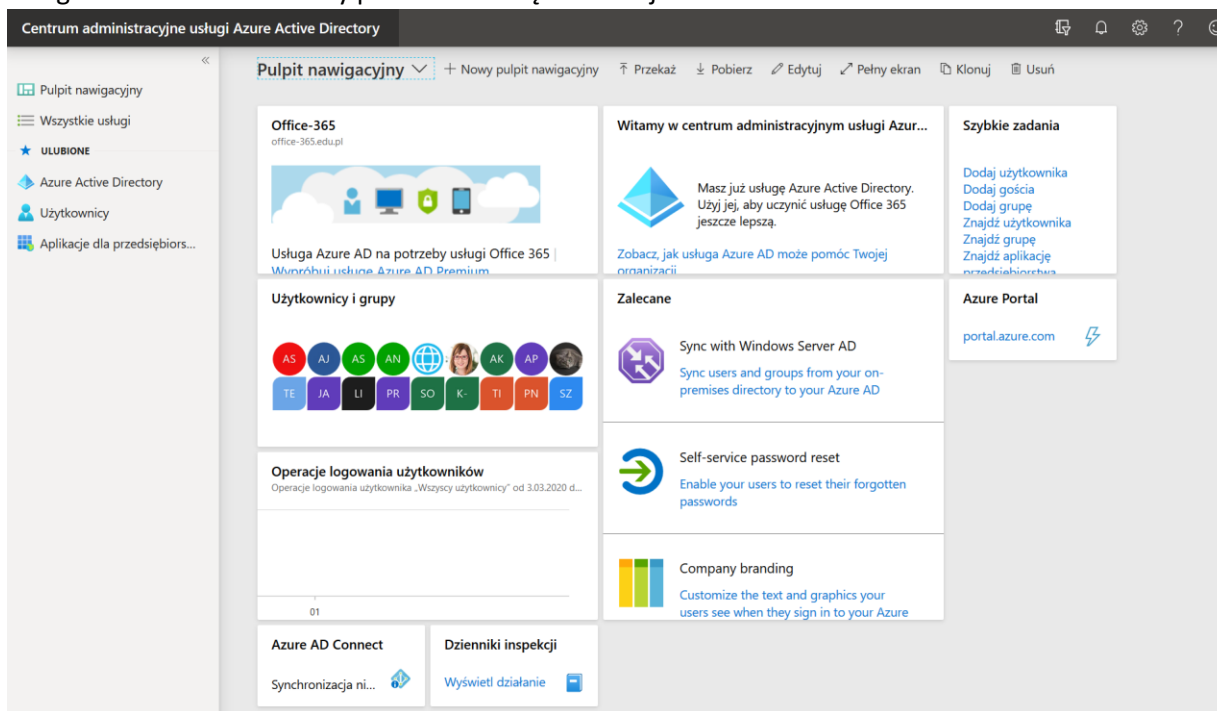
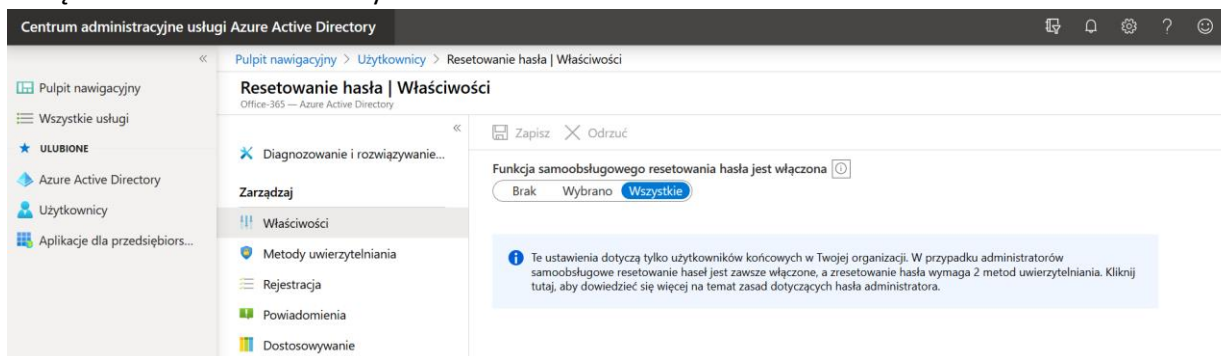


## Włączenie samoobsługowego odzyskiwania haseł oraz włączenie/wyłączenie MFA.

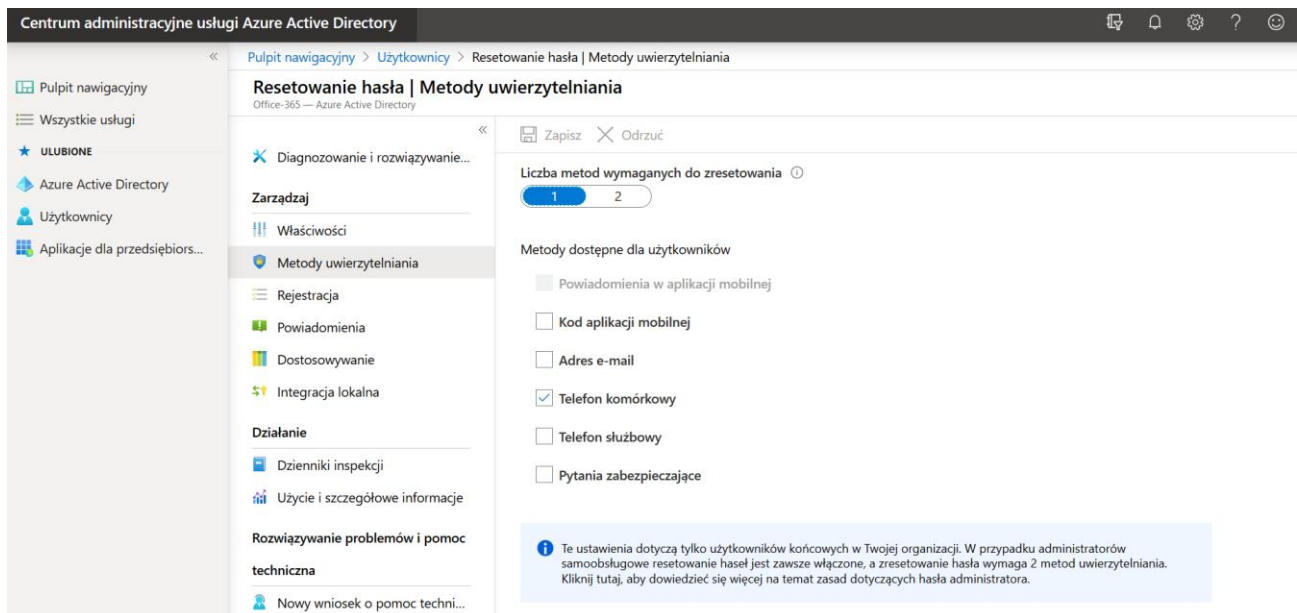
1. Logujemy się do Office 365 i z dostępnych ikon wybieramy *Administracja*.
2. Następnie w *panelu administratora* musimy kliknąć *Pokaż wszystko* oraz wybrać *Azure Active Directory*. Centrum usługi Azure Active Directory pokaże nam się na nowej karcie.



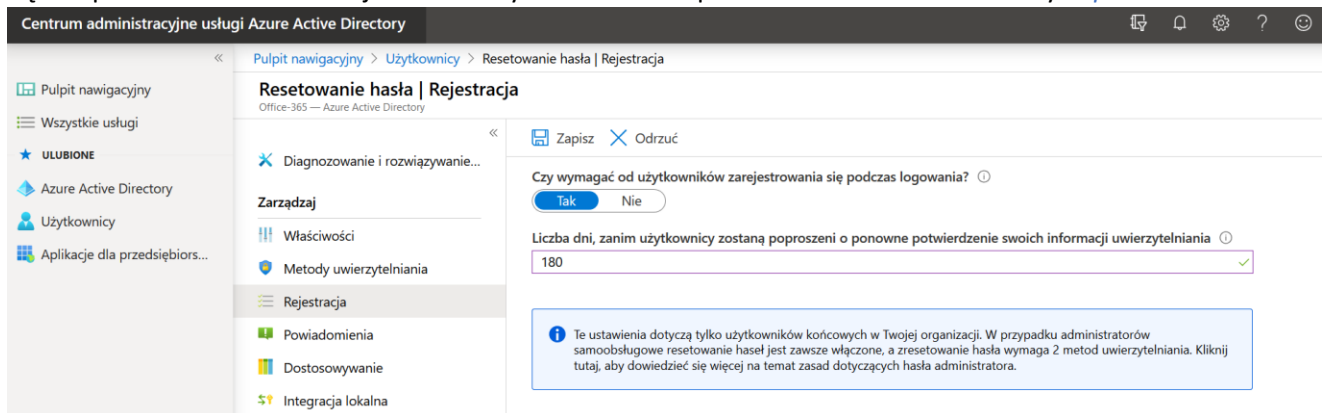
3. Po lewej stronie w menu wybieramy *Użytkownicy->Resetowanie haseł*. Wybranie tych opcji przeniesie nas do zarządzania właściwościami użytkownika.



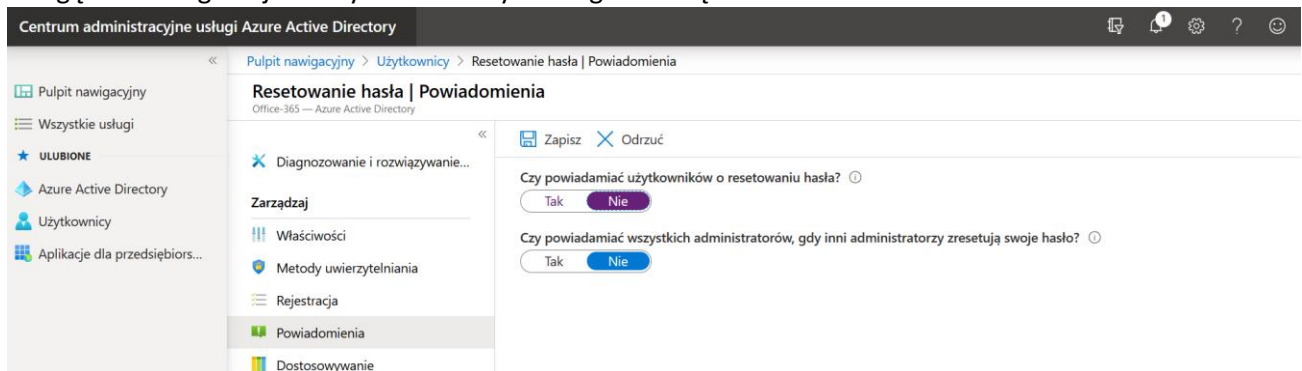
4. We wspomnianych *Właściwościach* ustawiamy, czy chcemy, aby użytkownicy sami mogli sobie odzyskiwać hasło zaznaczając opcję zaznaczając *Wszystkie*, a następnie *Zapisz*. Włączenie samoobsługowego odzyskiwania haseł zostało włączone.  
Po włączeniu tej pozycji użytkownicy będą monitowani o informacje kontaktowe podczas następnego logowania. Gdy użytkownik zechce zresetować swoje hasło, użyjemy tych informacji, aby wysłać mu kod, którego będzie można użyć do potwierdzenia tożsamości, a następnie wybrania nowego hasła.
5. Teraz musimy powiedzieć naszemu systemowi, jakie dane będą to tego celu potrzebne. Klikamy na kolejnej opcji po prawej stronie, czyli *Metody uwierzytelnienia*.



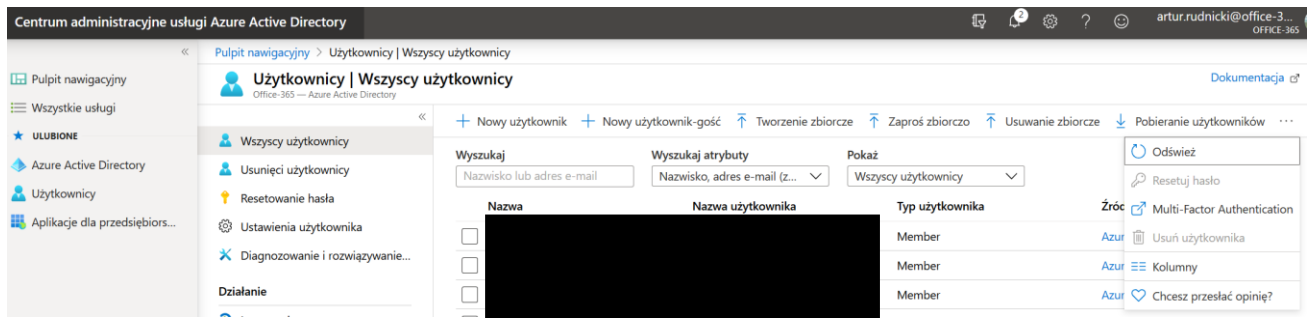
6. W tym miejscu należy wybrać ile metod będziemy wymagali i jakie. Po określeniu potrzebnych informacji klikamy **Zapisz**.
7. Przy częstych zmianach nr telefonów warto również ustawić, co jaki czasookres system będzie pytał użytkownika o weryfikację go. W tym celu klikamy po lewej stronie na **Rejestracja** i tam wprowadzamy co ile dni system będzie potwierdzał informacje do uwierzytelniania. Po wprowadzeniu wartości klikamy **Zapisz**.



8. Ostatnią rzeczą, którą możemy ustawić to informowanie administratora o zmianie haseł. Klikamy na **Powiadomienia** po prawej stronie i wybieramy odpowiadające nam opcje. Po wszystkim klikamy **Zapisz** i całą usługę bezobsługowej zmiany haseł mamy skonfigurowaną.



9. Jak już zdefiniowaliśmy opcje uwierzytelniania to możemy w celach bezpieczeństwa włączyć dla np. nauczycieli wieloskładnikowe logowanie. Będąc w Centrum administracyjnym Azure Active Directory klikamy **Użytkownicy->Wszyscy użytkownicy->Multi-Factor Authentication**. Okno **Uwierzytelnianie wieloskładnikowe** powinno nam się otworzyć w nowej karcie.



## uwierzytelnianie wieloskładnikowe użytkownicy ustawienia usługi

Uwaga: z usługi Multi-Factor Authentication mogą korzystać tylko użytkownicy posiadający licencję do korzystania z usług Microsoft Online Services. [Dowiedz się więcej, jak licencjonować innych użytkowników.](#)

Przed rozpoczęciem zapoznaj się z informacjami w przewodniku [wdrażania uwierzytelniania wieloskładnikowego.](#)

Widok:  Stan uwierzytelnienia wieloskładnikowego:

<input type="checkbox"/>	NAZWA WYŚWIETLANA	NAZWA UŻYTKOWNIKA	STAN USŁUGI MULTI-FACTOR AUTH
<input type="checkbox"/>			Wyłączone
<input type="checkbox"/>			Wyłączone
<input type="checkbox"/>			Wyłączone
<input type="checkbox"/>			Wyłączone

Wybierz użytkow

10. Opcje **MFA** ustawimy klikając u góry w opcje [ustawienia usługi](#). Wybieramy nam potrzebne opcje i klikamy **Zapisz**.

## uwierzytelnianie wieloskładnikowe użytkownicy ustawienia usługi

### hasła aplikacji

- Zezwalaj użytkownikom na tworzenie haseł aplikacji do logowania się do aplikacji niekorzystających z przeglądarki
- Nie zezwalaj użytkownikom na tworzenie haseł aplikacji do logowania się do aplikacji niekorzystających z przeglądarki

### opcje weryfikacji

Metody dostępne dla użytkowników:

- Połączenie z telefonem
- SMS na telefon
- Powiadomienie przez aplikację mobilną
- Kod weryfikacyjny z aplikacji mobilnej lub tokenu sprzętowego

### pamiętaj dane usługi multi-factor authentication

- Zezwalaj użytkownikom na zapamiętywanie danych uwierzytelniania wieloskładnikowego na zaufanych urządzeniach
- Liczba dni, po upływie których urządzenie musi zostać ponownie uwierzytelnione (1–60):

11. Włączenie/wyłączenie **MFA** wykonamy w opcji [użytkownicy](#). W celu włączenia/wyłączenia **MFA** wybieramy użytkownika/użytkowników. Przy włączeniu **MFA** warto dla wybranych użytkowników określić pewne ustawienia klikając na [Zarządzaj ustawieniami użytkownika](#).

## Zarządzaj ustawieniami użytkownika

- Wymagaj od wybranych użytkowników ponownego podania metod kontaktu
- Usuń wszystkie istniejące hasła aplikacji wygenerowane przez wybranych użytkowników
- Przywróć uwierzytelnianie wieloskładnikowe na wszystkich zapamiętanych urządzeniach

zapisz

anuluj

12. Po wybraniu odpowiednich ustawień klikamy **Zapisz**.

13. Jeżeli ustawienia użytkownika zostały wybrane klikamy po prawej stronie **Włącz**. Następnie musimy potwierdzić włączenie klikając w oknie, które nam wyskoczyło **Włącz usługę Multi-Factor Auth**, a następnie zamknij.

### Informacje o włączaniu uwierzytelniania wieloskładnikowego

Przeczytaj informacje w przewodniku wdrażania, jeśli jeszcze ich nie znasz.

Jeśli użytkownicy nie logują się regularnie za pośrednictwem przeglądarki, możesz wysłać im to łącze do rejestracji w uwierzytelnianiu wieloskładnikowym: <https://aka.ms/MFASetup>

### Aktualizacje ukończone pomyślnie

Uwierzytelnianie wieloskładnikowe jest teraz włączone na wybranych kontaktach.

włącz usługę multi-factor auth

anuluj

zamknij

## uwierzytelnianie wieloskładnikowe użytkownicy ustawienia usługi

Uwaga: z usługi Multi-Factor Authentication mogą korzystać tylko użytkownicy posiadający licencję do korzystania z usług Microsoft Online Services. [Dowiedz się więcej, jak licencjonować innych użytkowników.](#)

Przed rozpoczęciem zapoznaj się z informacjami w przewodniku wdrażania uwierzytelniania wieloskładnikowego.

Widok:  🔍

Stan uwierzytelniania wieloskładnikowego:

aktualizacja zbiorcza

<input type="checkbox"/>	NAZWA WYŚWIETLANA ▲	NAZWA UŻYTKOWNIKA	STAN USŁUGI MULTI-FACTOR AUTH	
<input type="checkbox"/>			Włączone	Wybierz użytkow
<input type="checkbox"/>			Włączone	

14. Jeżeli chcemy wyłączyć te ustawienia, po prostu odnajdujemy użytkownika z włączoną opcją MFA, zaznaczamy go i klikamy **Wyłącz**.