User Authentication Commands

connectorctl userauth lock

To lock out a **spacesadmin** user from the GUI after a specific interval or incorrect password login attempts, use the **connectorctl userauth lock** command.

connectorctl userauth lock { **-d** *deny-attempt-count* | **-i** *interval* | **-s** }

Syntax Description

Keywords and Variables	Description
-d *deny-attempt-count*	Number of incorrect login attempts.
-i *interval*	Lock out the interval.
-s	Shows current configuration.

Command History

Release 3	This command is introduced.

Examples

The following example shows how to lock out the **spacesadmin** user from the GUI for a period of 4 minutes after 2 unsuccessful login attempts with an incorrect password:

```
[spacesadmin@ connector ~]$ connectorctl userauth lock -d 2 -i 4
Executing command:userauth
Command execution status:Success

Successfully updated user lock profile
```

The following example shows how to view the current lockout configurations:

```
[spacesadmin @ connector ~ ]S connectorctl userauth lock - s
Executing command:userauth
Command execution status:Success

Deny attempt count:3
Lockout interval:1
```

connectorctl userauth password

To configure the strength of the password, set an expiry period and minimum length of the password, use the **connectorctl userauth password** command.

connectorctl userauth password { **-l** *password-length* | **-p { yes | no }** | **-r { yes | no }** | **-e { yes | no }** | **-u** *password-reuse* | **-s** }

Syntax Description

Keywords and Variables	Description
-l *password-length*	Minimum password length. Default value is eight.
-p { yes | no }	Enables a strong password. Default value is no.
-r { yes | no }	Rejects a weak password. Default value is yes.
-e { yes | no }	Password expires after 60 days. Default value is no.
-u *password-reuse*	Number of previous passwords that can be reused. Default value is zero.
-s	Shows current configuration

Command History

Release 3	This command is introduced.

Examples

The following example shows how to define the minimum length of the password as 9, configure a flag that requires a strong password, configure a flag that rejects a weak password, set the password to expire after 60 days, and configure that one previous password cannot be reconfigured again.

```
[spacesadmin@connector ~]$ connectorctl userauth password -l 9 -p yes -r yes -e yes -u 1
Executing command:userauth
Command execution status:Success
-----------------------
Updated password policy
User password expiry set to 60 days
Successfully updated user password profile
```

The following example shows how to view the password limitations currently configured.

```
[spacesadmin@connector ~]$ connectorctl userauth password -s
Executing command:userauth
Command execution status:Success
-----------------------
Password length: 8
Enable strong password: no
Reject weak password: yes
Expire password after 60 days: no
Number of previous passwords which cannot be reused: 0
```

connectorctl userauth reset

To reset the user password and lock configuration to system default, use the **connectorctl userauth reset** command.

connectorctl userauth reset

Syntax Description

This command has no keywords or arguments.

Command History

Release 3	This command is introduced.

Examples

```
[spacesadmin@connector ~]$ connectorctl userauth reset
Executing command:userauth
Command execution status:Success
-----------------------
User auth profile reset to system default
```