Sisukord

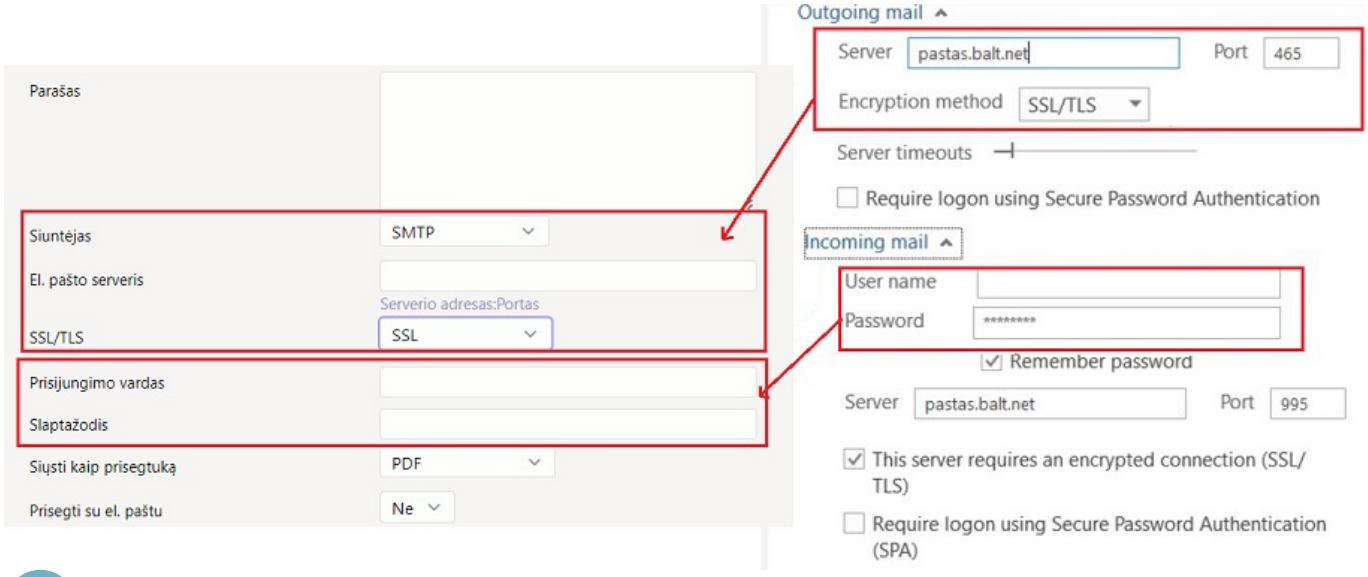
1. SMTP nustatymų konfigūravimas 3
2. "Gmail" pašto konfigūravimas 4
3. SPF - Jei el. laiškai atkeliauja atgal arba yra klasifikuojami kaip "spam" 5
4. TXT įrašo peržiūrėjimas „Windows“ operacinėje sistemoje 6
5. „Directo“ paskyrimas įgaliotuoju siuntėju 6
6. DKIM (DomainKeys Identified Mail) 7
7. Testavimas 7

1. SMTP nustatymų konfigūravimas

Pašto serverio konfigūravimą galite rasti vartotojo nustatymuose: NUSTATYMAI→ASMENINIAI NUSTATYMAI→VARTOTOJAS.

Svarbu užpildyti šiuos nustatymų laukelius:

1. **Siuntėjas** - čia nurodome SMTP, jeigu norime kad Directo laiškus siųstų per asmeninį pašto serverį. Jeigu čia paliekame Directo, laiškai bus siunčiami iš Directo serverio, tačiau kai kurie pašto serveriai gali blokuoti Directo siunčiamus laiškus.
2. **El. pašto serveris** - čia nurodome pašto serverio adresą bei port'ą. Juos galite rasti Outlook programoje.
3. **SSL** - čia pasirenkame TAIP, jeigu jūsų nurodytas pašto serveris naudoja SSL.
4. **Prisijungimo vardas** - čia nurodomas prisijungimo vardas, kurį naudojate nurodytam pašto serveriui.
5. **Slaptažodis** - čia nurodomas prisijungimo slaptažodis, kurį naudojate nurodytam pašto serveriui.



SVARBU: laukelyje El. paštas turite nurodyti tą pašto adresą, kurio nustatymus suvedėte. Kitu atveju Directo negalės išsiųsti laiškų.

Jeigu Jūs naudojate **Office 365**, tuomet reikia atlikti tokius nustatymus:

1. **SSL/TLS** - čia pasirenkame **StartSSL/SSL/TLS**.
2. Reikia per Office 365 admin panelę įjungti Authenticate SMTP. Šis pakeitimas įsijungia po paros laiko. Jeigu nebus įjungtas šis nustatymas, neveiks siuntimas.
3. **El. pašto serveris** - smtp.office365.com: (portas 25 arba 587 arba 465 arba 2525)
4. Taip pat reikia nueiti į Microsoft 365 admin center → Vartotojai → Aktyvūs vartotojai → Vartotojas → Paštas → Valdyti el.pašto programėles čia → Autentifikuotas SMTP turi būti parinktas čia ir pažymėti varnelę prie **Authenticated SMTP**

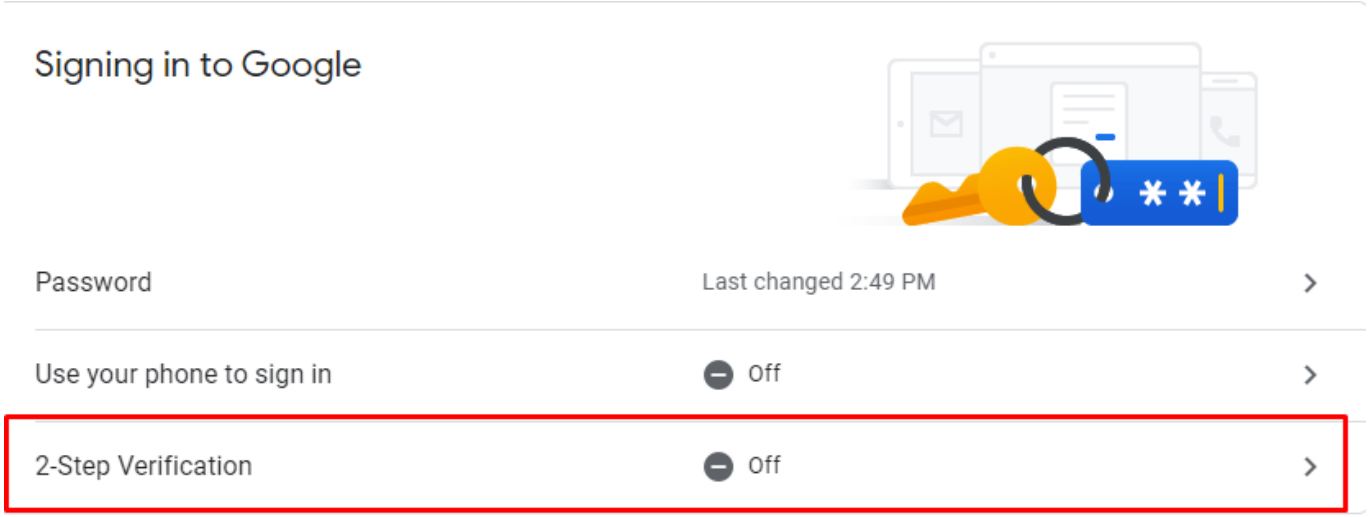
Jeigu SMTP serveryje yra sukonfigūruotas prieigos apribojimas pagal IP adresus, įtraukite

`login.directo.ee` (arba IP adresus `90.190.150.210` ir `90.190.150.212`) į leistinų (trusted) siuntėjų sąrašą.

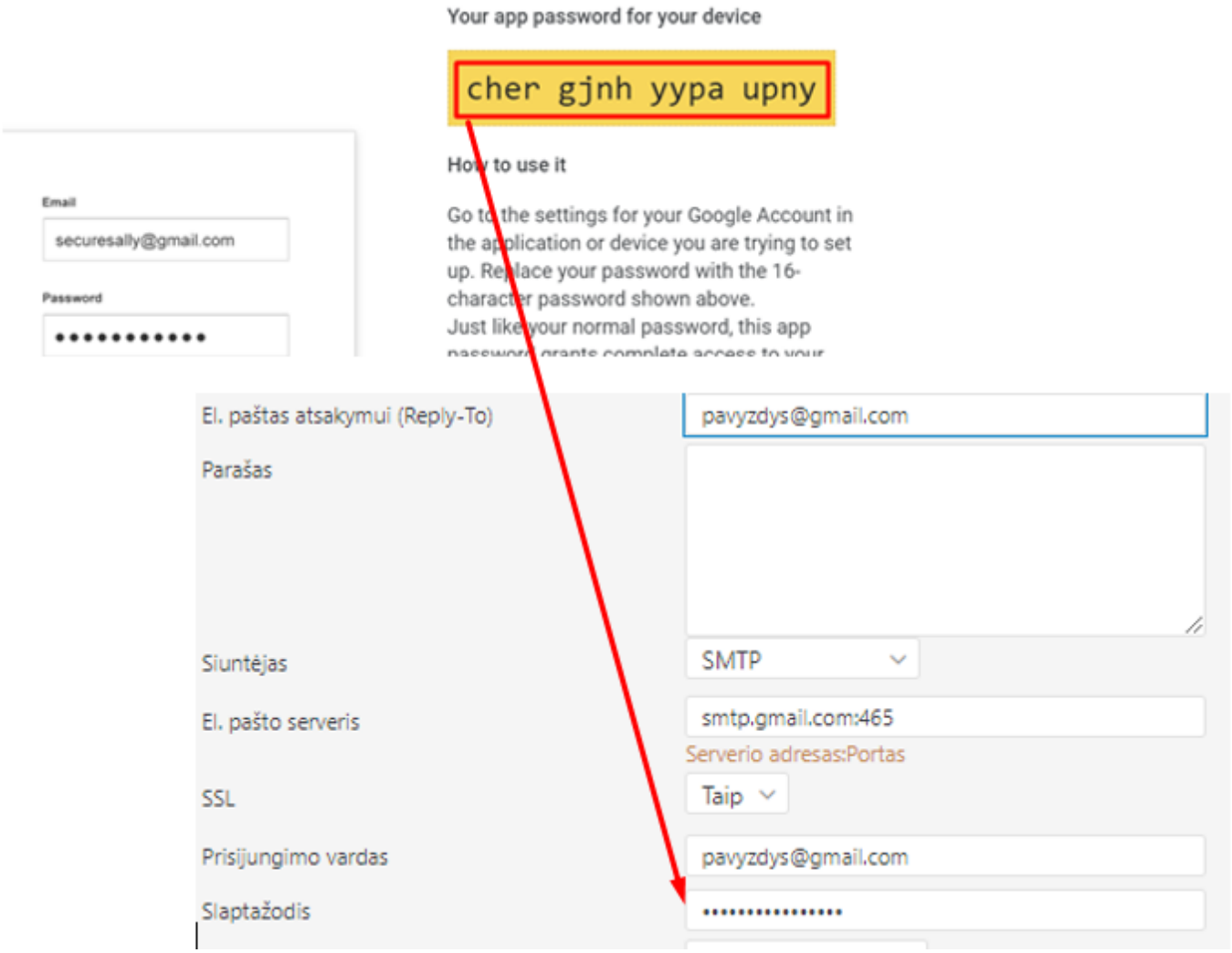
2. "Gmail" pašto konfigūravimas

Norėdami siųsti el. laiškus iš Directo naudodamiesi @gmail.com paštu turite „Google“ paskyroje, atlikti vienkartinį veiksmą, t.y. sukurti atskirą slaptažodį „APP password“.

- Einame į savo Google paskyrą (Security skiltis) ;
- *Signing in to Google* dalyje reikia aktyvuoti *2-Step Veritication* (turi būti **ON**) (jei jis jau aktyvuotas pereikite prie kito žingsnio). Spaudžiame *2-Step Veritication* → GET STARTED → suvedamo savo „Gmail“ pašto slaptažodį → TEXT message (gausime į telefoną SMS žinute kodą) → suvedame 6 skaitmenų gautą kodą (tik skaičiai) ir patvirtiname *2-Step Veritication* aktyvavimą (TURN ON);



- Grįžtame prie Google paskyros (Security skilties) *Signing in to Google* dalyje pasirenkame *App passwords* → suvedame savo el pašto slaptažodį. Select app → Mail, Select devise → Other ir galite nurodyti pavadinimą pvz Directo, spaudžiame Generate;
- Sugeneruojams ilgas slaptažodis, kurį reikia įvesti Directo asmeniniuose nustatymuose į laukelį slaptažodis (siūlome Ctrl+C ir Ctrl+V):



- „Gmail“ el. Pašto serveris Directo konfigūracijoje turėtų būti nustatytas kaip **smtp.gmail.com:465** ir SSL → TAIP.

3. SPF - Jei el. laiškai atkeliauja atgal arba yra klasifikuojami kaip "spam"

Sender Policy Framework (SPF) yra naudojamas tam, kad el. laiško siuntėjas siųsdamas laišką neatrodytų kaip nepažįstamas gavėjams. SPF veikia domeno pagrindu ir yra įgyvendinamas, jei priimančiosios šalies domenas ir siuntėjo šalis palaiko SPF standartą. Techniškai tai yra DNS TXT įrašas, kurį patikrina gavėjas. Daugiau galite perskaityti čia ir čia.

SPF leidžia gavėjui patikrinti, ar serveris, siunčiantis el. laišką („Directo“), turi teisę atstovauti tam žmogui ar įmonei, kam jis bando siųsti. Kadangi „Directo“ paprastai siunčia laiškus iš įmonės adreso, gali susidaryti situacija, kai siunčiami tiesioginiai laiškai patenka į „spam“ aplanką gavėjo pusėje arba gaunami atgal, nes gavėjas patikrina ir nustato, kad „Directo“ serveris nėra įgaliotas siųsti laiškus įmonės vardu.

Jei nenorite leisti „Directo“ siųsti laiškų į Jūsų domeną, alternatyvus sprendimas yra vis tiek nustatyti „Directo“ kaip siuntėją, tačiau naudoti Reply-To antraštę, kuriai priskirtas tikrasis siuntėjas. Daugiau apie tai galite perskaityti čia.

4. TXT įrašo peržiūrėjimas „Windows“ operacinėje sistemoje

Norėdami sužinoti, kaip šiuo metu sukonfigūruotas Jūsų įmonės DNS TXT įrašas, paleidžiame Command Prompt programą (paspaudžiame klavišus Windows + R, įrašome *cmd.exe* ir paspaudžiame OK). Tada įrašome šias komandas, po kiekvienos komandos paspausdami klavišą Enter (*manodomenas.lt* pakeičiame į Jūsų įmonės domeną):

- nslookup
- set type=TXT
- manodomenas.lt

Rezultato pavyzdys - jis reiškia, kad leidžiama siųsti laišką iš savo el. pašto serverio ir *pavyzdys.lt*, o iš kitų serverių siunčiami laiškai bus atmesti:

```
Non-authoritative answer:
directo.ee text =
        "v=spf1 mx a:pavyzdys.lt -all"
```

5. „Directo“ paskyrimas įgaliotuoju siuntėju

Tam, kad „Directo“ galėtų be problemų siųsti el. laiškus Jūsų įmonės vardu, TXT įraše turėtų būti:

```
a:directo.gate.ee
```

Jeigu būtina naudoti IP adresą vietoje domeno, TXT įraše naudokite `ip4:90.190.150.210 ip4:90.190.150.211 ip4:90.190.150.212 ip4:90.190.150.213`

Masiniam laiškų siuntimui yra naudojamas IP adresas `90.190.150.82`

Mažiausias SPF įrašas, kurį leidžiama siųsti į pašto serverį pagal numatytuosius nustatymus, atrodytų taip:

```
v=spf1 mx a:directo.gate.ee -all
```

SPF įrašas turi būti pateiktas kaip vienas įrašas. Jei esamas SPF TXT įrašas jau yra, „Directo“ leidžiantį įrašą reikia pridėti prie esamo. Pagal aukščiau pateikto rezultato pavyzdį, naujas įrašas atrodytų taip:

```
v=spf1 mx a:pavyzdys.lt a:directo.gate.ee -all
```

pavyzdys.lt yra domeno, kuriam leidžiama siųsti el. laiškus, pavyzdys - jo nereikia pridėti, kad

„Directo“ galėtų siųsti el. laiškus

6. DKIM (DomainKeys Identified Mail)

DKIM yra PKI (Public Key Infrastructure) pagrindo būdas pasirašyti siunčiamus el. laiškus, kad būtų užtikrintas jų patikimumas. Kiekvienam domenui yra aprašomas viešas to domeno raktas (public key) ir pridedamas prie domeno DNS įrašo. Panašiai kaip SPF, DKIM apibūdinamas kaip TXT įrašas.

DKIM yra būtinas norint užtikrinti taisyklingą DMARC veikimą. Daugiau apie DKIM galite perskaityti čia.

„Directo“ pasirašo siunčiamus pranešimus directo.ee domeno atžvilgiu. Jei norite, galite ir būtų prasminga pakeisti esantį domeną eidami į NUSTATYMAI → Pagrindiniai nustatymai → Bendri nustatymai → „Siunčiamų el. pašto laiškų DKIM parašo domenas“ į savo įmonės domeną. Būtina sąlyga, kad tai veiktų, kad „Directo“ viešasis raktas būtų pridėtas prie sukonfigūruoto domeno taip:

Directo DKIM parinkiklis (selector) yra **directo**, tai yra, jei domenas nustatytas kaip *manoimone.lt* (ir „Directo“ yra vartotojo siuntėjo el. pašto adresas su tuo pačiu domenu), tada TXT įrašą šio domeno DNS reikia suformatuoti taip:

DKIM HOST pavadinimas: `directo._domainkey.manoimone.lt`
DKIM TXT reikšmė: `k=rsa;`
`p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA7muJiXYB8Y8AmaicjrQn5fItuJ8IkRJ/6h9v65AommktFOdtzBXDxNDWaLHEjSWxNThMFqxw1NRWLgZOUFaTrQ4wmjJ4QyJoCTvBTklqxtyoCJM/WK3JtWtDfV44R5dZZNSygNgx8RP6G6ivcWXzc1+DiObYgED4BtG72wBGD7oJXIdCV5qG4s41KYDMoJzHdBBAf4rYroaFCzUi85U6p8A6u32gHjRM6ybv7cr74EMncXlV3yj8JQ7xGHOxnEC2MMEDA4xArnLexQ9qjqCL9lWy7QadVaMjhev6D79r6QCOEBG3tBtQk6nGzclbrmDntWc5g4+yKz/TqDgSWYS8JwIDAQAB;`

7. Testavimas

Išbandyti SPF ir DKIM galite čia.

DNS įrašų sinchronizavimas gali užtrukti, todėl jūsų atlikti pakeitimai gali neatsispindėti realiuoju laiku ir bandymas gali nepavykti iškart.

From:
https://wiki.directo.ee/ - **Directo Help**

Permanent link:
https://wiki.directo.ee/lt/smtp

Last update: **2023/09/26 14:46**