



Navodila za namestitev in uporabo VPN odjemalca Cisco AnyConnect Secure Mobility Client

Ministrstvo za javno upravo

Direktorat za informatiko

Kazalo vsebine



Opis storitve	3
Oddaljen dostop v omrežje HKOM	3
Prezem Cisco AnyConnect VPN odjemalca (ver. 4.5.x):	3
Seznam podprtih protivirusnih programov	4
Namestitev odjemalca in povezava v omrežje HKOM	5
Ročna namestitev odjemalca	5
AnyConnect odjemalec za mobilne naprave	7
Avtomatska namestitev odjemalca	8
Ravnanje v primeru opozorila (Untrusted VPN Server Blocked)	11
Prijava in odjava v omrežje HKOM	13
Navodila za nastavitve strežnika proxy za delo v omrežju HKOM	14
Nastavitev lokalnega požarnega zidu	15
Povezave do Cisco AnyConnect tehnične dokumentacije	16
Odpravljanje napak	16
Prijava/odpravljanje težav z oddaljenim dostopom:	16
Sistem za oddaljeno pomoč uporabniku »isl.gov.si«	16

Opis storitve

VPN storitev omogoča na varen način povezave v HKOM omrežje državnih organov ne glede na to, kje se uporabnik/ca nahaja in preko katerega omrežja dostopa (implementirana je zunanja VPN gruča požarnih pregrad – dostop iz Interneta ter notranja VPN gruča požarnih pregrad, katera omogoča dostop uporabnika iz kateregakoli lokalnega omrežja HKOM organizacije).

Oddaljen dostop v omrežje HKOM

Za dostop v omrežje HKOM preko Cisco AnyConnect odjemalca potrebujete:

- Aktivno internetno povezavo ali HKOM povezavo v primeru prijave na notranjo VPN gručo požarnih pregrad
 - Veljaven geselnik (OTP naprava / generator gesel) ali odobren dostop preko dvostopenjskega SMS overjanja (2FA - sistem SMS)
 - Administratorske pravice za namestitev Cisco AnyConnect odjemalca (ob prvi prijavi/namestitvi)
 - Nameščeno in delujočo predpisano proti-virusno zaščito ¹
 - Spletni brskalnik, samo v primeru avtomatske namestitve AnyConnect odjemalca (Firefox, Safari ali Internet Explorer z nameščenim dodatkom Active X ali Java Runtime Environment)
-
- **Android** [AnyConnect ICS+](#) (Google Play )
 - **IOS** [AnyConnect](#) (App store )

Prevzem Cisco AnyConnect VPN odjemalca (ver. 4.5.x):

- <https://vpndist.gov.si>
- <https://pgc5.gov.si>
- <https://pgc5.sigov.si> (znotraj HKOM omrežja)

¹ Pri prijavi v omrežje HKOM preko VPN odjemalca Cisco AnyConnect Secure Mobility Client se preverja ustrežna protivirusna zaščita, ki je nameščena na uporabnikovem računalniku. Trenutno je objavljen seznam zahtevane protivirusne zaščite, ki se bo lahko spreminjal in dopolnjeval.

Podprte so vse različice operacijski sistemov:

- Windows različice 7, 8, 8.1, 10 (32 bit / 64 bit)
- Mac OS X 10.10, 10.11, 10.12
- Linux RedHat 6, 7 in Ubuntu 12.04 (LTS), 14.04 (LTS), 16.04 (samo LTS-64- bit)

OPOMBA: Podpora za Windows XP je s 1. 1. 2018 s strani podjetja Microsoft Corporation in Cisco Corporation ukinjena!
Dostop do omrežja HKOM iz naprav, ki uporabljajo stari OS WIN XP ni več mogoč.

Seznam podprtih protivirusnih programov

- **Sophos Plc. (Sophos Anti-Virus), zadnja posodobitev < 21 dni**
- Microsoft Cor. (Windows Defender), zadnja posodobitev < 21 dni
- Trend Micro Inc. (Trend Micro Titanium), zadnja posodobitev < 21 dni
- Symantec Cor. (Norton AntiVirus), zadnja posodobitev < 21 dni
- McAfee, Inc. (McAfee AntiVirus), zadnja posodobitev < 21 dni
- Cisco System, Inc. (Cisco Advance Malware Protection for Endpoints), zadnja posodobitev < 21 dni
- **Kaspersky Lab (Kaspersky Endpoint Security), zadnja posodobitev < 21 dni**
- F-Secure Corporation (F-Secure Anti-Virus), zadnja posodobitev < 21 dni
- **ESET Software (NOD32), zadnja posodobitev < 21 dni**
- Palo Alto Networks, Inc. (Traps), zadnja posodobitev < 21 dni
- Panda Security, S.L. (Panda Adaptive Defence 360), zadnja posodobitev < 21 dni

Opombe: za dostop do omrežja HKOM mora biti na računalniku nameščen in aktiven vsaj eden od naštetih protivirusnih programov. V zgoraj naštetih alinejah je za posameznega proizvajalca protivirusnih programov v oklepaju naveden primer protivirusnega programa (lahko se uporablja tudi kakšen drug od navedenega proizvajalca npr.: Microsoft Cor. = *Microsoft Security Essentials*).

Katere verzije zgoraj navedenih protivirusnih programov lahko prepoznamo z obstoječim klientom, ki ga uporabljamo v HKOM omrežju lahko preverite na URL linku, ki naveden v poglavju [Povezave do Cisco AnyConnect Secure Mobility Client tehnične dokumentacije](#) (str.17, **HostScan 4.6.03051** AntiVirus, AntiSpyware, and Firewall).

Namestitev odjemalca in povezava v omrežje HKOM

Namestitev odjemalca lahko izvedemo preko **ročnega** ali **avtomatskega** načina.

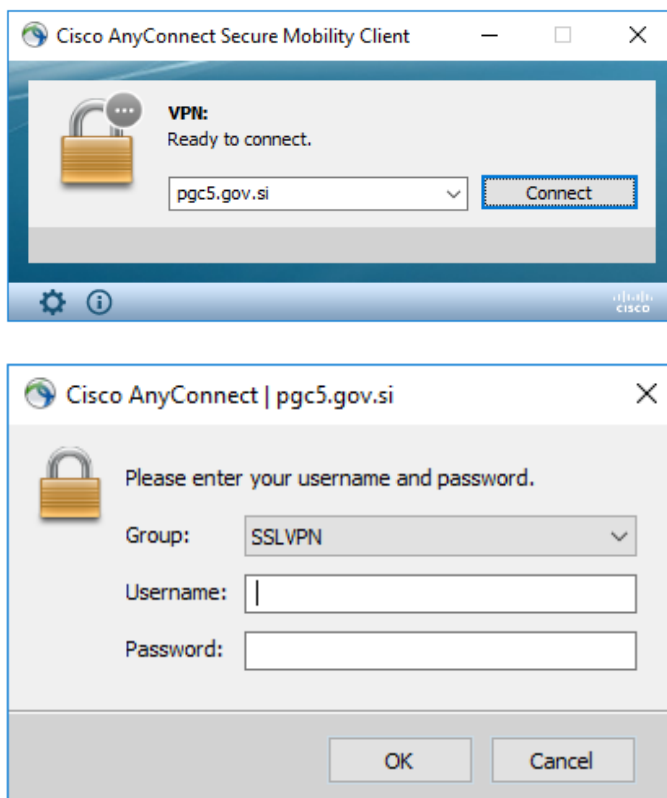
Ročna namestitev odjemalca

Izvedemo prevzem programa na distribucijski strani <https://vpndist.gov.si> ali <https://vpndist.sigov.si> ter »ročno« namestimo VPN odjemalec Cisco AnyConnect Secure Mobility Client. Prijava je mogoče z enim od geselnikov (OTP, sms, APP).

Po namestitvi odjemalca je potrebno pri prvi prijavi na zunanjo vstopno točko **pgc5.gov.si** izbrati povezovalno grupo:

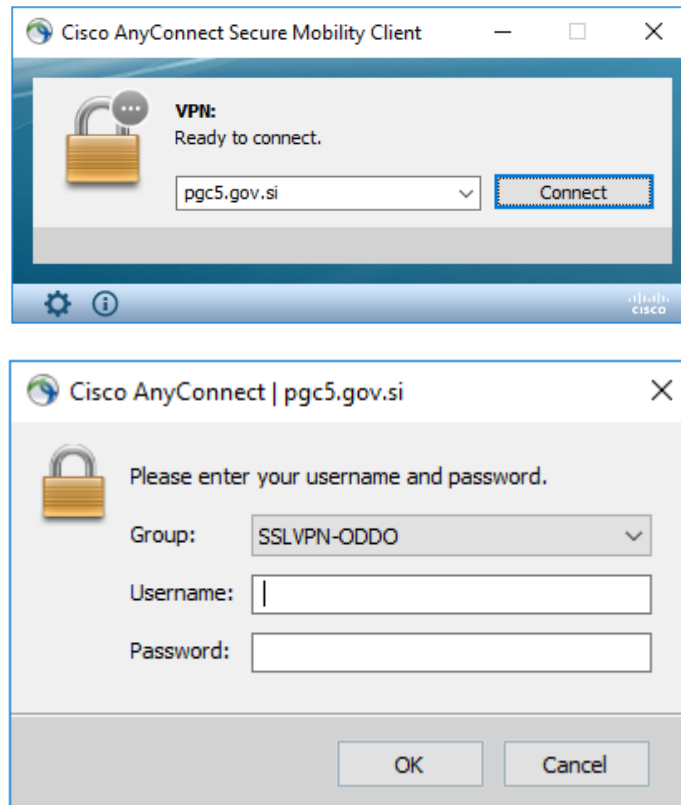
- VPNSSL prijava preko OTP naprave RSA SecurID ali Entrust (v nadaljevanju velja tudi za RSA ali Entrust SMS overjanje) ali
- VPNSSL-ODDO prijava preko dvostopenjske SecureKey ODDO SMS avtentikacije

Prijava s sredstvom močnega overjanja: RSA SecurID ali Entrust



Slika 1: Izbira prijavne grupe za prijavo z RSA SecurID ali Entrust

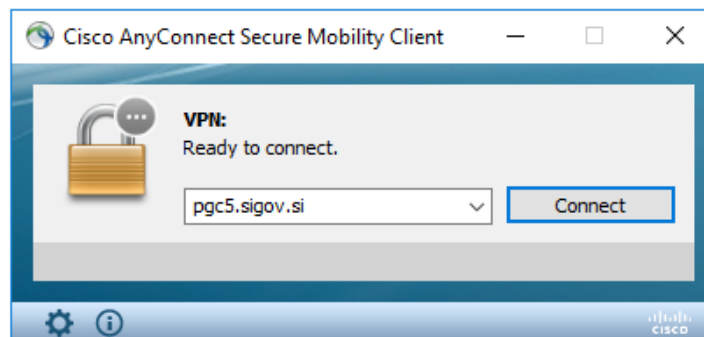
Prijava s sredstvom močnega overjanja: SecureKey (ODDO)

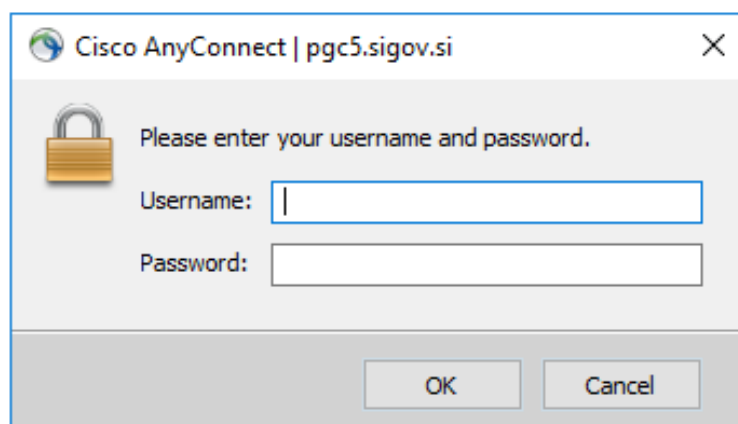


Slika 2: Izbira prijave grupe za prijavo s SecureKey - ODDO

Prijava preko notranje vstopne točke *pgc5.sigov.si* **smo poenotili**, tako da ni **potrebno izbirati prijave grupe glede na sredstvo močnega oviranja**.

Prijava s sredstvom močnega overjanja: RSA SecurID, Entrust ali SecureKey (ODDO)





Slika 3: Prijava preko notranje vstopne točke

AnyConnect odjemalec za mobilne naprave

AnyConnect odjemalec za mobilne naprave lahko prevzamete na:

Android: [AnyConnect¹](#) (Google Play )

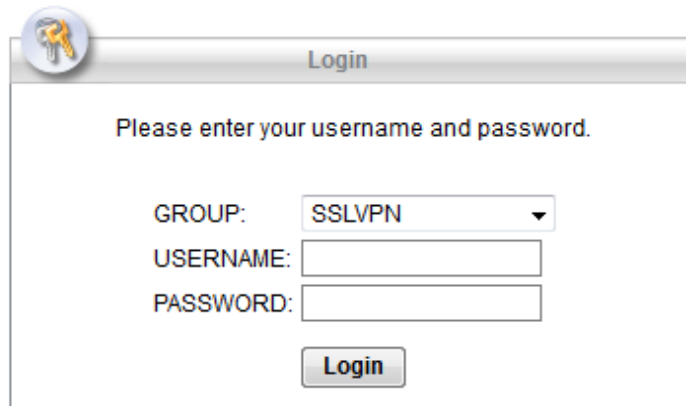
IOS: [AnyConnect¹](#) (App store )

¹Opomba: v iskalno polje vpišite AnyConnect in prevzemite zadnjo verzijo aplikacije.

Avtomatska namestitev odjemalca

Avtomatska namestitev in povezava v omrežje HKOM z Cisco AnyConnect odjemalcem poteka preko zunanjega spletnega naslova <https://pgc5.gov.si> (iz Interneta) ali notranjega spletnega naslova <https://pgc5.sigov.si> (iz omrežja HKOM), katerega vpišemo v spletni brskalnik (Firefox, Safari ali Internet Explorer z nameščenim dodatkom Active X ali Java Runtime Environment, priporočamo da uporabite MS Internet Explorer).

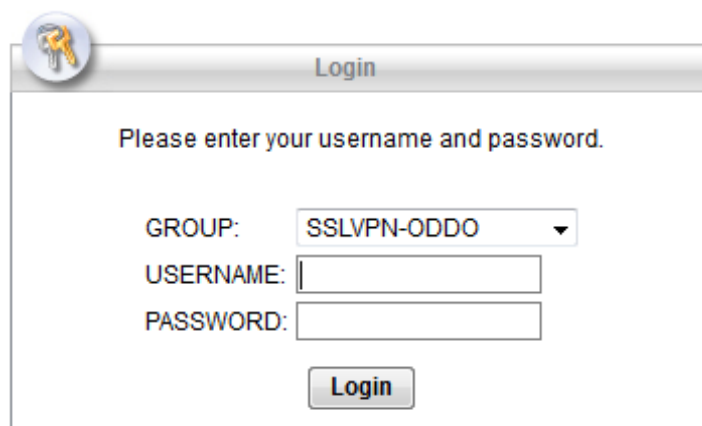
Odpre se nam ekran, kjer vpišemo uporabniško ime in **PIN** + **trenutno številko iz geselnika** (*SecurID* ali *Entrust*).



The screenshot shows a web browser window titled "Login". The main text reads "Please enter your username and password." Below this, there are three input fields: "GROUP:" with a dropdown menu showing "SSLVPN", "USERNAME:" with a text box, and "PASSWORD:" with a text box. A "Login" button is positioned below the password field.

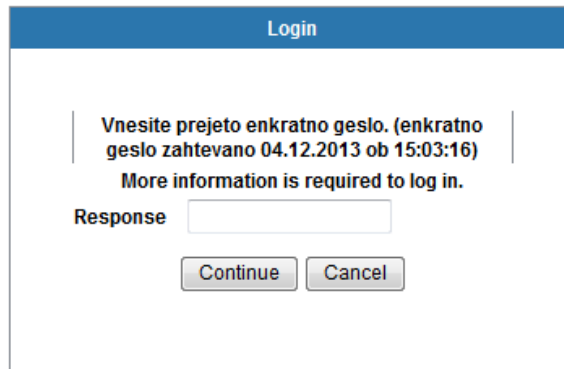
Slika 4: Avtentikacija s SecurID ali Entrust

V primeru, da ima uporabnik pravico dostopati tudi preko dvostopenjske SecureKey ODDO SMS avtentikacije (uporaba enkratnih gesel prejetih preko SMS sporočila) potem moramo izbrati povezovalno grupo SSLVPN-ODDO. Sledi dvostopenjska avtentikacija: **uporabniško ime** + **PIN** ter v drugi fazi vpis **enkratnega gesla**, ki smo ga prejeli preko SMS sporočila.



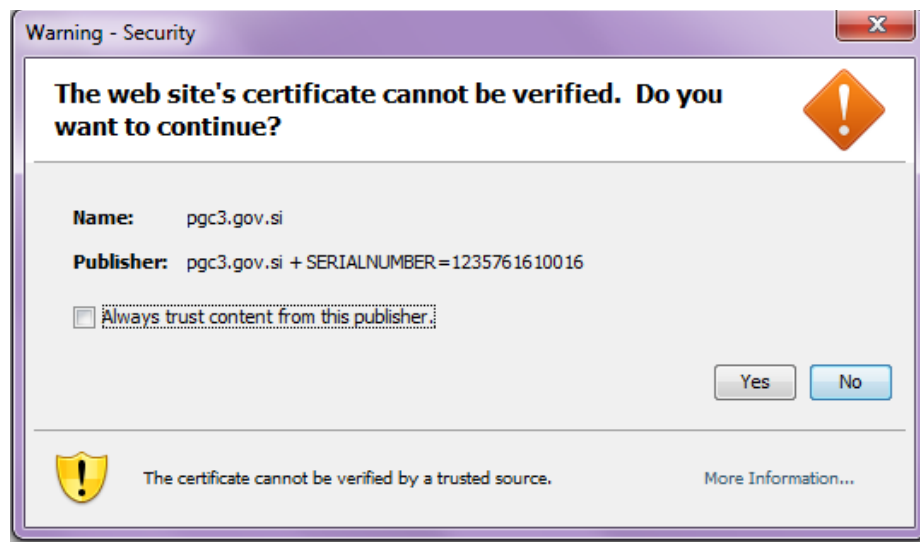
The screenshot shows a web browser window titled "Login". The main text reads "Please enter your username and password." Below this, there are three input fields: "GROUP:" with a dropdown menu showing "SSLVPN-ODDO", "USERNAME:" with a text box, and "PASSWORD:" with a text box. A "Login" button is positioned below the password field.

Slika 5: Avtentikacija z SecureKey ODDO SMS



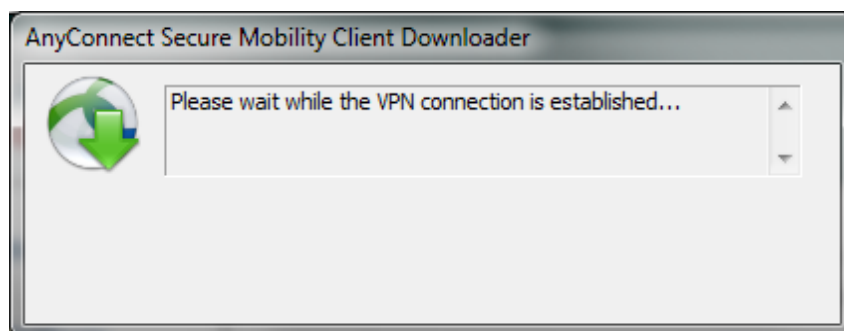
Slika 6: Avtentikacija preko SecureKey ODDO SMS (2. faza)

V primeru, da se nam pred prijavnim oknom prikaže opozorilo za certifikat, tako kot podaja spodnja slika (lahko tudi za certifikat `pgc5.gov.si` ali `pgc4.gov.si`), kliknemo »Yes« - sprejmemo certifikat in nadaljujemo z namestitvijo odjemalca.



Slika 7: Varnostno opozorilo

Po uspešni prijavi se na našem računalniku prične avtomatski postopek za namestitev odjemalca Cisco AnyConnect. Sledi prenašanje instalacijskih datotek na lokalni računalnik (to lahko traja dalj časa odvisno od hitrosti vaše Internetne povezave) ter namestitev odjemalca. V primeru, da se avtomatski postopek ne sproži ročno prenesite odjemalca ter ga ročno namestite.




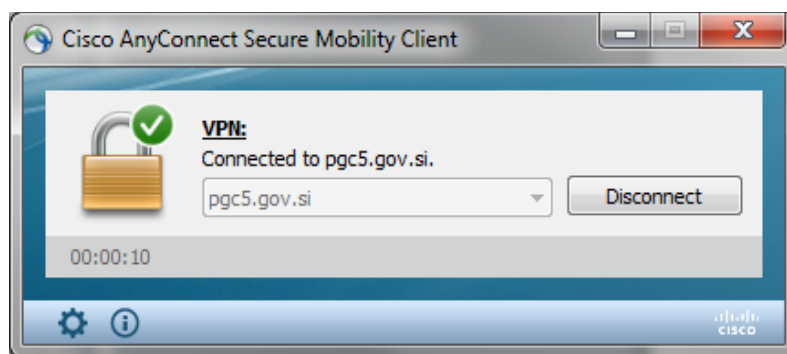
Slika 8: Prenos in namestitev AnyConnect odjemalca

Po uspešni namestitvi odjemalca se nam pojavi naslednje okno, ki nas obvesti, da je varna povezava vzpostavljena in hkrati se pojavi ikona, preko katere kontroliramo trenutno povezavo v omrežju HKOM.




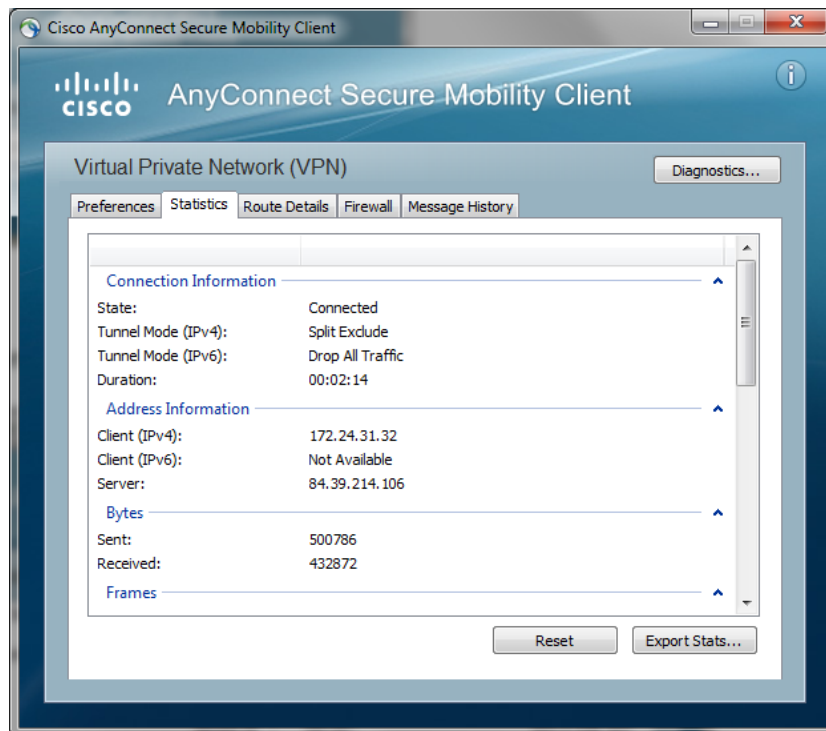
Slika 9: Vzpostavljena varna povezava v omrežju HKOM - AnyConnect ikona

S klikom na ikono  na desni strani opravilne vrstice/»Notification Area« se nam prikaže okno o trenutnem stanju povezave.



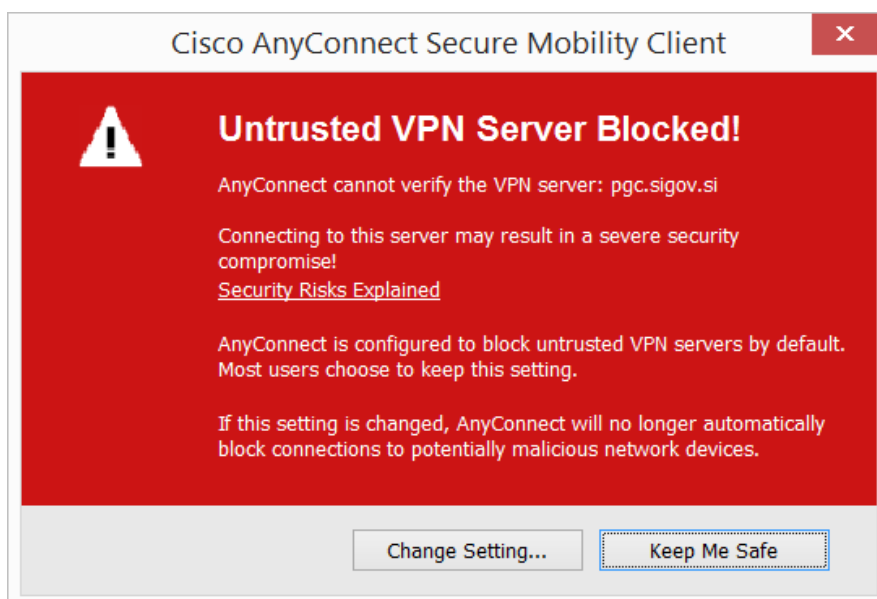
Slika 10: Vzpostavljena povezava v omrežju HKOM – stanje povezave

Dostop do podrobnega pregleda povezave izvedemo s klikom na gumb Advance .



Slika 11: Statistika/pregled vzpostavljene povezave

Ravnanje v primeru opozorila (Untrusted VPN Server Blocked)



Slika 12: Varnostno opozorilo, če ni nameščenega korenškega cert. SIGOV-CA

Pojdite na stran <https://vpndist.gov.si> in spodaj kliknite na povezavo **IDENTITETA SIGOV-CA**, s čimer boste namestili korenski certifikat od SIGOV-CA (<http://www.sigov-ca.si/sigov-ca.crt>).

REPUBLICA SLOVENIJA
MINISTRSTVO ZA JAVNO UPRAVO
DIREKTORAT ZA INFORMATIKO
Sistem za oddaljen dostop v omrežje HKOM

Načini dostopa v omrežje HKOM preko tehnologije VPN

Vloga za odobritev dostopa ali spremembo pravic (Prijava ni potrebna.)	
Geselnik RSA SecurID za SSL VPN Prevzem programske opreme in navodil za VPN dostop Prijava z geselnikom SecurID Sinhronizacija geselnika	
Geselnik SMS za SSL VPN ODDO Prevzem programske opreme in navodil za VPN dostop Prijava s sistemom enkratnih gesel ODDO	

Za dostop do podrobnih navodil in programske opreme je potrebna prijava z enim od gornjih sredstev.
V primeru težav:

- pokličite Ministrstvo za javno upravo: 080 2002
- pišite na podporo uporabnikom: geselniki.mju@gov.si


V primeru, da se pri vzpostavljanju povezave prikaže varnostno opozorilo "Untrusted VPN Server Blocked", preverite, ali imate v vašem brskalniku Internet Explorer nameščeno digitalno potrdilo izdajatelja SIGOV-CA. Digitalno potrdilo lahko avtomatsko namestite v vaš brskalnik na tej povezavi: **IDENTITETA SIGOV-CA**. V primeru, da se vam digitalno potrdilo ne namesti v brskalnik Internet Explorer (IE ni vaš prevzeti brskalnik) pre-kopirajte <http://www.sigov-ca.si/sigov-ca.crt> povezavo v IE ter ročno namestite digitalno potrdilo.

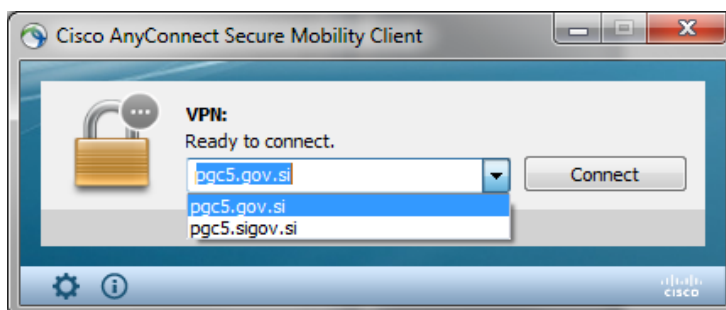
Slika 13: Povezava za avtomatsko namestitev certifikata SIGOV-CA

Prijava in odjava v omrežje HKOM

PRIJAVA


Po namestitvi AnyConect odjemalca izvedemo prijavo v omrežje HKOM s klikom na:

- Ikono  na desni strani opravilne vrstice/»Notification Area« ali
- Start tipka → All Programs → Cisco → Cisco AnyConnect Secure Mobility Client → Cisco AnyConnect Secure Mobility Client (primer za OS WIN-7).
- Izberemo naslov VPN gruča požarnih pregrad ter kliknemo »Connect«:
 - **pgc5.gov.si** (dostop do omrežja HKOM iz Interneta preko SecurID, Entrust ali SecureKey ODDO avtentikacije)
 - **pgc5.sigov.si** (dostop znotraj HKOM omrežja do druge lokacije v omrežju HKOM preko SecurID, Entrust ali SecureKey ODDO avtentikacije)

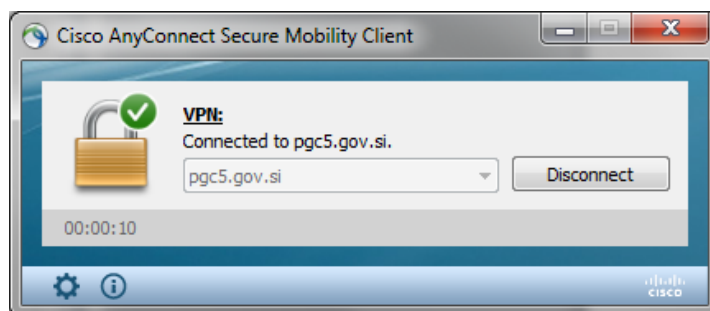


Slika 14: Izbira povezovalnega profila in prijava

ODJAVA

Za odjavo iz omrežja HKOM kliknemo na ikono  na desni strani opravilne vrstice/»Notification Area« ali pa odpremo program na poti: Start tipka → All Programs → Cisco → Cisco AnyConnect Secure Mobility Client → Cisco AnyConnect Secure Mobility Client (primer za OS WIN-7).

Prikaže se nam naslednje okno. Odjavimo se s klikom na »Disconnect«.



Slika 15: Odjava iz omrežja

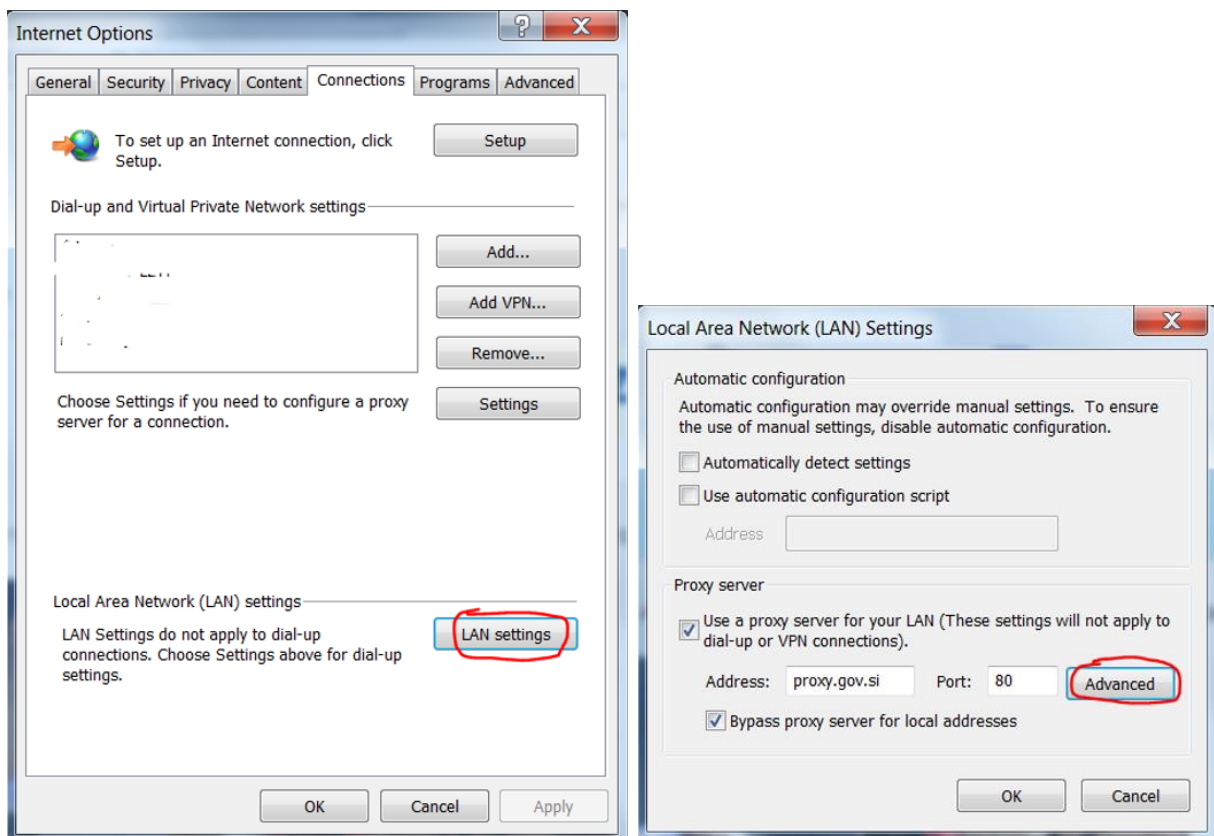
Navodila za nastavitve strežnika proxy za delo v omrežju HKOM

AnyConnect odjemalec izvede **avtomatsko nastavitvev** strežnika proxy za delov omrežju HKOM v **Microsoft Internet Explorer** ter vrnitev vseh spremenjenih nastavitvev proxy strežnika ob prekinitvi AnyConnect povezave.

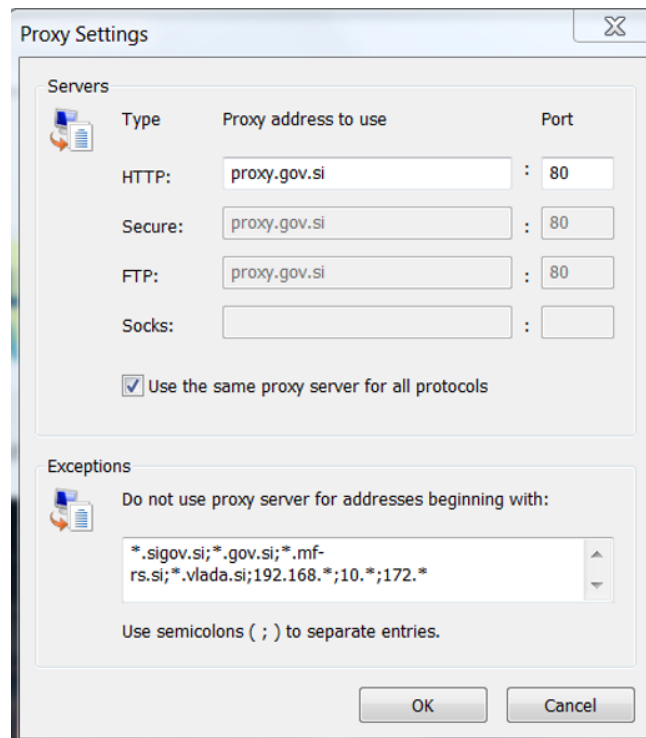
Z januarjem 2018 smo omogočili **avtomatsko nastavitvev proxy strežnika** za vse skupine VPN uporabnikov in sicer s sledečimi nastavitvami:

- Proxy strežnik: **proxy.gov.si:80**
- Izjeme: ***.sigov.si, *.gov.si, *.mf-rs.si, *.vlada.si, 192.168.*, 10.*, 172.***

V primeru, da omenjene avtomatske nastavitve za Vas niso ustrezne (zaradi dostopa do internih http/https strežnikov ali nastavitvev drugega proxy strežnika na Vašem organu), podajamo navodila za **ročno nastavitvev strežnika proxy** v omrežju HKOM za spletni brskalnik MS Internet Explorer.



Slika 16: Nastavitvev proxy strežnika v MS IE (Internet Options/Connections/LAN settings)



Slika 17: Nastavitev proxy strežnika v MS IE (Internet Options/Connections/LAN settings/Advanced)

Nastavitev lokalnega požarnega zidu

V primeru, da imate v vaši organizaciji od koder vzpostavljate AnyConnect povezavo v HKOM omrežje, uporabljate lokalno požarno pregrado, je potrebno za delovanje povezave odpreti sledeče poti:

- 1) **Vrata (port)**
 - a. TCP 443
 - b. UDP 443 (DTLS)
 - c.
- 2) **Ponorni IP**
 - a. 84.39.214.105 (pgc5.gov.si)
 - b. 84.39.214.106 (pgc3.gov.si)
 - c. 84.39.214.107 (pgc4.gov.si)

Opomba: predlagamo, da se za ponorni IP vzame *celoten HKOM naslovni prostor, ki je namenjen za oddaljen dostop* = 84.39.214.104/29.

Povezave do Cisco AnyConnect tehnične dokumentacije

[Opombe k izdaji AnyConnect \(Release Notes 4.5\)](#)

[Error and System Messages](#)

Uradna stran Cisco, ki obrazloži sporočeno napako odjemalca in predlaga postopek za odpravo napake.

[FAQ za VPN \(AnyConnect\)](#)

Pogosta vprašanja in odgovori o VPN povezavi na uradni strani proizvajalca.

[Hostscan Support Charts](#)

Spisek protivirusnih programov, ki jih lahko prepozna AnyConnect klient, ki ga uporabljamo v HKOM omrežju (verzija **HostScan 4.6.03051**).

Odpravljanje napak

Prijava/odpravljanje težav z oddaljenim dostopom:

- pon. - pet., med 8.00 - 16.00 uro na e-naslov: **hkom@gov.si** oz. na tel. številko **080-2002** (center za pomoč uporabnikom),
- pon. – pet., 16.00 - 22.00 ure na e-naslov: **ekc@gov.si** oz. na tel. številko **080-2002** (center za pomoč uporabnikom)
- sicer HKOM dežurni tel. (upravitelj omrežja): tel. številko **041-630-364** ali **041-633-789**

Sistem za oddaljeno pomoč uporabniku »isl.gov.si«

Dežurni vam bo najlaže pomagal, če boste uporabili sistem za oddaljeno pomoč uporabnikom, ki se nahaja na spletnem mestu <https://isl.gov.si>

»ISL Light Clienty« odjemalca lahko prevzamete na naslovu <https://isl.gov.si>.

Prijava napak pri uporabi storitve **isl.gov.si** je možna na tel. številko **01/478-8597** ali na **gregor.skerlep@gov.si**.