Namestitev SSL certifikata

NAVODILA STRANKAM ZA **PRIDOBITEV IN NAMESTITEV SSL CERTIFIKATA**

JANTAR D.O.O.
Kranjska cesta 24
4202 Naklo

T: 04 277 18 13
E: podpora@jantar.si

SSL certifikat je ključnega pomena za spletne strani zaradi več pomembnih razlogov, ki se nanašajo na varnost, zasebnost, zaupanje uporabnikov in skladnost s standardi. Spodaj so navedeni eni ključnih razlogov, zakaj je SSL certifikat pomemben:

1. Šifriranje podatkov: SSL (Secure Sockets Layer) certifikat šifrira podatke, ki se prenašajo med uporabnikovim brskalnikom in strežnikom. To pomeni, da so podatki, kot so osebni podatki, gesla, številke identifikacijskih sredstev in druge občutljive informacije, zaščiteni pred prestrezanjem in nepooblaščenim dostopom.

2. Avtentikacija: SSL certifikat zagotavlja, da je spletna stran, s katero se uporabnik povezuje, resnično tista, za katero se predstavlja. S tem se preprečujejo t.i. phishing napadi, kjer napadalci ustvarijo lažne spletne strani, da bi ukradli osebne podatke uporabnikov.

3. Zaupanje uporabnikov: Ko uporabniki vidijo, da ima spletna stran nameščen SSL certifikat (kar se pogosto označuje z ikono ključavnice v naslovni vrstici brskalnika), jim to daje večje zaupanje, da je spletna stran varna za uporabo.

Tudi programska oprema Codeks omogoča varno HTTPS komunikacijo z uporabo SSL certifikatov. Na naslednjih straneh najdete podrobna navodila za pridobitev in namestitev SSL certifikata za ustrezno delovanje s Codeks programsko opremo. Ta navodila so del osnovne dokumentacije za programsko opremo Codeks.

HTTP + SSL = HTTPS



16.3.3. Šifriran prenos podatkov med uporabnikom in strežnikom

Glavna prednost uporabe *HTTPS (HyperText Transfer Protocol Secure)* komunikacije je šifriranje podatkov, ki se izmenjajo med uporabnikom (klientom) in strežnikom. Uporaba *SSL (Secure Sockets Layer)* certifikata uporabniku zagotavlja, da resnično komunicira z vašim strežnikom in da so njegovi poslani podatki varni pred nepooblaščenim ogledom.

Pri vzpostavitvi HTTPS komunikacije je izmenjava podatkov med vašim strežnikom in računalnikom uporabnika (odjemalca) zašifrirana s šifrirnim ključem, ki je shranjen v SSL certifikatu. Tako zašifrirani podatki so brez ključa za dešifriranje, ki pa ga pozna le strežnik, neberljivi.

Tudi programska oprema Codeks omogoča HTTPS komunikacijo z uporabo SSL certifikatov. Za uporabo SSL certifikata v programski opremi Codeks morate:

1. Pridobiti domeno za programsko opremo Codeks na vašem strežniku;

   Za vaš Codeks strežnik morate pridobiti domeno, glede na katero bo kasneje lahko izdan SSL certifikat za vaš Codeks strežnik (predlagamo, da uporabite poddomeno vaše spletne strani). Domeno za Codeks strežnik pridobite od vašega registratorja domene (pogosto hkrati tudi ponudnika spletnega gostovanja), nato pa uredite nastavitve DNS strežnikov tako, da izbrana domena kaže na vstopno točko vašega lokalnega omrežja (na usmerjevalnik, angl. router), v katerem je nameščena programska oprema Codeks.

2. Pridobiti SSL certifikat za domeno na strežniku, kjer teče programska oprema Codeks; 705

   Programska oprema Codeks omogoča uporabo katerega koli plačljivega SSL certifikata ter tudi brezplačnih SSL certifikatov ustvarjenih s storitvijo *Let's Encrypt* (https://letsencrypt.org/).

3. Uvoziti certifikat na strežnik programske opreme Codeks; 706

   Pridobljen SSL certifikat je potrebno uvoziti (namestiti) na Codeks strežnik.

4. Ustrezno nastaviti nastavitve požarnega zidu na vstopni točki vašega lokalnega omrežja (usmerjevalnik, angl. router); 707

   Omogočiti morate dostop prek požarnega zidu vstopne točke vašega lokalnega sistema, ki dovoljuje zunanjim poizvedbam, da znotraj lokalne mreže dostopajo do strežnika, kjer teče programska oprema Codeks.

5. Ustrezno nastaviti nastavitve požarnega zidu na strežniku programske opreme Codeks; 708

   Omogočiti morate dostop prek požarnega zidu strežnika, kjer teče programske oprema Codeks, ki dovoljuje zunanjim poizvedbam, da dostopajo do aplikacije Codeks na strežniku.

6. Vklopiti HTTPS komunikacijo in urediti nastavitve za HTTPS komunikacijo v programski opremi Codeks; 709

   Omogočiti morate uporabo nameščenega SSL certifikata v programski opremi Codeks ter urediti nekatere druge nastavitve za pravilno delovanje programske opreme Codeks.

16.3.3.1. Pridobitev domene in SSL certifikata

Pridobitev komercialnega SSL certifikata

Komercialne SSL certifikate, ki so izdani s strani svetovno znanih in akreditiranih *Certificate Authority* institucij, lahko kupite pri enem od ponudnikov SSL certifikatov, ki ga izberete sami. Izbrani ponudnik vas bo vodil skozi postopek pridobitve certifikata ter vam na koncu izdal *SSL certifikat*, ki je namenjen namestitvi na vaš strežnik. S certifikatom se vaš strežnik uporabniku predstavi kot varen ter zagotovi, da bo vsa komunikacija z uporabnikom šifrirana. Najpomembnejša prednost komercialnih SSL certifikatov je daljša veljavnost certifikata, saj so komercialni certifikati navadno izdani vsaj za obdobje enega leta, veljavnost posameznega brezplačnega Let's Encrypt certifikata pa je omejena na 90 dni.

Pridobitev SSL certifikata Let's Encrypt

SSL certifikati, ki so pridobljeni prek spletne storitve *Let's Encrypt*, so brezplačni ter akreditirani s strani *Let's Encrypt*, ki je brezplačen, avtomatiziran in odprt organ za izdajo digitalnih potrdil (*Certificate Authority*). Izdajo takšnega potrdila morate s pomočjo orodij ponujenih s strani *Let's Encrypt* izvesti sami, prav tako pa morate kasneje poskrbeti za redno zamenjavo SSL certifikata (vsak *Let's Encrypt* certifikat je veljaven 90 dni, nato je potrebno ustvariti nov SSL certifikat). Več o *Let's Encrypt* certifikatih ter navodila za njihovo uporabo najdete na uradni spletni strani https://letsencrypt.org/.

Po pridobitvi SSL certifikata za vašo Codeks domeno je potrebno še dodati SSL certifikat na Codeks strežnik 706, urediti nastavitve požarnega zidu vstopne točke vašega lokalnega omrežja ter strežnika Codeks programske opreme 707 in urediti nastavitve za HTTPS komunikacijo v programski opremi Codeks 709.

16.3.3.2. Dodajanje certifikata na strežnik

1. Za dodajanje SSL certifikata na Codeks strežnik v *iskalno vrstico Start menija* vpišite mmc in zaženite program mmc (Microsoft Management Console).
2. V *oknu korenske konzole* izberite Datoteka -> Dodaj/Odstrani snapp-in ...
3. V novem oknu izberite Certificates in pritisnite Dodaj >.
4. V novem oknu izberite Computer account in pritisnite Naprej.
5. Izberite Local computer in pritisnite Dokončaj.

Pritisnite V redu, da zaprete pogovorno okno.

6. V *prvem* razdelku okna konzole dvokliknite na Certificates (Local Computer).

Dvokliknite na Osebna.

7. V *tretjem* razdelku okna (razdelek Dejanja) kliknite Več dejanj -> Vsa opravila -> Import ...
8. V oknu *čarovnika za uvažanje potrdil* kliknite Naprej.
9. Izberite Prebrskaj ... in poiščite svoj SSL certifikat (*.pfx).

Desno spodaj nad gumboma Odpri ter Prekliči s spustnega seznama izberite tip datoteke Izmenjava osebnih podatkov (*pfx).

Označite svoj certifikat in kliknite Odpri. Kliknite Naprej.

Vnesite geslo za certifikat in kliknite Naprej.

10. Izberite možnost Shrani vsa potrdila v to shrambo ter v polju Shramba potrdil: izberite Osebna.

Kliknite Naprej. Kliknite Dokončaj. Sistem vas ob končanem procesu obvesti, da je uvoz uspel.

Zaprite okno konzole.

S tem ste uspešno namestili certifikat na vaš strežnik. V nadaljevanju je potrebno še urediti nastavitve požarnega zidu vstopne točke vašega lokalnega omrežja ter strežnika Codeks programske opreme 707 in urediti nastavitve za HTTPS komunikacijo v programski opremi Codeks 709.

16.3.3.3. Nastavitve požarnega zidu vstopne točke in Codeks strežnika

Nastavitve požarnega zidu vstopne točke v vaše lokalno omrežje

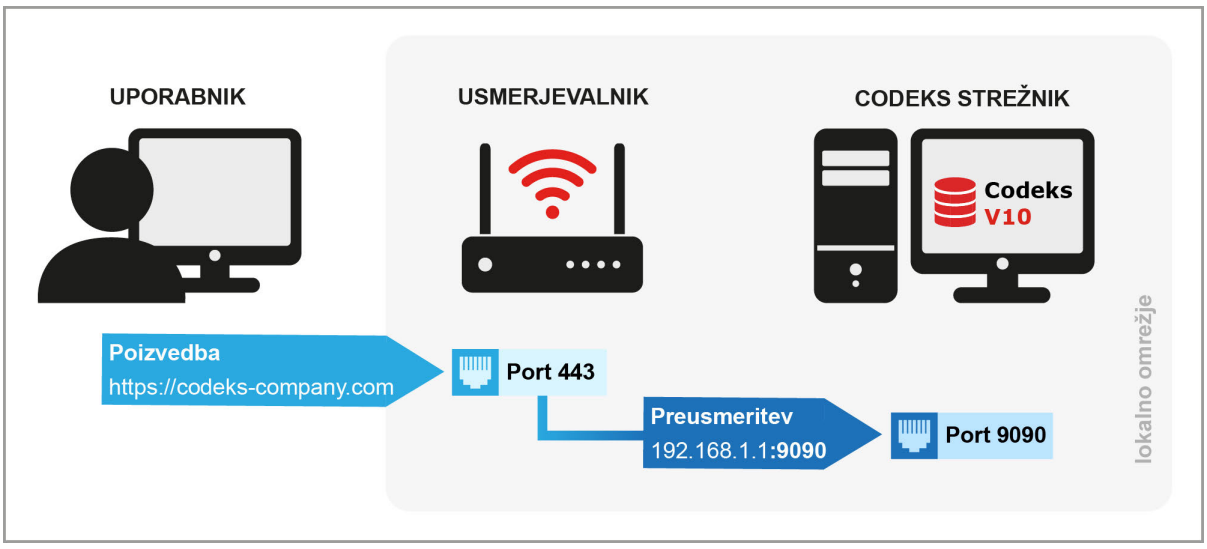
Omogočiti morate dostop prek požarnega zidu vstopne točke vašega lokalnega sistema (prek usmerjevalnika, angl. router), ki dovoljuje zunanjim poizvedbam, da znotraj lokalne mreže dostopajo do strežnika, kjer teče programska oprema Codeks.

Najprej morate zagotoviti dostop zunanjih poizvedb do usmerjevalnika prek TCP vrat (TCP port) 443, nato pa tudi preusmeritev na ustrezni kanal in dostop do Codeks strežnika prek TCP vrat, ki so določena za dostop do Codeks znotraj vaše lokalne mreže.



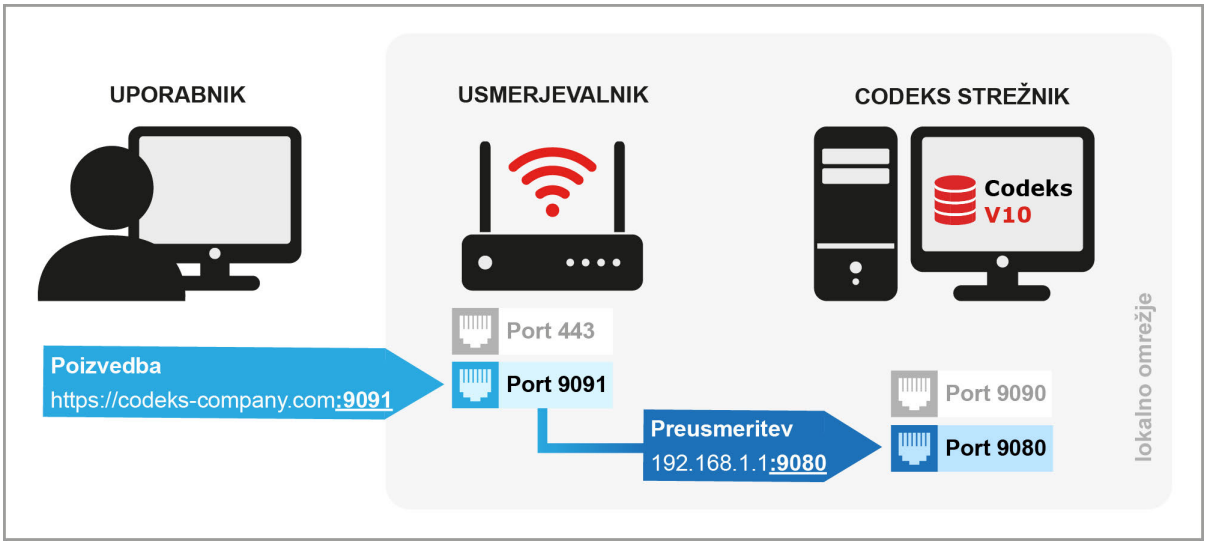
TCP vrata (TCP port), prek katerih znotraj lokalne mreže dostopate do Coderks strežnika, so zapisana v programu Codeks Service Manager.

Primer 1: Standarna konfiguracija



Pri standarni konfiguraciji sistema zunanje HTTPS poizvedbe za dostop do aplikacije Codeks (npr. https://codeks-company.com) prihajajo do usmerjevalnika (routerja) vašega lokalnega omrežja prek TCP vrat (port) 443, ki so po standardu namenjena varni šifrirani SSL komunikaciji. Ko usmerjevalnik prejme zunanjo poizvedbo za povezavo do aplikacije Codeks na port 443, jo v lokalnem notranjem omrežju preusmeri do ustreznega strežnika, kjer je nameščena programska oprema Codeks, na TCP vrata 9090, ki so privzeto določena za dostop do aplikacije Codeks.

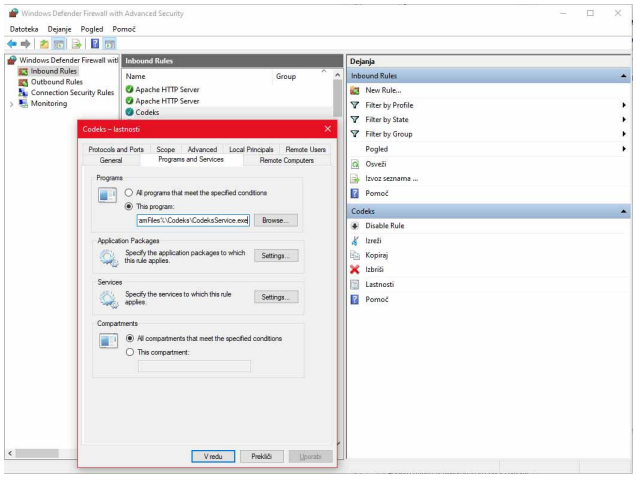
Primer 2: Konfiguracija po meri



V primeru, da zunanje HTTPS poizvedbe z enako domeno, kot je določena za dostop do aplikacije Codeks, že dostopajo do druge aplikacije prek standardnih TCP vrat 433 (npr. do spletne strani), morate na usmerjevalniku za dostop do aplikacije Codeks določiti druga TCP vrata (npr. 9091). V takšnih primerih bodo uporabniki, ki želijo dostopati do aplikacije Codeks, poleg naslova domene svoji poizvedbi nujno morali dopisati tudi ustrezna TCP vrata (npr. https://codeks-company.com:9091). Samo tako bo usmerjevalnik poizvedbo preusmeril do pravilnega strežnika, kjer je nameščena programska oprema Codeks. Usmerjevalnik poizvedbo preusmeri na TCP vrata Codeks strežnika, ki jih lahko poljubno določite v programu *Codeks Service Manager*.

Nastavitve požarnega zidu strežnika programske opreme Codeks

Na strežniku, kjer teče programske oprema Codeks, morate omogočiti dostop prek požarnega zidu, ki dovoljuje zunanjim poizvedbam, da dostopajo do aplikacije Codeks na strežniku.



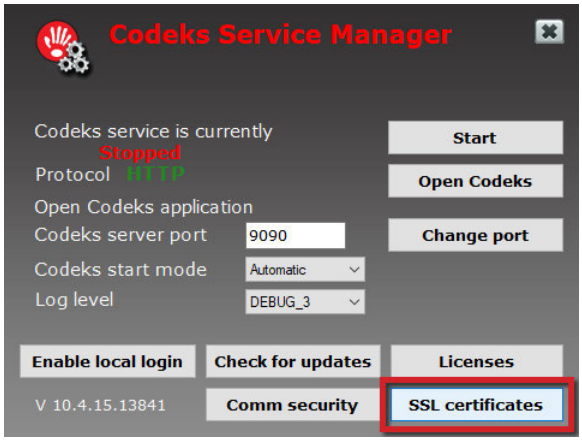
V nadaljevanju je potrebno še urediti nastavitve za HTTPS komunikacijo v programski opremi Codeks 709.

16.3.3.4. Vklop varne komunikacije v Codeks Service Manager in ostale nastavitve

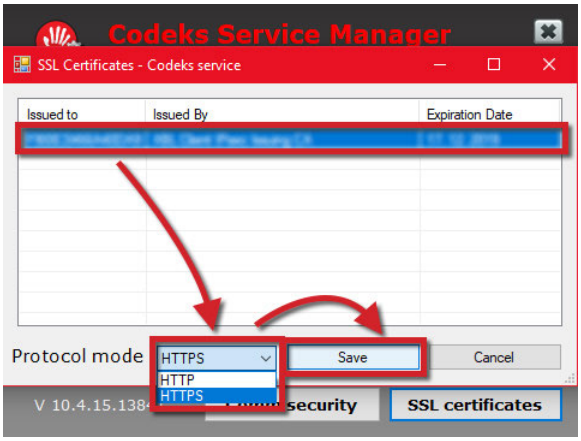
Vklop varne HTTPS komunikacije

Za vklop šifriranega komuniciranja med strežnikom in uporabnikom je potrebno v program Codeks *uvoziti certifikat* ter nastaviti *HTTPS komunikacijski protokol*.

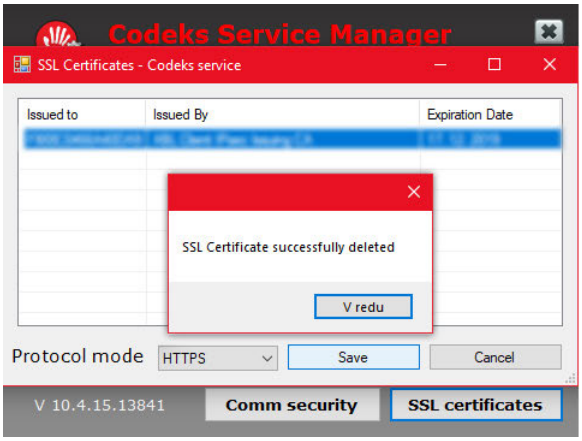
1. Zaženite program *Codeks Service Manger* in ustavite storitev s klikom na gumb *Stop*.
2. Nato kliknite gumb *SSL Certificates*.

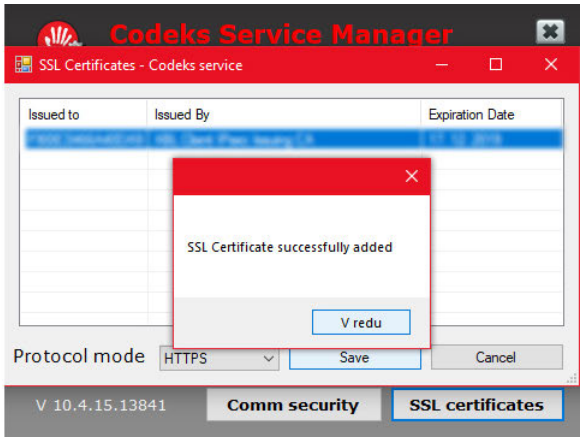


3. V novem oknu na seznamu označite vaš SSL certifikat.
4. Nato v spustnem seznamu spodaj izberite HTTPS ter kliknite *Save*.

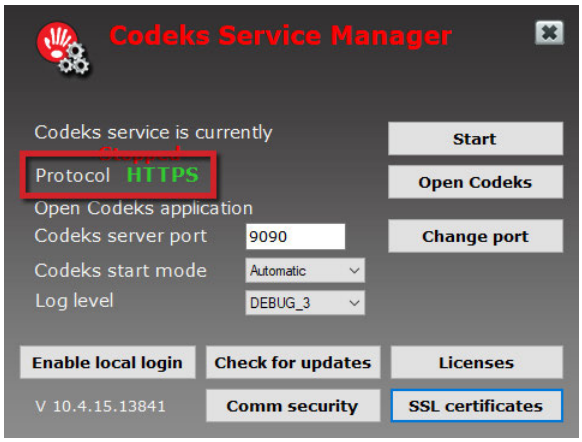


5. O uspešno opravljeni namestitvi vas obvestita dve obvestili:
„SSL certificate successfully deleted.“ in „SSL certificate successfully added.“





6. S tem ste uspešno vklopili varno komunikacijo med uporabnikom in strežnikom. Nova nastavitev bo vidna v programu *Codeks Service Manager*, kjer pod *Protocol* sedaj zapisano *HTTPS*.



Spremembo komunikacijskega protokola pa lahko opazite tudi v naslovni vrstici vašega brskalnika:



Ob uporabi Codeks aplikacije se bo sedaj spletni naslov začel z https:// in ne več http://.

OPOZORILO!
Če ste način varne komunikacije s z vašim strežnikom omogočili naknadno po namestitvi Codeks programske opreme, o spremembi komunikacijskega protokola obvezno obvestite vse vaše uporabnike. Stari URL naslov za dostop do aplikacije Codeks (z *http://*) namreč ne bo več deloval, ampak ga je potrebno zamenjati z novim, ki uporablja *https://*.

OPOZORILO!
V primeru, da po vklopu varne HTTPS povezave, z mobilnimi napravami ne morete vzpostaviti povezave z vašim strežnikom, spremenite nastavitev *Številke vrat* v mobilni aplikaciji *Codeks Mobility* na vaši mobilni napravi. Za komunikacijo z vašim strežnikom vpišite vrata (port) 443, ki so po standardu za HTTPS določena kot privzeta za varno (https://) komunikacijo.

Dodatne nastavitve za HTTPS komunikacijo v Codeks

Potem ko vklopite varno HTTPS komunikacijo v programu *Codeks Service Manager,* preglejte in ustrezno popravite še naslednje nastavitve:

- v *Nastavitve -> Nastavitve -> zavihek Nastavitve e-pošte*:
  - omogočite nastavitev *SMTP uporabi SSL;*
  - vpišite celoten nov URL naslov vašega Codeks strežnika pod nastavitev *URL strežnika (povezave)* (npr. *https://example.com/)*

