[MS-FASP]: Firewall and Advanced Security Protocol

This topic lists the Errata found in the MS-FASP document 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 V27.0 – 2018/09/12.

Errata Published*	**Description**
2019/02/19	In Section 2.2.36, FW_RULE, several field names and values have been corrected. Changed from: ...and Direction MUST be FW_DIRECTION_IN. Changed to: ...and Direction MUST be FW_DIR_IN. Changed from: ...LocalPorts MUST be 0 if the Direction is FW_DIRECTION_OUT. Changed to: ...LocalPorts MUST be 0 if the Direction is FW_DIR_OUT. Changed from: ...or the FW_RULE_FLAGS_AUTHENTICATE_WITH_ENCRYPT flag MUST be set on the wFlags field. Changed to: ...or the FW_RULE_FLAGS_AUTHENTICATE_WITH_ENCRYPTION flag MUST be set on the wFlags field. In Section 2.2.50, FW_CS_RULE_FLAGS, several enumeration flag value names and description titles have been changed. Changed from: ...FW_CS_RULE_TUNNEL_BYPASS_IF_ENCRYPTED = 0x08, FW_CS_RULE_OUTBOUND_CLEAR = 0x10 Changed to: ...FW_CS_RULE_FLAGS_TUNNEL_BYPASS_IF_ENCRYPTED = 0x08, FW_CS_RULE_FLAGS_OUTBOUND_CLEAR = 0x10 Changed from: ... FW_CS_RULE_TUNNEL_BYPASS_IF_ENCRYPTED: This flag MUST only be set on tunnel mode rules. If this flag is set and traffic is already arriving encrypted, it is exempted from the tunnel.

Errata Published*	Description
	FW_CS_RULE_OUTBOUND_CLEAR: This flag MUST only be set on tunnel mode rules. If set, when outbound traffic matches the rule, it leaves unprotected, but inbound traffic MUST arrive through the tunnel. Changed to: ...FW_CS_RULE_FLAGS_TUNNEL_BYPASS_IF_ENCRYPTED: This flag MUST only be set on tunnel mode rules. If this flag is set and traffic is already arriving encrypted, it is exempted from the tunnel. FW_CS_RULE_FLAGS_OUTBOUND_CLEAR: This flag MUST only be set on tunnel mode rules. If set, when outbound traffic matches the rule, it leaves unprotected, but inbound traffic MUST arrive through the tunnel. In Section 2.2.60, FW_AUTH_SUITE_FLAGS, an enumeration flag value name and description title have been changed. Changed from: ...W_AUTH_SUITE_FLAGS_ALLOW_PROXY Changed to: ...FW_AUTH_SUITE_FLAGS_ALLOW_PROXY In Section 2.2.63, FW_AUTH_SET2_10, several flag names have been corrected. Changed from: All such contiguous suites that have a specific signing flag (either none, ECDSA256, or ECDSA384) MUST have the same value for the FW_AUTH_SUITE_FLAG_HEALTH_CERT flag. It MUST be set either in all or in none. Changed to: All such contiguous suites that have a specific signing flag (either none, ECDSA256, or ECDSA384) MUST have the same value for the FW_AUTH_SUITE_FLAGS_HEALTH_CERT flag. It MUST be set either in all or in none. Changed from: If the set has a machine certificate suite that has a wFlag that contains the flag FW_AUTH_SUITE_FLAGS_HEALTH_CERT, all machine certificate method suites in the set MUST also have this flag. Changed to: If the set has a machine certificate suite that has a wFlags field that contains the flag FW_AUTH_SUITE_FLAGS_HEALTH_CERT, all machine certificate method suites in the set MUST also have this flag. In Section 2.2.64, FW_AUTH_SET, several flag names have been corrected. Changed from: All such contiguous suites that have a specific signing flag (either none, ECDSA256, or ECDSA384) MUST have the same value for the FW_AUTH_SUITE_FLAG_HEALTH_CERT flag. Changed to:

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>All such contiguous suites that have a specific signing flag (either none, ECDSA256, or ECDSA384) MUST have the same value for the FW_AUTH_SUITE_FLAGS_HEALTH_CERT flag.
Changed from:
If the set has a machine certificate suite that has a wFlag that contains the flag FW_AUTH_SUITE_FLAGS_HEALTH_CERT, all machine certificate method suites in the set MUST also have this flag.
Changed to:
If the set has a machine certificate suite that has a wFlags field that contains the flag FW_AUTH_SUITE_FLAGS_HEALTH_CERT, all machine certificate method suites in the set MUST also have this flag.
In Section 2.2.73, FW_CRYPTO_SET, an extra space in the name FW_CRYPTO _HASH_SHA256 has been removed.
Changed from:
All Phase1 suites MUST NOT have a Hash field that has the FW_CRYPTO_HASH_NONE value and MUST have either MD5 (FW_CRYPTO_HASH_MD5) or SHA (FW_CRYPTO_HASH_SHA1, FW_CRYPTO _HASH_SHA256, FW_CRYPTO_HASH_SHA384) valid values.
Changed to:
All Phase1 suites MUST NOT have a Hash field that has the FW_CRYPTO_HASH_NONE value and MUST have either MD5 (FW_CRYPTO_HASH_MD5) or SHA (FW_CRYPTO_HASH_SHA1, FW_CRYPTO_HASH_SHA256, FW_CRYPTO_HASH_SHA384) valid values.
In Section 2.2.90, FW_QUERY_CONDITION, changed from:
If the matchType field is equal to FW_MATH_TYPE_EQUAL, the matchKey field MUST be either FW_MATCH_KEY_GROUP or FW_MATCH_KEY_DIRECTION.
Changed to:
If the matchType field is equal to FW_MATCH_TYPE_EQUAL, the matchKey field MUST be either FW_MATCH_KEY_GROUP or FW_MATCH_KEY_DIRECTION.
In Section 3.1.4.12, RRPC_FWSetConfig (Opnum 11), changed from:
The caller wants to set a LOG_MAX_FILE_SIZE that is not within the valid values [min, max]."
Changed to:
The caller wants to set a FW_PROFILE_CONFIG_LOG_MAX_FILE_SIZE that is not within the valid values [min, max].
Changed from:
The LOG_FILE_PATH configuration value contains the following invalid characters: /,*,?,",<,>,|.
Changed to:</td></tr>
</table>

Errata Published*	**Description**
	The FW_PROFILE_CONFIG_LOG_FILE_PATH configuration value contains the following invalid characters: /,*,?,",<,>,|. In the following sections, the string name “wszSetID” has been changed to “wszSetId”: 3.1.4.19 RRPC_FWSetAuthenticationSet (Opnum 18) 3.1.4.20 RRPC_FWDeleteAuthenticationSet (Opnum 19) 3.1.4.21 RRPC_FWDeleteAllAuthenticationSets (Opnum 20) 3.1.4.24 RRPC_FWSetCryptoSet (Opnum 23) 3.1.4.25 RRPC_FWDeleteCryptoSet (Opnum 24) 3.1.4.54 RRPC_FWSetAuthenticationSet2_10 (Opnum 53) 3.1.4.57 RRPC_FWSetCryptoSet2_10 (Opnum 56) 3.1.4.64 RRPC_FWSetAuthenticationSet2_20 (Opnum 63) In Section 4.3, Enumerating the Firewall Rules, a parameter has been changed. Changed from: [in] WORD wFlag = 0 Changed to: [in] WORD wFlags = 0

*Date format: YYYY/MM/DD