

Security-Parameter

 Sprache: **Deutsch** · [English](#)

Security-Parameter

Sicherheitsrichtlinien konfigurieren – Passwortstärke, Sperren, IP-Filter, Session-Timeout und Passwort-Reset-Mails.

REFERENZ

ADMINISTRATOR

STAND: JUL 2026

GILT FUER NUCLOS 4.2026.X

Auf dieser Seite

- [Parameter](#)
- [Reguläre Ausdrücke für die Passwortkomplexität](#)
- [Verwandte Seiten](#)

In den System-Parametern definierst du die Sicherheitsrichtlinien des Systems – Passwortstärke, Sperren, IP-Beschränkungen und Session-Timeout.

Parameter

Parameter	Wert	Beschreibung
SECURITY_PASSWORD_STRENGTH_LENGTH	5	Minimale Passwortlänge.
SECURITY_PASSWORD_STRENGTH_REGEX	RegExp	Regulärer Ausdruck für die Passwortkomplexität (Beispiele unten).
SECURITY_PASSWORD_STRENGTH_DESCRIPTION	Text	Beschreibung des RegExp, wird dem Benutzer angezeigt.
SECURITY_PASSWORD_HISTORY_DAYS	90	Zeitraum (Tage), in dem ein Passwort nicht wiederverwendet werden darf.
SECURITY_PASSWORD_HISTORY_NUMBER	3	Anzahl der letzten Passwörter, die nicht wiederverwendet werden dürfen.
SECURITY_PASSWORD_INTERVAL	90	Zeitraum (Tage), nach dem das Passwort geändert werden muss.
SECURITY_LOCK_ATTEMPTS	5	Ungültige Loginversuche bis zur automatischen Kontosperrung.
SECURITY_LOCK_USER_PERIOD	10	Tage ohne Login, nach denen ein Konto automatisch gesperrt wird.
SECURITY_PASSWORD_BASED_AUTHENTICATION_ALLOWED	true	<i>false</i> deaktiviert den passwortbasierten Login komplett (nur noch SSO); REST antwortet mit 403.
SECURITY_IP_ALLOW_REMOTEING	Text	Beschränkt das Remoteing-Interface auf IPs (kommasepariert, CIDR erlaubt, z.B. 192.168.1.0/24).
SECURITY_IP_ALLOW_REMOTEING_LOG_ENABLED	true	Steuert Warnmeldungen über geblockte Requests (ab 4.2022.16).
SECURITY_IP_BLOCK_ATTEMPTS	5	Max. Loginversuche je Zeitintervall; danach 429 Too Many Requests.
SECURITY_IP_BLOCK_PERIOD_IN_SECONDS	60	Zeitraum (s) für die o.g. Loginversuche.
SECURITY_IP_PROXY_LIST	Text	Proxy-IPs; wertet dann X-Forwarded-For von hinten aus, um die echte Client-IP zu ermitteln.
SECURITY_SESSION_TIMEOUT_IN_SECONDS	60	Serverseitiges Timeout der HTTP-Sessions (nicht „Angemeldet bleiben“).
RESET_PW_EMAIL_SUBJECT / _MESSAGE	Text	Betreff/Text der Passwort-Reset-Mail (Platzhalter {0}-{3}); muss gesetzt sein, damit die Funktion verfügbar ist.
USERNAME_EMAIL_SUBJECT / _MESSAGE	Text	Betreff/Text der „Benutzername vergessen“-Mail (Platzhalter {0}-{2}).

Reguläre Ausdrücke für die Passwortkomplexität

Beispiele für SECURITY_PASSWORD_STRENGTH_REGEX:

Regulärer Ausdruck	Restriktionen	Beispiele
--------------------	---------------	-----------

^[6,12]\$	Länge 6–12 Zeichen.	passwort, 123456
^[a-zA-Z]\w{5,11}\$	Länge 6–12; erstes Zeichen Buchstabe; nur Buchstaben/Zahlen/Unterstrich.	passwort, pa33w_r1
^(?=.*\d).[6,12]\$	Länge 6–12; mindestens eine Ziffer.	passwor1, Pa33worT
^(?=.*\d)(?=.*[a-z])(?=.*[A-Z]).{6,12}\$	Länge 6–12; je 1 Groß-, Kleinbuchstabe und Ziffer.	Passwor1, pa33woRT
^(?=[^d_]*?\d)\w(\w[!@#%\$%]){6,12}	Länge 6–12; Sonderzeichen erlaubt; erstes Zeichen keine Ziffer/_; mind. 1 Ziffer.	pa\$\$wort1, pa!@#\$%1

Verwandte Seiten

 Benutzer

Konten.

[Öffnen](#)

 Parameter

Alle Parameter.

[Öffnen](#)