CLI Commands during Installation and Upgrade

Live Data CLI Commands

Supported Character Set for Live Data Installation CLI Commands

When working with the CLI (and not exclusively for Live Data), you can use plain alphanumeric characters [0-9] [A-Z] [a-z] and the following additional characters:

- ". " (dot)

- "!" (exclamation mark)

- "@" (at sign)

- "#" (number sign)

- "$" (dollar)

- "%" (percent)

- "^" (caret)

- "*" (star)

- "_" (underscore)

- "+" (plus sign)

- "=" (equal sign)

- "~" (tilde)

- ":" (colon)

- "(" and ")" (open and close parentheses)

- "{" and "}" (open and close brackets)

- "[" and "]" (open and close square brackets)

Spaces are used as input separators. Most special characters carry specific meaning to the Cisco Voice Operating System (VOS) command console (for example, "\", "|", and so on). Characters above standard ASCII are mostly ignored.

Privilege Levels for Live Data Commands

The Live Data CLI commands support the following privilege levels:

- Ordinary

- Advanced

Each Live Data command has a required privilege level related to the sensitivity of data it exposes or its ability to severely affect the operation of the application. The privilege level for each command is the minimum level required; a user with a higher privilege level also has access to the command.

The Cisco Voice Operating System (VOS) also supports a higher privilege level for the administrative user; this user is configured at installation. When the administrative user creates other users (with the set account name command), the administrative user sets each newly created user's privilege level. (For more information about the set account command, see the *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.)

Live Data AW DB Access

The Live Data AW DB access commands allow you to configure and display CCE AW DB (real-time distributor) access for the Contact Center Enterprise Live Data Product Deployment Selection. By default, the set and show commands also test the connection from Live Data to the primary or secondary AW database, check to see if the configured user has appropriate AW DB access, and report the results.

set live-data aw-access

Required Minimum Privilege Level: Advanced

Use this command to set the access information to the primary or secondary CCE AW. The command also automatically tests the connection from Live Data to the primary or secondary AW, checks to see if the configured user has appropriate AW DB access, and reports the results.

You can use the optional skip-test parameter if you do not want the test performed. No checking is done to see if the configured user has appropriate AW DB access, and no results are reported.

Command Syntax
set live-data aw-access {primary | secondary} *addr port db user* [*skip-test*]
addr

Specifies the hostname or IP address of the primary or secondary CCE AW (maximum 255 characters).

port

Specifies the listening port of the database server (range 1 through 65535).

db

Specifies the database name (maximum 128 characters).

user

Specifies the login user (maximum128 characters).

skip-test

Skips the testing of the connection from Live Data to the primary or secondary AW. No checking is done to see if the configured user has appropriate AW DB access, and no results are reported. The skip-test parameter is optional.

Command Default   When you execute this command, it prompts you to specify the login password (maximum 128 characters) to use for authentication with AW database access.

unset live-data aw-access

Required Minimum Privilege Level: Advanced

Use this command to unset the access information to the primary or secondary CCE AW DB.

Command Syntax
unset live-data aw-access {primary | secondary}

There is a single, required parameter with two possible values.

show live-data aw-access

Required Minimum Privilege Level: Ordinary

Use this command to display the primary and secondary CCE AW DB access information and test the connection from Live Data to each AW DB, check to see if the configured user (on each node) has appropriate AW DB access, and report the results.

You can use the optional skip-test parameter if you do not want the test performed. No checking is done to see if the configured user (on each node) has appropriate AW DB access, and no results are reported.

Command Syntax
show live-data aw-access [*skip-test*]

Shows the configured primary and secondary CCE AW DB access information. There are no required parameters.

skip-test

Skips the testing of the connection from Live Data to the primary or secondary AW. No checking is done to see if the configured user (on each node) has appropriate AW DB access, and no results are reported. The skip-test parameter is optional.

Live Data Cluster Configuration

Use the following commands to set, unset, or show Live Data cluster configuration information.

set live-data secondary

Required Minimum Privilege Level: Advanced

Use this command to register the Live Data secondary node.

Command Syntax
set live-data secondary *name*

name

Specifies the hostname or ip address of the Live Data secondary node.

unset live-data secondary

Required Minimum Privilege Level: Advanced

Use this command to unset Live Data secondary node configuration.

unset live-data secondary

There are no required parameters.

show live-data secondary

Required Minimum Privilege Level: Ordinary

Use this command to show Live Data secondary node configuration information.

show live-data secondary

There are no required parameters.

Live Data CORS Configuration

Live Data CORS commands allow you to configure CORS and hence allow web applications running on different origins to communicate with Live Data.

Note Live Data CORS commands are available only after installing Cisco Unified Intelligence Center Release 11.6(1) ES18 or later in Unified CCE 11.6 release and Cisco Unified Intelligence Center Release 12.0(1) ES06 or later in Unified CCE 12.0 release respectively.

Ensure that the CORS update commands are run on all the live data nodes in the cluster.

After you make changes to the CORS status, allowed origins, allowed headers, or exposed headers, restart the Unified CCE Live Data NGINX service.

utils live-data cors status

Required Minimum Privilege Level: Ordinary

Use this command to query the Live Data CORS status.

Command Syntax
utils live-data cors status

There are no required parameters.

utils live-data cors enable

Required Minimum Privilege Level: Advanced

Use this command to enable CORS in Live Data.

Command Syntax
utils live-data cors enable

There are no required parameters.

✎

Note　For Unified Intelligence Centre gadgets (Live Data) to load in Cisco Finesse, ensure to:

- Enable CORS using `utils cuic cors enable` and `utils live-data cors enable` commands.

- Set the Finesse host URL in `utils cuic cors allowed_origin add URLs` and `utils live-data cors allowed_origin add URLs` commands.

    Examples:

    - https://<finesse-FQDN>

    - https://<finesse-FQDN>:port

utils live-data cors disable

Required Minimum Privilege Level: Advanced

Use this command to disable CORS in Live Data.

Command Syntax
utils live-data cors disable

There are no required parameters.

utils live-data cors allowed_origin list

Required Minimum Privilege Level: Ordinary

Use this command to display the list of allowed URLS that can make CORS request to Live Data.

Command Syntax
utils live-data cors allowed_origin list

There are no required parameters.

utils live-data cors allowed_origin add

Required Minimum Privilege Level: Advanced

Use this command to add the given list of URLs to the allowed origin list.

Command Syntax
utils live-data cors allowed_origin add *URLs*

URLs

Comma separated list of URLs (without spaces) that has to be added to the allowed origins list. The URL should be of the format: **http[s]://<hostname>[:port]**

utils live-data cors allowed_origin delete

Required Minimum Privilege Level: Advanced

Use this command to delete a particular URL entry or all the URL entries from the allowed origins list.

Command Syntax
utils live-data cors allowed_origin delete

There are no required parameters. This command will prompt for a choice to delete a particular entry or all URL entries from allowed origins list.

Example

Utils live-data cors allowed_origin delete

1. https://cisco.com

2. https://google.com

a: all

q: quit

utils live-data cors allowed_headers list

Required Minimum Privilege Level: Ordinary

Use this command to display the list of allowed headers that the client can use to make CORS request to Live Data.

Command Syntax
utils live-data cors allowed_headers list

There are no required parameters.

utils live-data cors allowed_headers add

Required Minimum Privilege Level: Advanced

Use this command to add the given list of headers to the allowed header list.

Command Syntax
utils live-data cors allowed_headers add *headers*

headers

Comma separated list of headers (without spaces) that has to be added to the allowed headers list.

utils live-data cors allowed_headers delete

Required Minimum Privilege Level: Advanced

Use this command to delete a particular header entry or all the header entries from the allowed headers list. The header names are case-insensitive and any duplicate header name will be ignored.

Command Syntax
utils live-data cors allowed_headers delete

There are no required parameters. This command will prompt for a choice to delete a particular entry or all the header entries from the allowed headers list.

Example

Utils live-data cors allowed_headers delete

1. Header1

2. Header2

a: all

q: quit

utils live-data cors exposed_headers list

Required Minimum Privilege Level: Oridnary

This command displays the list of exposed headers that the client can expect from Live Data when it makes CORS request to Live Data .

Command Syntax
utils live-data cors exposed_headers list

There are no required parameters.

utils live-data cors exposed_headers add headers

Required Minimum Privilege Level: Oridnary

This command adds given list of headers to the exposed header list.

Command Syntax
utils live-data cors exposed_headers add *headers*

headers

Comma separated list of headers that has to be added to the exposed headers list.

utils live-data cors exposed_headers delete

Required Minimum Privilege Level: Oridnary

This command deletes a particular header entry or all the header entries from the exposed headers list. The header names are case-insensitive, any duplicate header name will be ignored.

Command Syntax
utils live-data cors exposed_headers delete

There are no required parameters. This command will prompt for a choice to delete a particular entry or all header entries from exposed headers list.

Example

Utils live-data cors exposed_headers delete.

1. Header1

2. Header2

    a: all

    q: quit

Live Data Reporting Configuration

set live-data reporting-interval

Required Minimum Privilege Level: Advanced

Use this command to set the Live Data reporting interval in minutes. The reporting interval is the duration of time for which values are aggregated and reported for the **To Interval** fields.

Command Syntax
set live-data reporting-interval   *reporting-interval-in-minutes*
reporting-interval-in-minutes

Specifies the reporting interval in minutes. The valid values are 5, 10, 15, 30, and 60 minutes.

When you set the Live Data reporting interval, restart the publisher and then the subscriber. Restart the inactive node and then the active node by using the **utils system restart** command. (For more information about the command, refer to the *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.)

If you restart only the publisher and not the subscriber, the new reporting interval takes effect only on the publisher; likewise, if you restart the subscriber but not the publisher, only the subscriber uses the newly set reporting interval.

When the publisher and the subscriber restart, use the show live-data reporting-interval command to validate the new interval.

show live-data reporting-interval

Required Minimum Privilege Level: Ordinary

Use this command to show the configured and current reporting interval for both the Live Data publisher and subscriber.

Command Syntax
show live-data reporting-interval

unset live-data reporting-interval

Required Minimum Privilege Level: Advanced

Use this command to reset the Live Data reporting interval to the default value (which is five minutes).

Command Syntax
unset live-data reporting-interval

When you reset the Live Data reporting interval, restart the publisher and then the subscriber. Restart the inactive node and then the active node by using the **utils system restart** command. (For more information about the command, refer to the *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.)

If you restart only the publisher and not the subscriber, the reset interval takes effect only on the publisher; likewise, if you restart the subscriber but not the publisher, only the subscriber uses the reset reporting interval.

When the publisher and the subscriber restart, use the show live-data reporting-interval command to validate the new interval.

Live Data Services Registration

set live-data cuic-datasource

Required Minimum Privilege Level: Advanced

Use this command to create or update the Live Data data source in Cisco Unified Intelligence Center.

You can run the command from either the Side A or Side B (not both) Live Data node; and you must run it once for each of the Cisco Unified Intelligence Center Publisher nodes. The AW Distributor and Cisco Unified Intelligence Center Publisher must be in service.

You can use this command after you:

- Set the AW DB connection information on the same node where you want to run this command.

- Configure Live Data endpoints in the Machine Service table.

Note You must run this command when there is a change in machine service inventory table. The changes can occur when,

- Recreating the node in Unified CCE Inventory

- Restoring AW database using EDMT

- Running the **set livedata machine-services** CLI command (for 4K and above)

Command Syntax
set live-data cuic-datasource *cuic-addr cuic-port cuic-user*
cuic-addr

Specifies the Cisco Unified Intelligence Center publisher node's fully qualified domain name (FQDN). This node must be in service.

cuic-port

Specifies the Cisco Unified Intelligence Center REST API port, which must be 8444.

cuic-user

Specifies the user name to use for authentication with Cisco Unified Intelligence Center. By default, Cisco Unified Intelligence Center requires that you specify `CUIC` as the domain with the user name (for example, `CUIC\administrator`).

This user must have system configuration administrative privileges.

Command Default When you execute this command, it prompts you to specify the password to use for authentication with Cisco Unified Intelligence Center.

show live-data cuic-datasource

Required Minimum Privilege Level: Ordinary

Use this command to list the Live Data data source configuration in Cisco Unified Intelligence Center.

You can use this command after you:

- Set the AW DB connection information on the same node where you want to run this command.

- Configure Live Data endpoints in the Machine Service table.

Command Syntax
show live-data cuic-datasource *cuic-addr cuic-port cuic-user*
cuic-addr

Specifies the Cisco Unified Intelligence Center publisher node's fully qualified domain name (FQDN).

cuic-port

Specifies the Cisco Unified Intelligence Center REST API port, which must be 8444.

cuic-user

Specifies the user name to use for authentication with Cisco Unified Intelligence Center. By default, Cisco Unified Intelligence Center requires that you specify `CUIC` as the domain with the user name (for example, `CUIC\administrator`).

Command Default   When you execute this command, it prompts you to specify the password to use for authentication with Cisco Unified Intelligence Center.

unset live-data cuic-datasource

Required Minimum Privilege Level: Advanced

Use this command to delete the existing Live Data data source. Ensure that there are no existing reports or report templates that reference the Live Data data source before you run the command; otherwise, the command fails.

After you run this command successfully, you can no longer generate Live Data reports.

You can use this command after you:

- Set the AW DB connection information on the same node where you want to run this command.

- Configure Live Data endpoints in the Machine Service table.

Command Syntax
unset live-data cuic-datasource   *cuic-addr cuic-port cuic-user*
cuic-addr

Specifies the Cisco Unified Intelligence Center publisher node's fully qualified domain name (FQDN).

cuic-port

Specifies the Cisco Unified Intelligence Center REST API port, which must be 8444.

cuic-user

Specifies the user name to use for authentication with Cisco Unified Intelligence Center. By default, Cisco Unified Intelligence Center requires that you specify `CUIC` as the domain with the user name (for example, `CUIC\administrator`).

This user must have system configuration administrative privileges.

Command Default   When you execute this command, it prompts you to specify the password to use for authentication with Cisco Unified Intelligence Center.

set live-data machine-services

✎

Note   This command is not valid for coresident deployments. If you have a coresident deployment, use the System Inventory in the Unified CCE Administration tool.

Required Minimum Privilege Level: Advanced

Use this command to set or update the Machine Service table with the latest information from Live Data services (publisher and subscriber).

✎

Note   You must run the **set live-data cuic-datasource** CLI command after executing the **set live-data machine-services** command.

Command Syntax
set live-data machine-services *awdb-user*
awdb-user

Use the `user@domain` format to specify the AW database domain user with write-access permission. The domain is a fully qualified domain name (FQDN). The username is a user principal name. The user must be authorized to change Unified CCE configuration.

Command Default

When you execute this command, it prompts you to specify the login password to use for authentication with AW database access.

show live-data machine-services

Required Minimum Privilege Level: Ordinary

Use this command to display Live Data entries in the Machine Services table.

Command Syntax
show live-data machine-services [*awdb-user*]
awdb-user

Use the `user@domain` format to specify the AW database domain user with at least read-access permission.

Command Default

When you execute this command, it prompts you to specify the login password to use for authentication with AW database access.

Transport Layer Security CLI Commands

Note These CLI commands are only for VOS systems. They are not available for VMs running Windows Server.

TLS Server Minimum Version

set tls server min-version

Use this command to set the current TLS minimum version for inbound connections.

Command Syntax

set tls server min-version {1.0|1.1|1.2}
1.0

Specifies the TLS server minimum version 1.0 for inbound connections.

1.1

Specifies the TLS server minimum version 1.1 for inbound connections.

1.2

Specifies the TLS server minimum version 1.2 for inbound connections.

show tls server min-version

Use this command to display the current TLS minimum version for inbound connections.

Command Syntax
show tls server min-version

TLS Client Minimum Version

set tls client min-version

Use this command to set the current TLS minimum version for outbound connections.

Command Syntax

set tls client min-version {1.0|1.1|1.2}
1.0

Specifies the TLS client minimum version 1.0 for outbound connections.

1.1

Specifies the TLS client minimum version 1.1 for outbound connections.

1.2

Specifies the TLS client minimum version 1.2 for outbound connections.

show tls server min-version

Use this command to display the current TLS minimum version for inbound connections.

Command Syntax
show tls server min-version

show tls server min-version