Stop the service
Restart the service

Description:
The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to network resources. Wired networks that do not enforce 802.1X authentication are unaffected by the DOT3SVC service.

Name	Description	Status	Startup Type	Log On As
Windows Security Service	Windows Se...	Running	Manual	Local Syste...
Windows Time	Maintains d...	Running	Automatic (...	Local Service
Windows Update	Enables the ...	Running	Manual (Trig...	Local Syste...
Windows Update Medic Ser...	Enables rem...	Running	Manual	Local Syste...
WinHTTP Web Proxy Auto-...	WinHTTP i...	Running	Manual	Local Service
Wired AutoConfig	The Wired A...	Running	Manual	Local Syste...
WLAN AutoConfig	The WLANS...		Manual	Local Syste...
WMI Performance Adapter	Provides pe...		Manual	Local Syste...
Work Folders	This service ...		Manual	Local Service
Workstation	Creates and...	Running	Automatic	Network S...
WWAN AutoConfig	This service ...		Manual	Local Syste...
Xbox Accessory Manageme...	This service ...		Manual (Trig...	Local Syste...
Xbox Live Auth Manager	Provides au...		Manual	Local Syste...
Xbox Live Game Save	This service ...		Manual (Trig...	Local Syste...
Xbox Live Networking Service	This service ...		Manual	Local Syste...

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**.



Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

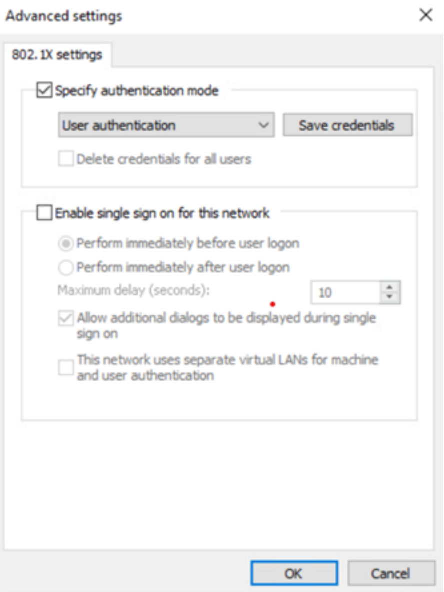
Choose a network authentication method:

Microsoft: EAP-TTLS

□ Remember my credentials for this connection each time I'm logged on

□ Fallback to unauthorized network access

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



Advanced settings

802.1X settings

☑ Specify authentication mode

User authentication | Save credentials

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

○ Perform immediately after user logon

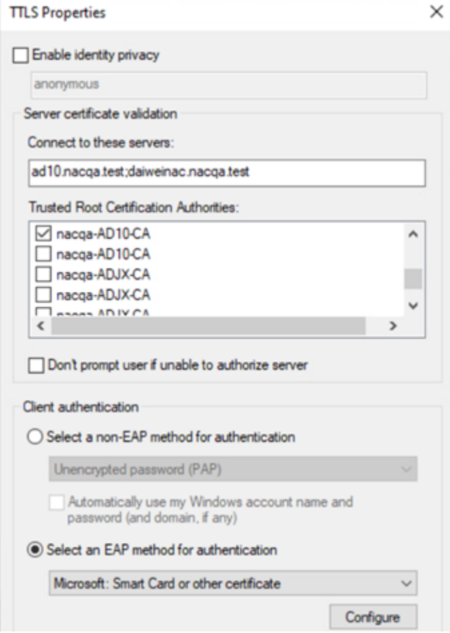
Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

OK | Cancel

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.



TTLS Properties

□ Enable identity privacy

anonymous

Server certificate validation

Connect to these servers:

ad10.nacqa.test;daiweinac.nacqa.test

Trusted Root Certification Authorities:

☑ nacqa-AD10-CA

□ nacqa-AD10-CA

□ nacqa-ADJX-CA

□ nacqa-ADJX-CA

□ Don't prompt user if unable to authorize server

Client authentication

○ Select a non-EAP method for authentication

Unencrypted password (PAP)

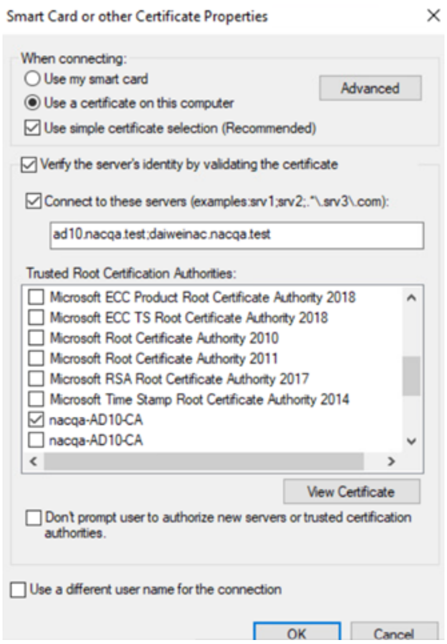
□ Automatically use my Windows account name and password (and domain, if any)

● Select an EAP method for authentication

Microsoft: Smart Card or other certificate

Configure

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



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Verify the server's identity by validating the certificate

☑ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

ad10.nacqa.test;daiweinac.nacqa.test

Trusted Root Certification Authorities:

- □ Microsoft ECC Product Root Certificate Authority 2018
- □ Microsoft ECC TS Root Certificate Authority 2018
- □ Microsoft Root Certificate Authority 2010
- □ Microsoft Root Certificate Authority 2011
- □ Microsoft RSA Root Certificate Authority 2017
- □ Microsoft Time Stamp Root Certificate Authority 2014
- ☑ nacqa-AD10-CA
- □ nacqa-AD10-CA

□ Don't prompt user to authorize new servers or trusted certification authorities.

□ Use a different user name for the connection

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