

Security parameters

🌐 Language: [Deutsch](#) · [English](#)

📖 Security parameters

Configure security policies – password strength, lockouts, IP filtering, session timeout and password reset mails.

REFERENZ ADMINISTRATOR UPDATED: JUL 2026 APPLIES TO NUCLOS 4.2026.X

On this page

- Parameters
- Regular expressions for password complexity
- Related pages

In the system parameters you define the system's security policies – password strength, lockouts, IP restrictions and session timeout.

Parameters

Parameter	Value	Description
SECURITY_PASSWORD_STRENGTH_LENGTH	5	Minimum password length.
SECURITY_PASSWORD_STRENGTH_REGEX	regexp	Regular expression for password complexity (examples below).
SECURITY_PASSWORD_STRENGTH_DESCRIPTION	text	Description of the regexp, shown to the user.
SECURITY_PASSWORD_HISTORY_DAYS	90	Period (days) during which a password may not be reused.
SECURITY_PASSWORD_HISTORY_NUMBER	3	Number of recent passwords that may not be reused.
SECURITY_PASSWORD_INTERVAL	90	Period (days) after which the password must be changed.
SECURITY_LOCK_ATTEMPTS	5	Invalid login attempts until the account is locked automatically.
SECURITY_LOCK_USER_PERIOD	10	Days without login after which an account is locked automatically.
SECURITY_PASSWORD_BASED_AUTHENTICATION_ALLOWED	true	<i>false</i> disables password login entirely (SSO only); REST answers 403.
SECURITY_IP_ALLOW_REMOTING	text	Restricts the remoting interface to IPs (comma-separated, CIDR allowed, e.g. 192.168.1.0/24).
SECURITY_IP_ALLOW_REMOTING_LOG_ENABLED	true	Controls warnings about blocked requests (from 4.2022.16).
SECURITY_IP_BLOCK_ATTEMPTS	5	Max. login attempts per interval; then 429 Too Many Requests.
SECURITY_IP_BLOCK_PERIOD_IN_SECONDS	60	Period (s) for the above login attempts.
SECURITY_IP_PROXY_LIST	text	Proxy IPs; then evaluates X-Forwarded-For from the end to find the real client IP.
SECURITY_SESSION_TIMEOUT_IN_SECONDS	60	Server-side timeout of HTTP sessions (not „stay signed in“).
RESET_PW_EMAIL_SUBJECT / _MESSAGE	text	Subject/text of the password reset mail (placeholders {0}-{3}); required for the feature to be available.
USERNAME_EMAIL_SUBJECT / _MESSAGE	text	Subject/text of the „forgot user name“ mail (placeholders {0}-{2}).

Regular expressions for password complexity

Examples for SECURITY_PASSWORD_STRENGTH_REGEX:

Regular expression	Restrictions	Examples
--------------------	--------------	----------

<code>^[6,12]\$</code>	Length 6–12 characters.	password, 123456
<code>^[a-zA-Z]\w{5,11}\$</code>	Length 6–12; first character a letter; only letters/digits/underscore.	password, pa33w_r1
<code>^(?=.*\d).[6,12]\$</code>	Length 6–12; at least one digit.	password1, Pa33worT
<code>^(?=.*\d)(?=.*[a-z])(?=.*[A-Z]).{6,12}\$</code>	Length 6–12; at least one upper-case, one lower-case letter and one digit.	Passwor1, pa33woRT
<code>^(?=[^\d_].*\d)\w(\w[!@#%\$%]){6,12}</code>	Length 6–12; special characters allowed; first character not a digit/_; at least 1 digit.	pa\$\$wort1, pa!@#\$%1

Related pages

 User

Accounts.

[Open](#)

 Parameter

All parameters.

[Open](#)