

Instrukcja instalacji i konfiguracji uwierzytelniania wieloskładnikowego (MFA) Microsoft Authenticator

Wersja dokumentu: 1.0

Odpowiedzialny za dokument: PL_IT

Data aktualizacji: 19.11.2024, Michał Horbiński



Wstęp

MFA czyli uwierzytelnianie dwuskładnikowe to dodatkowy element zabezpieczający konto przed nieuprawnionym dostępem.

W przypadku tej instrukcji, będzie zastosowany **Microsoft Authenticator** w wersji na urządzenia mobilne z systemem Android i iOS.

Zasada działania tego zabezpieczenia:

Próbując się zalogować na różne konta w DaVita, należy uruchomić na telefonie Microsoft Authenticator i w programie do którego się logujemy wpisać wyświetlany na telefonie token logowania.

Token to jednorazowy kod zmieniający się co określony czas.

Jest on przypisany do użytkownika i konta. Wpisuje się go w momencie logowania do przypisanego konta.

Mogą wystąpić również inne sposoby uwierzytelniania np. pole wyboru cyfry która jest zgodna z tą wyświetlaną w aplikacji, lub wpisanie numeru dostarczonego wraz z SMSem.



Instalacja

Microsoft

Authenticator

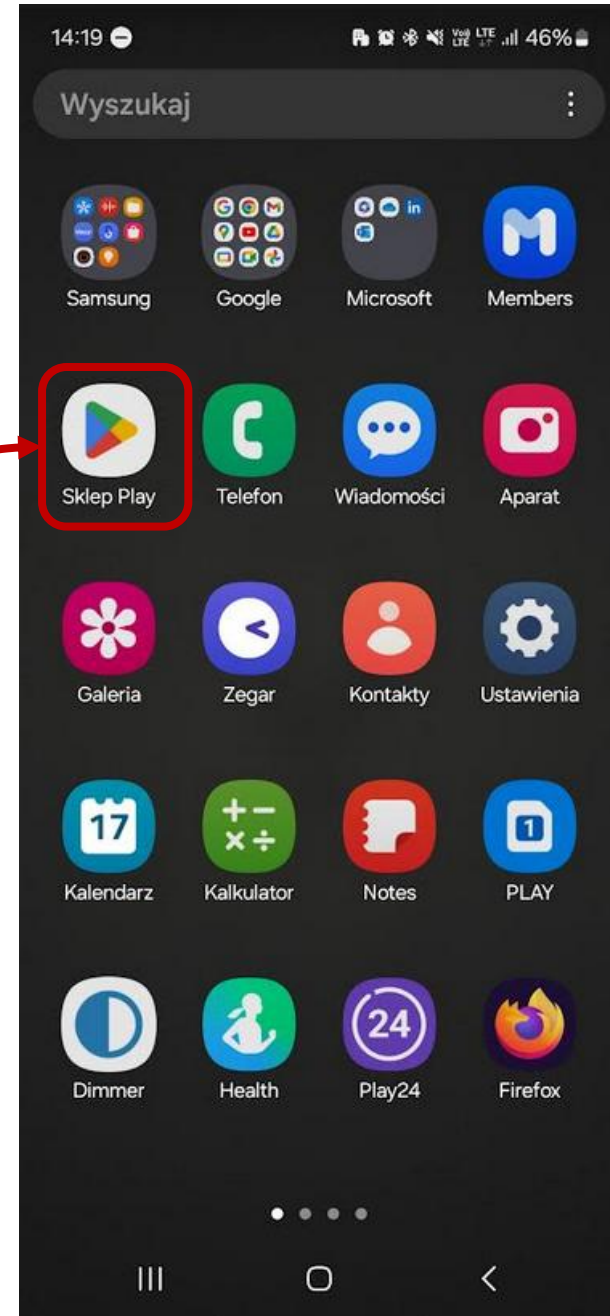
Android



Instalacja Android

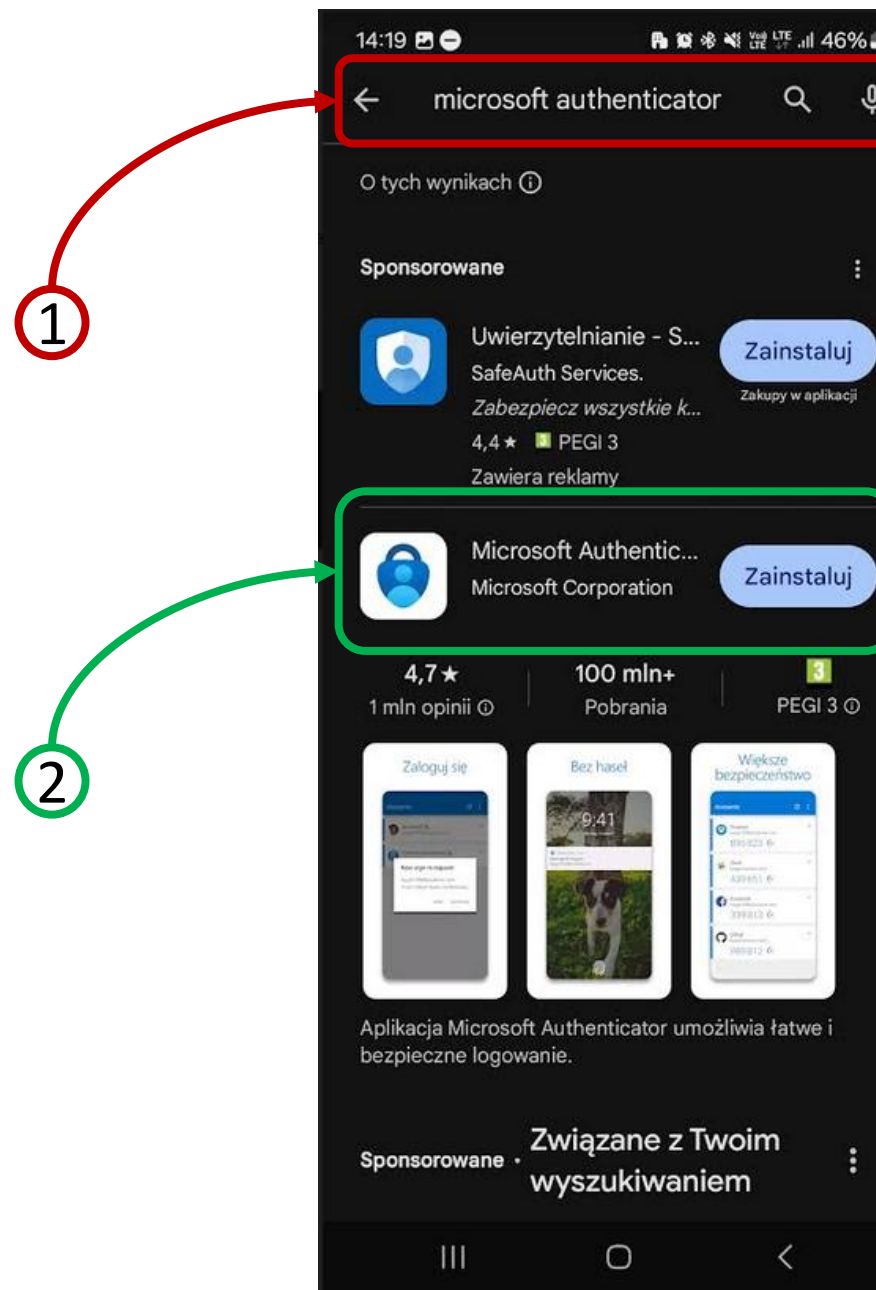
1. Będąc w profilu firmy wchodzimy w „Sklep Play” ① w celu pobrania aplikacji „Microsoft Authenticator”

①



Instalacja Android

1. Wyszukujemy przy pomocy lupy ① „Microsoft Authenticator”
2. Instalujemy „Microsoft Authenticator” ② postępując zgodnie z komunikatami na ekranie.



Instalacja

Microsoft

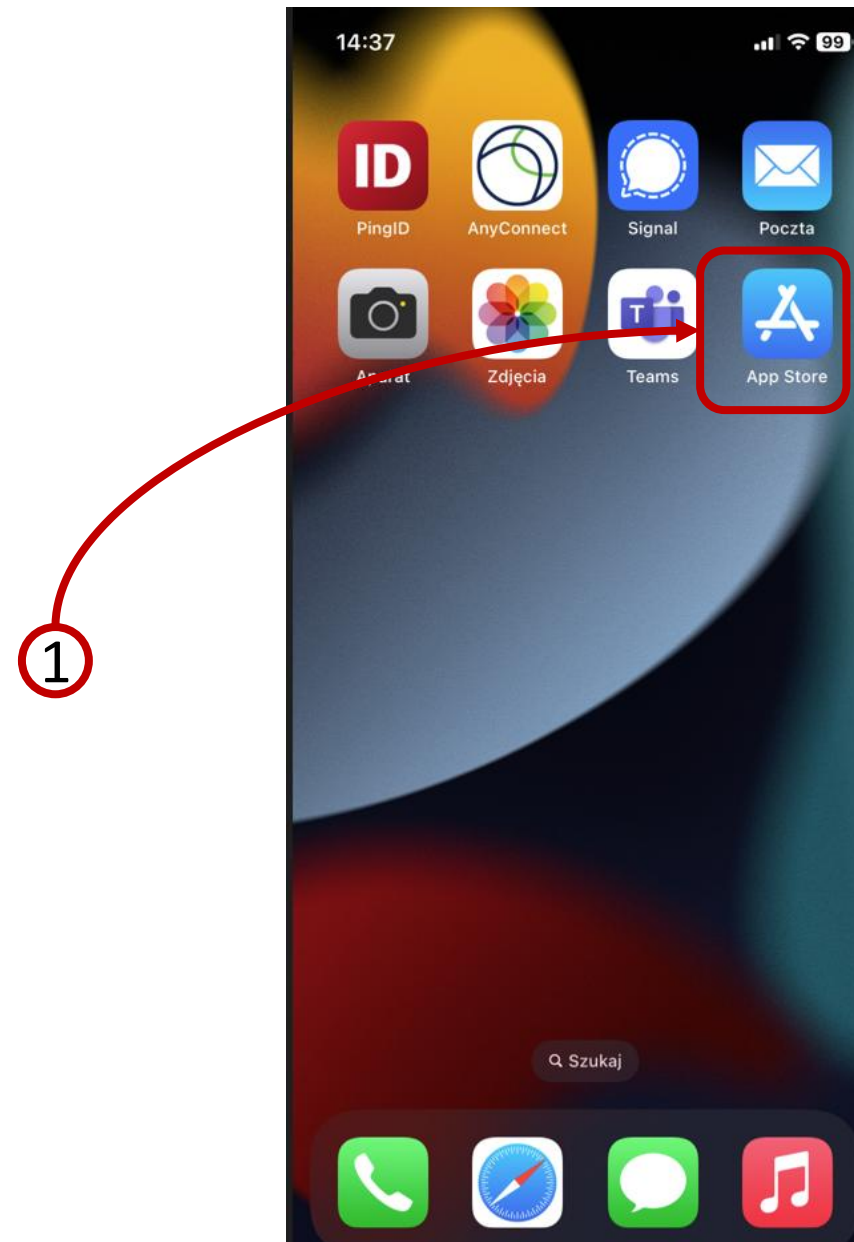
Authenticator

iOS



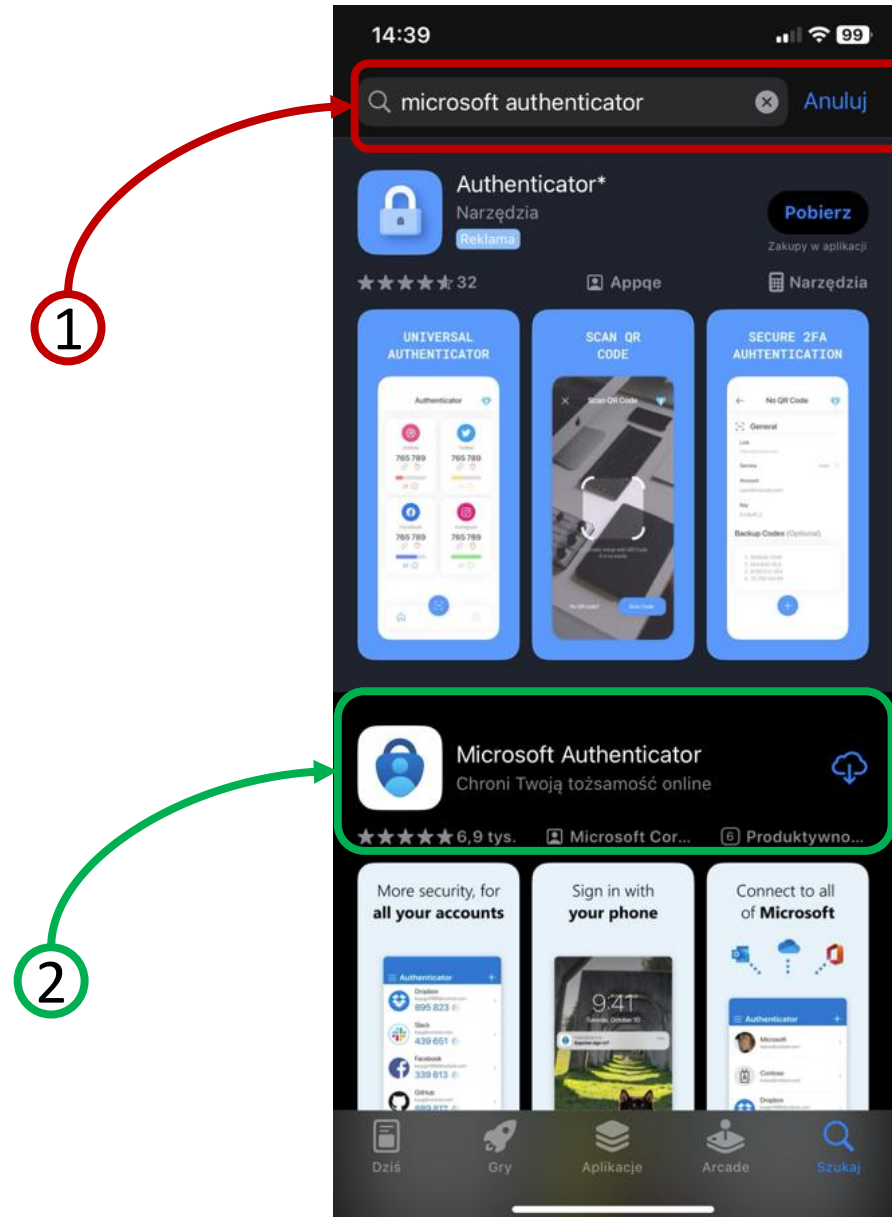
Instalacja iOS

1. Wchodzimy w „App Store”
w celu pobrania aplikacji
„Microsoft Authenticator” ①



Instalacja iOS

1. Wyszukujemy przy pomocy lupy **1** „Microsoft Authenticator”
2. Instalujemy „Microsoft Authenticator” **2** postępując zgodnie z komunikatami na ekranie.



Aktywacja



Aktywacja MFA

1. Na ekranie powitania aplikacji Microsoft Authenticator należy dotknąć „Akceptuj” ①

①



Aktywacja MFA

1. Na drugim ekranie aplikacji Microsoft Authenticator należy dotknąć „Kontynuuj” ①

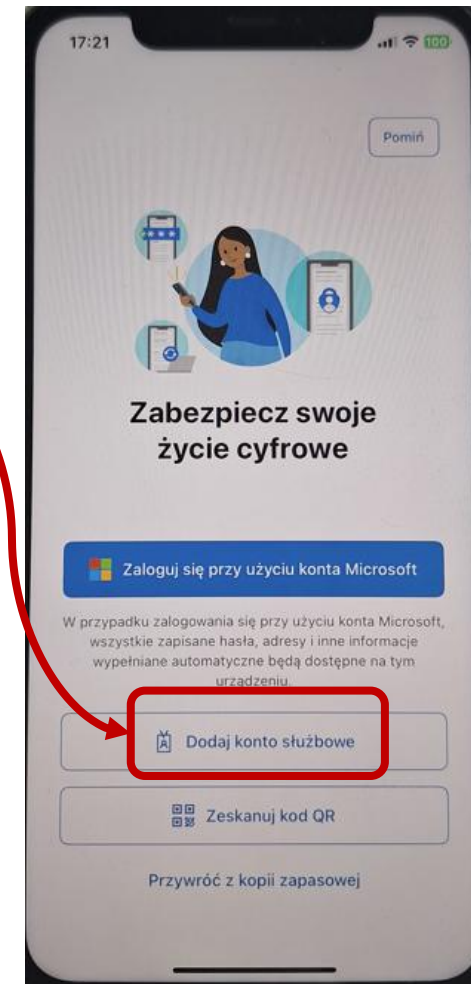
①



Aktywacja MFA

1. Na trzecim ekranie aplikacji Microsoft Authenticator należy dotknąć „Dodaj konto służbowe” ①

①



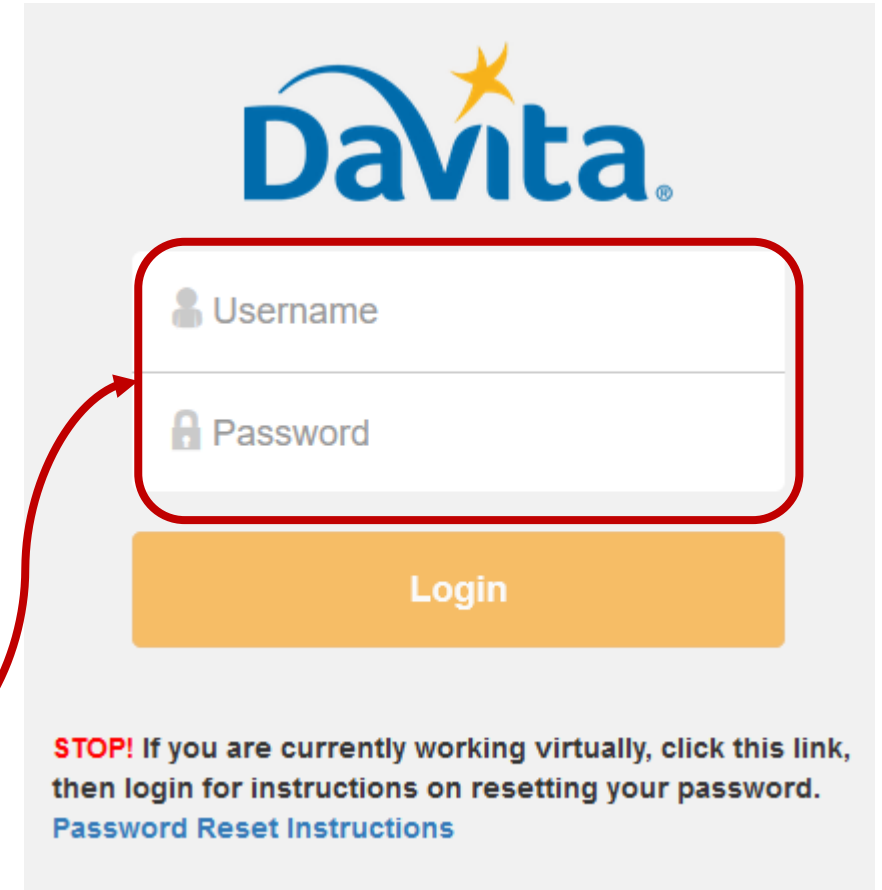
Aktywacja MFA

1. Zostaniemy przeniesieni na stronę logowania DaVita, gdzie należy podać nasze login i hasło domenowe (to samo które jest używane przy logowaniu się do komputera). ①

UWAGA!

By zalogować się do systemu należy być w sieci firmowej!

①



DaVita

Username

Password

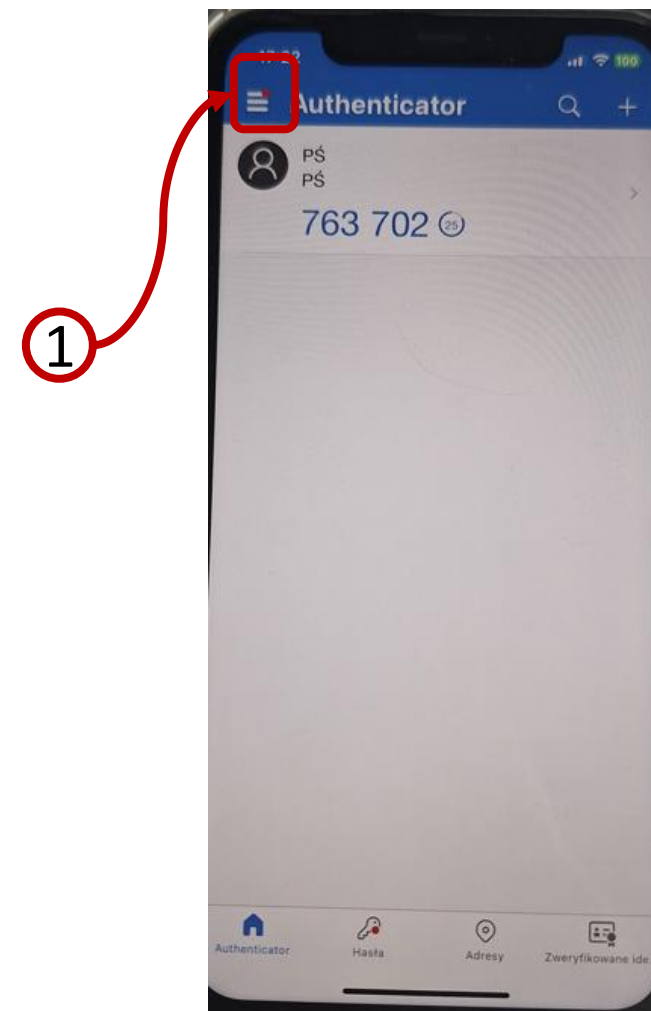
Login

STOP! If you are currently working virtually, click this link, then login for instructions on resetting your password.
[Password Reset Instructions](#)



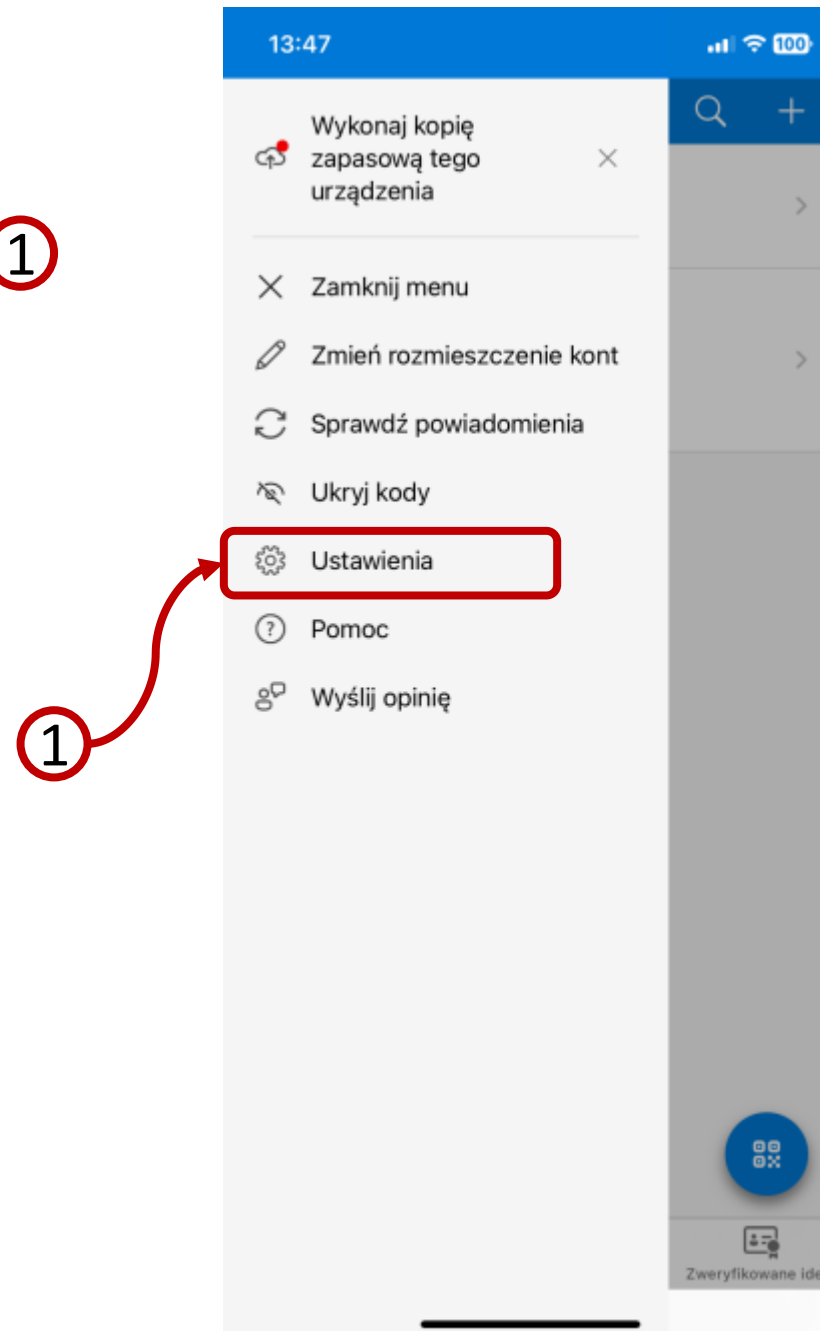
Rejestracja urządzenia

1. Pod instalacji i zalogowaniu, należy zarejestrować urządzenie.
2. W tym celu na głównej stronie aplikacji należy wejść w menu opcji. ①



Rejestracja urządzenia

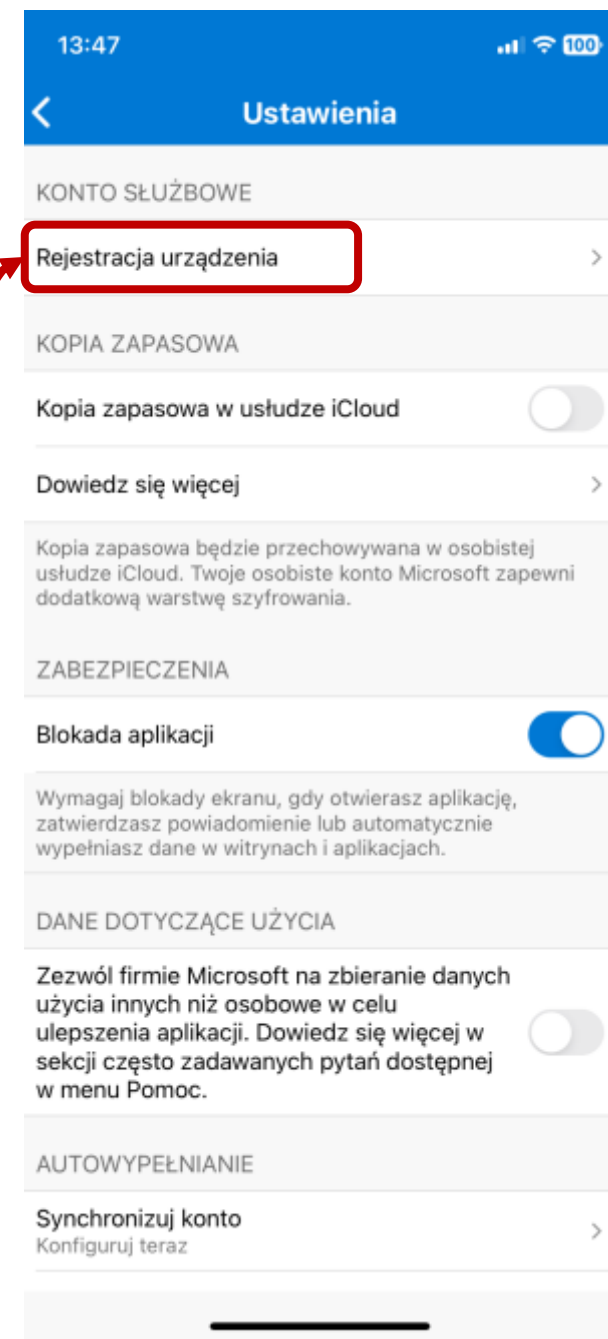
1. W menu należy wybrać „Ustawienia”. ①



Rejestracja urządzenia

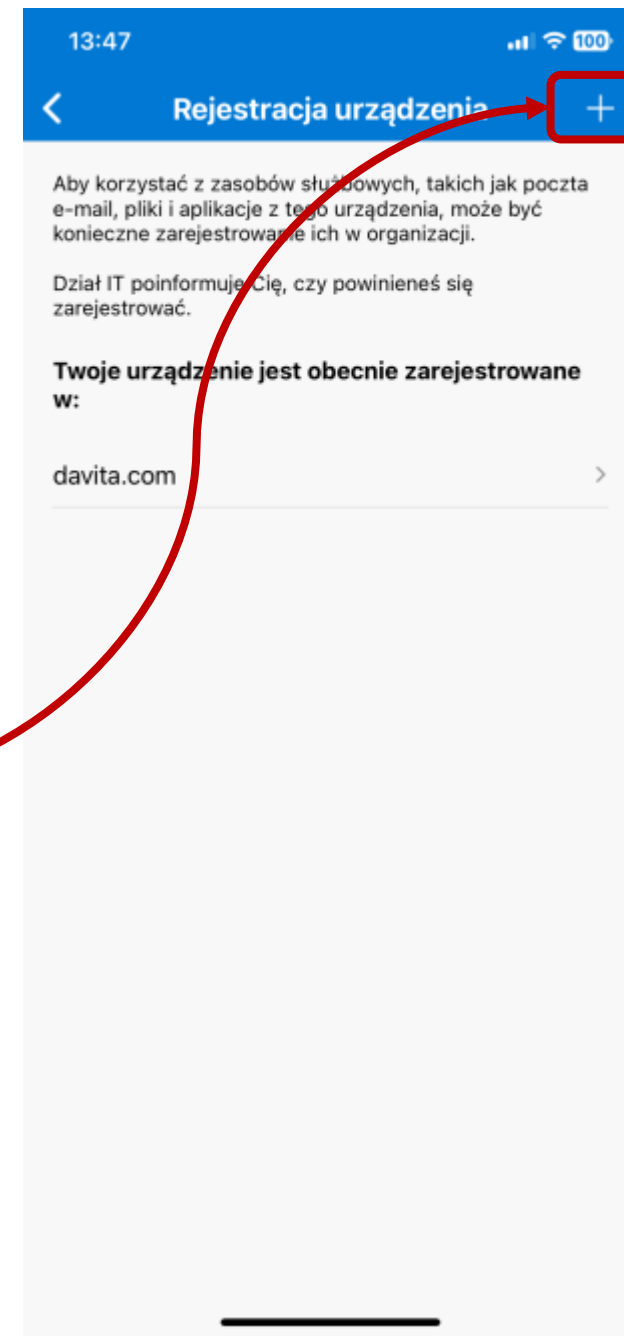
1. W menu ustawienia wybrać "Rejestracja urządzenia".¹

1



Rejestracja urządzenia

1. W menu rejestracji należy kliknąć "+". ①



Rejestracja urządzenia

1. W należy wpisać swój służbowy e-mail ①
„@davita.com” ②

Nacisnąć „Zarejestruj urządzenie”
a następnie postępować z instrukcjami na
ekranie.

13:47 100%

< Rejestracja urządzenia

Wprowadź adres e-mail używany w organizacji:

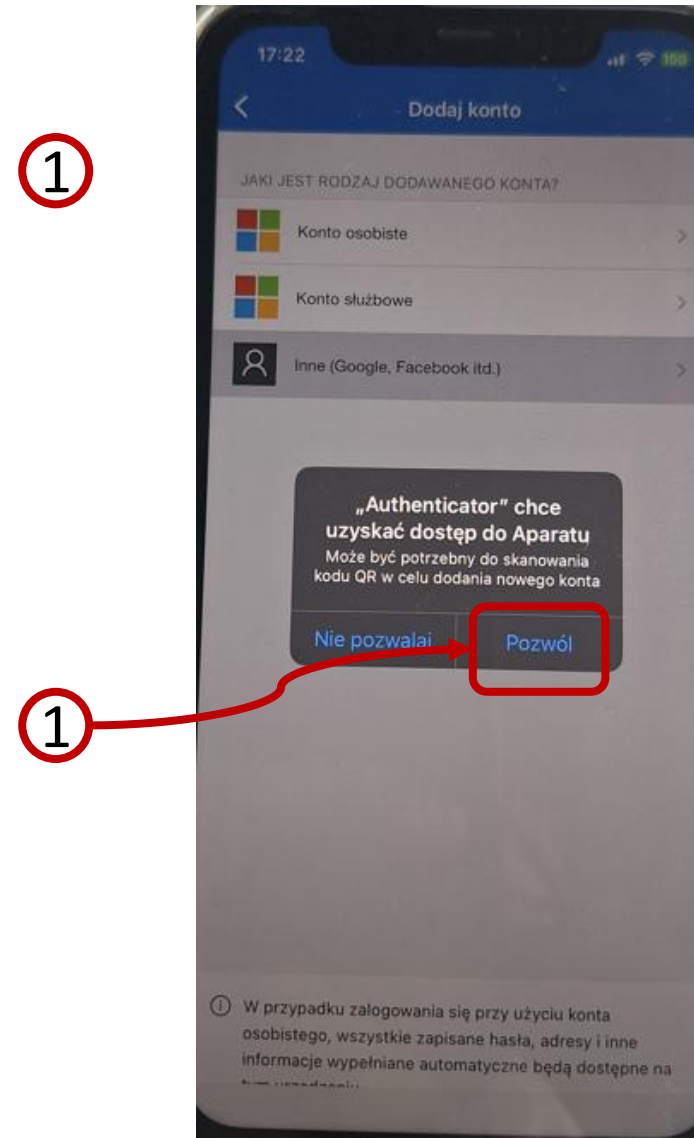
Adres e-mail organizacji

Zarejestruj urządzenie



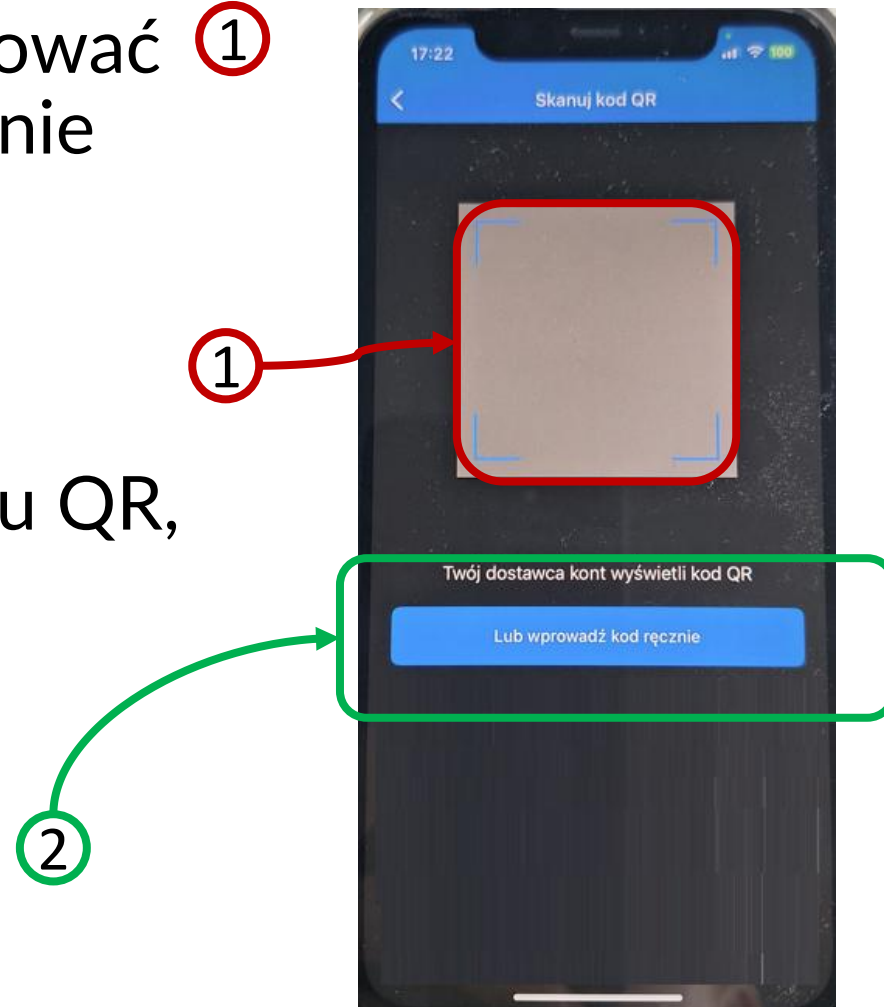
Aktywacja MFA

1. W przypadku pytania o dostęp do kamery/aparatu – należy się zgodzić! ①



Aktywacja MFA

1. Włączy się aparat. Należy zeskanować kod QR wyświetlający się na ekranie komputera, który uruchomiliśmy wcześniej. ①
2. Jeżeli nie można zeskanować kodu QR, należy wprowadzić ręcznie. ②



Aktywacja MFA

1. Konto powinno dodać się do aplikacji i wyświetlać się na głównej stronie.

1

