# Security-Parameter

In den System-Parametern können verschiedene Sicherheitsrichtlinien definiert werden:

| Parameter | Wert | Beschreibung |
|---|---|---|
| **SECURITY_PASSWORD_STRENGTH_LENGTH** | 5 | Minimale Passwortlänge |
| **SECURITY_PASSWORD_STRENGTH_REGEXP** | Regulärer Ausdruck | Regulärer Ausdruck zur Definition der Passwortkomplexität (Beispiele finden Sie hier) |
| **SECURITY_PASSWORD_STRENGTH_DESCRIPTION** | Text | Beschreibung des Regulären Ausdrucks. Wird dem Benutzer angezeigt. |
| **SECURITY_PASSWORD_HISTORY_DAYS** | 90 | Zeitraum in Tagen, in dem ein Benutzer ein Passwort nicht wiederverwenden darf |
| **SECURITY_PASSWORD_HISTORY_NUMBER** | 3 | Anzahl der letzten Passwörter, die ein Benutzer nicht wiederverwenden darf |
| **SECURITY_PASSWORD_INTERVAL** | 90 | Zeitraum in Tagen, nach dem ein Benutzer das eigene Passwort ändern muss |
| **SECURITY_LOCK_ATTEMPTS** | 5 | Anzahl der ungültigen Loginversuche, nach der ein Benutzerkonto automatisch gesperrt wird |
| **SECURITY_LOCK_USER_PERIOD** | 10 | Zeitraum in Tagen, nach dem ein Benutzer automatisch gesperrt wird, falls er sich in dieser Zeit nicht eingeloggt hat |
| | | |
| **SECURITY_PASSWORD_BASED_AUTHENTICATION_ALLOWED** | true | Deaktiviert den passwortbasierten Login komplett (Wert **false**). Auch der RESTful Service weist dann solche Loginversuche mit einem 403 FORBIDDEN zurück. Einzig die Authentifizierung über einen SSO Dienst ist dann noch erlaubt.<br><br>Default: **true** |
| | | |
| **SECURITY_IP_ALLOW_REMOTING** | Text | Ermöglicht die Einschränkung des Remoting Interfaces (vorwiegend vom Rich-Client verwendet) auf die genannten IP Adresse(n). Kommaseparierte Liste die auch eine Schreibweise im CIDR Format erlaubt. Beispiel **192.168.1.0/24** für einen Adressbereich von 192.168.1.0 bis 192.168.1.255<br>Änderungen werden nicht gleich aktiv, es kann bis zu einer Minute dauern.<br><br>Ist der Parameter undefiniert, erfolgt keine Einschränkung. Alle Client Rechner können das Remoting Interface verwenden. |
| **SECURITY_IP_ALLOW_REMOTING_LOG_ENABLED** | true | ab Nuclos 4.2022.16:<br>Steuert die Ausgabe von Warnmeldungen über geblockte Requets (Wert **false** deaktiviert alle Warnmeldungen). Nur in Verwendung, wenn eine Filterung mittels SECURITY_IP_ALLOW_REMOTING erfolgt.<br><br>Default: **true** |
| **SECURITY_IP_BLOCK_ATTEMPTS** | 5 | Maximal erlaubte Anzahl von Login-Versuchen in einem Zeitintervall. Wird die Anzahl erreicht, werden weitere Loginversuche von der gleichen IP mit HTTP-Status "429 Too Many Requests" abgewiesen.<br><br>Ist der Parameter undefiniert oder <= 0, erfolgen niemals IP-Sperren. |
| **SECURITY_IP_BLOCK_PERIOD_IN_SECONDS** | 60 | Der Zeitraum in welchem die o.g. Anzahl an Loginversuchen stattfinden darf, in Sekunden.<br><br>Ist der Parameter undefiniert oder <= 0, erfolgen niemals IP-Sperren. |

| | | |
|---|---|---|
| **SECURITY_IP_PROXY_LIST** | Text | Wenn IP-Sperren aktiv sind oder das Remoting Interface eingeschränkt wurde, kann optional über diesen Parameter eine kommaseparierte Liste von Proxy-IPs definiert werden.<br><br>Wird dann ein Loginversuch / Remoting-Request von einer IP festgestellt, die sich auf dieser Liste befindet, so wird stattdessen versucht, den X-Forwarded-For Header des Requests auszuwerten. Die meisten Proxys tragen hier die IP, von der sie selbst den Request erhalten haben, an letzter Stelle ein. Der Werte wird daher von hinten nach vorne durchsucht bis eine IP gefunden wurde, die nicht als Proxy definiert wurde. Diese IP wird dann ggf. blockiert bzw. geprüft ob die Verwendung des Remoting Interface erlaubt ist. |
| | | |
| **SECURITY_SESSION_TIMEOUT_IN_SECONDS** | 60 | Definiert das serverseitige Timeout der (HTTP) Sessions. Betrifft nicht die Option "Angemeldet bleiben" beim Webclient Login. |
| | | |
| **RESET_PW_EMAIL_SUBJECT** | Text | Betreff für eine Email beim Passwortreset, muss gesetzt sein damit Funktion verfügbar ist |
| **RESET_PW_EMAIL_MESSAGE** | Text | Text für eine Email beim Passwortreset, muss gesetzt sein damit Funktion verfügbar ist.<br><br>Verfügbare Platzhalter:<br><br>• {0} - Vorname<br>• {1} - Nachname<br>• {2} - username<br>• {3} - password reset token<br><br>Der eigentliche Passwortreset erfolgt via Aufruf von https://initiativemusik-dev.lucaas.net/webclient/#/account/resetPassword/{2}/{3} |
| **USERNAME_EMAIL_SUBJECT** | Text | Betreff für eine Email bei vergessenem Nutzernamen, muss gesetzt sein damit Funktion verfügbar ist |
| **USERNAME_EMAIL_MESSAGE** | Text | Text für eine Email beim vergessenem Nutzernamen, muss gesetzt sein damit Funktion verfügbar ist<br><br>Verfügbare Platzhalter:<br><br>• {0} - Vorname<br>• {1} - Nachname<br>• {2} - username |