Sisukord

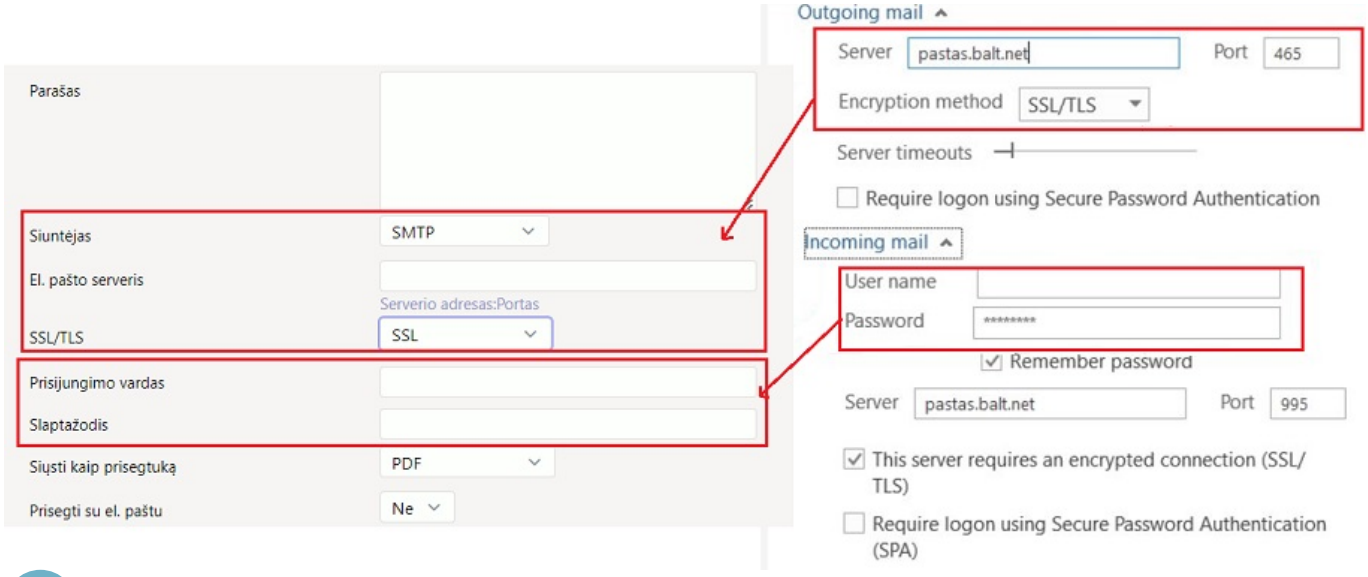
1. SMTP nustatymų konfigūravimas 3
2. "Gmail" pašto konfigūravimas 4
3. SPF - Jei el. laiškai atkeliauja atgal arba yra klasifikuojami kaip "spam" 5
4. TXT įrašo peržiūrėjimas „Windows“ operacinėje sistemoje 6
5. „Directo“ paskyrimas įgaliotuoju siuntėju 6
6. DKIM (DomainKeys Identified Mail) 7
7. Testavimas 7
8. Pakeitimai nuo 2026 m. 7
8.1 Google Gmail konfigūravimas 8
8.2 Microsoft 365 nustatymas 9
8.3 Zonos nustatymai 11
8.4 Viena konfigūracija, keli vartotojai 11
8.5 Directo – „Reply-To“ nustatymas 11

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**

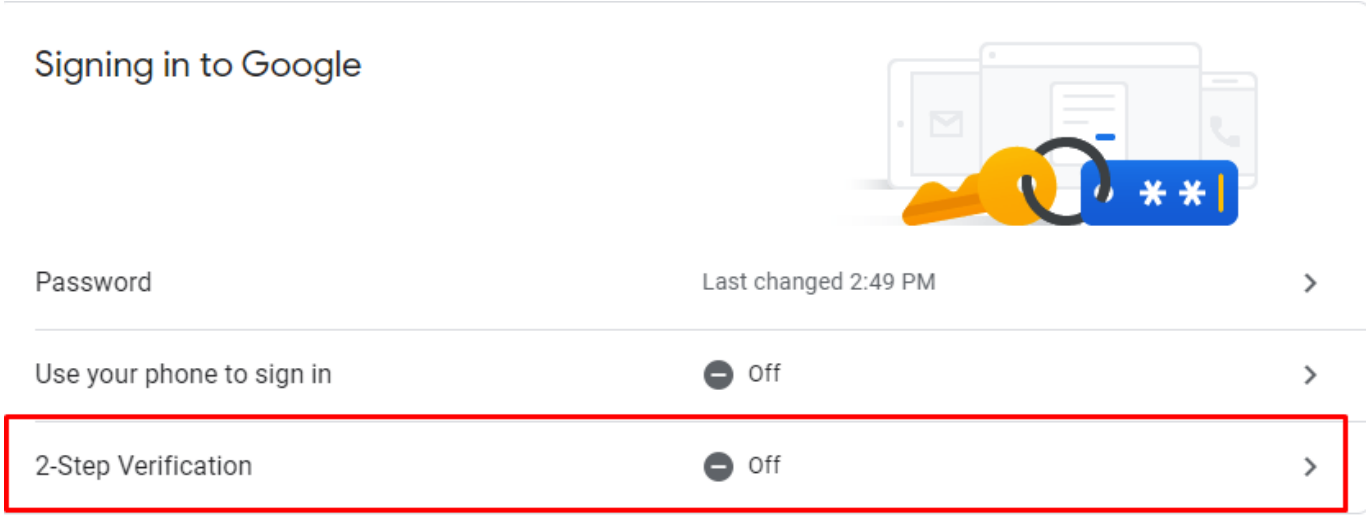
Jeigu SMTP serveryje yra sukonfigūruotas prieigos apribojimas pagal IP adresus, įtraukite

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

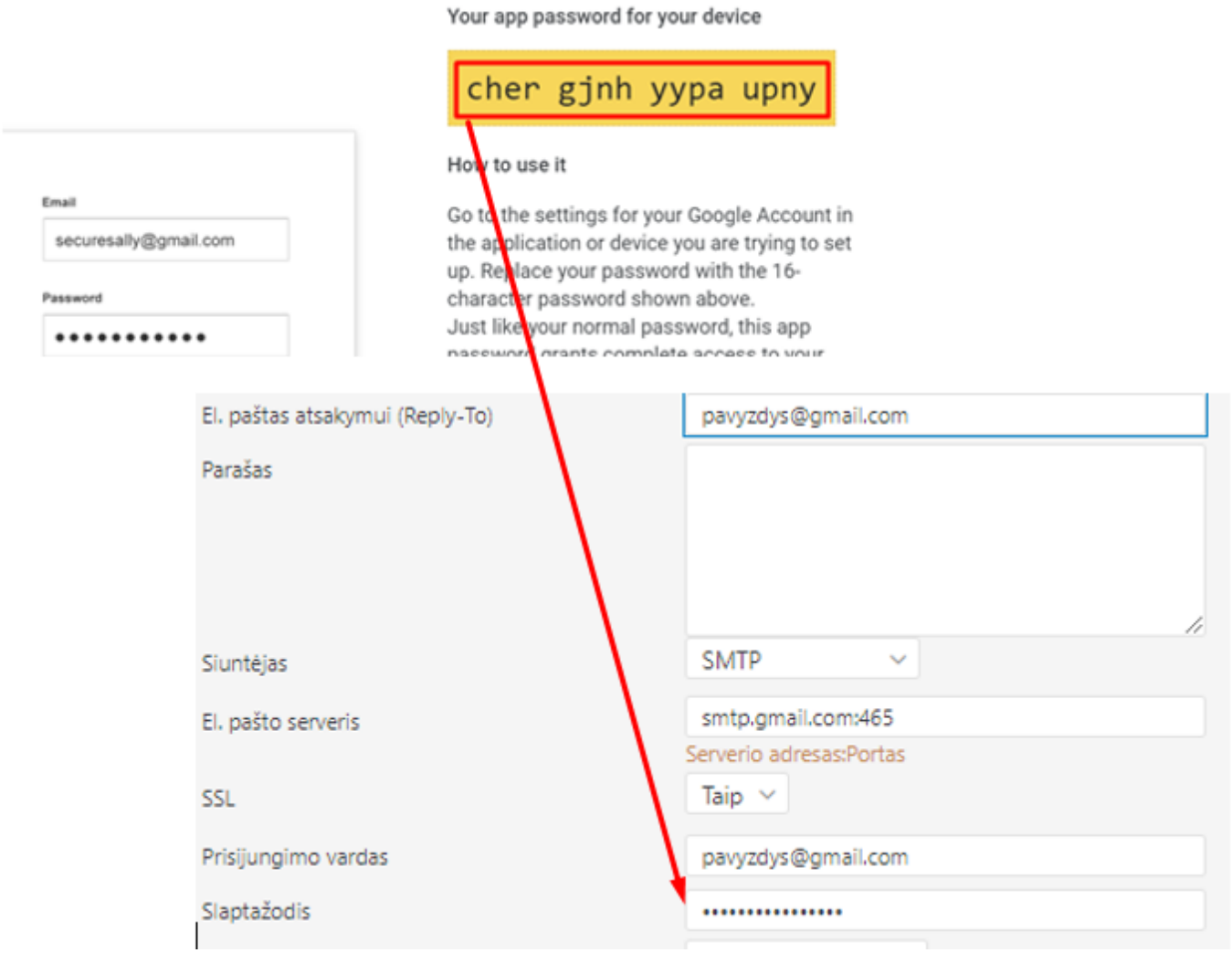
2. "Gmail" pašto konfigūravimas

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.

8. Pakeitimai nuo 2026 m.

Pagal numatytuosius nustatymus el. laiškai iš „Directo“ siunčiami per „Directo“ serverį directo.gate.ee (90.190.150.212), ir daugeliu atvejų vartotojui nereikia galvoti, kaip siunčiami jo laiškai. Tačiau yra išskirtinių situacijų, kai galimybė nurodyti siuntėjo serverį gali būti labai naudinga. Be to, šiuo atveju leidžiamos visos paslaugos, kurioms reikalingas masinio pašto modulis (pvz., sąskaitų faktūrų išrašymas ir klientų el. pašto adresai).

Konfigūracija nustatoma pagal vartotoją (tačiau gali būti taikoma ir globaliai) ir pasiekiama per

vartotojo kortelę, pasirinkus **Pagrindinis meniu → Asmeniniai → Vartotojas**. Norint matyti nustatymus, iš el. pašto siuntimo parinkčių reikia pasirinkti SMTP. Galima nustatyti šiuos parametrus:

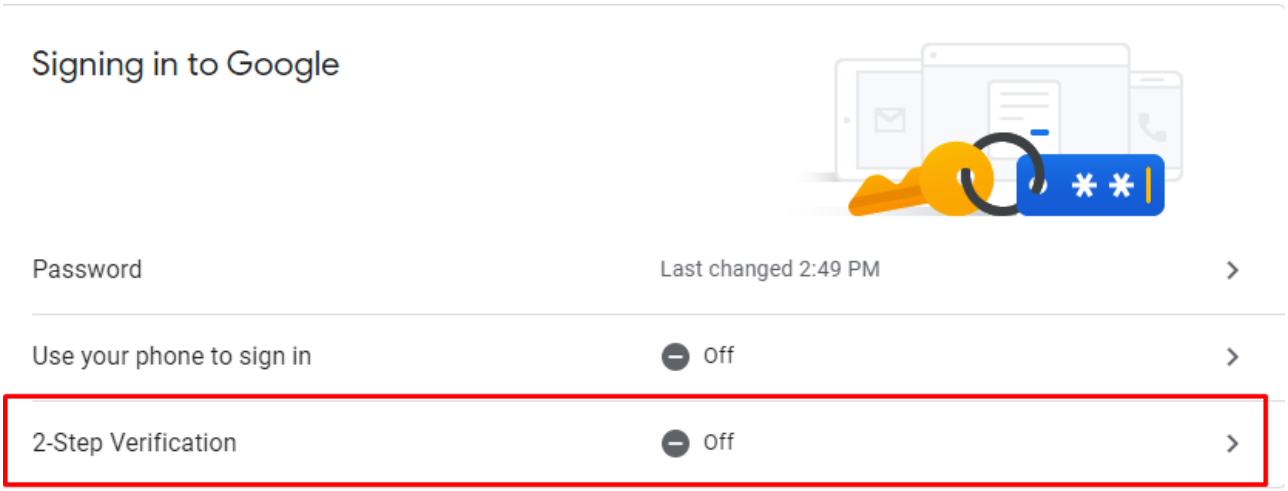
1. **Serveris ir prievadas –** prievadai 25, 465 ir 587 yra atidaryti.
2. **SSL/TLS –** jei reikalingas šifruotas ryšys, pasirinkite tinkamą nustatymą pagal jūsų SMTP serverio reikalavimus. Įprastai SSL naudojamas su 465 prievadu, o StartSSL/SSL/TLS yra saugūs pasirinkimai visiems kitiems prievadams. Jei pasirinktą NIE, el. laiškai tarp Directo ir SMTP serverio siunčiami „atvirai“, be šifravimo.
3. **Prisijungimo vardas –** el. pašto paskyros naudotojas (**PASTABA!** Jei jūsų pašto serveris nereikalauja autentifikacijos, vartotojo lauko nepildykite).
4. **Slaptažodis –** el. pašto paskyros slaptažodis.

1. Išbandyti paslaugų teikėjai: Gmail, Telia (mail.ee), Microlink/Telia (Exchange Mlx plus) ir zone.ee, tačiau turėtų veikti su bet kuriuo el. pašto paslaugų teikėju, leidžiančiu siųsti laiškus per savo pašto serverį (per SMTP).
2. Siunčiant iš „Google Gmail“ paskyros, išsiųstas el. laiškas taip pat bus išsaugotas aplanke „Gmail Sent“, todėl atrodys, kad el. laiškas būtų išsiųstas iš paties „Gmail“.
3. Už bet kokias klaidas ir el. laiškų neišsiuntimą, kai naudojate savo serverio konfigūraciją, atsako vartotojas, taip pat už riziką, kad gaunantys serveriai užblokuos jūsų el. pašto paskyrą.
4. Jei SMTP serveris sukonfigūruotas siųsti el. laiškus ir norima apriboti prieigą pagal IP, toliau išvardinti IP adresai turėtų būti sukonfigūruoti :
    - 90.190.150.210
    - 90.190.150.211
    - 90.190.150.212
    - 90.190.150.213
    - 90.190.150.82

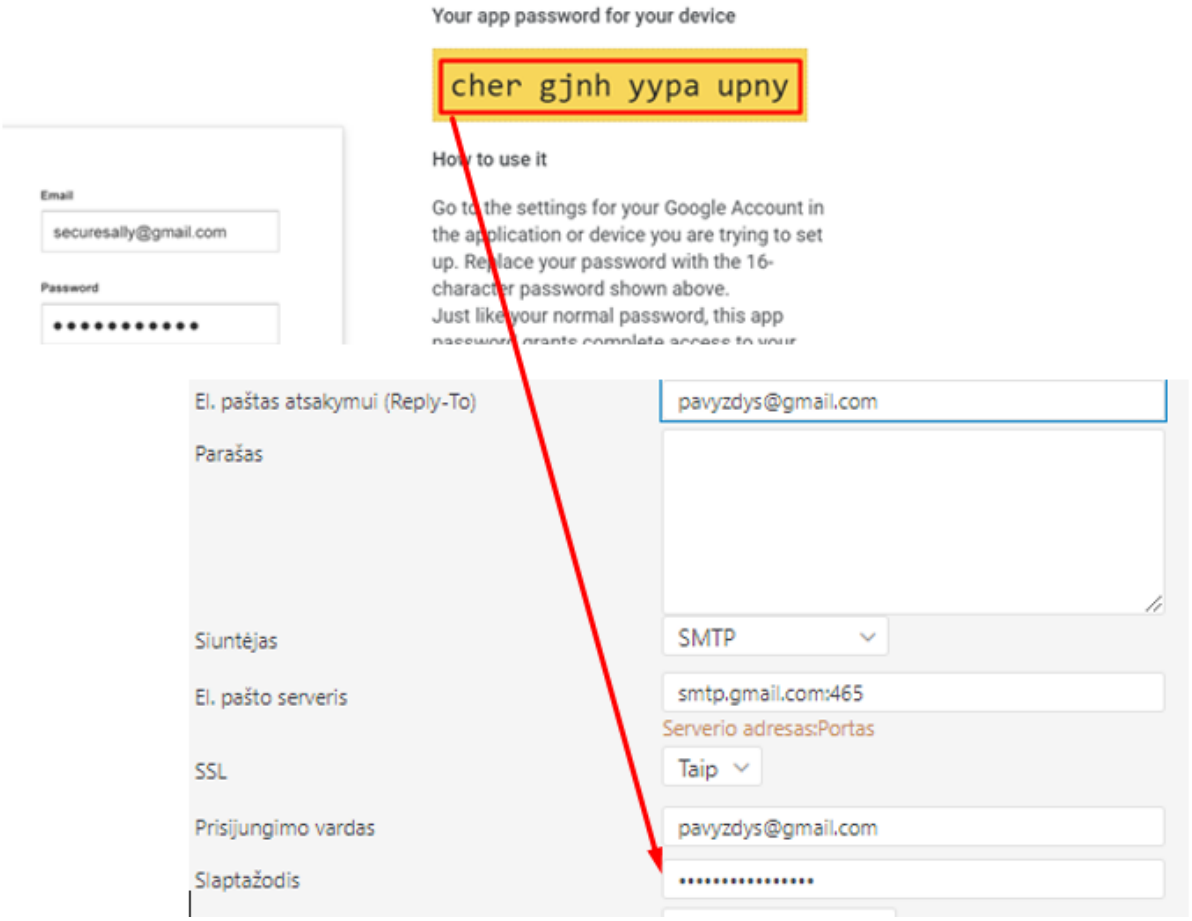
8.1 Google Gmail konfigūravimas

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

1. Einame į savo Google paskyrą (Security skiltis).
2. *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 atveju Directo sistemoje nustatykite pašto serverį: smtp.gmail.com:465, o SSL/TLS protokolui pasirinkite SSL.

8.2 Microsoft 365 nustatymas

Pastaba! Nuo 2026 m. balandžio mėn. Microsoft 365 turi būti konfigūruojama naudojant OAUTH metodą pagal žemiau pateiktas instrukcijas, kadangi tradicinis

prisijungimo vardas / slaptažodis / programėlės slaptažodis nebebus palaikomi.

Būtina sąlyga: Microsoft 365 naudotojas turi turėti įjungtą **Authenticated SMTP**.
Tai galima sukonfigūruoti Microsoft 365 administratoriaus lange — tiek visai organizacijai, tiek atskiriems naudotojams.

1. Įjunkite „Authenticated SMTP“ savo paskyrai

Tam reikalingos administratoriaus teisės. Jei jų neturite, paprašykite administratoriaus įjungti jums:

Atidarykite Microsoft 365 Admin Center ir pasirinkite:

➡ Vartotojai
➡ Aktyvūs vartotojai
➡ Pasirinkite savo vartotoja
➡ Paštas (Mail)
➡ Valdyti el. pašto programas (Manage email apps)

 Įsitikinkite, kad „Authenticated SMTP“ varnelė yra pažymėta

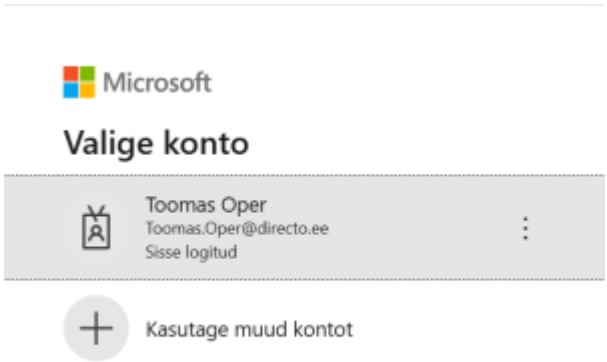
2. Reikalingi konfigūracijos duomenys

Konfigūracija atliekama kiekvienam naudotojui individualiai ir nustatoma vartotojo kortelėje, pasirinkus **Pagrindinis meniu → Asmeniniai → Vartotojas**.

Laukas	Reikšmė
Siuntėjas (Mail sender)	Microsoft 365 OAUTH
El. pašto serveris	smtp.office365.com:587
SSL/TLS	StartTLS / SSL / TLS
Prisijungimo vardas (Username)	Jūsų Microsoft 365 el. pašto adresas (pvz. name@company.com)

3. Prisijunkite su savo Microsoft 365 paskyra

- 1. Spauskite mygtuką „Authenticate Microsoft 365“
- 2. Atsidarys Microsoft prisijungimo langas



- 3. Prisijunkite naudodami įprastą Office 365 el. paštą ir slaptažodį.
- 4. Sėkmingai prisijungus langas automatiškai užsidarys ir būsite paprašyti suteikti leidimus.
- 5. Tuomet spauskite **Accept** (Sutinku).

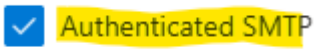
 Nuo šiol el. laiškai bus siunčiami saugiai per jūsų Office 365 paskyrą.

 Jei viskas atlikta sėkmingai, matysite pranešimą: **„Microsoft 365 has been authenticated“**

Senasis metodas (galios iki 2026 m. balandžio):

- **Serveris:** smtp.office365.com:25
- **SSL/TLS:** StartSSL / SSL / TLS
- Jei naudojamas **MFA (daugiafaktoris autentifikavimas)**, Directo sistemai turi būti sukurtas **programėlės slaptažodis (App password)**

Microsoft 365 Admin Center → **Users → Active Users → [User] → Mail → Manage email apps**

\ Čia turi būti pažymėta **Authenticated SMTP** \ 

Jei siunčiant pasirodo klaida ERR: 334, perskaitykite pateiktą instrukciją čia

8.3 Zonos nustatymai

Serveris priklauso nuo Zone nustatymų. Patikrinkite, koks yra jūsų domeno SMTP serveris čia– jis gali būti, pavyzdžiui, `smtp.zone.ee:465` arba `smtp.zone.eu:465`.
SSL/TLS: SSL

8.4 Viena konfigūracija, keli vartotojai

Pasitaiko atvejų, kai atsiranda poreikis nustatyti vienodą el. pašto siuntimo konfigūraciją visiems vartotojams (pavyzdžiui, kai įmonė turi savo el. pašto serverį).
Tam galima sukonfigūruoti nustatymus vienam vartotojui ir jo vartotojo kodą nustatyti kaip **Sistemos kodą**: „Mail sending user code – šio vartotojo SMTP konfigūracija naudojama kaip pagrindas el. laiškų siuntimui“.

Tokiu atveju visi vartotojai automatiškai perima tą pačią konfigūraciją.
Vis dėlto, išlieka galimybė atskirai nustatyti tik konkretaus vartotojo parametrus, pavyzdžiui, vartotojo vardą ir slaptažodį (šiuo atveju serverio informacija jau imama iš bendrinės vartotojo konfigūracijos).

8.5 Directo – „Reply-To“ nustatymas

Įprastai, el. laiškų siuntimo **FROM** adresas arba siuntėjas, visada yra tas el. pašto adresas, kuris nurodytas vartotojo kortelėje.
Jeigu pageidaujama, siuntimo formatą galima pakeisti taip, kad siuntėjo adresas būtų **company_name@event.data.directo.ee**, o **reply-to** lauke būtų naudojamas vartotojo kortelėje nurodytas el. pašto adresas. Tam vartotojo kortelėje reikia atsidaryti:

`Pagrindinis meniu → Nustatymai → Asmeniniai nustatymai → Vartotojas, pasirinkti lauką Siuntėjas ir nustatyti reikšmę Directo-Reply-To.`

Tokiu atveju gavėjas matys, kad siuntėjo adresas yra Directo, tačiau atsakant į tokį laišką, atsakymas

vis tiek bus nukreiptas į el. pašto adresą (nurodytą „reply-to“ antraštėje).

Ši parinktis gali būti tinkama, kai nenorima keisti SPF įrašo (leidžiant Directo sistemai būti autorizuotai siųsti laiškus įmonės vardu), tačiau dėl SPF apribojimų iš Directo siunčiami laiškai patenka į šlamštą arba visai nebūna pristatomi.

Siuntėjo adresas šiuo atveju yra Directo „event“ pašto dėžutės adresas. Tai reiškia, kad jei laiško išsiųsti nepavyksta ir jis „grįžta atgal“, klaidos pranešimas taip pat bus nukreiptas į šį siuntėjo adresą. Tokiu atveju pranešimas atsidurs Directo „Event“ modulyje, kuriame bus galima nustatyti klaidos priežastį.

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

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

Last update: **2025/11/27 08:05**