NOW-PROTO 1.0

Messages

Transport

The NOW virtual channel protocol use an RDP dynamic virtual channel ("DevolutionsNowAgent") as a transport type.

Message Syntax

The following sections specify the NOW protocol message syntax. Unless otherwise specified, all fields defined in this document use the little-endian format.

Common Structures

NOW_INTEGER

Signed and unsigned integer encoding structures of various sizes.

ⓘ NOW_VARU32

The NOW_VARU32 structure is used to encode signed integer values in the range [0, 0x3FFFFFFF].

c (2 bits): A 2-bit integer containing an encoded representation of the number of bytes in this structure.

Value	Meaning
0	The val1 field is present (1 byte)
1	The val1, val2 fields are present (2 bytes)
2	The val1, val2, val3 fields are present (3 bytes)
3	The val1, val2, val3, val4 fields are present (4 bytes)

val1 (6 bits): A 6-bit integer containing the 6 most significant bits of the integer value represented by this structure.

val2 (1 byte): An 8-bit integer containing the second most significant bits of the integer value represented by this structure.

val3 (1 byte): An 8-bit integer containing the third most significant bits of the integer value represented by this structure.

val4 (1 byte): An 8-bit integer containing the least significant bits of the integer value represented by this structure.

NOW_STRING

ⓘ NOW_VARSTR

The NOW_VARSTR structure is used to represent variable-length strings that could be large, while remaining compact in size for small strings.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
len (variable)
str (variable)

len (variable): A NOW_VARU32 structure containing the string length, excluding the null terminator.

str (variable): The UTF-8 encoded string excluding the null terminator.

NOW_HEADER

The NOW_HEADER structure is the header common to all NOW protocol messages.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1		
msgSize		
msgClass	msgType	msgFlags

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class.

Flag	Meaning
NOW_NEGOTIATION_MSG_CLASS_ID 0x10	Protocol negotiation class
NOW_SYSTEM_MSG_CLASS_ID 0x11	System message class
NOW_SESSION_MSG_CLASS_ID 0x12	Session message class

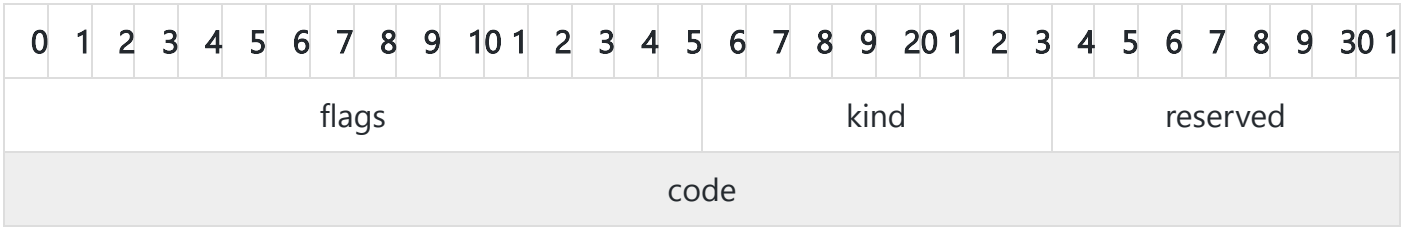
Flag	Meaning
NOW_EXEC_MSG_CLASS_ID 0x13	Exec message class

msgType (1 byte): The message type, specific to the message class.

msgFlags (2 bytes): The message flags, specific to the message type and class.

NOW_STATUS

Operation execution status code.



flags (2 bytes): Status flags.

Value	Meaning
NOW_EXEC_RESULT_ERROR 0x0001	This flag set for all error statuses.
NOW_EXEC_RESULT_ERROR_MESSAGE 0x0002	`errorMessage` field is present and contains optional error message.

kind (1 byte): The status kind. When `NOW_EXEC_RESULT_ERROR` is set, this field represents error kind.

Value	Meaning
NOW_EXEC_RESULT_ERROR_KIND_GENERIC 0x0000	`code` value is undefined and could be ignored.
NOW_EXEC_RESULT_ERROR_KIND_NOW 0x0001	`code` contains NowProto-defined error code.
NOW_EXEC_RESULT_ERROR_KIND_WINAPI 0x0002	`code` field contains Windows error code.
NOW_EXEC_RESULT_ERROR_KIND_UNIX 0x0003	`code` field contains Unix error code.

For successful operation this field value is operation specific.

reserved (1 byte): Reserved value. Should be set to 0 and ignored during parsing.

code (4 bytes): The status code.

- If `NOW_EXEC_RESULT_ERROR` flag is NOT set, this value represents operation-specific code (e.g. process exit code).
- If `NOW_EXEC_RESULT_ERROR` is set, this value represents error code according to `NOW_EXEC_RESULT_ERROR_KIND_*` value. If no error kind flags set, value of this field is undefined and should be ignored.
    - `NOW_EXEC_RESULT_ERROR_KIND_NOW` codes:

Value	Meaning
NOW_CODE_IN_USE 0x0001	Resource (e.g. exec session id is already in use).
NOW_CODE_INVALID_REQUEST 0x0002	Sent request is invalid (e.g. invalid exec request params).
NOW_CODE_ABORTED 0x0003	Operation has been aborted on the server side.
NOW_CODE_NOT_FOUND 0x0004	Resource not found.
NOW_CODE_ACCESS_DENIED 0x0005	Resource can't be accessed.
NOW_CODE_INTERNAL 0x0006	Internal error.
NOW_CODE_NOT_IMPLEMENTED 0x0007	Operation is not implemented on current platform.

    - `NOW_EXEC_RESULT_ERROR_KIND_WINAPI`: code contains standard WinAPI error.
    - `NOW_EXEC_RESULT_ERROR_KIND_UNIX`: code contains standard UNIX error code.

errorMessage(variable, optional): this value contains optional error message if `NOW_EXEC_RESULT_ERROR_MESSAGE` flag is set

Negotiation Messages

NOW_NEGOTIATION_MSG

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1		
msgSize		
msgClass	msgType	msgFlags

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_NEGOTIATION_MSG_CLASS_ID).

msgType (1 byte): The message type.

Value	Meaning
NOW_NEGOTIATION_CAPSET_MSG_ID 0x01	NOW_NEGOTIATION_CAPSET_MSG

NOW_NEGOTIATION_CAPSET_MSG

This message is first set by the server side, to advertise capabilities.

Received server message should be downgraded by the client (remove non-intersecting capabilities) and sent back to the server at the start of DVC channel communications. DVC channel should be closed if protocol versions are not compatible.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1	
msgSize	
msgClass	msgType / msgFlags
versionMajor	versionMinor
systemCapset	
sessionCapset	
execCapset	
heartbeatInterval(optional)	

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_NEGOTIATION_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_NEGOTIATION_CAPSET_MSG_ID).

msgFlags (2 bytes): Message flags.

Flag	Meaning
NOW_NEGOTIATION_SET_HEATBEAT 0x0001	`heartbeat` field is present.

versionMajor (1 byte): Major protocol version. Breaking changes in protocol should increment major version; Protocol implementations with different major version are not compatible.

versionMinor (1 byte): Minor protocol version. Incremented when new non-breaking feature is added.

systemCapset (4 bytes): System commands capabilities set.

Flag	Meaning
NOW_CAP_SYSTEM_SHUTDOWN 0x0001	System shutdown command support.

sessionCapset (4 bytes): Session commands capabilities set.

Flag	Meaning
NOW_CAP_SESSION_LOCK 0x00000001	Lock command support.
NOW_CAP_SESSION_LOGOFF 0x00000002	Logoff command support.
NOW_CAP_SESSION_MSGBOX 0x00000004	Message box command support.

execCapset (4 bytes): Remote execution capabilities set.

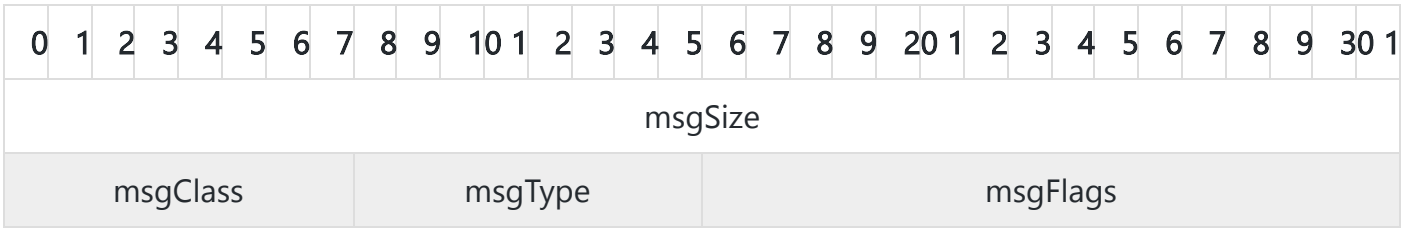
Flag	Meaning
NOW_CAP_EXEC_STYLE_RUN 0x00000001	Generic "Run" execution style.
NOW_CAP_EXEC_STYLE_PROCESS 0x00000002	CreateProcess() execution style.

Flag	Meaning
NOW_CAP_EXEC_STYLE_SHELL 0x00000004	System shell (.sh) execution style.
NOW_CAP_EXEC_STYLE_BATCH 0x00000008	Windows batch file (.bat) execution style.
NOW_CAP_EXEC_STYLE_WINPS 0x00000010	Windows PowerShell (.ps1) execution style.
NOW_CAP_EXEC_STYLE_PWSH 0x00000020	PowerShell 7 (.ps1) execution style.

heartbeatInterval (4 bytes, optional): A 32-bit unsigned integer, which represents periodic heartbeat interval *hint* for a server (60 seconds by default). Disables periodic heartbeat if set to `0`.

System Messages

NOW_SYSTEM_MSG



msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_SYSTEM_MSG_CLASS_ID).

msgType (1 byte): The message type.

Value	Meaning
NOW_SYSTEM_INFO_REQ_ID 0x01	NOW_SYSTEM_INFO_REQ_MSG
NOW_SYSTEM_INFO_RSP_ID 0x02	NOW_SYSTEM_INFO_RSP_MSG
NOW_SYSTEM_SHUTDOWN_ID 0x03	NOW_SYSTEM_SHUTDOWN_MSG

NOW_SYSTEM_SHUTDOWN_MSG

The NOW_SYSTEM_SHUTDOWN_MSG structure is used to request a system shutdown.NOW_SESSION_LOGOFF_MSG

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1		
msgSize		
msgClass	msgType	msgFlags
timeout		
message		

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_SYSTEM_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_SYSTEM_SHUTDOWN_MSG_ID)

msgFlags (2 bytes): The message flags.

Flag	Meaning
NOW_SHUTDOWN_FLAG_FORCE 0x0001	Force shutdown
NOW_SHUTDOWN_FLAG_REBOOT 0x0002	Reboot after shutdown

timeout (4 bytes): This system shutdown timeout, in seconds.

message (variable): A NOW_STRING structure containing an optional shutdown message.

Session Messages

NOW_SESSION_MSG

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1		
msgSize		
msgClass	msgType	msgFlags

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_SESSION_MSG_CLASS_ID).

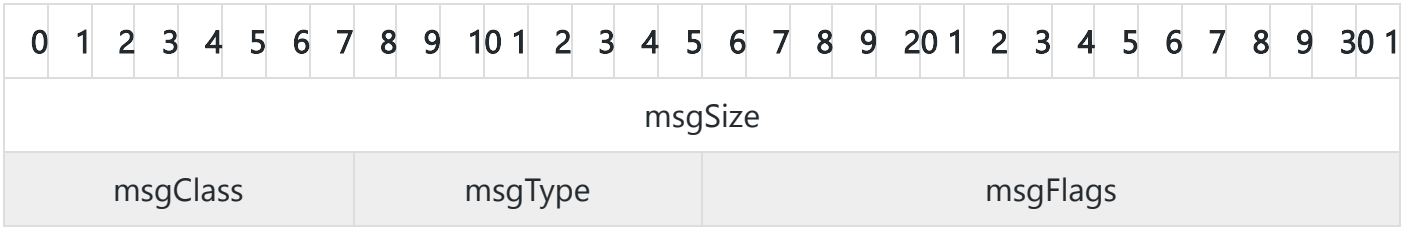
msgType (1 byte): The message type.

Value	Meaning
NOW_SESSION_LOCK_MSG_ID 0x01	NOW_SESSION_LOCK_MSG
NOW_SESSION_LOGOFF_MSG_ID 0x02	NOW_SESSION_LOGOFF_MSG
NOW_SESSION_MESSAGE_BOX_MSG_REQ_ID 0x03	NOW_SESSION_MESSAGE_BOX_MSG
NOW_SESSION_MESSAGE_BOX_RSP_MSG_ID 0x04	NOW_SESSION_MESSAGE_RSP_MSG

msgFlags (2 bytes): The message flags.

NOW_SESSION_LOCK_MSG

The NOW_SESSION_LOCK_MSG is used to request locking the user session.



msgSize (4 bytes): The message size, excluding the header size (8 bytes).

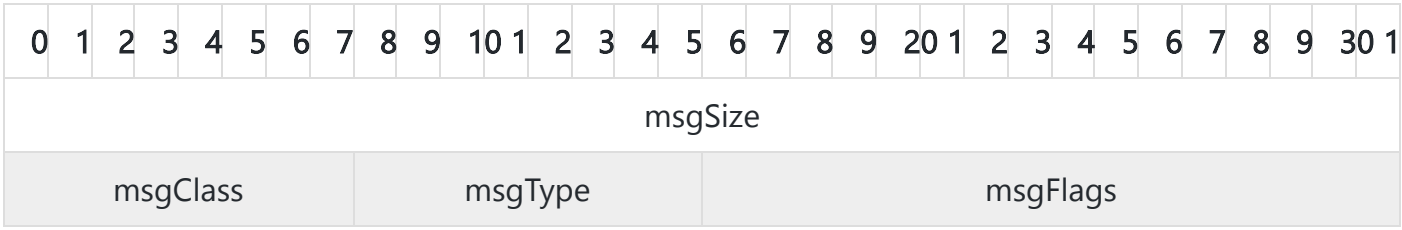
msgClass (1 byte): The message class (NOW_SESSION_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_SESSION_LOCK_MSG_ID).

msgFlags (2 bytes): The message flags.

NOW_SESSION_LOGOFF_MSG

The NOW_SESSION_LOGOFF_MSG is used to request a user session logoff.



msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_SESSION_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_SESSION_LOGOFF_MSG_ID).

msgFlags (2 bytes): The message flags.

NOW_SESSION_MSGBOX_REQ_MSG

The NOW_SESSION_MSGBOX_REQ_MSG is used to show a message box in the user session, similar to what the WTSSendMessage function does.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
msgSize
msgClass | msgType | msgFlags
requestId
style
timeout
text (variable)
title (variable, optional)

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_SESSION_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_SESSION_MESSAGE_BOX_MSG_ID).

msgFlags (2 bytes): The message flags.

Flag	Meaning
NOW_MSGBOX_FLAG_TITLE 0x00000001	Set if `title` field is present
NOW_MSGBOX_FLAG_STYLE 0x00000002	The style field contains a non-default value
NOW_MSGBOX_FLAG_TIMEOUT 0x00000004	The timeout field contains a non-default value
NOW_MSGBOX_FLAG_RESPONSE 0x00000008	A response message is expected (don't fire and forget)

requestId (4 bytes): the message request id, sent back in the response.

style (4 bytes): The message box style, ignored if NOW_MSGBOX_FLAG_STYLE is not set. MBOK is the default, refer to the MessageBox function for all possible styles. This field may be ignored on platforms other than Windows.

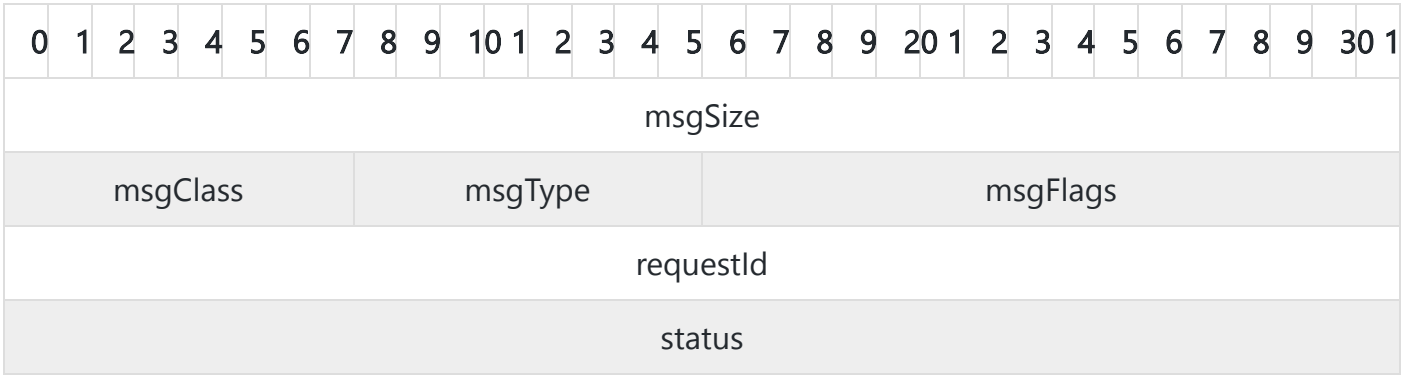
timeout (4 bytes): The timeout, in seconds, that the message box dialog should wait for the user response. This value is ignored if NOW_MSGBOX_FLAG_TIMEOUT is not set.

text (variable): The message box text.

title (variable, optional): The message box title.

NOW_SESSION_MSGBOX_RSP_MSG

The NOW_SESSION_MSGBOX_RSP_MSG is a message sent in response to NOW_SESSION_MSGBOX_REQ_MSG if the NOW_MSGBOX_FLAG_RESPONSE has been set, and contains the result from the message box dialog.



msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_SESSION_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_SESSION_MESSAGE_RSP_MSG_ID).

msgFlags (2 bytes): The message flags.

requestId (4 bytes): The corresponding message box request id.

status (4 bytes): `NOW_STATUS` structure containing message box request status. `status.code` contains message box response code, defined as following:

Value	Meaning
IDABORT 3	Abort

Value	Meaning
IDCANCEL 2	Cancel
IDCONTINUE 11	Continue
IDIGNORE 5	Ignore
IDNO 7	No
IDOK 1	OK
IDRETRY 4	Retry
IDTRYAGAIN 10	Try Again
IDYES 6	Yes
IDTIMEOUT 32000	Timeout

Execution Messages

NOW_EXEC_MSG

The NOW_EXEC_MSG message is used to execute remote commands or scripts.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1		
msgSize		
msgClass	msgType	msgFlags

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type.

Value	Meaning
NOW_EXEC_CAPSET_MSG_ID 0x00	NOW_EXEC_CAPSET_MSG
NOW_EXEC_ABORT_MSG_ID 0x01	NOW_EXEC_ABORT_MSG
NOW_EXEC_CANCEL_REQ_MSG_ID 0x02	NOW_EXEC_CANCEL_REQ_MSG
NOW_EXEC_CANCEL_RSP_MSG_ID 0x03	NOW_EXEC_CANCEL_RSP_MSG
NOW_EXEC_RESULT_MSG_ID 0x04	NOW_EXEC_RESULT_MSG
NOW_EXEC_DATA_MSG_ID 0x05	NOW_EXEC_DATA_MSG
NOW_EXEC_RUN_MSG_ID 0x10	NOW_EXEC_RUN_MSG
NOW_EXEC_PROCESS_MSG_ID 0x11	NOW_EXEC_PROCESS_MSG
NOW_EXEC_SHELL_MSG_ID 0x12	NOW_EXEC_SHELL_MSG
NOW_EXEC_BATCH_MSG_ID 0x13	NOW_EXEC_BATCH_MSG
NOW_EXEC_WINPS_MSG_ID 0x14	NOW_EXEC_WINPS_MSG
NOW_EXEC_PWSH_MSG_ID 0x15	NOW_EXEC_PWSH_MSG
NOW_EXEC_HEARTBEAT_MSG_ID 0x20	NOW_EXEC_HEARTBEAT_MSG

msgFlags (2 bytes): The message flags.

NOW_EXEC_ABORT_MSG

The NOW_EXEC_ABORT_MSG message is used to abort a remote execution immediately due to an unrecoverable error. This message can be sent at any time without an explicit response message. The session is considered aborted as soon as this message is sent.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
msgSize
msgClass	msgType	msgFlags
sessionId
exitCode

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_EXEC_ABORT_MSG_ID).

msgFlags (2 bytes): The message flags.

sessionId (4 bytes): A 32-bit unsigned integer containing a unique remote execution session id.

exitCode (4 bytes): Exit code for application abort (Ignored if not supported by OS).

NOW_EXEC_CANCEL_REQ_MSG

The NOW_EXEC_CANCEL_REQ_MSG message is used to cancel a remote execution session.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
msgSize
msgClass	msgType	msgFlags
sessionId

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_EXEC_CANCEL_REQ_MSG_ID).

msgFlags (2 bytes): The message flags.

sessionId (4 bytes): A 32-bit unsigned integer containing a unique remote execution session id.

NOW_EXEC_CANCEL_RSP_MSG

The NOW_EXEC_CANCEL_RSP_MSG message is used to respond to a remote execution cancel request.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
msgSize
msgClass	msgType	msgFlags
sessionId
status

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_EXEC_CANCEL_RSP_MSG_ID).

msgFlags (2 bytes): The message flags.

sessionId (4 bytes): A 32-bit unsigned integer containing a unique remote execution session id.

status (4 bytes): `NOW_STATUS` structure containing message box request status. `status.code` should be set to 0.

NOW_EXEC_RESULT_MSG

The NOW_EXEC_RESULT_MSG message is used to return the result of an execution request. The session is considered terminated as soon as this message is sent.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
msgSize
msgClass	msgType	msgFlags
sessionId
status (variable)

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_EXEC_RESULT_MSG_ID).

msgFlags (2 bytes): The message flags.

sessionId (4 bytes): A 32-bit unsigned integer containing a unique remote execution session id.

status (variable): `NOW_STATUS` structure containing session execution result. `status.code` contains process exit code on success.

NOW_EXEC_DATA_MSG

The NOW_EXEC_DATA_MSG message is used to send input/output data as part of a remote execution.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1		
msgSize		
msgClass	msgType	msgFlags
sessionId		
data (variable)		

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_EXEC_DATA_MSG_ID).

msgFlags (2 bytes): The message flags.

Flag	Meaning
NOW_EXEC_FLAG_DATA_FIRST 0x00000001	This is the first data message.
NOW_EXEC_FLAG_DATA_LAST 0x00000002	This is the last data message, the command completed execution.
NOW_EXEC_FLAG_DATA_STDIN 0x00000004	The data is from the standard input.
NOW_EXEC_FLAG_DATA_STDOUT 0x00000008	The data is from the standard output.
NOW_EXEC_FLAG_DATA_STDERR 0x00000010	The data is from the standard error.

Message should contain exactly one of `NOW_EXEC_FLAG_DATA_STDIN`, `NOW_EXEC_FLAG_DATA_STDOUT` or `NOW_EXEC_FLAG_DATA_STDERR` flags set.

First stream message should always contain `NOW_EXEC_FLAG_DATA_FIRST` flag.

`NOW_EXEC_FLAG_DATA_LAST` should indicate EOF for a stream, all consecutive messages for the given stream will be ignored by either party (client or sever).

sessionId (4 bytes): A 32-bit unsigned integer containing a unique remote execution session id.

data (variable): The input/output data represented as `NOW_VARBUF`

NOW_EXEC_RUN_MSG

The NOW_EXEC_RUN_MSG message is used to send a run request. This request type maps to starting a program by using the "Run" menu on operating systems (the Start Menu on Windows, the Dock on macOS etc.). The execution of programs started with NOW_EXEC_RUN_MSG is not followed and does not send back the output.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1		
msgSize		
msgClass	msgType	msgFlags
sessionId		
command (variable)		

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_EXEC_RUN_MSG_ID).

msgFlags (2 bytes): The message flags.

sessionId (4 bytes): A 32-bit unsigned integer containing a unique remote execution session id.

command (variable): A NOW_VARSTR structure containing the command to execute.

NOW_EXEC_PROCESS_MSG

The NOW_EXEC_PROCESS_MSG message is used to send a Windows CreateProcess() request.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1		
msgSize		
msgClass	msgType	msgFlags
sessionId		
filename (variable)		

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
parameters (variable, optional)
directory (variable, optional)

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_EXEC_PROCESS_MSG_ID).

msgFlags (2 bytes): The message flags.

Flag	Meaning
NOW_EXEC_FLAG_PROCESS_PARAMETERS_SET 0x00000001	Message contains `parameters` field if set
NOW_EXEC_FLAG_PROCESS_DIRECTORY_SET 0x00000002	Message contains `directory` field if set

sessionId (4 bytes): A 32-bit unsigned integer containing a unique remote execution session id.

filename (variable): A NOW_VARSTR structure containing the file name. Corresponds to the lpApplicationName parameter.

parameters (variable, optional): A NOW_VARSTR structure containing the command parameters. Corresponds to the lpCommandLine parameter.

directory (variable, optional): A NOW_VARSTR structure containing the command working directory. Corresponds to the lpCurrentDirectory parameter.

NOW_EXEC_SHELL_MSG

The NOW_EXEC_SHELL_MSG message is used to execute a remote shell script.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1		
msgSize		
msgClass	msgType	msgFlags
sessionId		
command (variable)		
shell (variable, optional)		

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
directory (variable, optional)

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_EXEC_SHELL_MSG_ID).

msgFlags (2 bytes): The message flags.

Flag	Meaning
NOW_EXEC_FLAG_SHELL_SHELL_SET 0x00000001	Message contains `shell` field if set
NOW_EXEC_FLAG_SHELL_DIRECTORY_SET 0x00000002	Message contains `directory` field if set

sessionId (4 bytes): A 32-bit unsigned integer containing a unique remote execution session id.

command (variable): A NOW_VARSTR structure containing the script file contents to execute.

shell (variable, optional): A NOW_VARSTR structure containing the shell to use for execution. If no shell is specified, the default system shell (/bin/sh) will be used.

directory (variable, optional): A NOW_VARSTR structure containing the command working directory.

NOW_EXEC_BATCH_MSG

The NOW_EXEC_BATCH_MSG message is used to execute a remote batch script.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1		
msgSize		
msgClass	msgType	msgFlags
sessionId		
command (variable)		
directory (variable, optional)		

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_EXEC_BATCH_MSG_ID).

msgFlags (2 bytes): The message flags.

Flag	Meaning
NOW_EXEC_FLAG_BATCH_DIRECTORY_SET 0x00000002	Message contains `directory` field if set

sessionId (4 bytes): A 32-bit unsigned integer containing a unique remote execution session id.

command (variable): A NOW_VARSTR structure containing the script file contents to execute.

directory (variable, optional): A NOW_VARSTR structure containing the command working directory.

NOW_EXEC_WINPS_MSG

The NOW_EXEC_WINPS_MSG message is used to execute a remote Windows PowerShell (powershell.exe) command.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1		
msgSize		
msgClass	msgType	msgFlags
sessionId		
command (variable)		
executionPolicy (variable, optional)		
configurationName (variable, optional)		

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_EXEC_WINPS_MSG_ID).

msgFlags (2 bytes): The message flags, specifying the PowerShell command-line arguments.

Flag	Meaning
NOW_EXEC_FLAG_PS_NO_LOGO 0x00000001	PowerShell -NoLogo option
NOW_EXEC_FLAG_PS_NO_EXIT 0x00000002	PowerShell -NoExit option
NOW_EXEC_FLAG_PS_STA 0x00000004	PowerShell -Sta option
NOW_EXEC_FLAG_PS_MTA 0x00000008	PowerShell -Mta option
NOW_EXEC_FLAG_PS_NO_PROFILE 0x00000010	PowerShell -NoProfile option
NOW_EXEC_FLAG_PS_NON_INTERACTIVE 0x00000020	PowerShell -NonInteractive option
NOW_EXEC_FLAG_PS_EXECUTION_POLICY 0x00000040	`executionPolicy` field is set and specifies the PowerShell -ExecutionPolicy parameter
NOW_EXEC_FLAG_PS_CONFIGURATION_NAME 0x00000080	`configurationName` field is set and specifies the PowerShell -ConfigurationName parameter

sessionId (4 bytes): A 32-bit unsigned integer containing a unique remote execution session id.

command (variable): A NOW_VARSTR structure containing the command to execute.

executionPolicy (variable, optional): A NOW_VARSTR structure containing the execution policy (-ExecutionPolicy) parameter value.

configurationName (variable, optional): A NOW_VARSTR structure containing the configuration name (-ConfigurationName) parameter value.

NOW_EXEC_PWSH_MSG

The NOW_EXEC_PWSH_MSG message is used to execute a remote PowerShell 7 (pwsh) command.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1
sessionId
command (variable)
executionPolicy (variable, optional)
configurationName (variable, optional)

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_EXEC_PWSH_MSG_ID).

msgFlags (2 bytes): The message flags, specifying the PowerShell command-line arguments, same as with NOW_EXEC_WINPS_MSG.

sessionId (4 bytes): A 32-bit unsigned integer containing a unique remote execution session id.

command (variable): A NOW_VARSTR structure containing the command to execute.

executionPolicy (variable, optional): A NOW_VARSTR structure, same as with NOW_EXEC_WINPS_MSG.

configurationName (variable, optional): A NOW_VARSTR structure, same as with NOW_EXEC_WINPS_MSG.

NOW_EXEC_HEARTBEAT_MSG

The NOW_EXEC_HEARTBEAT_MSG message is sent immediately after execution session has started and then is sent periodically on intervals specified during negotiation phase.

0 1 2 3 4 5 6 7 8 9 10 1 2 3 4 5 6 7 8 9 20 1 2 3 4 5 6 7 8 9 30 1		
msgSize		
msgClass	msgType	msgFlags
sessionId		

msgSize (4 bytes): The message size, excluding the header size (8 bytes).

msgClass (1 byte): The message class (NOW_EXEC_MSG_CLASS_ID).

msgType (1 byte): The message type (NOW_EXEC_HEARTBEAT_MSG_ID).

msgFlags (2 bytes): The message flags.

sessionId (4 bytes): A 32-bit unsigned integer containing a unique remote execution session id.

Version History

- 1.0
    - Initial protocol version