



CLI structure

SANtricity commands

NetApp
November 15, 2022

Table of Contents

- CLI structure 1
 - Structure of CLI commands 1
 - Interactive mode 1
 - CLI command wrapper syntax 1
 - Downloadable SMcli command line parameters 3
 - Legacy command line parameters 8

CLI structure

Structure of CLI commands

The CLI commands are in the form of a command wrapper and elements embedded into the wrapper. A CLI command consists of these elements:

- A command wrapper identified by the term `SMcli`
- The storage array identifier
- Terminals that define the operation to be performed
- Script commands

The CLI command wrapper is a shell that identifies storage array controllers, embeds operational terminals, embeds script commands, and passes these values to the script engine.

All CLI commands have the following structure:

```
SMcli *storageArray terminal script-commands*;
```

- `SMcli` invokes the command line interface.
- `storageArray` is the name or the IP address of the storage array.
- `terminal` is a CLI value that defines the environment and the purpose for the command.
- `script-commands` are one or more script commands or the name of a script file that contains script commands. (The script commands configure and manage the storage array.)

If you enter an incomplete or inaccurate `SMcli` string that does not have the correct syntax, parameter names, options, or terminals, the script engine returns usage information.

Interactive mode

If you enter `SMcli` and a storage array name, but do not specify CLI parameters, script commands, or a script file, the command line interface runs in interactive mode. Interactive mode lets you run individual commands without prefixing the commands with `SMcli`.

In interactive mode, you can enter a single command, view the results, and enter the next command without typing the complete `SMcli` string. Interactive mode is useful for determining configuration errors and quickly testing configuration changes.

To end an interactive mode session, type the operating system-specific command. For Linux, this key combination is **Control-D**. For Windows, this key combination is **Control-Z + ENTER**.

CLI command wrapper syntax

General syntax forms of the CLI command wrappers are listed in this section. The conventions used in the CLI command wrapper syntax are listed in the following table.

Convention	Definition
a b	Alternative ("a" or "b")
<i>italicized-words</i>	Needs user input to fulfill a parameter (a response to a variable)
[...] (square brackets)	Zero or one occurrence (square brackets are also used as a delimiter for some command parameters)
{ ... } (curly braces)	Zero or more occurrences
(a b c)	Choose only one of the alternatives
a & b	And/or. This is used for https client mode, when you can use with one or both controller IP addresses. This way, if one controller is not responding, SMcli will use the alternative IP address. This also covers the case when both IP addresses are required, such as for firmware download.



To run all of the CLI commands you must have administrator privileges. Some CLI commands will run without administrator privileges. Many commands, however, will not run. If the CLI command does not run because you do not have correct privileges, the CLI returns an exit code of 12.

Example in https client mode

The following examples demonstrate the https client mode command line parameters described in [Command line parameters](#).

```
SMcli (Controller A host-name-or-IP-address&|
Controller B host-name-or-IP-address) -u username -p password -c
"commands;" [-clientType (auto | https | symbol)]
```



If you do not specify a `clientType`, but do include the `-u` option and the `username` variable, the system will use either `https` or `symbol` client mode, whichever is available.

Examples in symbol client mode

The following examples demonstrate the `symbol` client mode command line parameters described in [Command line parameters](#).

```
SMcli **-a** **email:** email-address [host-name-or-IP-address1 [host-  
name-or-IP-address2]] [**-n** storage-system-name | **-w** wwID | **-h**  
host-name] [**-I** information-to-include] [**-q** frequency] [**-S**]
```



The `-a` command line option is not supported for the E2800 or E5700 storage array.

```
SMcli **-x** **email:** email-address [host-name-or-IP-address1 [host-  
name-or-IP-address2]] [**-n** storage-system-name | **-w** wwID | **-h**  
host-name] [**-S**]
```



The `-x` command line option is not supported for the E2800 or E5700 storage array.

```
SMcli (**-a** | **-x**) **trap:** community, host-name-or-IP-address  
[host-name-or-IP-address1 [host-name-or-IP-address2]] [**-n** storage-  
system-name | **-w** wwID | **-h** host-name] [**-S**]
```



The `-a` and `-x` command line options are not supported for the E2800 or E5700 storage array.

```
SMcli **-d** [**-w**] [**-i**] [**-s**] [**-v**] [**-S**]
```



The `-s` command line option is not supported for the E2800 or E5700 storage array.

```
SMcli host-name-or-IP-address **-F** email-address [**-g**  
contactInfoFile] [**-S**]
```

```
SMcli **-A** [host-name-or-IP-address [host-name-or-IP-address]] [**-S**]
```

```
SMcli **-X** (**-n** storage-system-name | **-w** wwID | **-h** host-name)
```

```
SMcli **-?**
```

Downloadable SMcli command line parameters

11.60 and newer downloadable SMcli command line parameters

The SANtricity OS 11.60 release includes the ability to download and install the http-based version of CLI (also referred to as "Secure CLI" or SMcli) directly through the SANtricity System Manager. This downloadable version of the SMcli is available on EF600, EF300, E5700, EF570, E2800, and EF280 controllers. To download the SMcli within the SANtricity System Manager, select **Settings > System** and **Add-ons > Command Line Interface** .



A Java Runtime Environment (JRE), version 8 and above, must be available on the management system where you plan to run the CLI commands.

As with previous versions of the SMcli, the SMcli downloadable through the SANtricity System Manager has a unique set of parameters. For information on using command line parameters for SANtricity OS 11.53 and older releases, see [Legacy command line parameters](#)

Multifactor authentication

If SAML (Security Assertion Markup Language) is enabled, only access tokens can be used with the CLI. If SAML is not enabled, the username/password or access tokens can be used. Access tokens can be generated through the SANtricity System Manager.

Table 1. Access token, username, and password parameters


Parameter	Definition
-t	Defines the access token to be used for authentication with a storage array. An access token is a replacement for supplying the username and password.
-T (uppercase)	This argument requires one of two arguments: <ul style="list-style-type: none">• <code>access_token-file</code> - Contains the access token to use for authentication• <code>-</code> (dash) - Read the access token from stdin
-u	Follow this parameter with the <i>username</i> variable. This parameter is required whenever an access token is not used.
-p	Defines the password for the storage array on which you want to run commands. A password is not necessary under these conditions: <ul style="list-style-type: none">• A password has not been set on the storage array.• The password is specified in a script file that you are running.


Parameter	Definition
-P (uppercase)	<p>This argument requires one of two arguments:</p> <ul style="list-style-type: none"> • <i>password_file</i> - Contains the password to use for authentication. • - (one dash) - Read the password from <code>stdin</code>.

General https mode command line parameters

The downloadable SMcli only supports https mode. The following are commonly used command line parameters for https mode.

Table 2. https command line parameters

Parameter	Definition
<i>host-name-or-IP-address</i>	<p>Specifies either the host name or the Internet Protocol (IP) address (<i>xxx.xxx.xxx.xxx</i>) of an out-of-band managed storage array.</p> <p>When managing out-of-band storage management through the Ethernet connection on each controller, you must specify the <i>host-name-or-IP-address</i> of the controllers.</p>
-k	<p>This optional argument allows an https client to operate in insecure mode. This means that the storage array's certificate will not be validated. By default, if omitted, the proper validation will be performed.</p> <div>  <p>For additional information on managing storage array certificates, see Managing stored certificates command line parameters.</p> </div>
-e	Runs the commands without performing a syntax check first.
-L (uppercase)	Displays the legal notices for Downloadable SMcli.

Parameter	Definition
-n	<p>Specifies the locally stored label on which you want to run the script commands. This is optional when you use <i>host-name-or-IP-address</i>. The locally stored label is required when the <i>host-name-or-IP-address</i> is not used.</p> <div>  <p>For additional information on using locally stored labels to manage storage arrays, see Managing stored arrays command line parameters.</p> </div>
-o	<p>Specifies a file name for all output text that is a result of running the script commands. Use the -o parameter with these parameters:</p> <ul style="list-style-type: none"> • -c • -f <p>If you do not specify an output file, the output text goes to standard output (stdout). All output from commands that are not script commands is sent to stdout, regardless of whether this parameter is set.</p>
-S (uppercase)	<p>Suppresses informational messages describing the command progress that appear when you run script commands. (Suppressing informational messages is also called silent mode.) This parameter suppresses these messages:</p> <ul style="list-style-type: none"> • Performing syntax check • Syntax check complete • Executing script • Script execution complete • SMcli completed successfully
-version	Displays the downloadable SMcli version
-?	Shows usage information about the CLI commands.

Managing stored arrays

The following command line parameters allow you to manage stored arrays through your locally stored label.



The locally stored label may not match the actual storage array name displayed under the SANtricity System Manager.

Table 3. Managing stored arrays command line parameters


Parameter	Definition
<code>SMcli storageArrayLabel show all</code>	Displays all locally stored labels and their associated addresses
<code>SMcli storageArrayLabel show label <LABEL></code>	Displays the addresses associated with the locally stored label named <LABEL>
<code>SMcli storageArrayLabel delete all</code>	Deletes all locally stored labels
<code>SMcli storageArrayLabel delete label <LABEL></code>	Deletes the locally stored label named <LABEL>
<code>SMcli <host-name-or-IP-address> [host-name-or-IP-address] storageArrayLabel add label <LABEL></code>	<ul style="list-style-type: none"> • Adds a locally stored label with name <LABEL> containing the addresses provided • Updates are not directly supported. To update, delete label and then re-add. <div>  <p>The SMcli does not contact the storage array when adding a locally stored label.</p> </div>

Table 4. Managing stored certificates command line parameters

Parameter	Definition
<code>SMcli localCertificate show all</code>	Displays all trusted certificates stored locally
<code>SMcli localCertificate show alias <ALIAS></code>	Displays a locally stored trusted certificate with the alias <ALIAS>
<code>SMcli localCertificate delete all</code>	Deletes all trusted certificates stored locally
<code>SMcli localCertificate delete alias <ALIAS></code>	Deletes a locally stored trusted certificate with the alias <ALIAS>
<code>SMcli localCertificate trust file <CERT_FILE> alias <ALIAS></code>	<ul style="list-style-type: none"> • Saves a certificate to be trusted with the alias <ALIAS> • The certificate to be trusted is downloaded from the controller in a separate operation, such as using a web browser

Parameter	Definition
SMcli <host-name-or-IP-address> [host-name-or-IP-address] localCertificate trust	<ul style="list-style-type: none"> • Connects to each address and saves the certificate returned into the trusted certificate store • The hostname or IP address specified is used as the alias for each certificate saved this way • User should verify the certificate on the controller(s) is to be trusted before running this command • For highest security, the trust command that takes a file should be used to ensure the certificate did not change between user validation and running of this command

Legacy command line parameters

11.53 and older command line parameters

The SANtricity OS 11.40 release introduced, for the E2800 and E5700 controllers with embedded web services, the ability to interact on the Command Line using a secure HTTPS protocol. These controllers can optionally use the SYMBol protocol for Command Line interactions instead. The SYMBol protocol is the only supported protocol for the E2700 and E5600 controllers. To preserve existing scripts and minimize transition time, the CLI options and grammar are preserved as much as possible. However, there are some differences in the capabilities of the E2800 and E5700 controllers with regards to security, authentication, AutoSupport, and alert messaging that render some of the CLI grammar for those controllers obsolete. However, in some cases the grammar is only obsolete on the E2800 or E5700 when the new https protocol is used.

For the new parameters that only apply to the **https** client type, it follows that they also apply only to the E2800 or E5700 controllers.

Table 5. https command line parameters




Parameter	Definition
-clientType	<p>This argument forces the creation of an appropriate script engine. Use this optional parameter with one of the following values:</p> <ul style="list-style-type: none"> • auto - Device discovery is automatically performed to detect the appropriate script engine type. • https - A REST-based script engine is created. • symbol - A SYMBol-based script engine is created.


Parameter	Definition
-u	<p>Follow this parameter with the <i>username</i> variable. The username is only required for the https client type. This argument is not applicable to the symbol client type and will be silently ignored.</p> <p>If the username argument is specified, device discovery is performed to determine the correct client type (https vs. symbol).</p>
-P	<p>This argument requires one of two arguments:</p> <ul style="list-style-type: none"> • <i>password_file</i> - Contains the password to use for authentication. • - (one dash) - Read the password from <i>stdin</i>. <p>Note that the addition of this argument is applicable to all controllers, regardless of whether the https client type or symbol client type is used.</p>
-k	<p>This optional argument allows an https client to operate in insecure mode. This means that the storage array's certificate will not be validated. By default, if omitted, the proper authentication will be performed. This argument is not applicable to the symbol client type and will be silently ignored.</p>

Command line parameters that only apply to E2700 or E5600 controllers

Because the E2700 and E5600 controllers do not have embedded alert management capabilities, these command line parameters are applicable. These parameters are not applicable to the E2800 or E5700 controllers.

Table 6. E2700 and E5600 command line parameters

Parameter	Definition
-a	<p>Adds a Simple Network Management Protocol (SNMP) trap destination or an email address alert destination.</p> <ul style="list-style-type: none"> • When you add an SNMP trap destination, the SNMP community is automatically defined as the community name for the trap, and the host is the IP address or Domain Name Server (DNS) host name of the system to which the trap should be sent. • When you add an email address for an alert destination, the email-address is the email address to which you want the alert message to be sent. <div>  <p>This command line option is obsolete for the E2800 and E5700 storage arrays. Use the RESTful API, SANtricity System Manager, or cURL commands.</p> </div>
-m	<p>Specifies the host name or the IP address of the email server from which email alert notifications are sent.</p> <div>  <p>This command line option is obsolete for the E2800 and E5700 storage arrays. Use the RESTful API, SANtricity System Manager, or cURL commands.</p> </div>
-s (lowercase)	<p>Shows the alert settings in the configuration file when used with the -d parameter.</p> <div>  <p>This command line option is obsolete for the E2800 and E5700 storage arrays. Use the RESTful API, SANtricity System Manager, or cURL commands.</p> </div>

Parameter	Definition
-x (lowercase)	<p>Removes an SNMP trap destination or an email address alert destination. The <i>community</i> is the SNMP community name for the trap, and the <i>host</i> is the IP address or DNS host name of the system to which you want the trap sent.</p> <div>  <p>This command line option is obsolete for the E2800 and E5700 storage arrays. Use the RESTful API, SANtricity System Manager, or cURL commands.</p> </div>

Command line parameters that apply to all controllers running with a symbol client type

Table 7. Symbol client command line parameters

Parameter	Definition
-R (uppercase)	<p>Defines the user role for the password. The roles can be either:</p> <ul style="list-style-type: none"> • admin — The user has privilege to change the storage array configuration. • monitor — The user has privilege to view the storage array configuration, but cannot make changes. <p>The -R parameter is valid only when used with the -p parameter, which specifies that you define a password for a storage array.</p> <p>The -R parameter is required only if the dual password feature is enabled on the storage array. The -R parameter is not necessary under these conditions:</p> <ul style="list-style-type: none"> • The dual password feature is not enabled on the storage array. • Only one admin role is set and the monitor role is not set for the storage array.

Command line parameters applicable to all controllers and all client types

Table 8. All controller and client type command line parameters

Parameter	Definition
<i>host-name-or-IP-address</i>	<p>Specifies either the host name or the Internet Protocol (IP) address (<i>xxx.xxx.xxx.xxx</i>) of an in-band managed storage array or an out-of-band managed storage array.</p> <ul style="list-style-type: none"> • If you are managing a storage array by using a host through in-band storage management, you must use the <i>-n</i> parameter or the <i>-w</i> parameter if more than one storage array is connected to the host. • If you are managing a storage array by using out-of-band storage management through the Ethernet connection on each controller, you must specify the <i>host-name-or-IP-address</i> of the controllers. • If you have previously configured a storage array in the Enterprise Management Window, you can specify the storage array by its user-supplied name by using the <i>-n</i> parameter. • If you have previously configured a storage array in the Enterprise Management Window, you can specify the storage array by its World Wide Identifier (WWID) by using the <i>-w</i> parameter.
<i>-A</i>	Adds a storage array to the configuration file. If you do not follow the <i>-A</i> parameter with a <i>host-name-or-IP-address</i> , auto-discovery scans the local subnet for storage arrays.
<i>-c</i>	Indicates that you are entering one or more script commands to run on the specified storage array. End each command with a semicolon (;). You cannot place more than one <i>-c</i> parameter on the same command line. You can include more than one script command after the <i>-c</i> parameter.
<i>-d</i>	Shows the contents of the script configuration file. The file content has this format: <i>storage-system-name host-name1 host-name2</i>
<i>-e</i>	Runs the commands without performing a syntax check first.
<i>-F</i> (uppercase)	Specifies the email address from which all alerts will be sent.

Parameter	Definition
-f (lowercase)	Specifies a file name that contains script commands that you want to run on the specified storage array. The -f parameter is similar to the -c parameter in that both parameters are intended for running script commands. The -c parameter runs individual script commands. The -f parameter runs a file of script commands. By default, any errors that are encountered when running the script commands in a file are ignored, and the file continues to run. To override this behavior, use the <code>set session errorAction=stop</code> command in the script file.
-g	Specifies an ASCII file that contains email sender contact information that will be included in all email alert notifications. The CLI assumes that the ASCII file is text only, without delimiters or any expected format. Do not use the -g parameter if a <code>userdata.txt</code> file exists.
-h	Specifies the host name that is running the SNMP agent to which the storage array is connected. Use the -h parameter with these parameters: <ul style="list-style-type: none"> • -a • -x
-I (uppercase)	Specifies the type of information to be included in the email alert notifications. You can select these values: <ul style="list-style-type: none"> • <code>eventOnly</code> — Only the event information is included in the email. • <code>profile</code> — The event and array profile information is included in the email. <p>You can specify the frequency for the email deliveries using the -q parameter.</p>
-i (lowercase)	Shows the IP address of the known storage arrays. Use the -i parameter with the -d parameter. The file content has this format: <code>storage-system-name IP-address1 IPaddress2</code>

Parameter	Definition
-n	<p>Specifies the name of the storage array on which you want to run the script commands. This name is optional when you use a <i>host-name-or-IP-address</i>. If you are using the in-band method for managing the storage array, you must use the -n parameter if more than one storage array is connected to the host at the specified address. The storage array name is required when the <i>host-name-or-IP-address</i> is not used. The name of the storage array that is configured for use in the Enterprise Management Window (that is, the name is listed in the configuration file) must not be a duplicate name of any other configured storage array.</p>
-o	<p>Specifies a file name for all output text that is a result of running the script commands. Use the -o parameter with these parameters:</p> <ul style="list-style-type: none"> • -c • -f <p>If you do not specify an output file, the output text goes to standard output (stdout). All output from commands that are not script commands is sent to stdout, regardless of whether this parameter is set.</p>
-p	<p>Defines the password for the storage array on which you want to run commands. A password is not necessary under these conditions:</p> <ul style="list-style-type: none"> • A password has not been set on the storage array. • The password is specified in a script file that you are running. • You specify the password by using the -c parameter and this command: <pre>set session password=password</pre>

Parameter	Definition
-P	<p>This argument requires one of two arguments:</p> <ul style="list-style-type: none"> • <code>password_file</code> - contains the password to use for authentication. • <code>-(dash)</code> - read the password from <code>stdin</code>. <p>Note that the addition of this argument is applicable to all controllers, regardless of whether the https client type or symbol client type is used.</p>
-q	<p>Specifies the frequency that you want to receive event notifications and the type of information returned in the event notifications. An email alert notification containing at least the basic event information is always generated for every critical event. These values are valid for the <code>-q</code> parameter:</p> <ul style="list-style-type: none"> • <code>everyEvent</code> — Information is returned with every email alert notification. • <code>2</code> — Information is returned no more than once every two hours. • <code>4</code> — Information is returned no more than once every four hours. • <code>8</code> — Information is returned no more than once every eight hours. • <code>12</code> — Information is returned no more than once every 12 hours. • <code>24</code> — Information is returned no more than once every 24 hours. <p>Using the <code>-I</code> parameter you can specify the type of information in the email alert notifications.</p> <ul style="list-style-type: none"> • If you set the <code>-I</code> parameter to <code>eventOnly</code>, the only valid value for the <code>-q</code> parameter is <code>everyEvent</code>. • If you set the <code>-I</code> parameter to either the <code>profile</code> value or the <code>supportBundle</code> value, this information is included with the emails with the frequency specified by the <code>-q</code> parameter.

Parameter	Definition
-quick	Reduces the amount of time that is required to run a single-line operation. An example of a single-line operation is the <code>recreate snapshot volume</code> command. This parameter reduces time by not running background processes for the duration of the command. Do not use this parameter for operations that involve more than one single-line operation. Extensive use of this command can overrun the controller with more commands than the controller can process, which causes operational failure. Also, status updates and configuration updates that are collected usually from background processes will not be available to the CLI. This parameter causes operations that depend on background information to fail.
-s (uppercase)	<p>Suppresses informational messages describing the command progress that appear when you run script commands. (Suppressing informational messages is also called silent mode.) This parameter suppresses these messages:</p> <ul style="list-style-type: none"> • <code>Performing syntax check</code> • <code>Syntax check complete</code> • <code>Executing script</code> • <code>Script execution complete</code> • <code>SMcli completed successfully</code>
-v	Shows the current global status of the known devices in a configuration file when used with the <code>-d</code> parameter.
-w	Specifies the WWID of the storage array. This parameter is an alternate to the <code>-n</code> parameter. Use the <code>-w</code> parameter with the <code>-d</code> parameter to show the WWIDs of the known storage arrays. The file content has this format: <code>storage-system-name world-wide-ID IP-address1 IP-address2</code>
-x (uppercase)	Deletes a storage array from a configuration.
-?	Shows usage information about the CLI commands.

Copyright information

Copyright © 2022 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.