

**Instrukcja logowania
wieloskładnikowego (MFA)
przy pomocy PINGID**

Wstęp

Celem tej instrukcji jest zaprezentowanie krok po kroku procesu logowania wieloskładnikowego (MFA) wykorzystywanego między innymi do logowania do Intranetu (<https://intranet.davita.com>) przy użyciu aplikacji PingID. PingID to narzędzie, które umożliwia uwierzytelnianie wieloskładnikowe, co oznacza, że oprócz tradycyjnego hasła, wykorzystuje się dodatkowy czynnik bezpieczeństwa, taki jak kod jednorazowy generowany na urządzeniu mobilnym.

Instrukcja ta ma na celu pomóc użytkownikom w bezproblemowym dostępie do Intranetu poprzez korzystanie z aplikacji PingID. W kolejnych sekcjach zostaną opisane niezbędne kroki, które należy podjąć, aby zalogować się do intranetu za pomocą PingID. Ważne jest, aby pamiętać, że instrukcja ta jest ogólnym przewodnikiem i może się różnić w zależności od konfiguracji systemu lub wersji aplikacji PingID.

SZYFROWANIE DANYCH



PRYWATNY KLUCZ

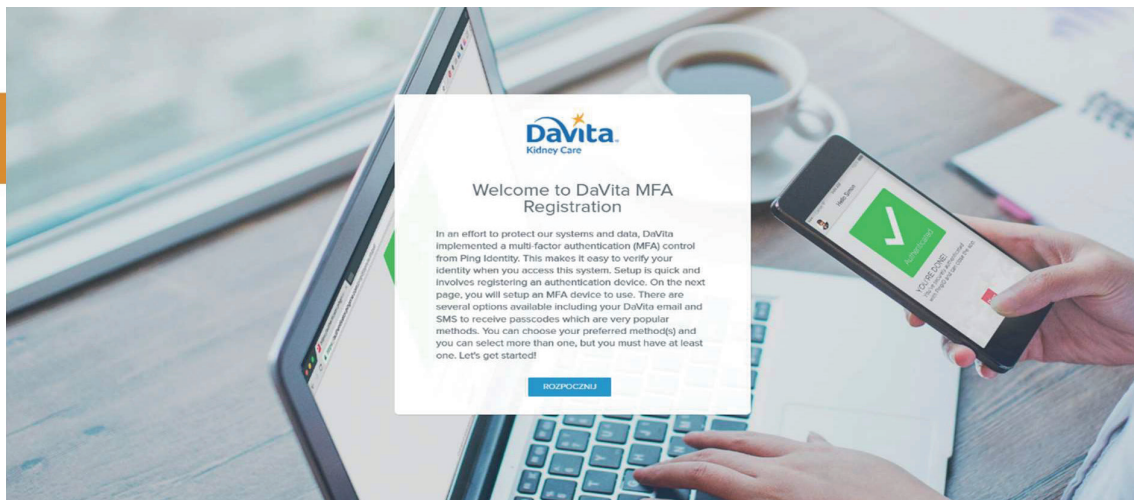


OCHRONA INTERNETU



Pierwsze logowanie i ustawienie PingID

Po wejściu na stronę Intranetu i zalogowaniu swoim loginem i hasłem (tymi samymi których używamy w celu zalogowania się do komputera) strona przekieruje nas do rejestracji MFA.



Po kliknięciu przycisku rozpocznij przejdziemy na stronę dodawania nowego urządzenia uwierzytelniającego. W tym miejscu wybieramy metodę jaką chcemy uwierzytelniać logowanie do Intranetu.



Dodaj nowe urządzenie



Aplikacja mobilna PingID

Dla maksymalnej wygody użytkownika zainstaluj PingID i zeskanuj kod QR, aby sparować swoje urządzenie mobilne. Jeśli to konieczne, możesz też wprowadzić kod parowania ręcznie.



Klucz parowania: 2799 6719 5304



Inne metody uwierzytelniania



SMS



E-mail



Desktop



Aplikacja uwierzytelniająca

Uwierzytelnianie za pomocą telefonu z systemem IOS lub Android

Uwierzytelnianie z wykorzystaniem aplikacji zainstalowanej na telefonie jest preferowaną metodą, gdyż daje największy poziom bezpieczeństwa. Możemy zainstalować aplikację PingID na dwa sposoby. Używając odnośnika do sklepu Apple Store i sklepu Google Play który znajduje się pod kluczem parowania lub wchodząc w aplikację Apple Store dla IOS lub Google Play dla Androida a następnie ręczne wyszukanie oraz zainstalowanie aplikacji PingID.

3

Dodaj nowe urządzenie

**Aplikacja mobilna PingID**
Dla maksymalnej wygody użytkownika zainstaluj PingID i zeskanuj kod QR, aby sparować swoje urządzenie mobilne. Jeśli to konieczne, możesz też wprowadzić kod parowania ręcznie.



Klucz parowania: 2799 6719 5304

Available for iPhone & iPad

Available for Android

Inne metody uwierzytelniania

SMS

E-mail

Desktop

Aplikacja uwierzytelniająca

Zapisz klucz parowania podany poniżej kodu QR. Będzie potrzebny potem w celu uwierzytelnienia urządzenia na telefonie. Teraz trzeba potwierdzić Terms of Service, następnie dwa razy nacisnąć przycisk kontynuuj.

4

Terms of Service
The Ping Identity Corporation ("Ping", "we", or "our") mobile device or computer application and related software (the "Application", or the "App") is to be used exclusively in connection with Ping's PingOne or PingID service together with the Application, the "Service". Ping offers the Service only to legal entities ("Customers") who have entered into a binding agreement with Ping as "Customer Agreement".

You may only use the Service, including the Application, if you are an authorized user of a Customer. Such authorized users, and any others who download, access, use, purchase and/or subscribe to the Service collectively or individually "you" or "users", must do so under the following terms and conditions of use.

THIS END USER LICENSE AGREEMENT (THIS "AGREEMENT") SHALL CONSTITUTE THE ENTIRE AGREEMENT BETWEEN YOU AND PING CONCERNING YOUR USE OF THE SERVICE. BY USING THE SERVICE, YOU AGREE TO AND ACCEPT THIS AGREEMENT. YOU MAY USE THE SERVICE ONLY IN ACCORDANCE WITH THIS AGREEMENT. IF YOU DO NOT AGREE WITH ALL THE TERMS OF THIS AGREEMENT, YOU SHALL NOT BE ENTITLED TO USE THE SERVICE.

1. SERVICE AND RESTRICTIONS

1.1 Ping shall provide the Service, including the Application, to you only for the term of the Customer Agreement (the "Term"). During the Term or otherwise, you shall not (i) modify, disassemble, decompile or reverse engineer the Service, including the Application, except to the extent that such restriction is expressly prohibited by law; (ii) share, rent, lease, loan, resell, sublicense, distribute or otherwise transfer the Service to any third party or

Accept

**Important**
To securely authenticate with PingID, you will need to approve the following prompts: push notifications, camera and location.

I Understand

Welcome to PingID
General Overview
PingID is a security application that's used to verify your identity when accessing services or resources at your organization. You'll respond to authentication requests on your mobile phone or tablet.

First Pairing
To use the PingID application, you first need to pair your device by scanning a QR code or by entering a pairing key provided by your company's IT administrator or HelpDesk.

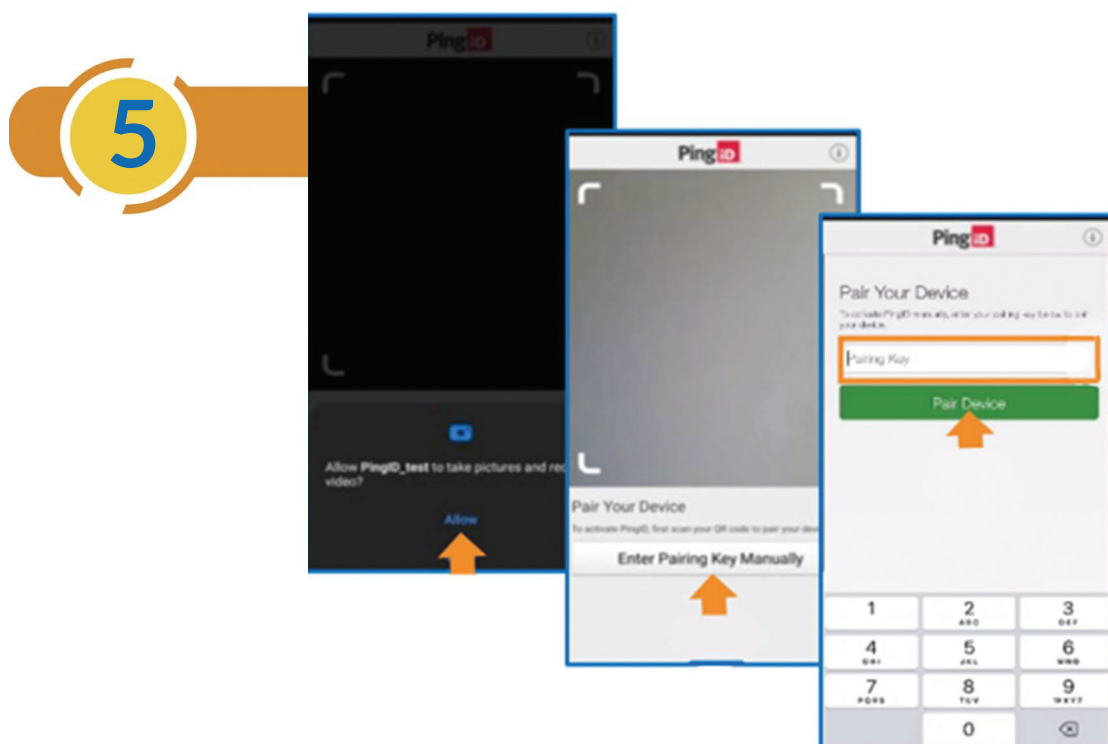
Restoring or Upgrading Devices
Because PingID is a security application, it can't be restored to a new mobile phone or tablet from a backup. If you restore or upgrade your device, you can activate it at your company's device management portal, or follow these steps:

01. On your old device, open PingID and t settings icon

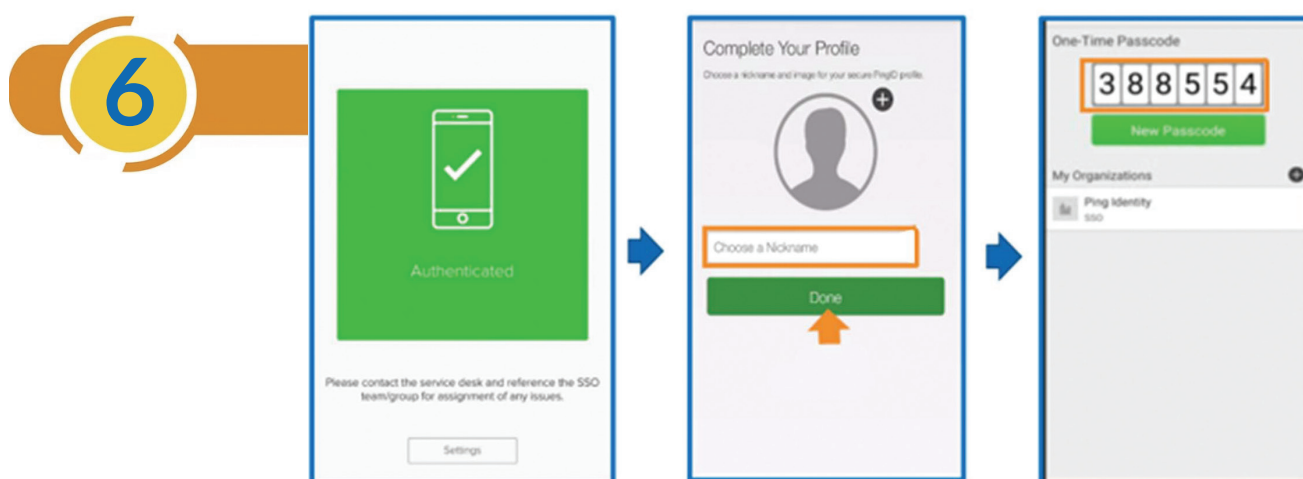
02. Choose "Change Device" from the menu, follow the prompts to pair your new device.

Continue

Kolejnym korkiem jest zezwolenie aplikacji na dostęp do notyfikacji, kamery, i lokalizacji i zeskanowanie kodu QR lub kliknięcie w przycisk do wpisania klucza parowania a następnie wpisanie go w polu widocznym nad przyciskiem sparuj urządzenie.



Po udanym parowaniu należy wpisać swoją nazwę użytkownika i zatwierdzić.



Uwierzytelnianie za pomocą wiadomości SMS

Po kliknięciu w ikonkę SMS strona przekieruje nas do . Należy pamiętać o zmianie numeru kierunkowego na polski. Po wpisaniu numeru i kliknięciu przycisku dalej, strona poprosi nas o wpisanie kodu weryfikacyjnego, który przyjdzie w wiadomości SMS na podany numer telefonu.



SMS

Podaj numer telefonu, którego chcesz użyć do uwierzytelnienia.



Anuluj **Dalej**

Wyrażam zgodę na otrzymywanie jednorazowego kodu dostępu od Ping Identity. Mogą obowiązywać opłaty za przesyłanie wiadomości i transmisję danych. Odpowiedz HELP, aby uzyskać pomoc, lub STOP, aby anulować subskrypcję. [Polityka prywatności](#) | [Zasady i warunki](#)

Weryfikacja

Wysłano wiadomość do +48 

Podaj otrzymany kod dostępu.

178122

Anuluj **Weryfikuj**

Wyrażam zgodę na otrzymywanie jednorazowego kodu dostępu od Ping Identity. Mogą obowiązywać opłaty za przesyłanie wiadomości i transmisję danych. Odpowiedz HELP, aby uzyskać pomoc, lub STOP, aby anulować subskrypcję. [Polityka prywatności](#) | [Zasady i warunki](#)

Następnie przyjdzie kolejny kod na podany numer telefonu który trzeba wpisać w zaznaczonym miejscu, który będzie już naszym kodem logowania.



Sharepoint

Wysłano SMS do Mobile 1 (*****51)

Podaj otrzymany kod dostępu.



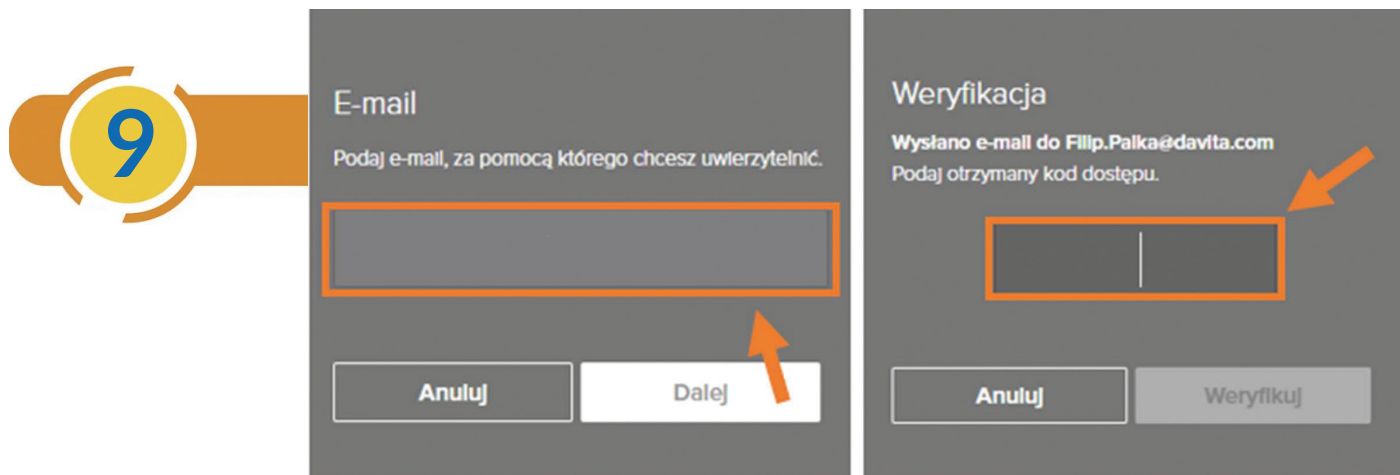
Wyślij kod dostępu ponownie

Zaloguj

[Nie masz ze sobą urządzenia?](#)

Uwierzytelnianie za pomocą poczty internetowej

Po kliknięciu w ikonkę poczty, strona przekieruje do okienka w którym poprosi o podanie adresu email. Adres może być już wypełniony automatycznie. Jeśli nie będzie wpisany, należy wpisać swój adres email na który będą przychodzić kody uwierzytelniające. Następnie trzeba sprawdzić podany adres email i wpisać kod uwierzytelniający w podanym miejscu, który przyjdzie z adresu noreply@pingidentity.com.



9

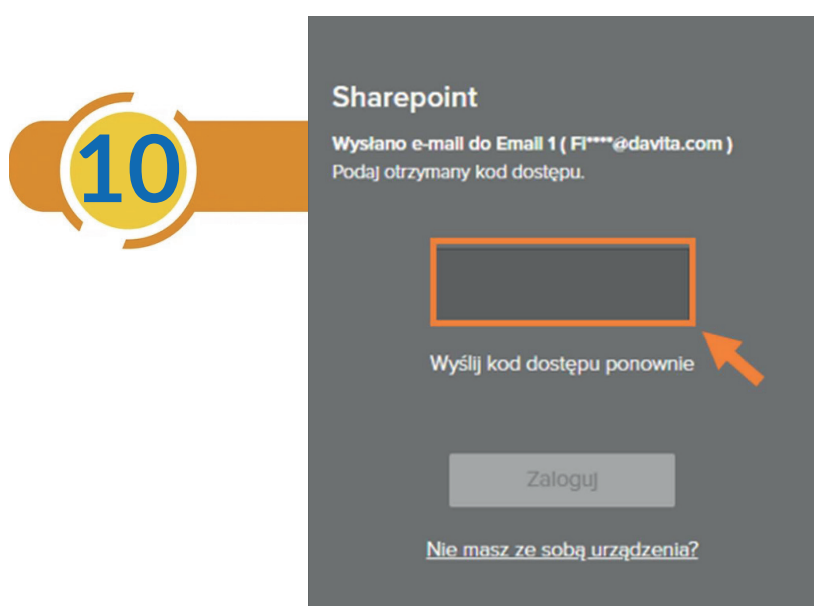
E-mail
Podaj e-mail, za pomocą którego chcesz uwierzytelnić.

Anuluj Dalej

Weryfikacja
Wysłano e-mail do Filip.Palka@davita.com
Podaj otrzymany kod dostępu.

Anuluj Weryfikuj

Następnie przyjdzie kolejny kod na podany adres email który trzeba wpisać w zaznaczonym miejscu, który będzie już naszym kodem logowania.



10

Sharepoint
Wysłano e-mail do Email 1 (F****@davita.com)
Podaj otrzymany kod dostępu.

Wyślij kod dostępu ponownie

Zaloguj

[Nie masz ze sobą urządzenia?](#)

FAQ

Oto kilka często zadawanych pytań (FAQ) dotyczących aplikacji PingID, która oferuje wieloskładnikowe uwierzytelnianie (MFA):

1. Q: Czym jest PingID?

A: PingID to aplikacja mobilna służąca do wieloskładnikowego uwierzytelniania (MFA) w celu zwiększenia bezpieczeństwa logowania do różnych usług i aplikacji.

2. Q: Jak działa PingID?

A: Po zainstalowaniu aplikacji PingID na urządzeniu mobilnym, użytkownicy mogą skonfigurować swoje konta, a następnie wykorzystać aplikację do generowania kodów jednorazowych lub otrzymywania powiadomień push w celu uwierzytelnienia swojej tożsamości podczas logowania.

3. Q: Czy PingID jest bezpieczny?

A: PingID stosuje różne środki bezpieczeństwa, takie jak szyfrowanie i technologie uwierzytelniania, aby chronić dane użytkowników. Warto również pamiętać, że bezpieczeństwo PingID zależy od odpowiedniej ochrony samego urządzenia mobilnego, na którym jest zainstalowana aplikacja.

4. Q: Czy PingID działa offline?

A: Aplikacja PingID może generować kody jednorazowe, nawet jeśli nie masz dostępu do sieci internetowej. Jednak w przypadku uwierzytelniania opartego na powiadomieniach push wymagane jest połączenie internetowe.

5. Q: Czy PingID działa z innymi aplikacjami i usługami?

A: Tak, PingID może być zintegrowany z różnymi aplikacjami i usługami, które oferują obsługę wieloskładnikowego uwierzytelniania (MFA). Dostawca usług musi jednak obsługiwać PingID jako metodę uwierzytelniania.

6. Q: Czy mogę używać PingID na więcej niż jednym urządzeniu?

A: Tak, możesz skonfigurować PingID na wielu urządzeniach mobilnych. Możesz również przenieść swoje konto PingID z jednego urządzenia na inne, jeśli na przykład wymienisz telefon.