

CRANIX-2FA Zwei-Faktor-Authentifizierung

Das CRANIX-2FA-Zusatzmodul bietet eine zusätzliche Sicherheitsebene für den Zugriff auf die Administrationsoberfläche des CRANIX/CEPHALIX Servers.

"Generell empfiehlt das BSI die sogenannte Zwei-Faktor-Authentifizierung. Bei dieser zweistufigen Abfrage wird neben dem Passwort zusätzlich z.B. die Eingabe eines Codes (verschickt auf ein anderes Gerät in Ihrem Besitz), ein Fingerabdruckscan oder ein USB-Token zur Identifikation gefordert. Sie erhöht das Maß an Sicherheit um ein Vielfaches.

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/accountschutz_node.html

Nach erfolgreicher Anmeldung wird eine PIN an eine E-Mailadresse gesendet oder Sie müssen ein zeitlich begrenztes Einmalpasswort (TOTP) von Ihrer Authenticator-App eintragen um die Weboberfläche des Servers benutzen zu können. Der Administrator kann festlegen welche Benutzer 2FA verwenden müssen. Das kann persönlich oder gruppenweise erfolgen. Nach dem Erwerb des CRANIX-2FA-Zusatzmoduls müssen auf dem Server folgende Schritte ausgeführt werden um CRANIX-2FA zu verwenden:

4.2 Verwendung von CRANIX-2FA

Hat ein Administrator die `crx2fa.use` ACL einem Benutzer zugewiesen, wird dieser bei nächster Anmeldung dazu aufgefordert, die Zwei-Faktor-Authentifizierung einzurichten.

1. Nach erfolgreicher Anmeldung wird man zur Verwaltung von CRX-2FA geleitet und **keine** anderen Funktionen sind erreichbar.
2. Man kann 2 Typen von 2FA-Konfigurationen anlegen: TOTP und MAIL.
3. Es wird empfohlen beide Zwei-Faktor-Authentifizierungsmöglichkeiten einzurichten.
4. Folgende Parameter können gesetzt werden
 1. Typ von zweifaktor Authorisierung: **TOTP** oder **MAIL**
 2. Pin Gültigkeit in Sekunden:
 3. Wie lange ist eine PIN gültig.
 1. Bei TOTP-2FA liegt der gültige Bereich zwischen 30 und 60 Sekunden und kann nach der Erstellung nicht geändert werden.

2. Bei MAIL-2FA liegt der gültige Bereich zwischen 120 und 600 Sekunden und kann nach der Erstellung geändert werden.

4. Gültigkeit einer 2FA Anmeldung. Für die eingestellte Gültigkeitsdauer müssen Sie sich am selben Gerät nicht noch mal per 2FA anmelden. Gültiger Bereich 1 bis 12 Stunden. Empfohlen wird 12 Stunden. Diese Einstellung kann auch später geändert werden.
5. Bei MAIL-2FA müssen Sie noch eine gültige E-Mailadresse eintragen, auf die Sie immer Zugriff haben. Diese Adresse können Sie später auch ändern.
6. Bei TOTP-2FA wird ein QR-Code generiert, welchen Sie mit einer Authenticator-App importieren müssen ! Folgende Apps wurden getestet:

[[privacyIDEA für iOS](#)]

[[Google Authenticator für iOS](#)]

[[privacyIDEA für Android](#)]

[[Google Authenticator für Android](#)]

CRANIX
Ivarkoly (Varkoly Lehrer) Cranix zweifaktor Authorisierung...

Profil

Konfigurieren Sie Ihre zweifaktor Authorisierung

Typ von zweifaktor Authorisierung	TOTP	▼
Pin Gültigkeit	30	Sekunden
Gültigkeit einer Sitzung	12	Stunden

QR CODE ERSTELLEN

1. Wählen Sie den 2FA Typ
2. Setzen Sie die Gültigkeit eines Pins in Sekunden. min: 30 max: 60
3. Setzen Sie die Gültigkeit eines Pins in Stunden. min: 1 max: 24
4. Es ist empfohlen alle 2FA Typen zu konfigurieren.
5. Laden Sie den privacyIDEA oder Google Authenticator App auf Ihr mobiles Gerät!

iOS:
Android:


6. Erstellen Sie einen QRCode auf dieser Seite.
7. Importieren (scannen) Sie das QRCode mit Ihrem Authenticator App!
8. Haben Sie Probleme mit Ihrem App, löschen Sie das QRCode und erstellen Sie ein neues!
9. Haben Sie Ihr Mobilgerät verloren, löschen Sie das QRCode und erstellen Sie ein neues!
10. Nachdem der QRCode generiert wurde, können Sie nur noch die Gültigkeit eines 2FA Sessions ändern.
11. Bitte beachten Sie, dass man die 2FA-Konfiguration, die man zur Anmeldung benutzt hat nicht selber löschen kann.

TOTP CRX2FA


CRANIX () Cranix zweifaktor Authorisierung

Konfigurieren Sie Ihre zweifaktor Authorisierung

Typ von zweifaktor Authorisierung	TOTP	
Pin Gültigkeit	30	Sekunden
Gültigkeit einer Sitzung	12	Stunden
Serial	CRX_cephtlx-..._9F68D4ABB4F94	



1. Wählen Sie den 2FA Typ
2. Setzen Sie die Gültigkeit eines Pins in Sekunden, min: 30 max: 60
3. Setzen Sie die Gültigkeit eines Pins in Stunden, min: 1 max: 24
4. Es ist empfohlen alle 2FA Typen zu konfigurieren.



QR-Code

CRANIX Ivarkoly (Varkoly Lehrer) Cranix zweifaktor Authorisierung...

Profil

Konfigurieren Sie Ihre zweifaktor Authorisierung

Typ von zweifaktor Authorisierung	MAIL	
Pin Gültigkeit	300	Sekunden
Gültigkeit einer Sitzung	12	Stunden
Email Address	email@domain.com	

1. Wählen Sie den 2FA Typ
2. Setzen Sie die Gültigkeit eines Pins in Sekunden. min: 30 max: 600
3. Setzen Sie die Gültigkeit eines Pins in Stunden. min: 1 max: 24
4. Es ist empfohlen alle 2FA Typen zu konfigurieren.
5. Tragen Sie Ihre E-Mailadresse ein
6. Sie können später alle Parameter ändern.
7. Bitte beachten Sie, dass man die 2FA-Konfiguration, die man zur Anmeldung benutzt hat nicht selber löschen kann.

CRX2fa

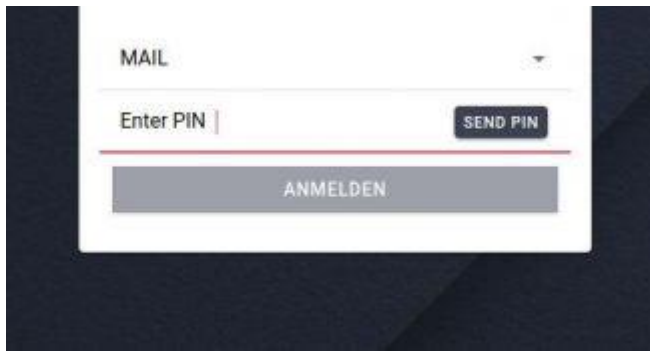
Mail CRX2FA

Nachdem man mindestens eine CRX2FA konfiguriert hat, muss man sich abmelden!

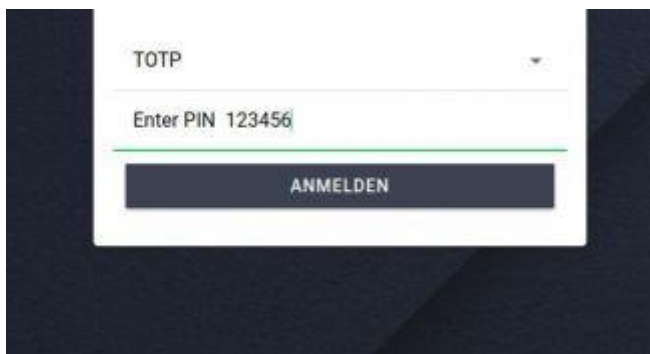
Nach erneuter Anmeldung wird man aufgefordert ein PIN einzugeben. Ggf muss man einen CRX2FA Typ auswählen. Beim MAIL-Typ muss also zuerst ein Pin gesendet werden.

Anmeldung mit CRANIX 2FA

CRX2FA Typ auswählen



PIN senden



PIN eingeben und anmelden