



DeviceDeployer Admin Guide and Reference Manual

April 2024

Table of Contents

Introduction	1
Command Line Arguments	2
General examples	2
Help	3
List of available arguments	3
Professional services are available	5

Introduction

DeviceDeployer is a power tool that allows you to pre-configure SafeConsoleReady Devices (DL4, K350, Sentry ONE) in as little as 30 seconds, with no button pushing required. Plug devices, one after another, into a Windows PC out of the box and see them immediately become securely configured, no further device interaction is required. No accessories are needed. The device is ready to hand to your end-user, either they pick their own password according to your policy¹ OR it has been preset with a random password that you provide them.

DeviceDeployer works for both centrally and locally managed devices

Presetting devices with powerful random passwords for locally managed devices OR connecting them to SafeConsole has never been quicker or more effortless.

Password management is superior with SafeConsole but possible when locally managed

The scalable method for remote password resets with an audit trail is available when managing devices with SafeConsole. If the K350 or DL4 is not centrally managed and a User role is activated, the user data can be recovered using the Admin role password. It is also possible to output device details and Admin passwords into an Excel-ready CSV file with DeviceDeployer.

¹ Notify your account manager when you place your order as all firmware versions do not supports this feature.



```
DeviceDeployer --dsu --al=42 --tk=https://nightly.safeconsolecloud.io/connect --pwd=RAND --pwdlog=pwds.csv --cont
Warning: software update is disabled while SafeConsole registration is enabled.
Please ensure the device software is up-to-date or the device will not be able to unlock after registration.
Scanning for device...
Device(s) found:
DL40000013

Detected device Type: DL4FIP5
Detected device Serial: DL40000013
Device(s) found:
DL40000013

Registering device to SafeConsole...
```

Screenshot of the DeviceDeployer connecting a DL4 to SafeConsole.

Command Line Arguments

Open a Command prompt and run the tool (default name DeviceDeployer, or DeviceDeployer.exe) with any of the following arguments. Some arguments require others.

Professional services are available

DeviceDeployer is possible to use with DataLocker devices, and dedicated support is available from our professional services team. Talk to your account manager for more information. Note that DeviceDeployer is not supported by general DataLocker support.

General examples

```
DeviceDeployer --al=42 --cont --log=output.txt --sc=1
```

(Sets the autolock time to 42 minutes, sets SafeConsole on, turns on continuous mode, and logs to output.txt)

```
DeviceDeployer --al 42 --cont --log output.txt --sc 1
```

(Same settings, but using spaces instead of =)

Note that if = is used, the parameter value must immediately follow. If you wish to use spaces instead, do not use the = sign.

```
DeviceDeployer --cont --pwd=RAND --pwdlog=pwd.csv
```

(Turn on continuous mode, set a random admin password, log generated passwords to pwd.csv on desktop)

```
DeviceDeployer -h
```

Displays all command-line options



Help

-?, -h, - Displays help and all command-line options.

List of available arguments

DataLocker DeviceDeployer
Client version: 6.5.1

Usage: DeviceDeployer [options]
DataLocker DeviceDeployer

Options:

-?, -h, --help	Displays help on commandline options.
--help-all	Displays help including Qt specific options.
--log, --logfile <file>	Log output to [file] specified(on desktop), e.g. --log=update.txt
--cont, --continuous	Run this application in continuous mode. Allows devices to be configured in sequence without re-launching.
--cpwd, --currentpassword <password>	Send current administrator password [password]. Required to change admin password if the drive is initialized.
--tk, --token <token>	Set SafeConsole registration token to [token].



--utk, --usertoken <token>

Set SafeConsole user token to [token].

--dsu, --disablesoftwareupdate

Do not update device client software. Important note: if SafeConsole registration is being performed, the client must be up-to-date in order to unlock afterwards.

-e, --email <email>

Set SafeConsole user email to [email].

--sn, --serialnumber <serialnumber>

Use on a specific device, otherwise use the first device found.

--cf1 <cf1>

First custom message field for SafeConsole registration.

--cf2 <cf2>

Second custom message field for SafeConsole registration.

--cf3 <cf3>

Third custom message field for SafeConsole registration.

--reset

Resets a device that has been registered to SafeConsole and where the policy allows it ('Disable users from resetting device' is unchecked).



<code>--pwd, --adminpassword <password></code>	Set administrator password to [password]. Use RAND to generate a random password. if RAND is used, requires the use of --pwdlog. Note that if the drive is initialized, you must also use --cpwd.
<code>--pwdlog, --passwordlog <file></code>	Write passwords changed to csv [file] on desktop, along with device serial number and timestamp
<code>--bm, --blockmenu <block></code>	Block out on-device menus for configured items (1) or unblock items (0) [block]. Note: only works if the device is not registered to SafeConsole.
<code>-u, --user <user></code>	Set password to [user] to enable user account or disable user account (0). The default and best practice is to allow the user to set their own password. Use RAND to generate a random password. if RAND is used, requires the use of --pwdlog.
<code>--sc, --safeconsole <on></code>	Set safeconsole mode on (1) or off (0) [on].
<code>--ro, --readonly <on></code>	Set readonly mode on (1) or off (0) [on].
<code>--al, --autolock <time></code>	Set autolock time in minutes (2-261) or off (0) [time].
<code>--pl, --passwordlength <length></code>	Set minimum password length (8-30) to [length]



<code>--ra, --requirealphabet <on></code>	Set requirement for alphabet in password on (1) or off (0) [on]
---	---

<code>--rn, --requirenumber <on></code>	Set requirement for number in password on (1) or off (0) [on]
---	---

<code>--rs, --requirespecial <on></code>	Set requirement for special character in password on (1) or off (0) [on]
--	--

<code>--mfa, --maxfailedattempts <max></code>	Set requirement for max failed unlock attempts (10-50) to [max]
---	---

<code>--det, --detonatedevice <on></code>	Set device destruction (not only data) when brute forced. On (1) or off (0) [on]
---	--

<code>--fpc, --forcepasswordchange <forcepasswordchange></code>	Force the admin account to change password on the next use (1) or keep using default password (0).
---	--

<code>--rem, --reportremovable <reportremovable></code>	(K350 only) Have the device report as removable (1) / fixed (0)
---	---