Universal Message Service (OMS) 7.6.x Reference Guide

Universal Agent 7.6.x

© 2024 by Stonebranch, Inc. All Rights Reserved.

Table of Contents

1 Universal Message Service

Universal Message Service (OMS) is a message-oriented middleware component used to send and receive messages between Universal Automation Center product components distributed over a computer network.

Product components that currently utilize OMS are Universal Automation Center Agent (UAG) and the Universal Controller, referred to generally as OMS clients. OMS provides for asynchronous, secure, and reliable message communication between a large number of OMS clients.

The OMS component itself consists of an OMS Server and an OMS Administration Utility. Detailed information on both are documented on these pages.

OMS clients establish persistent TCP/IP socket connections with the OMS Server. The Transport Layer Security (TLS) protocol, commonly referred to as SSL/TLS, may be used to provide data privacy and integrity of all data transmitted between OMS clients and the OMS Server. SSL/TLS additionally provides the option for OMS clients to authenticate the OMS Server using digital certificates.

Application data is sent and received between the OMS clients as OMS messages. OMS provides for asynchronous communication, where an OMS client sends a message to an OMS queue that is maintained on the OMS server. An OMS queue represents a message destination from which OMS clients can send and receive messages. An OMS message will remain in the OMS queue until another OMS client receives the message from the OMS Server. Asynchronous communication allows for OMS clients to produce messages and consume messages at different times. The producers and the consumers of messages do not have to be connected to the OMS Server at the same time.

OMS provides for reliable message communication by placing all OMS queued messages in persistent storage in an OMS message database; data is retained even if power to that database is shut off.

2 OMS Server

The OMS Server is a central communication hub for OMS clients. The OMS Server maintains persistent OMS messages in a message database in order to provide message reliability. As messages are received, the OMS server routes messages to the appropriate OMS clients.

The OMS Server is deployed as a server component managed by the Universal Broker. The Universal Broker manages server components by providing the following services:

- Start and stop servers
- Manager server configuration data
- Monitor server status
- Provide server restart services

The OMS Server is defined as an *auto-started* server. As such, it is started and stopped automatically when Universal Broker is started and stopped.

3 OMS Administration Utility

The OMS Administration Utility is available to obtain information on the state of the OMS server and to provide support and diagnostic services. Access to the Administration Utility should be limited to the group responsible for administering the OMS server.

The Administration Utility is a command line program that interacts with the local OMS server. Access to its services can be controlled with UACL entries.

4 Detailed Information

The following pages provide detailed information for OMS:

- OMS Server
- OMS Administration Utility
- Universal Message Service Additional Information

5 OMS Server

5.1 OMS Server

The OMS Server is a central communication hub for OMS clients. The OMS server maintains persistent OMS messages in a message database in order to provide message reliability. As messages are received, the OMS Server routes messages to the appropriate OMS clients.

The OMS Server is deployed as a server component managed by Universal Broker. Universal Broker manages server components by providing the following services:

- Start and stop servers
- Manager server configuration data
- Monitor server status
- Provide server restart services

The OMS Server is defined as an *auto-started* server. As such, it is started and stopped automatically when Universal Broker is started and stopped.

5.1.1 Configuration

The OMS Server is configured using a set of configuration options that change its default behavior.

For detailed information on the configuration options, see OMS Server Configuration Options.

5.1.2 Component Definition

The Component Definition defines the OMS server to the Universal Broker. A component definition consists of a set of options the Universal Broker uses to provide server component services.

For detailed information on the Component Definition options, see OMS Server Component Definition Options.

5.1.3 Universal Access Control List

Universal Access Control Lists (UACLs) provide an additional layer of control for the OMS server. UACL entries are available to limit OMS client access to the OMS server.

For detailed information about UACL entries, see OMS Server UACL Entries.

5.1.4 Message Database

The OMS server maintained persistent OMS messages in a message database. The message database is maintain on persistent storage in order to provide message reliability.

For detailed information on the OMS message database, see OMS Server Message Database.

5.1.5 Universal Controller Connectivity

When a Universal Controller cluster node is not processing work, it is possible that its OMS Server connection can be silently dropped.

To detect this, a cluster node issues a heartbeat through the OMS server, and back to itself, every 30 seconds if no outgoing activity to the OMS server has occurred. The difference between the time the Controller issues the heartbeat and the time it receives the heartbeat is logged in the **opswise.log**.

5.1.6 OMS Server High Availability

The OMS server provides critical communication infrastructure for the Universal Automation Center product line. In order to provide reliable service, an OMS server High Availability (HA) deployment is required.

For detailed information on the OMS message database, see OMS Server High Availability.

5.2 OMS Server Configuration Options

5.2.1 Overview

This page provides links to detailed information on the configuration options available for use with the OMS Server.

The options are listed alphabetically, without regard to any specific operating system.

5.2.2 Configuration Options Information

For each configuration option, these pages provide the following information.

5.2.2.1 Description

Describes the configuration option and how it is used.

5.2.2.2 Usage

Provides a table of the following information:

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	<Format / Value>					

5.2.2.2.1 Method

Identifies the method used to specify OMS configuration options:

- Configuration File Keyword

5.2.2.2.2 Syntax

Identifies the syntax of the method used to specify the option:

- Format: Specific characters that identify the option.
- Value: Type of value(s) to be supplied for this method.

5.2.2.2.3 (Operating System)

Identifies the operating systems for which each method of specifying the option is valid:

- IBM i
- HP NonStop
- UNIX
- Windows
- z/OS

5.2.2.3 Values

Identifies all possible values for the specified value type.

Defaults are identified in **bold type**.

5.2.2.4 <Additional Information>

Identifies any additional information specific to the option.

5.2.3 Configuration Options List

The following table identifies all OMS configuration options. Each **Option Name** is a link to detailed information about that option.

Option Name	Description
AUTHENTICATE_PEER	Controls whether or not OMS server will validate host name and/or IP addresss of the incoming client connection based on its certificate.
CODE_PAGE	Universal Translate Table (utt) file to use for network data translation to and from the local code page and Unicode.
DNS_CACHE_TIMEOUT	Number of seconds that a successfully resolved host name is cached.
INDEX_CACHE_SIZE	Size of the memory cache used to store the message index.
INSTALLATION_DIRECTORY	Directory where OMS is installed.
MAX_CONNECTIONS	Maximum number of concurrent connections that can be made to an OMS server.
MAX_DATA_FILE_SIZE	Maximum size of a message data file.
MAX_MESSAGE_SIZE	Maximum message size allowed by the OMS server.

Option Name	Description
MAX_SSL_PROTOCOL	Maximum SSL/TLS protocol level that will be negotiated and used for communications channels.
MESSAGE_LANGUAGE	Message catalog used to format messages.
MESSAGE_LEVEL	Level of messages written.
MIN_SSL_PROTOCOL	Minimum SSL/TLS protocol level that will be negotiated and used for communications channels.
MSG_CHUNK_SIZE	Size limit where messages exceeding the limit will be split into "chunks" no larger than that limit for transmission.
MSG_CLEANUP_INTERVAL	Interval for message data file clean-up.
MSG_DATA_FLUSH_INTERVAL	Interval for message data flush to disk.
MSG_SUPPRESSION_LIST	List of message IDs representing Universal messages to be suppressed.
NLS_DIRECTORY	Directory where OMS message catalog and code page tables are located.
OTEL_ENABLE_TRACING	Specification for whether or not OMS will export traces to the Opentelemetry collector.
OTEL_EXPORT_METRICS	Specification for whether or not OMS will export metrics to the Opentelemetry collector.
OTEL_METRICS_ENDPOINT	URL used to export OMS metric data using the OTLP/HTTP(S) protocol to the Opentelemetry Collector.
OTEL_METRICS_EXPORT_INTERVAL	Interval for how often to export the metrics to the Opentelemetry Collector.
OTEL_SERVICE_NAME	Value of the `service.name` resource attribute used to identify OMS in traces and metrics.
OTEL_SSL_CA_CERT_PATH	Full path to the file containing one or more X.509 trusted certificates in PEM format. The certificate(s) will be used to validate the Opentelemetry Collector (server).
OTEL_SSL_CLIENT_CERT_PATH	Full path to an X.509 certificate used to identify OMS to the Opentelemetry Collector. This option is only needed for HTTP connections where client authentication is set up in the Opentelemetry Collector.
OTEL_SSL_CLIENT_KEY_PATH	Full path to the PEM formatted file containing the private key associated with the client certificate specified by the OTEL_SSL_CLIENT_CERT_PATH option. This option is only needed for HTTP connections where client authentication is set up in the Opentelemetry Collector.
OTEL_SSL_INSECURE_SKIP_VERIFY	Specification for whether or not to validate the Opentelemetry Collector's (server's) certificate against the locally configured CA certificate.
OTEL_TRACE_ENDPOINT	URL used to export OMS trace data using the OTLP/HTTP(S) protocol to the Opentelemetry Collector.
REQUIRE_SSL	Specification for whether or not the OMS Server will enforce the use of SSL/TLS connections by clients.
SERVICE_BACKLOG	Size of the service interface backlog queue in TCP/IP for pending connection requests.
SERVICE_IP_ADDRESS	IP address on which to accept OMS connection requests.
SERVICE_PORT	Port to use to listen for OMS connection requests.
SERVICE_TIMEOUT	Number of seconds of inactivity before the OMS server considers the connection as inactive and closes the connection.

Option Name	Description
SPOOL_DIRECTORY	Directory where OMS maintains the message database.
SSL_CIPHER_LIST	List of acceptable SSL/TLS cipher suites to use for network communication.
SSL_CIPHER_SUITES	SSL/TLS 1.3 specific cipher suites that are acceptable to use for network communications between OMS clients and the OMS server.
TMP_DIRECTORY	Directory in which OMS will create temporary files.
TRACE_DIRECTORY	Directory into which trace files are written if the MESSAGE_LEVEL option is set to **trace**.
TRACE_FILE_LINES	Maximum number of lines written to the trace file.
TRACE_TABLE	Memory trace table specifications.

5.2.4 AUTHENTICATE_PEER - OMS configuration option

5.2.4.1 Description

The AUTHENTICATE_PEER option specifies whether or not OMS server will validate the host name and/or IP address of the client that tries to connect. The information taken from the client's session must match the information in the client's certificate in order for the validation to be successful.

5.2.4.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	authenticate_peer *option*			✓	✓	✓

5.2.4.3 Value

option is the specification for whether or not the OMS Server will authenticate peer's host name and/or IP address.

Valid values for *option* are:

- **yes**
  Authenticate hostname and/or IP address
- **no**
  Do not authenticate hostname and/or ip address

Default is yes.

5.2.5 CODE_PAGE - OMS configuration option

5.2.5.1 Description

The CODE_PAGE option specifies the character code page that is used to translate text data received and transmitted over the network.

The Universal Translate Table (UTT) files are used to translate between Unicode and the local single-byte code page.

5.2.5.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	codepage *codepage*			✓	✓	

5.2.5.3 Value

codepage is the character code page that is used to translate data.

codepage references a Universal Translate Table (UTT) file provided with the product (see UTT Files for information on UTT files). UTT files are used to translate between Unicode and the local single-byte code page. (All UTT files end with an extension of **.utt**.)

5.2.5.3.1 Default

The default code page is different for different operating systems:

- ISO8859-1 (8-bit ASCII): ASCII-based operating systems
- IBM1047 (EBCDIC): EBCDIC-based operating system

See Character Code Pages for a complete list of character code pages provided by Stonebranch Inc. for use with Universal Agent components.

5.2.6 DNS_CACHE_TIMEOUT - OMS configuration option

5.2.6.1 Description

The DNS_CACHE_TIMEOUT option specifies the number of seconds that a successfully resolved host name is cached.

When the host name resolver is asked to resolve a host name into an IP address, the host entry returned is saved in the DNS cache. The next call to resolve a host name will return the cached entry and not go back to the resolve. The cached entry is considered valid until the cache time-out period is reached.

The DNS cache provides a performance improvement as the resolution of a host name can take some time depending on the environment.

5.2.6.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	dns_cache_timeout *seconds*			✓	✓	

5.2.6.3 Value

seconds is the number of seconds that a DNS cached host entry remains valid.

A value of **0** disables caching of host entries.

Default is 120.

5.2.7 INDEX_CACHE_SIZE - OMS configuration option

5.2.7.1 Description

The INDEX_CACHE_SIZE option specifies the size of the memory cache used to store the message index. The message index provides quick access to the messages in the message data files. Additionally, the message index stores non-persistent messages. The message index cache size specifies the size of the memory cache used to store the index.

5.2.7.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	index_cache_size *size*			✓	✓	

5.2.7.3 Value

size is the size (in bytes) of the memory cache used to store the index.

Valid values for *size* are any number in the range 262144 to 2147483647.

Default is 1048576.

5.2.8 INSTALLATION_DIRECTORY - OMS configuration option

5.2.8.1 Description

The INSTALLATION_DIRECTORY option specifies the OMS base installation directory.

Note

This is a required option.

5.2.8.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	installation_directory *directory*			✓	✓	

5.2.8.3 Value

directory is the name of the OMS base installation directory.

A full path name is required.

UNIX	If OMS is installed in `/opt/universal/oms`, specify that entire path name: `/opt/universal/oms`.
Windows	The default is set in the `omss.conf` file at installation time.

5.2.9 MAX_CONNECTIONS - OMS configuration option

5.2.9.1 Description

The MAX_CONNECTIONS option specifies the maximum number of concurrent connections that can be made to an OMS server.

5.2.9.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	max_connections *number*			✓	✓	

5.2.9.3 Values

number specifies the maximum number of concurrent connections that can be made to an OMS server.

Valid values are 64 to 30,000.

Default is 2048.

> **Note**
>
> The actual maximum connection limit may be constrained by system resources or system imposed limits.

5.2.10 MAX_DATA_FILE_SIZE - OMS configuration option

5.2.10.1 Description

The MAX_DATA_FILE_SIZE option specifies the maximum size of the OMS message data file.

When the maximum size of the message data file has been reached, a new data file is created.

5.2.10.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	max_data_file_size *size*			✓	✓	

5.2.10.3 Value

size is the size (in bytes) of the OMS message data file.

Valid values for *size* are any number in the range 5412352 to 536870912.

Default is 25000000.

5.2.11 MAX_MSG_SIZE - OMS configuration option

5.2.11.1 Description

The MAX_MESSAGE_SIZE option specifies the maximum message size allowed by the OMS server. Messages exceeding the limit will not be accepted by the server.

The MAX_MESSAGE_SIZE option supports a range of 6144000 bytes to 1073741824 bytes (1 gigabyte).

5.2.11.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	max_msg_size *size [unit]*			✓	✓	

5.2.11.3 Values

The *size* value specifies the maximum allowable size for messages.

The *size* value is specified in units of *unit*. Possible *unit* values are

Unit	Description
B	Bytes (the default)
K	Kilobytes (1024 bytes)
M	Megabytes (1048576 bytes)
G	Gigabytes (1073741824 bytes)

The *unit* value is case insensitive.

The maximum supported buffer size is 1G. The default is unit is B.

Default value is 6144000.

5.2.12 MAX_SSL_PROTOCOL - OMS configuration option

5.2.12.1 Description

The MAX_SSL_PROTOCOL option specifies the maximum SSL/TLS protocol level that will be negotiated and used for communications channels.

5.2.12.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	max_ssl_protocol *option*			✓	✓	

This option is NOT currently supported on HP-UX and z/OS

5.2.12.3 Values

option is the specification for the maximum SSL/TLS protocol level that will be supported.

- **TLS1_2**
  Maximum SSL/TLS protocol is TLS 1.2.
- **TLS1_3**
  Maximum SSL/TLS protocol is TLS 1.3.

Default is TLS1_2.

5.2.13 MESSAGE_LANGUAGE - OMS configuration option

5.2.13.1 Description

The MESSAGE_LANGUAGE option specifies the Universal Message Catalog (UMC) that is used to format messages.

There is a message catalog for each language. The first three characters of the language are used as a three-character suffix of the member name. All UMC files have a **.UMC** extension.

> **Note**
>
> Currently, the only message catalog provided is for English.

5.2.13.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	language *language*			✓	✓	

5.2.13.3 Value

language is the name of the UMC file.

> **UNIX**
>
> The location of the UMC file is specified by the NLS_DIRECTORY option.

Default is *ENGLISH* (UMC member USSMCENG is used).

5.2.14 MESSAGE_LEVEL - OMS configuration option

5.2.14.1 Description

The MESSAGE_LEVEL option specifies the level of messages to write.

Messages of the specified severity level and the levels below it are written. For example, if **info** is specified, **info**, **warn**, and **error** messages are written.

5.2.14.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	message_level *level*			✓	✓	

5.2.14.3 Values

level is the level of messages to write.

Valid values for *level* are:

- **trace**
  Writes trace messages used for diagnostic purposes (see #Trace Files).

> **Note**
>
> Use **trace** only as directed by Stonebranch, Inc. Customer Support.

- **audit**
  Writes audit, informational, warning, and error messages.
- **info**
  Writes informational, warning, and error messages.
- **warn**
  Writes warning and error messages.
- **error**
  Writes error messages only.

Default is info.

5.2.14.4 Trace Files

UNIX	The trace file is created in the directory `/var/opt/universal/trace`.

Windows	The trace file is created in the OMS installation directory, which defaults to `C:\Program Files\Universal\oms`

5.2.15 MIN_SSL_PROTOCOL - OMS configuration option

5.2.15.1 Description

The MIN_SSL_PROTOCOL option specifies the minimum SSL/TLS protocol level that will be negotiated and used for communications channels.

5.2.15.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	min_ssl_protocol *option*			✓	✓	✓

5.2.15.3 Values

option is the specification for the minimum SSL/TLS protocol level that will be supported.

- **TLS1_0**
  Minimum SSL/TLS protocol is TLS 1.0.
- **TLS1_2**
  Minimum SSL/TLS protocol is TLS 1.2.
- **TLS1_3**

  > TLS 1.3 is NOT currently supported on HP-UX and z/OS

  Minimum SSL/TLS protocol is TLS 1.3.

Default is TLS1_2.

5.2.16 MSG_CHUNK_SIZE - OMS configuration option

5.2.16.1 Description

The MSG_CHUNK_SIZE option specifies a size limit where messages exceeding the limit will be split into "chunks" no larger than that limit for transmission. The message "chunks" will be sent to the OMS server as individual messages during message production. The message chunks will be preserved on the OMS server in a "transaction queue" while waiting to be consumed.

The MSG_CHUNK_SIZE option supports a range of 6144000 bytes to 2147483647 bytes.

A special minimum value of 0 will disable message chunking. All messages will be sent as a single transfer.

Specifying a value greater than or equal to the configured maximum message size (MAX_MESSAGE_SIZE) will effectively disable message chunking.

The MSG_CHUNK_SIZE option supports a functional range of 6144000 bytes to 1073741824 bytes (1 gigabyte).

5.2.16.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	max_msg_size *size [unit]*			✓	✓	

5.2.16.3 Values

The *size* value specifies threshold where messages exceeding the threshold will be transferred in chunks.

The *size* value is specified in units of *unit*. Possible *unit* values are

Unit	Description
B	Bytes (the default)
K	Kilobytes (1024 bytes)
M	Megabytes (1048576 bytes)
G	Gigabytes (1073741824 bytes)

The *unit* value is case insensitive.

The maximum supported buffer size is 1G. The default is unit is B.

Default value is 6144000.

5.2.17 MSG_CLEANUP_INTERVAL - OMS configuration option

5.2.17.1 Description

The MSG_CLEANUP_INTERVAL option specifies the interval at which OMS message data files are cleaned up.

Message data file clean-up consists of examining each message data file and removing empty message data files.

5.2.17.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	msg_cleanup_interval *seconds*			✓	✓	

5.2.17.3 Value

seconds is the interval (in seconds) at which OMS message data files are cleaned up.

Valid values for *seconds* are any number in the range 60 to 2147483647.

Default is 1800.

5.2.18 MSG_DATA_FLUSH_INTERVAL - OMS configuration option

5.2.18.1 Description

The MSG_DATA_FLUSH_INTERVAL specifies the number of message write operations performed at which data is flushed to disk.

By default, each message is flushed to disk after it is written in order to maintain message reliability and availability. However, disk flushes are very slow. If OMS server throughput outweighs message reliability and availability, the flush interval can be increased so that disk flushes are performed after an additional number of message records are written.

5.2.18.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	msg_data_flush_interval *number*			✓	✓	

5.2.18.3 Value

number is the interval at which OMS message data is flushed to disk after the message record it is written

Valid values for *number* are any positive, non-zero number.

Default is 1.

5.2.19 MSG_SUPPRESSION_LIST - OMS configuration option

5.2.19.1 Description

The MSG_SUPPRESSION_LIST option specifies a list of message IDs representing Universal messages to be suppressed.

The list consists of zero or more comma-separated Universal message ID numbers. For example:

- 193 - Suppress message UNV0193W only.
- 192,193 - Suppress message UNV0192W and UNV0193W.

Suppressed messages are not printed to logs or output, even if a condition arises that normally would produce the message(s).

5.2.19.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	msg_suppression_list *list*			✓	✓	

5.2.19.3 Values

list is the list of message IDs representing Universal messages to be suppressed.

5.2.20 NLS_DIRECTORY - OMS configuration option

5.2.20.1 Description

The NLS_DIRECTORY option specifies the name of the directory where the OMS message catalog and code page tables are located.

5.2.20.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	nls_directory *directory*			✓	✓	

5.2.20.3 Values

directory is the name of the directory where the catalog and tables are located.

Full path names are recommended.

Relative path names are relative to the **universal** installation directory.

5.2.20.3.1 Default

UNIX	Default is `/opt/universal/nls`.
Windows	Default is `..\nls`.

5.2.21 OTEL_ENABLE_TRACING - OMS configuration option

5.2.21.1 Description

The OTEL_ENABLE_TRACING option specifies whether OMS will export traces to the Opentelemetry collector.

5.2.21.2 Usage

Method	Syntax	IBM i	UNIX	Windows	z/OS
Configuration File Keyword	otel_enable_tracing *value*		✓	✓	

Note

This option is **NOT** available on:

- Solaris
- HP-UX
- z/OS

5.2.21.3 Values

value is case-insensitive and must be either **YES** or **NO**.

Default is NO.

5.2.22 OTEL_EXPORT_METRICS - OMS configuration option

5.2.22.1 Description

The OTEL_EXPORT_METRICS option specifies whether OMS will export metrics to the Opentelemetry collector.

Exported Metrics

See Provided Metrics for the list of metrics exported by OMS.

Usage

Method	Syntax	IBM i	UNIX	Windows	z/OS

Configuration File Keyword	otel_export_metrics *value*		✓	✓	

Note

This option is **NOT** available on:

- Solaris
- HP-UX
- z/OS

5.2.22.2 Values

value is case-insensitive and must be either **YES** or **NO**.

Default is NO.

5.2.23 OTEL_METRICS_ENDPOINT - OMS configuration option

5.2.23.1 Description

The OTEL_METRICS_ENDPOINT option specifies the URL used to export OMS metric data using the OTLP/HTTP(S) protocol to the Opentelemetry Collector.

Note

For HTTPS connections, the URL must start with `https://`

Note

As of UA 7.6.0.0, only `OTLP/HTTP` protocol is supported. `OTLP/gRPC` is **NOT** supported.

Usage

Method	Syntax	IBM i	UNIX	Windows	z/OS
Configuration File Keyword	otel_metrics_endpoint *url*		✓	✓	

Note

This option is **NOT** available on:

- Solaris
- HP-UX
- z/OS

5.2.23.2 Values

url must be a properly formatted, according to Opentelemetry conventions.

Default is `http://localhost:4318`

5.2.24 OTEL_METRICS_EXPORT_INTERVAL - OMS configuration option

5.2.24.1 Description

The OTEL_METRICS_EXPORT_INTERVAL option specifies how often to export the metrics to the Opentelemetry Collector.

Usage

Method	Syntax	IBM i	UNIX	Windows	z/OS
Configuration File Keyword	otel_metrics_export_interval *interval*		✓	✓	

Note

This option is **NOT** available on:

- Solaris
- HP-UX
- z/OS

5.2.24.2 Values

interval must be specified in seconds and must be greater than 0.

Default is `60` **seconds (Opentelemetry Default).**

5.2.25 OTEL_SERVICE_NAME - OMS configuration option

5.2.25.1 Description

The OTEL_SERVICE_NAME option sets the value of the `service.name` resource attribute used to identify OMS in traces and metrics.

Usage

Method	Syntax	IBM i	UNIX	Windows	z/OS
Configuration File Keyword	otel_service_name *name*		✓	✓	

Note

This option is **NOT** available on:

- Solaris
- HP-UX
- z/OS

5.2.25.2 Values

Default is `omssrv`

5.2.26 OTEL_SSL_CA_CERT_PATH - OMS configuration option

5.2.26.1 Description

The OTEL_SSL_CA_CERT_PATH option specifies the full path to the file containing one or more X.509 trusted certificates in PEM format. The certificate(s) will be used to validate the Opentelemetry Collector (server). This option should only be specified for secure, HTTPS endpoints (ignored for HTTP).

Note

To use the host platform's trust certificates instead, do NOT specify this option.

Usage

Method	Syntax	IBM i	UNIX	Windows	z/OS
Configuration File Keyword	otel_ssl_ca_cert_path *value*		✓	✓	

Note

This option is **NOT** available on:

- Solaris
- HP-UX
- z/OS

5.2.26.2 Values

value must be a fully-qualified path to the CA Certificate.

No default value is set.

5.2.27 OTEL_SSL_CLIENT_CERT_PATH - OMS configuration option

5.2.27.1 Description

The OTEL_SSL_CLIENT_CERT_PATH option specifies the full path to an X.509 certificate used to identify OMS to the Opentelemetry Collector. This option is only needed for HTTP connections where client authentication is set up in the Opentelemetry Collector.

Usage

Method	Syntax	IBM i	UNIX	Windows	z/OS
Configuration File Keyword	otel_ssl_client_cert_path *value*		✓	✓	

Note

This option is **NOT** available on:

- Solaris
- HP-UX
- z/OS

5.2.27.2 Values

value must be a fully-qualified path to the client certificate.

No default value is set.

5.2.28 OTEL_SSL_CLIENT_KEY_PATH - OMS configuration option

5.2.28.1 Description

The OTEL_SSL_CLIENT_KEY_PATH option specifies the full path to the PEM formatted file containing the private key associated with the client certificate specified by the OTEL_SSL_CLIENT_CERT_PATH option. This option is only needed for HTTP connections where client authentication is set up in the Opentelemetry Collector.

Usage

Method	Syntax	IBM i	UNIX	Windows	z/OS
Configuration File Keyword	otel_ssl_client_key_path *value*		✓	✓	

Note

This option is **NOT** available on:

- Solaris
- HP-UX
- z/OS

5.2.28.2 Values

value must be a fully-qualified path to the key.

No default value is set.

5.2.29 OTEL_SSL_INSECURE_SKIP_VERIFY - OMS configuration option

5.2.29.1 Description

The OTEL_SSL_INSECURE_SKIP_VERIFY option specifies whether to validate the Opentelemetry Collector's (server's) certificate against the locally configured CA certificate (specified by OTEL_CA_CERT_PATH option).

Usage

Method	Syntax	IBM i	UNIX	Windows	z/OS
Configuration File Keyword	otel_ssl_insecure_skip_verify *value*		✓	✓	

Note

This option is **NOT** available on:

- Solaris
- HP-UX
- z/OS

5.2.29.2 Values

value is case-insensitive and must be either **YES** or **NO**.

Default is NO (Opentelemetry Collector's certificate will NOT be validated).

5.2.30 OTEL_TRACE_ENDPOINT - OMS configuration option

5.2.30.1 Description

The OTEL_TRACE_ENDPOINT option specifies the URL used to export OMS trace data using the OTLP/HTTP(S) protocol to the Opentelemetry Collector.

Note

For HTTPS connections, the URL must start with `https://`

Note

As of UA 7.6.0.0, only `OTLP/HTTP` protocol is supported. `OTLP/gRPC` is **NOT** supported.

Usage

Method	Syntax	IBM i	UNIX	Windows	z/OS
Configuration File Keyword	otel_trace_endpoint *url*		✓	✓	

Note

This option is **NOT** available on:

- Solaris
- HP-UX
- z/OS

5.2.30.2 Values

url must be a properly formatted, according to Opentelemetry conventions.

Default is `http://localhost:4318`

5.2.31 REQUIRE_SSL - OMS configuration option

5.2.31.1 Description

The REQUIRE_SSL option specifies whether or not the OMS Server will enforce the use of SSL/TLS connections by clients.

5.2.31.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	require_ssl *option*			✓	✓	

5.2.31.3 Values

option is the specification for whether or not the OMS Server will enforce the use of SSL/TLS connections.

Valid values for *option* are:

- **yes**
  Enforce the use of SSL/TLS.
- **no**
  Do not enforce the use of SSL/TLS.

Default is yes.

5.2.32 SERVICE_BACKLOG - OMS configuration option

5.2.32.1 Description

The SERVICE_BACKLOG option specifies the size of the service interface backlog queue in TCP/IP for pending connection requests.

5.2.32.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	service_backlog *size*			✓	✓	

5.2.32.3 Value

size is the size of the service interface backlog queue in TCP/IP.

Valid values for *size* are any number greater than 0.

Default is 200.

5.2.33 SERVICE_IP_ADDRESS - OMS configuration option

5.2.33.1 Description

The SERVICE_IP_ADDRESS option specifies the IP interface on which to accept OMS connection requests.

5.2.33.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	service_ip_address *ipaddress*			✓	✓	

5.2.33.3 Value

ipaddress is the IP address on which to accept network connection requests.

Valid values for *ipaddress* are:

- Dotted numeric format (for example, *20.30.40.50*)
- Domain name format (for example, *myinterface*).
- ***** (all interfaces or the only interface in a single-interface system)

Default is *.

5.2.34 SERVICE_PORT - OMS configuration option

5.2.34.1 Description

The SERVICE_PORT option specifies the port to use to listen for OMS connection requests.

5.2.34.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	service_port *port*			✓	✓	

5.2.34.3 Values

port is the port to use to listen for OMS connection requests.

Valid values for *port* are:

- Numeric value (for example, 7000)
- Service name (for example, **ubroker**)

Default is 7878.

> **Note**
>
> It is recommended that you use the default port, 7878, unless that conflicts with other services.

5.2.35 SERVICE_TIMEOUT - OMS configuration option

5.2.35.1 Description

The SERVICE_TIMEOUT option specifies the number of seconds of inactivity before the OMS server considers the connection as inactive and closes the connection.

A connection is considered inactive if no data is sent or received over that connection.

5.2.35.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	service_timeout *seconds*			✓	✓	

5.2.35.3 Value

seconds is the number of seconds of inactivity before the OMS server considers the connection as inactive and closes the connection.

Valid values for *seconds* are any number greater than 0.

Default is 600.

5.2.36 SPOOL_DIRECTORY - OMS configuration option

5.2.36.1 Description

The SPOOL_DIRECTORY option specifies the name of the directory where the OMS maintains its message database.

All OMS Servers in an OMS cluster must specify the same message database location via this option.

5.2.36.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	spool_directory *directory*			✓	✓	

5.2.36.3 Values

directory is the name of the OMS spool files directory.

Relative path names are relative to the OMS installation directory. Full path names are recommended.

5.2.36.3.1 Default

UNIX	Default is `/var/opt/universal/spool/oms`.
Windows	Default is `C:\Program Files\Universal\spool\oms`.

5.2.37 SSL_CIPHER_LIST - OMS configuration option

5.2.37.1 Description

The SSL_CIPHER_LIST option specifies one or more SSL/TLS cipher suites that are acceptable to use for network communications between OMS clients and the OMS server.

5.2.37.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	ssl_cipher_list *cipherlist*			✓	✓	

5.2.37.3 Value

cipherlist is a comma-separated list of SSL/TLS cipher suites. The following table identifies the list of SSL/TLS cipher suites supported for this option.

The list is in default order, with the most preferred suite first and the least preferred suite last.

Cipher Suite	Description
AES256-GCM-SHA384	256-bit AES encryption in Galois Counter Mode, SHA-2 384-bit message digest.
AES256-SHA	256-bit AES encryption with SHA-1 message digest.
AES128-GCM-SHA256	128-bit AES encryption in Galois Counter Mode, SHA-2 256-bit message digest.
AES128-SHA	128-bit AES encryption with SHA-1 message digest.
ECDHE-RSA-AES256-GCM-SHA384	Ephemeral Elliptic Curve Diffie-Hellman Key Exchange, RSA authentication, 256-bit AES encryption in Galois Counter Mode, SHA-2 384-bit message digest.
ECDHE-ECDSA-AES256-GCM-SHA384	Ephemeral Elliptic Curve Diffie-Hellman Key Exchange, ECDSA authentication, 256-bit AES encryption in Galois Counter Mode, SHA-2 384-bit message digest.
ECDHE-RSA-AES128-GCM-SHA256	Ephemeral Elliptic Curve Diffie-Hellman Key Exchange, RSA authentication, 128-bit AES encryption in Galois Counter Mode, SHA-2 256-bit message digest.
ECDHE-ECDSA-AES128-GCM-SHA256	Ephemeral Elliptic Curve Diffie-Hellman Key Exchange, ECDSA authentication, 128-bit AES encryption in Galois Counter Mode, SHA-2 256-bit message digest.
RC4-SHA	128-bit RC4 encryption with SHA-1 message digest.
RC4-MD5	128-bit RC4 encryption with MD5 message digest.
DES-CBC3-SHA	128-bit Triple-DES encryption with SHA-1 message digest.
DES-CBC-SHA	128-bit DES encryption with SHA-1 message digest. **Note** As of Universal Agent 6.7.0.0, DES-CBC-SHA is supported only on HP-UX. Additionally, any Agents on HP-UX that accept connections from, or attempt connections to, Agents on other platforms must be configured with at least one currently supported cipher suite besides DES-CBC-SHA. Therefore, those HP-UX Agents cannot be configured only with DES-CBC-SHA in their list of cipher suites.
NULL-SHA256	No encryption and SHA-2 256-bit message digest.
NULL-SHA	No encryption and SHA-1 message digest.
NULL-MD5	No encryption and MD5 message digest.

5.2.38 SSL_CIPHER_SUITES - OMS configuration option

5.2.38.1 Description

The SSL_CIPHER_SUITES option specifies one or more **SSL/TLS 1.3 specific** cipher suites that are acceptable to use for network communications between OMS clients and the OMS server.

This option is specific to TLS 1.3. To configure ciphers for TLS 1.2 and earlier, see the `ssl_cipher_list` option.

5.2.38.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	ssl_cipher_suites *ciphers*			✓	✓	

The option is NOT currently supported on HP-UX

5.2.38.3 Value

ciphers is a comma-separated list of SSL/TLS 1.3 specific cipher suites. The following table identifies the list of SSL/TLS cipher suites supported for this option.

The list is in default order, with the most preferred suite first and the least preferred suite last.

Cipher Suite	Description
TLS_AES_256_GCM_SHA384	256-bit AES encryption in Galois Counter Mode, SHA-2 384-bit message digest
TLS_CHACHA20_POLY1305_SHA256	256-bit CHACHA encryption with POLY1305 message authentication, SHA-2 256-bit message digest
TLS_AES_128_GCM_SHA256	128-bit AES encryption in Galois Counter Mode, SHA-2 256-bit message digest

5.2.39 TMP_DIRECTORY - OMS configuration option

5.2.39.1 Description

The TMP_DIRECTORY option specifies the directory in which OMS will create temporary files.

5.2.39.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	tmp_directory *directory*			✓	✓	

5.2.39.3 Values

directory is the name of the directory.

A fully qualified path name must be specified.

5.2.39.3.1 Defaults

UNIX	Default is `/var/opt/universal/tmp`.
Windows	Default is `..\tmp`.

5.2.40 TRACE_DIRECTORY - OMS configuration option

5.2.40.1 Description

The TRACE_DIRECTORY option specifies the directory into which OMS trace files are written (if the MESSAGE_LEVEL option value is set to **trace**).

Trace files capture the flow of OMS, and may be requested by Stonebranch customer support to diagnose complex problems.

5.2.40.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	trace_directory *directory*			✓	✓	

5.2.40.3 Values

directory is the name of the directory for trace files.

Full path names are recommended.

5.2.40.3.1 Defaults

UNIX	Default is `/var/opt/universal/trace`.
Windows	Default is `C:\Program Files\Universal\OmsSrv`.

5.2.41 TRACE_FILE_LINES - OMS configuration option

5.2.41.1 Description

The TRACE_FILE_LINES option specifies the maximum number of lines to write to the trace file.

A trace file is generated when the MESSAGE_LEVEL option is set to **trace**.

The trace file will wrap around when the maximum number of lines has been reached and start writing trace entries after the trace header lines.

The average number of bytes per trace file line is approximately 50.

5.2.41.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	trace_file_lines *lines*			✓	✓	

5.2.41.3 Values

lines is the maximum number of lines to write to the trace file.

Default is 500,000. (If space is limited in the trace file directory, set *lines* to a smaller value.)

5.2.42 TRACE_TABLE - OMS configuration option

5.2.42.1 Description

The TRACE_TABLE option specifies the size of a wrap-around trace table maintained in memory.

(Trace data can be written to the trace table or written to a file as it is produced.)

The trace table is written to a file when the program ends under the conditions specified in this option.

Tracing is activated, and a trace file is generated, when the MESSAGE_LEVEL option is set to **trace**.

5.2.42.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	trace_table *size, condition*			✓	✓	

5.2.42.3 Values

size is the size (in bytes) of the trace table.

The size can be suffixed with either of the following characters:

- **M** indicates that the size is specified in megabytes
- **K** indicates that the size is specified in kilobytes

For example, *50M* indicates that 50 X 1,048,576 bytes of memory is allocated for the trace table.

> **Note**
>
> If *size* is **0**, the trace table is not used.

Default is 0.

condition is the condition under which the trace table is written.

Possible values for *condition* are:

- **error**
  Write the trace table if the program ends with a non-zero exit code.
- **always**
  Write the trace table when the program ends regardless of the exit code.
- **never**
  Never write the trace table.

Default is never.

5.3 OMS Server Component Definition Options

5.3.1 Overview

This page provides links to detailed information about the options that comprise OMS Server component definitions.

The options are listed alphabetically, without regard to any specific operating system.

5.3.2 Component Definition Options Information

For each component definition option, these pages provide the following information.

5.3.2.1 Description

Describes the option and how it is used.

5.3.2.2 Usage

Provides a table of the following information:

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Component Definition Keyword	<Format / Value>					

5.3.2.2.1 Method

Identifies the method used for specifying an OMS component definition option:

- Component Definition Keyword

5.3.2.2.2 Syntax

Identifies the syntax of the method used to specify the option:

- Format: Specific characters that identify the option.
- Value: Type of value(s) to be supplied for this method.

5.3.2.2.3 (Operating System)

Identifies the operating systems for which the method of specifying the option is valid:

- IBM i
- HP NonStop
- UNIX
- Windows
- z/OS

5.3.2.3 Values

Identifies all possible values for the specified value type.

Defaults are identified in **bold type**.

5.3.3 Component Definition Options List

The following table identifies all of the options that can comprise an OMS component definition. Each **Option Name** is a link to detailed information about that option.

Option Name	Description
AUTOMATICALLY_START	Specification for whether or not the OMS Server starts automatically when Universal Broker is started.
COMPONENT_NAME	Name by which the clients know the OMS Server.
CONFIGURATION_FILE *	Name of the OMS Server configuration file.
RESTART	Specification for whether or not the OMS Server should be restarted if it ends.
RESTART_CONDITIONS	Exit conditions criteria for which the OMS server is considered eligible for restart.
RESTART_DELAY	Number of seconds to wait before restarting the OMS Server.
RESTART_MAX_FREQUENCY	Maximum frequency the OMS Server can be restarted.
RUNNING_MAXIMUM	Maximum number of OMS Servers that can run simultaneously.
START_COMMAND *	Program name of the OMS Server.
WORKING_DIRECTORY *	Directory used as the working directory of the OMS Server.
* These options are required in all component definitions.	

5.3.4 AUTOMATICALLY_START - OMS Component Definition option

5.3.4.1 Description

The AUTOMATICALLY_START option specifies whether or not the Universal Message Service (OMS) Server starts automatically when the Universal Broker is started.

> **Note**
>
> AUTOMATICALLY_START is optional in a component definition.

5.3.4.2 Usage

Method	Parameter / Value	IBM i	HP NonStop	UNIX	Windows	z/OS
Component Definition Keyword	auto_start *option*			✓	✓	

5.3.4.3 Values

option is the specification for how the OMS Server is started.

Valid values for *option* are:

- **yes**
  OMS Server is started automatically when Universal Broker is started.
- **no**
  OMS Server is not started automatically when Universal Broker is started.

5.3.5 COMPONENT_NAME - OMS Component Definition option

5.3.5.1 Description

The COMPONENT_NAME option specifies the name of the Universal Message Service (OMS) Server.

Component start requests refer to OMS Server by this name.

> **Note**
>
> COMPONENT_NAME is optional in a component definition. If it is not specified, the file name is used as the component name.

5.3.5.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Component Definition Keyword	component_name *name*			✓	✓	

5.3.5.3 Values

name is the name of the OMS server.

There is only one valid value for *name*:

- **oms**
  (This is the name of the OMS Server component definition file / member.)

This name should not be changed.

5.3.6 CONFIGURATION_FILE - OMS Component Definition option

5.3.6.1 Description

The CONFIGURATION_FILE option specifies the name of the Universal Message Service (OMS) configuration file.

Note

CONFIGURATION_FILE is required in a component definition.

5.3.6.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Component Definition Keyword	configuration_file *member* **or** configuration_file *file*			✓	✓	

5.3.6.3 Values

member / *file* is the name of the configuration member / file.

UNIX

Full path name of the configuration file. The file name can be any valid file name. The installation default is **/etc/universal/oms.conf**.

Windows

Full path name of the configuration file. The file name can be any valid file name. The installation default is **c:\Documents and Settings\All Users\Application Data\Universal\conf\oms.conf**.

z/OS

Member name of the component configuration file in the **UNVCONF** library allocated to the Universal Broker ddname **UNVCONF**. The installation default is **OMSCFG00**.

5.3.7 RESTART - OMS Component Definition option

5.3.7.1 Description

The RESTART option specifies whether or not the Universal Message Service (OMS) Server should be restarted if it ends.

Note

RESTART is optional in a component definition.

An OMS Server is restarted when the following conditions are met:

1. Universal Broker is not in shutdown mode.
2. OMS Server has not been stopped by Universal Broker, Universal Control, or Universal Enterprise Controller. This is considered a controlled shutdown.
3. RESTART option value is **yes**.
4. OMS Server's exit conditions must meet one of the values specified by the RESTART_CONDITIONS option.
5. OMS Server must not have been restarted more than specified by the RESTART_MAX_FREQUENCY option.

5.3.7.2 Usage

Method	Parameter / Value	IBM i	HP NonStop	UNIX	Windows	z/OS
Component Definition Keyword	restart *option*			✓	✓	

5.3.7.3 Values

option is the specification for how the OMS Server is restarted.

Valid values for *option* are:

- **yes**
  OMS Server is restarted automatically by the Universal Broker if the OMS Server stops.
- **no**
  OMS Server is not restarted automatically by the Universal Broker if the OMS Server stops.

5.3.8 RESTART_CONDITIONS - OMS Component Definition option

5.3.8.1 Description

The RESTART_CONDITIONS option specifies the exit conditions of the OMS Server for which it should be considered eligible for restart.

> **Note**
>
> RESTART_CONDITIONS is optional in a component definition.

If the exit conditions of the OMS Server do not meet the criteria, it will not be restarted.

5.3.8.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	restart_conditions *conditions*			✓	✓	✓

5.3.8.3 Values

conditions is a comma-separated list of exit conditions.

The exit conditions names are based on the Universal Agent return codes. Category names are used instead of numeric values, as the exit code numeric value may not be consistent across all platforms.

The exit conditions are:

ABNORMAL	OMS Server ended abnormally due to a UNIX signal, Windows Exception, z/OS ABEND, etc.
SUCCESS	OMS Server ended normally with exit code 0.
WARN	OMS Server ended normally with a warning exit code.
ERROR	OMS Server ended normally with an error exit code.
FATAL	OMS Server ended normally with a fatal exit code.
CONFIG	OMS Server ended normally with a configuration error exit code.

SECURITY	OMS Server ended normally with a security related exit code.
NETWORK	OMS Server ended normally with a network related exit code.
SHUTDOWN	OMS Server ended normally with a shutdown related exit code.
LICENSE	OMS Server ended normally with a license violation related exit code.
ALL	All of the above.

Default is ABNORMAL,FATAL,ERROR.

5.3.9 RESTART_DELAY - OMS Component Definition option

5.3.9.1 Description

The RESTART_DELAY option specifies the number of seconds to wait from the time the Universal Broker detects that the OMS Server has ended until Universal Broker restarts it.

> **Note**
>
> RESTART_DELAY is optional in a component definition.

5.3.9.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	restart_delay *seconds*			✓	✓	✓

5.3.9.3 Values

seconds is the number of seconds to wait.

Default is 5.

5.3.10 RESTART_MAX_FREQUENCY - OMS Component Definition option

5.3.10.1 Description

The RESTART_MAX_FREQUENCY option specifies the maximum frequency in which the OMS Server can be restarted in a specific time interval.

> **Note**
>
> RESTART_MAX_FREQUENCY is optional in a component definition.

If the UAG Server becomes eligible for restart but exceeds the maximum restart frequency, it will not be restarted.

5.3.10.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Configuration File Keyword	restart_max_frequency *number/interval*			✓	✓	✓

5.3.10.3 Values

number is the maximum number of restarts.

interval is the time interval in which the specified maximum number of restarts (*number*) is allowed.

Valid values for interval are **week**, **day**, **hour**, and **minute**.

Default is 2 / minute.

5.3.11 RUNNING_MAXIMUM - OMS Component Definition option

5.3.11.1 Description

The RUNNING_MAXIMUM option specifies the maximum number of Universal Message Service (OMS) Servers that can run simultaneously.

If this maximum number is reached, any command received to start an OMS Server is rejected.

Note

RUNNING_MAXIMUM is optional in a component definition.

5.3.11.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Component Definition Keyword	running_max *maximum*			✓	✓	

5.3.11.3 Values

maximum is the maximum number of OMS Servers that can run simultaneously.

Default is 1.

Note

If you specify 0 for *maximum*, the default (1) will be used. To use 0 for the maximum number of servers, specify -1 or less for *maximum*.

5.3.12 START_COMMAND - OMS Component Definition option

5.3.12.1 Description

The START_COMMAND option specifies the full path name (member name for z/OS) of the OMS Server program.

Optionally, START_COMMAND also can specify command line options.

Note

START_COMMAND is required in a component definition.

5.3.12.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Component Definition Keyword	start_command *member* **or** start_command *name[options]*			✓	✓	

5.3.12.3 Values

member / *name* is the full path name of the OMS Server program.

options is the optional list of command line options.

z/OS

member is the program object of the OMS Server. The program object must be in the Universal Broker's search order for loading program objects. The default location is the SUNVLOAD library allocated to the Universal Broker's STEPLIB ddname.

Alternatively, *member* can be the fully specified path of a USS external link to the UAG Server program. The external link must be owned by UID 0.

options is not a valid value.

UNIX

name is the full path name of the OMS Server program.

Windows

name is the full path name of the OMS Server program. This name is defined at installation; it is not modifiable from the Universal Configuration Manager.

5.3.13 WORKING_DIRECTORY - OMS Component Definition option

5.3.13.1 Description

The WORKING_DIRECTORY option specifies the full path name used as the working directory of the Universal Message Service (OMS) Server.

Note

WORKING_DIRECTORY is required in a component definition.

5.3.13.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Component Definition Keyword	working_directory *directory*			✓	✓	

5.3.13.3 Values

directory is the full path name of the working directory.

Default is (.).

Caution

Do not change this directory.

UNIX and Windows

directory is the full path name of the directory that the OMS Server uses as its working directory.

z/OS

directory is the HFS directory name that the OMS Server uses as its working directory.

5.4 OMS Server UACL Entries

5.4.1 OMS Server UACL Entries

This page provides links to detailed information on the Universal Access Control List (UACL) entries available for use with the OMS Server.

The UACL entries are listed alphabetically, without regard to any specific operating system.

5.4.2 UACL Entries Information

For each UACL entry, these pages provide the following information.

5.4.2.1 Description

Describes the UACL entry and how it is used.

5.4.2.2 Usage

Provides a table of the following information:

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
UACL File Keyword	<Type / Rule>					

5.4.2.2.1 Method

Identifies the method used for specifying a UACL entry:

- UACL FIle Keyword

5.4.2.2.2 Syntax

Identifies the syntax of the method used for a UACL entry:

- Type: Universal Agent component to which the rule applies.
- Rule: Client's identity, request to which the entry pertains, and security attributes that the entry enforces.

5.4.2.2.3 (Operating System)

Identifies the operating systems for which the method of specifying the UACL entry is valid:

- IBM i

- HP NonStop
- UNIX
- Windows
- z/OS

5.4.2.3 Values

Identifies all possible values for the fields in a UACL entry rule.

Defaults are identified in **bold type**.

5.4.3 UACL Entries List

The following table identifies all OMS UACL Entries. Each **UACL Entry Name** is a link to detailed information about that option.

UACL Entry Name	Description
OMS_ACCESS	Controls from which TCP/IP addresses clients are permitted to establish a TCP/IP connection with the OMS server.
OMS_CERT_ACCESS	Supports client authentication by managing access using properties presented by a client's X.509 certificate.
OMS_MAINTENANCE	Controls which users are permitted to perform OMS maintenance operations.

5.4.4 OMS_ACCESS - UACL Entry

5.4.4.1 Description

An OMS_ACCESS UACL entry controls from which TCP/IP addresses clients are permitted to establish a TCP/IP connection with the OMS server.

5.4.4.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
UACL File Keyword	oms_access *host,access,certrule*			✓	✓	

5.4.4.3 Values

Valid values for *access* are

- **allow** to allow access to the OMS server.
- **deny** to deny access to OMS server.

Refer to UACL Entries for details on *host* specification.

Default is **allow**.

Valid values for *certrule* are:

- **cert** - When *access* is **allow**, the connect is initially accepted but subject to OMS_CERT_ACCESS evaluation.
- **nocert** - Access is governed by host matching rather than client certificate presentation.

Default is **nocert**.

5.4.4.3.1 Examples

5.4.4.3.1.1 Scenario 1

The following example grants access to any OMS client (e.g., UAG Server) with an IP address of 10.20.30.40, provided that client did not provide an X.509 certificate. It will refuse all other connection requests from clients that do not present a certificate. (With no encoded **,cert** rules, connections from clients that provide X.509 certificates are permitted access by default.)

oms_access	10.20.30.40,allow
oms_access	ALL,deny

5.4.4.3.1.2 Scenario 2

The following example *conditionally* grants access to any OMS client (e.g., UAG Server) with an IP address of 10.20.30.40 that presents an X.509 certificate. Before accepting the connection, OMS Server will look for a matching CERT_MAP entry and use its *certid* value to evaluate the OMS_CERT_ACCESS rules.

oms_access	10.20.30.40,allow,cert

Scenario 2a

Given the following CERT_MAP and OMS_CERT_ACCESS entries, OMS Server will accept the above connection.

- OMS will see that the cert_map entry **S2A** matches the incoming client request
- OMS will apply the OMS_CERT_ACCESS rule with the **S2A** id, which grants access to client connection requests originating from 10.20.30.40

cert_map	id=S2A,ipaddress=10.20.30.40
oms_cert_access	S2A,allow
oms_cert_access	*,deny

Scenario 2b

Given the following CERT_MAP and OMS_CERT_ACCESS entries, OMS Server will reject the above connection.

- OMS will fail to find a cert_map entry that matches the incoming client certificate's information
- OMS will apply the global OMS_CERT_ACCESS rule which rejects all connection requests from clients whose certificate information does not match a cert_map entry

cert_map	id=S2A,ipaddress=10.20.40.50
oms_cert_access	S2A,allow
oms_cert_access	*,deny

5.4.4.3.1.3 Scenario 3

The following example is functionality equivalent to Scenario 1, above.

oms_access	10.20.30.40,allow,nocert

5.4.4.3.1.4 Scenario 4

For a more detailed example, consider the following UACL entries:

1	oms_access	10.20.30.40,allow,nocert
2	oms_access	all,allow,cert
3	oms_access	all,deny,nocert
1	oms_cert_access	S4,allow
2	oms_cert_access	*,deny
1	cert_map	id=S4,ipaddress=10.20.30.40

Scenario 4a

A client with a reported IP address of 10.20.30.40 attempts to connect to OMS Server and that client *does not* provide an X.509 certificate.

Result: OMS Server grants the connection using oms_access rule 1.

Scenario 4b

A client with a reported IP address of 10.20.40.50 attempts to connect to OMS Server and that client *does not* provide an X.509 certificate.

Result: OMS Server rejects the connection using oms_access rule 3.

Scenario 4c

A client with a reported IP address of 10.20.40.50 attempts to connect to OMS Server. That client presents an X.509 certificate to OMS.

In this case:

- OMS Server will first evaluate oms_access rules with a *certrule* value of **cert**.
- OMS Server will conditionally accept the condition based on oms_access rule 2.
- OMS Server will use the information to the client certificate to locate a matching cert_map entry.
- No matching cert_map entry exists, OMS Server proceeds to the next oms_cert_access entry.

Result: OMS Server rejects the connection using oms_cert_access rule 2.

Scenario 4d

A client with a reported IP address of 10.20.30.40 attempts to connect to OMS Server. That client presents an X.509 certificate to OMS.

In this case:

- OMS Server will first evaluate oms_access rules with a *certrule* value of **cert**.
- OMS Server will conditionally accept the condition based on oms_access rule 2.
- OMS Server will use the information to the client certificate to locate a matching cert_map entry.
- The cert_map rule is a match.
- OMS Server uses the cert_map's id value to locate a matching oms_cert_access entry.

Result: OMS Server accepts the connection using oms_cert_access rule 1.

5.4.4.3.2 Default

oms_access	ALL,allow.nocert

5.4.5 OMS_CERT_ACCESS - UACL Entry

5.4.5.1 Description

An OMS_CERT_ACCESS UACL entry supports client authentication by managing access using properties presented by a client's X.509 certificate.

5.4.5.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
UACL File Keyword	oms_cert_access *certid,access*			✓	✓	

5.4.5.3 Values

Valid values for *access* are

- **allow** - The OMS Server can accept connection requests from the client.
- **deny** - The OMS Server should not accept connection requests from the client

Default is **allow**.

See UACL Entries for details on *certid*.

5.4.5.4 OMS_ACCESS Interaction

OMS Server will only evaluate OMS_CERT_ACCESS entries for client connection requests that satisfy the following conditions:

- The client presents an X.509 certificate to OMS Server
- An OMS_ACCESS entry must exist whose *host* value matches the hostname or IP address reported by the client
- The *access* value in the matching OMS_ACCESS entry must be **allow**
    - If the *access* value is **deny**, the connection request is rejected with no further evaluation
- The *certrule* value in the matching OMS_ACCESS entry must be **cert** (see OMS_ACCESS for background on why this interaction exists)
    - If the *certrule* value is **nocert**, OMS Server will proceed to the next OMS_ACCESS entry.

When these conditions are met, OMS Server will *conditionally* accept the client connection. Final acceptances depends on the result of OMS_CERT_ACCESS evaluation.

5.4.5.5 OMS_CERT_ACCESS Evaluation

OMS Server will only evaluate OMS_CERT_ACCESS rules when an client connection request satisfies the conditions listed above. When those conditions are met, OMS Server will conditionally accept the connection, pending the results of the OMS_CERT_ACCESS evaluation, described below.

- OMS Server will look for a CERT_MAP entry that matches information in the client's certificate.
- OMS Server will use that CERT_MAP entry's *certid* value to locate a matching OMS_CERT_ACCESS entry.
    - If OMS Server does not find a match, it will permit the connection.
    - If a match is found, OMS Server will permit or reject the connection based on the entry's *access* value (i.e., **allow** or **deny**).

UAG Server Client Certificates

You must set UAG Server's SSL_CLIENT_AUTH option to send any configured certificate/private key from UAG Server to OMS Server.

Additional Certificate Authentication

Prior to UACL rule evaluation, OMS Server may also reject in one of two ways:

- If OMS Server cannot authenticate the client certificate's issuer (i.e., CA validation fails), OMS will refuse the connection.
- If the OMS Server configuration option AUTHENTICATE_PEER is set to **yes** and the client certificate does not contain a hostname or IP address that matches the client system's DNS Name or IP Address, OMS will refuse the connection.

- When AUTHENTICATE_PEER is **no**, OMS Server relies solely on the OMS_CERT_ACCESS rules to accept or reject connections based on client certificate information.

CERT_MAP Requirement

If you intend to author OMS_CERT_ACCESS rules into your configuration, you must also have one or more CERT_MAP entries defined. The Universal Agent does not support a configuration where OMS_CERT_ACCESS rules exist without CERT_MAP entries.

5.4.5.5.1 Examples

5.4.5.5.1.1 Scenario 1

The following example *conditionally* grants access to any OMS client (e.g., UAG Server) with an IP address of 10.20.30.40 that presents an X.509 certificate. Before accepting the connection, OMS Server will look for a matching CERT_MAP entry and use its *certid* value to evaluate the OMS_CERT_ACCESS rules.

oms_access	10.20.30.40,allow,cert

Scenario 2a

Given the following CERT_MAP and OMS_CERT_ACCESS entries, OMS Server will accept the above connection.

- OMS will see that the cert_map entry **S2A** matches the incoming client request
- OMS will apply the OMS_CERT_ACCESS rule with the **S2A** id, which grants access to client connection requests originating from 10.20.30.40

cert_map	id=S2A,ipaddress=10.20.30.40
oms_cert_access	S2A,allow
oms_cert_access	*,deny

Scenario 2b

Given the following CERT_MAP and OMS_CERT_ACCESS entries, OMS Server will reject the above connection.

- OMS will fail to find a cert_map entry that matches the incoming client certificate's information
- OMS will apply the global OMS_CERT_ACCESS rule which rejects all connection requests from clients whose certificate information does not match a cert_map entry

cert_map	id=S2A,ipaddress=10.20.40.50

oms_cert_access	S2A,allow
oms_cert_access	*,deny

5.4.5.5.1.2 Scenario 2

The following example grants access to any OMS client (e.g., UAG Server) with an IP address of 10.20.30.40, *provided that client did not provide an X.509 certificate*.

oms_access	10.20.30.40,allow,nocert

5.4.5.5.1.3 Scenario 3

For a more detailed example, consider the following UACL entries:

1	oms_access	10.20.30.40,allow,nocert
2	oms_access	all,allow,cert
3	oms_access	all,deny,nocert
1	oms_cert_access	S4,allow
2	oms_cert_access	*,deny
1	cert_map	id=S4,ipaddress=10.20.30.40

Scenario 3a

A client with a reported IP address of 10.20.30.40 attempts to connect to OMS Server and that client *does not* provide an X.509 certificate.

Result: OMS Server grants the connection using oms_access rule 1.

Scenario 3b

A client with a reported IP address of 10.20.40.50 attempts to connect to OMS Server and that client *does not* provide an X.509 certificate.

Result: OMS Server rejects the connection using oms_access rule 3.

Scenario 3c

A client with a reported IP address of 10.20.40.50 attempts to connect to OMS Server. That client presents an X.509 certificate to OMS.

In this case:

- OMS Server will first evaluate oms_access rules with a *certrule* value of **cert**.
- OMS Server will conditionally accept the condition based on oms_access rule 2.
- OMS Server will use the information to the client certificate to locate a matching cert_map entry.
- No matching cert_map entry exists, OMS Server proceeds to the next oms_cert_access entry.

Result: OMS Server rejects the connection using oms_cert_access rule 2.

Scenario 3d

A client with a reported IP address of 10.20.30.40 attempts to connect to OMS Server. That client presents an X.509 certificate to OMS.

In this case:

- OMS Server will first evaluate oms_access rules with a *certrule* value of **cert**.
- OMS Server will conditionally accept the condition based on oms_access rule 2.
- OMS Server will use the information to the client certificate to locate a matching cert_map entry.
- The cert_map rule is a match.
- OMS Server uses the cert_map's id value to locate a matching oms_cert_access entry.

Result: OMS Server accepts the connection using oms_cert_access rule 1.

5.4.6 OMS_MAINTENANCE - UACL Entry

5.4.6.1 Description

An OMS_MAINTENANCE UACL entry controls which users are permitted to perform OMS administration operations using the OMS Administration Utility.

5.4.6.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
UACL File Keyword	oms_maintenance *local_user,set_access,delete_access,list_access*			✓	✓	

5.4.6.3 Values

The UACL rule consists of the following positional fields:

Field	Values	Description
local_user	*name*	Local user name. May contain generic pattern matching characters.
set_access	{allow|deny}	Allow or deny access to the OMSADM SET commands.
delete_access	{allow|deny}	Allow or deny access to the OMSADM DELETE commands.
list_access	{allow|deny}	Allow or deny access to the OMSADM LIST commands.

5.4.6.3.1 Examples

oms_maintenance	root,allow,allow,allow	Permit local user *root* access to all OMSADM commands.
oms_maintenance	joe,deny,deny,allow	Permit local user *joe* access to OMSADM LIST command only.
oms_maintenance	*,deny,deny,deny	Deny access to all other users.

5.4.6.3.2 Default

oms_maintenance	*,allow,allow,allow

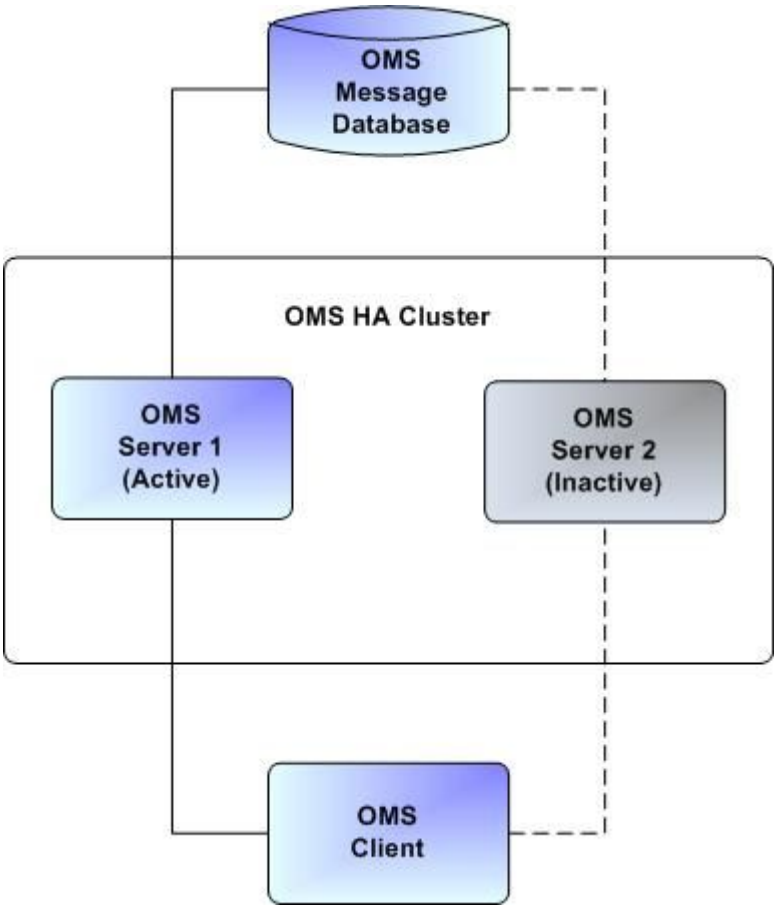
5.5 OMS Server High Availability

5.5.1 Overview

Universal Message Service (OMS) is a communication middleware component providing network communications between the distributed Universal Automation Center components. OMS availability is a core requirement for a majority of the Universal Automation Center services. Universal Automation Center deployment requiring near 100% reliability and availability requires an OMS High Availability (HA) cluster deployment.

An OMS HA cluster consists of one active OMS Server and one or more inactive (passive) OMS Servers sharing a common OMS message database. OMS clients are configured with a list of OMS server addresses, one address for each OMS Server in the HA cluster. If the active OMS Server become unavailable, one of the inactive OMS Servers automatically assumes the role of the active OMS Server. OMS clients detect that the original active OMS Server is not available and automatically fail-over to the new active OMS Server. The shared OMS message database Ensures that no messages are lost when there is a change in the active OMS Server.

The following diagram illustrates a simple HA cluster configuration. It consists of two OMS Servers deployed on two different machines. *OMS Server 1* is the active OMS Server and *OMS Server 2* is the inactive OMS Server. Both OMS Servers share a common OMS message database. The OMS clients connect to the active OMS Server.



5.5.2 High Availability Configuration

Configuring an HA cluster consists of the following steps:

Step 1	Deploy the OMS message database on a shared file system that is available to all OMS Server cluster members.
Step 2	Configure the OMS Server cluster members to use the shared OMS message database.
Step 3	Configure the OMS clients with the list of OMS server cluster members.

5.5.2.1 Shared OMS Message Database

The OMS message database must reside on a shared file system accessible by each of the OMS Server cluster members. The shared OMS message database is utilized for the following capabilities:

1. The active OMS server selection process.
2. OMS message availability in fail-over scenarios.

The OMS Server cluster members determine the active OMS Server by obtaining an exclusive lock on a lock file in the OMS message database directory. The active OMS Server holds the file lock for the entire time it is executing. The inactive OMS Servers check every three seconds to see if the file lock is available. If the active OMS Server terminates, the exclusive file lock

will be released, allowing one of the inactive OMS Servers to obtain exclusive access to the file lock. The OMS Server that obtains the file lock becomes the active OMS Server in the cluster.

The file system on which the OMS message database resides may be on a SAN or a network file system. The file system must support distributed file locks. On POSIX-based systems, such as UNIX and Linux, NFS version 4 or higher may be used. NFS version 3 does not support reliable file locks and must not be used. On Windows-based systems, SMB accessible file systems do provide support for file locks. Other network file systems are available. Check with the file system vendor to determine if POSIX compliant distributed file locks are supported.

The shared file system on which the OMS message database is located should be deployed as an HA configuration. If the shared file system becomes unavailable, the OMS HA cluster members will not have access to the OMS message database and will be rendered inoperable.

5.5.2.2 OMS Server Cluster

An OMS Server cluster consists of two or more OMS Servers sharing a common OMS message database. The OMS Servers should be installed on different machines in order to provide fault tolerance in the case of machine failure. The OMS message database contains platform-specific data types. Consequentially, all OMS Servers in the HA cluster must be installed on the same operating systems and hardware architectures - data size (32-bit or 64-bit) and encoding (little-endian or big-endian) - must be the same between all OMS Server cluster members.

Each OMS Server in the HA cluster must be configured to use the same, shared OMS message database. The OMS Server SPOOL_DIRECTORY OMS configuration option specifies the location of the OMS message database. Its value must be the same for all cluster members.

5.5.2.3 OMS Clients

OMS clients are configured with the address of the OMS Server used for network communications. OMS clients support using both a single, non-HA OMS Server as well as an OMS Server HA cluster. In the case of an HA cluster, the OMS clients support automatic fail-over between the OMS Server cluster members. OMS clients utilize an OMS HA cluster by configuring the OMS clients with an ordered, comma-separated list of OMS Server addresses. The OMS Servers specified in the address list must be members of the same HA cluster. If an OMS Server is specified that is not a member of the same OMS HA cluster, the results are unpredictable.

Below is an example OMS Server HA cluster address list.

```
oms1.acme.com,oms2.acme.com,oms3.acme.com
```

OMS clients will connect to the first OMS Server in the OMS Server address list, `oms1.acme.com`. If that OMS server is not available, the OMS client will attempt to connect to the next OMS Server in the list, `oms2.acme.com`, and so on, until it has successfully connected to an OMS Server. If none of the OMS Servers are available, the OMS client will wait for a period of time and try again to establish a connection with one of the OMS Servers. When an OMS client establishes a connection, it will utilize the OMS Server for network communications. If the connection fails for any reason, the OMS client will start the process of establishing a connection with the next OMS Server in the OMS Server list until it is successful.

See the documentation for a specific OMS client for details on how the OMS Server address list is specified for that OMS client.

5.6 OMS Server SSL/TLS Configuration

5.6.1 Overview

The OMS server supports Secure Socket Layer / Transport Layer Security (SSL/TLS). SSL/TLS provides for data privacy and integrity as well as OMS server authentication by the OMS clients. Whether SSL/TLS is used for network communications is determined by the OMS client configuration.

The OMS server supports both SSL/TLS encryption and authentication.

5.6.2 OMS Client to OMS Server SSL/TLS Encryption

There are two types of OMS clients:

- Universal Agent UAG component
- Universal Controller

Each can be configured separately to support SSL/TLS encryption.

5.6.2.1 UAG to OMS SSL Configuration

It is recommended that the following configuration options are reviewed and adjusted to suit your security requirements.

5.6.2.1.1 UAG Server (OMS Client) Configuration: uags.conf

Option	Keyword	Values	Description
ENABLE_SSL	N/A	YES	Prior to Universal Agent 7.0.0.0, ENABLE_SSL was a configurable value that allowed the SSL/TLS protocol to be disabled for network communication between UAG and OMS. Starting with Universal Agent 7.0.0.0, the ability to configure this option was removed and SSL/TLS is always used for UAG/OMS communication.
MIN_SSL_PROTOCOL	min_ssl_protocol	TLS1_0 or TLS1_2, (default = TLS1_2)	Specifies the minimum SSL/TLS protocol level that will be negotiated and used. This also can be set in the OMS server configuration; both the OMS server and OMS clients must contain at least one common protocol in order to successfully communicate. You should be aware that older versions may not support TLS1_2.
SSL_CIPHER_LIST	ssl_cipher_list	list of cipher suites	Specifies one or more acceptable cipher suites to use for network communication. You should review this list and adjust it in order to enforce the level of encryption to suit your security policy requirements. This also can be set in the OMS server configuration; both the OMS server and OMS clients must contain at least one common cipher suite in order to successfully communicate. You should be aware that different versions may not support all of the same cipher suites.

5.6.2.2 Universal Controller (OMS Client) Configuration

By default, Universal Controller uses the default SSL/TLS context; check with your server administrator for information on how your environment is configured.

5.6.2.2.1 Universal Controller Configuration: opswise.properties

Property	Desscription
uc.trustmanager.ssl.protocols	Comma-separated list of SSL/TLS protocols that can be negotiated and used. This also can be set in the OMS server configuration; both the OMS server and OMS clients must contain at least one common protocol in order to successfully communicate. You should be aware that older versions may not support TLS1_2.

5.6.2.3 OMS Server Configuration

5.6.2.3.1 OMS Server Configuration: oms.conf

Option	Keyword	Values	Description
MIN_SSL_PROTOCOL	min_ssl_protocol	TLS1_0 or TLS1_2, (default = TLS1_2)	Specifies the minimum SSL/TLS protocol level that will be negotiated and used. This also can be set in the UAGS server configuration; both the OMS server and OMS clients must contain at least one common protocol in order to successfully communicate. You should be aware that older versions may not support TLS1_2.
SSL_CIPHER_LIST	ssl_cipher_list	list of cipher suites	Specifies one or more acceptable cipher suites to use for network communication. You should review this list and adjust it in order to enforce the level of encryption to suit your security policy requirements. This also can be set in the UAGS server configuration; both the OMS server and OMS clients must contain at least one common cipher suite in order to successfully communicate. You should be aware that different versions may not support all of the same cipher suites.

5.6.3 OMS Server Authentication

Each OMS client can request to authenticate the OMS server. If this option, is configured the OMS client will validate the OMS server certificate to ensure that the OMS server host is valid. This is done by validating the OMS host or IP address in the OMS client's OMS server definition with the Common Name (CN) of the OMS server certificate. The OMS server inherits its certificate from its Universal Broker.

5.6.3.1 OMS Server Certificate Configuration: ubroker.conf

Option	Keyword	Description
CERTIFICATE	certificate	Specifies the location of the file that contains the PEM-formatted X.509 certificate.
PRIVATE_KEY	private_key	Specifies the location of the PEM-formatted file that contains the RSA private key associated with OMS Server's UBROKER X.509 certificate.

Option	Keyword	Description
PRIVATE_KEY_PWD	private_key_password	If the RSA private key requires a password or passphrase; specifies that password or passphrase.

5.6.3.2 UAG (OMS Client) Configuration: uags.conf

Option	Keyword	Values	Description
SSL_SERVER_AUTH	ssl_server_auth	YES or NO, (default = NO)	Specifies whether or not UAG authenticates the OMS server certificate as part of the SSL handshake.

5.6.3.3 Controller (OMS Client) Configuration

The Controller specifies whether or not to authenticate the OMS server certificate as part of the SSL/TLS handshake, based on whether the Authenticate OMS Server field is checked in the OMS Server Details for that OMS server in the Controller user interface.

5.6.4 OMS Client Authentication

The OMS server can decide from which TCP/IP addresses OMS clients are permitted to establish a TCP/IP connection with the OMS server.

5.6.4.1 OMS Server UACL Configuration: uacl.conf

UACL Entry	Keyword	Values	Description
OMS_ACCESS	oms_access	HOST,{allow|deny}	Controls from which TCP/IP addresses clients are permitted to establish a TCP/IP connection with the OMS server.

6 OMS Administration Utility

6.1 OMS Administration Utility

The OMS Administration Utility is available to obtain information on the state of the OMS server and to provide support and diagnostic services. Access to the Administration Utility should be limited to the group responsible for administering the OMS server.

The Administration Utility is a command line program that interacts with the local OMS server. Access to its services can be controlled with UACL entries.

The Administration Utility provides the following capabilities:

- List OMS client connection information
- List OMS queue information
- List OMS message data file segments and perform segment integrity check
- Delete OMS queues
- Active a message trace
- Test I/O performance of a particular file system

6.2 Additional Information

The following pages provide additional detailed information for the OMS Administration utility:

- OMS Administration Utility Commands
- OMS Administration Utility Command Options

6.3 OMS Administration Utility Commands

6.3.1 OMS Administration Utility Commands

This page identifies and provides links to detailed information on all OMS Administration Utility commands.

Each command has command options associated with it that can be used to specify additional information / actions for an execution of that command.

6.3.2 Command Information

Each command name in the Commands List, below, is a link to the following information about that command:

Command Description	Description of the operation(s) performed by the command.
Command Line Syntax	Syntax of the command and its options on the command line.

Command Argument	Command line expression (short and/or long form) and description of the command argument.
Command Options	Description of the configuration options associated with the option and a link to detailed information about those options.

6.3.3 Commands List

The following table identifies all OMS Administration Utility commands.

Command	Description
DELETE	Deletes OMS objects of a specified type in the OMS Server.
LIST	Lists OMS objects of a specified type in the OMS Server.
SET	Sets OMS option group in the OMS Server.
TEST	Executes a specified test.

6.3.4 DELETE - OMS Administration Utility Command

6.3.4.1 Description

The DELETE command deletes OMS queues in the OMS Server.

Data loss

When a queue is deleted, all messages in a queue are also deleted.

6.3.4.2 Command Line Syntax

The following figure illustrates the command line syntax of the DELETE command, using the command line, long form of its command options.

```
-delete queue -queuename qname
    [-codepage codepage]
    [-file cmfile]
    [-encryptedfile ecmfile [-key ecmdkey]]
    [-level msglevel]
    [-nls_directory directory]
    [-port port]
```

6.3.4.3 Command Options

The following table describes all DELETE command options and provides the command line, long form of each option illustrated in the DELETE command line syntax, above.

Command Option Name	Command Line Long Form	Description
QUEUE_NAME	-queuename	OMS queue name to select for listing or deleting.
CODE_PAGE	-codepage	Local code page used to translate text data from and to the OMS Server.
FILE	-file	Command file that contains OMS Administration Utility (**omsadm**) command line options.
ENCRYPTED_FILE	-encryptedfile	Command file encrypted by the Universal Encrypt (**uencrypt**) utility.
KEY	-key	Encryption key used to encrypt the encrypted command file.
MESSAGE_LEVEL	-level	Severity level of messages to be written.
NLS_DIRECTORY	-nls_directory	Directory in which to find the Universal Translation Table (UTT) file specified by the CODE_PAGE command option.
PORT	-port	TCP port on which the local OMS Server is listening for connections.

6.3.5 HELP - OMS Administration Utility Command

6.3.5.1 Description

The HELP command prints the OMS Administration Utility command line help and exits.

6.3.5.2 Command Argument

The HELP command can be expressed as either:

- **-h** (Short form)
- **-?** (Short form)
- **-help** (Long form)

6.3.5.3 Command Line Syntax

The following figure illustrates the command line syntax of the HELP command, using its command line, long form.

```
-help
```

6.3.6 LIST - OMS Administration Utility Command

6.3.6.1 Description

The LIST command lists OMS objects in the OMS Server of a specified type. The following information may be listed:

- OMS client connections
- OMS message queues
- OMS message data files

6.3.6.2 Command Line Syntax

The following figures illustrate the command line syntax of the LIST command, using the command line, long form of its command options.

```
-list {connections CNN_OPTS | queues QUE_OPTS | data DATA_OPTS} GENERAL_OPTS

CNN_OPTS

    [-clientid id]
    [-print prtopt]
    [-summary opt]
    [-headers opt]

QUE_OPTS

    [-queuename qname]
    [-print prtopt]
    [-summary opt]
    [-headers opt]

DATA_OPTS

    -datafile datafile
    [-offset offset]


GENERAL_OPTS

    [-codepage codepage]
    [-file cmfile]
    [-encryptedfile ecmfile [-key ecmdkey]]
    [-level msglevel]
    [-nls_directory directory]
    [-port port]
```

6.3.6.3 Command Options

The following table describes all LIST command options and provides the command line, long form of each option illustrated in the LIST command line syntax, above.

Command Option Name	Command Line Long Form	Description
CLIENT_ID	-clientid	OMS connection client ID to select.
DATA_FILE	-datafile	OMS message data file to be listed.
HEADERS	-headers	Specification for whether or not the column header line is printed.
OFFSET	-offset	Offset into the OMS message data file where the data list will start to list message data file segments.
PRINT	-print	Category of information to print.
SUMMARY	-summary	Specification for whether or not to print a summary line after listing the requested OMS objects.
QUEUE_NAME	-queuename	OMS queue name to select for listing or deleting.
CODE_PAGE	-codepage	Local code page used to translate text data from and to the OMS Server.
FILE	-file	Command file that contains OMS Administration Utility (**omsadm**) command line options.
ENCRYPTED_FILE	-encryptedfile	Command file encrypted by the Universal Encrypt (**uencrypt**) utility.
KEY	-key	Encryption key used to encrypt the encrypted command file.
MESSAGE_LEVEL	-level	Severity level of messages to be written.
NLS_DIRECTORY	-nls_directory	Directory in which to find the Universal Translation Table (UTT) file specified by the CODE_PAGE command option.
PORT	-port	TCP port on which the OMS Server is listening for connections.

6.3.6.4 List Information

The information the LIST command prints is determined by the OMS object being listed and the PRINT option value. The table below lists all potential information listed by its column header name.

Header Name	Object	Description
CERT	connection	The OMS client digital certificate if provided.
CLIENT_ID	connection	The OMS client ID, also known as connection ID.
CONNECT_TIME	connection	The time the OMS client connected to the OMS server.

Header Name	Object	Description
CONS_CNT	connection and queue	For connections, the number of registered OMS consumers on the connection. For queues, the number of registered OMS consumers on the queue.
CREATE_TIME	queue	The time the queue was created. Note that the queue create time is reset when the OMS server start.
IP_ADDRESS	connection	The OMS client IP address.
LAST_REQUEST_TIME	connection	The last time a request was received from the OMS client.
LAST_REQUEST_NAME	connection	The name of the last request command received from the OMS client.
MSG_CNT	queue	The number of OMS messages in the queue.
MSG_CONS_CNT	connection	The number of total OMS messages consumed on the OMS client connection.
MSG_PROD_CNT	connection	The number of total OMS messages produced on the OMS client connection.
MSGQ_CNT	connection	The number of message or replies pending delivery to the OMS client.
PND_ACK	queue	Whether there is an OMS message delivery acknowledgement pending on the queue.
PND_CONSUMER	queue	The OMS client from which the OMS server is waiting for message delivery acknowledgement.
PROD_CNT	connection	The number of registered OMS producers on the connection.
QUEUE_NAME	queue	The name of the queue.
SENDING	connection	Whether data is in the process of being sent to the OMS client or not.
STATE	connection	The state of the OMS connection.
RECVING	connection	Whether data is in the process of being received from the OMS client or not.
REQUEST	connection	The OMS client request command in the process of being serviced by the OMS server.
TYPE	connection	The OMS connection type.
VERSION	connection	The OMS client library version used by the OMS client.

6.3.7 SET - OMS Administration Utility Command

6.3.7.1 Description

The SET command sets up an OMS message trace in the OMS Server. A message trace is used by Stonebranch Customer Support to diagnose OMS messaging related problems.

Caution

Message bodies may contain private data. The message trace file should be protected from unauthorized access.

The OMS server supports one active message trace at a time.

When a message trace is activated, the message trace path name is printed in the Universal Broker log. The OMS message trace file is created in the OMS server trace directory, which defaults to the following locations:

Platform	Directory
UNIX	`/var/opt/universal/trace`
Windows	`C:\Program Files\Universal\OmsSrv`

6.3.7.2 Command Line Syntax

The following figure illustrates the command line syntax of the SET command, using the command line, long form of its command options.

```
-set msgtrace
    [-trace opt]
    [-tracebodymax length]
    [-tracefmt hdrfmt[,bodyfmt]]
    [-traceid id]
    [-tracetimeout timeout]
    [-codepage codepage]
    [-file cmfile]
    [-encryptedfile ecmfile [-key ecmdkey]]
    [-level msglevel]
    [-nls_directory directory]
    [-port port]
```

6.3.7.3 Command Options

The following table describes all SET command options and provides the command line, long form of each option illustrated in the SET command line syntax, above.

Command Option Name	Command Line Long Form	Description
TRACE	-trace	Instruction to start a message trace on the OMS server or stop an active message trace on the OMS server.
TRACE_BODY_MAX	-tracebodymax	Specification for whether or not the message body is included in the message trace and if so, the maximum number of bytes to include in the trace.

Command Option Name	Command Line Long Form	Description
TRACE_FMT	-tracefmt	Format of the message header and body in the message trace.
TRACE_ID	-traceid	Text value used to generate the message trace file name.
TRACE_TIMEOUT	-tracetimeout	Length of time that a trace is active.
CODE_PAGE	-codepage	Local code page used to translate text data from and to the OMS Server.
FILE	-file	Command file that contains OMS Administration Utility (**omsadm**) command line options.
ENCRYPTED_FILE	-encryptedfile	Command file encrypted by the Universal Encrypt (**uencrypt**) utility.
KEY	-key	Encryption key used to encrypt the encrypted command file.
MESSAGE_LEVEL	-level	Severity level of messages to be written.
NLS_DIRECTORY	-nls_directory	Directory in which to find the Universal Translation Table (UTT) file specified by the CODE_PAGE command option.
PORT	-port	TCP port on which the OMS Server is listening for connections.

6.3.8 TEST - OMS Administration Utility Command

6.3.8.1 Description

The TEST command executes a disk write test to provide a simple measure of a file system performance. The write test is performed in a manner that simulates the I/O methods used by the OMS Server when writing OMS messages to the OMS message database.

I/O performance of a file system is dependent on many factors. A detailed analysis of the performance of an I/O subsystem is beyond the scope of this document. The purposes of the test I/O command is to provide general performance numbers to evaluate the suitability of the file system for the OMS server message database.

The test I/O command writes a specified number of 512-byte blocks to a specified file. By default, each block is flushed to disk to simulate the I/O pattern of the OMS server. The flush interval can be specified to match the configured flush interval of the OMS server.

Some general guidelines for performing an I/O test:

- I/O subsystem performance will vary considerably due to a number of factors, so the test should be performed a number of times to get a good statistical sampling.
- The I/O test file must reside on the file system being considered for the OMS message database.
- The OMS Administration Utility command must be executed from the system on which the OMS server executes. If the file system being tested is a network based file system, this is particular important in order to know the network performance impact as well.

The I/O test will print the results of the test as the number of blocks written per second. As a general guideline, the following table categorizes the message rate.

Rate	Category
> 500	fast
300 - 499	medium
100 - 299	slow
< 100	very slow

6.3.8.2 Command Line Syntax

The following figure illustrates the command line syntax of the TEST command, using the command line, long form of its command options.

```
-test io
    -iocount iocnt
    -iofile iofile
    [-ioflush ioflushcnt]
    [-codepage codepage]
    [-file cmfile]
    [-encryptedfile ecmfile [-key ecmdkey]]
    [-level msglevel]
    [-nls_directory directory]
    [-port port]
```

6.3.8.3 Command Options

The following table describes all TEST command options and provides the command line, long form of each option illustrated in the TEST command line syntax, above.

Command Option Name	Command Line Long Form	Description
IO_COUNT	-iocnt	Number of 512-byte blocks to write in the I/O write test.
IO_FILE	-iofile	File name used for the I/O write test.
IO_FLUSH	-ioflushcnt	Frequency in which data is flushed to disk as part of the I/O write test.
CODE_PAGE	-codepage	Local code page used to translate text data from and to the OMS Server.
FILE	-file	Command file that contains OMS Administration Utility (**omsadm**) command line options.
ENCRYPTED_FILE	-encryptedfile	Command file encrypted by the Universal Encrypt (**uencrypt**) utility.
KEY	-key	Encryption key used to encrypt the encrypted command file.
MESSAGE_LEVEL	-level	Severity level of messages to be written.

Command Option Name	Command Line Long Form	Description
NLS_DIRECTORY	-nls_directory	Directory in which to find the Universal Translation Table (UTT) file specified by the CODE_PAGE command option.
PORT	-port	TCP port on which the OMS Server is listening for connections.

6.3.8.4 Examples

The following example executes an I/O test in the default OMS message database directory on UNIX systems. The example writes 1000 512-byte blocks to the test file `iotest`.

The user must have sufficient permissions to the OMS message database directory to create the `iotest` file.

```
omsadm -test io -iofile /var/opt/universal/spool/oms/iotest -iocount 1000
```

The output of the above command will provide the number of 512-byte blocks written per second.

```
UNV6105I I/O write test: count=1000, flush interval=1, rate=761.61 blocks/sec.
```

6.3.9 VERSION - OMS Administration Utility Command

6.3.9.1 Description

The VERSION command prints the version of the OMS Administration Utility and exits.

6.3.9.2 Command Line Syntax

The following figure illustrates the command line syntax of the VERSION command, using its command line, long form.

```
-version
```

6.4 OMS Administration Utility Command Options

6.4.1 Overview

This page provides links to detailed information on the command options available for use with the OMS Administration Utility.

The options are listed alphabetically, without regard to any specific operating system.

6.4.2 Command Options Information

For each command option, these pages provide the following information.

6.4.2.1 Description

Describes the command option and how it is used.

6.4.2.2 Usage

Provides a table of the following information:

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	<Format / Value>					
Command Line, Long Form	<Format / Value>					

6.4.2.2.1 Method

Identifies the method used to specify OMS Administration Utility command options:

- Command Option, Short Form (case-sensitive)
- Command Option, Long Form (not case-sensitive)

6.4.2.2.2 Syntax

Identifies the syntax of the method used to specify the option:

- Format: Specific characters that identify the option.
- Value: Type of value(s) to be supplied for this method.

6.4.2.2.3 (Operating System)

Identifies the operating systems for which each method of specifying the option is valid:

- IBM i
- HP NonStop
- UNIX
- Windows
- z/OS

6.4.2.3 Values

Identifies all possible values for the specified value type.

A value must be separated from the option name by at least one space.

Defaults are identified in **bold type**.

6.4.2.4 <Additional Information>

Identifies any additional information specific to the option.

6.4.3 Command Options List

The following table identifies all OMS Administration Utility command options.

Option	Description
CLIENT_ID	OMS connection client ID to select.
CODE_PAGE	Local code page used to translate text data from and to the OMS Server.
DATA_FILE	OMS message data file to be listed.
ENCRYPTED_FILE	Command file (see #FILE, below) encrypted by the Universal Encrypt (**uencrypt**) utility.
FILE	Command file that contains OMS Administration Utility (**omsadm**) command line options.
HEADERS	Specification for whether or not the column header line is printed for the output of the LIST command.
IO_COUNT	Number of 512-byte blocks to write in the I/O write test.
IO_FILE	File name used for the I/O write test.
IO_FLUSH	Frequency in which data is flushed to disk as part of the I/O write test.
KEY	Encryption key used to encrypt the encrypted command file <ecmdfile>.
KEYSTORE_PATH	Path to a local or remote Universal Broker service interface from which an encryption key can be obtained.
MESSAGE_LEVEL	Severity level of messages to be written.
NLS_DIRECTORY	Directory in which to find the Universal Translation Table (UTT) file specified by the #CODE_PAGE option.
OFFSET	Offset into the OMS message data file where the data list will start to list message data file segments.
PORT	TCP port on which the OMS Server is listening for connections.
PRINT	Category of information to printed when listing an OMS object.
QUEUE_NAME	OMS queue name to select for listing or deleting.
SUMMARY	Specification for whether or not to print a summary line after listing the requested OMS objects.
TRACE	Instruction to start a message trace on the OMS server or stop an active message trace on the OMS server.
TRACE_BODY_MAX	Specification for whether or not the message body is included in the message trace.

Option	Description
TRACE_FMT	Format of the message header and body in the message trace.
TRACE_ID	Text value used to generate the message trace file name.
TRACE_TIMEOUT	Length of time that a trace is active.

6.4.4 CLIENT_ID - OMS Administration Utility command option

6.4.4.1 Description

The CLIENT_ID option specifies the OMS connection client ID to select.

If no ID is provided, all OMS connections are selected.

6.4.4.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	
Command Line, Long Form	-clientid *id*			✓	✓	

6.4.4.3 Values

id is the OMS connection client ID to select.

id can contain generic pattern matching characters:

- An asterisk (*) matches zero or more characters.
- A question mark (?) matches one character.
- The escape character is a forward slash (/), which can be used to escape pattern matching characters.

6.4.4.4 Command Usage

The CLIENT_ID option is used in the following OMS Administration Utility command:

- LIST

6.4.5 CODE_PAGE - OMS Administration Utility command option

6.4.5.1 Description

The CODE_PAGE option specifies the character code page that is used to translate text data to and from the OMS Server.

The Universal Translate Table (UTT) files are used to translate between Unicode and the local single-byte code page.

6.4.5.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	-t *codepage*			✓	✓	
Command Line, Long Form	-codepage *codepage*			✓	✓	

6.4.5.3 Values

codepage is the character code page that is used to translate data.

codepage references a Universal Translate Table (UTT) file in the directory specified by the NLS_DIRECTORY command option.

UTT files are used to translate between Unicode and the local single-byte code page. (All UTT files end with an extension of **.utt**.)

6.4.5.3.1 Default

Default is different for different operating systems:

- ISO8859-1 (8-bit ASCII): ASCII-based operating systems
- IBM1047 (EBCDIC): EBCDIC-based operating system

See Character Code Pages for a complete list of character code pages provided by Stonebranch Inc. for use with Universal Agent.

6.4.5.4 Command Usage

The CODE_PAGE option is used in the following OMS Administration Utility commands:

- DELETE
- LIST
- SET
- TEST

6.4.6 DATA_FILE - OMS Administration Utility command option

6.4.6.1 Description

The DATA_FILE option specifies the OMS message data file to be listed.

6.4.6.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	-d *datafile*			✓	✓	
Command Line, Long Form	-datafile *datafile*			✓	✓	

6.4.6.3 Values

datafile is the OMS message data file to be listed.

6.4.6.4 Command Usage

The DATA_FILE option is used in the following OMS Administration Utility command:

- LIST

6.4.7 ENCRYPTED_FILE - OMS Administration Utility command option

6.4.7.1 Description

The ENCRYPTED_FILE option specifies a command file encrypted by the Universal Encrypt (**uencrypt**) utility.

6.4.7.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	-x *ecmdfile*			✓	✓	
Command Line, Long Form	-encryptedfile *ecmdfile*			✓	✓	

6.4.7.3 Values

ecmdfile is the command file encrypted by the Universal Encrypt utility.

6.4.7.4 Command Usage

The ENCRYPTED_FILE option is used in the following OMS Administration Utility commands:

- DELETE
- LIST
- SET

- TEST

6.4.8 FILE - OMS Administration Utility command option

6.4.8.1 Description

The FILE option specifies a command file that contains OMS Administration Utility command line options.

A command file is a text file with command line options specified on one or more lines.

6.4.8.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	-f *cmdfile*			✓	✓	
Command Line, Long Form	-file *cmdfile*			✓	✓	

6.4.8.3 Values

cmdfile is the command file that contains OMS Administration Utility command line options.

6.4.8.4 Command Usage

The FILE option is used in the following OMS Administration Utility commands:

- DELETE
- LIST
- SET
- TEST

6.4.9 HEADERS - OMS Administration Utility command option

6.4.9.1 Description

The HEADERS option specifies whether or not the column header line is printed for the output of the OMS Administration Utility LIST command.

6.4.9.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Long Form	-headers *option*			✓	✓	

6.4.9.3 Values

option is the specification for whether or not the column header line is printed.

Valid values for *options* are:

- **yes**
  Column header line is printed.
- **no**
  Column header line is not printed.

Default is yes.

6.4.9.4 Command Usage

The HEADERS option is used in the following OMS Administration Utility command:

- LIST

6.4.10 IO_COUNT - OMS Administration Utility command option

6.4.10.1 Description

The IO_COUNT option specifies the number of 512-byte blocks to write in the I/O write test.

6.4.10.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	
Command Line, Long Form	-iocount *iocnt*			✓	✓	

6.4.10.3 Values

iocnt is the number of 512-byte blocks to write in the I/O write test.

6.4.10.4 Command Usage

The IO_COUNT option is used in the following OMS Administration Utility command:

- TEST

6.4.11 IO_FILE - OMS Administration Utility command option

6.4.11.1 Description

The IO_FILE option specifies the file name used for the I/O write test.

- If the file does not exist, it will be created.
- If the file does exist, it will be truncated.

The file should be located on the same file system being considered for the OMS server message data store.

6.4.11.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	
Command Line, Long Form	-iofile *iofile*			✓	✓	

6.4.11.3 Values

iofile is the file name used for the I/O write test.

6.4.11.4 Command Usage

The IO_FILE option is used in the following OMS Administration Utility command:

- TEST

6.4.12 IO_FLUSH - OMS Administration Utility command option

6.4.12.1 Description

The IO_FLUSH option specifies the frequency (number of block writes) at which data is flushed to disk as part of the I/O write test.

6.4.12.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Long Form	-ioflush *iofluschcnt*			✓	✓	

6.4.12.3 Values

ioflushcnt is the frequency (number of block writes) at which data is flushed to disk as part of the I/O write test.

Default is 1. (Data is flushed every block write.)

6.4.12.4 Command Usage

The IO_FLUSH option is used in the following OMS Administration Utility command:

- TEST

6.4.13 KEY - OMS Administration Utility command option

6.4.13.1 Description

The KEY option specifies the encryption key used by the Universal Encrypt (**uencrypt**) utility to encrypt the encrypted command file.

6.4.13.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	-K *ecmdkey*			✓	✓	
Command Line, Long Form	-key *ecmdkey*			✓	✓	

6.4.13.3 Values

ecmdkey is the encryption key used to encrypt the encrypted command file.

6.4.13.4 Command Usage

The KEY option is used in the following OMS Administration Utility commands:

- DELETE
- LIST
- SET
- TEST

6.4.14 KEYSTORE_PATH - OMS Administration Utility command option

6.4.14.1 Description

The KEYSTORE_PATH option specifies the path to a local or remote Universal Broker service interface from which an encryption key can be obtained.

6.4.14.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	-p *path*			✓	✓	
Command Line, Long Form	-keypath *path*			✓	✓	

6.4.14.3 Value

path is the path to the local or remote Universal Broker service interface.

6.4.15 MESSAGE_LEVEL - OMS Administration Utility command option

6.4.15.1 Description

The MESSAGE_LEVEL option specifies the severity level of messages to write.

Messages of the specified severity level and the levels below it are written. For example, if **info** is specified, **info**, **warn**, and **error** messages are written.

6.4.15.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	-l *msglevel*			✓	✓	
Command Line, Long Form	-level *msglevel*			✓	✓	

6.4.15.3 Values

msglevel is the level of messages to write.

Valid values for *msglevel* are:

- **trace**
  Writes trace messages used for diagnostic purposes to file **omsadm.trc**.

> **Note**
>
> Use **trace** only as directed by Stonebranch, Inc. Customer Support.

- **audit**
  Writes audit, informational, warning, and error messages.
- **info**
  Writes informational, warning, and error messages.
- **warn**
  Writes warning and error messages.
- **error**
  Writes error messages only.

Default is warn.

6.4.15.4 Command Usage

The MESSAGE_LEVEL option is used in the following OMS Administration Utility commands:

- DELETE
- LIST
- SET
- TEST

6.4.16 NLS_DIRECTORY - OMS Administration Utility command option

6.4.16.1 Description

The NLS_DIRECTORY option specifies the directory in which to find the Universal Translation Table (UTT) file specified by the CODE_PAGE option.

6.4.16.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	
Command Line, Long Form	-nls_directory *directory*			✓	✓	

6.4.16.3 Values

directory is the directory in which to find the Universal Translation Table (UTT) file specified by the CODE_PAGE option.

6.4.16.4 Command Usage

The NLS_DIRECTORY option is used in the following OMS Administration Utility commands:

- DELETE
- LIST
- SET
- TEST

6.4.17 OFFSET - OMS Administration Utility command option

6.4.17.1 Description

The OFFSET option specifies the offset into the OMS message data file where the data list will start to list message data file segments.

6.4.17.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	-o *offset*			✓	✓	
Command Line, Long Form	-offset *offset*			✓	✓	

6.4.17.3 Values

offset is the offset into the OMS message data file where the data list will start to list message data file segments.

6.4.17.4 Command Usage

The OFFSET option is used in the following OMS Administration Utility command:

- LIST

6.4.18 PORT - OMS Administration Utility command option

6.4.18.1 Description

The PORT option specifies the TCP port on which the local OMS Server is listening for connections.

6.4.18.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	-p *port*			✓	✓	
Command Line, Long Form	-port *port*			✓	✓	

6.4.18.3 Values

port is the TCP port on which the local OMS Server is listening for connections.

6.4.18.4 Command Usage

The PORT option is used in the following OMS Administration Utility commands:

- DELETE
- LIST
- SET
- TEST

6.4.19 PRINT - OMS Administration Utility command option

6.4.19.1 Description

The PRINT option specifies the category of information to print when listing an OMS object.

6.4.19.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	
Command Line, Long Form	-print *prtinfo*			✓	✓	

6.4.19.3 Values

prtinfo is the category of information to print when listing an OMS object.

Valid values for *prtinfo* are:

- **BASIC**
  Prints only the basic information.

- **STATE**
  Prints object state information.
- **STATISTICS**
  Prints object statistics.
- **ALL**
  Prints all object information.

6.4.19.4 Command Usage

The PRINT option is used in the following OMS Administration Utility commands:

- LIST

6.4.20 QUEUE_NAME - OMS Administration Utility command option

6.4.20.1 Description

The QUEUE_NAME option specifies the OMS queue name to select for listing or deleting.

For a LIST command: If an OMS queue name is not provided, all queues are listed.

For a DELETE command: An OMS queue name must be provided.

6.4.20.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	
Command Line, Long Form	-queuename *qname*			✓	✓	

6.4.20.3 Values

qname specifies the OMS queue name to select for listing or deleting.

qname can contain generic pattern matching characters:

- An asterisk (*) matches zero or more characters.
- A question mark (?) matches one character.
- The escape character is a forward slash (/), which can be used to escape pattern matching characters.

6.4.20.4 Command Usage

The QUEUE_NAME option is used in the following OMS Administration Utility commands:

- DELETE
- LIST

6.4.21 SUMMARY - OMS Administration Utility command option

6.4.21.1 Description

The SUMMARY option specifies whether or not to print a summary line after listing the requested OMS objects.

The contents of the summary depends on the objects being listed.

6.4.21.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	
Command Line, Long Form	-summary *option*			✓	✓	

6.4.21.3 Values

option specifies whether or not to print a summary line after listing the requested OMS objects.

Valid values for *option* are:

- **yes**
  Print the summary line.
- **no**
  Do not print the summary line.

Default is no.

6.4.21.4 Command Usage

The SUMMARY option is used in the following OMS Administration Utility command:

- LIST

6.4.22 TRACE - OMS Administration Utility command option

6.4.22.1 Description

The TRACE option specifies whether to start a message trace on the OMS server or stop an active message trace on the OMS server.

A message trace file is created by the OMS server in the product trace directory.

6.4.22.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	
Command Line, Long Form	-trace *option*			✓	✓	

6.4.22.3 Values

option specifies whether to start a message trace on the OMS server or stop an active message trace on the OMS server.

Valid values for *option* are:

- **on**
  Start a message trace on the OMS server.
- **off**
  Stop an active message trace on the OMS server.

Default is on.

6.4.22.4 Command Usage

The TRACE option is used in the following OMS Administration Utility command:

- SET

6.4.23 TRACE_BODY_MAX - OMS Administration Utility command option

6.4.23.1 Description

The TRACE_BODY_MAX option specifies whether or not the message body is included in a message trace and what the maximum size that should be traced.

Caution

Message bodies may contain private data. The message trace file should be protected from unauthorized access.

6.4.23.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	
Command Line, Long Form	-tracebodymax *length*			✓	✓	

6.4.23.3 Values

length specifies whether or not the message body is included in a message trace and the maximum size of the body included in the trace.

For message bod type **map**, *length* applies to the individual **map** name values.

Valid values for *length* are:

- **0**
  The message body is not included in the message trace.
- **1 (or greater)**
  This maximum number of bytes of the message body is included in the message trace.

Default is 0.

6.4.23.4 Command Usage

The TRACE_BODY_MAX option is used in the following OMS Administration Utility command:

- SET

6.4.24 TRACE_FMT - OMS Administration Utility command option

6.4.24.1 Description

The TRACE_FMT option specifies the format of the message header and body in a message trace.

6.4.24.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	
Command Line, Long Form	-tracefmt *hdrfmt*[,*bodyfmt*]			✓	✓	

6.4.24.3 Values

hdrfmt specifies the format of the message header.

Valid values for *hdrfmt* are:

- **REPORT**
  Header fields are formatted on separate lines.
- **LINE**
  All header fields are formatted on a single line as comma-separated list of K=V values.

Default is REPORT.

bdyfmt (optionally) specifies the format of the message body if it is printed (see the TRACE_BODY_MAX command option).

Valid values for *bdyfmt* are:

- **FORMAT**
  Print the message body in its native, human-readable format.
- **DUMP**
  Print the body as a hexidecimal dump. If the value being printed is a string, a line dump format is used; otherwise, a block dump format is used.
- **LINE**
  Print the message body on a single line.

6.4.24.4 Command Usage

The TRACE_FMT option is used in the following OMS Administration Utility command:

- SET

6.4.25 TRACE_ID - OMS Administration Utility command option

6.4.25.1 Description

The TRACE_ID option specifies a text value used to generate the message trace file name.

The file name will be prefixed with this text value.

The remaining portion of the file name is a date and time stamp with a file extension of **.trc**.

6.4.25.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	
Command Line, Long Form	-traceid *id*			✓	✓	

6.4.25.3 Values

id specifies the text value used to generate the message trace file name.

Default is omsmsg.

6.4.25.4 Command Usage

The TRACE_ID option is used in the following OMS Administration Utility command:

- SET

6.4.26 TRACE_TIMEOUT - OMS Administration Utility command option

6.4.26.1 Description

The TRACE_TIMEOUT option specifies the length of time that a trace is active.

6.4.26.2 Usage

Method	Syntax	IBM i	HP NonStop	UNIX	Windows	z/OS
Command Line, Short Form	n/a			✓	✓	
Command Line, Long Form	-tracetimeout *time* [,*unit*]			✓	✓	

6.4.26.3 Values

time specifies the length of *unit* of time that a trace is active.

If *unit* is not specified, the time is in seconds.

Default is 300s (300 seconds).

unit (optionally) specifies the unit of time specified in *time*.

Valid values for *unit* are:

- **s**
  Seconds
- **m**
  Minutes
- **h**
  Hours
- **d**
  Days

6.4.26.4 Command Usage

The TRACE_TIMEOUT option is used in the following OMS Administration Utility command:

- SET

7 Universal Message Service Additional Information

7.1 OMS Additional Information

The following table identifies and provides links to additional information used by or specific to OMS.

Information	Description
Character Code Pages	Character code pages provided by Stonebranch Inc. for use with Universal Agent components on each supported operating system.
UTT Files	Universal Translate Table (UTT) files are used to translate between Unicode and the local single-byte code page.

7.2 Character Code Pages - OMS

The following table identifies the character code pages provided by Stonebranch Inc. for use with Universal Agent on each supported operating system.

Code Page	CCSID	z/OS	UNIX	Windows	IBM i / HFS	IBM i / LIB	HP NonStop
IBM037	037	✓			✓	✓	
IBM273	273	✓			✓	✓	
IBM277	277	✓			✓	✓	
IBM278	278	✓			✓	✓	
IBM280	280	✓			✓	✓	
IBM284	284	✓			✓	✓	
IBM500	500	✓			✓	✓	
IBM875	875	✓					
IBM1025		✓					
IBM1047		✓			✓	✓	
IBM1140	1140	✓			✓	✓	
IBM1141	1141	✓			✓	✓	

Code Page	CCSID	z/OS	UNIX	Windows	IBM i / HFS	IBM i / LIB	HP NonStop
IBM1142	1142	✓			✓	✓	
IBM1143	1143	✓			✓	✓	
IBM1144	1144	✓			✓	✓	
IBM1145	1145	✓			✓	✓	
IBM1146	1146	✓			✓	✓	
IBM1147	1147	✓			✓	✓	
IBM1148	1148	✓			✓	✓	
IBM4971	4971	✓					
ISO8859-1	819		✓	✓	✓		✓
ISO8859-2	912		✓	✓	✓		✓
ISO8859-3	913		✓	✓	✓		✓
ISO8859-4	914		✓	✓	✓		✓
ISO8859-5	915		✓	✓	✓		✓
ISO8859-6	1089		✓	✓	✓		✓
ISO8859-7	813		✓	✓	✓		✓
ISO8859-8	916		✓	✓	✓		✓
ISO8859-9	920		✓	✓	✓		✓
ISO8859-10			✓	✓	✓		✓
ISO8859-13	921		✓	✓	✓		✓
ISO8859-14			✓	✓	✓		✓
ISO8859-15	923		✓	✓	✓		✓
PC437	437			✓	✓		
PC737	737			✓	✓		
PC775	775			✓	✓		
PC850	850			✓	✓		
PC852	852			✓	✓		

Code Page	CCSID	z/OS	UNIX	Windows	IBM i / HFS	IBM i / LIB	HP NonStop
PC855	855			✓	✓		
PC857	857			✓	✓		
PC860	860			✓	✓		
PC861	861			✓	✓		
PC862	862			✓	✓		
PC863	863			✓	✓		
PC864	864			✓	✓		
PC865	865			✓	✓		
PC866	866			✓	✓		
PC869	869			✓	✓		
PC874	874			✓	✓		
WIN1250	1250			✓	✓		
WIN1251	1251			✓	✓		
WIN1252	1252			✓	✓		
WIN1253	1253			✓	✓		
WIN1254	1254			✓	✓		
WIN1255	1255			✓	✓		
WIN1256	1256			✓	✓		
WIN1257	1257			✓	✓		
WIN1258	1258			✓	✓		

7.3 UTT Files - OMS

The following table identifies the Universal Translate Table (UTT) files that are used to translate between Unicode and the local single-byte code page.

Operating System	UTT File Location*
IBM i	UTT files are located in the **UNVPRD520/UNVNLS** file. *codepage* is the member name of the UTT file.
z/OS	UTT files are members of the PDS allocated to the Broker ddname **UNVNLS**. *codepage* specifies the member name.
UNIX	UTT files are located in the directory specified by the NLS_DIRECTORY option, which defaults to **/opt/universal/nls**. *codepage* is the base file name of the UTT file.
Windows	UTT files are located in the **NLS** subdirectory of the installation directory. *codepage* is the base file name of the UTT file.
HP NonStop	UTT files are located in the **$SYSTEM.UNVNLS** subvolume. *codepage* is the base file name of the UTT file.