



Externer Outlook-Web-Zugriff (OWA) mit Zwei-Faktor-Authentifizierung (2FA)

Hintergrund

Um den rechtlichen Anforderungen zu genügen und digitale Identität zu gewährleisten, müssen externe Zugriffe mit einer Zwei-Faktor-Authentifizierung (2FA) abgesichert werden.

Bei den VPN-Zugängen wurde diese Maßnahme zur Erhöhung der Sicherheit am MRI bereits umgesetzt.

Für den externen Zugriff auf Ihr E-Mail-Postfach über <u>https://owaproxy.mri.tum.de,</u> z.B. aus dem eigenen Internet, LTE, WKS, Baycom), brauchen Sie zur Anmeldung neben dem Benutzernamen und Passwort den zweiten Faktor zwingend ab 19.10.2022.

Die Generierung des zweiten Faktors erfolgt über ein Token. Dieses können Sie

a) als **Softwaretoken** mit Komfortfunktionen an Ihrem Smartphone im IDM Userportal https://auth.mri.tum.de einrichten

(Ausführliche Anleitung im Intranet der IT unter: https://intranet.mri.tum.de/it)

b) als Hardwaretoken im MRI-Service-Portal unter <u>2-Faktor Hardware Token</u> bestellen

(Nur für Mitarbeiter*innen des MRI möglich.)

Sollten Sie bereits registriert sein und ein Token zur Generierung des zweiten Faktors für Ihren VPN-Zugang nutzen, kann dieses auch für den Outlook-Web-Zugriff verwendet werden.







Einrichtung Outlook-Web-Zugriff mit Zwei-Faktor-Athentifizierung (2FA) & Software-Token

1) Am Smartphone: Download und Installation der App

Die Installation der *NetIQ Authenticator App* auf einem Smartphone ist die Voraussetzung, um Ihr Gerät im Anwenderportal als zweiten Faktor registrieren zu können. Den Link zur App finden Sie als Barcode auf Seite 1 dieser Anleitung. Auf dienstlichen Smartphones kann der NetIQ Authenticator über den MRI App Store heruntergeladen werden (Symbol mit dem Namen *Hub*), was keine Anmeldung am App-Store erfordert.



Für private Smartphones gehen Sie bei der Installation wie folgt vor (Beispiel: Apple iOS):









03:41 App Store	.ul 🗢 🔳	03:48 4 App Store	.al 🗢 🛋		
NetlQ Advanced	Authentication			03:48	
END USER LICENSE AGREEMENT	r			< App Store	an 🔹 🖷
Advanced Authentication 6.3 Advanced Authentication 6.3 Clic Advanced Authentication 6.3 Lim COVID-19 Evaluation Software	ents lited			united Altorety	
IMPORTANT: LICENSOR IS PROV SOFTWARE TO LICENSER (THE C ETHER AS AN INDIVUAL OR O LEGAL ENTITY AS ITS EMPLOYEI FOR ITS USE SUBJECT TO LICEN TERMS AND CONDITIONS SET F END USER LICENSE AGREEMENT EARLIER RELEASES OF THE LICE READ THEM CAREFULLY TO ENS UNDERSTANDING BEFORE PRO- CONTAIN ADDITIONAL RESTRIC SOFTWARE, PLEASE OIRECT AN MICRO FOCUS LEGAL DEPARTM MICRO FOCUS LEGAL DEPARTM MICRO FOCUS LEGAL DEPARTM CROBET OTHE TERMS AND CON AGREE TO THE TERMS AND CON	IDING THIS LICENSED DRIGINAL PURCHASER N BEHALF OF ANOTHER E OR AUTHORIZED AGENT) ISEE'S AGREEMENT TO THE ORTH BELOW. THESE BUFFERENT FROM THE FISS THAT ACCOMPANIED INSED SOFTWARE, PLEASE JURE FULL ZEEDING, AS THEY MAY TIONS ON USE OF THE ENT AT A. IF LICENSEE DOES NOT JOITIONS OF THIS LICENSE DEFINISTION OF THIS LICENSE	Legen Sie die neue PIN fe	ost.	Geben Sie die PIN erneut ein.	
AUBREMENT, DLENSDE WILL NO THE LICENSED SOFTWARE. BY BUTTON OR SIMILAR ACCEPTAN INSTALLATION, OR BY ODPYING SOFTWARE, LICENSE ACKNOW THIS LICENSE AGREEMENT, UNE THIS LICENSE AGREEMENT, UNE TO BE BOUND BY ITS TERMS AN LICENSED SOFTWARE IS LICENS For this End User LICENSE Agreent	DI BE ADTHORAZED TO USE LICKING THE ACCEPT ICE MECHANISM DURING OR USING THE LICENSED LEDGES THAT IT HAS READ ERSTOOD IT, AND AGREED DI CONDITIONS. THE IED NOT SOLD.			Seven Sie die Pilk enteurent.	ОК
the following terms shall have the "Documentation" means the Lice that is included with the Licensed	e meanings given below: nsor user documentation d Software.				
"Licensee" means the single lega rightfully acquires the Licensed S from a distributor or reseller of Li	al entity or person that Software from Licensor or Icensor.	Legen Sie einen F verwenden Sie sr	PIN fest. Diesen PIN päter, um sich in der	Wiederholen Sie den PIN.	
"License Options" means those I	Ablehnen	App <i>NetlQAdvan</i> anzumelden.	ced Authentication	L	
Akzeptieren Sie die	Bedingungen	-			
der App.	· · · · · · · · · · · · · · · · · · ·				
		L			

03:49 App Sto	re :	l 🗢 🛋	15:03		all 🗢 🔳
=	Registrierte Authenticators	+		Registrierte Authenticators	+
Keine Regis	Authenticators gefunden trieren Sie einen Authenticator.		Keine Regist	Authenticators gefunden rieren Sie einen Authenticator.	
	"NetlQ Auth" möchte dir Mitteilungen senden Mitteilungen können Hirweise, Tönr und Symbolkennzeichen sein. Sie können in den Einstellungen konfiguriert werden.	,			
	Nicht erlauben Erlauben				
Dami Veldu Erlau	it die App entsprechende ungen senden kann, bitte <i>ben</i> auswählen.) Э	Die A weite	op ist nun bereit für die ren Schritte.	•

Version 1.1





2) Am Computer: Registrierung des Smartphones als zweiter Faktor im Anwenderportal

Nachdem Sie die App *NetIQ Advanced Authentication* installiert haben, melden Sie sich bitte zum Registrieren Ihres Smartphones mit Ihrem MRI-(KKS)-Windows-Account und Passwort am Anwenderportal <u>https://auth.mri.tum.de</u> an. Das Portal erreichen Sie mit allen gängigen Browsern von intern (KKS), als auch extern (Internet, Baycom, Eduroam, LTE, ...). Bitte beachten Sie, dass der Browser Microsoft Internet Explorer (IE) nicht mehr unterstützt wird.

Benutzername		Kanakum rechts der law Sechnische Universitzt München	TUT	Multifaktor Authentifizierun
Nächste		Verzei	chnispassw	Passwort
Copyright © 2021 Micro Focu	s. Alle Rechte vorbehalten.		••••••	
		Näc	hste At	bbrechen

Nun können Sie das gewünschte Software-Verfahren auswählen und einrichten (Beispiel: NetlQ *Push*):

Herein Multifaktor Authentif	zierung	
Multifaktor Authentifi Authentifizierungsmethoden Registrierte Methoden sind Authenticators, die Sie be verwenden können. Einmalpasswort-Methoden sind The registrierten Einfachmethoden für die Anme Umpersonnt UDAP-Passwort Hinzufügen	zierung vereits registriert haben und zur Anmeldung [Authenticators mit Einmalpasswort. dung Waltifaktor Authent Verfügbare Methoden für die R Wählen Sie eine Authentifizierungsmethode für di kann die Methode zur Anmeldung verwendet were Authenticators mit Einmalpasswort. Willie Sie eine Authentifizierungsmethode für di kann die Methode zur Anmeldung verwendet were Authenticators mit Einmalpasswort. Willie Sie eine Authentifizierungsmethode für di kann die Methode zur Anmeldung verwendet were Authenticators mit Einmalpasswort. Willie Sie eine Authentifizierungsmethode für di kann die Methode zur Anmeldung verwendet were Authenticators mit Einmalpasswort.	Iffizierung Begistrierung aus. Nach der Registrierung ier Einmalpasswort-Methoden sind Image: Strierung Image: Strierung: Strierung
		Die AdvAuth-Mobil-App stellt einen Einmalpasswort-Code bereit, der als Ersatzmethode verwendet werden kann, wenn auf dem Smartphone keine Internetverbindung verfugbar ist. Speichem Abbrechen





3) Am Smartphone: Registrierung als zweiter Faktor im Anwenderportal

Nehmen Sie nun Ihr Smartphone und fügen Sie den zweiten Faktor in der App *NetlQ Advanced Authentication* hinzu. Wählen Sie oben rechts das Plus-Zeichen und im Anschluss scannen Sie den QR Code.

15:03	Abbrechen Authenticator hinzufügen	Abbrechen Schabl. bearb. Sichem 16:30 🕈 📼
E Registrierte Authenticators	C C C C C C C C C C C C C	Konto 1. 2. MRI Push (Software-Token) Weitere Informationen Weitere Informationen Smartphase-Authenticators (Software-Token)
Registrieren Sie einen Authenticator.	Exceptions Medice energy is a Affective and account of the energy is exception of the energy is a characteristic of the energy is a chara	Hier können Sie wieder eine Bezeichnung vergeben, ggf. die Gleiche wie zuvor im Anwendungsportal.
		"Token" qwertzuiopü
	Der QR Code wird gescannt	asdfghjklöä
	game anote	↔ vxcvbnm 🛪

4) Am Computer: Speichern der Registrierung Im Anwendungsportal wird nun auch die erfolgreiche Registrierung angezeigt, bitte klicken.

"Speichern"



per E-Mail an servicedesk@mri.tum beantragen.





Externer Outlook-Web-Zugriff (OWA) mit Zwei-Faktor-Authentifizierung (2FA)

Anmeldung an Ihrem E-Mail Postfach über <u>https://owaproxy.mri.tum.de</u> ab 19.10.22:

1) Bitte rufen Sie wie gewohnt Ihr E-Mail Postfach über die Adresse <u>https://owaproxy.mri.tum.de</u> auf und geben Sie Ihren Windows Benutzernamen und Ihr Passwort ein.

Klinikum rechts der Isar Technische Universität München	Outlook Web App
Benutzername	
Passwort	
Anmelden	

2) Bei der Anmeldemethode wählen Sie bitte die von Ihnen als 2. Faktor eingerichtete Methode aus:

Kinikum rechts der Isar Technische Universität München	Multifaktor Authentifizierung
Anmeld Wählen Sie aus der na	emethode auswählen Ichfolgenden Liste aus
Akzeptieren der A	Anfrage (NetIQ / ~
Akzeptieren der Eingabe des 6-st	Anfrage (NetIQ App) elligen Token-Pin
Copyright © 202	21 Micro Focus. Alle Rechte vorbehalten.

a) Methode 1: Akzeptieren der Anfrage (NetlQ App)

Bitte bestätigen Sie auf Ihrem Smartphone die Push Anfrage *Akzeptieren* in der NetlQ App, bei Zeitüberschreitung laden Sie die Seite <u>https://owaproxy.mri.tum.de</u> bitte erneut.

Kinikum rechts der Isar Technische Universität München	Multifaktor Authentifizierung
Bitte Anmeldung in der No Offline OTP Options	etlQ App bestätigen ∨
Abbrechen Copyright © 2021 M	licro Focus. Alle Rechte vorbehalten.





b) Methode 2: Eingabe der sechsstelligen Token-Pin

Bitte übertragen Sie die sechsstellige Token-Pin von Ihrem Hardwaretoken in die Eingabemaske und klicken Sie auf *Weiter*. Im Anschluss werden Sie an Ihrem E-Mail-Postfach angemeldet und können wie gewohnt weiterarbeiten.

Falls Sie bei der Methode Akzeptieren der Anfrage (Net/Q App) mit Ihrem Smartphone keine Internetverbindung haben sollten, können Sie auch den in der App generierten Token für die Methode 6-stellige Token-Pin nutzen.

Klinikum rechts der Isar Technische Liniversität München	TUT	Multifaktor Authentifizierung
I	Bitte geben S	ie Ihren Token ein
Vom Smar Hardwarete	tphone erzeugter S oken	Softwaretoken oder
Code eir	ngeben	
	Ð	Ausblenden
Weiter	Erneut senden	Abbrechen
	Copyright © 2021 Micro	Focus. Alle Rechte vorbehalten.

Notfall/Verlust: Anmeldung am AnyConnect VPN Client über ein Einmalpasswort

Wenn beispielsweise durch Verlust kein zweiter Faktor verfügbar ist, können Sie über den ServiceDesk (<u>servicedesk@mri.tum.de</u>) ein Einmalpasswort beantragen und als Token für die Methode *Eingabe des 6-stelligen Token-Pin* nutzen.

Schlussbemerkung

Gern können Sie Ihre Verbesserungsvorschläge oder konstruktive Kritik senden an: <u>alexander.ritter@mri.tum.de</u>