

Universal Control 7.5.x Quick Reference Guide

Universal Agent 7.5.x

© 2024 by Stonebranch, Inc. All Rights Reserved.

Table of Contents

1	Usage	4
1.1	uctl COMMAND HOST [LOCAL] [USER] [OPTIONS...]	4
1.2	uctl {-help -version}	4
2	Format	5
2.1	COMMAND {-start -stop -refresh } [-file -encryptedfile [-key]]	5
2.2	HOST -host [-port] [-hostname_retry_count] [-outboundip]	5
2.3	LOCAL [-bif_directory] [-plf_directory] [-system_id]	5
2.4	USER [-userid [-password]]	6
2.5	OPTIONS [{-help -version} [-cmdid] [-crl] [-lang] [-level] [-delay] [-codepage] [- ctl_ssl_cipher_list] [-default_cipher] [-cert -private_key [-private_key_pwd]] [saf_key_ring [-saf_key_ring_label]] [-ssl_implementation] [-ca_certs [- verify_host_name] [-verify_serial_number]]	6

1 Usage

1.1 `uctl COMMAND HOST [LOCAL] [USER] [OPTIONS...]`

1.2 `uctl {-help|-version}`

2 Format

There is a long form and, for most options, a short form available for specifying each option on the command line. The long form is not case-sensitive; the short form is case-sensitive.

Options must be prefixed with a dash (-) character. If an option value is specified, the option and its value must be separated by at least one space.

2.1 COMMAND { -start | -stop | -refresh } [-file | -encryptedfile [-key]]

Long Form	Short Form	Description
-start <i>compname</i>	n/a	Name of the component that is to be started.
-stop <i>compid</i>	-s <i>compid</i>	ID of the component that is to be terminated.
-refresh [<i>compname</i>]	-R [<i>compname</i>]	Name of the component to be refreshed. If no <i>compname</i> is specified, send a REFRESH command to a Universal Broker to instruct it to re-read its configuration parameters and re-read its component definitions.
-file <i>file</i>	-f <i>file</i>	Name of a file from which UCTL options are read.
-encryptedfile <i>file</i>	-x <i>file</i>	Name of an encrypted file from which UCTL options are read. Encrypted UCTL option files are created using Universal Encrypt.
-key <i>key</i>	-K <i>key</i>	Key that was passed to Universal Encrypt when the UCTL option file was encrypted.

2.2 HOST -host [-port] [-hostname_retry_count] [-outboundip]

Long Form	Short Form	Description
-host <i>hostaddress</i>	-i <i>hostaddress</i>	Host network address in dotted form (1.2.3.4) or a host domain name.
-port <i>port</i>	-p <i>port</i>	Host port number on which Universal Broker is listening. Default is the Universal Broker default.
-hostname_retry_count <i>count</i>	n/a	Number of attempts to resolve the host name.
-outboundip <i>host</i>	n/a	Host network address to bind to for all outbound connections. <i>host</i> format is dotted form (1.2.3.4) or a host domain name.

2.3 LOCAL [-bif_directory] [-plf_directory] [-system_id]

Long Form	Short Form	Description
-bif_directory <i>directory</i> ^U	n/a	Broker Interface File (BIF) directory where the Universal Broker interface file is located.
-plf_directory <i>directory</i> ^U	n/a	Program Lock File (PLF) directory where the program lock files are located.
-system_id <i>ID</i> ^Z	n/a	Local Universal Broker with which the UCMD Manager must register before the Manager performs any request.
^U Available for use on UNIX operating systems only. ^Z Available for use on z/OS operating systems only.		

2.4 USER [-userid [-password]]

Long Form	Short Form	Description
-userid <i>user</i>	-u <i>user</i>	Remote user ID with which the command runs.
-pwd <i>password</i>	-w <i>password</i>	Remote user ID's password.

2.5 OPTIONS [{-help | -version} | [-cmdid] [-crl] [-lang] [-level] [-delay] [-codepage] [-ctl_ssl_cipher_list] [-default_cipher] [-cert -private_key [-private_key_pwd]] [saf_key_ring [-saf_key_ring_label]] [-ssl_implementation] [-ca_certs [-verify_host_name] [-verify_serial_number]]

Long Form	Short Form	Description
-ca_certs <i>file</i>	n/a	Name of a PEM-formatted file containing the X.509 certificates for trusted Certificate Authorities (CAs).
-cert <i>file</i>	n/a	Name of a PEM-formatted file containing an X.509 certificate used to identify UCMD to the Broker.
-cmdid <i>id</i>	-C <i>id</i>	Identity of the started component.
-codepage <codepage>	-t <codepage>	Code page used to translate text on the local host.
-crl <i>file / ddname</i>	n/a	File name / ddname of the PEM-formatted file containing the Certificate Revocation List (CRL) issued by the trusted Certificate Authority.

Long Form	Short Form	Description
-ctl_ssl_cipher_list <i>ciphers</i>	n/a	SSL/TLS cipher suites (one or more, in their preferred order) for control SSL/TLS connections. <i>ciphers</i> is a comma-separated list of cipher suite names. Valid values are AES256-GCM-SHA384,AES256-SHA,AES128-GCM-SHA256,AES128-SHA,ECDHE-RSA-AES256-GCM-SHA384,ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AES128-GCM-SHA256,ECDHE-ECDSA-AES128-GCM-SHA256,RC4-SHA,RC4-MD5,DES-CBC3-SHA.
-delay <i>seconds</i>	-d <i>seconds</i>	Maximum delay for transmitting data that may be expected due to network conditions.
-help	-h	Write help file.
-lang <i>language</i>	-L <i>language</i>	Message and text language.
-level <i>level</i>	-l <i>level</i>	Message level: error, warn, info, audit, or trace.
-private_key <i>file</i>	n/a	Name of a PEM-formatted file containing the RSA private key corresponding to the X.509 certificate specified by -cert .
-private_key_pwd <i>password</i>	n/a	Password for the private key file specified by -private_key .
-saf_key_ring <i>name</i>	n/a	SAF (RACF is a SAF implementation) certificate key ring name that Universal Control should use for its certificate.
-saf_key_ring_label <i>label</i>	n/a	Label of the certificate in the SAF (RACF is a SAF implementation) certificate key ring that Universal Control should use for its certificate.
-ssl_implementation <i>option</i> ^Z	n/a	SSL/TLS implementation to be used for network communications. Valid values for <i>option</i> are: <ul style="list-style-type: none"> • openssl: OpenSSL SSL/TLS library is used. • system: z/OS system SSL library is used.
-verify_host_name <i>host</i>	n/a	Specification that the Broker's X.509 certificate must identify a host name that matches <host>.
-verify_serial_number <i>number</i>	n/a	Specification that the Broker's X.509 certificate must have a serial number that matches <i>number</i> . Hexadecimal format is specified with a prefix of 0x or 0X.
-version	-v	Write program version information and exit.
^Z Available for use on z/OS operating systems only.		