

# Configurazione VPN INRiM

A partire dal 5 dicembre 2019, è attiva presso l'Istituto la nuova VPN, basata sulla tecnologia **Cisco FlexVPN** (IKEv2).

L'autenticazione sulla VPN avviene con la stessa coppia di **username/password** che vengono usate per l'accesso sulla rete Wi-Fi *eduroam*, o il portale del cartellino elettronico GRUM con l'aggiunta del dominio **@inrim.it**. Si ricorda inoltre che, con la stessa coppia username/password, è consentito un solo accesso contemporaneo.

Nel caso vi siano problemi di autenticazione, contattare lo staff dei Sistemi Informatici.

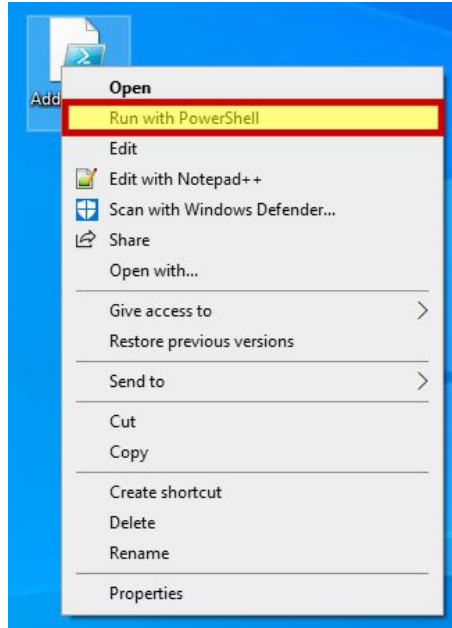
## Indice

<b>Indice</b>	<b>1</b>
<b>Windows 10</b>	<b>1</b>
Installazione automatica (consigliata)	1
Installazione manuale	2
<b>Windows 7 SP1</b>	<b>11</b>
EAP-TTLS	14
<b>Linux</b>	<b>15</b>
<b>Android</b>	<b>19</b>
<b>macOS</b>	<b>21</b>
<b>iOS e iPadOS</b>	<b>25</b>
<b>Lista delle modifiche</b>	<b>25</b>

## Windows 10

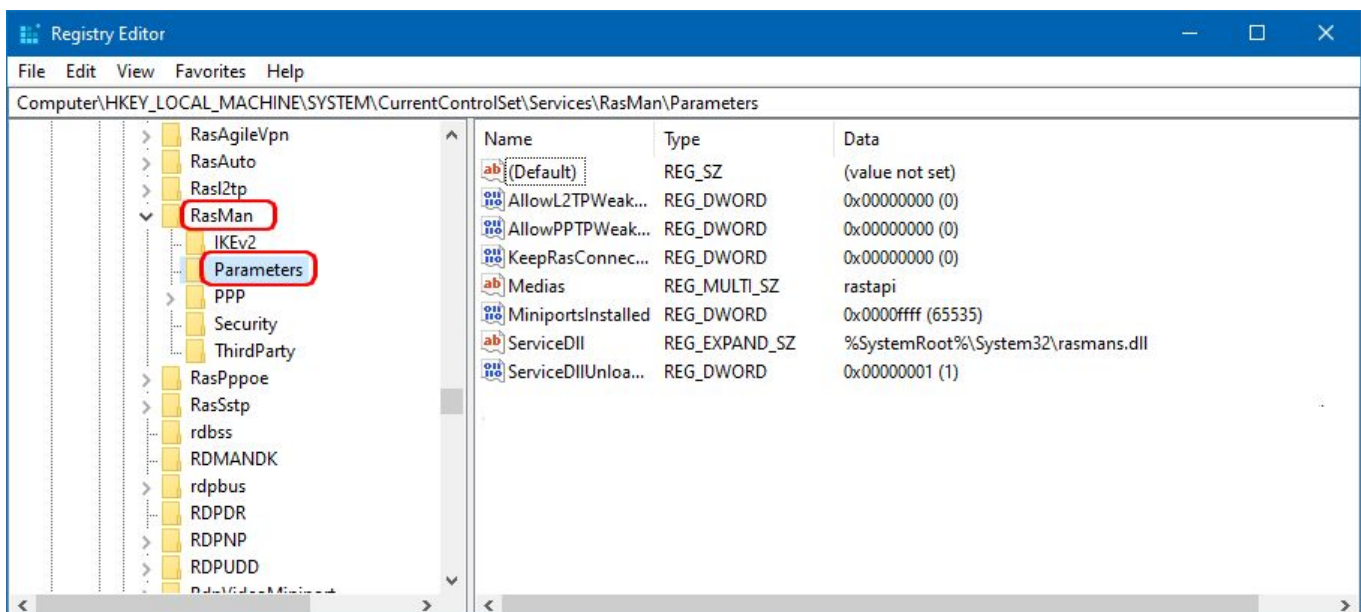
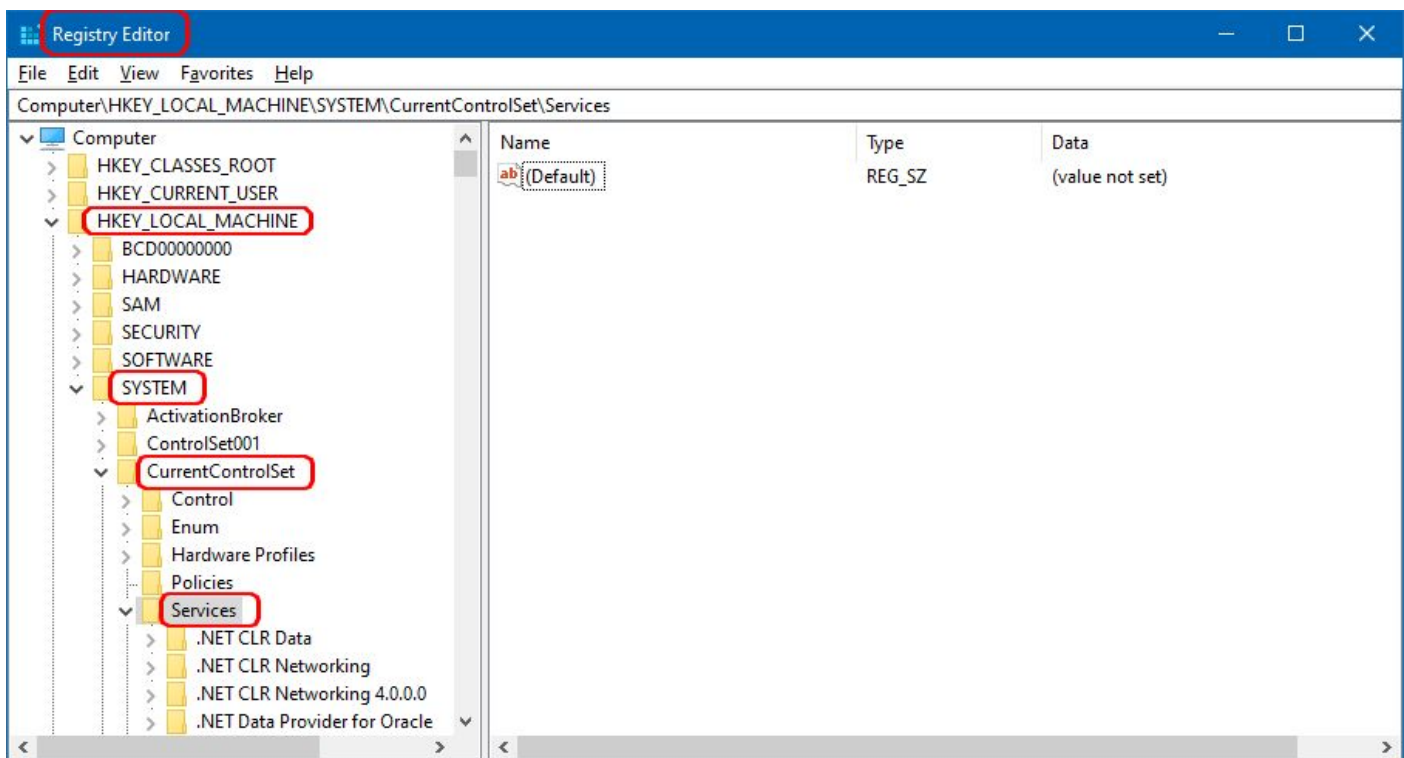
Installazione automatica (consigliata)

1. Aggiungere una chiave al registro di sistema, lanciando [WindowsVPN\\_StrongCrypto.reg](#)
2. Eseguire lo script PowerShell [AddINRiMVPN.ps1](#), cliccando col pulsante destro e facendo "Esegui con PowerShell"



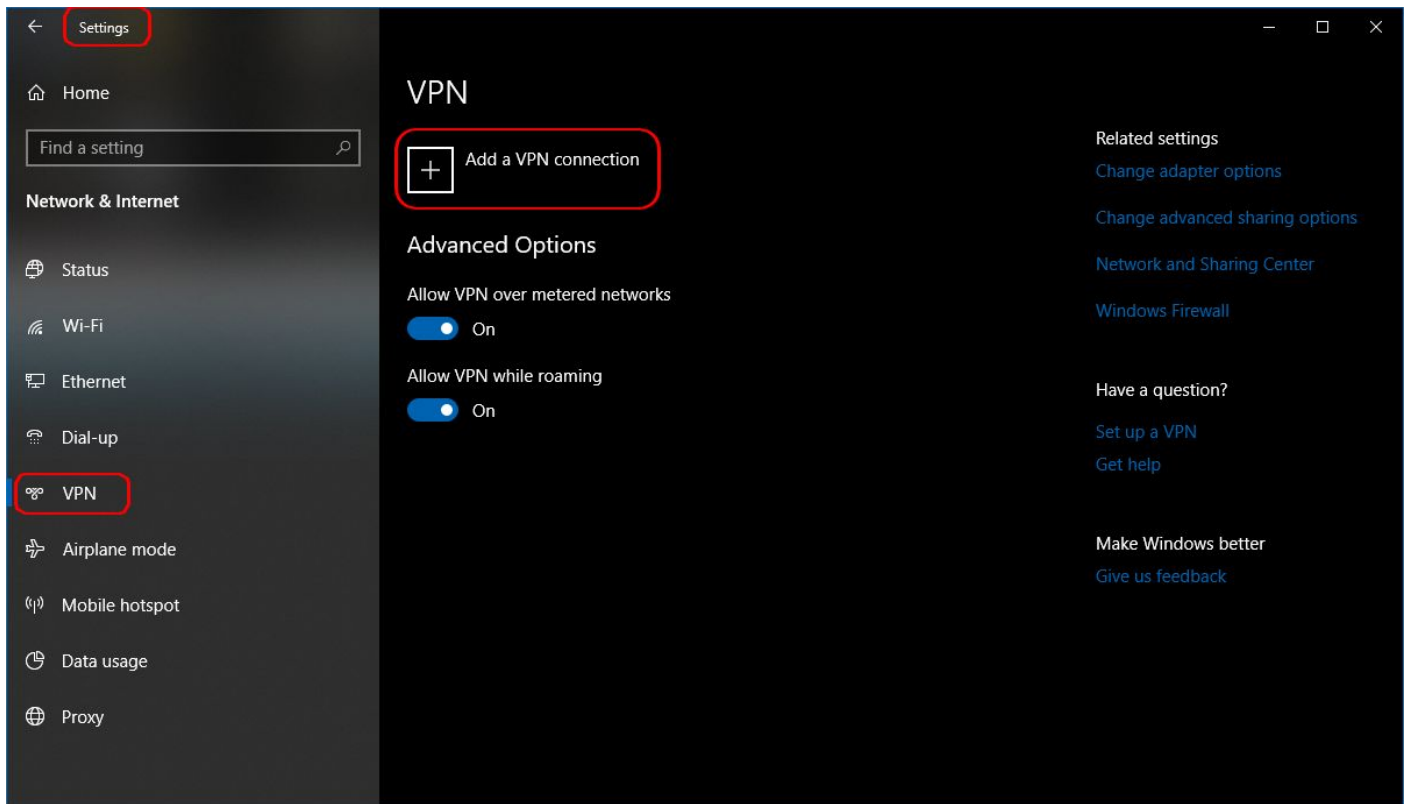
#### Installazione manuale

1. Aggiungere una chiave di registro
  - Eseguire Registry Editor (Start -> scrivere **regedit** -> Invio)
  - Posizionarsi in *HKEY\_LOCAL\_MACHINE -> SYSTEM -> CurrentControlSet -> Services -> RasMan -> Parameters*
  - Aggiungere una chiave di tipo **DWORD (32-bit) Value** con nome **NegotiateDH2048\_AES256** e assegnare il valore **1**





- Menu *Settings* -> *Network & Internet* -> *VPN*



- Configurare il nome della connessione (a piacere), nome del server a **rt.inrim.it**, tipo della VPN **IKEv2** e autenticazione nome utente/password.

Settings

## Add a VPN connection

VPN provider  
Windows (built-in) ▼

Connection name  
inrim-vpn

Server name or address  
rt.inrim.it

VPN type  
IKEv2 ▼

Type of sign-in info  
User name and password ▼

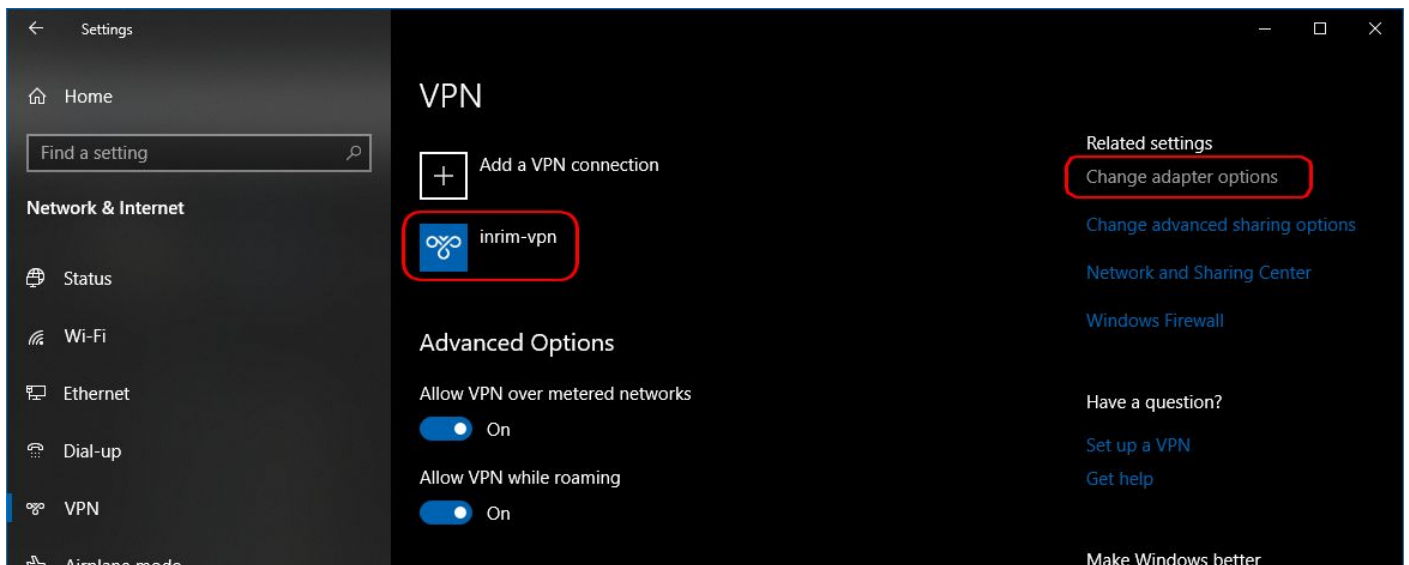
User name (optional)

Password (optional)

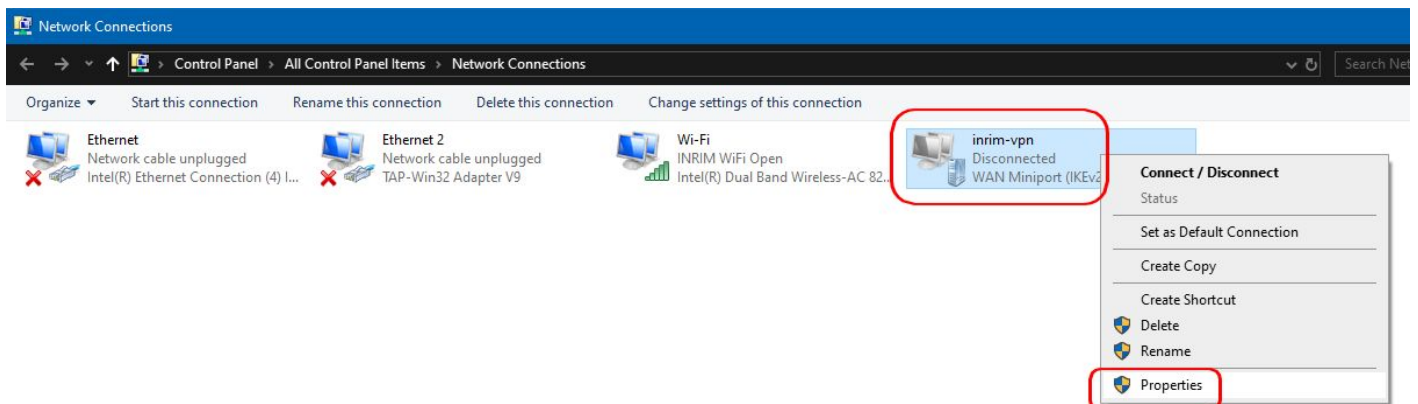
☐ Remember my sign-in info

Save Cancel

3. Configurare il nuovo adapter di rete

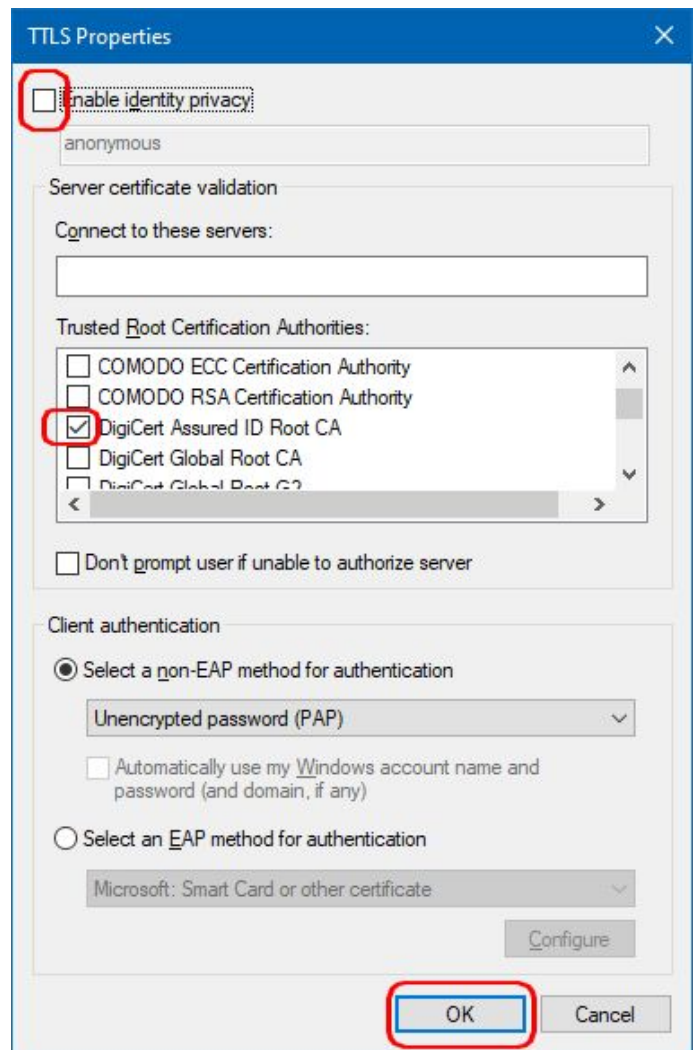
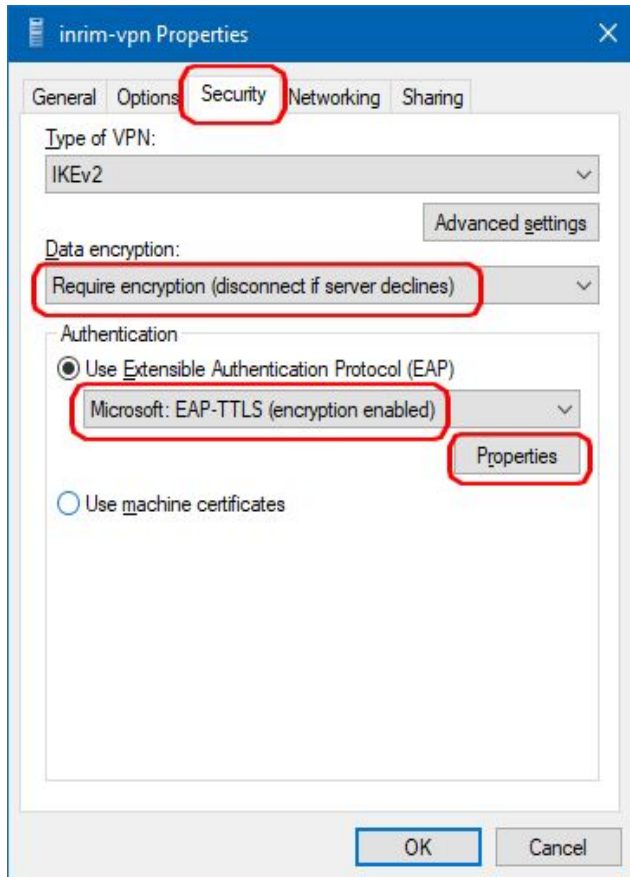


- Pulsante destro del mouse -> menu *Proprietà*



- Menu *Proprietà* -> tab *Sicurezza* ... configurazione come in figura
- Per **TLS**, cliccare su *Proprietà* -> selezionare **DigiCert Assured ID Root CA**

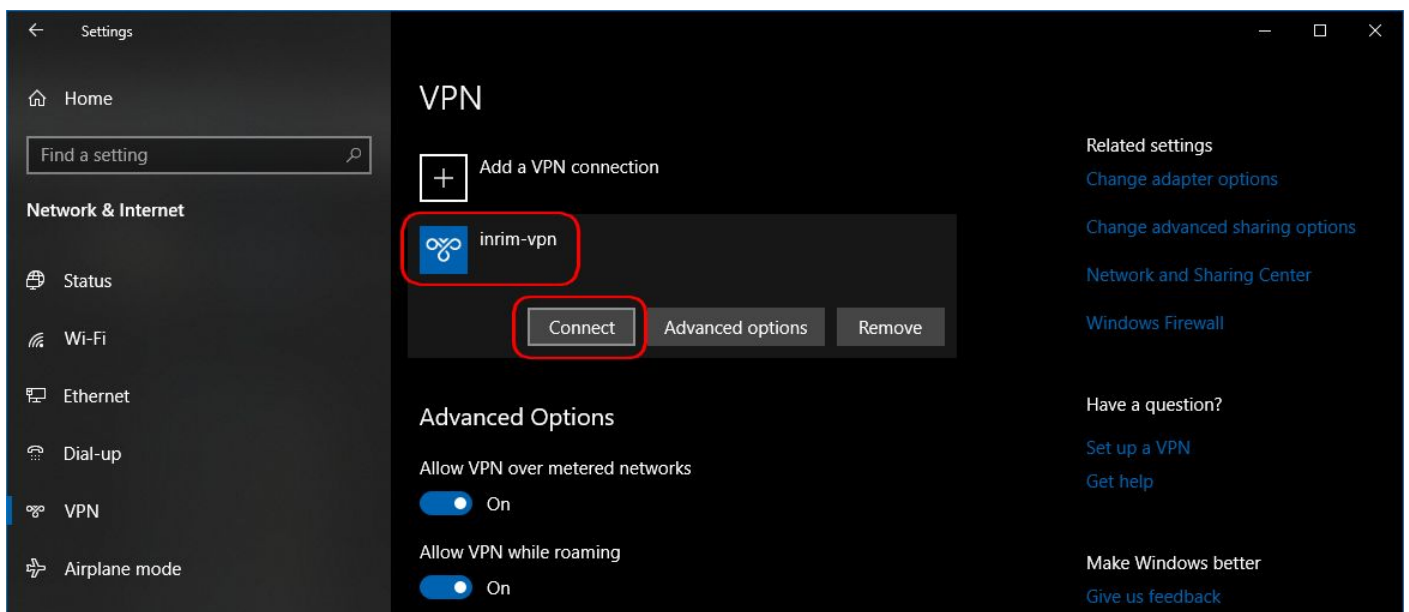




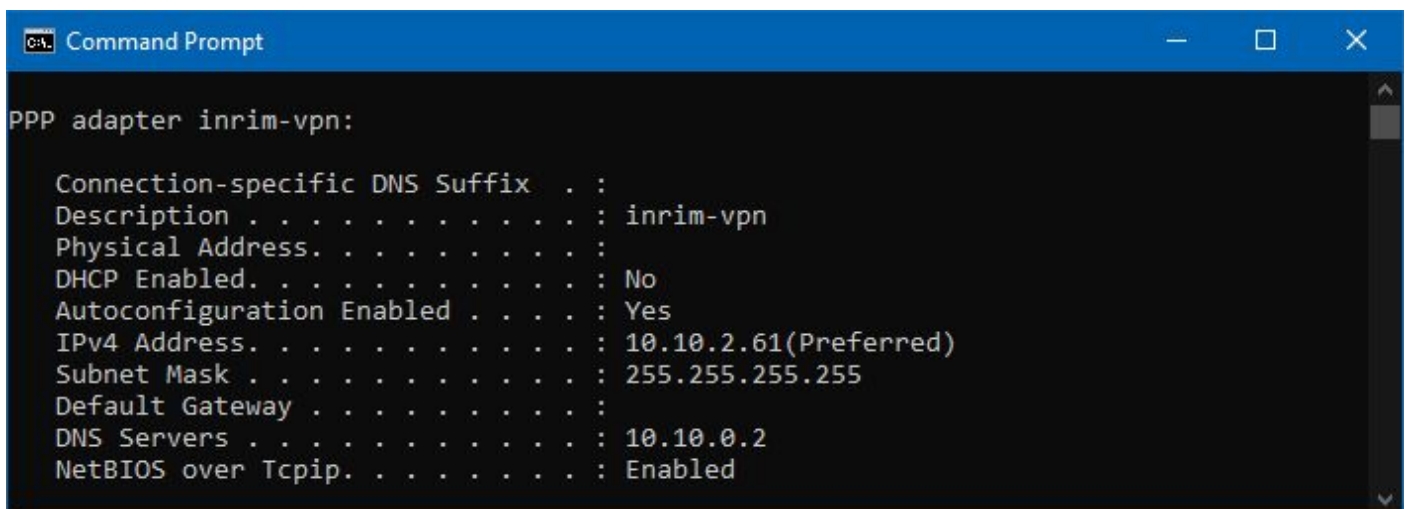
#### 4. Connessione

- Avviare la connessione specificando le proprie credenziali



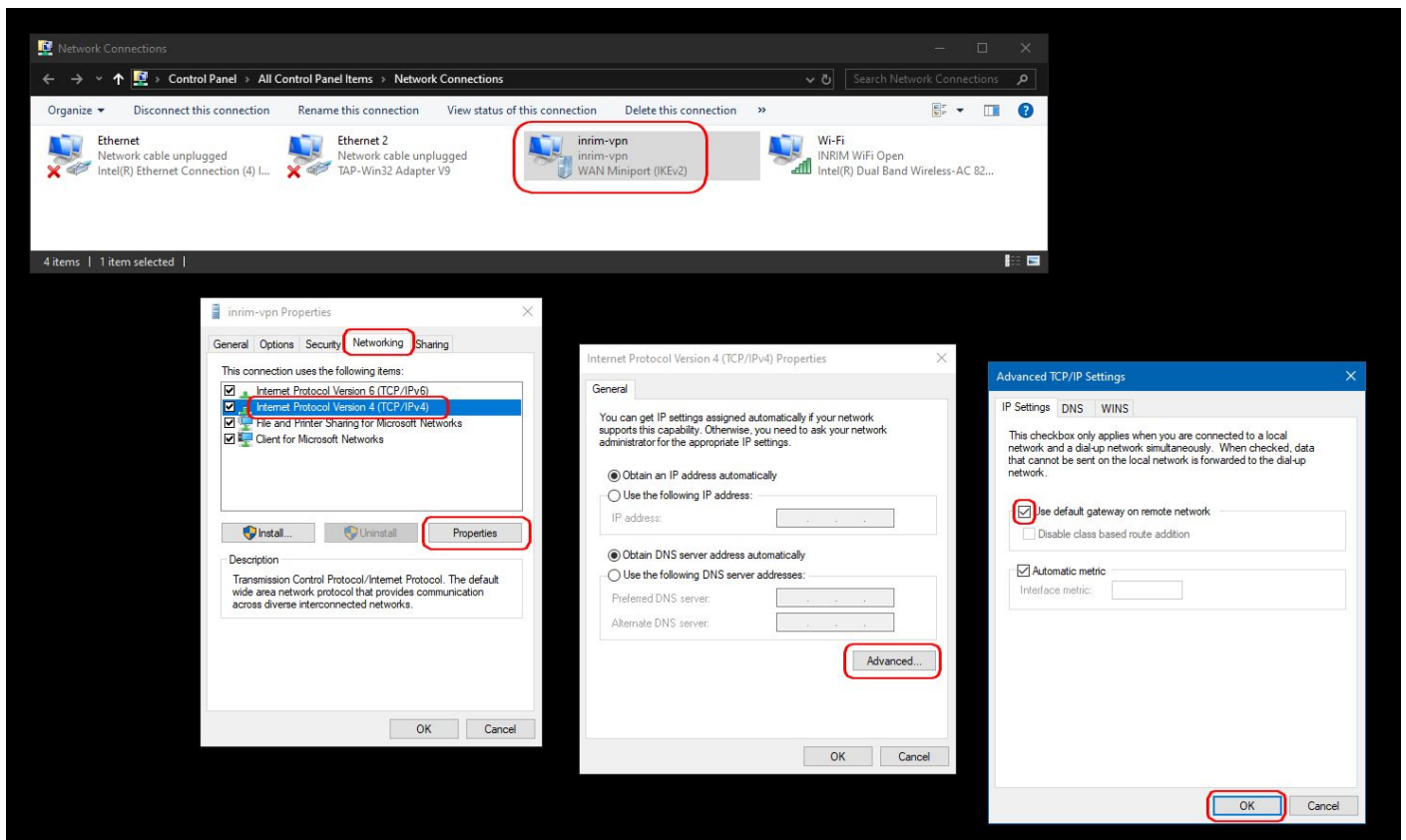


A questo punto si ha visibilità sulla rete intranet (10.10.x.y) dell'Istituto

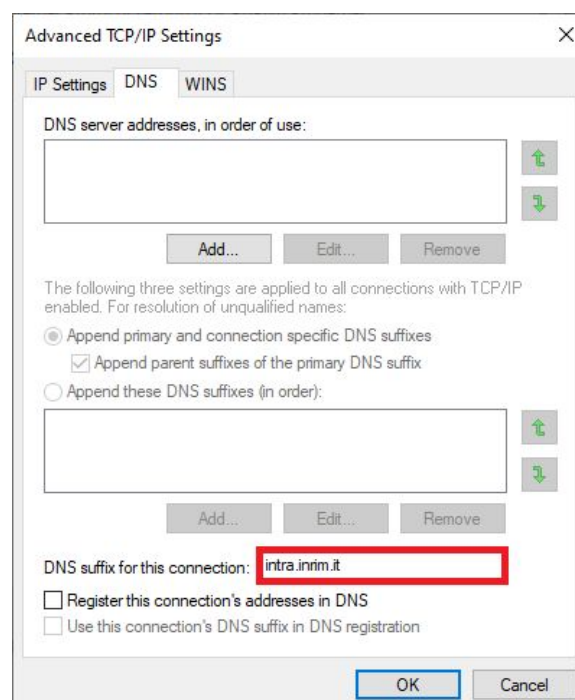


## 5. Accesso ad Internet tramite vpn

Se, oltre ai device sulle reti 10.10.x.y, si vuole uscire su Internet (ad esempio per consultare le riviste in abbonamento online), bisogna attivare l'utilizzo del gateway nelle proprietà.



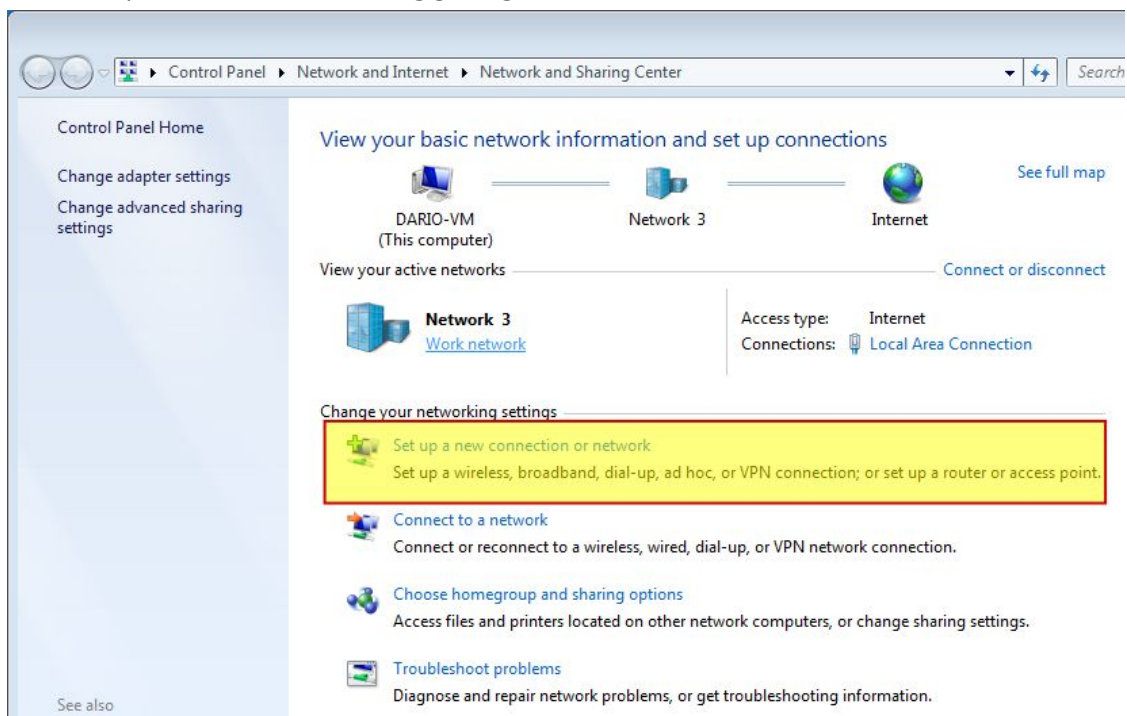
6. Risoluzione dei nomi di dominio: per poter accedere ai siti web interni senza dover digitare **.intra.inrim.it**, è necessario configurare il suffisso DNS di default. Per fare questo, bisogna accedere alla stessa finestra *“Advanced TCP/IP Settings”* del punto precedente, entrare nella scheda DNS ed inserire il suffisso di default **“intra.inrim.it”**.



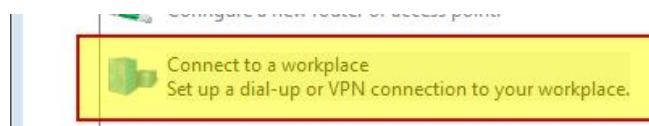
## Windows 7 SP1

**Attenzione:** il supporto ufficiale da parte di Microsoft di Windows 7 termina il 14 gennaio 2020. Pertanto, dopo quella data, non si può più garantire il funzionamento di questo sistema operativo con la VPN di istituto.

1. Verificare che la propria macchina sia completamente aggiornata
2. Installare la chiave del registro di sistema. Per fare questo, è possibile seguire il punto **1** delle istruzioni per Windows 10, oppure lanciare [WindowsVPN\\_StrongCrypto.reg](#)
3. Aggiungere una seconda chiave al registro di sistema, di tipologia **DWORD** nel percorso `HKEY_LOCAL_MACHINE -> SYSTEM -> CurrentControlSet -> services -> RasMan -> PPP -> EAP -> 13` con contenuto (esadecimale) **C00**. In alternativa, lanciare [Windows7\\_enableTLS12.reg](#)
  - o Nelle impostazioni di rete, aggiungere una nuova connessione.



4. Selezionare una connessione di tipologia VPN.



5. Selezionare il nome del server della VPN **rt.inrim.it**, dare un nome alla connessione (ad es. INRiM) e selezionare l'opzione di non connettersi immediatamente.

← Connect to a Workplace

How do you want to connect?

→ Use my Internet connection (VPN)  
Connect using a virtual private network (VPN) connection through the Internet.

→ Dial directly  
Connect directly to a phone number without going through the Internet.

[What is a VPN connection?](#)

← Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

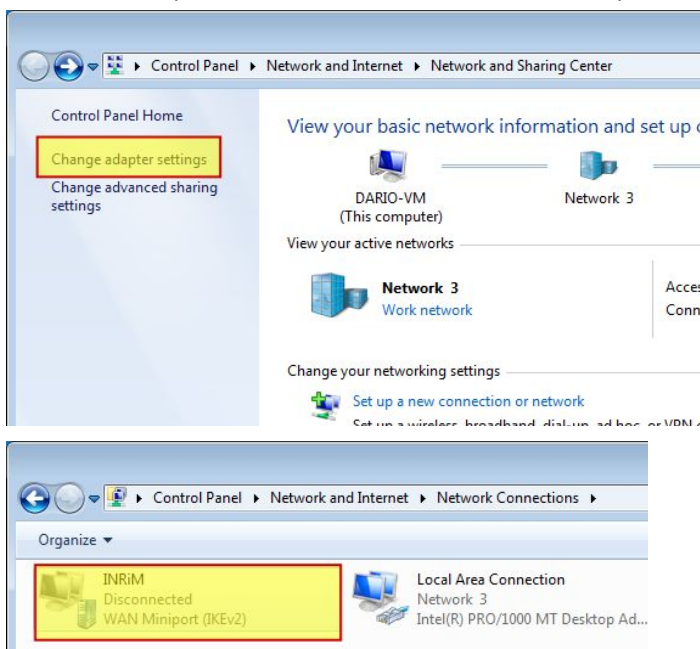
☐ Use a smart card

☐ Allow other people to use this connection  
This option allows anyone with access to this computer to use this connection.

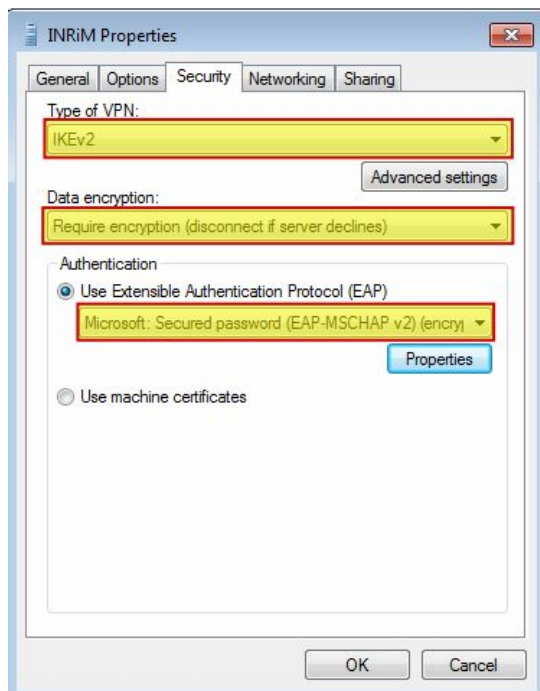
☒ Don't connect now; just set it up so I can connect later

6. Inserire nome utente e password e chiudere il wizard.

7. Aprire le impostazioni avanzate di rete, selezionare la connessione VPN appena creata, cliccare col pulsante destro del mouse e aprire le proprietà.



8. Nel tab “Sicurezza”, selezionare il tipo di VPN **IKEv2**, la crittografia obbligatoria e l'autenticazione EAP di tipo **EAP-MSCHAPv2**



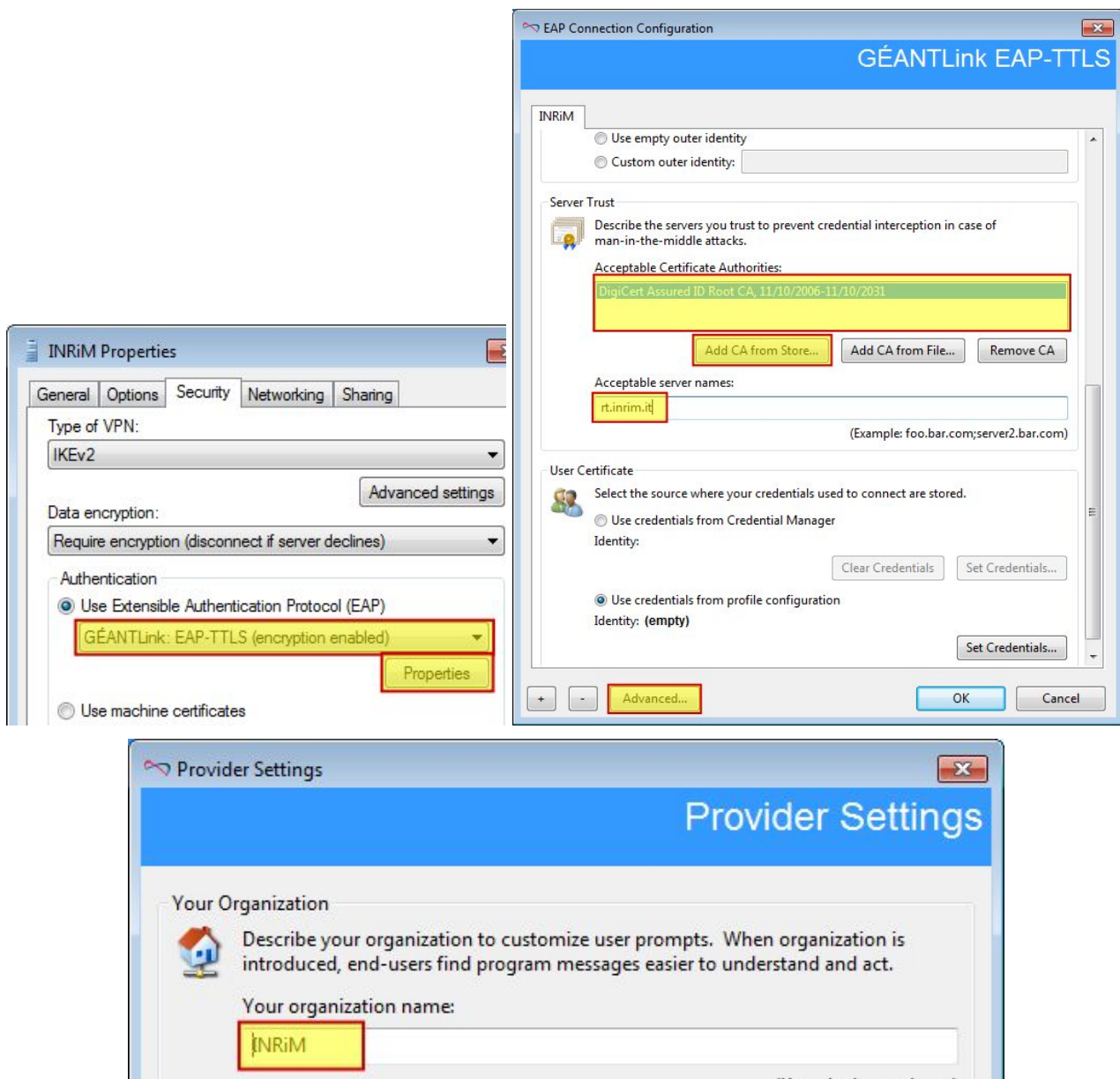
## EAP-TTLS

È possibile attivare la crittografia EAP-TTLS (più moderna e sicura rispetto a MSCHAPv2) anche su Windows 7. Per fare questo, è necessario installare un secondo supplicant EAP, **GEANTLink** disponibile su:

- <https://github.com/Amebis/GEANTLink/releases>

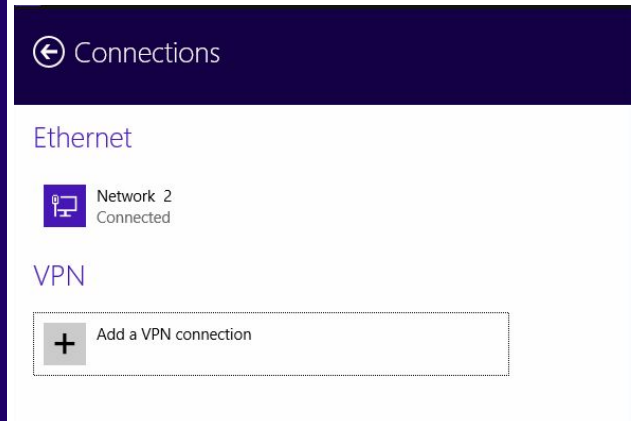
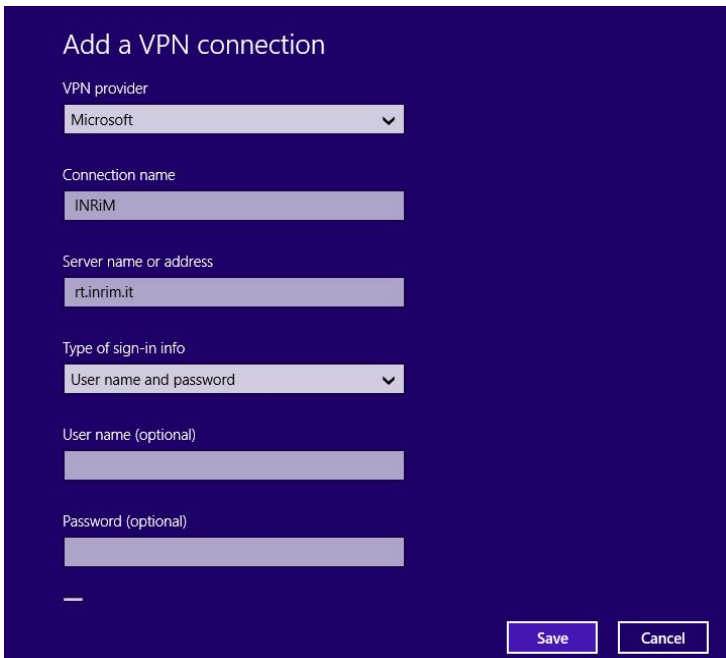
Una volta configurato, ritornare nel tab **Security** delle impostazioni VPN, selezionare **GEANTLink EAP-TTLS** e configurare il certificato, nome server e nome del provider come in figura.





## Windows 8.1

Le istruzioni di Windows 8.1 ricalcano quelle per Windows 7 SP1. Dopo aver verificato che il sistema sia completamente aggiornato e aver caricato le chiavi sul registro di sistema (punti 1-3 della guida per Windows 7 SP1), creare una nuova connessione come nelle figure:



Dopodichè, seguire i punti 7-8-9 della guida per Windows 7 SP1.

## Linux

**ATTENZIONE:** *Le istruzioni dettagliate di configurazione su Linux dipendono notevolmente dalla propria distribuzione e dalla propria configurazione. Pertanto, è possibile che queste istruzioni, sebbene siano state testate sulle distribuzioni più diffuse, necessitino di piccole modifiche/aggiustamenti.*

1. Installare un client che supporti IKEv2. Al momento, il migliore disponibile per Linux è [strongSwan](#). Si suggerisce l'installazione del client dai pacchetti della propria distribuzione, se sufficientemente recente. Questa guida suppone che la propria distribuzione usa **NetworkManager** per configurare la rete, in quanto è disponibile un plug-in di strongSwan per la configurazione grafica della VPN. Per le distribuzioni più diffuse basta installare:

**Arch Linux:**

```
pacman -S networkmanager-strongswan
```

**Debian, Ubuntu, Mint:**

```
apt install network-manager-strongswan libstrongswan-extra-plugins
```

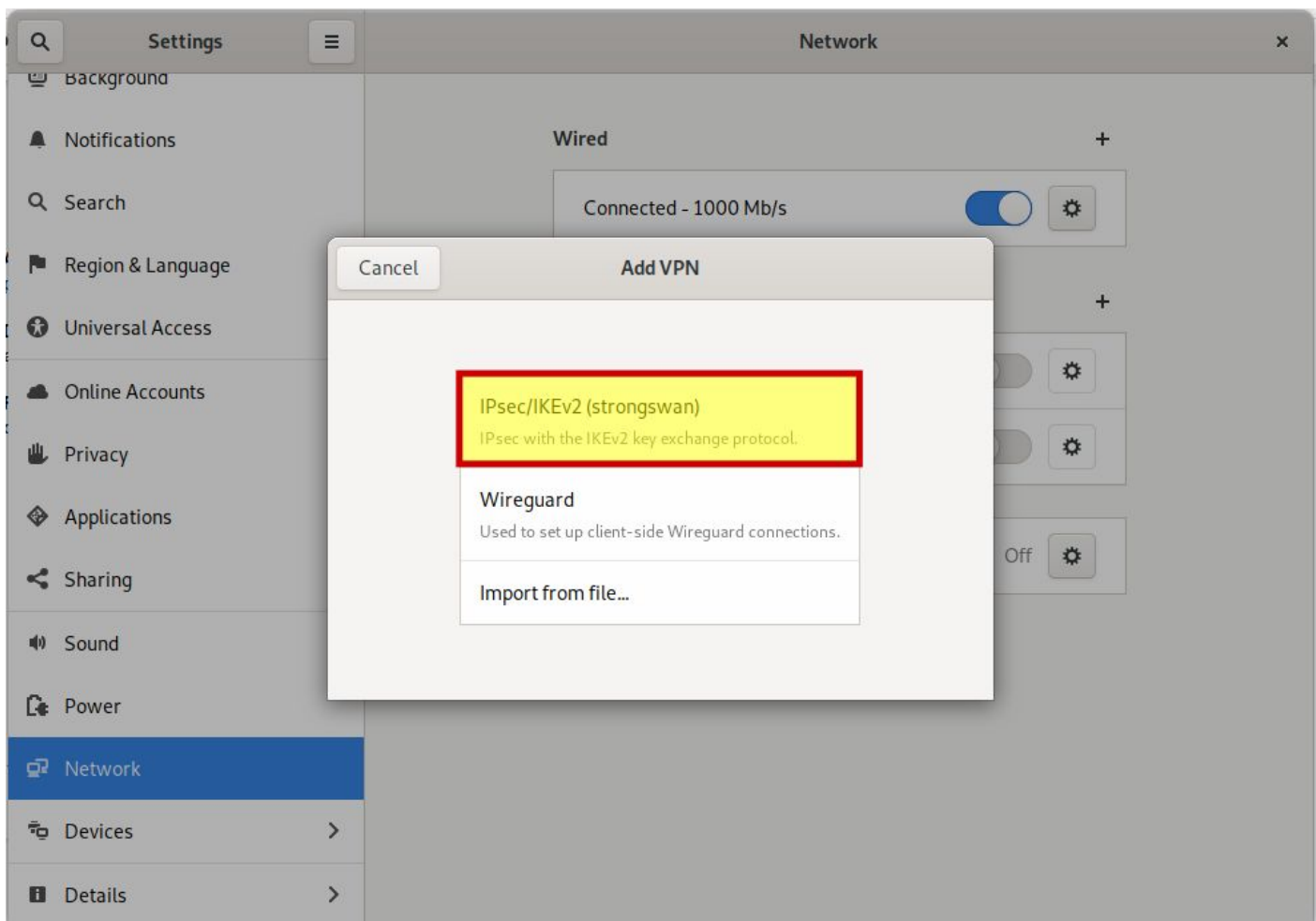
**ATTENZIONE:** A causa di un bug nella versione di strongSwan pacchettizzata in Ubuntu 16.04 e derivate (ad es. Linux Mint 18), non è possibile configurare la VPN usando NetworkManager. In questo caso, è necessario seguire la guida manuale,

oppure installare una versione più recente di strongSwan da sorgente. Per questo scopo, è possibile usare il seguente script: [InrimVpn.sh](https://inrim.it/InrimVpn.sh).

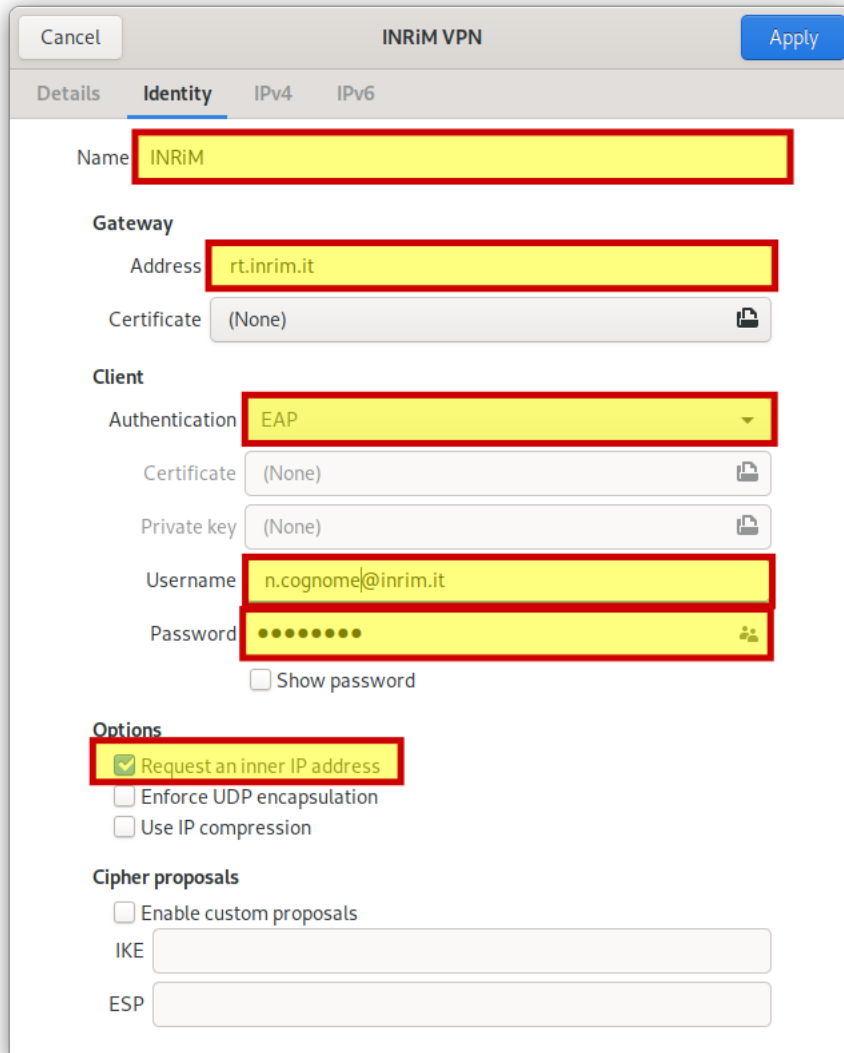
**Fedora, CentOS & RHEL (EPEL):**

```
dnf install NetworkManager-strongswan-gnome
```

2. Dalle impostazioni di rete (Settings -> Network), cliccare sul pulsante + per aggiungere una nuova VPN, e selezionare "IPsec/IKEv2 (strongswan)"



3. Inserire un nome per la VPN (qualsiasi), inserire l'indirizzo del gateway (**rt.inrim.it**), non selezionare il certificato (vengono usati quelli di sistema), selezionare l'autenticazione **EAP** ed inserire la propria coppia di nome utente e password. Per ultimo, richiedere un indirizzo IP interno.
4. Salvare ed uscire. La configurazione è ora completa.




Cancel Apply

Details **Identity** IPv4 IPv6


Name **INRiM**


**Gateway**


Address **rt.inrim.it**

Certificate (None) 


**Client**

Authentication **EAP** 

Certificate (None) 

Private key (None) 

Username **n.cognome@inrim.it**

Password **••••••••** 

☐ Show password

**Options**

☒ Request an inner IP address

☐ Enforce UDP encapsulation

☐ Use IP compression

**Cipher proposals**

☐ Enable custom proposals

IKE

ESP

5. (opzionale) Se si usa un sistema operativo recente, è consigliabile selezionare gli algoritmi di crittografia più moderni (*CNSA suite*), che garantiscono sicurezza e performance migliori rispetto a quelli di default.

#### Cipher proposals

☒ Enable custom proposals

IKE

ESP

## Configurazione manuale

Per le distribuzioni che non usano NetworkManager, o in altri casi particolari, è necessario procedere a modificare manualmente i file di configurazione di strongSwan. Per questi casi, viene fornita una traccia del file di configurazione **ipsec.conf**:

### **/etc/ipsec.conf:**

```
conn inrim
    dpdaction=restart
    dpddelay=30
    dpdtimeout=90
    fragmentation=yes
    leftsourceip=%config
    keyexchange=ikev2
    leftauth=eap-peap
    leftid=n.cognome@inrim.it
    rightauth=pubkey
    right=rt.inrim.it
    rightca="C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert
Assured ID Root CA"
    rightsubnet=0.0.0.0/0,::/0
    auto=add
    esp=aes256gcm16
    ike=aes256gcm16-prfsha384-ecp384
```

### **/etc/ipsec.secrets:**

```
n.cognome@inrim.it : EAP "(password)"
```

Il certificato della CA (DigiCertAssuredIDRootCA.pem) si recupera da:

<https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.crt>, dopo averlo convertito dal formato DER al formato PEM usando OpenSSL:

```
# openssl x509 -inform der -in DigiCertAssuredIDRootCA.crt -out
DigiCertAssuredIDRootCA.pem
```

Tale certificato deve essere messo nella directory `/etc/ipsec.d/cacerts`. Per permettere a strongSwan di leggere il certificato, va ricaricato il database con il comando

```
# ipsec rereadcacerts
```

## Problema di MTU

Sono stati registrati, su alcune distribuzioni, problemi di MTU (Maximum Transmission Unit), che causano una forte degradazione delle prestazioni nell'accesso ai siti internet. Questo è causato da un'errata configurazione del sistema operativo, che non consente agli algoritmi

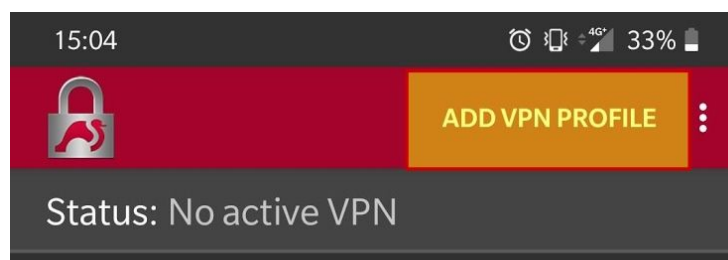
automatici di MTU discovery di funzionare correttamente. Se non si riesce a trovare la causa della mal configurazione, un possibile workaround è la riduzione manuale dell'MTU sull'interfaccia di rete collegata ad internet. Nel caso si usino algoritmi moderni di crittografia (AES-GCM), l'MTU corretta è **1390 bytes**, ma può essere anche inferiore in base alla propria connessione internet. Si consiglia di fare qualche prova con vari valori.

```
# ip link set dev <interf> mtu 1390
```

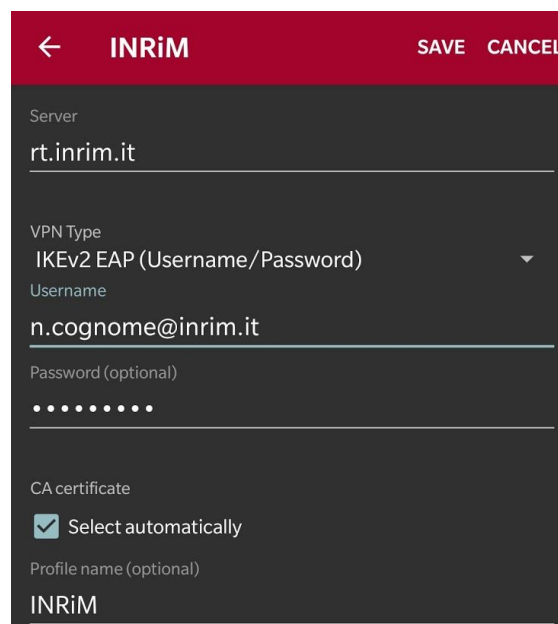
## Android

Analogamente a Linux, anche su Android è disponibile il client **strongSwan**.

1. Installare **strongSwan** dal **Google Play** store:  
<https://play.google.com/store/apps/details?id=org.strongswan.android>.
2. Da strongSwan, selezionare il pulsante in alto a destra "Add VPN Profile"



3. Nel profilo VPN, indicare il nome del server (**rt.inrim.it**), l'autenticazione (**IKEv2 EAP** username/password), inserire i propri username e password, selezionare un nome del



profilo (a piacere).



- 
4. (opzionale) Anche in questo caso, se si utilizza un dispositivo recente, è possibile migliorare sicurezza e performance della connessione selezionando algoritmi moderni di crittografia.

### Algorithms

Optionally configure specific algorithms to use for IKEv2 and/or IPsec/ESP instead of the defaults. Refer to our wiki for a [list of algorithm identifiers](#) (note that not all are supported by this app). Both fields take a list of algorithms, each separated by a hyphen.

IKEv2 Algorithms

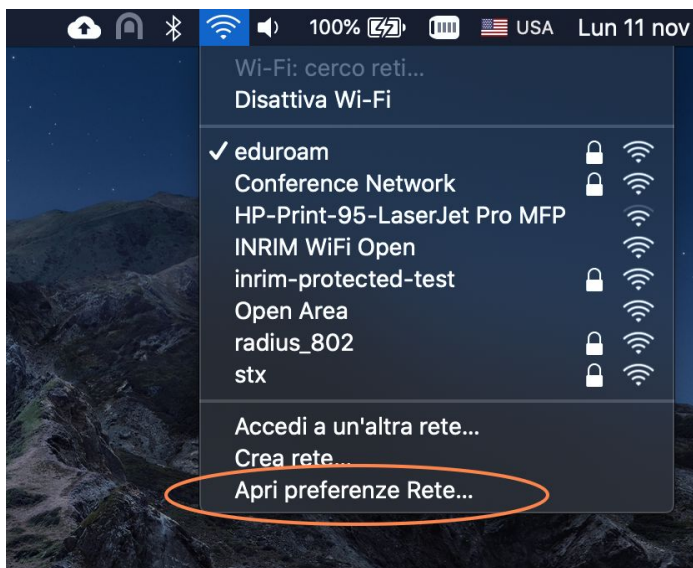
aes256gcm16-prfsha384-ecp384

IPsec/ESP Algorithms

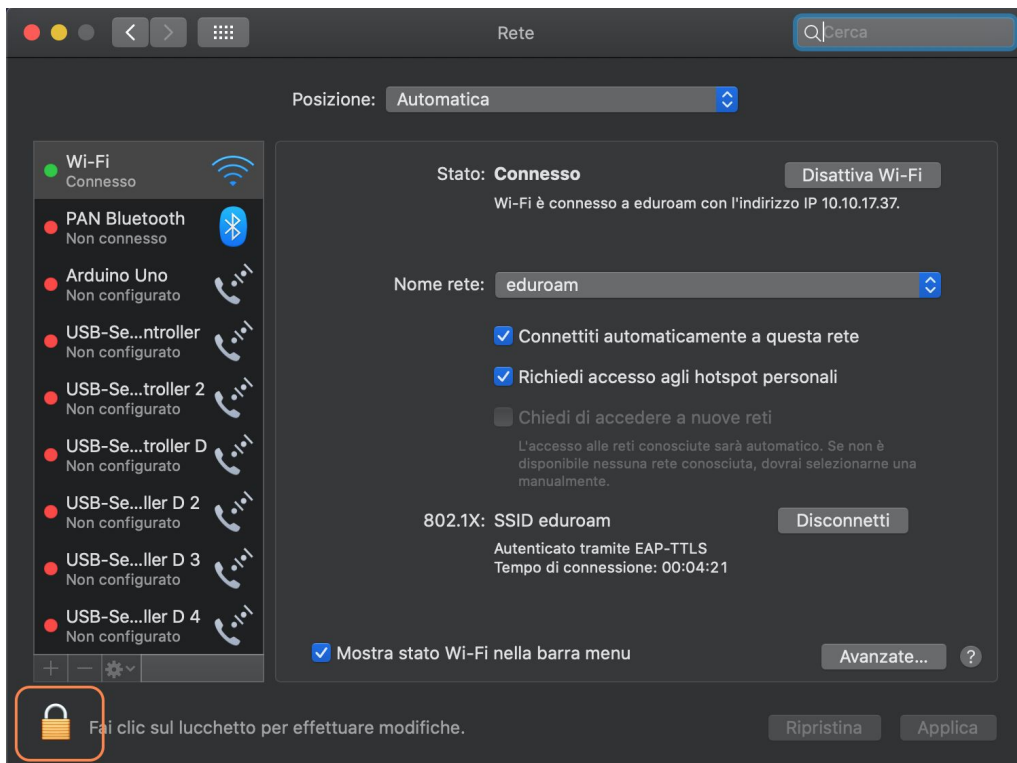
aes256gcm16

## macOS

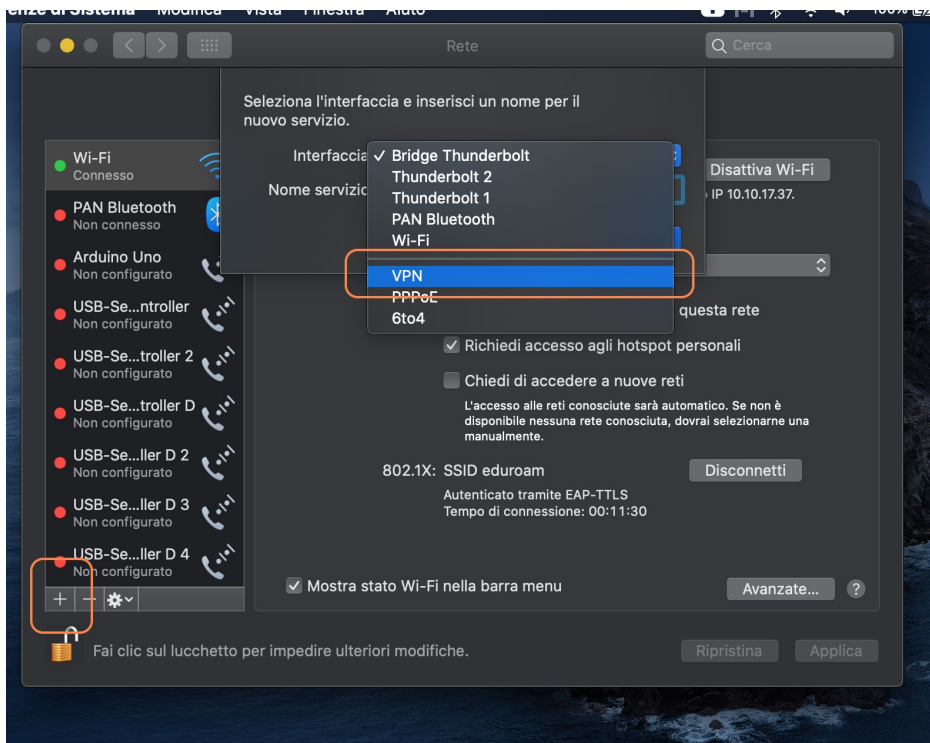
1. Aprire la configurazione di rete



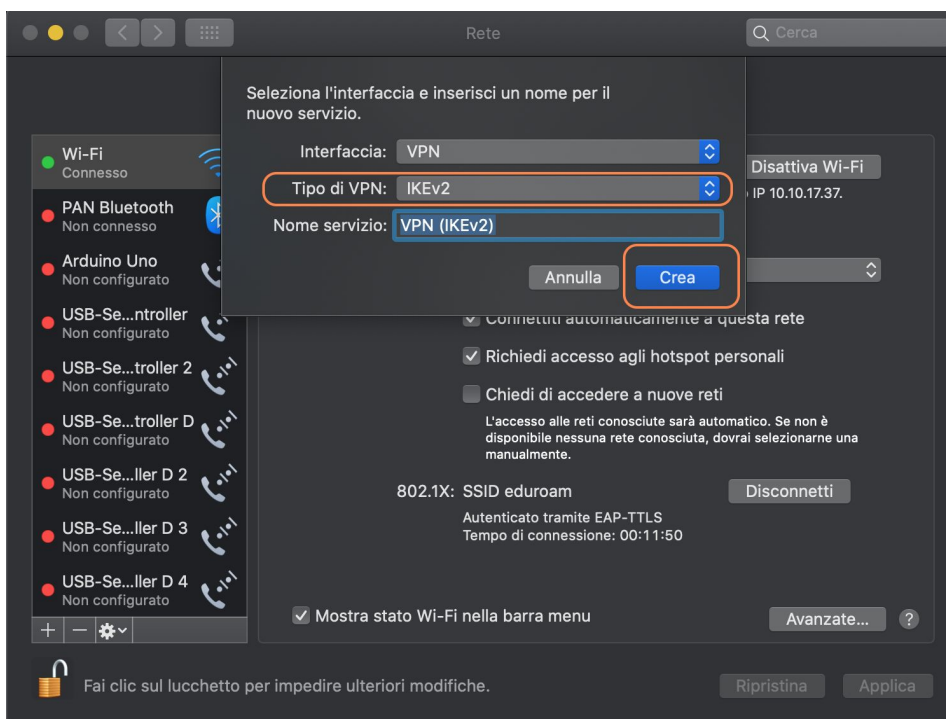
2. Sbloccare la sicurezza per aggiungere la configurazione del servizio



3. Click su "+" per aggiungere il nuovo servizio

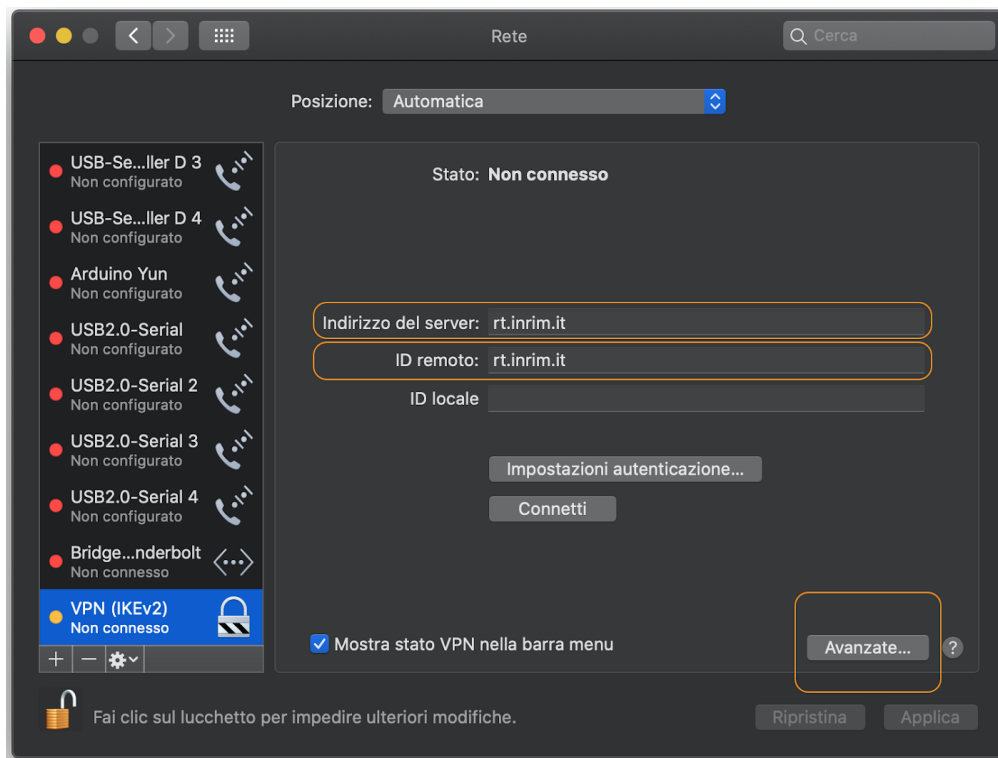
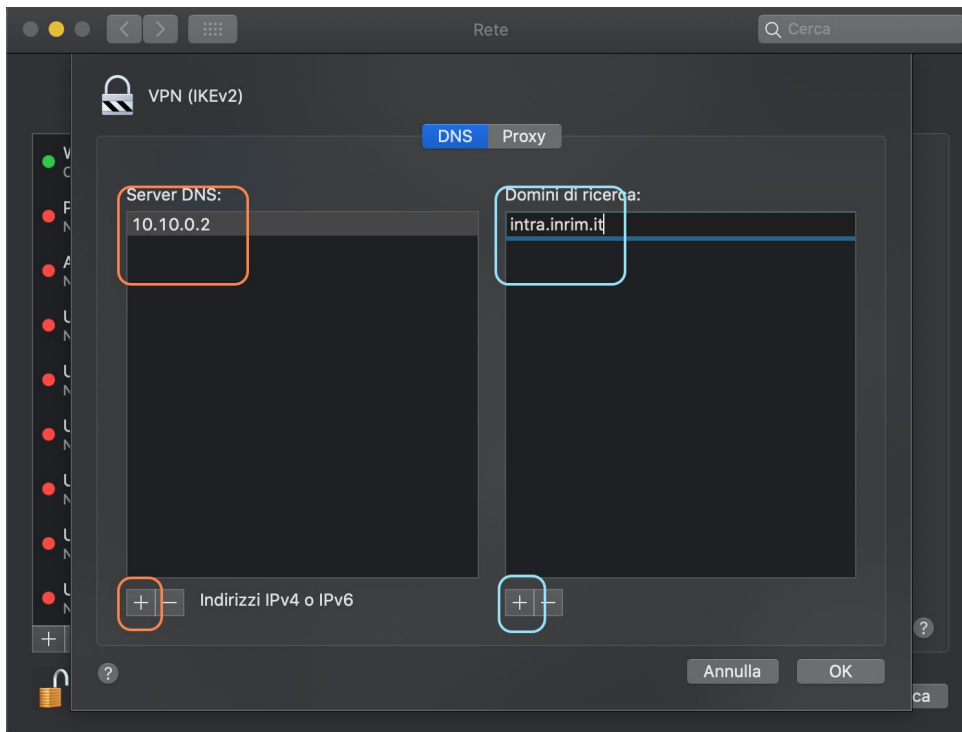


#### 4. selezionare **Vpn** → **IKEv2**

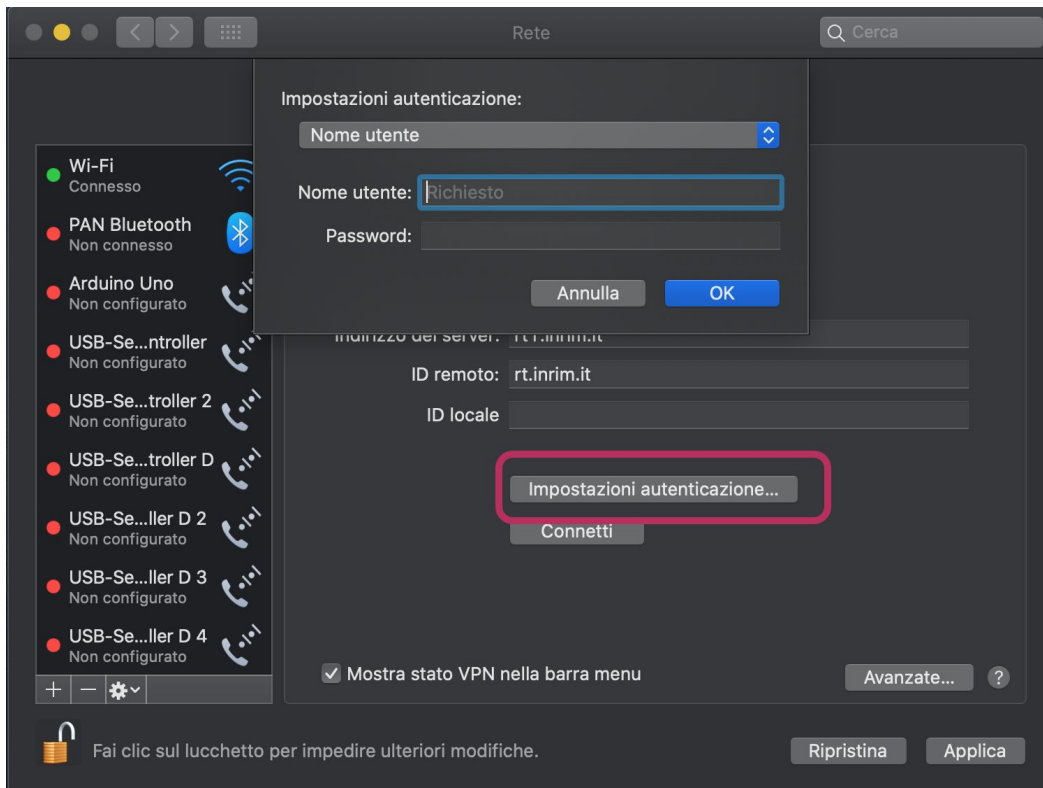


#### 5. Impostare indirizzo server: **rt.inrim.it**

6. con avanzate configurare **Dns** → **10.10.0.2** e **10.200.1.10** , **Domini ricerca** → **intra.inrim.it**



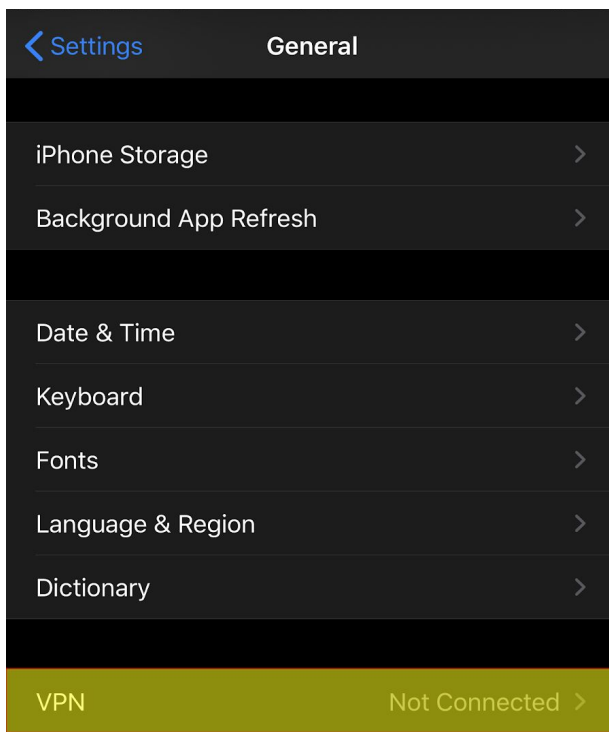
7. Cliccare su **Impostazioni autenticazione** ed inserire le proprie credenziali  
**n.cognome@inrim.it**



8. Connetti

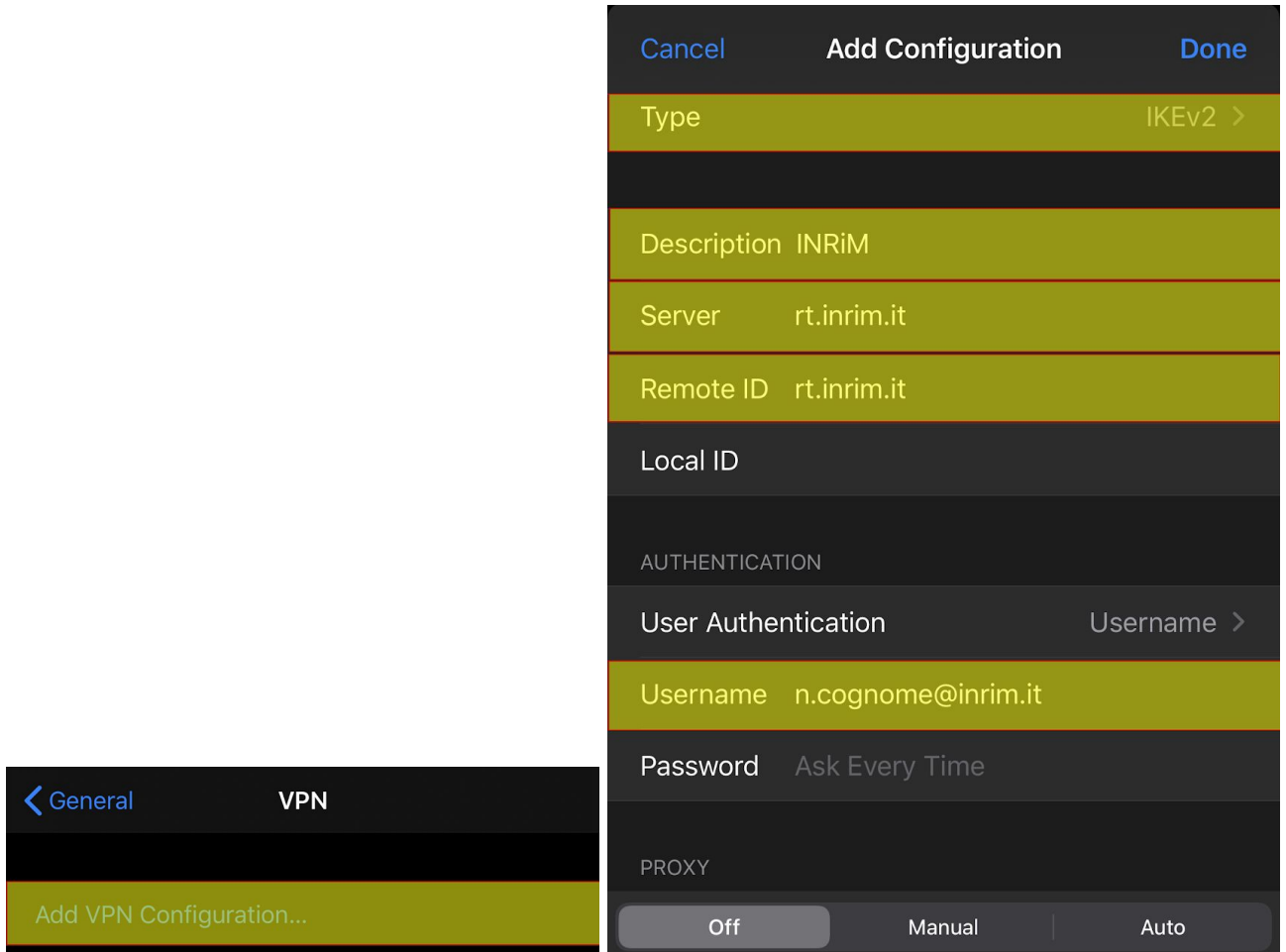
## iOS e iPadOS

1. Entrare nelle **Impostazioni** -> **Generali** -> **VPN**.





2. Aggiungere una nuova VPN, e selezionare il tipo (**IKEv2**), la descrizione (a piacere), il nome del server e l'identità remota (**rt.inrim.it**) e l'username ([n.cognome@inrim.it](mailto:n.cognome@inrim.it)).



The image shows two overlapping screenshots of an iOS VPN configuration interface. The background screenshot shows the 'VPN' settings page with a 'General' tab selected and an 'Add VPN Configuration...' button. The foreground screenshot is a detailed view of the 'Add Configuration' dialog box, which is titled 'Add Configuration' and has 'Cancel' and 'Done' buttons. The dialog contains the following fields:

- Type:** IKEv2 >
- Description:** INRiM
- Server:** rt.inrim.it
- Remote ID:** rt.inrim.it
- Local ID:** (empty)
- AUTHENTICATION:**
  - User Authentication:** Username >
  - Username:** n.cognome@inrim.it
  - Password:** Ask Every Time
- PROXY:**
  - Off** (selected)
  - Manual
  - Auto

3. Salvare e chiudere. Ora è possibile accedere alla VPN dalle impostazioni di rete.

## Lista delle modifiche

Data	Modifiche	Autore/i
02/12/2019	<ul style="list-style-type: none"><li>• Pubblicazione versione iniziale</li></ul>	D. Pileri
05/12/2019	<ul style="list-style-type: none"><li>• Modifica nome del server VPN:<ul style="list-style-type: none"><li>◦ rtl.inrim.it -&gt; <b>rt.inrim.it</b></li></ul></li></ul>	D. Pileri
06/12/2019	<ul style="list-style-type: none"><li>• Aggiunta istruzioni per iOS/iPadOS</li></ul>	D. Pileri
11/12/2019	<ul style="list-style-type: none"><li>• Sistemato errore nella configurazione di strongSwan su Linux (ipsec.conf)</li></ul>	D. Pileri
17/12/2019	<ul style="list-style-type: none"><li>• Aggiunta traccia di configurazione per Windows 8.1</li></ul>	D. Pileri
27/12/2019	<ul style="list-style-type: none"><li>• Aggiunte precisazioni e sistemazione di piccoli errori nella configurazione su Linux</li></ul>	D. Pileri
25/02/2020	<ul style="list-style-type: none"><li>• Aggiunto server DNS secondario <b>10.200.1.10</b></li></ul>	D. Pileri
09/03/2020	<ul style="list-style-type: none"><li>• Modifica configurazione Windows 7 usando MSCHAPv2, per migliore compatibilità.</li></ul>	D. Pileri