

(MFA) dla urządzeń mobilnych z systemem iOS

Uniwersytet Jagielloński

Centrum Informatyki

WERONS IELLOW

Dział Infrastruktury Systemów Informatycznych

Data dokumentu: luty 2024, Wersja:1.1 Autorzy: Monika Adamiec (m.adamiec@uj.edu.pl) Estera Ambroż (estera.ambroz@uj.edu.pl)

INFORMACJA TELEADRESOWA

Centrum Informatyki, Dział Infrastruktury Systemów Informatycznych, ul. Reymonta 4, Kraków E-mail: ci@uj.edu.pl | Web: https://it.uj.edu.pl

Spis treści

Konfiguracja podwójnego uwierzytelniania (MFA) dla urządzeń mobilnych z systemem iOS $_$	_ 1
Etap 1 - Pobieranie aplikacji na urządzenie mobilne	_ 3
Etap 2 - Włączanie zabezpieczenia na koncie UJ	_ 5
Etap 3 - Zgłoszenie gotowości do włączenia podwójnego uwierzytelnienia	14
Etap 4 - logowanie po włączeniu podwójnego uwierzytelniania	15
Dodatkowe czynności wymagane dla niektórych urządzeń oraz aplikacji	18
Urządzenia z systemem iOS, na których konto UJ było uprzednio skonfigurowane	_18
Klient synchronizacji OneDrive	_23

ETAP 1 - POBIERANIE APLIKACJI NA URZĄDZENIE MOBILNE

Pierwszym krokiem, aby poprawnie rozpocząć konfigurację dwufaktorowego logowania (podwójnego uwierzytelniania), jest pobranie na swoje urządzenie mobilne (smartfon lub tablet) aplikacji **Microsoft Authenticator** z App Store.



Po pobraniu aplikacji i jej uruchomieniu wyświetli się informacja o prywatności danych, którą należy zatwierdzić wybierając opcję *Akceptuj*. Na kolejnym ekranie należy wybrać opcję Kontynuuj. Nie ma konieczności wyrażania zgody na zbieranie przez aplikację dodatkowych danych.



Następnie wyświetli się kolejny ekran, w którym możliwy jest wybór sposobu połączenia aplikacji z kontem uniwersyteckim.

Na tym chwilowo kończymy używanie naszej aplikacji, aż do momentu włączenia zabezpieczenia na swoim koncie na komputerze. Oznacza to, że chwilowo nie wybieramy żadnej z poniższych opcji.



Przywróć z kopii zapasowej

ETAP 2 - WŁĄCZANIE ZABEZPIECZENIA NA KONCIE UJ

Korzystając z komputera należy otworzyć przeglądarkę internetową i zalogować się na stronie *office.com* używając uniwersyteckiego identyfikatora logowania. Następnie należy kliknąć w ikonę profilu (ze swoimi inicjałami, bądź zdjęciem), która znajduje się w prawym górnym rogu i wybrać *Wyświetl konto*.



Następnie w menu po lewej stronie wybieramy *Informacje zabezpieczające*.





Na stronie Informacji zabezpieczających należy wybrać opcję Dodaj metodę.

Moje logowania	
A Przegląd	Informacje zabezpieczające
𝒫 Informacje zabezpiecz	Poniżej przedstawiono metody, których używasz w celu logowania się do konta lub resetowania hasła.
🖻 Organizacje	+ Dodaj metodę
💻 Urządzenia	Brak elementów do wyświetlenia.
A Prywatność	Utracone urządzenie? Wyloguj się wszędzie

Następnie otworzy się okno, w którym wybieramy metodę drugiego uwierzytelniania. Należy wybrać pozycję *Aplikacja uwierzytelniania*, a następnie kliknąć przycisk *Dodaj*.

Moje logowania	
R Przegląd R Informacje zabezpiecz	Informacje zabezpieczające Ponizej przedstawiono metody, których używasz w celu logowania się do konta lub resetowania hasła.
🖻 Organizacje	+ Dodaj metodę Brak elementów do wyświetlenia.
 Urządzenia Prywatność 	Utracone urz Dodaj metodę ×
	Którą metodę chcesz dodać? Wybierz metodę Aplikacja uwierzytelniania Telefon Alternatywny numer telefonu Telefon biurowy

Następnie system poprosi o pobranie aplikacji. Postępując zgodnie z tą instrukcją aplikację na telefonie mamy już zainstalowaną, dlatego wybieramy opcję *Następne*.



W kolejnym kroku również należy wybrać opcję Następne.



Wyświetlony zostanie kod QR, który należy zeskanować za pomocą zainstalowanej wcześniej aplikacji Microsoft Authenticator.



W tym celu należy ponownie uruchomić aplikację Microsoft Authenticator na urządzeniu mobilnym.

Istnieją dwa możliwe scenariusze wyświetlenia informacji na urządzeniu mobilnym użytkownika.

1. Widok dodawania nowego konta

Jeśli wyświetli się poniższy widok należy wybrać Dodaj konto.



Następnie należy wybrać z listy *Konto służbowe*, co spowoduje pojawienie się okna. W oknie należy wybrać opcję *Skanuj kod QR*.



Centrum <u>Inf</u>ormatyki Następnie należy zeskanować w aplikacji kod QR, który wyświetlił się na ekranie komputera.



Po zeskanowaniu pojawia się komunikat *Włączono blokadę aplikacji. Aby lepiej chronić aplikację Authenticator blokada aplikacji jest teraz domyślnie włączona. Aby ją wyłączyć, przejdź do ustawień aplikacji.* Oznacza to, że za każdym razem przed wejściem do aplikacji konieczne będzie jej odblokowanie w taki sam sposób w jaki odblokowywany jest ekran telefonu.

Po zeskanowaniu kodu QR należy powrócić do zakładki Informacje zabezpieczające otwartej uprzednio w przeglądarce internetowej i wybrać opcję *Następne*.



W przeglądarce zostanie wyświetlony dwucyfrowy kod, który należy wprowadzić w aplikacji Microsoft Authenticator na urządzeniu mobilnym.

Microsoft	Authentica	tor					×
	Spróbujm	ny					
_	Zatwierdź pow pokazany pon	viadomienie, iżej.	, które w	ysyłamy d	lo Twojej aplika 32	cji, wprowadzają	: numer
						Wstecz	Następne
		Authentic Universe stera a Wprowa zalogov	Czy próbu Sytet Jagiel ambroz@uj adź wyświe wać. Wprow Wprow Hasta , GHI PORS Z	ujesz się za loński .edu.pl tlany numer, a 32 NIE WI Platności 2 ABC 5 JKL 8 TUV 0	+ Q i Ilogować? Iby się ar TAK IIE, TO NIE JA DZĘ NUMERU Q WXYZ VXYZ		

Ostatnim krokiem jest wybranie opcji *Następne* w kolejnym komunikacie wyświetlonym w przeglądarce. Po wykonaniu powyższych czynności metoda powinna zostać poprawnie skonfigurowana.

Microsoft Authenticator						
Powiadomienie zatwierdzone						
	Wstecz	Następne				

2. Widok wyboru akcji

Centrum

Informatyki

Jeśli wyświetli się poniższy widok należy wybrać Zeskanuj kod QR.

Następnie należy zeskanować w aplikacji kod QR, który wyświetlił się na ekranie komputera.

Po zeskanowaniu pojawia się komunikat *Włączono blokadę aplikacji. Aby lepiej chronić aplikację* Authenticator blokada aplikacji jest teraz domyślnie włączona. Aby ją wyłączyć, przejdź do ustawień *aplikacji.* Oznacza to, że za każdym razem przed wejściem do aplikacji konieczne będzie jej odblokowanie w taki sam sposób w jaki odblokowywany jest ekran telefonu.

Po zeskanowaniu kodu QR w aplikacji mobilnej pojawi się konto uniwersyteckie.

Authenticator	+	Q	÷	12:21 😤 🔳
Uniwersytet Jagielloński			>	< ® Uniwersytet Jagi
				Włączono powiadomienia Za pomocą tego urządzenia możesz zatwierdzać powiadomienia w celu weryfikowania logowania
				Kod hasła jednorazowego
				🕵 Włącz logowanie za pomocą telefonu >
				🔍 Zmień hasło >
				RE Aktualizuj informacje zabezpieczające
				Sprawdź ostatnią aktywność
Authenticator Hasła Płatności	(O) Adresy	(Zwery	fikowa	

Po zeskanowaniu kodu QR należy powrócić do zakładki Informacje zabezpieczające otwartej uprzednio w przeglądarce internetowej i wybrać opcję *Następne*.

W przeglądarce zostanie wyświetlony dwucyfrowy kod, który należy wprowadzić w aplikacji Microsoft Authenticator na urządzeniu mobilnym.

Microsoft	Authenticato	or				×
\checkmark	Spróbujmy					
_	Zatwierdź powia pokazany poniże	domienie, które v zj,	vysyłamy o	lo Twojej aplika 32	cji, wprowadzają	c numer
					Wstecz	Następne
	A	Czy prób Uniwersytet Jagi estera.ambroz@u Wprowadź wyświ załogować. Wpro dławy wyro Hasia 1 4 GHI 7 PQRS X	ujesz się za elloński etlany numer, wadź tutaj num 32 NIE W Platności 2 ABC 5 JKL 8 TUV 0	alogować? aby się ar TAK HIE, TO NIE JA HIZĘ NUMERU 3 DEF 6 MNO 9 WXYZ V		

Kolejnym krokiem jest wybranie opcji *Następne* w kolejnym komunikacie wyświetlonym w przeglądarce.

Microsoft Authenticator					
Powiadomienie zatwierdzone					
Wstecz	Następne				

Centrum Informatyki Ostatnim krokiem jest wybranie domyślnej metody logowania w zakładce *Informacje zabezpieczające*. Należy wybrać *Uwierzytelnianie oparte na aplikacji – powiadomienie*.

Informacje zabezpieczając	e
Poniżej przedstawiono metody, których używasz w c	elu logowania się do konta lub resetowania hasła.
Domyślna metoda logowania: Microsoft Authentica	ator — powiadomienie Zmień
Zmień domyślną metodę	ę ×
Której metody chcesz użyć do zalog	gowania się?
Uwierzytelnianie oparte na aplikacj	ji — powiadomienie 🛛 🗸
	Wstecz Potwierdź

ETAP 3 - ZGŁOSZENIE GOTOWOŚCI DO WŁĄCZENIA PODWÓJNEGO UWIERZYTELNIENIA

W kolejnym kroku należy zgłosić swoją gotowość do włączenia podwójnego uwierzytelniania wypełniając poniższy formularz:

https://forms.office.com/e/VwsQUUAGsR

Formularz dostępny jest po zalogowaniu się kontem UJ.

ETAP 4 - LOGOWANIE PO WŁĄCZENIU PODWÓJNEGO UWIERZYTELNIANIA

W ciągu kilku kolejnych godzin aplikacje na komputerze bądź na innych urządzeniach będą zgłaszały prośbę o potwierdzenie logowania drugim faktorem.

Gdy jesteśmy zalogowani na urządzeniach to zostaniemy wylogowani i poproszeni o ponowne zalogowanie, a kolejno o potwierdzenie logowania w aplikacji Microsoft Authenticator na urządzeniu mobilnym.

Gdy użytkownik zostanie poproszony o wpisanie kodu weryfikacyjnego powinien uruchomić aplikację na swoim telefonie (urządzeniu mobilnym) i wprowadzić wyświetlany kod.

Centrum Informatyki Możliwa jest również zmiana opcji weryfikacji poprzez wybranie Użyj innej opcji weryfikacji.

Kolejno należy wybrać Wyślij powiadomieni do mojej aplikacji mobilnej.

Wtedy na ekranie komputera wyświetli się liczba:

Uniwersytet Jagielloński

Ze względów bezpieczeństwa wymagamy dodatkowych informacji umożliwiających zweryfikowanie Twojego konta

Otwórz aplikację Microsoft Authenticator i naciśnij widoczny poniżej numer, aby się zalogować.

91

. . .

Użyj innej opcji weryfikacji

Na naszym urządzeniu mobilnym wyświetli się komunikat, który poprosi o zatwierdzenie logowania poprzez podanie liczby wyświetlonej na ekranie komputera i kliknięcie opcji TAK.

Po wpisaniu liczby należy potwierdzić logowanie wzorem lub kodem blokady ekranu urządzenia mobilnego.

DODATKOWE CZYNNOŚCI WYMAGANE DLA NIEKTÓRYCH URZĄDZEŃ ORAZ APLIKACJI

Dla niektórych urządzeń oraz aplikacji będzie wymagane dodatkowe działanie, aby podwójne uwierzytelnianie zostało w pełni skonfigurowane oraz synchronizacja danych na urządzeniu nie została wstrzymana.

Urządzenia z systemem iOS, na których konto UJ było uprzednio skonfigurowane

Urządzenia z systemem operacyjnym iOS (iPhone lub iPad) nie wyświetlają informacji o konieczności ponownego zalogowania się do konta po skonfigurowaniu podwójnego uwierzytelniania. Niezbędne jest w takim wypadku usunięcie konta UJ z urządzenia i ponowne dodanie.

Aby usunąć konto UJ z urządzenia iOS, należy:

1. Otworzyć Ustawienia urządzenia ikoną:

2. W ustawieniach należy przejść do opcji *Hasła i konta* (dla wersji iOS 13.x lub starszej) lub do opcji *Mail*, a następnie *Konta* (dla wersji iOS 14.x lub nowszej)

II Orange	LTE 09:49	99% 🔲	•II Orang	ie LTE	09:48	99% 🗖
	Ustawienia		< Usta	awienia	Mail	
	Bateria	>	DOS	TĘP (MAIL)		
	Prywatność	>		Siri i wysz	zukiwanie	>
A	App Store	>	4	Powiador Banery, Plak	nienia ^{ietki}	>
	Portfel i Apple Pay	>	((T))	Dane sied	ci kom.	
2	Hasła	>	Kon	ta		2 >
	Mail	>	LIST	A WIADOMOŚ	CI	
۲	Kontakty	>	Pod	gląd		2 wiersze >
	Kalendarz	>	Pok	aż etykiety	Do/Dw	
	Notatki	>	Opc	cje na liście		>
:=	Przypomnienia	>	14/14/1	DOMOÉCI		
-	Notatki głosowe	>	Dat	viordzei	uuonia	
	Telefon	>	Och	nrona prywa	atności	>

Centrum Informatyki 3. Należy wybrać konto UJ, nazwane standardowo Exchange:

	Orange LTE	^{09:48} Konta	99	9% 🔳
Ì				
	KONTA			
	iCloud Nieaktywne			>
	Exchange Mail, Kalendarze			>
l	Dodaj konto			>
	Pobierz nowe da	ine	Push	>

4. W widoku konta u dołu strony należy kliknąć Usuń konto oraz potwierdzić operację usuwania:

Orange LTE 09:49	99% 🔲	•• Orange LTE 09:50	98%
Konta Exchange		Konta Exchange	
EXCHANGE		EXCHANGE	
Konto	.uj.ed >	Konto .uj.ed.	>
Mail		Mail	0
(C) Kontakty		(C) Kontakty	
Kalendarze		Kalendarze	D
Przypomnienia		Przypomnienia	
Notatki		Notatki	
Synchronizuj pocztę	1 miesiąc >	Wyłącz Kalendarze Czy na pewno kontynuować? Wszystkie kalenc Exchange zostana usuniete z iPhone'a.	larze
Odpowiedź	Wył. >	Usuń z iPhone'a	
Usuń konto	,	Anuluj	

Po usunięciu konta UJ z urządzenia wyświetli się widok *Konta*, na którym nie będzie już widoczne konto UJ. W tym momencie można dodać konto na nowo poprzez następujące kroki:

1. W widoku Konta wybierz opcję Dodaj konto, a następnie Microsoft Exchange:

Mail Orange LTE 09:53	97% 🗩	Ill Orange LTE 09:53 Konta Dodaj kor	97% 🔳
KONTA		iClα	bud
Nieaktywne Dodai konto	<u> </u>		
			change
Pobierz nowe dane	Push >	Goog	e
		yaho	o.
		Aol	•
		💽 Outloc	k.com
		Inne	

2. W pole *Email* należy wprowadzić adres mailowy z domeny UJ oraz kliknąć *Dalej*:

•• Orai	nge LTE			09:54			9	6% 🔲
Anul	uj		Ex	chan	ge		ſ	Dalej
Ema	il						uj.edu	.pl
Opis		Mo	oje ko	onto l	Excha	ange		
Doda Excha Admir zdaln	Dodanie konta Exchange umożliwi administratorowi Exchange zdalnie zarządzać Twoim urządzeniem. Administrator może dodawać/usuwać ograniczenia oraz zdalnie wymazywać urządzenie. ID urządzenia Exchange							
q	w	e r	t	:)	/ l	. ا	i o	р
а	S	d	f	g	h	j	k	Ι
¢	z	x	С	V	b	n	m	$\overline{\mathbf{x}}$
123	Û	sp	acja	(0		ret	turn

3. W oknie Czy chcesz zalogować się na swoim koncie Exchange należy kliknąć Zaloguj się:

	ŝ	09:54	Orange LTE	
alej		Exchange	Anuluj	
ol	uj.edu		Email	
		vehande	Opis	
oraz	a ć na ange " za rmy ysłany do ysłania ange.	Chcesz się zalogować na swoim koncie Exchange " uj.edu.pl" za pośrednictwem firmy Microsoft? Twój adres email zostanie wysłany do firmy Microsoft w celu uzyskania informacji o koncie Exchange.		
	ie	ionfiguruj ręczn		
		Zaloguj się		
	ysłany do yskania ange. ie	es email zostanie w Microsoft w celu uzy macji o koncie Exch Configuruj ręczn Zaloguj się	Twój ac firmy info	

4. Zostanie wyświetlona strona logowania UJ, na której należy podać hasło:

••II Orange L	E 09:57	95% 🔲
Anuluj	🔒 sts.uj.edu.pl	S AA

Uniwersytet J	Jagielloński
---------------	--------------

Zaloguj		
@uj.edu.pl		
Hasło		
Zaloguj		
Odzyskaj hasło		
© 2018 Microsoft		
	•	
$\langle \rangle$	۲ <u>)</u>	\checkmark

5. Następnie wyświetli się komunikat o konieczności zweryfikowania logowania drugim faktorem z informacją o liczbie, którą należy wpisać:

6. W aplikacji Microsoft Authenticator pojawi się prośba o zatwierdzenie logowania wraz z miejscem na wpisanie liczby:

Centrum Informatyki 7. Po zatwierdzeniu logowania należy wybrać aplikacje, które mają synchronizować dane z konta UJ do urządzenia według preferencji oraz kliknąć przycisk *Zachowaj*. Po tej czynności konto UJ jest dodane do urządzenia, a dane są synchronizowane:

Klient synchronizacji OneDrive

Aplikacja OneDrive instalowana na komputerze do synchronizacji plików z dyskiem chmurowym wymaga po skonfigurowaniu podwójnego uwierzytelnienia ponownego zalogowania się do usługi.

W tym celu należy kliknąć ikonę klienta OneDrive na pasku zadań komputera **kliknąć ikonę klikając w** monit z prośbą o ponowne zalogowanie, zalogować się kontem UJ.

W aplikacji Microsoft Authenticator na urządzeniu mobilnym pojawi się prośba o zatwierdzenie logowania. Po tym zatwierdzeniu aplikacja OneDrive ponownie rozpocznie synchronizację plików z komputerem.