SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for Wi-Fi Network

gemalto
security to be free

All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Document Number: 007-014051-001, Rev. A

Release Date: January 2018

Contents

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, in this case, Wi-Fi Network, Authenticated with an NPS Radius Server Role which is a Microsoft Windows component.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. SAC enables the implementation of strong two-factor authentication using standard certificates, as well as encryption and digital signing of data. The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering security for web access, network logon, email, and data. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

An effective strong authentication solution must be able to address data breaches on the rise for companies to protect their information assets and comply with privacy regulations. Data encryption is a common technique used by enterprises today, but to be most effective, it must be accompanied by strong two factor user authentication to desktop, mobile, and laptop computer applications. Working together, encryption and authentication reduce risk and stop unauthorized access to sensitive data.

SafeNet smart card certificate-based tokens and secure USB certificate-based tokens are interoperable with Wi-Fi Network, providing a solution for encryption and strong access control that prevents unauthorized access to sensitive data and stops information loss and exposure. The integrated solution delivers greater security, reduced operational costs, and improved compliance by adding smart card-based strong user authentication to Wi-Fi Network.

Gemalto’s X.509 certificate-based USB tokens and smart cards have been integrated with Wi-Fi Network, providing two-factor authentication at both pre-boot and Microsoft Windows levels.

The Gemalto’s X.509 certificate-based USB tokens and smart cards provide secure storage for the certificates needed for endpoint encryption for Wi-Fi Network functionality to boot up. If Gemalto’s X.509 certificate-based USB token or smart card is not inserted in the client machine, or if the certificates are deleted, revoked, or expired, the Wi-Fi Network software will not boot up and the data on the laptop will stay encrypted and secure.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Wi-Fi Network using Gemalto tokens or smart cards.

It is assumed that the Wi-Fi Network is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

Wi-Fi Network can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC) Typical installation mode**— SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.

For more details about different SAC installation modes, please refer to the Customization section in *SafeNet Authentication Client Administrator Guide.*

Environment

The integration environment that was used in this document is based on the following software versions:

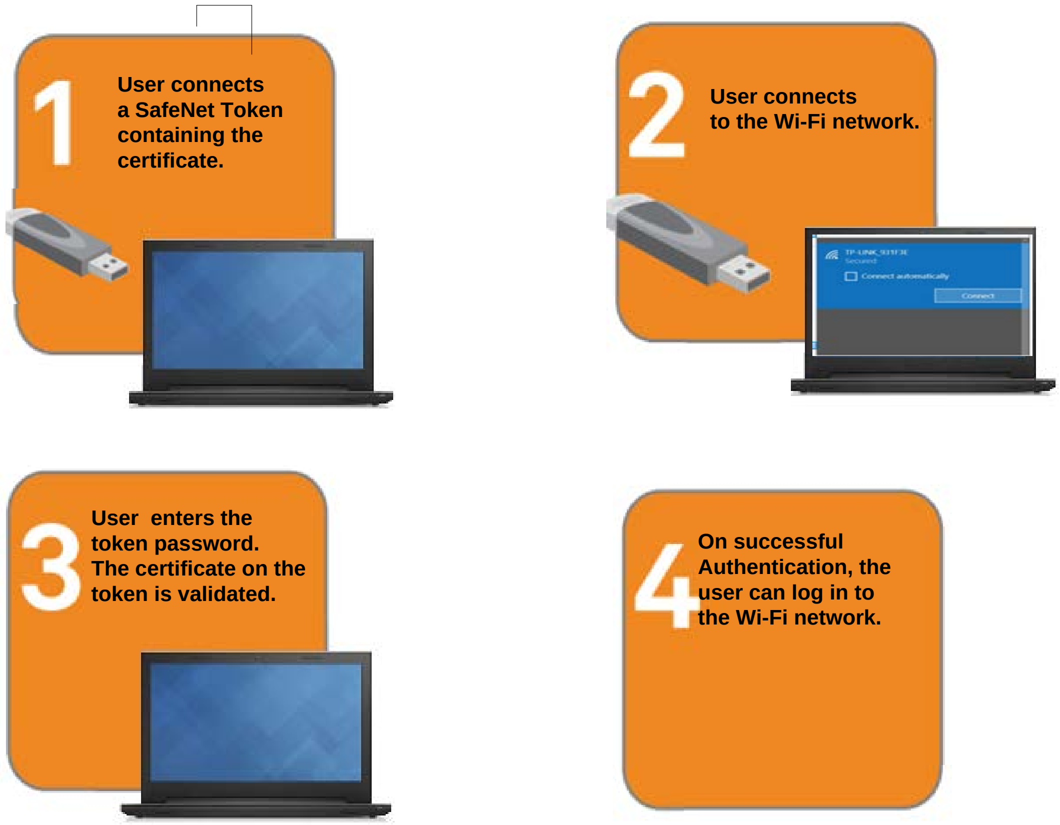
- **SafeNet Authentication Client (SAC)** - SAC 10.4 Post GA
- **TP-LINK 931F3E Wireless N router**
- **Windows Server 2008R2** installed with Active Directory, Certificate Authority, NPS Radius
- **Win 10 1703 -** Installed on Laptop PC Domain Joined.

Audience

This document is targeted at system administrators who are familiar with Wi-Fi Network, and are interested in adding multi-factor authentication capabilities during pre-boot using SafeNet tokens.

Authentication Flow

The diagram below illustrates the flow of certificate-based authentication To Wi-Fi Network:


1
User connects a SafeNet Token containing the certificate.
2
User connects to the Wi-Fi network.
Connect automatically
Connect
3
User enters the token password. The certificate on the token is validated.
4
On successful Authentication, the user can log in to the Wi-Fi network.

Prerequisites

To enable users to perform authentication to Wi-Fi Network using Gemalto tokens and smart cards, ensure the following:

- Users can authenticate to the Wi-Fi Network environment with a static password before configuring to use Gemalto tokens and smart cards.
- If SafeNet Authentication Manager (SAM) is used to manage the tokens, Token Policy Object (TPO) must be configured with MS CA connector. For further details, refer to the section “Connector for Microsoft CA” in the *SafeNet Authentication Manager Administrator’s Guide*.
- Users have a Gemalto token or smart card with a valid certificate enrolled.
- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. Any CA can be used. In this guide, integration is demonstrated using Microsoft CA.
- SafeNet Authentication Client (SAC 10.4 Post GA) must be installed on all client machines.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (SAC 10.4 Post GA) supports the following tokens and smart cards:

Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

Smart Cards

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

For all supported devices please refer to *SafeNet Authentication Client Customer Release Notes*.

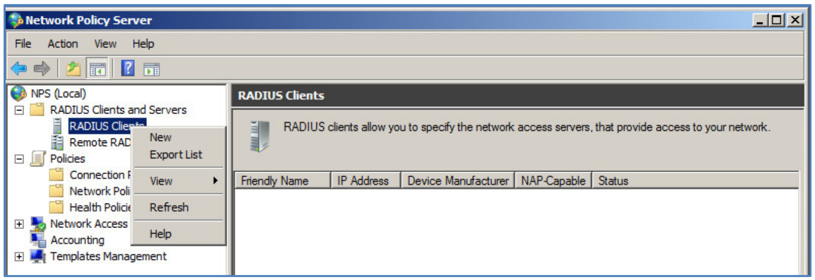
Configuring NPS RADIUS Server

Complete the procedures in this section to configure CBA Authentication for two-factor authentication. Following configuration, users will be able to authenticate using certificates on their smart cards or tokens.

In this example: Network Policy Server in Windows Server is demonstrated as a RADIUS server.

Configure the Wi-Fi Device as RADIUS Client

1. Open the Network Policy Server Console. Under **Policies > Expand RADIUS Clients and Servers**, right-click **RADIUS Clients**, and click **New**.

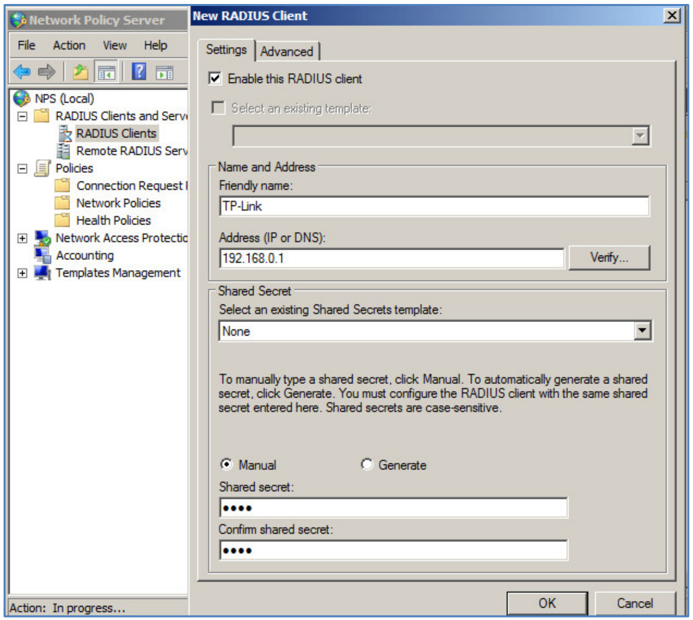


RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

2. Enter the details of the Wi-Fi Device (In This Example**: TP-LINK**) and enter the following under **Settings**:
    - Select **Enable Radius Client**
    - **Friendly Name:** enter device name
    - **Address:** enter device IP
    - **Shared secret:** Choose generation method (in this example, Manual)
    - **Under shared secret:** enter the shared secret that will be defined on Wi-Fi device.



☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: TP-Link

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

Shared Secret

Select an existing Shared Secrets template: None

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

● Manual ○ Generate

Shared secret: ••••

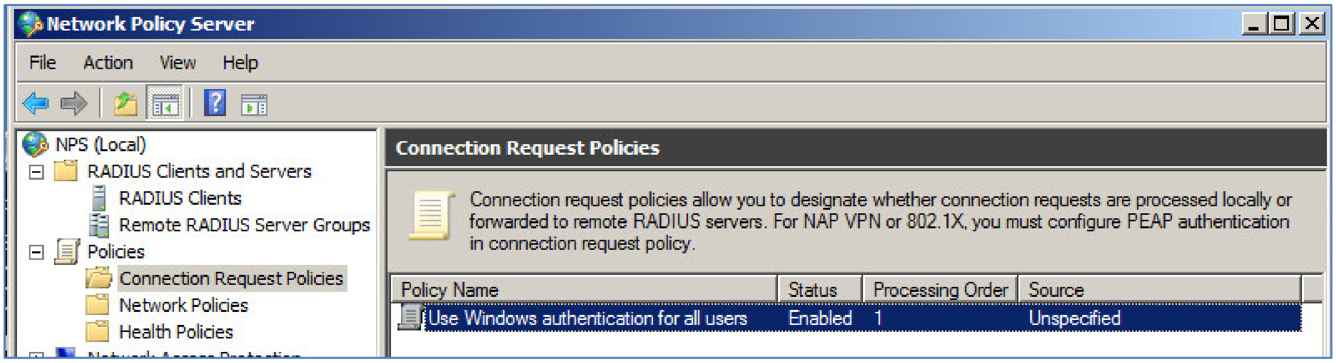
Confirm shared secret: ••••

OK Cancel

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

Configuring NPS Policies for Wireless - IEEE 802.11

1. Open the Network Policy Server console
2. Select **Policies > Connection Request Policies** and ensure that **Use Windows authentication for all users** is enabled.

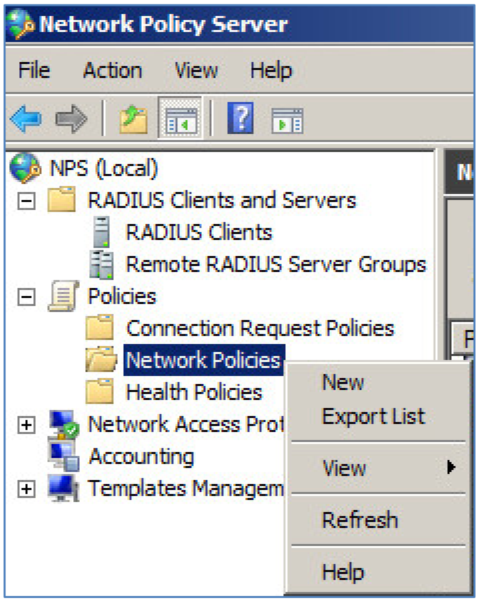

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Connection Request Policies
Network Policies
Health Policies
Connection Request Policies

Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers. For NAP VPN or 802.1X, you must configure PEAP authentication in connection request policy.

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

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

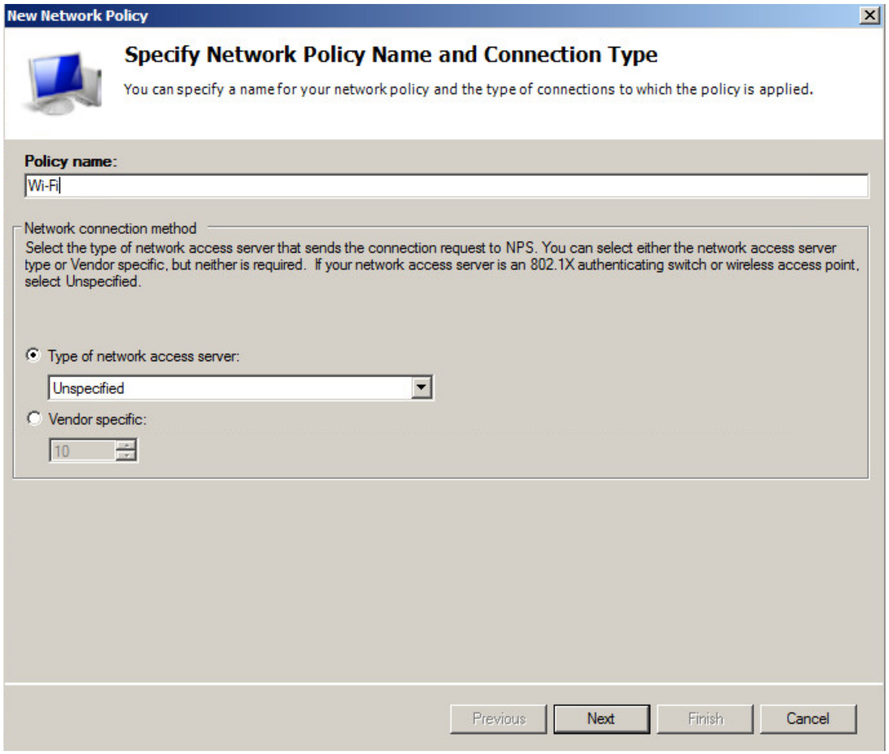
3. Under **Policies,** right-click **Network Policies** and select **New**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. Under **Policy Name,** enter the required name.

5. Under **Type of network access server**, select **Unspecified,** and click **Next**.



Specify Network Policy Name and Connection Type

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

Policy name: Wi-Fi

Network connection method

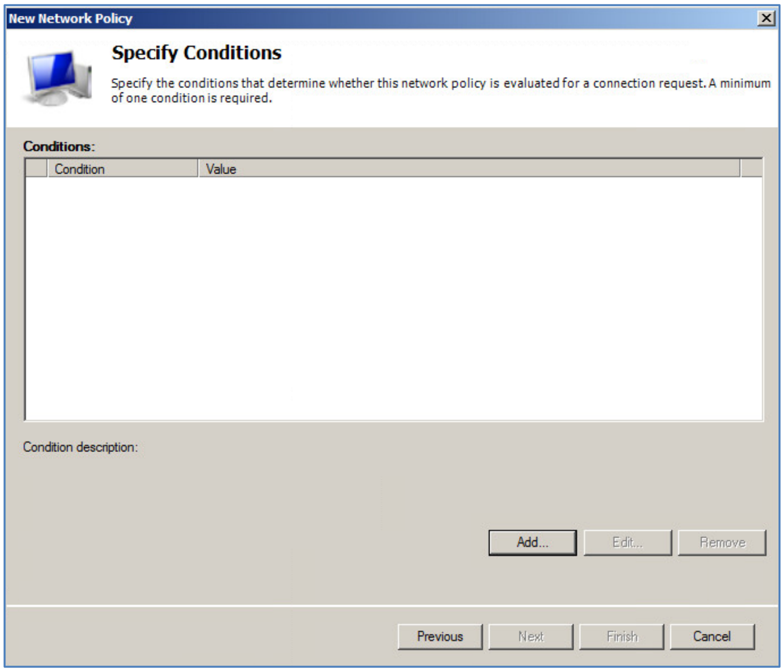
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

● Type of network access server: Unspecified

○ Vendor specific: 10

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

6. In the **Specify Conditions** window, click **Add**.



Specify Conditions

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

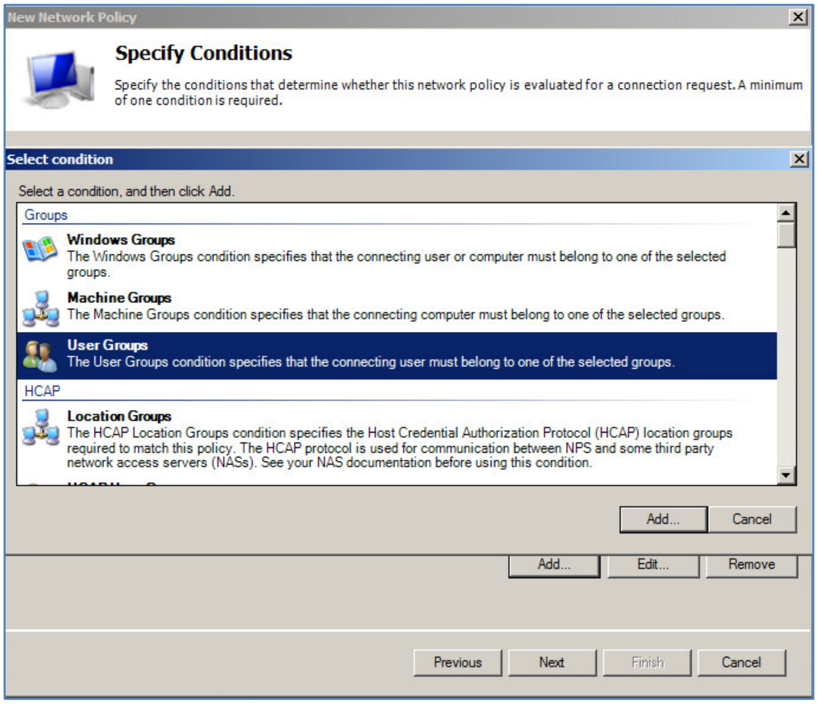
Conditions:

Condition	Value

Condition description:

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

7. Choose **User Groups** and click **Add**.



Specify Conditions

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

Select a condition, and then click Add.

Groups

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

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

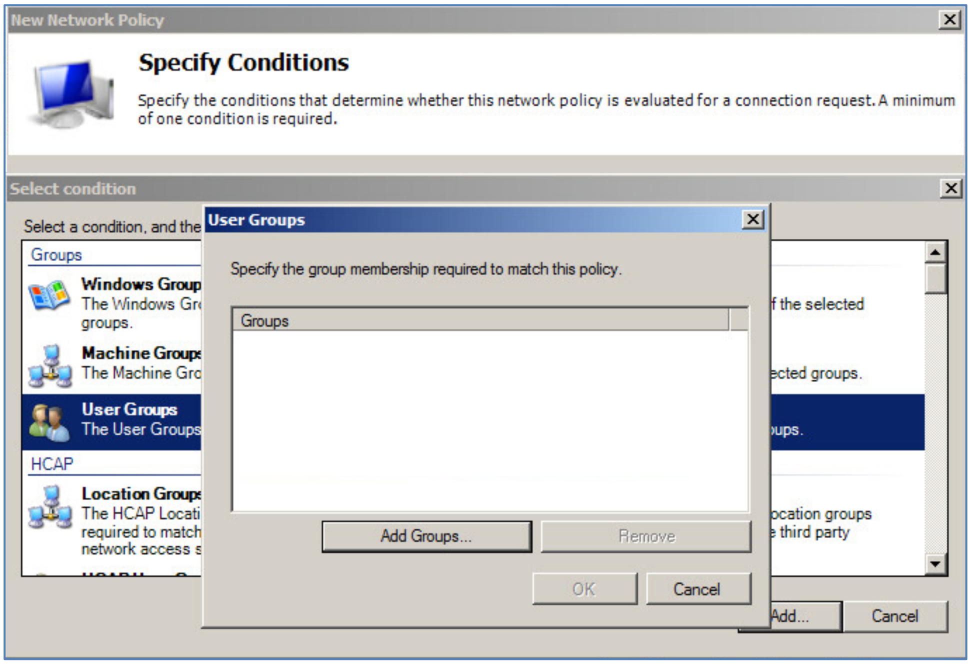
User Groups
The User Groups condition specifies that the connecting user must belong to one of the selected groups.

HCAP

Location Groups
The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

8. Click **Add Groups**


New Network Policy

Specify Conditions

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

Select condition

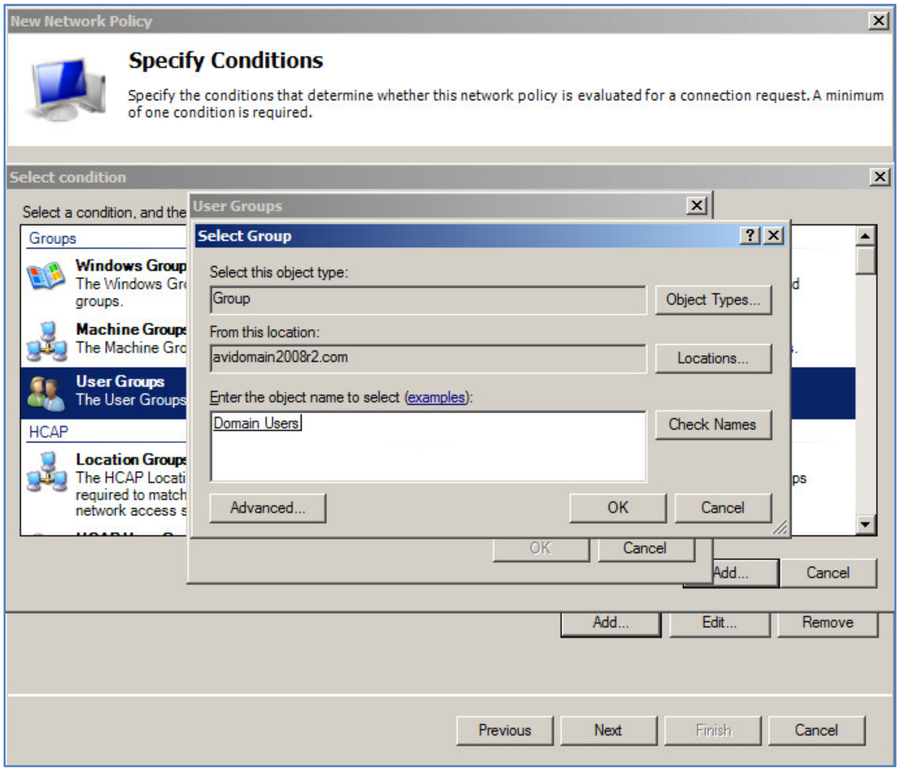
Select a condition, and the

User Groups

Specify the group membership required to match this policy.

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

9. Add **Domain Users,** and Click **OK Twice**


New Network Policy

Specify Conditions

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

Select condition

Select a condition, and the

User Groups

Select Group

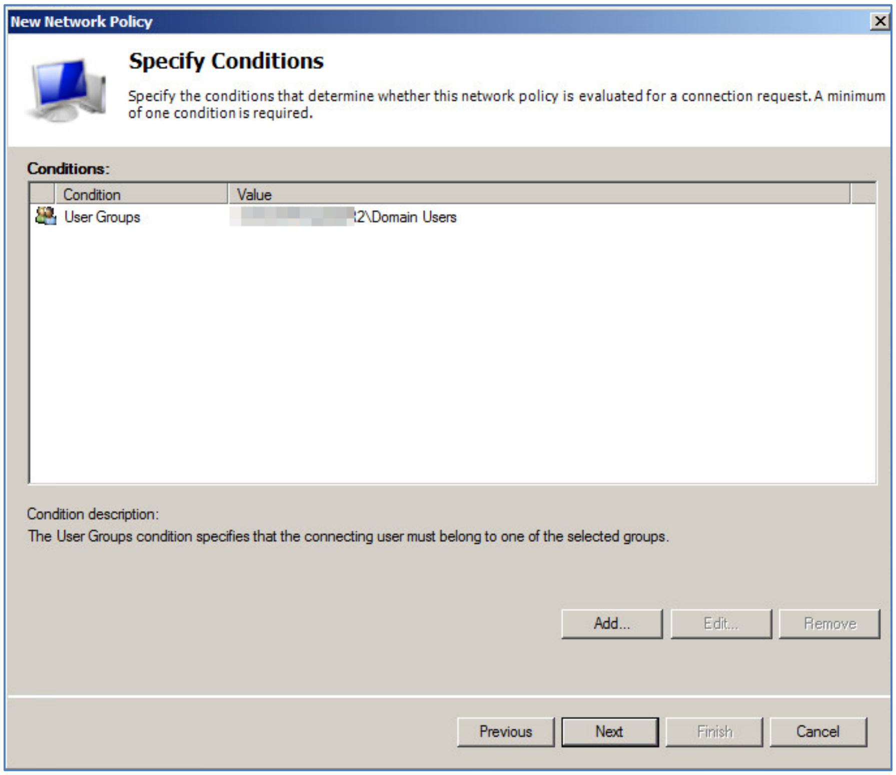
Select this object type: Group

From this location: avidomain2008r2.com

Enter the object name to select (examples): Domain Users

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

10. Click **Add** Again



Specify Conditions

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

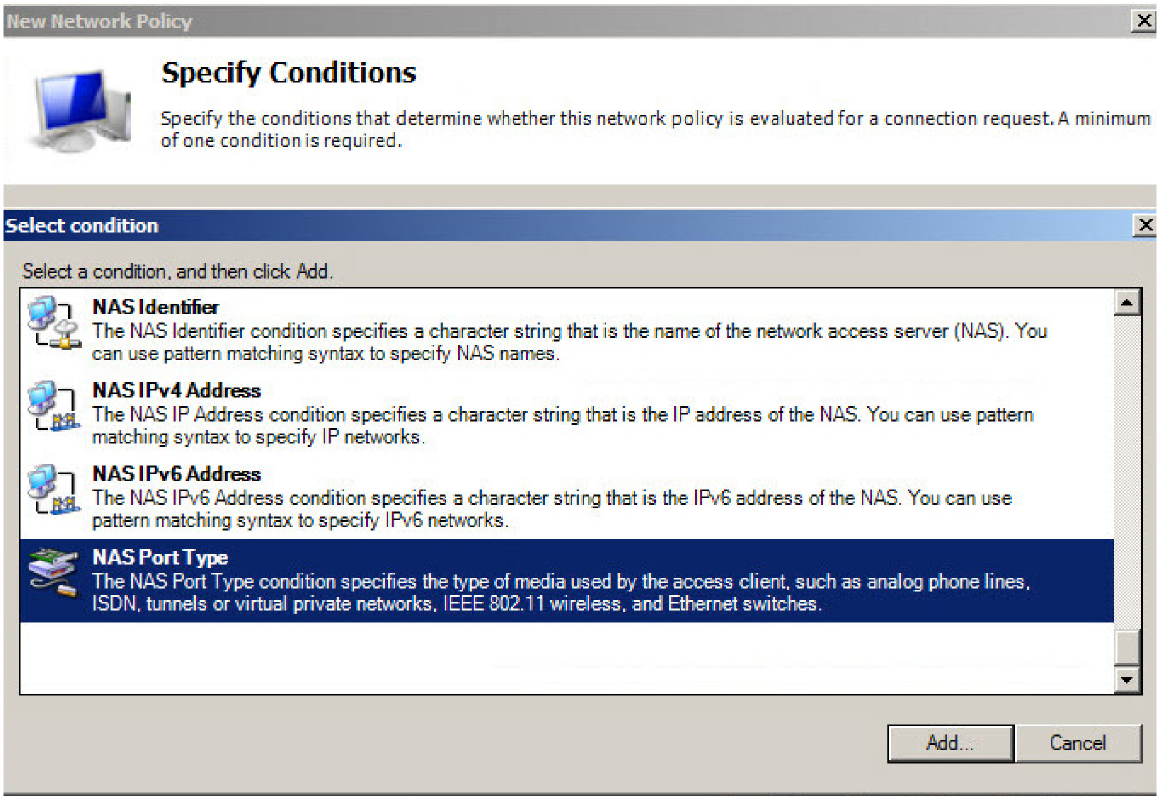
Conditions:

Condition	Value
User Groups	[redacted]2\Domain Users

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

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

11. Choose **NAS Port Type**, and click **Add**.



New Network Policy

Specify Conditions

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

Select condition

Select a condition, and then click Add.

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

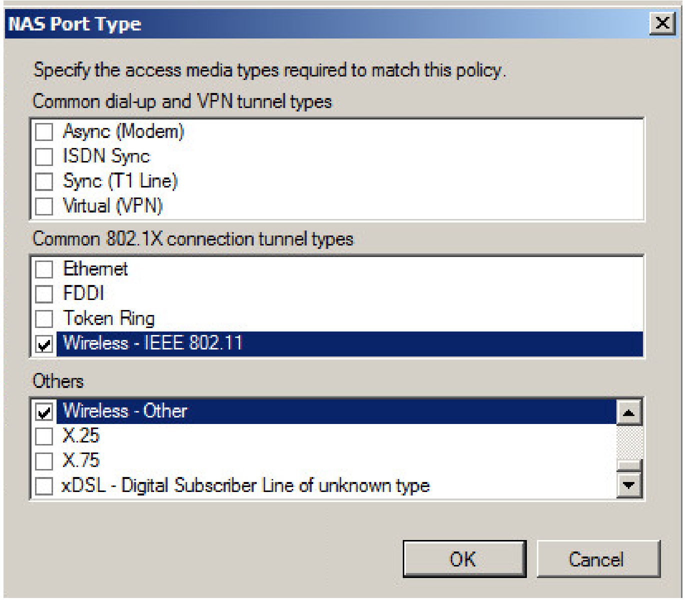
NAS IPv4 Address
The NAS IP Address condition specifies a character string that is the IP address of the NAS. You can use pattern matching syntax to specify IP networks.

NAS IPv6 Address
The NAS IPv6 Address condition specifies a character string that is the IPv6 address of the NAS. You can use pattern matching syntax to specify IPv6 networks.

NAS Port Type
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

12. Select **Wireless – IEEE 802.11** and **Wireless – Other** and click **OK**.



NAS Port Type

Specify the access media types required to match this policy.

Common dial-up and VPN tunnel types

☐ Async (Modem)
☐ ISDN Sync
☐ Sync (T1 Line)
☐ Virtual (VPN)

Common 802.1X connection tunnel types

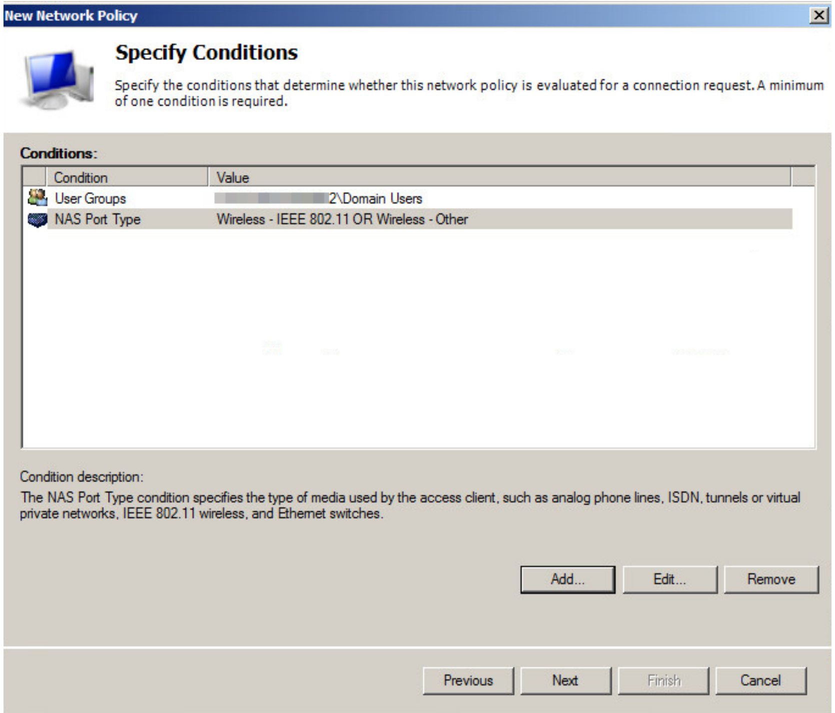
☐ Ethernet
☐ FDDI
☐ Token Ring
☑ Wireless - IEEE 802.11

Others

☑ Wireless - Other
☐ X.25
☐ X.75
☐ xDSL - Digital Subscriber Line of unknown type

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

3. Ensure that **NAS Port Type Condition** was added, and click **Next**.



Specify Conditions

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

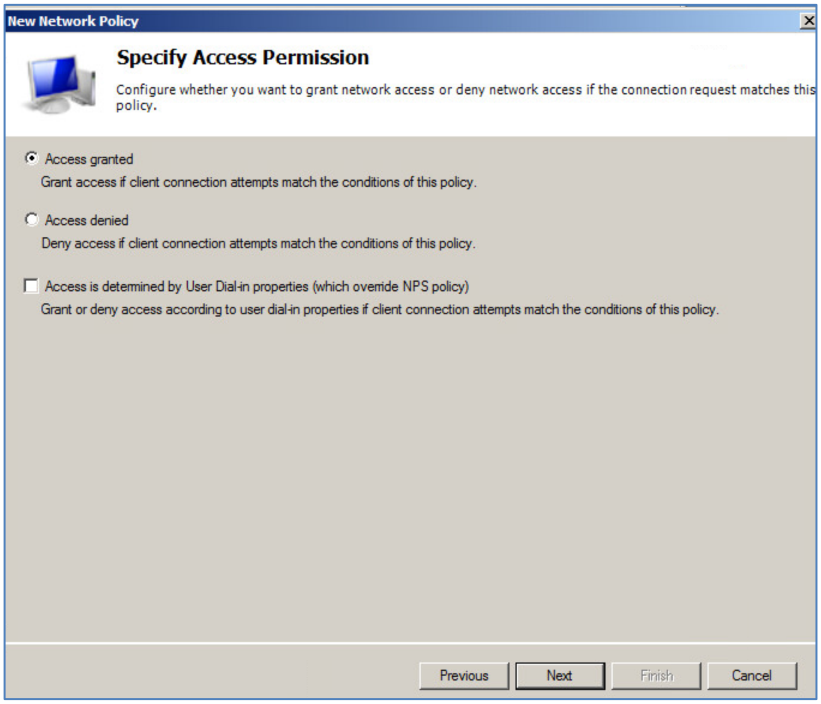
Conditions:

Condition	Value
User Groups	[redacted]2\Domain Users
NAS Port Type	Wireless - IEEE 802.11 OR Wireless - Other

Condition description:
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. Select **Access Granted,** and click **Next**



Specify Access Permission

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

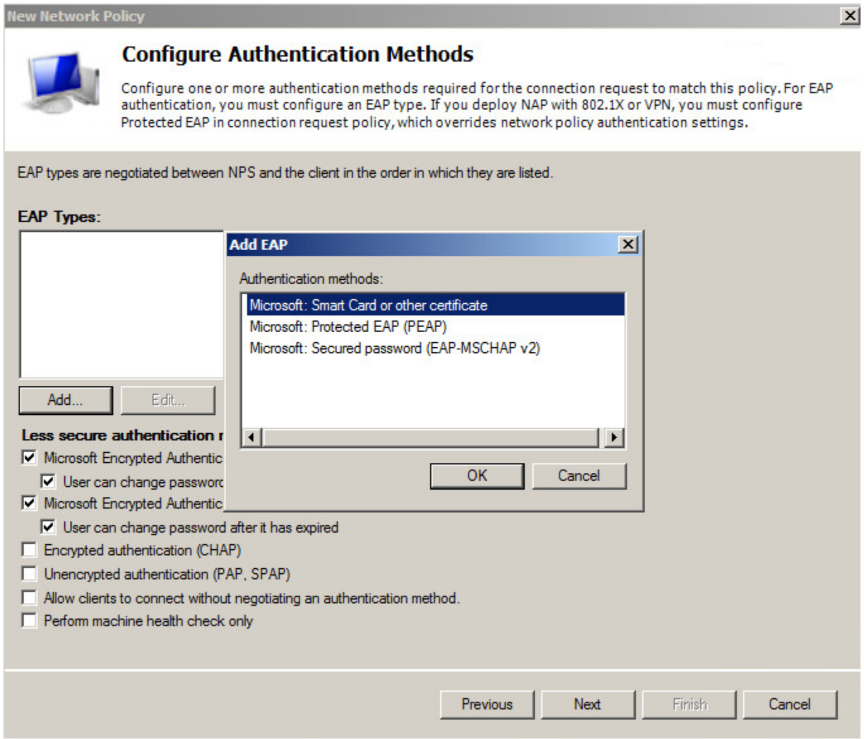
● Access granted
Grant access if client connection attempts match the conditions of this policy.

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

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

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

5. In the **Configure Authentication Methods** screen, click **Add.**
6. In the **Add EAP** window**,** choose **Microsoft: Smart Card or other certificate**, and click **OK**.



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

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

EAP Types:

Add EAP

Authentication methods:

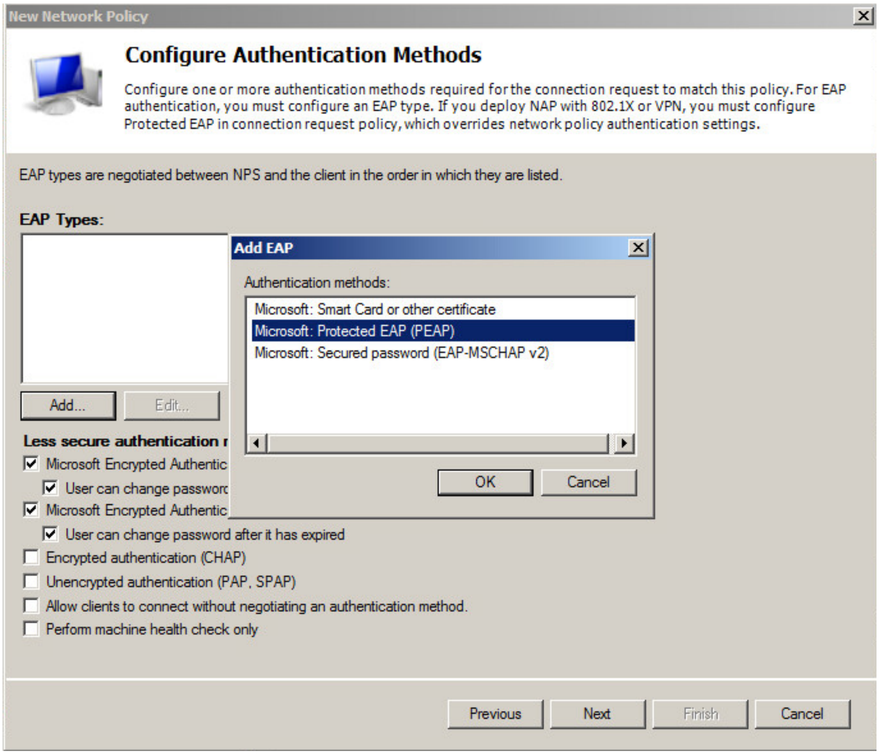
- Microsoft: Smart Card or other certificate
- Microsoft: Protected EAP (PEAP)
- Microsoft: Secured password (EAP-MSCHAP v2)

Less secure authentication r

☑ Microsoft Encrypted Authentic
  ☑ User can change passworc
☑ Microsoft Encrypted Authentic
  ☑ User can change password after it has expired
☐ Encrypted authentication (CHAP)
☐ Unencrypted authentication (PAP, SPAP)
☐ Allow clients to connect without negotiating an authentication method.
☐ Perform machine health check only

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

7. In the **Add EAP** window, choose **Microsoft Protected EAP (PEAP),** and click **OK.**



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

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

EAP Types:

Add EAP

Authentication methods:

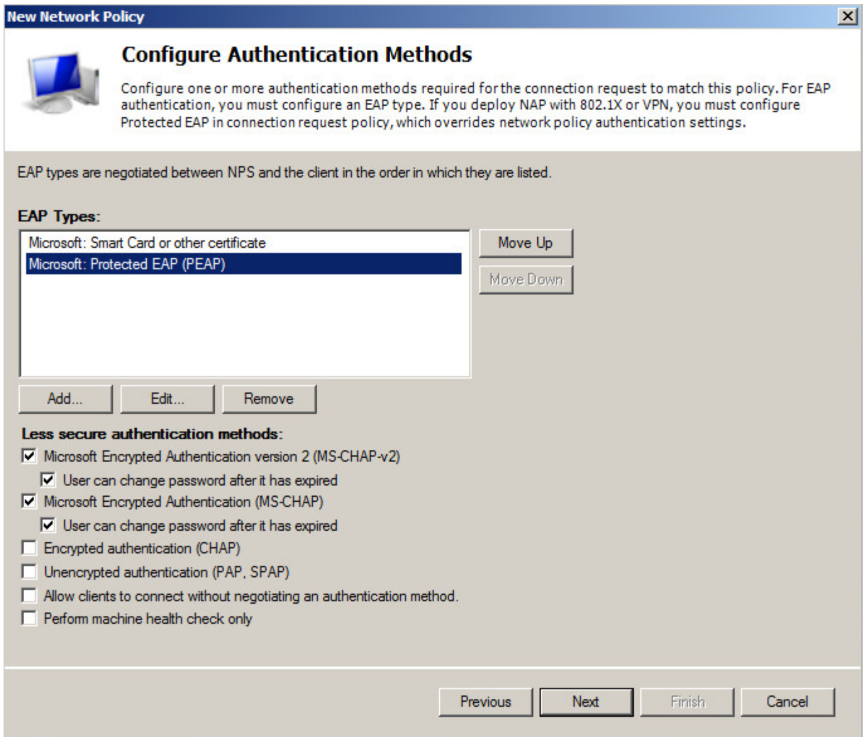
- Microsoft: Smart Card or other certificate
- Microsoft: Protected EAP (PEAP)
- Microsoft: Secured password (EAP-MSCHAP v2)

Less secure authentication r

☑ Microsoft Encrypted Authentic
  ☑ User can change passworc
☑ Microsoft Encrypted Authentic
  ☑ User can change password after it has expired
☐ Encrypted authentication (CHAP)
☐ Unencrypted authentication (PAP, SPAP)
☐ Allow clients to connect without negotiating an authentication method.
☐ Perform machine health check only

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

8. After Added Both, Select **Microsoft Protected EAP (PEAP)**, and click **Edit**.



New Network Policy

Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type. If you deploy NAP with 802.1X or VPN, you must configure Protected EAP in connection request policy, which overrides network policy authentication settings.

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

EAP Types:

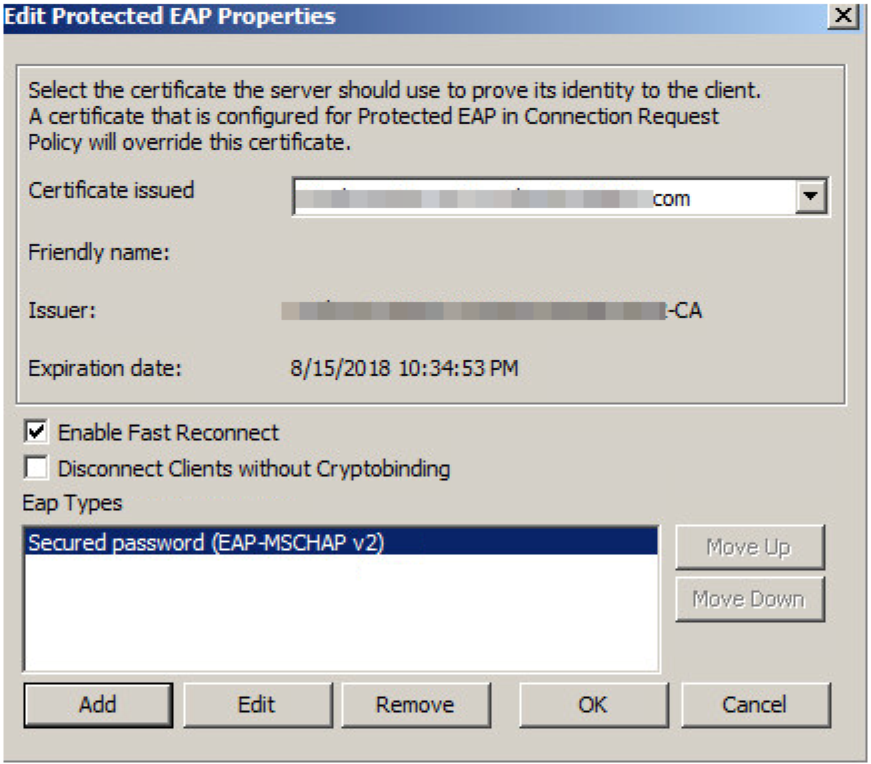
- Microsoft: Smart Card or other certificate
- Microsoft: Protected EAP (PEAP)

Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
☑ User can change password after it has expired
☑ Microsoft Encrypted Authentication (MS-CHAP)
☑ User can change password after it has expired
☐ Encrypted authentication (CHAP)
☐ Unencrypted authentication (PAP, SPAP)
☐ Allow clients to connect without negotiating an authentication method.
☐ Perform machine health check only

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

9. In the **Edit Protected EAP Properties** window, click **Add**



Edit Protected EAP Properties

Select the certificate the server should use to prove its identity to the client. A certificate that is configured for Protected EAP in Connection Request Policy will override this certificate.

Certificate issued [redacted]com

Friendly name:

Issuer: [redacted]-CA

Expiration date: 8/15/2018 10:34:53 PM

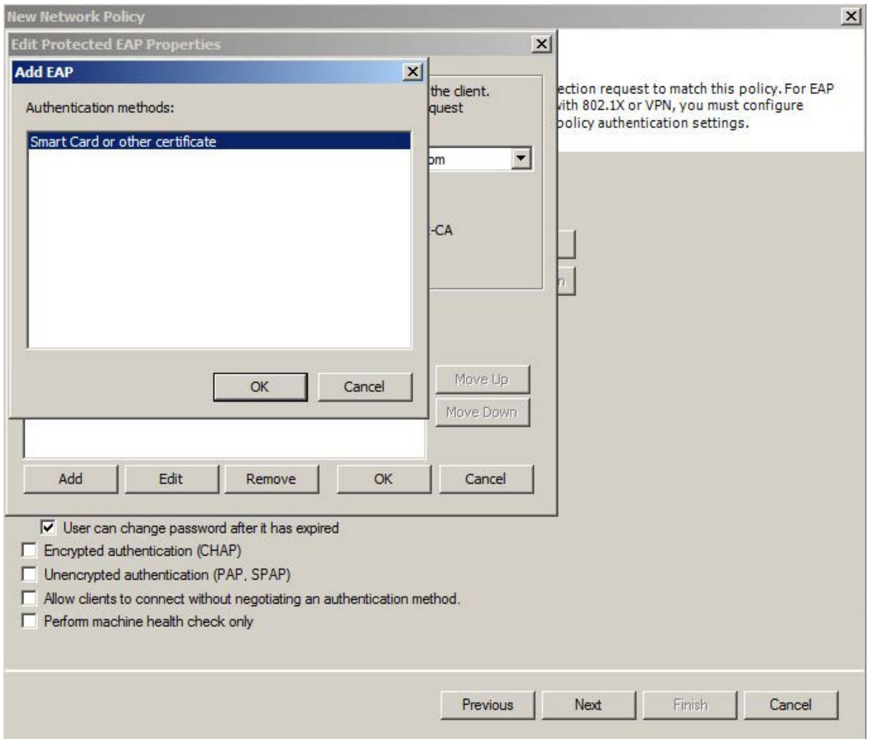
☑ Enable Fast Reconnect
☐ Disconnect Clients without Cryptobinding

Eap Types

- Secured password (EAP-MSCHAP v2)

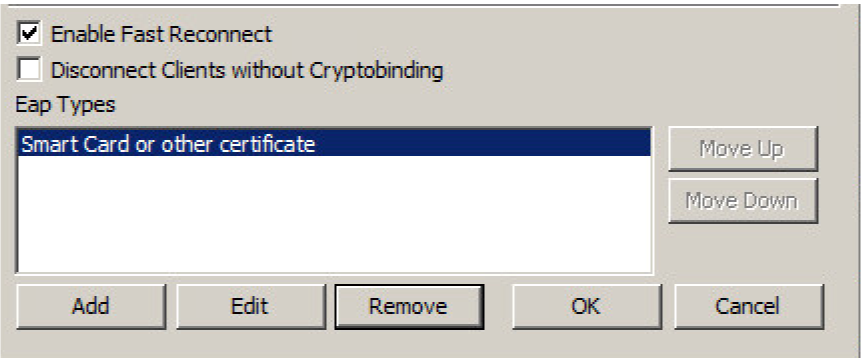
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

10. Select **Smart Card or other certificate** and click **OK.**


New Network Policy
Edit Protected EAP Properties
Add EAP
Authentication methods:
Smart Card or other certificate
OK
Cancel
the client.
quest
ection request to match this policy. For EAP
ith 802.1X or VPN, you must configure
policy authentication settings.
om
-CA
Move Up
Move Down
Add
Edit
Remove
OK
Cancel
☑ User can change password after it has expired
☐ Encrypted authentication (CHAP)
☐ Unencrypted authentication (PAP, SPAP)
☐ Allow clients to connect without negotiating an authentication method.
☐ Perform machine health check only
Previous
Next
Finish
Cancel

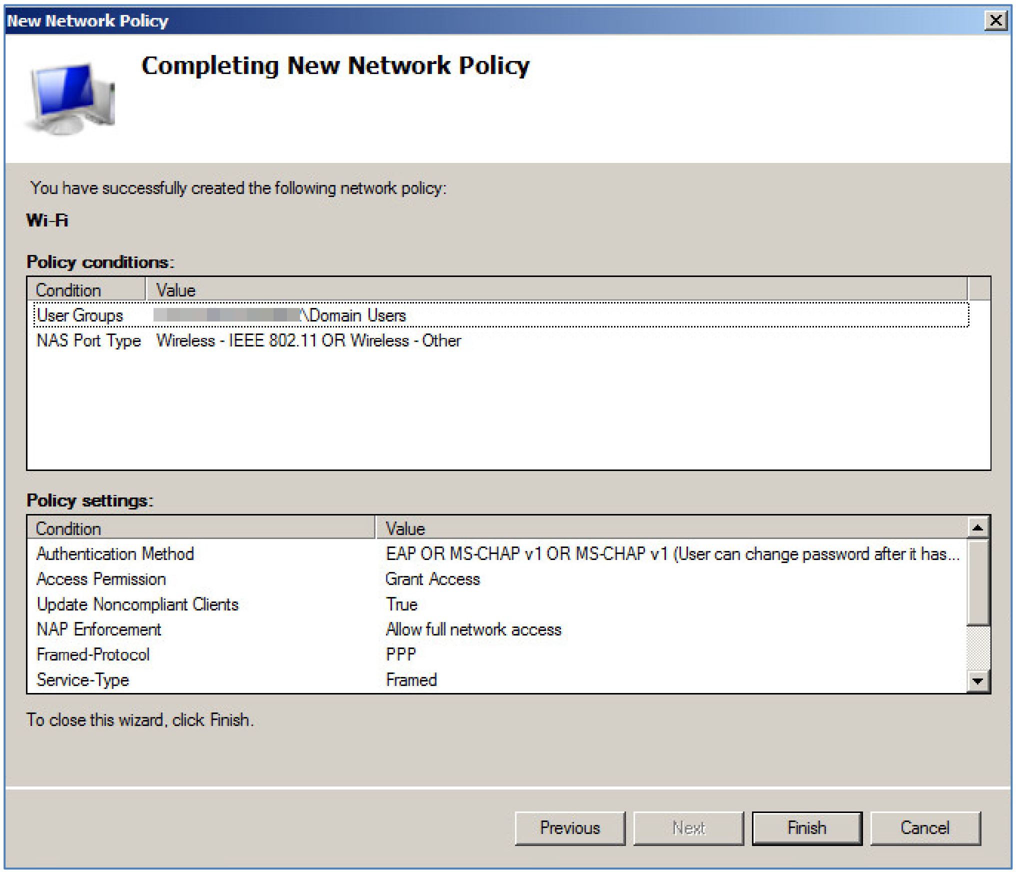
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

11. Move up or remove the unwanted methods (in this example only **Smart Card or other certificate** was configured) and click **OK.**


☑ Enable Fast Reconnect
☐ Disconnect Clients without Cryptobinding
Eap Types
Smart Card or other certificate
Move Up
Move Down
Add
Edit
Remove
OK
Cancel

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

12. Click **Next (**without changing the default values), and then click **Finish.**



New Network Policy

Completing New Network Policy

You have successfully created the following network policy:

Wi-Fi

Policy conditions:

Condition	Value
User Groups	[redacted]\Domain Users
NAS Port Type	Wireless - IEEE 802.11 OR Wireless - Other

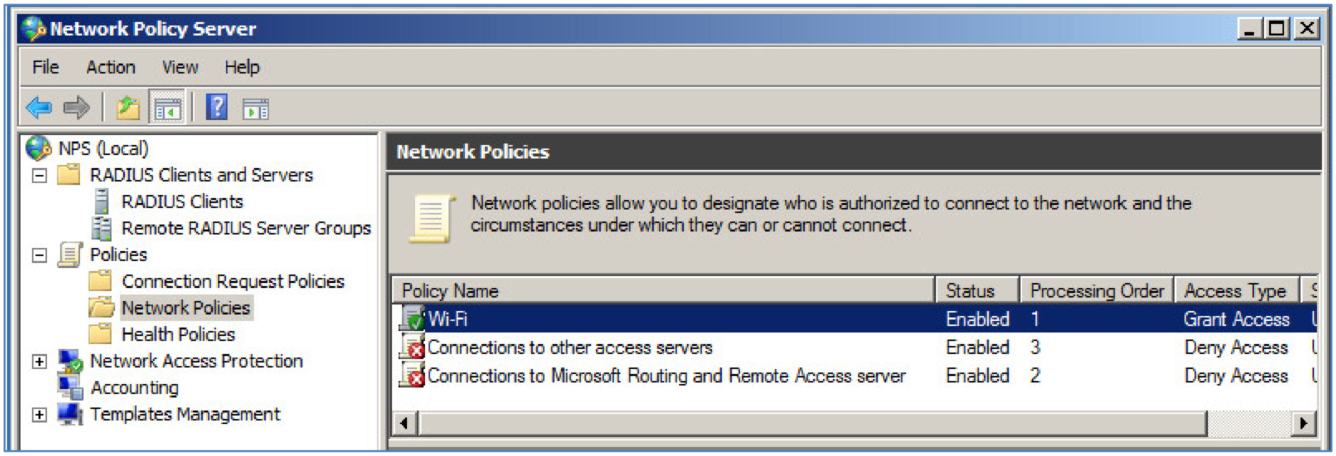
Policy settings:

Condition	Value
Authentication Method	EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has...
Access Permission	Grant Access
Update Noncompliant Clients	True
NAP Enforcement	Allow full network access
Framed-Protocol	PPP
Service-Type	Framed

To close this wizard, click Finish.

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

13. Move the new policy to the top of the **Network Policies** list**.**



Network Policies

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

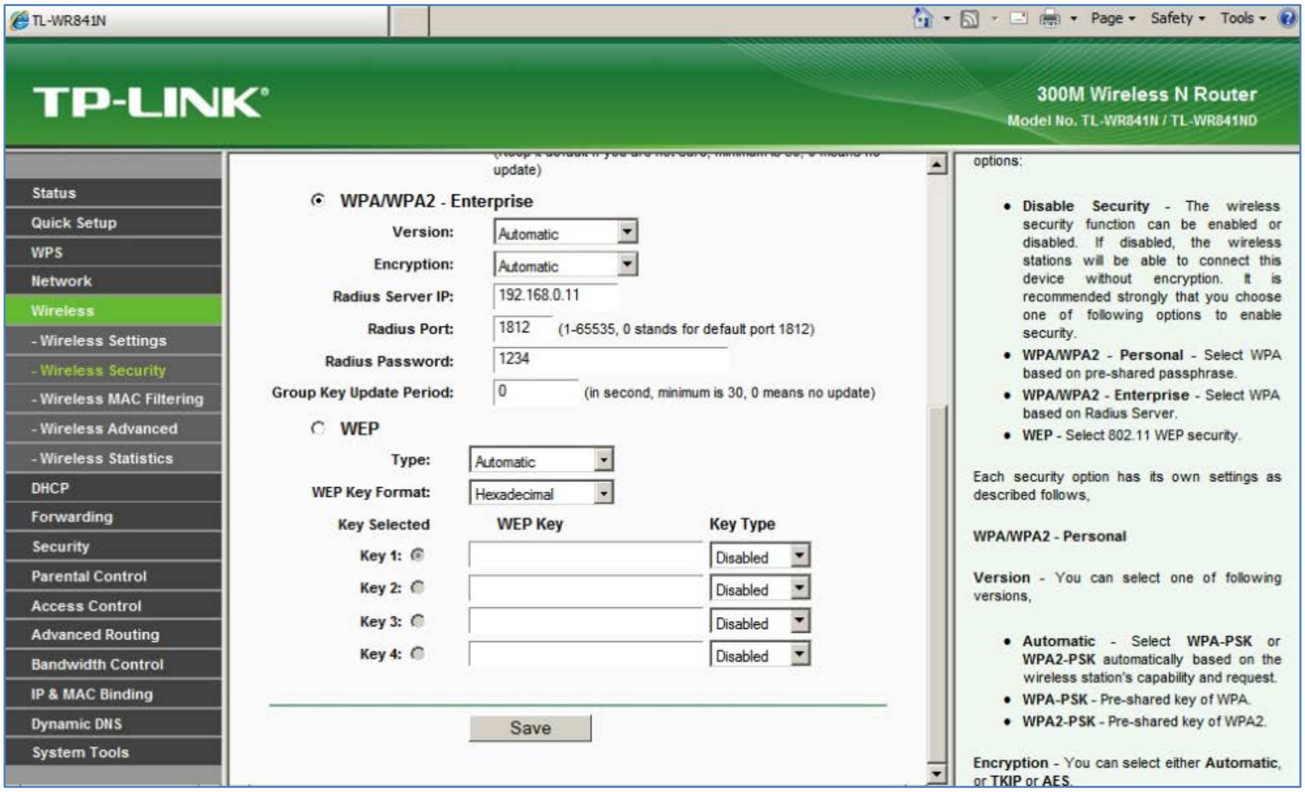
Policy Name	Status	Processing Order	Access Type	S
Wi-Fi	Enabled	1	Grant Access	U
Connections to other access servers	Enabled	3	Deny Access	U
Connections to Microsoft Routing and Remote Access server	Enabled	2	Deny Access	U

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

Configuring Wi-Fi Device

The steps demonstrated below are for a **TP-LINK 931F3E** device.

1. Connect and login to **TP-LINK Device > Under Wireless > Wireless Security,** and fill in the fields as follows:
    - Select **WPA/WPA2-Enterprise**
    - In **Version**, choose **Automatic**.
    - In **Encryption,** choose **Automatic**
    - In **Radius Server IP**, enter the Radius IP
    - In **Radius Password**, enter the shared secret as configured previously



update)

● WPA/WPA2 - Enterprise

Version: Automatic

Encryption: Automatic

Radius Server IP: 192.168.0.11

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password: 1234

Group Key Update Period: 0 (in second, minimum is 30, 0 means no update)

○ WEP

Type: Automatic

WEP Key Format: Hexadecimal

Key Selected	WEP Key	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

options:

- **Disable Security** - The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect this device without encryption. It is recommended strongly that you choose one of following options to enable security.
- **WPA/WPA2 - Personal** - Select WPA based on pre-shared passphrase.
- **WPA/WPA2 - Enterprise** - Select WPA based on Radius Server.
- **WEP** - Select 802.11 WEP security.

Each security option has its own settings as described follows,

WPA/WPA2 - Personal

Version - You can select one of following versions,

- **Automatic** - Select **WPA-PSK** or **WPA2-PSK** automatically based on the wireless station's capability and request.
- **WPA-PSK** - Pre-shared key of WPA.
- **WPA2-PSK** - Pre-shared key of WPA2.

Encryption - You can select either **Automatic**, or TKIP or **AES**.

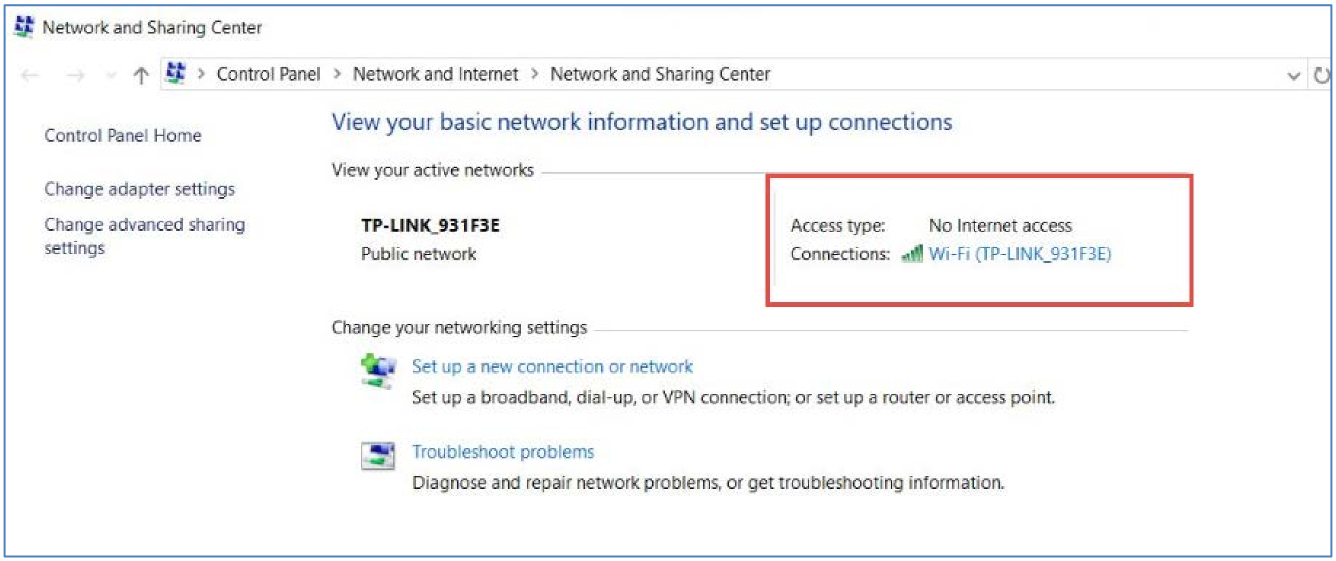
(The screen image above is from tp-linkt© software. Trademarks are the property of their respective owners.)

2. Click **Save**.

Configuring Wi-Fi Connection Client Side

Prerequisites: The steps Demonstrated below are for a Wi-Fi Connection that is already successfully connected to the Wi-Fi Device, and where the authentication method has been changed to Certificate Based Authentication.

1. Open **Network and Sharing Center** and click on the Wi-Fi Connection.


Network and Sharing Center
Control Panel > Network and Internet > Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings

View your basic network information and set up connections

View your active networks

TP-LINK_931F3E
Public network

Access type: No Internet access
Connections: Wi-Fi (TP-LINK_931F3E)

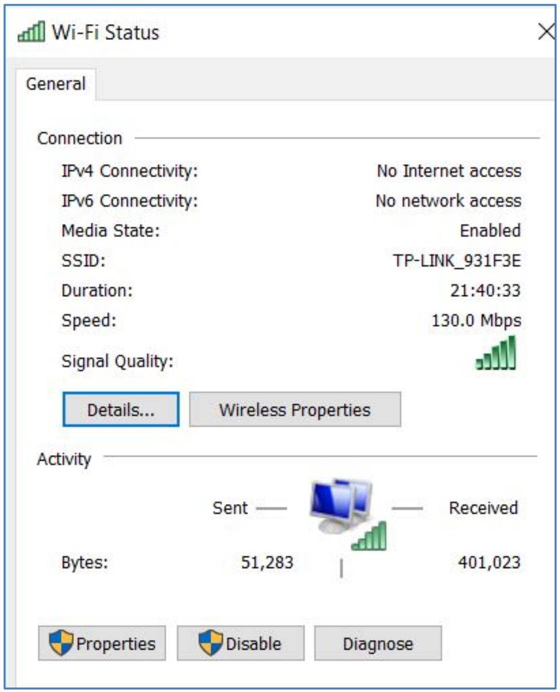
Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

2. Click **Wireless Properties**.



Connection

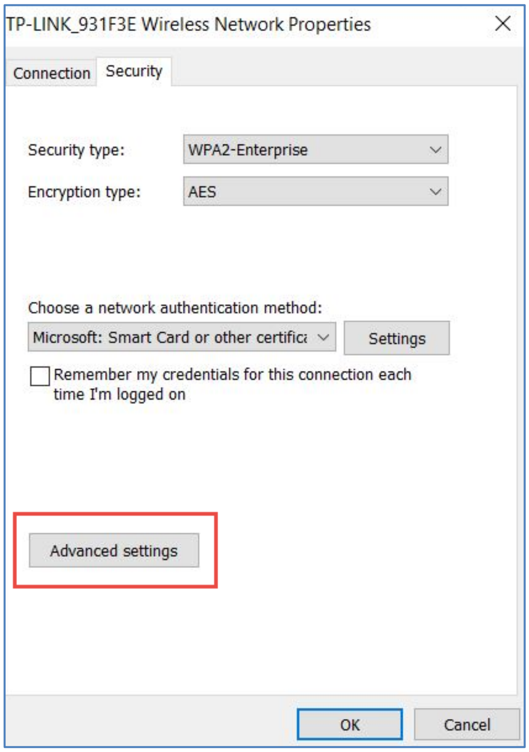
IPv4 Connectivity: No Internet access
IPv6 Connectivity: No network access
Media State: Enabled
SSID: TP-LINK_931F3E
Duration: 21:40:33
Speed: 130.0 Mbps
Signal Quality:

Activity

Sent — Received
Bytes: 51,283 | 401,023

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

3. In the **Wireless Network Properties** window, click the **Security** tab, then click **Advanced Settings.**



TP-LINK_931F3E Wireless Network Properties

Connection | Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Smart Card or other certific; Settings

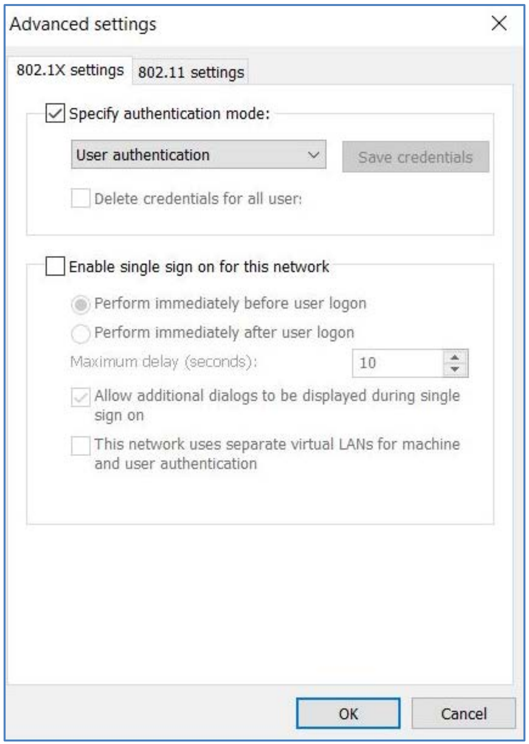
□ Remember my credentials for this connection each time I'm logged on

Advanced settings

OK Cancel

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. In the **Advanced Settings** window, select the **Specify authentication mode,** then select **User Authentication**



Advanced settings

802.1X settings | 802.11 settings

☑ Specify authentication mode:

User authentication | Save credentials

□ Delete credentials for all user:

□ 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

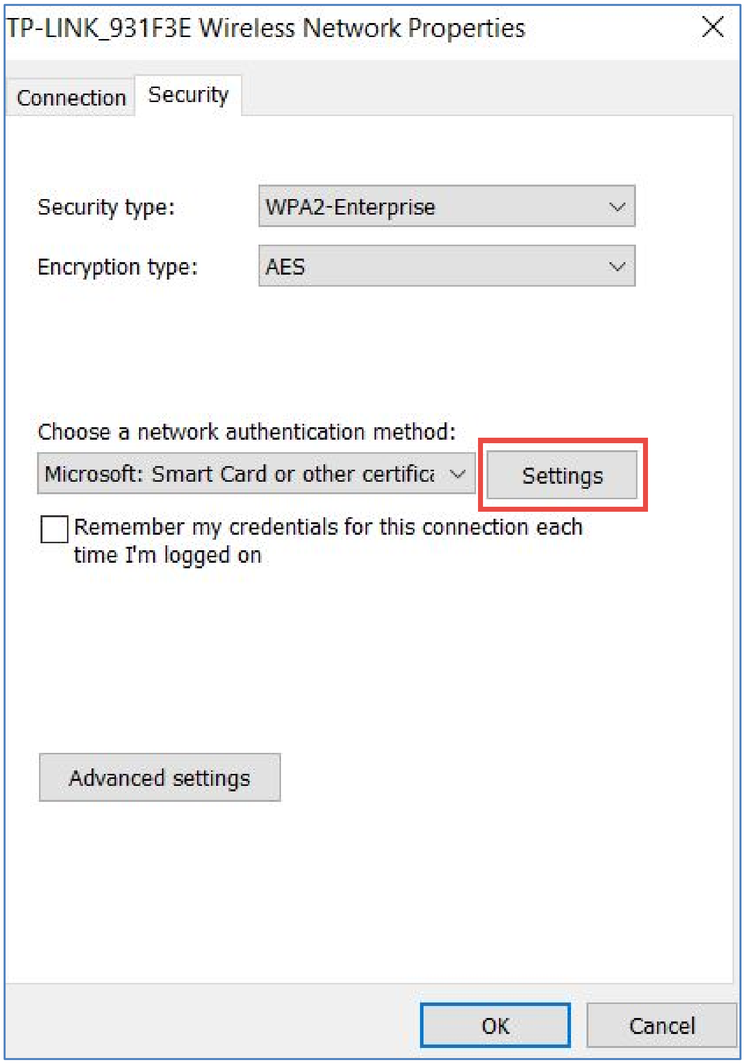
□ This network uses separate virtual LANs for machine and user authentication

OK Cancel

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

5. Click **OK** to return to **Wireless Network Properties**, **Security** tab.

6. In the **Wireless Network Properties** window, click the **Security** tab, then configure as follows:
   - **Security Type**: select **WPA2-Enterprise**.
   - **Encryption Type**: select **AES**.
   - **Choose a network authentication method:** select **Microsoft: Smart Card or other certificate**
7. Click **Settings** (placed to the right of the Microsoft: Smart Card or other certificate).



TP-LINK_931F3E Wireless Network Properties

Connection | Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

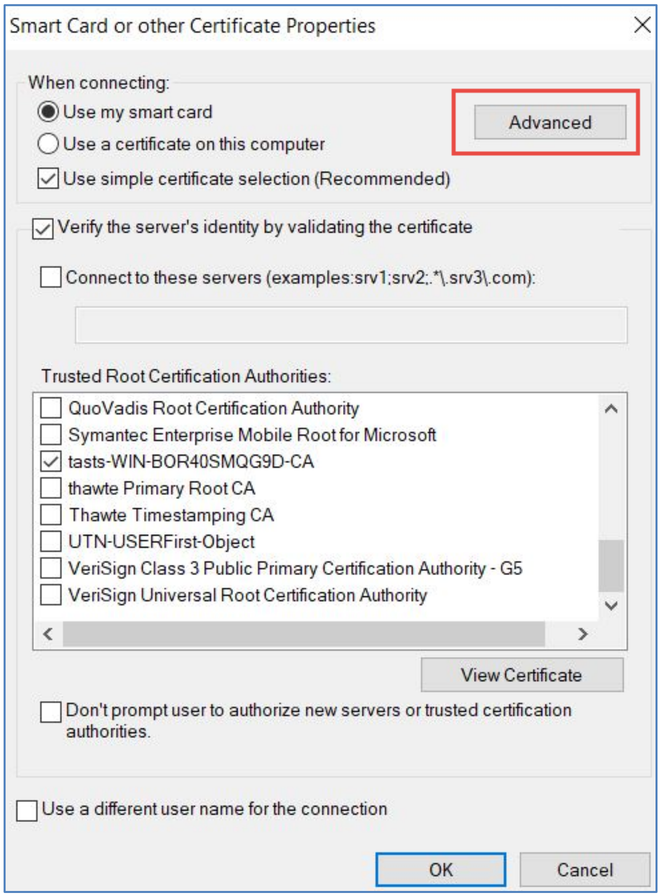
Microsoft: Smart Card or other certific

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

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

8. In the **Smart Card or other Certificate Properties** window, under **When Connecting**, do the following:
   - Select **Use My Smart Card**
   - Select **Use Simple certificate selection**
   - Select **Verify the server's identity by validating the certificate**
   - Under **Trusted Root Certification Authorities**, select the trusted domain root CA

9. Click **Advanced**.



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):

Trusted Root Certification Authorities:

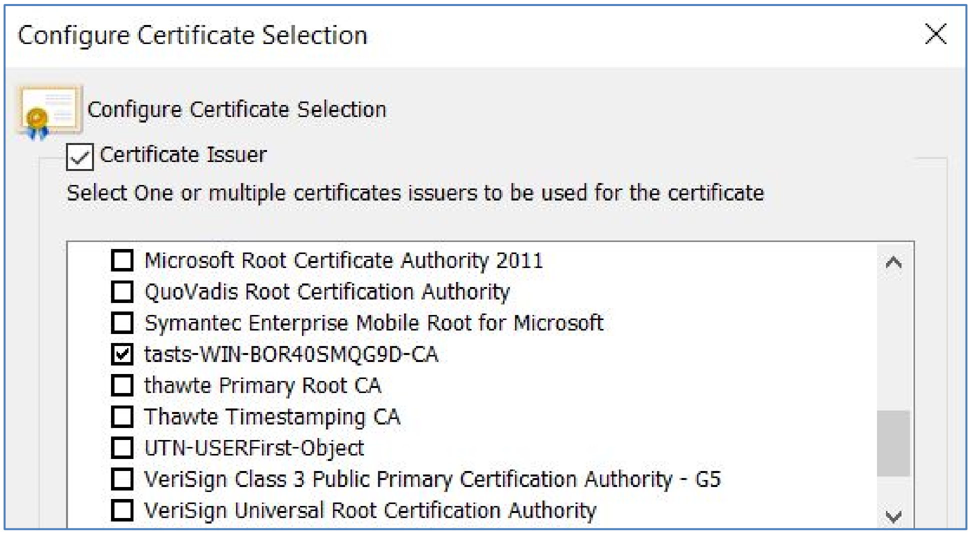
□ QuoVadis Root Certification Authority
□ Symantec Enterprise Mobile Root for Microsoft
☑ tasts-WIN-BOR40SMQG9D-CA
□ thawte Primary Root CA
□ Thawte Timestamping CA
□ UTN-USERFirst-Object
□ VeriSign Class 3 Public Primary Certification Authority - G5
□ VeriSign Universal Root Certification Authority

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

□ Use a different user name for the connection

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

10. In the **Configure Certificate Selection** window, select **Certificate Issuer** and select the trusted domain root CA.



Configure Certificate Selection

Configure Certificate Selection

☑ Certificate Issuer

Select One or multiple certificates issuers to be used for the certificate

□ Microsoft Root Certificate Authority 2011
□ QuoVadis Root Certification Authority
□ Symantec Enterprise Mobile Root for Microsoft
☑ tasts-WIN-BOR40SMQG9D-CA
□ thawte Primary Root CA
□ Thawte Timestamping CA
□ UTN-USERFirst-Object
□ VeriSign Class 3 Public Primary Certification Authority - G5
□ VeriSign Universal Root Certification Authority

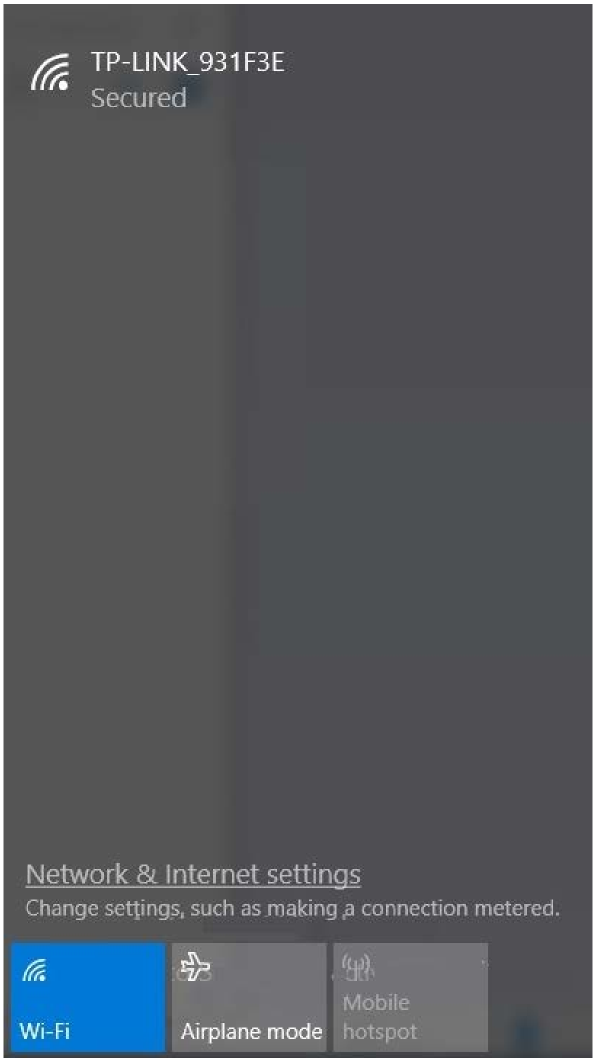
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

11. Click **OK** repeatedly until all the screens are closed.

Running the Solution

Enroll a Smartcard User certificate on the smart card/token.

1. Connect token.
2. From the Windows **Taskbar** menu, select **Network > Wi-Fi.**

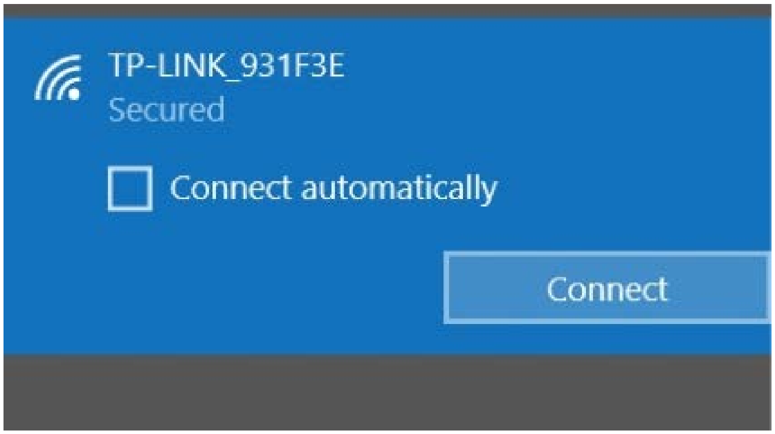


TP-LINK_931F3E
Secured

Network & Internet settings
Change settings, such as making a connection metered.

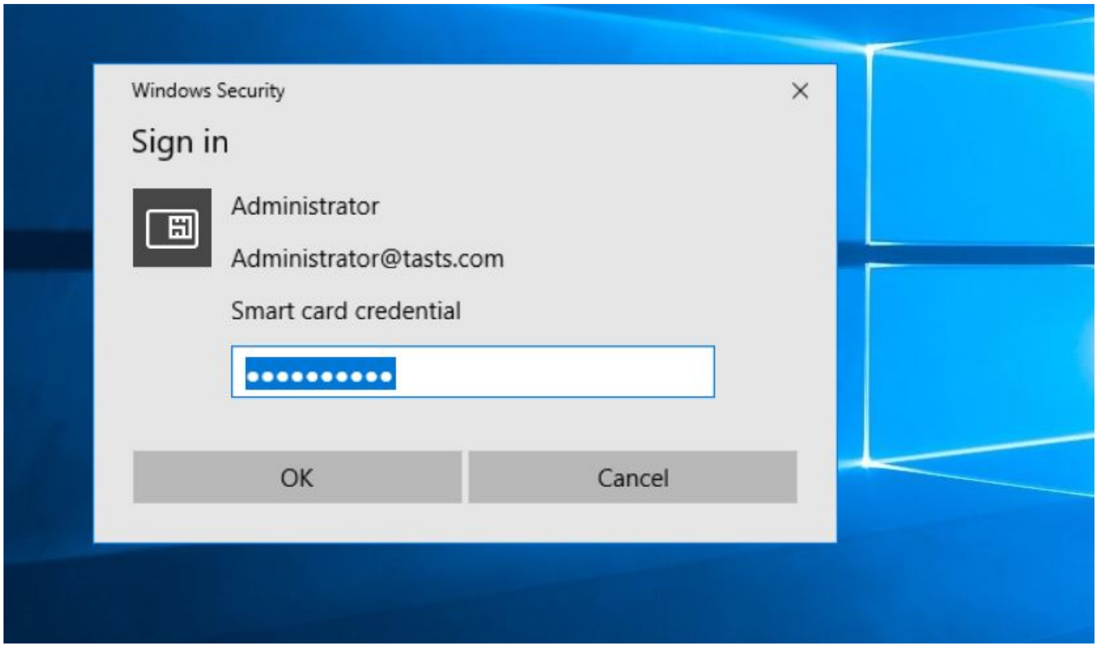
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

3. Select the Wi-Fi network and click **Connect.**



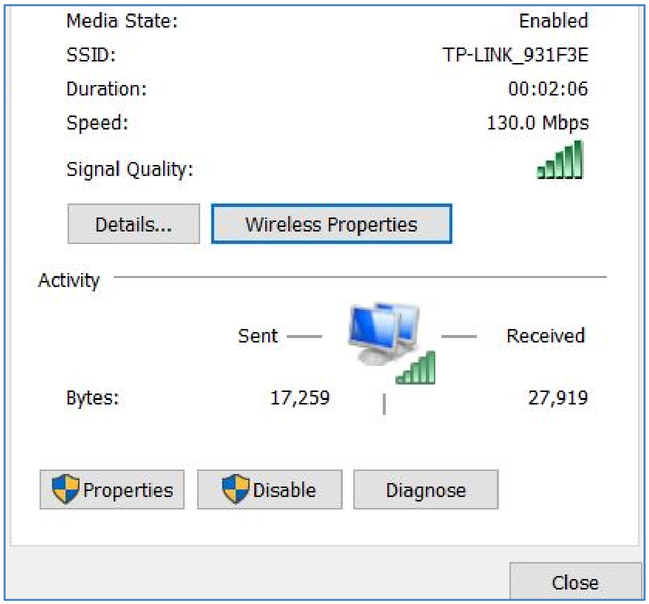
(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

4. In the **Windows Security Sign in** window, enter the credentials in the **Smart card credential** field, and click **OK**.



(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)

The Wi-Fi is now connected.



Media State: Enabled

SSID: TP-LINK_931F3E

Duration: 00:02:06

Speed: 130.0 Mbps

Signal Quality:

Bytes: Sent 17,259 Received 27,919

(The screen image above is from Microsoft$^{©}$ *software. Trademarks are the property of their respective owners*.)

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

Region	**Telephone number** (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Global	+1-410-931-7520
Australia	1800.020.183
China	North: 10800-713-1971 South: 10800-1301-932
France	0800-912-857
Germany	0800-181-6374
India	000.800.100.4290
Israel	180-931-5798
Italy	800-786-421
Japan	0066 3382 1699

Region	**Telephone number** (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Korea	+82 2 3429 1055
Netherlands	0800.022.2996
New Zealand	0800.440.359
Portugal	800.863.499
Singapore	800.1302.029
Spain	900.938.717
Sweden	020.791.028
Switzerland	0800.564.849
United Kingdom	0800.056.3158
United States	(800) 545-6608