[MS-SMB2]: Server Message Block (SMB) Protocol Versions 2 and 3

This topic lists the Errata found in [MS-SMB2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V53.0 – 2017/09/15.

Errata Published*	Description
2017/11/27	In Section 3.3.5.20.3, Handling SMB2_0_INFO_SECURITY, the following paragraph was changed from: If the OutputBufferLength given in the client request is either zero or is insufficient to hold the information requested, the server MUST fail the request with STATUS_BUFFER_TOO_SMALL. If Connection.Dialect is "3.1.1", the server MUST return error data containing the buffer size, in bytes, that would be required to return the requested information, as specified in section 2.2.2, with ByteCount set to 12, ErrorContextCount set to 1, and ErrorData set to SMB2 ERROR Context response with ErrorDataLength set to 4, ErrorId set to 0, and ErrorContextData is set to the buffer size, in bytes, indicating the minimum required buffer length; otherwise, the server MUST return error data with ByteCount set to 2 and ErrorData set to a 4-byte value indicating the minimum required buffer length. The server MUST NOT return STATUS_BUFFER_OVERFLOW with an incomplete security descriptor to the client as in the previous cases. If the underlying object store returns an error, the server MUST fail the request with the error code received. Changed to: If the OutputBufferLength given in the client request is either zero or is insufficient to hold the information requested, the server MUST fail the request with STATUS_BUFFER_TOO_SMALL. If Connection.Dialect is "3.1.1", the server MUST return error data containing the buffer size, in bytes, that would be required to return the requested information, as specified in section 2.2.2, with ByteCount set to 12, ErrorContextCount set to 1, and ErrorData set to SMB2 ERROR Context response with ErrorDataLength set to 4, ErrorId set to 0, and ErrorContextData is set to the buffer size, in bytes, indicating the minimum required buffer length; otherwise, the server MUST return error data with ByteCount set to 24 and ErrorData set to a 4-byte value indicating the minimum required buffer length. The server MUST NOT return STATUS_BUFFER_OVERFLOW with an incomplete security descriptor to the client as in the previous cases. If the underlying object store returns an error, the server MUST fail the request with the error code received.
2017/11/27	In Section 3.3.5.9, Receiving an SMB2 CREATE Request, changed from: … For open requests on a share of type STYPE_DISKTREE (as indicated by TreeConnect.Share.Type), the server MUST do the following: … If CreateOptions includes FILE_NO_INTERMEDIATE_BUFFERING and DesiredAccess includes FILE_APPEND_DATA, the server MUST set FILE_APPEND_DATA to zero in the DesiredAccess field in the request. Changed to:

Errata Published*	Description
	… For open requests on a share of type STYPE_DISKTREE (as indicated by TreeConnect.Share.Type), the server MUST do the following: … If CreateOptions includes FILE_NO_INTERMEDIATE_BUFFERING and DesiredAccess includes FILE_APPEND_DATA, the server MUST set FILE_APPEND_DATA to zero in the DesiredAccess field in the request. The server MUST set the following flags to zero in the CreateOptions field: ● FILE_COMPLETE_IF_OPLOCKED ● FILE_SYNCHRONOUS_IO_ALERT ● FILE_SYNCHRONOUS_IO_NONALERT ● FILE_OPEN_FOR_FREE_SPACE_QUERY
2017/11/27	In Section 3.3.4.7, Object Store Indicates a Lease Break, the following was changed from: If Open.Connection is NULL, the server MUST close the Open as specified in section 3.3.4.17 for the following cases: ● Open.IsResilient is FALSE, Open.IsDurable is FALSE, and Open.IsPersistent is FALSE. ● Lease.BreakToLeaseState does not contain SMB2_LEASE_HANDLE_CACHING and Open.IsDurable is TRUE. Changed to: If Open.Connection is NULL, Open.IsResilient is FALSE and Open.IsPersistent is FALSE, the server MUST close the Open as specified in section 3.3.4.17 for the following cases: ● Open.IsDurable is FALSE. ● Lease.BreakToLeaseState does not contain SMB2_LEASE_HANDLE_CACHING and Open.IsDurable is TRUE.
2017/10/30	In Section 3.3.5.2.9, Verifying the Session, the last paragraph has been changed from: If Connection.Dialect belongs to the SMB 3.x dialect family, Session.EncryptData is TRUE, and RejectUnencryptedAccess is TRUE, the server MUST locate the Request in Connection.RequestList for which Request.MessageId matches the MessageId value in the SMB2 header of the request. If Request.IsEncrypted is FALSE, the server MUST fail the request with STATUS_ACCESS_DENIED. Changed to: If Connection.Dialect belongs to the SMB 3.x dialect family, and Session.EncryptData is TRUE, the server MUST locate the Request in Connection.RequestList for which Request.MessageId matches the MessageId value in the SMB2 header of the request. If Request.IsEncrypted is FALSE, the server MUST fail the request with STATUS_ACCESS_DENIED. In Section 3.3.5.2.11, Verifying the Tree Connect, the following has been changed from:

Errata Published*	Description
	If the server implements the SMB 3.x dialect family, it MUST return STATUS_ACCESS_DENIED for the following cases: ● If TreeConnect.Share.EncryptData is TRUE, RejectUnencryptedAccess is TRUE, and Request.IsEncrypted is FALSE. ● If EncryptData is TRUE, RejectUnencryptedAccess is TRUE, and Request.IsEncrypted is FALSE. If the server implements the SMB 3.x dialect family, EncryptData or TreeConnect.Share.EncryptData or Request.IsEncrypted is TRUE, RejectUnencryptedAccess is TRUE, and Connection.ServerCapabilities does not include SMB2_GLOBAL_CAP_ENCRYPTION, the server MUST fail the request with STATUS_ACCESS_DENIED. Changed to: If Connection.Dialect belongs to the SMB 3.x dialect family, it MUST return STATUS_ACCESS_DENIED for the following cases: ● If TreeConnect.Share.EncryptData is TRUE, and Request.IsEncrypted is FALSE. ● If EncryptData is TRUE, and Request.IsEncrypted is FALSE. If Connection.Dialect belongs to the SMB 3.x dialect family, EncryptData or TreeConnect.Share.EncryptData or Request.IsEncrypted is TRUE, and Connection.ServerCapabilities does not include SMB2_GLOBAL_CAP_ENCRYPTION, the server MUST fail the request with STATUS_ACCESS_DENIED.
2017/10/02	In Section 3.3.5.17, Receiving an SMB2 ECHO Request, changed from: … If Connection.SessionTable is empty, the server SHOULD<343> disconnect the connection. The server MUST construct an SMB2 ECHO Response following the syntax specified in section 2.2.29 and MUST send it to the client. … Changed to: … If Connection.SessionTable is empty, the server SHOULD<343> disconnect the connection. The server MUST verify the session, as specified in section 3.3.5.2.9, if any of the following conditions is TRUE: ▪ SMB2_FLAGS_SIGNED bit is set in the Flags field of the SMB2 header of the request. ▪ The request is not encrypted, and the SessionId field of the SMB2 header of the request is not zero. The server MUST construct an SMB2 ECHO Response following the syntax specified in section 2.2.29 and MUST send it to the client. …

*Date format: YYYY/MM/DD