

Table of Contents

Instrukcja konfiguracji wysyłki wiadomości e-mail w Directo	3
Domyślne ustawienia	3
Gdzie skonfigurować ustawienia?	3
Parametry do ustawienia	4
Odpowiedzialność użytkownika	5
Adresy IP do whitelisty	5
Konfigurowanie konta Google Gmail	5
Kroki konfiguracji	5
Dodatkowa informacja	6
Konfigurowanie konta Microsoft 365	6
Warunek wstępny	7
Jak włączyć uwierzytelniony SMTP?	7
Konfiguracja w Directo	7
Proces uwierzytelnienia	7
Dodatkowe uwagi	8
Jedna konfiguracja, wielu użytkowników	8
Odpowiedź bezpośrednia	8

Instrukcja konfiguracji wysyłki wiadomości e-mail w Directo

Domyślne ustawienia

Directo wysyła wiadomości e-mail z serwera:

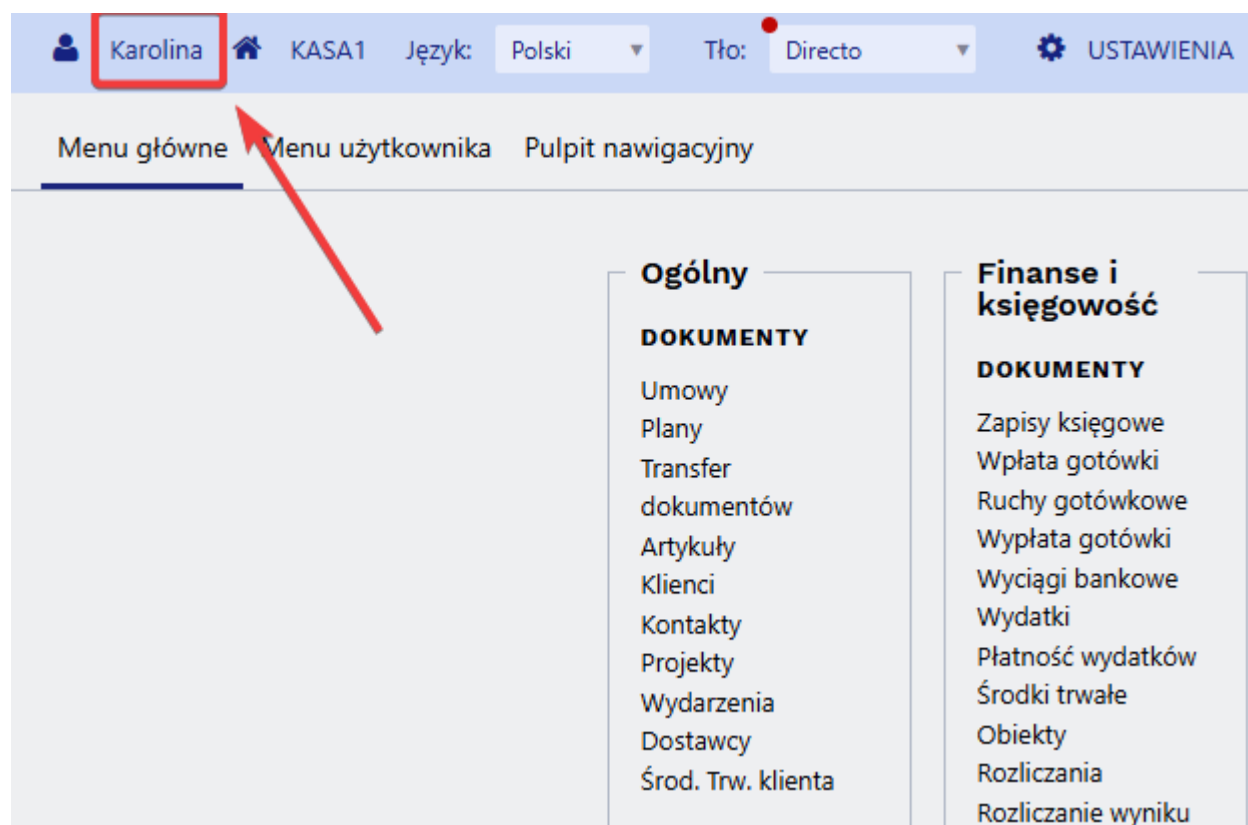
`directo.gate.ee (90.190.150.212)`

W większości przypadków użytkownik nie musi zmieniać sposobu wysyłki. Jednak w szczególnych sytuacjach możliwość określenia własnego serwera SMTP jest bardzo pomocna. Po włączeniu tej opcji aktywują się również wszystkie usługi wymagające modułu masowej wysyłki e-mail (np. masowa wysyłka faktur, listów do klientów).

Gdzie skonfigurować ustawienia?

Konfiguracja jest indywidualna dla użytkownika (można ją też ustawić [globalnie](#)) i odbywa się w:

Menu główne → Ustawienia → Ustawienia własne → Użytkownik lub z Menu głównego wciskając na nazwę użytkownika



Parametry do ustawienia

Aby ustawienia były widoczne, w polu **Nadawca wiadomości e-mail** należy wybrać opcję **SMTP**.

The screenshot shows the 'Ustawienia własne > Użytkownik' (Personal Settings > User) page. It is divided into two main sections: 'Informacja' (Information) and 'Domyślne' (Defaults). The 'Informacja' section contains fields for 'Nazwa' (Name) set to 'Directo HELP' and 'Grupa' (Group) set to 'SUPER_PL'. The 'Domyślne' section contains fields for 'Nr. Tel. biura' (Office phone) set to '+4800000', 'Nr. Tel.' (Phone) set to '+4823000', 'E-mail' set to 'info@directo.pl', 'Kopia ukryta (BCC)' (Hidden copy (BCC)), 'Odpowiedź do (Reply To)' (Reply to) set to 'HELP', and 'Podpis' (Signature). Below these, the 'Nadawca wiadomości' (Message sender) dropdown is set to 'SMTP'. A red box highlights the 'SMTP' option, and a red arrow points to a sub-section containing 'Serwer poczty mailowej i port' (Email server and port), 'SSL/TLS', 'Nazwa użytkownika' (Username), and 'Hasło' (Password). The 'Serwer poczty mailowej i port' field is set to 'test.gmail.cm:465', 'SSL/TLS' is set to 'SSL', 'Nazwa użytkownika' is set to 'test@gmail.com', and 'Hasło' is masked with dots.

1. **Serwer poczty mailowej i port.** Dostępne porty: 25, 465, 587.
2. **SSL/TLS.** Jeśli wymagana jest szyfrowana komunikacja, wybierz zgodnie z wymaganiami serwera SMTP.
 - Standardowo:
 - Port 465 → SSL
 - Porty 25 i 587 → StartSSL/SSL/TLS
 - Opcja **NIE** oznacza brak szyfrowania (połączenie „otwarte”).
3. **Nazwa użytkownik.** Login konta e-mail.
Uwaga: Jeśli serwer nie wymaga uwierzytelniania, pozostaw pole puste.

4. **Hasło.** Hasło do konta e-mail.

Odpowiedzialność użytkownika

Za błędy i niedostarczenie wiadomości odpowiada użytkownik korzystający z własnych ustawień serwera.

Istnieje ryzyko zablokowania konta e-mail przez serwery odbiorcze.

Adresy IP do whitelisty

Jeśli serwer SMTP ogranicza dostęp na podstawie adresu IP, należy dodać:

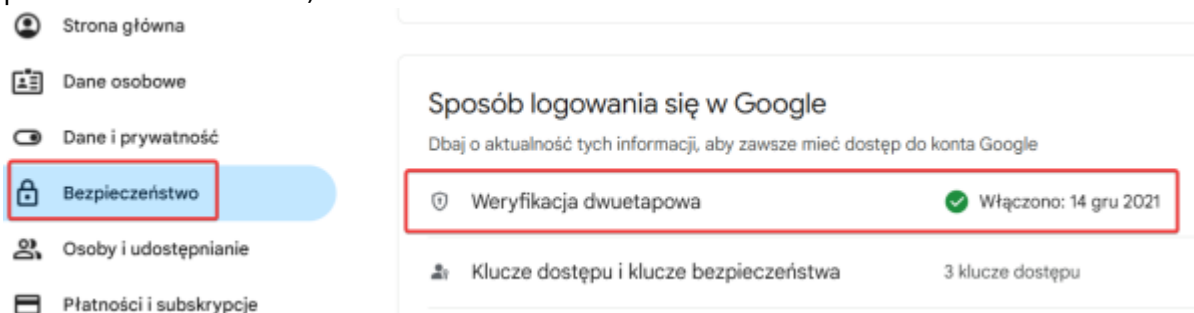
```
90.190.150.210
90.190.150.211
90.190.150.212
90.190.150.213
90.190.150.219
90.190.150.82
```

Konfigurowanie konta Google Gmail

Aby wysyłać wiadomości e-mail z konta Gmail przez Directo, należy przejść jednorazową procedurę utworzenia **hasła aplikacji** i użyć go w konfiguracji SMTP w Directo.

Kroki konfiguracji

1. **Włącz weryfikację dwuetapową w Google.** Hasło aplikacji można utworzyć tylko wtedy, gdy włączona jest weryfikacja dwuetapowa.
 - Zaloguj się do swojego konta [Google](#).
 - Przejdź do ustawień zabezpieczeń i włącz weryfikację dwuetapową (najprostsza metoda to potwierdzenie SMS-em).



- Po zakończeniu wróć do strony ustawień zabezpieczeń.
2. **Utwórz hasło aplikacji.** W sekcji wybierz:
 - **Nazwę aplikacji:** np. Poczta

- Kliknij **Utwórz**.

← Hasła do aplikacji

Hasła do aplikacji ułatwiają logowanie się na konto Google w starszych aplikacjach i usługach, które nie obsługują nowoczesnych standardów zabezpieczeń.

Używanie haseł do aplikacji jest mniej bezpieczne niż korzystanie z aktualnych aplikacji i usług, które obsługują nowoczesne standardy zabezpieczeń. Zanim utworzysz hasło do aplikacji, sprawdź, czy aplikacja rzeczywiście wymaga go na potrzeby logowania.

[Więcej informacji](#)

Nie masz haseł do aplikacji.

Aby utworzyć nowe hasło do aplikacji, wpisz poniżej jej nazwę...

Nazwa aplikacji

Utwórz

- Otrzymasz 16-znakowy kod (wyświetlany ze spacjami).



Uwaga: Skopiuj kod i wprowadź go w Directo **bez spacji**.

3. Wprowadź dane w Directo

- **Serwer SMTP:** smtp.gmail.com:465
- **SSL/TLS:** SSL
- **Użytkownik:** Twój adres Gmail
- **Hasło:** Utworzone hasło aplikacji (bez spacji).

Dodatkowa informacja

Wiadomości wysyłane z konta Gmail będą widoczne w folderze **Elementy wysłane** w Gmailu.

Konfigurowanie konta Microsoft 365



UWAGA! Od kwietnia 2026 r. Microsoft wycofuje obsługę tradycyjnego logowania SMTP

opartego na **użytkownik/hasło/hasło aplikacji**.

Wysyłka e-maili musi być skonfigurowana z wykorzystaniem metody **OAUTH**.

Warunek wstępny

- Konto Microsoft 365 musi mieć włączoną funkcję **Uwierzytelniony SMTP**.
- Opcję tę można ustawić w **Microsoft 365 Admin Center** globalnie lub dla każdego użytkownika.

Jak włączyć uwierzytelniony SMTP?

1. Zaloguj się do **Microsoft 365 Admin Center**.
2. Wybierz:

Użytkownicy → Aktywni użytkownicy → [Twój użytkownik] → Poczta/E-mail → Zarządzaj aplikacjami e-mailowymi

3. ☐ Upewnij się, że opcja **Uwierzytelniony SMTP** jest zaznaczona.

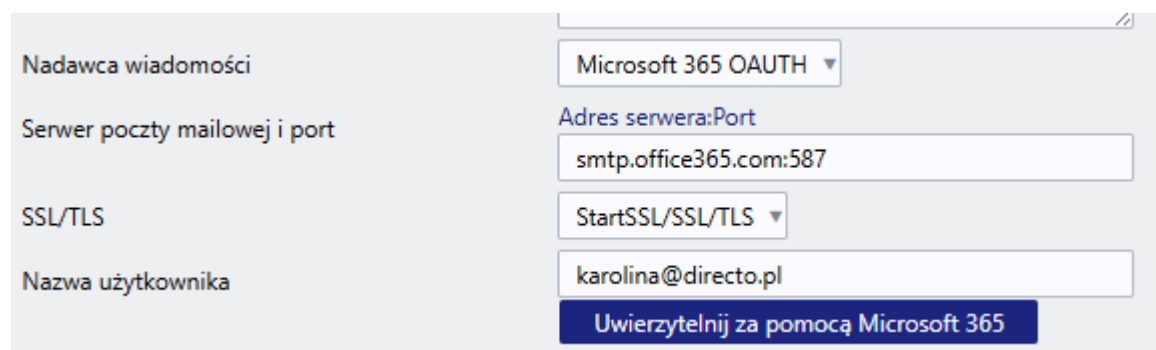
Konfiguracja w Directo

Ścieżka do ustawień: [Ustawienie Directo](#)

W polu **Nadawca e-maila** wybierz: **Microsoft 365 OAUTH**

Parametry

Opis	Wartość
Nadawca e-maila	Microsoft 365 OAUTH
Serwer poczty mailowej i port	smtp.office365.com:587
SSL/TLS	StartTLS / SSL / TLS
Nazwa użytkownika	Twój adres e-mail w usłudze Microsoft 365 (np. nazwa@firma.pl)



The screenshot shows a configuration window with the following fields and values:

- Nadawca wiadomości:** Microsoft 365 OAUTH (selected in a dropdown)
- Serwer poczty mailowej i port:** smtp.office365.com:587
- SSL/TLS:** StartSSL/SSL/TLS (selected in a dropdown)
- Nazwa użytkownika:** karolina@directo.pl
- Buttons:** "Uwierzytelnij za pomocą Microsoft 365" (highlighted in blue)

Proces uwierzytelnienia

1. Kliknij przycisk „**Uwierzytelnij za pomocą Microsoft 365**”.

2. Otworzy się okno logowania Microsoft.
3. Zaloguj się, używając swojego adresu e-mail i hasła Microsoft 365.
4. Potwierdź wymagane uprawnienia („Zgadzam się”).
5. ☐ Jeśli wszystko przebiegło pomyślnie, zobaczysz komunikat:
„Microsoft 365 został uwierzytelniony”.

Dodatkowe uwagi

- Jeśli opcja uwierzytelnienia nie działa, sprawdź:
 - Czy włączono **SMTP Auth** w Microsoft 365 Admin Center.
 - Czy użytkownik ma odpowiednie uprawnienia.
- Po migracji na OAUTH nie będzie możliwe używanie haseł aplikacji. ☐ Jeśli wszystko przebiegło pomyślnie, zobaczysz komunikat: „Microsoft 365 został uwierzytelniony”

Jedna konfiguracja, wielu użytkowników

Zdarzają się sytuacje (na przykład firma posiada własny serwer pocztowy), w których konieczne jest przypisanie tej samej konfiguracji wszystkim użytkownikom podczas wysyłania. W tym celu można przypisać ustawienia jednemu użytkownikowi, a następnie przypisać dany kod użytkownika jako reprezentację systemu. Meili saatmise kasutaja kood - antud kasutaja SMTP konfiguratsioon on aluseks meilide saatmisele. W rezultacie wszyscy użytkownicy automatycznie otrzymują tę samą konfigurację. Możliwe jest jednak przypisanie na przykład tylko nazwy użytkownika i hasła dla każdego użytkownika z osobna (w takim przypadku serwer będzie już pochodził z globalnej konfiguracji użytkownika).

Odpowiedź bezpośrednia

Zazwyczaj podczas wysyłania wiadomości e-mail adres nadawcy (FROM) to zawsze adres e-mail przypisany do karty użytkownika. W razie potrzeby format wysyłania wiadomości e-mail można zmienić tak, aby adres nadawcy to `companyname@event.data.directo.ee`, a nagłówek „Repeat-to” to adres e-mail karty użytkownika. W tym celu należy **w menu głównym karty użytkownika → Osobiste → Użytkownik** ustawić opcję **„Directo-Reply-to”** w polu **„Nadawca wiadomości e-mail”**.

W takim przypadku adres nadawcy będzie widoczny dla odbiorcy jako adres Directo, ale jeśli odpowiesz na wiadomość wysłaną w ten sposób, adres odbiorcy odpowiedzi nadal zostanie przypisany do prawidłowego adresu (tego, który pierwotnie podano w nagłówku odpowiedzi).

Opcja ta może okazać się przydatna w sytuacji, gdy nie chcesz zmieniać rekordu SPF (zezwolić firmie Directo na bycie nadawcą domeny firmy), ale po wysłaniu wiadomości e-mail z usługi Directo wiadomości trafiają do spamu lub w ogóle nie są dostarczane, ponieważ obowiązuje [SPF piirang](#).

Adres, na który jest wysyłana, to w zasadzie [Directo sündmuse postkasti aadress](#). To z kolei oznacza, że jeśli wiadomość e-mail nie zostanie wysłana i „zwróci się”, ponieważ w przypadku błędów odpowiedź i tak zostanie wysłana bezpośrednio na adres nadawcy, dotrze ona do modułu Zdarzenia Directo jako zdarzenie, gdzie można już zidentyfikować przyczynę błędu.

From:

<https://wiki.directo.ee/> - **Directo Help**

Permanent link:

https://wiki.directo.ee/pl/meiliserveri_seadistamine?rev=1762855724

Last update: **2025/11/11 12:08**

