Regione Puglia

Assessorato alle Politiche della Salute

Area Promozione delle politiche della salute, delle persone e delle pari opportunità

Collegamento alla RUPAR-SPC via VPN

Manuale utente

Versione 1.10

22 Dicembre 2014

Indice

DIRITTI DI AUTORE E CLAUSOLE DI RISERVATEZZA

Il presente documento è stato prodotto da InnovaPuglia nell'ambito dell'affidamento codificato come SAN001.2010.

STORIA DEL DOCUMENTO

Versione	Stato	Chi	Data	Memorizzato in:
1.4	FINALE	InnovaPuglia	30/11/2012	
1.5	FINALE	InnovaPuglia	28/01/2013	
1.6	FINALE	InnovaPuglia	29/01/2013	
1.07	FINALE	InnovaPuglia	01/02/2013	
1.08	FINALE	InnovaPuglia	05/02/2013	
1.09	FINALE	InnovaPuglia	17/05/2013	
1.10	FINALE	InnovaPuglia	22/12/2014	

STORIA DELLE REVISIONI

Versione	Modifiche
1.0	Versione iniziale
1.4	Inseriti riferimenti a Portale della Salute
1.5	Inserita procedura di accettazione del Regolamento di utilizzo della RUPAR-SPC
1.6	Rettificato orario del Servizio HelpDesk
1.07	Rimosso riferimento al Numero Verde del Servizio Assistenza (Servizio HelpDesk)
1.08	Aggiornati loghi
1.09	Inserita documentazione per tablet e smartphone Apple
1.10	Inserita documentazione per Cisco Anyconnect Inserita documentazione per Mac-book Apple

MODIFICHE PREVISTE

Le modifiche potranno avvenire a seguito di revisioni o di intese con la Regione Puglia.

TABELLA REDAZIONE E APPROVAZIONE

Responsabile redazione	Responsabile approvazione
InnovaPuglia SpA	InnovaPuglia SpA

1 Introduzione

1.1 Scopo e campo di applicazione del documento

Scopo del documento è descrivere le attività che un soggetto deve realizzare per accedere – se autorizzato dal Servizio Sanitario Regionale della Regione Puglia - in maniera protetta, alla RUPAR-SPC e per mezzo di essa per collegarsi ai sistemi informativi sanitari resi disponibili su RUPAR-SPC.

Il documento descrive anche i correlati servizi di assistenza tecnica predisposti per fornire informazioni e per risolvere eventuali problematiche.

1.2 Il contesto di riferimento

Nel contesto dell'attuazione del Piano della Sanità Elettronica la Regione Puglia ha promosso la realizzazione presso InnovaPuglia (società in house della Regione Puglia) del Centro Servizi Sanità Elettronica Regionale che accorpa in un unico punto - con le necessarie caratteristiche tecniche in materia di servizi di elaborazione e di comunicazione nonché con le necessarie competenze professionali - l'erogazione di sistemi informativi a valenza regionale. Alcuni esempi di sistemi informativi ospitati nel Centro Servizi Sanità Elettronica Regionale sono: Sistema Informativo Sanitario Territoriale (SIST), Nardino, Sistema di gestione dell'approvvigionamento dei farmaci inclusi PHT in Distribuzione per Conto, sistema informativo delle vaccinazioni (Giava), Sistema Informativo Sanitario Regionale (Edotto – limitatamente alle funzioni dell'area applicativa Direzionale), sistema informativo di anatomia patologica, sistema informativo di pseudonimizzazione.

Le risorse del Centro Servizi Sanità Elettronica Regionale, così come quelle di altri sistemi informativi quale Edotto, sono disponibili solo attraverso l'infrastruttura di comunicazione della pubblica amministrazione della Regione Puglia denominata RUPAR-SPC.

Il Centro Servizi Sanità Elettronica Regionale realizza anche il punto di accoglienza tecnica per utenza afferente al SSR che non abbia accesso diretto alla RUPAR-SPC ma che risulta connessa alla rete Internet pubblica. Mediante il punto di accoglienza del Centro Servizi Sanità Elettronica Regionale, tale utenza può accedere ai sistemi informativi sanitari resi disponibili dalla Regione Puglia e dalle Aziende Sanitarie su RUPAR-SPC. Esempi di tali categorie di utenza possono essere:

- **Medici di Famiglia (Medici di Medicina Generale e Pediatri di Libera Scelta)** che operano presso i loro studi medici professionali;
- **Medici dell'Emergenza Sanitaria Territoriale (118)** che operano in ambienti privi – ad oggi – della connessione alla Intranet aziendale;
- **Medici di Continuità Assistenziale** che operano in ambienti privi – ad oggi – della connessione alla Intranet aziendale;
- **Medici dei Servizi Territoriali** che operano in ambienti privi – ad oggi – della connessione alla Intranet aziendale;
- **Medici Specialisti Ambulatoriali Interni** che operano in ambienti privi – ad oggi – della connessione alla Intranet aziendale;
- **Operatori di altre professionalità sanitarie (psicologi, chimici, biologi, veterinari, ...)** che operano in ambienti privi – ad oggi – della connessione alla Intranet aziendale;

- **Operatori di strutture sanitarie private accreditate** che non dispongono né di un collegamento alla RUPAR-SPC né di un collegamento alla Intranet della ASL con cui hanno un accordo contrattuale;
- **Operatori di fornitori di dispositivi protesici**.

1.3 Acronimi

Acronimo	Descrizione
CAD	Codice dell'Amministrazione Digitale
CMS	CNS Management System (o Sistema Gestione CNS)
CN	Community Network
PdR	Porta di Rete RUPAR-SPC
RUPAR-SPC	Rete Unitaria della Pubblica Amministrazione – Sistema Pubblico di Connettività
SPC	Sistema Pubblico di Connettività
VPN	Virtual Private Network

1.4 Riferimenti

1. Decreto Legislativo 7 marzo 2005, n. 82 – Codice dell'Amministrazione Digitale

2 Fasi di lavoro

Per l'utenza che non dispone di un collegamento diretto alla RUPAR-SPC ma dispone di un collegamento alla rete pubblica Internet, il collegamento alla RUPAR-SPC prevede la esecuzione di **attività una tantum** e di **attività ripetitive** che differiscono in funzione dell'ambiente operativo (Microsoft Windows, Apple iOS) che si sta utilizzando.

Con riferimento all'ambiente **Microsoft Windows**:

a) Le **attività una tantum** sono le seguenti:

- Acquisizione del software Cisco VPN Client o Cisco AnyConnect a seconda del sistema operativo della propria postazione di lavoro da utilizzarsi per l'esecuzione del collegamento (Sezione **Microsoft Windows: Acquisizione Cisco VPN Client**);
- Installazione del software Cisco VPN Client o Cisco AnyConnect (Sezione **Microsoft Windows: Installazione di Cisco VPN Client**);
- Configurazione del profilo di collegamento (Sezione **Comparirà la finestra di inizio installazione. Cliccare su "Next"(Figura 16)**
- 

Figura 16

1. Apparirà il contratto di licenza per il quale è necessario selezionare la casella **"I accept the license agreement"** e cliccare su **"Next"** (Figura 17)

Figura 17

2. Per iniziare l'installazione scegliere **"Install"** (Figura 18)

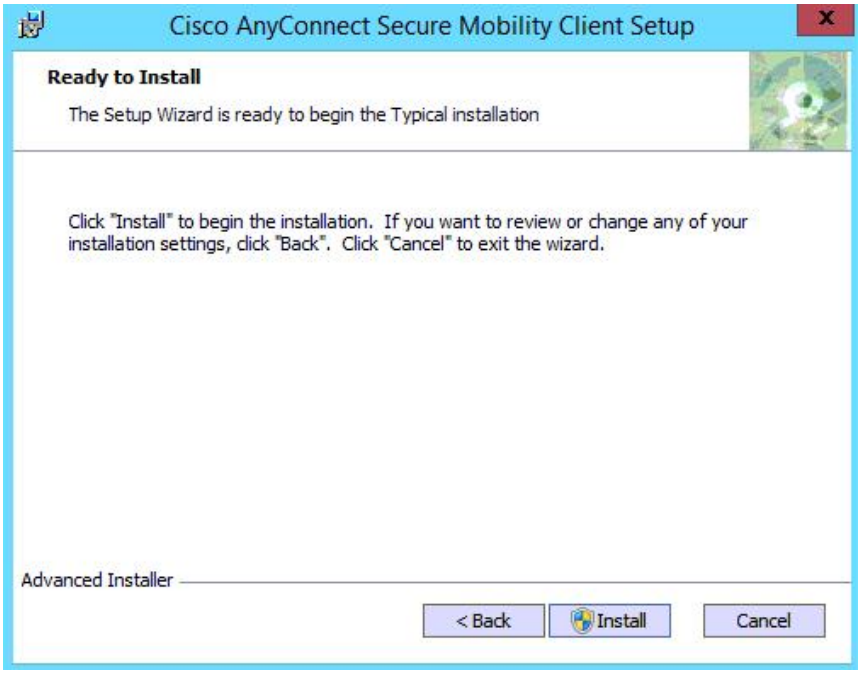


Figura 18

3. Al termine dell'installazione cliccare su **"Finish" (Figura 19)**

Figura 19

- Microsoft Windows: Creazione profilo per il collegamento protetto al Centro Servizi Sanità Elettronica Regionale).
- Accettazione del Regolamento RUPAR-SPC (Sezione **Microsoft Windows: Accettazione del Regolamento di utilizzo della RUPAR-SPC**).

b) Le **attività ripetitive** sono le seguenti:

- creazione del collegamento protetto (Sezione **Microsoft Windows: Avviamento del collegamento protetto al Centro Servizi Sanità Elettronica Regionale**);
- conclusione del collegamento protetto (Sezione **Microsoft Windows: Conclusione del collegamento protetto al Centro Servizi Sanità Elettronica Regionale**).

La descrizione delle attività fa riferimento ad un PC con installato Microsoft Windows 7.

Con riferimento all'ambiente **Apple iOS**:

a) Le **attività una tantum** sono le seguenti:

- Configurazione del profilo di collegamento (Sezione **Apple - Connessione mediante tablet e smartphone**).
- Configurazione del profilo di collegamento (Sezione **Apple – Connessione mediante Mac-book**).
- Accettazione del Regolamento RUPAR-SPC (Sezione **17 Apple - Accettazione del Regolamento di utilizzo della** RUPAR-SPC).

b) Le **attività ripetitive** sono le seguenti:

- creazione del collegamento protetto (Sezione **Apple - Avvio Connessione VPN con smartphone e tablet**);

3 Prerequisiti

Il prodotto individuato e reso disponibile dalla Regione Puglia per la gestione del collegamento VPN è – in funzione delle caratteristiche della propria stazione di lavoro - **Cisco AnyConnect VPN Client e Cisco VPN Client**.

Per poter installare correttamente il software Cisco è necessario che sul computer operante in ambiente Microsoft Windows sia installato un programma per la decompressione di file in formato ZIP.

Riferimenti per lo scarico di software per la compressione/decompressione:

Software	URL
PeaZip	http://peazip.sourceforge.net/
ZIPGenius	http://www.zipgenius.it/

4 Microsoft Windows: Acquisizione Cisco VPN Client o Cisco AnyConnect

Per acquisire il software Cisco VPN Client o Cisco AnyConnect è necessario:

- collegarsi al Portale Regionale della Salute **http://www.sanita.puglia.it,**
- accedere all'area "**Centro Servizi Sanitari Regionale**" della sezione "**Progetti**" cliccando sul relativo link:

- ed effettuare il download del software selezionando l'opportuno link in funzione del tipo di sistema operativo:

Software	**Microsoft Windows XP**		**Microsoft Vista-Seven**		**Microsoft Windows 8**
	32-bit	**64-bit**	**32-bit**	**64-bit**	**32-bit 64-bit**
cisco VPN client v. 5.0 32-bit XP-Vista-Seven	√		√		
cisco VPN client v. 5.0 64-bit XP-Vista-Seven		√		√	
cisco AnyConnect v. 3.1.01065			√	√	√

La sezione successiva fornisce informazioni su come determinare il tipo di sistema operativo installato.

4.1 Determinazione del tipo di sistema operativo Microsoft Windows (32 o 64 bit) è installato sul proprio PC

Per determinare quale tipo di sistema operativo Microsoft Windows (32 o 64 bit) è installato sul proprio PC, eseguire - in funzione del tipo di sistema operativo installato – una delle procedure di seguito riportate suggerite dal supporto Microsoft (http://support.microsoft.com/kb/827218/it).

4.1.1 Windows Vista, Windows 7 e Windows 8

Se si dispone di Windows Vista, Windows 7 e Windows 8 esistono due metodi per determinare se è in esecuzione una versione a 32 bit o una versione a 64 bit. Se un metodo non funziona, provare l'altro metodo.

Metodo 1: Visualizzare la finestra di sistema nel Pannello di controllo

1. Fare clic su **Start** , digitare **sistema** nella casella **Inizia ricerca** e quindi fare clic su **sistema** nell'elenco **programmi** .
2. Il sistema operativo viene visualizzato come segue:
   - Per un sistema operativo a 64 bit, **sistema operativo a 64 bit** viene visualizzato per il **tipo di sistema** in **sistema** (Figura 1).
   - Per una versione a 32 bit del sistema operativo, **sistema operativo a 32 bit** viene visualizzato per il **tipo di sistema** in **sistema**.

Metodo 2: Visualizzare la finestra delle informazioni di sistema

1. Fare clic su **Start** , digitare **sistema** nella casella **Inizia ricerca** e quindi fare clic su **Informazioni di sistema** nell'elenco **programmi** .
2. Quando il **Sistema di riepilogo** è selezionata nel riquadro di spostamento, il sistema operativo viene visualizzato come segue:
   - **Per un sistema operativo a 64 bit, x64 e PC viene visualizzato per il tipo di sistema alla voce**.
   - **Per un sistema operativo in versione a 32 bit, basate su x86 PC viene visualizzato per il tipo di sistema alla voce** .

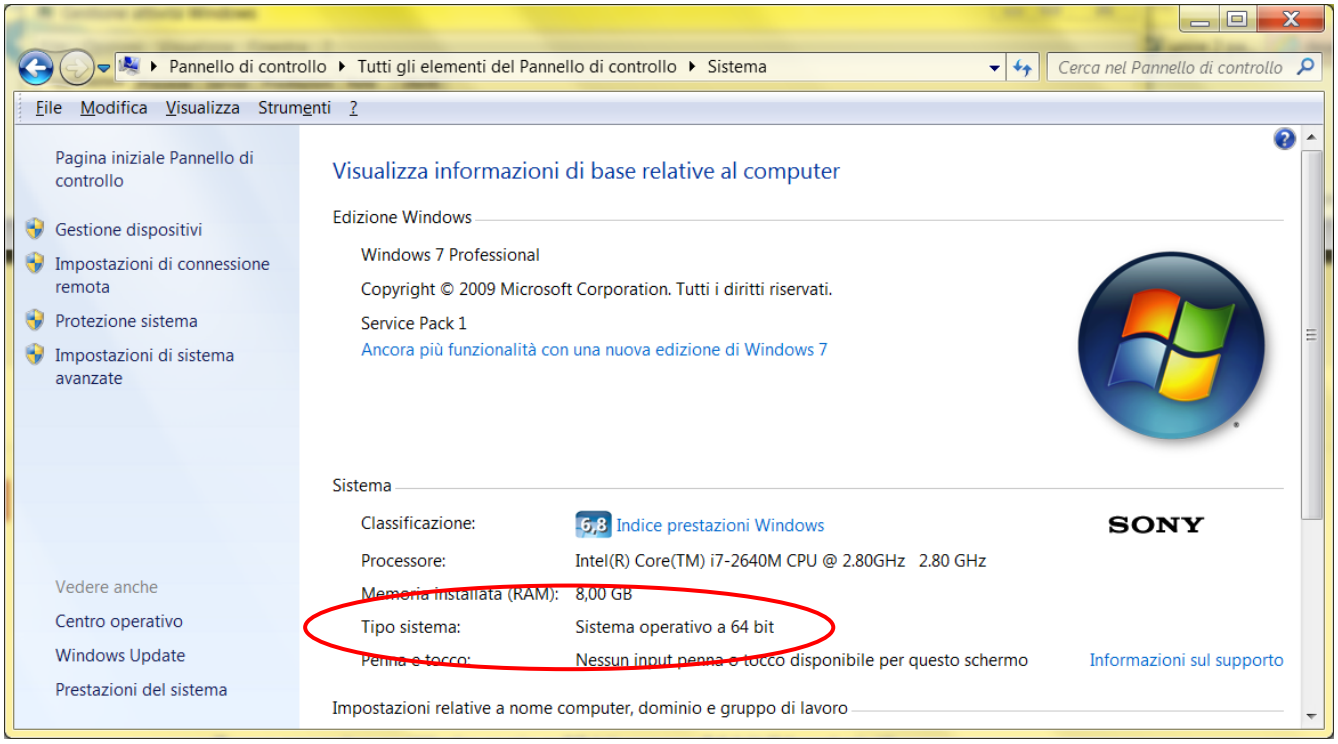


Figura 1

4.1.2 Windows XP

Se si dispone di Windows XP, esistono due metodi per determinare se è in esecuzione una versione a 32 bit o una versione a 64 bit. Se un metodo non funziona, provare l'altro metodo.

Metodo 1: Proprietà di sistema di visualizzazione nel Pannello di controllo

1. Fare clic su **Start** e scegliere **Esegui**.
2. Digitare **sysdm. Cpl** e quindi fare clic su **OK**.
3. Fare clic sulla scheda **Generale** . Il sistema operativo viene visualizzato come segue:
   - Per un sistema operativo a 64 bit, **Windows XP Professional x64 Edition versione <*year*="">** viene visualizzato in **sistema**.
   - Per una versione a 32 bit del sistema operativo, **Windows XP Professional versione <*Year*></*Year*>** viene visualizzato in **sistema**.

Nota <*Year*></*Year*> è un segnaposto per un anno.

Metodo 2: Visualizzare la finestra delle informazioni di sistema

1. Fare clic su **Start** e scegliere **Esegui**.
2. Digitare **winmsd. Exe** e quindi fare clic su **OK**.
3. Quando nel riquadro di spostamento viene selezionato **Risorse di sistema** , individuare **processore** in un **elemento** nel riquadro dei dettagli. Prendere nota del valore.
   - Se il valore indicato per **processore** inizia con **x86**, il computer è in esecuzione una versione a 32 bit di Windows.

- Se il valore indicato per **processore** inizia con **IA-64** o **AMD64**, il computer è in esecuzione una versione a 64 bit di Windows.

5 Microsoft Windows: Installazione di Cisco VPN Client

Per installare il Cisco VPN Client in ambiente Microsoft Windows, eseguire la seguente procedura:

1. Dopo aver effettuato il download del software Cisco VPN Client sul proprio computer, cliccare due volte sull'icona del file scaricato (**Errore. L'origine riferimento non è stata trovata.**).

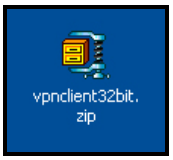


Figura 2

2. Si aprirà il programma di decompressione (ad es., WinZIP) all'interno del quale è necessario cliccare due volte sul file (Figura 3).

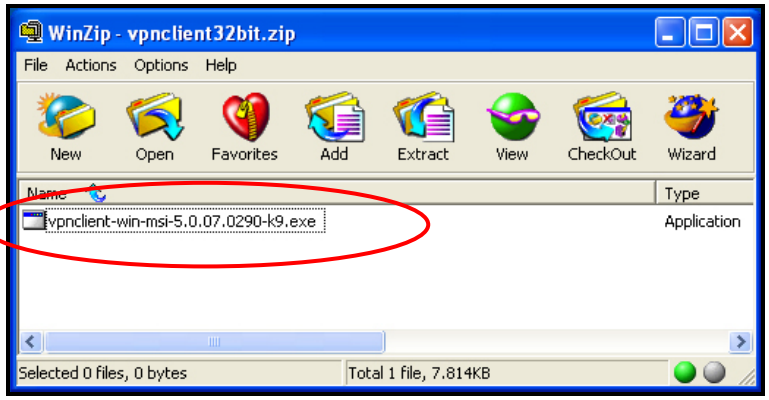


Figura 3

3. Cliccare su ***"Unzip"*** per procedere con l'estrazione dei file necessari per l'installazione (Figura 4).

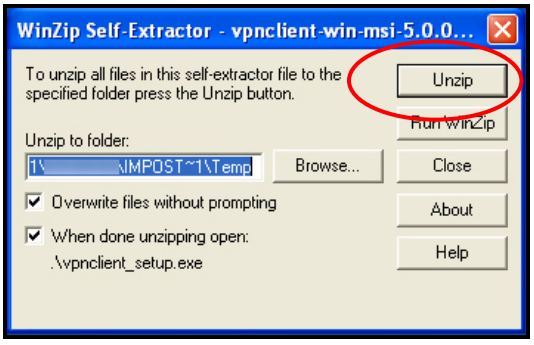


Figura 4

4. Al termine dell'estrazione dei file cliccare su ***"Ok"*** (Figura 5)**.**

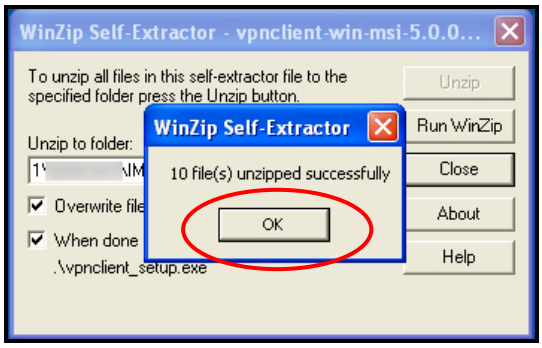


Figura 5

5. Selezionare la lingua per l'installazione e cliccare su "***OK"*** (Figura 6)**.**

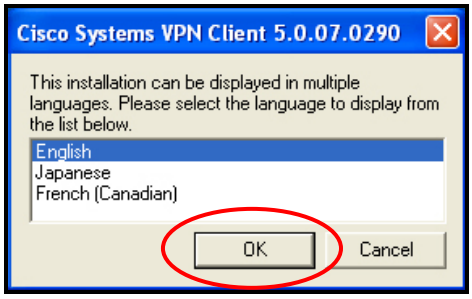


Figura 6

6. Comparirà la finestra di inizio installazione. Cliccare su **"Next"** (Figura 7)

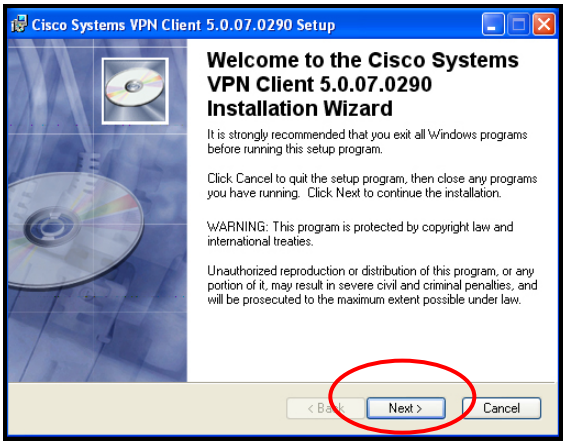


Figura 7

7. Apparirà il contratto di licenza per il quale è necessario selezionare la casella **"I accept the license agreement"** e cliccare su **"Next"** (Figura 8)

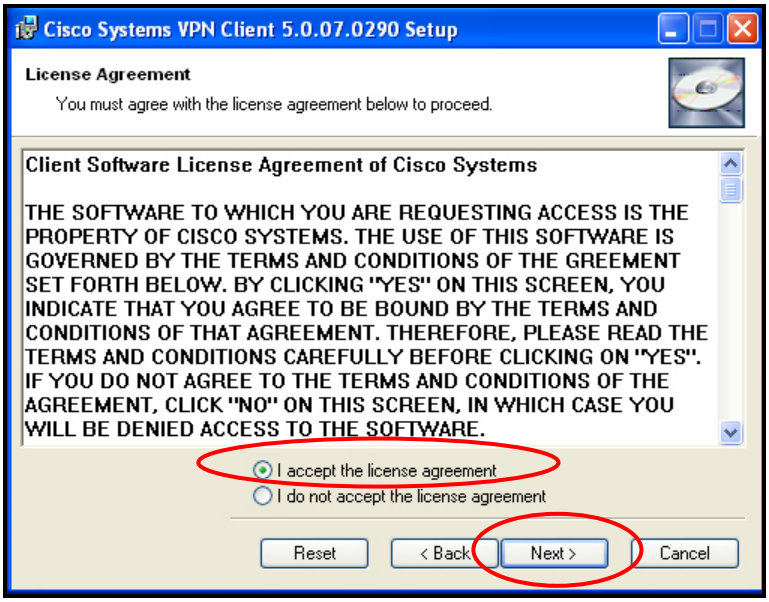


Figura 8

8. Verrà visualizzata la finestra di scelta del percorso di installazione del software. Scegliere **"Next"** per eseguire l'installazione nella cartella di destinazione predefinita (Figura 9)

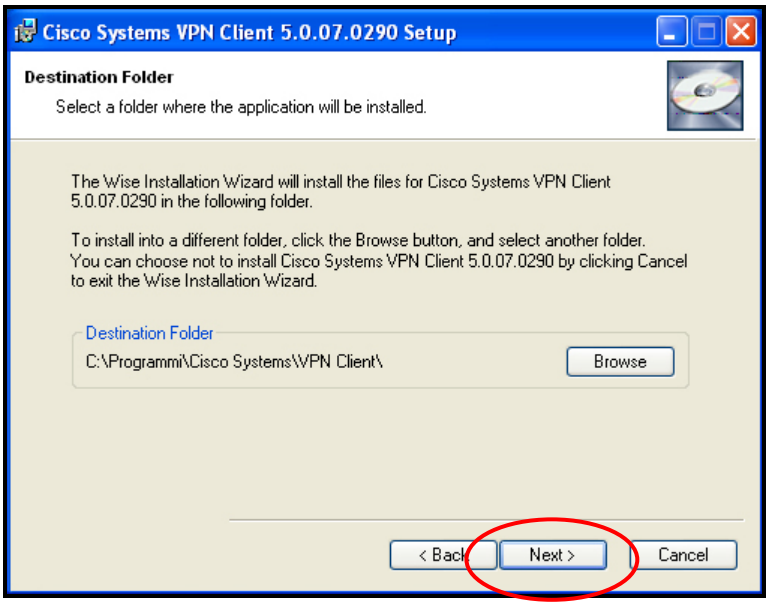


Figura 9

9. Per iniziare l'installazione scegliere **"Next"** (Figura 10)

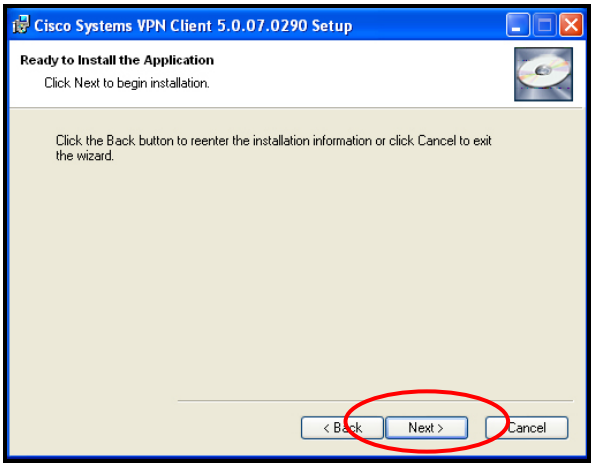


Figura 10

10. La procedura guidata è pronta per l'installazione. L'operazione potrebbe richiedere alcuni minuti. Nel frattempo verrà visualizzata la figura seguente.

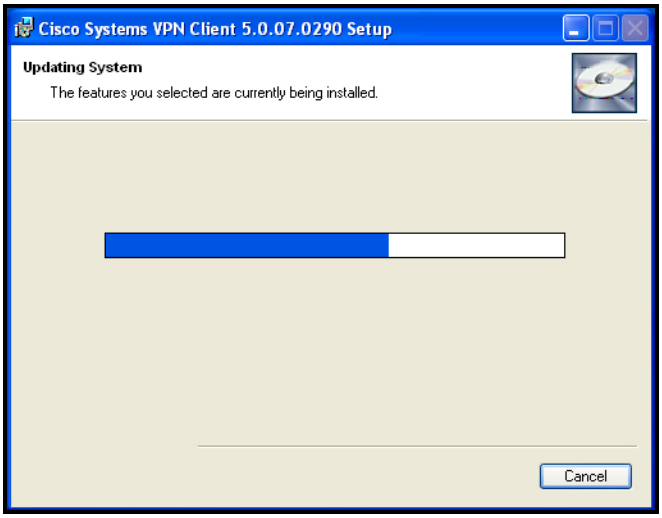


Figura 11

11. Al termine dell'installazione cliccare su **"Finish"** (Figura 12).

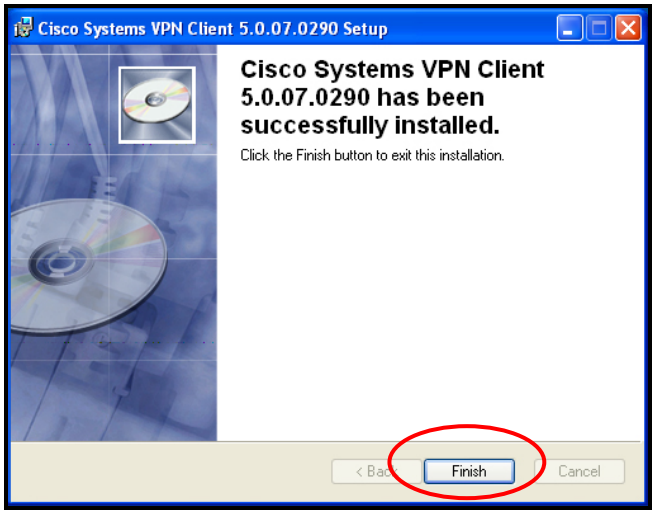


Figura 12

12. Il software è ora installato. Cliccare su **"Yes"** per riavviare il computer (Figura 13). È possibile riavviare manualmente il PC selezionando **Start – Arresta il sistema – Riavvia il sistema**

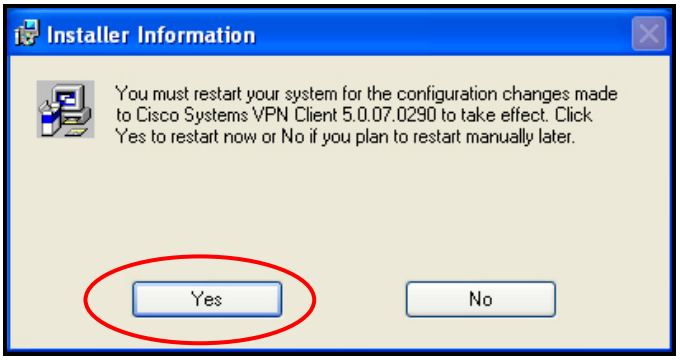


Figura 13

6 Microsoft Windows: Installazione di Cisco AnyConnect

Per installare il Cisco AnyConnect in ambiente Microsoft Windows, eseguire la seguente procedura:

4. Dopo aver effettuato il download del software Cisco VPN Client sul proprio computer, cliccare due volte sull'icona del file scaricato (Figura 14).

Figura 14

5. Si aprirà il programma di decompressione (ad es. WinZIP) all'interno del quale è necessario cliccare due volte sul file (Figura 15).

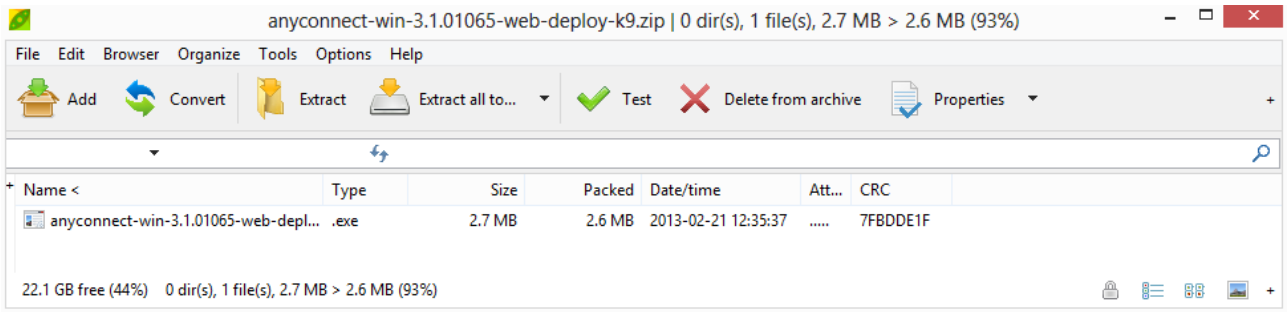
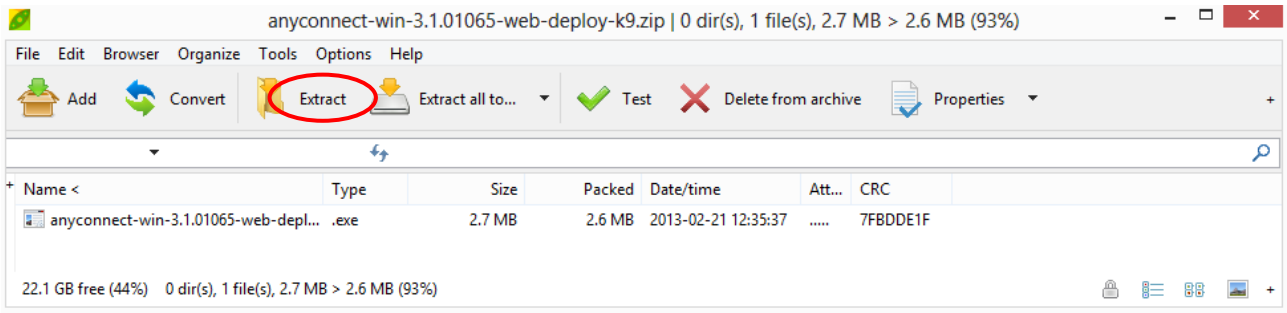


Figura 15

6. Cliccare su ***"Extract"*** per procedere con l'estrazione dei file necessari per l'installazione



7. Comparirà la finestra di inizio installazione. Cliccare su **"Next"**(Figura 16)

Figura 16

8. Apparirà il contratto di licenza per il quale è necessario selezionare la casella **"I accept the license agreement"** e cliccare su **"Next"** (Figura 17)

Figura 17

9. Per iniziare l'installazione scegliere **"Install"** (Figura 18)

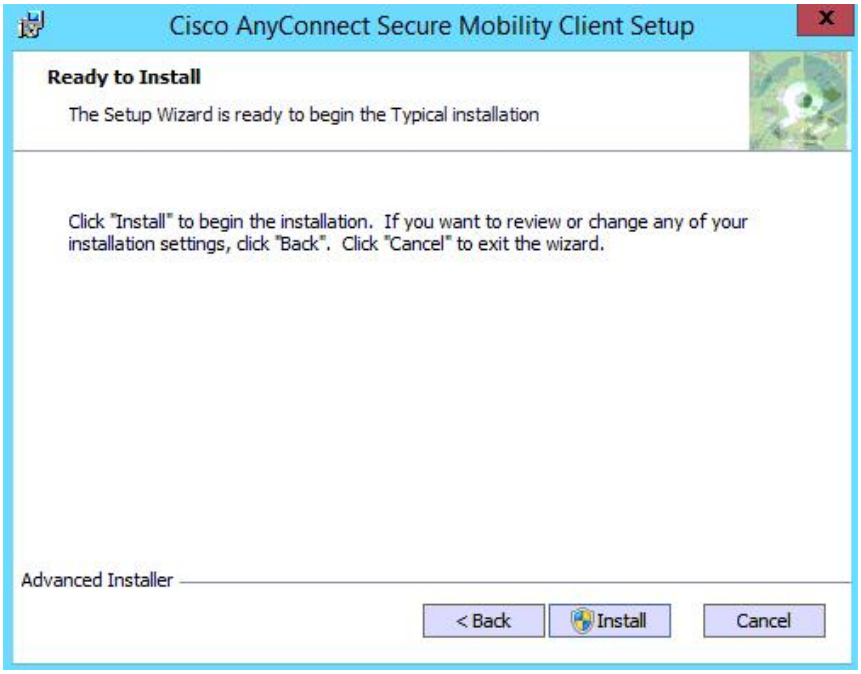


Figura 18

10. Al termine dell'installazione cliccare su **"Finish" (Figura 19)**

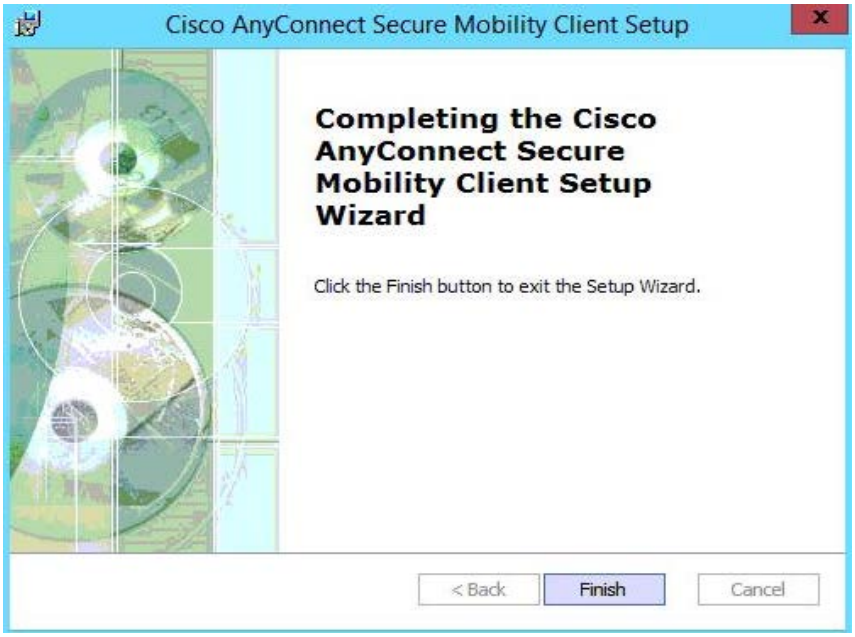


Figura 19

7 Microsoft Windows: Creazione profilo per il collegamento protetto al Centro Servizi Sanità Elettronica Regionale attraverso il Cisco VPN Client

Prima di poter realizzare un collegamento alla RUPAR-SPC - e di conseguenza poter accedere ai sistemi informatici che la Regione Puglia rende disponibile - è necessario creare un profilo per il collegamento in funzione della modalità di autenticazione – debole o forte - che si intende utilizzare.
Qualora si voglia predisporre il PC all'utilizzo di entrambe le modalità di autenticazione – debole e forte - è necessario generare 2 differenti profili.

7.1 Creazione profilo con credenziali deboli

Per creare il profilo per il collegamento protetto VPN al **Centro Servizi Sanità Elettronica Regionale** utilizzando le credenziali deboli, occorre eseguire i seguenti passi:

1. Eseguire l'applicazione Cisco VPN Client, cliccando su **Start -> Tutti i programmi -> Cisco Systems VPN Client - > VPN Client** (Figura 20 in Windows Vista/Seven e Figura 21 in Windows XP).

Nota:	Si consiglia di creare un collegamento sul desktop per avviare in maniera più agevole il software.

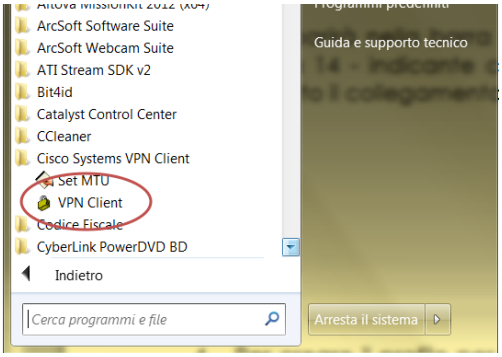


Figura 20

Figura 21

2. Apparirà la seguente immagine che indica che il caricamento dell'applicazione è in corso.

Figura 22

3. Comparirà - nella barra delle applicazioni di Windows o nella finestra delle icone nascoste - l'icona "Lucchetto aperto" - cerchiata in Figura 23 (Windows Vista/Seven) e Figura 24 (Windows XP) - indicante che l'applicazione Cisco VPN Client è stata avviata, ma non è stato attivato il collegamento protetto.

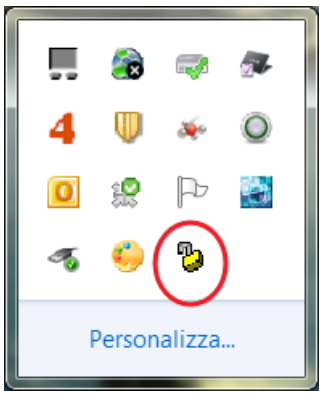


Figura 23

Figura 24

4. Per creare il profilo per il collegamento protetto, cliccare - all'interno dell'applicazione Cisco VPN Client - sul tasto **New**, posizionato in alto nella barra dei pulsanti (Figura 25).

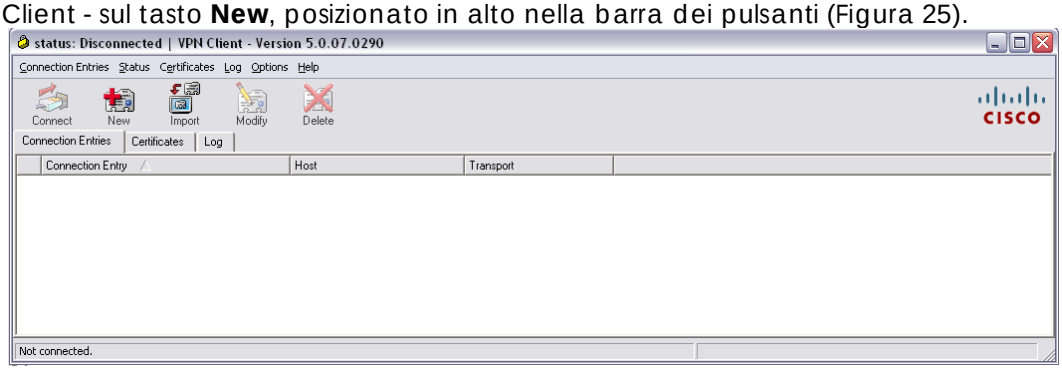


Figura 25

5. Digitare le seguenti informazioni nella finestra (Figura 26) che si aprirà:

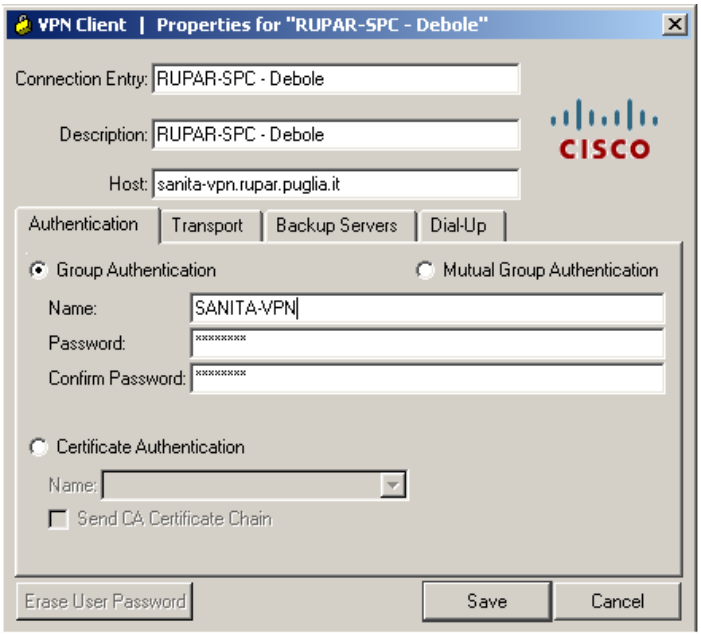


Figura 26

dove:

a) Connection Entry: **RUPAR-SPC – Debole**
b) Description: **RUPAR-SPC – Debole**
c) Host: **sanita-vpn.rupar.puglia.it**
d) Nella sezione **Authentication**:
   1. Selezionare il bottone **Group Authentication**
   2. Nel campo **Name** digitare **SANITA-VPN**[1]
   3. Nel campo **Password** digitare la prima password – associata alla etichetta "Pwd Gruppo" - specificata nella lettera di rilascio delle credenziali
   4. Nel campo **Confirm Password** digitare nuovamente la medesima password

7.2 Creazione profilo con credenziali forti (con CNS - Carta Nazionale dei Servizi)

Per creare il profilo per il collegamento protetto VPN al **Centro Servizi Sanità Elettronica Regionale** utilizzando le credenziali forti, è necessario che l'utente disponga di Carta Nazionale dei Servizi (CNS) e relativo lettore di smartcard e che abbia preventivamente installato il software di riconoscimento del dispositivo (p.es. Bit4id)

In questo caso occorre eseguire i seguenti passi:

1. Inserire la CNS nel lettore di smartcard

2. Eseguire l'applicazione Cisco VPN Client, cliccando su **Start -> Tutti i programmi -> Cisco Systems VPN Client - > VPN Client** (Figura 27 in Windows Vista/Seven e Figura 28 in Windows XP).

[1] Tutti i caratteri **devono** essere MAIUSCOLO

Nota:	Si consiglia di creare un collegamento sul desktop per avviare in maniera più agevole il software.

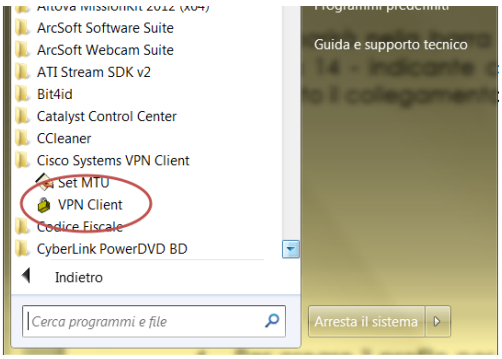


Figura 27

Figura 28

3. Apparirà la seguente immagine che indica che il caricamento dell'applicazione è in corso.

Figura 29

4. Comparirà - nella barra delle applicazioni di Windows o nella finestra delle icone nascoste - l'icona  "Lucchetto aperto" - cerchiata in Figura 30 (Windows Vista/Seven) e Figura 31 (Windows XP) - indicante che l'applicazione Cisco VPN Client è stata avviata, ma non è stato attivato il collegamento protetto.

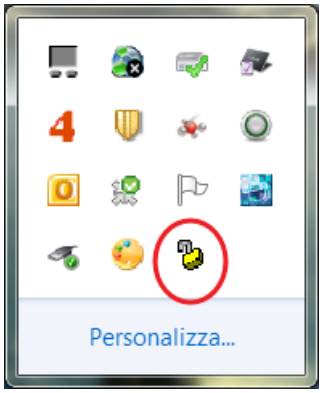


Figura 30

Figura 31

Per poter procedere alla creazione del profilo per il collegamento protetto con credenziali forti è necessario installare sul proprio computer i seguenti certificati:

- *Certificax\to Actalis per autenticazione CNS;*
- *Certificato Actalis per firma digitale CNS;*
- *Certificato Actalis_Server_Authentication_CA;*
- Certificato X.509_ca-certificate
- Certificato Actalis Authentication CA G2

Questi certificati possono essere scaricati dal Portale Regionale della Salute (http://www.sanita.puglia.it), nel percorso "**Sistemi Informativi**", "**RUPAR-SPC**", "**Materiali di riferimento**" e "**Certificati digitali**".

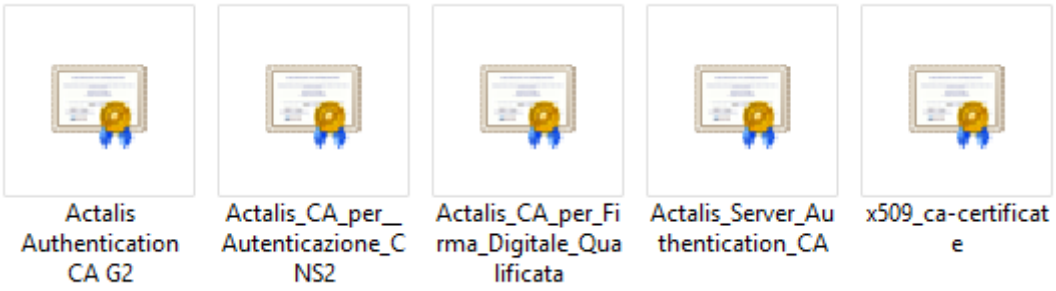


Figura 32

I certificati hanno lo scopo di validare l'identità digitale memorizzata all'interno della CNS, ovvero garantire che i certificati a bordo della CNS siano validi.

Attenzione: Di seguito è mostrata la procedura per installare un certificato (l'operazione deve essere ripetuta per tutti i certificati scaricati dal **Portale Regionale della Salute** (http://www.sanita.puglia.it), nel percorso "**Sistemi Informativi**", "**RUPAR-SPC**", "**Materiali di riferimento**" e "**Certificati digitali**" dal passo 4) al passo 12).

5. Inserire nel lettore di smartcard la propria CNS;

6. Avviare l'applicazione Cisco VPN Client e posizionarsi nella sezione "**Certificates**" (Figura 33).

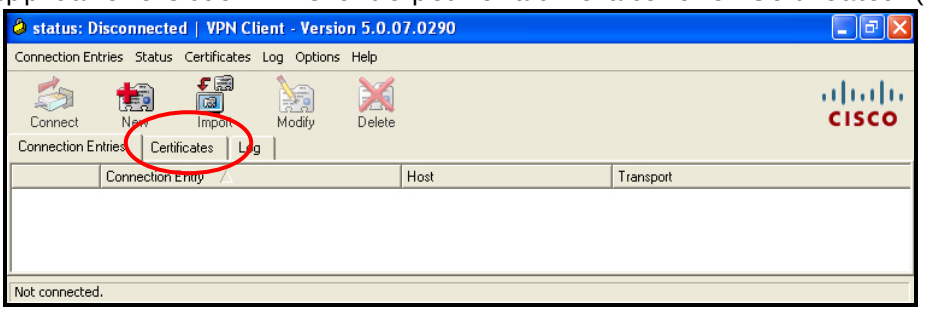


Figura 33

7. Cliccare sul pulsante "**Import**" (Figura 34).

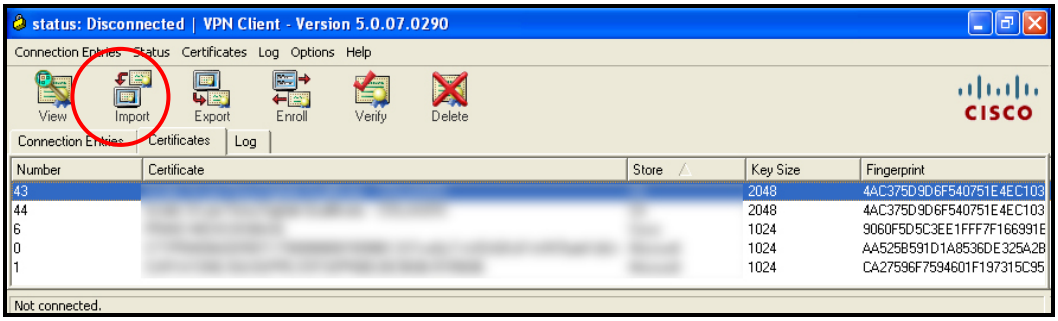


Figura 34

8. Selezionare "**Import from file**" e successivamente cliccare "**Browse**" (Figura 35).

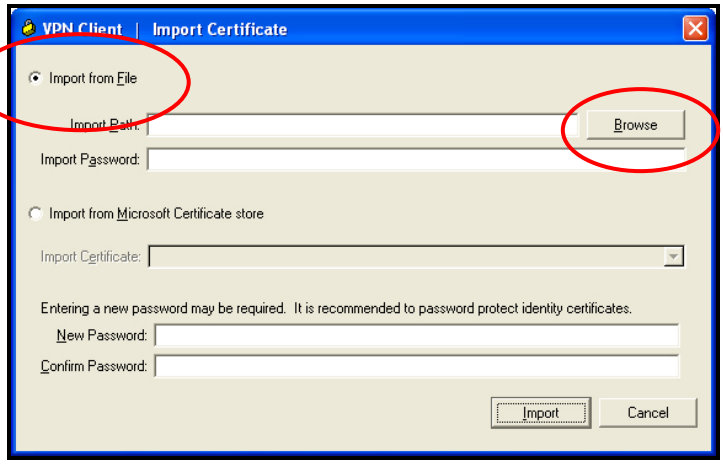


Figura 35

9. Selezionare il certificato che si è precedentemente scaricato. Successivamente cliccare su **"Apri"** ().

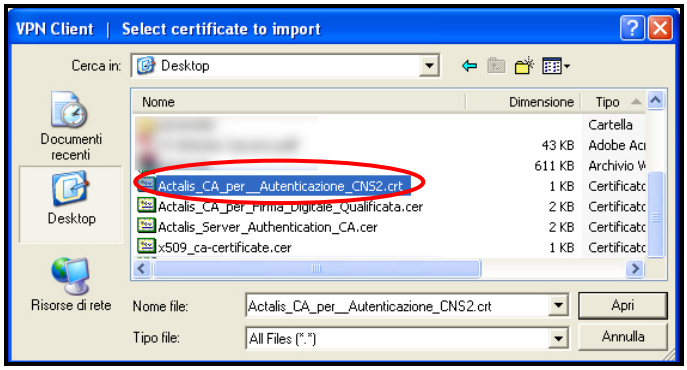


Figura 36

10. Dopo aver selezionato il certificato Cliccare su "**Import**", come mostrato in Figura 23.

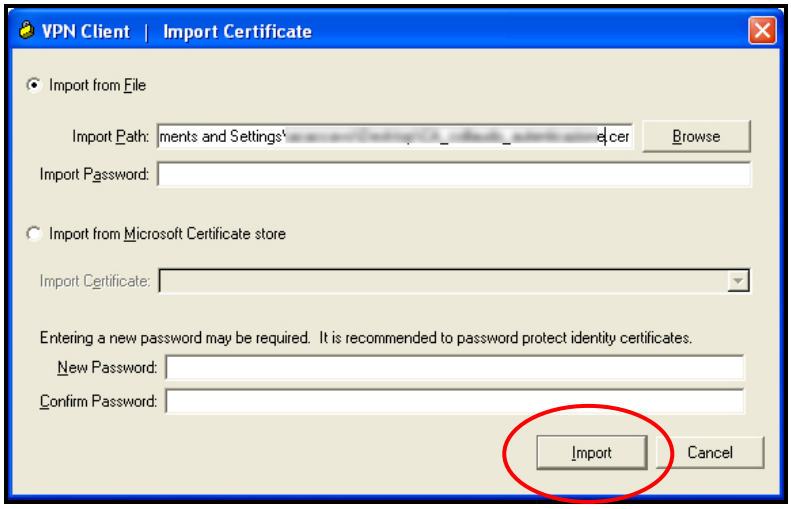


Figura 37

11. Il seguente messaggio confermerà la corretta installazione del certificato. Cliccare su **"OK"** per terminare l'importazione del certificato.

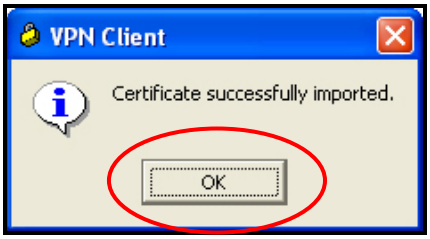


Figura 38

12. Cliccare due volte sul certificato e successivamente su "Apri", come mostrato in Figura 25.

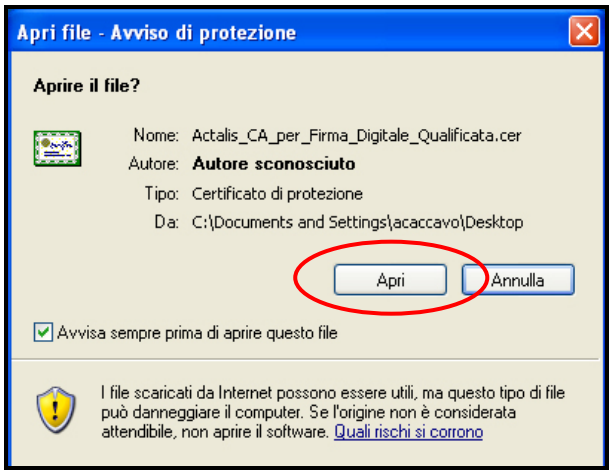


Figura 39

13. Cliccare su "Installa certificato..." e seguire le istruzioni mostrate.

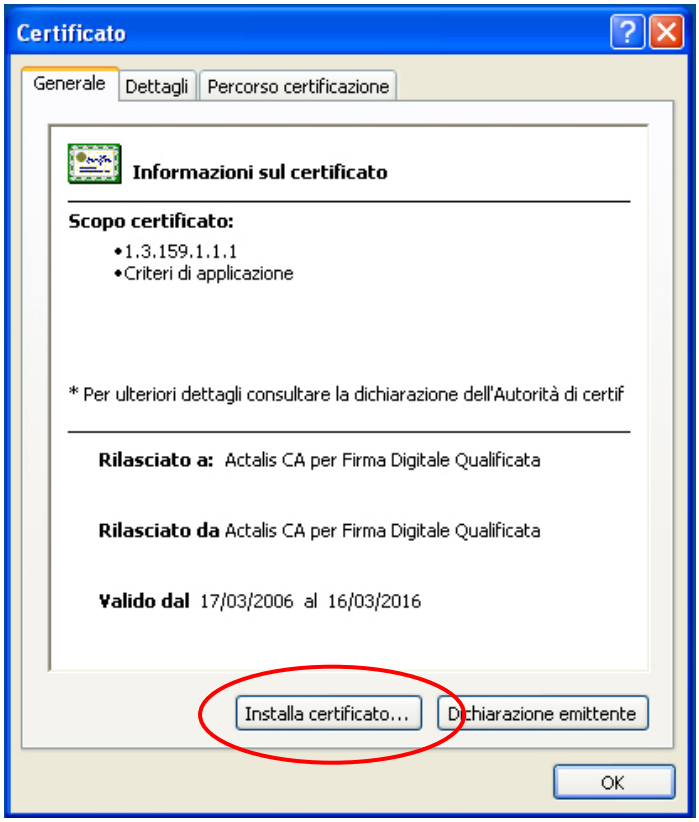


Figura 40

14. Cliccare nella barra delle applicazioni di Windows l'icona cerchiata in Figura 41

Figura 41

15. Ripetere tutti i passi a partire dal passo 4) per tutti i certificati precedentemente indicati.

16. Creare il collegamento protetto cliccando - all'interno dell'applicazione Cisco VPN Client - sul tasto **New**, posizionato in alto nella barra dei pulsanti (Figura 42).

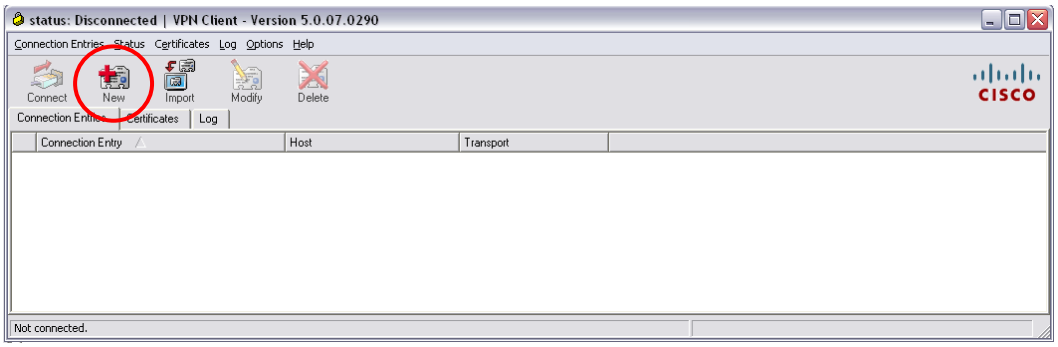


Figura 42

17. digitare le seguenti informazioni nella finestra che si aprirà:
    a) Connection Entry: **RUPAR-SPC – CNS**
    b) Description: **RUPAR-SPC – CNS**
    c) Host: **sanita-vpn.rupar.puglia.it**
    d) nella sezione **Authentication:**
        1. selezionare il bottone **Certificate Authentication**
        2. e selezionare nel menù a tendina "**Name**", il certificato di autenticazione (è necessario aver inserito la propria CNS altrimenti il certificato non comparirà).

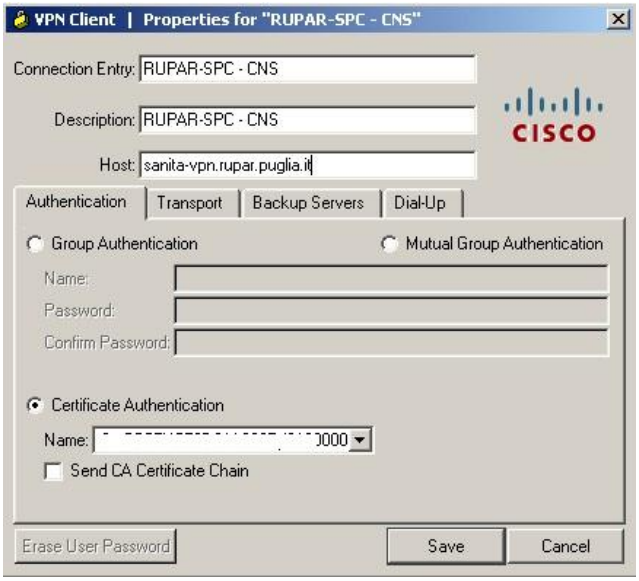


Figura 43

18. Lasciare inalterate tutte le altre voci delle altre sezioni e cliccare sul pulsante "Save", per salvare la configurazione.

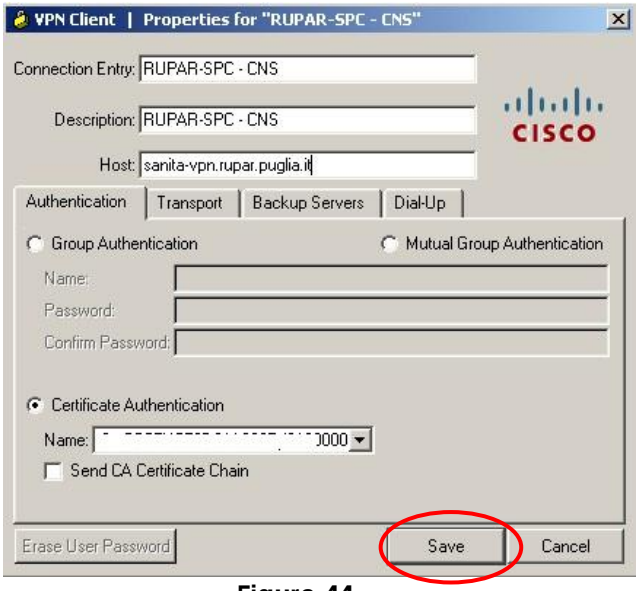

VPN Client | Properties for "RUPAR-SPC - CNS"
Connection Entry: RUPAR-SPC - CNS
Description: RUPAR-SPC - CNS
Host: sanita-vpn.rupar.puglia.it
CISCO
Authentication
Transport
Backup Servers
Dial-Up
Group Authentication
Mutual Group Authentication
Name:
Password:
Confirm Password:
Certificate Authentication
Name:
Send CA Certificate Chain
Erase User Password
Save
Cancel

Figura 44

8 Microsoft Windows: Creazione profilo per il collegamento protetto al Centro Servizi Sanità Elettronica Regionale attraverso il Cisco AnyConnect

8.1 Creazione profilo con credenziali deboli

Per creare il profilo per il collegamento protetto VPN al **Centro Servizi Sanità Elettronica Regionale** utilizzando le credenziali deboli, occorre eseguire i seguenti passi:

Nota: Si consiglia di creare un collegamento sul desktop con il programma AnyConnect per avviare in maniera più agevole il software.

1. Eseguire l'applicazione Cisco AnyConnect, cliccando su **Start -> Tutti i programmi -> Cisco - > Cisco AnyConnect Secure Mobility (Figura 45)**

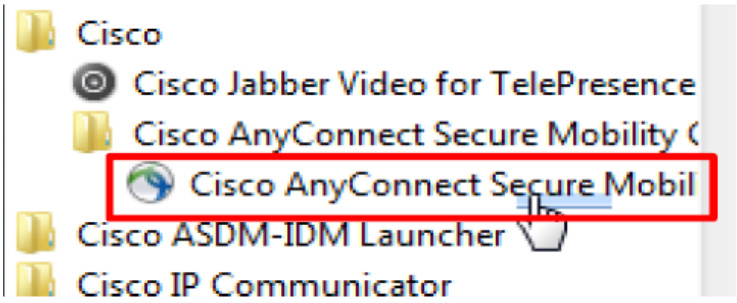


Figura 45

2. Comparirà - nella barra delle applicazioni di Windows o nella finestra delle icone nascoste - l'icona  indicante che l'applicazione Cisco AnyConnect è stata avviata, ma non è stato attivato il collegamento protetto.

3. Una volta eseguito, inserire all'interno del campo "VPN:", il seguente valore **sanita-vpn.rupar.puglia.it** e cliccare su **Connect (Figura 46)**

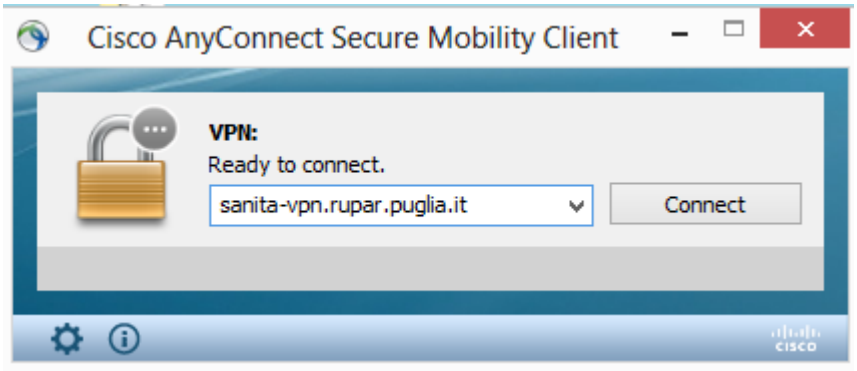


Figura 46

8.2 Creazione profilo con credenziali forti

Per creare il profilo per il collegamento protetto VPN al **Centro Servizi Sanità Elettronica Regionale** utilizzando le credenziali forti, è necessario che l'utente disponga di Carta Nazionale dei Servizi (CNS) e relativo lettore di smartcard e che abbia preventivamente installato il software di riconoscimento del dispositivo (p.es. Bit4id).

Inoltre deve eseguire il programma Cisco AnyConnect come amministratore (Figura 47 e 48).

Pertanto

1. cliccare su **Start -> Tutti i programmi -> Cisco - > Cisco AnyConnect Secure Mobility** e selezionare con il tasto destro la voce "Proprietà" (Figura 47)

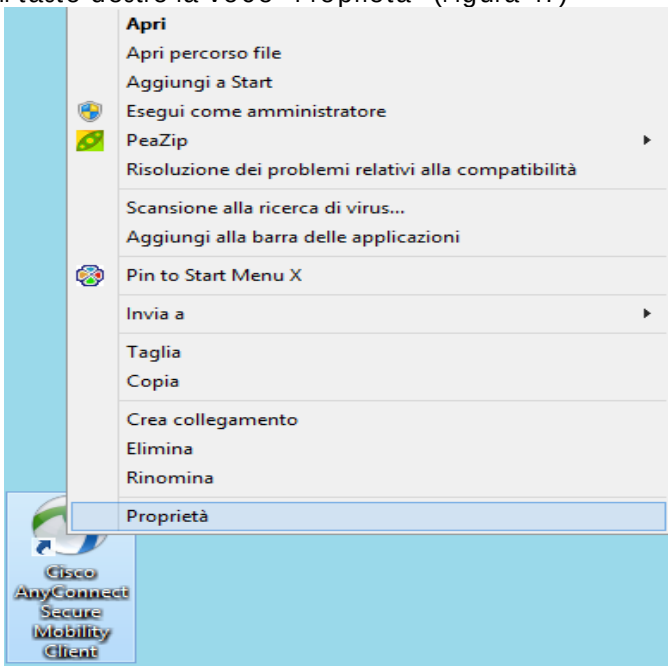


Figura 47

2. Successivamente dalla scheda "Compatibilità" spuntare la voce "Esegui come amministratore" e confermare da "OK"(Figura 48)

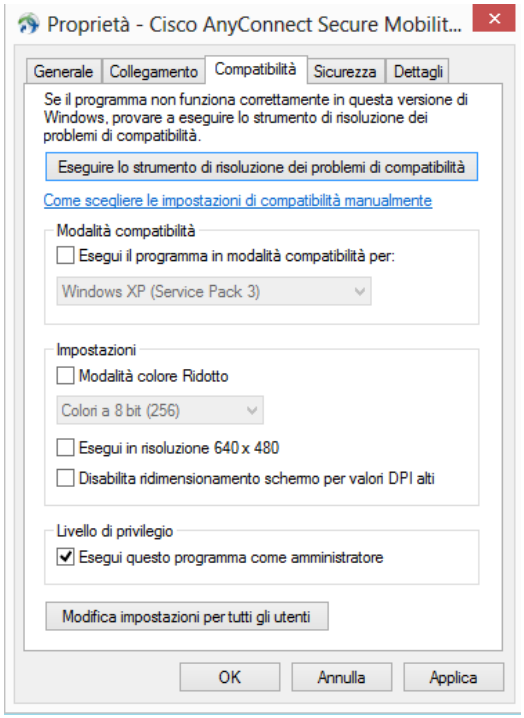


Figura 48

3. Eseguire l'applicazione Cisco AnyConnect, cliccando su **Start -> Tutti i programmi -> Cisco - > Cisco AnyConnect Secure Mobility (Figura 49)**

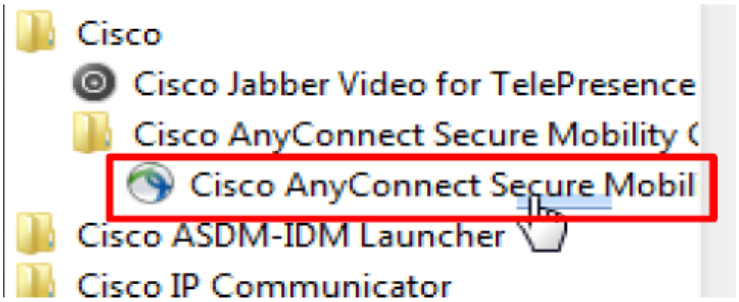


Figura 49

4. Comparirà - nella barra delle applicazioni di Windows o nella finestra delle icone nascoste - l'icona indicante che l'applicazione Cisco AnyConnect è stata avviata, ma non è stato attivato il collegamento protetto.

5. Inserire all'interno del campo "VPN:", il seguente valore **vpn.rmmg.rupar.puglia.it (Figura 50)**

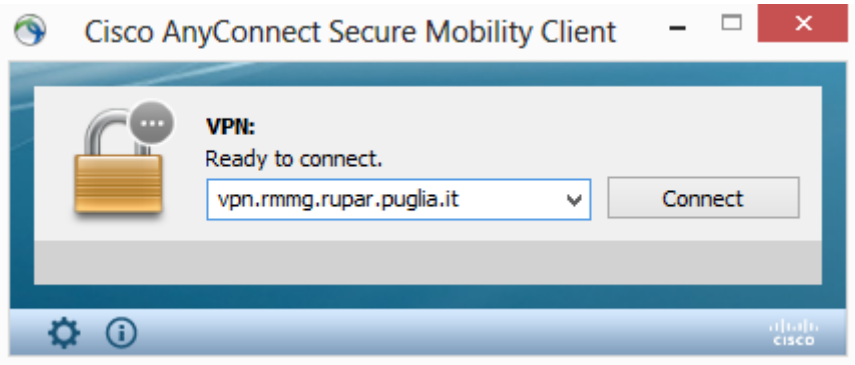


Figura 50

9 Microsoft Windows: Accettazione del Regolamento di utilizzo della RUPAR-SPC

Attenzione:

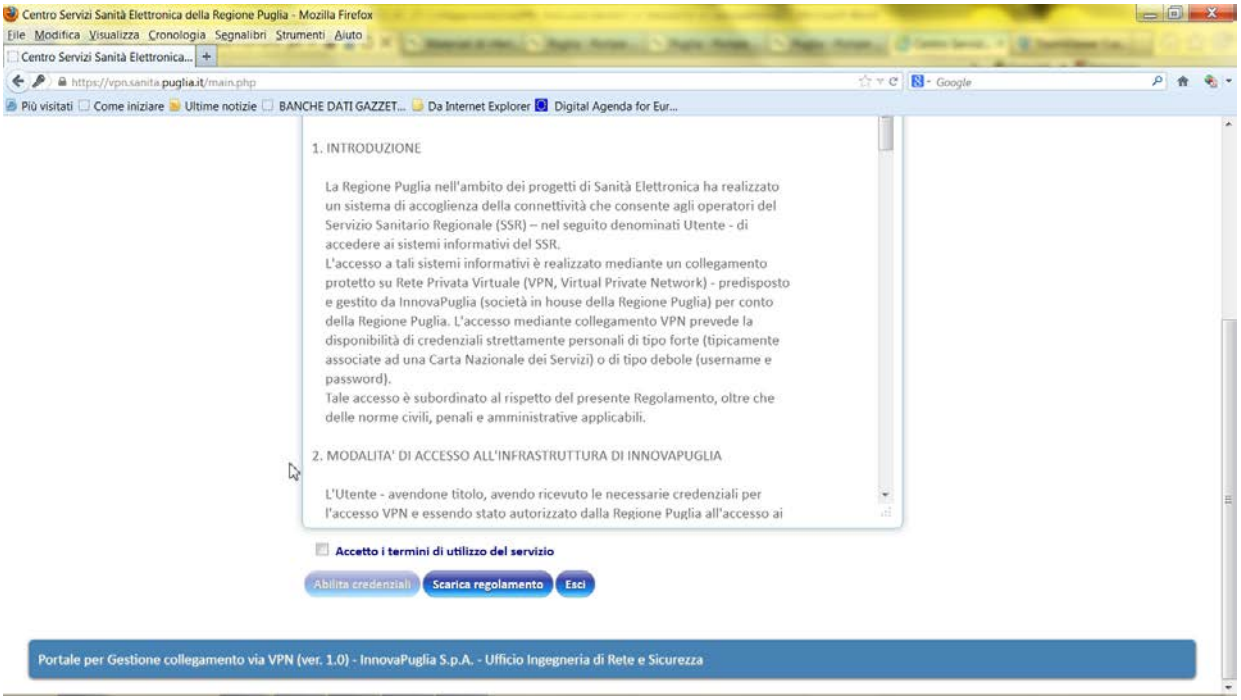
a) la procedura deve essere effettuata sempre prima di accedere al sistema informativo di interesse.

b) La procedura è indipendente – cioè deve essere eseguita – dal tipo di ambiente (Microsoft Windows, Apple iOS, Android) che si sta utilizzando

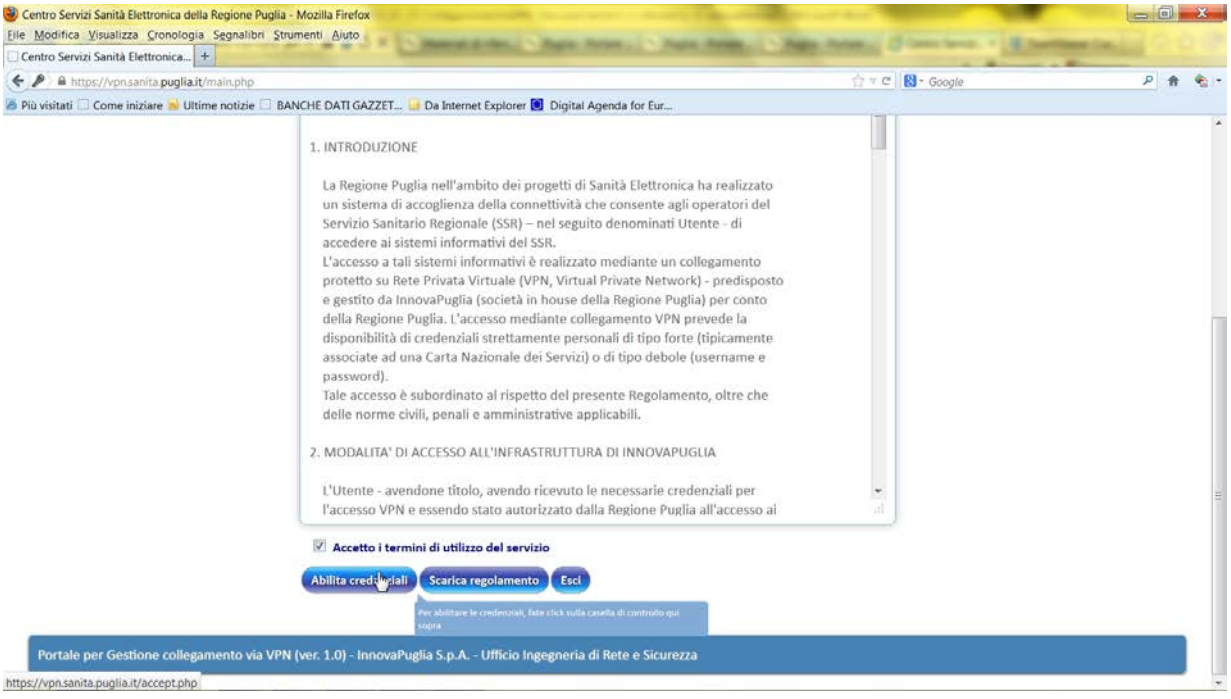
Prima di eseguire il primo collegamento alla RUPAR-SPC è necessario procedere con l'accettazione del Regolamento di utilizzo della RUPAR-SPC.
Eseguire la seguente procedura:

1. avviare il browser Internet e digitare la URL https://vpn.sanita.puglia.it

2. digitare le proprie credenziali di accesso rappresentate dal proprio **Codice fiscale** e dalla **password** scritta sulla comunicazione ricevuta
3. cliccare sul pulsante "**Login"**



4. selezionare la casella per dichiarare di accettare il **Regolamento di utilizzo della RUPAR-SPC** e cliccare sul bottone "**Abilita credenziali**"



10 Microsoft Windows: Avviamento del collegamento protetto al Centro Servizi Sanità Elettronica Regionale attraverso il Cisco VPN Client

Attenzione: la seguente procedura deve essere effettuata sempre prima di accedere al sistema informativo di interesse.

Per avviare il collegamento protetto con il Centro Servizi Sanità Elettronica Regionale, eseguire la seguente procedura:

5. avviare il software Cisco VPN Client
6. selezionare il profilo di collegamento di interesse
7. cliccare sul pulsante *"**Connect**"*

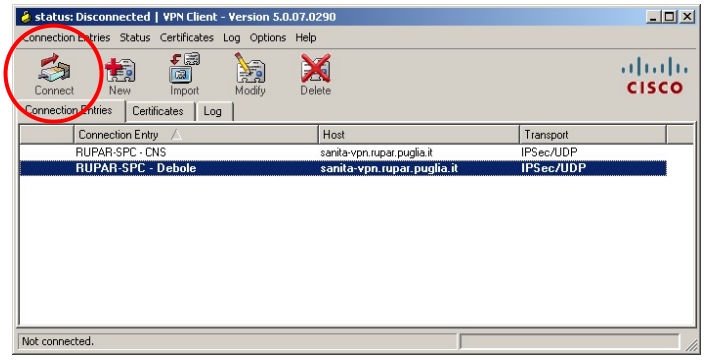


Figura 51

8. partirà la richiesta di collegamento selezionata e, dopo qualche istante, saranno richieste informazioni differenziate a secondo che si faccia uso di credenziali forti o deboli.

    a. nel caso il profilo di connessione sia stato configurato per l'utilizzo di **credenziali forti (CNS)**
        i. nel campo **PIN** digitare il **codice Pin della CNS** per identificare univocamente l'operatore che sta richiedendo l'accesso al Centro Servizi Sanità Elettronica Regionale (Figura).

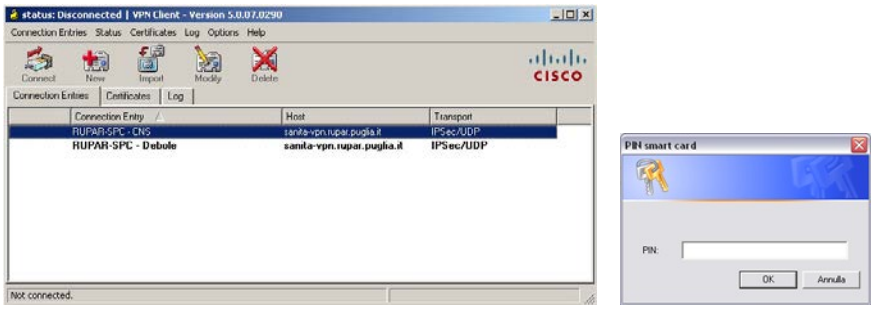


Figura 52

b. nel caso il profilo di connessione sia stato configurato per l'utilizzo di **credenziali deboli (Username e password)** (Figura) :
   i. nel campo **Username** digitare il proprio **codice fiscale**
   ii. nel campo **Password** digitare la seconda password – associata alla etichetta "Pwd Utente" - specificata nella lettera di rilascio delle credenziali

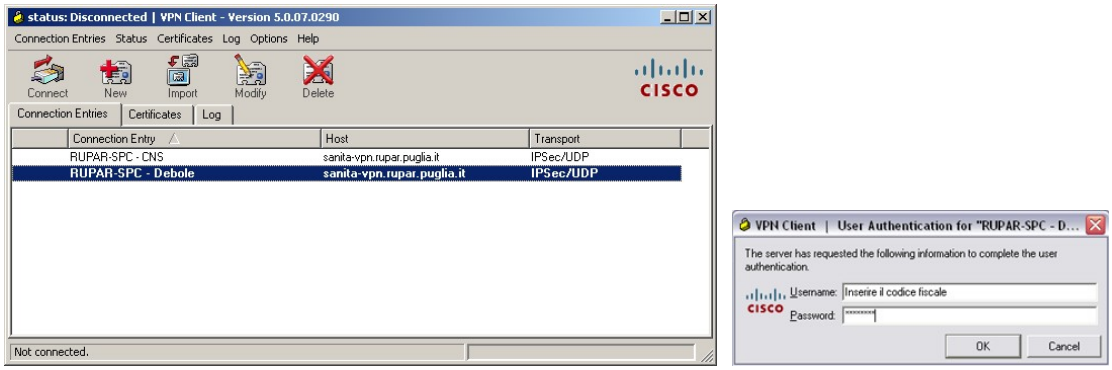


Figura 53

9. Inseriti tali valori, sarà necessario attendere qualche istante prima di essere effettivamente connessi all'indirizzo selezionato.

10. Nella barra delle applicazioni di Windows o nella finestra delle icone nascoste, comparirà l'icona (“Lucchetto chiuso”) - cerchiata in Figura - segno dell'avvenuto collegamento al Centro Servizi Sanità Elettronica Regionale.

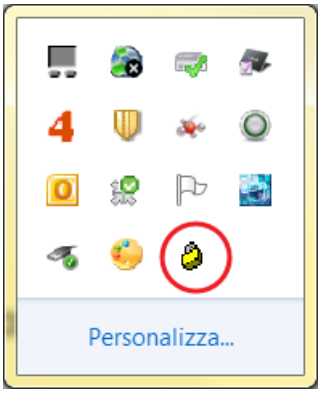


Figura 54

Se la connessione protetta al Centro Servizi Sanità Elettronica Regionale non risulta attiva, sarà visualizzata - nella barra delle applicazioni del computer o nella finestra delle icone nascoste - l'icona “Lucchetto aperto” .

Per ripristinare il collegamento protetto, è necessario cliccare due volte sulla relativa icona e, successivamente, cliccare sul pulsante “**Connect”**, come descritto precedentemente.

11 Microsoft Windows: Avviamento del collegamento protetto al Centro Servizi Sanità Elettronica Regionale attraverso il Cisco AnyConnect

Attenzione: la seguente procedura deve essere effettuata sempre prima di accedere al sistema informativo di interesse.

Per avviare il collegamento protetto con il Centro Servizi Sanità Elettronica Regionale, eseguire la seguente procedura:

1. avviare il software Cisco AnyConnect
2. cliccare sul pulsante "***Connect"***
3. partirà la richiesta di collegamento selezionata e, dopo qualche istante, saranno richieste informazioni differenziate a secondo che si faccia uso di credenziali forti o deboli:

    a. nel caso il profilo di connessione sia stato configurato per l'utilizzo di **credenziali forti (CNS)**

4. Apparirà una finestra per inserire il pin della smartcard (Figura 55)

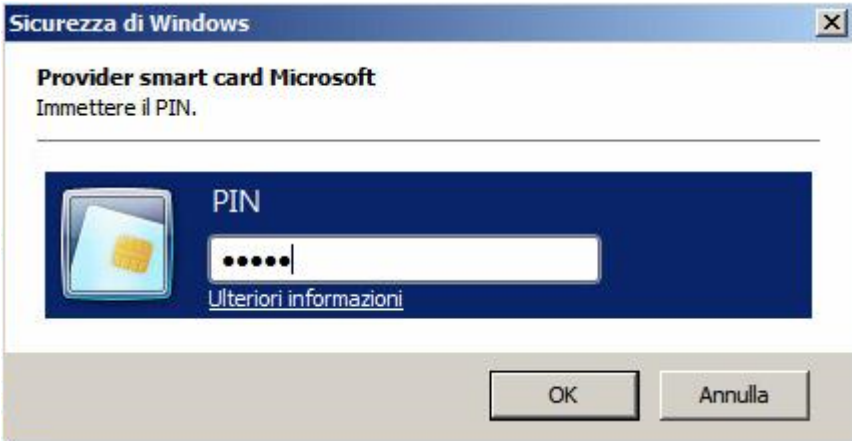


Figura 55

5. Apparirà un popup e dal menù a tendina, selezionare "**Rete dei Medici**"(Figura 56)

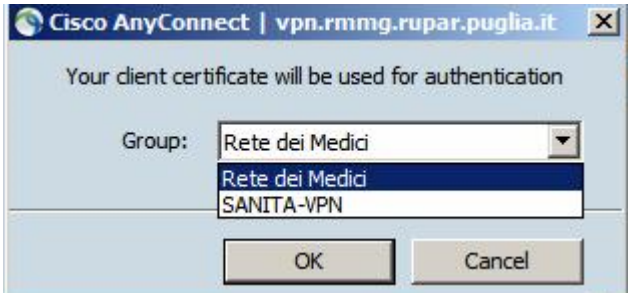


Figura 56

6. Al termine della verifica del pin con esito positivo, verrà instaurata la VPN-SSL (Figura 57)

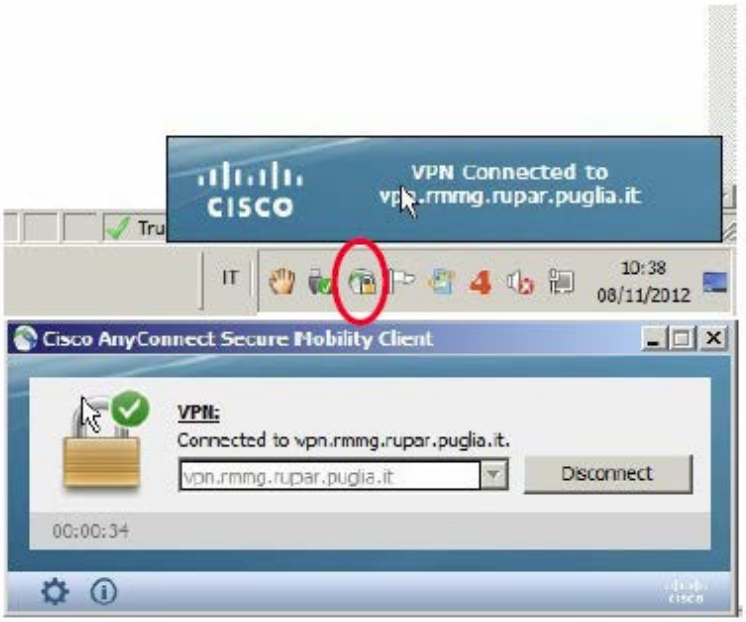
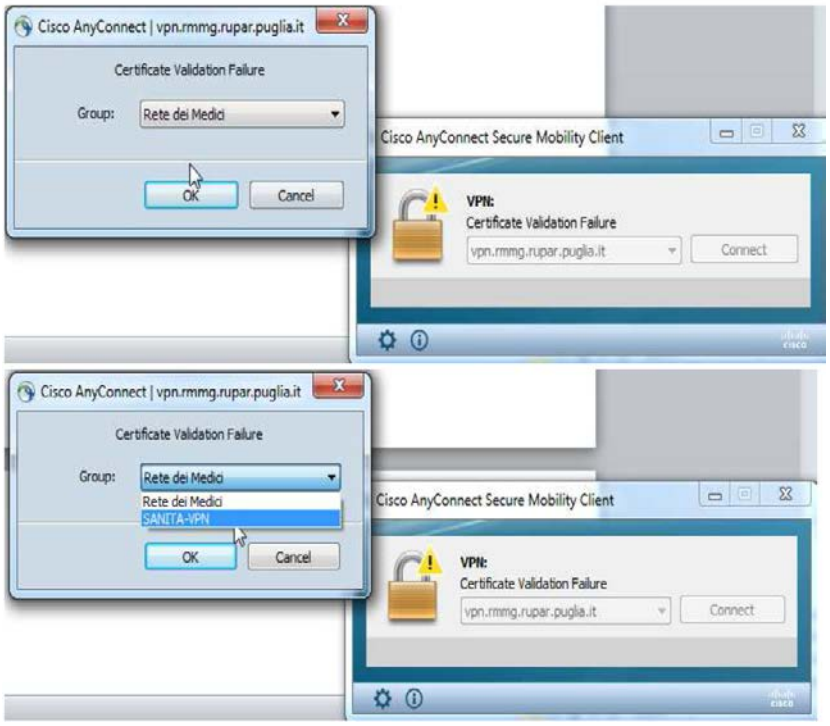


Figura 57

b. nel caso il profilo di connessione sia stato configurato per l'utilizzo di **credenziali deboli (username e password)**

4. Apparirà un popup e dal menù a tendina, selezionare "SANITA-VPN"



5. A questo punto, bisogna inserire le credenziali di accesso fornite

6. Al termine della verifica dei dati inseriti, verrà instaurata la VPN-SSL (Figura 58)

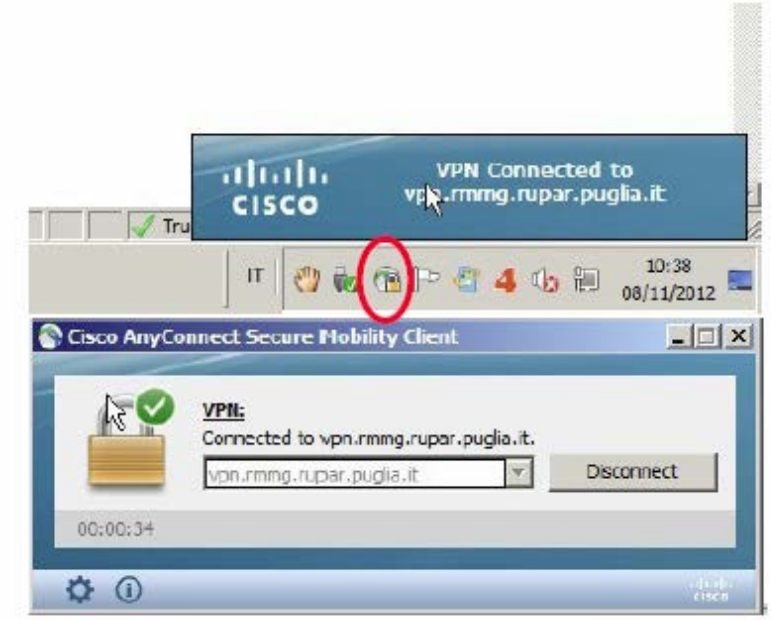

VPN Connected to
vpn.rmmg.rupar.puglia.it
IT
10:38
08/11/2012
Cisco AnyConnect Secure Mobility Client
VPN:
Connected to vpn.rmmg.rupar.puglia.it.
vpn.rmmg.rupar.puglia.it
Disconnect
00:00:34

Figura 58

12 Microsoft Windows: Conclusione del collegamento protetto al Centro Servizi Sanità Elettronica Regionale attraverso il Cisco VPN Client

Nel caso si renda necessario terminare il collegamento protetto (al termine della giornata lavorativa o per momentanea assenza dal computer), eseguire la seguente procedura:

- Cliccare due volte nella barra delle applicazioni sull'icona di Cisco VPN Client e successivamente cliccare sul pulsante **Disconnect** (Figura).

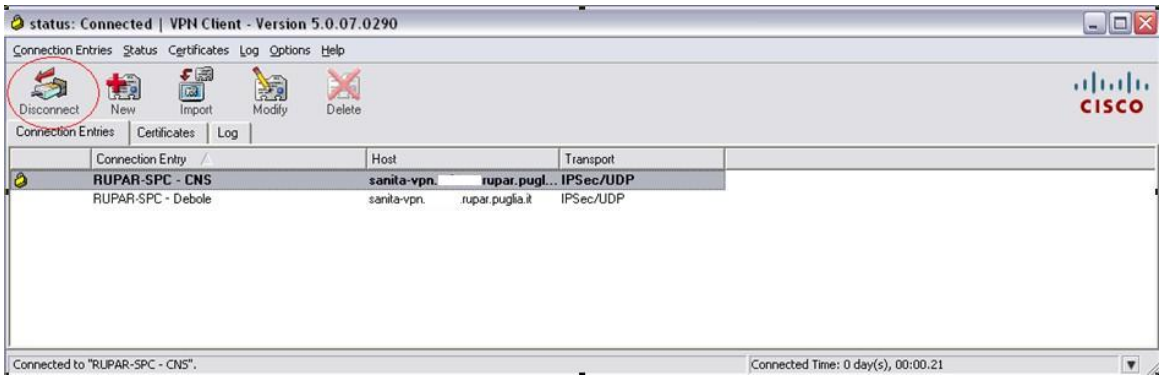


Figura 59

In entrambi i casi l'icona (“Lucchetto aperto”) - cerchiata in Figura - mostrerà che non è più attivo il collegamento protetto.

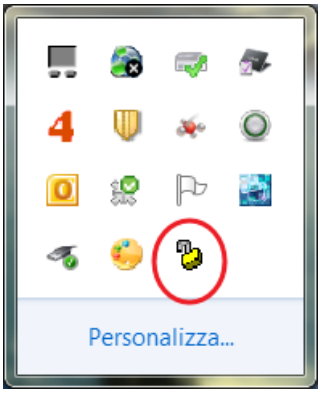


Figura 60

13 Microsoft Windows: Conclusione del collegamento protetto al Centro Servizi Sanità Elettronica Regionale attraverso il Cisco AnyConnect

Nel caso si renda necessario terminare il collegamento protetto (al termine della giornata lavorativa o per momentanea assenza dal computer), eseguire la seguente procedura:

- Cliccare due volte nella barra delle applicazioni sull'icona di Cisco VPN Client e successivamente cliccare sul pulsante **Disconnect**
- In entrambi i casi l'icona cerchiata in Figura 61 mostrerà che non è più attivo il collegamento protetto.

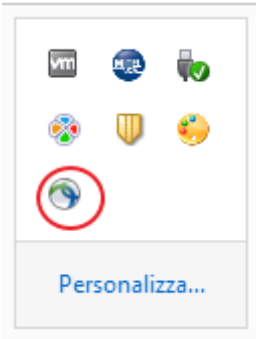


Figura 61

14 Apple - Connessione mediante tablet e smartphone

È possibile collegarsi in maniera protetta alla RUPAR-SPC - e per mezzo di essa accedere ai sistemi informativi sanitari su di essa resi disponibili - anche mediante tablet e smartphone della Apple.

Per poter realizzare il collegamento alla RUPAR-SPC via VPN occorre configurare il dispositivo nel seguente modo:

a) Selezionare la voce **Impostazione**

Figura 62

b) Sotto la voce **Generale**, selezionare **VPN:**

Figura 63

c) Selezionare "**Aggiungi config. VPN**"

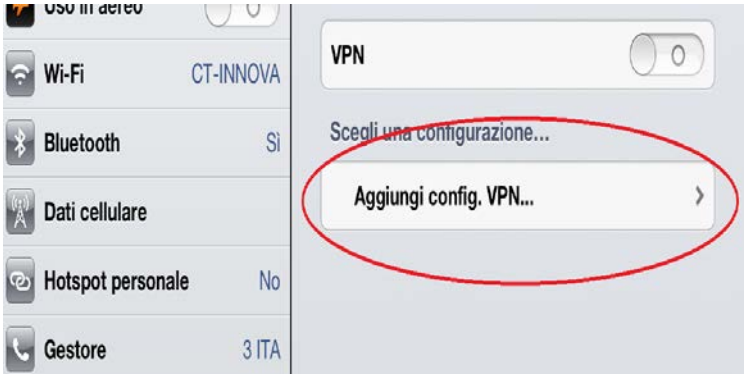


Figura 64

d) Selezionare la configurazione "**IPSec**"

Figura 65

e) Completare i campi secondo le informazioni contenute all'interno della lettera ricevuta:

Figura 66

avvalorando i campi nel seguente modo:

a) Descrizione: **RUPAR-SPC**
b) Server: **sanita-vpn.rupar.puglia.it**
c) Account: digitare il proprio codice fiscale
d) Password: digitare la seconda password – associata alla etichetta "**Pwd Utente**" - specificata nella lettera di rilascio delle credenziali
e) Nome Gruppo: **SANITA-VPN**
f) **Segreto:** digitare la password – associata alla etichetta "Pwd Gruppo" - specificata nella lettera di rilascio delle credenziali

f) Salvare la configurazione:

Figura 67

g) La configurazione risultante sarà:

Figura 68

15 Apple - Avvio Connessione VPN con smartphone e tablet

Per avviare il collegamento protetto con il Centro Servizi Sanità Elettronica Regionale, eseguire la seguente procedura:

a) Selezionare **impostazioni**:

Figura 67

b) Selezionare **VPN**

Figura 68

c) Inserire la password associata alla etichetta "**Pwd Utente**" - specificata nella lettera di rilascio delle credenziali:

Figura 69

d) Verificare che la connessione VPN sia attiva:

Figura 70

e) Avviare il browser Safari e digitare la URL del Centro Servizi Edotto di riferimento:

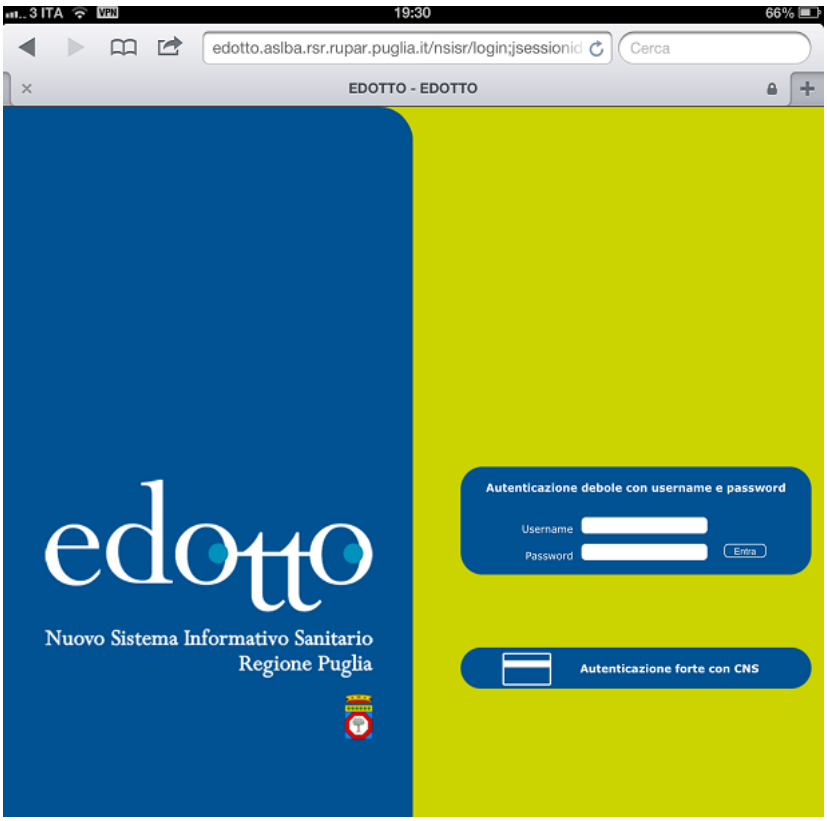


Figura 71

16 Apple – Connessione mediante Mac-book

Per avviare il collegamento protetto con il Centro Servizi Sanità Elettronica Regionale, eseguire la seguente procedura:

a. Selezionare **impostazioni**:

Figura 72

b. Fare clic su "**Network**"

c. Fare clic su "Aggiungi" (+) nella parte inferiore dell'elenco del servizio di connessione network, quindi scegliere "VPN" dal menù a comparsa "Interfaccia;

d. Scegliere come tipo di connessione "Cisco IP-sec" ed assegnare un nome al servizio VPN (p.e. Rupar-SPC-Debole) così come illustrato nell'immagine sottostante

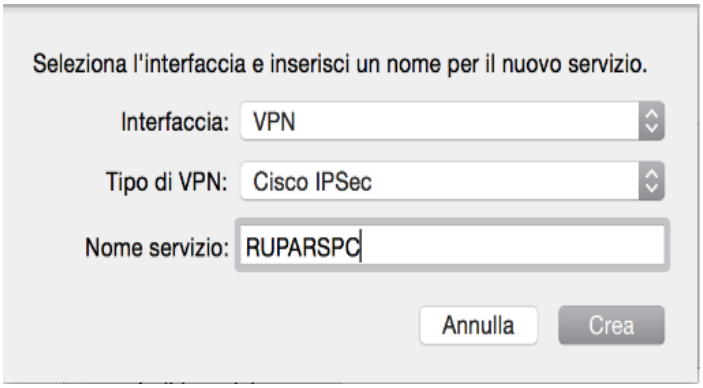


Figura 73

e cliccare su "Crea";

e. Inserire: - **L'indirizzo del server**: sanita-vpn.rupar.puglia.it;
- **Nome account**: codice fiscale;
- **Password**: associata alla etichetta "Pwd Utente" specificata nella lettera di rilascio delle credenziali

Figura 74

f. Fare clic su "Impostazioni autenticazione", quindi inserire:

- **Segreto Condiviso**: digitare la password associata alla etichetta "Pwd Gruppo" - specificata nella lettera di rilascio delle credenziali credenziali ;
- **Nome Gruppo**: SANITA-VPN;

Figura 75

Dopo aver inserito le informazioni di autenticazione dell'utente, fare clic su OK e su Connetti.

g. Successivamente verrà visualizzata una finestra di inserimento dei dati di autenticazione così come visualizzato successivamente:

Figura 76

Inserire pertanto la password utente specificata nella lettera di rilascio delle credenziali.

h. Al termine della verifica dei dati inseriti, verrà instaurata la connessione

Figura 77

17 Apple - Accettazione del Regolamento di utilizzo della RUPAR-SPC

Eseguire la stessa procedura descritta per l'ambiente Microsoft Windows nella sezione **Microsoft Windows: Accettazione del Regolamento di** utilizzo della RUPAR-SPC.

18 Servizio di Helpdesk

Per ulteriori informazioni e per assistenza nella configurazione del software per la realizzazione del collegamento alla RUPAR-SPC in modalità VPN e in caso di problemi tecnici, l'utente può contattare il Servizio di Assistenza tecnica (HelpDesk) all'utente del Centro Servizi Sanità Elettronica Regionale mediante uno dei seguenti canali:

1. **Telefono** – chiamando al numero verde, gratuito per chi chiama da rete fissa e mobile:

Attivo dal Lunedì al Venerdì – nei giorni lavorativi - dalle ore 08:30 alle ore 17:00

2. **Posta elettronica** – scrivendo un messaggio di posta elettronica all'indirizzo:

sanita.hd@sanita.puglia.it