

Windows Protocols Errata

This topic lists the Errata found in the Windows Protocols Technical Specifications, Overview Documents, and Reference documents since they were 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.

Errata are content issues in published versions of protocols documents that could impact an **implementation**. Examples of errata are errors or missing information in the normative sections of the Technical Specifications or in the use cases (examples) in the Technical Specifications and Overview Documents.

Content issues that don't impact an implementation, for example, editorial updates due to typos, formatting updates, and rewrites for readability and clarity, are **not** included in Errata.

The sections below list the Windows Protocols documents that contain active Errata (i.e., Errata not yet released with the documents on MSDN) and provide links to archived Errata (i.e., Errata already released with the documents on MSDN).

Protocols Documents with Active Errata

[\[MC-DTCXA\]: MSDTC Connection Manager OleTx XA Protocol](#)

[\[MS-ADA2\]: Active Directory Schema Attributes M](#)

[\[MS-ADA3\]: Active Directory Schema Attributes N-Z](#)

[\[MS-ADTS\]: Active Directory Technical Specification](#)

[\[MS-CFB\]: Compound File Binary File Format](#)

[\[MS-CIFS\]: Common Internet File System \(CIFS\) Protocol](#)

[\[MS-CMRP\]: Failover Cluster: Management API \(ClusAPI\) Protocol](#)

[\[MS-COMA\]: Component Object Model Plus \(COMplus\) Remote Administration Protocol](#)

[\[MS-CSSP\]: Credential Security Support Provider \(CredSSP\) Protocol](#)

[\[MS-DFSC\]: Distributed File System \(DFS\) Referral Protocol](#)

[\[MS-DHCPM\]: Microsoft Dynamic Host Configuration Protocol \(DHCP\) Server Management Protocol](#)

[\[MS-DNSP\]: Domain Name Service \(DNS\) Server Management Protocol](#)

[\[MS-DPWSSN\]: Devices Profile for Web Services \(DPWS\) Size Negotiation Extension](#)

[\[MS-DRSR\]: Directory Replication Service \(DRS\) Remote Protocol](#)

[\[MS-DTYP\]: Windows Data Types](#)

[\[MS-ECS\]: Enterprise Client Synchronization Protocol](#)

[\[MS-ERREF\]: Windows Error Codes](#)

[\[MS-FSA\]: File System Algorithms](#)

[\[MS-FSCC\]: File System Control Codes](#)

[\[MS-FSRVP\]: File Server Remote VSS Protocol](#)

[\[MS-GPOL\]: Group Policy: Core Protocol](#)

[\[MS-GSSA\]: Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS \(GSS-TSIG\) Protocol Extension](#)

[\[MS-HVRS\]: Hyper-V Remote Storage Profile](#)

[\[MS-IPAMM2\]: IP Address Management \(IPAM\) Management Protocol Version 2](#)

[\[MS-IRP\]: Internet Information Services \(IIS\) Inetinfo Remote Protocol](#)

[\[MS-LSAT\]: Local Security Authority \(Translation Methods\) Remote](#)

[\[MS-MWBF\]: Microsoft Web Browser Federated Sign-On Protocol](#)

[\[MS-NCT\]: Network Cost Transfer Protocol](#)

[\[MS-NFPB\]: Near Field Proximity Bidirectional Services Protocol](#)

[\[MS-NFPS\]: Near Field Proximity Sharing Protocol](#)

[\[MS-NKPU\]: Network Key Protector Unlock Protocol](#)

[\[MS-NNS\]: .NET NegotiateStream Protocol](#)

[\[MS-OAPX\]: OAuth 2.0 Protocol Extensions](#)

[\[MS-OTPCE\]: One-Time Password Certificate Enrollment Protocol](#)

[\[MS-RDPBCGR\]: Remote Desktop Protocol: Basic Connectivity and Graphics Remoting](#)

[\[MS-RDPEDYC\]: Remote Desktop Protocol: Dynamic Channel Virtual Channel Extension](#)

[\[MS-RDPEFS\]: Remote Desktop Protocol: File System Virtual Channel Extension](#)

[\[MS-RDPEGFX\]: Remote Desktop Protocol: Graphics Pipeline Extension](#)

[\[MS-RDPEGT\]: Remote Desktop Protocol Geometry Tracking Virtual Channel Protocol Extension](#)

[\[MS-RDPEPC\]: Remote Desktop Protocol: Print Virtual Channel Extension](#)

[\[MS-RDPERP\]: Remote Desktop Protocol: Remote Programs Virtual](#)

[\[MS-RDPESC\]: Remote Desktop Protocol: Smart Card Virtual Channel Extension](#)

[\[MS-RDPEUDP\]: Remote Desktop Protocol: UDP Transport Extension](#)

[\[MS-RDPEVOR\]: Remote Desktop Protocol: Video Optimized Remoting Virtual Channel Extension](#)

[\[MS-RDPRFX\]: Remote Desktop Protocol: RemoteFX Codec Extension](#)

[\[MS-RMPR\]: Rights Management Services \(RMS\): Client-to-Server Protocol](#)

[\[MS-RMSOD\]: Rights Management Services Protocols Overview](#)

[\[MS-RPCE\]: Remote Procedure Call Protocol Extensions](#)

[\[MS-RSMC\]: Remote Session Monitoring and Control Protocol](#)

[\[MS-RSVD\]: Remote Shared Virtual Disk Protocol](#)

[\[MS-SAMR\]: Security Account Manager \(SAM\) Remote Protocol \(Client-to-Server\)](#)

[\[MS-SFMWA\]: Server and File Management Web APIs](#)

[\[MS-SMB\]: Server Message Block \(SMB\) Protocol](#)

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

[\[MS-TDS\]: Tabular Data Stream Protocol](#)

[\[MS-TSGU\]: Terminal Services Gateway Server Protocol](#)

[\[MS-UAMG\]: Update Agent Management Protocol](#)

[\[MS-VHDX\]: Virtual Hard Disk v2 \(VHDX\) File Format](#)

[\[MS-W32T\]: W32Time Remote Protocol](#)

[\[MS-WFDAA\]: Wi-Fi Direct \(WFD\) Application to Application Protocol](#)

[\[MS-WFDPE\]: Wi-Fi Display Protocol Extension](#)

[\[MS-WSDS\]: WS-Enumeration Directory Services Protocol Extensions](#)

[\[MS-WSTEP\]: WS-Trust X.509v3 Token Enrollment Extensions](#)

[\[MS-WSUSAR\]: Windows Server Update Services: Administrative API Remoting Protocol](#)

[\[MS-WSUSSS\]: Windows Update Services: Server-Server Protocol](#)

Errata Archives

March 2, 2016 - [Download](#)

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

September 26, 2016 - [Download](#)

Last date updated: March 6, 2017

[MC-DTCXA]: MSDTC Connection Manager OleTx XA Protocol

This topic lists the Errata found in [MC-DTCXA] 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.

Errata below are for Protocol Document Version [V19.0 – 2016/07/14](#).

Errata Published*	Description
2016/10/10	<p>In Section 2.2.3.2.5, XATMUSER_MTAG_RMOPEN, changed the field definition for lenDSN from:</p> <p>lenDSN (4 bytes): A 32-bit unsigned integer that MUST contain the count of bytes in the DSN string that follows this message. It MUST be less than 3072.<1></p> <p><1> Section 2.2.3.2.5: On Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2, the provided values of the lenDSN field are confirmed to be less than 256.</p> <p>Changed to:</p> <p>lenDSN (4 bytes): A 32-bit unsigned integer that MUST contain the count of bytes in the DSN string that follows this message. The maximum value of this field is 3072, but it MAY<1> be limited to 256.</p> <p><1> Section 2.2.3.2.5: On Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2, the provided values of the lenDSN field are confirmed to be less than 256.</p>

*Date format: YYYY/MM/DD

[MS-ABTP]: Automatic Bluetooth Pairing Protocol

This topic lists the Errata found in [MS-ABTP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-ADA2]: Active Directory Schema Attributes M

This topic lists the Errata found in the MS-ADA2 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V29.0 - 2016/07/14](#).

Errata Published*	Description
2016/08/29	<p>In Section 2.209, Attribute msDS-AllowedDNSSuffixes, changed "forest" to "domain" in the description of the msDS-AllowedDNSSuffixes attribute.</p> <p>Changed from:</p> <p>For a given Active Directory forest, this attribute specifies the list of DNS suffixes (by their fully qualified domain name (FQDN) (1) ([MS-ADTS] section 1.1)) allowed to be used to identify computers that are members of that forest.</p> <p>Changed to:</p> <p>For a given Active Directory domain, this attribute specifies the list of DNS suffixes (by their fully qualified domain name (FQDN) (1) ([MS-ADTS] section 1.1)) allowed to be used to identify computers that are members of that domain.</p>

*Date format: YYYY/MM/DD

[MS-ADA3]: Active Directory Schema Attributes N-Z

This topic lists the Errata found in the MS-ADA3 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.

Errata below are for Protocol Document Version [V21.3 - 2016/07/14](#).

Errata Published*	Description
2017/01/23	<p>In Section 2.207, Attribute rIDUsedPool, the description of the attribute rIDUsedPool was revised to indicate that the attribute is not necessary for Active Directory to function and does not require a format definition beyond that required by the schema.</p> <p>Changed from:</p> <p>This attribute specifies the RID pools that have been used by a DC.</p> <p>Changed to:</p> <p>This attribute specifies the RID pools that have been used by a DC. It is set to zero and never changed. This attribute is not necessary for Active Directory to function. The protocol does not define a format beyond that required by the schema.</p>

*Date format: YYYY/MM/DD

[MS-ADDM]: Active Directory Web Services: Data Model and Common Elements

This topic lists the Errata found in [MS-ADDM] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-ADFSOAL]: Active Directory Federation Services OAuth Authorization Code Lookup Protocol

This topic lists the Errata found in [MS-ADFSOAL] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-ADFSPiP]: Active Directory Federation Services and Proxy Integration Protocol

This topic lists the Errata found in the MS-ADFSPiP 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-ADFSWAP]: Active Directory Federation Service (AD FS) Web Agent Protocol

This topic lists the Errata found in [MS-ADFSWAP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-ADSC]: Active Directory Schema Classes

This topic lists the Errata found in the MS-ADSC 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-ADTS]: Active Directory Technical Specification

This topic lists the Errata found in the MS-ADTS 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V43.0 - 2016/07/14](#).

Errata Published*	Description
2017/01/23	<p>In Section 6.1.5.3, RID Master FSMO Role, updated the value of ulExtendedOp from EXOP_FSMO_RID_REQ_ROLE to EXOP_FSMO_REQ_RID_ALLOC.</p> <p>Changed from:</p> <p>... that DC issues a request for additional RIDs to the domain's RID Master FSMO role owner (see [MS-DRSR] section 4.1.10.4.3, PerformExtendedOpRequestMsg with ulExtendedOp = EXOP_FSMO_RID_REQ_ROLE). The RID Master FSMO role owner responds to the request by retrieving RIDs from the domain's unallocated RID pool and assigns them to the pool of the requesting DC (see [MS-DRSR] section 4.1.10.5.12, ProcessFsmoRoleRequest with ulExtendedOp = EXOP_FSMO_RID_REQ_ROLE).</p> <p>Changed to:</p> <p>... that DC issues a request for additional RIDs to the domain's RID Master FSMO role owner (see [MS-DRSR] section 4.1.10.4.3, PerformExtendedOpRequestMsg with ulExtendedOp = EXOP_FSMO_REQ_RID_ALLOC). The RID Master FSMO role owner responds to the request by retrieving RIDs from the domain's unallocated RID pool and assigns them to the pool of the requesting DC (see [MS-DRSR] section 4.1.10.5.12, ProcessFsmoRoleRequest with ulExtendedOp = EXOP_FSMO_REQ_RID_ALLOC).</p>
2017/01/09	<p>In Section 5.1.1.2, Using SSL/TLS, changed from:</p> <p>If the client establishes the SSL/TLS-protected connection by means of connecting on a protected LDAPS port, then the connection is considered to be immediately authenticated (bound) as the credentials represented by the client certificate. An EXTERNAL bind is not required but is permitted.</p> <p>Changed to:</p> <p>If the client establishes the SSL/TLS-protected connection by means of connecting on a protected LDAPS port, then the connection is considered to be immediately authenticated (bound) as the credentials represented by the client certificate. An EXTERNAL bind is not allowed, and the bind will be rejected with an error.</p>
2016/12/19	<p>The sidCompatibilityVersion attribute has been added to the rootDSE modify operations, with a new section to document the attribute.</p> <p>Section 3.1.1.3.3 rootDSE Modify Operations was modified:</p> <p>Changed from:</p>

Errata Published*	Description																																																																																																																																																																																																						
	<table><tr><td>enableOptionalFeature</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr><tr><td>dumpReferences</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td>X</td><td></td><td></td><td></td><td></td></tr><tr><td>dumpLinks</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td>X</td><td>X</td><td>X</td></tr><tr><td>schemaUpdateIndicesNow</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td>X</td><td>X</td><td>X</td></tr><tr><td>Null</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td>X</td><td>X</td><td>X</td></tr></table> <p>Changed to:</p> <table><tr><td>enableOptionalFeature</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr><tr><td>dumpReferences</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td>X</td><td></td><td></td><td></td><td></td></tr><tr><td>sidCompatibilityVersion</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td></td><td>X</td><td></td><td>X</td><td></td></tr><tr><td>dumpLinks</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td>X</td><td>X</td><td>X</td></tr><tr><td>schemaUpdateIndicesNow</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td>X</td><td>X</td><td>X</td></tr><tr><td>null</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td>X</td><td>X</td><td>X</td></tr></table> <p>New section added:</p> <p>3.1.1.3.3.30 sidCompatibilityVersion</p> <p>The requester must have the "Allocate-Rids" control access right on the domain root of the DC. The requester must have the SE_DEBUG_PRIVILEGE. The DC must be the RID Master FSMO role owner. If any of these constraints are not met, an error is returned.</p> <p>This operation is triggered by setting the attribute to a decimal number that represents the sidCompatibilityVersion. The type of the modification can be an add or replace. Allowed values are "0" and "1". The DC returns an error if the value is not one of the allowed values. This operation updates the value of the rIDAvailablePool attribute on the RID Manager object (section 6.1.5.3). When the caller sets the SID compatibility version to "0", the updated value for the attribute is calculated as follows:</p> <p>updatedValue = 0x3FFFFFFF00000000 (existingValue & 0xFFFFFFFF)</p> <p>When the caller sets the SID compatibility version to "1", the updated value for the attribute is calculated as follows:</p> <p>updatedValue = 0x7FFFFFFF00000000 (existingValue & 0xFFFFFFFF)</p> <p>If updatedValue is less than existingValue, an error is returned. Otherwise, updatedValue replaces existingValue.</p> <p>The following shows an LDIF sample that performs this operation.</p> <pre>dn: changetype: modify add: sidCompatibilityVersion sidCompatibilityVersion: 1 -</pre>	enableOptionalFeature										X	X	X	X	X	X	X	X	dumpReferences												X	X					dumpLinks														X	X	X	X	schemaUpdateIndicesNow														X	X	X	X	Null														X	X	X	X	enableOptionalFeature										X	X	X	X	X	X	X	X	dumpReferences												X	X					sidCompatibilityVersion												X		X		X		dumpLinks														X	X	X	X	schemaUpdateIndicesNow														X	X	X	X	null														X	X	X	X
enableOptionalFeature										X	X	X	X	X	X	X	X																																																																																																																																																																																						
dumpReferences												X	X																																																																																																																																																																																										
dumpLinks														X	X	X	X																																																																																																																																																																																						
schemaUpdateIndicesNow														X	X	X	X																																																																																																																																																																																						
Null														X	X	X	X																																																																																																																																																																																						
enableOptionalFeature										X	X	X	X	X	X	X	X																																																																																																																																																																																						
dumpReferences												X	X																																																																																																																																																																																										
sidCompatibilityVersion												X		X		X																																																																																																																																																																																							
dumpLinks														X	X	X	X																																																																																																																																																																																						
schemaUpdateIndicesNow														X	X	X	X																																																																																																																																																																																						
null														X	X	X	X																																																																																																																																																																																						
2016/12/05	<p>In Section 1.2.1, Normative References, added the following reference:</p> <p>[RFC5952] Kawamura, S., Kawashima, M., "A Recommendation for IPv6 Address Text Representation", RFC 5952, August 2010, https://tools.ietf.org/html/rfc5952.</p>																																																																																																																																																																																																						
2016/12/05	<p>In Section 3.1.1.3.4.6, LDAP Policies, corrected a field name.</p>																																																																																																																																																																																																						

Errata Published*	Description																																																								
	<div>Changed from:</div> <table><tr><th>Policy name</th><th>A</th><th>D, G, J</th><th>M</th><th>R</th><th>U</th><th>X</th></tr><tr><td>...</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>SystemMemoryLimit</td><td></td><td></td><td></td><td></td><td>X</td><td>X</td></tr><tr><td>...</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table> <div>Changed to:</div> <table><tr><th>Policy name</th><th>A</th><th>D, G, J</th><th>M</th><th>R</th><th>U</th><th>X</th></tr><tr><td>...</td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>SystemMemoryLimitPercent</td><td></td><td></td><td></td><td></td><td>X</td><td>X</td></tr><tr><td>...</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>	Policy name	A	D, G, J	M	R	U	X	...							SystemMemoryLimit					X	X	...							Policy name	A	D, G, J	M	R	U	X	...							SystemMemoryLimitPercent					X	X	...						
Policy name	A	D, G, J	M	R	U	X																																																			
...																																																									
SystemMemoryLimit					X	X																																																			
...																																																									
Policy name	A	D, G, J	M	R	U	X																																																			
...																																																									
SystemMemoryLimitPercent					X	X																																																			
...																																																									
2016/08/15	<p>In two sections, added information that applies to the Active Directory implementation of VLV through Windows Server 2012 R2 without [MSKB-3106637] installed, or through Windows Server 2012 with [MSKB-3106637] installed.</p> <p>In Section 1.2.1, Normative References, included the following reference: [MSKB-3106637] Microsoft Corporation, "Incorrect results in LDAP query, domain controller restarts, or user logons are denied in Windows Server 2012 R2", https://support.microsoft.com/en-us/kb/3106637</p> <p>In Section 3.1.1.3.4.1.17, LDAP_CONTROL_VLVREQUEST and LDAP_CONTROL_VLVRESPONSE, included the following note at the end of the section: Active Directory support for VLV is specified in section 3.1.1.3.4.1 (see LDAP_CONTROL_VLVREQUEST and LDAP_CONTROL_VLVRESPONSE). The following information applies to the Active Directory implementation of VLV through Windows Server 2012 R2 without [MSKB-3106637] installed, or through Windows Server 2012 with [MSKB-3106637] installed: If an LDAP search has the LDAP_CONTROL_VLVREQUEST attached, a desired target object is specified using the greaterThanOrEqualTo choice, and the attribute specified in the sort control is of the 2.5.5.11 time syntax (section 3.1.1.2.2.2), a random object is returned, not an object that satisfies the greaterThanOrEqualTo value.</p>																																																								

*Date format: YYYY/MM/DD

[MS-AIPS]: Authenticated Internet Protocol

This topic lists the Errata found in the MS-AIPS 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-APDS]: Authentication Protocol Domain Support

This topic lists the Errata found in the MS-APDS 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-AZOD]: Authorization Protocols Overview

This topic lists the Errata found in the MS-AZOD 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-BKRP]: BackupKey Remote Protocol

This topic lists the Errata found in the MS-BKRP 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-CAPR]: Central Access Policy Identifier (ID) Retrieval Protocol

This topic lists the Errata found in the MS-CAPR 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-CHAP]: Extensible Authentication Protocol Method for Microsoft Challenge Handshake Authentication Protocol (CHAP)

This topic lists the Errata found in the MS-CHAP 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-CFB]: Compound File Binary File Format

This topic lists the Errata found in the MS-CFB 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.

Errata below are for Protocol Document Version [V5.0 - 2016/07/14](#).

Errata Published*	Description
2017/01/23	<p>In Section 2.6.4, Red-Black Tree, a product behavior note was updated to encompass Windows 10 and Windows Server 2016 in addition to earlier products.</p> <p>Changed from:</p> <p>...</p> <ul style="list-style-type: none">• For each UTF-16 code point, convert to uppercase by using the Unicode Default Case Conversion Algorithm, simple case conversion variant (simple case foldings), with the following notes.<2>Compare each uppercased UTF-16 code point binary value. <p><2>...</p> <p>For Windows Vista Windows Server 2008, Windows 7, Windows Server 2008 R2 operating system, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2: The compound file implementation conforms to the Unicode 5.0 Default Case Conversion Algorithm...</p> <p>Changed to:</p> <p>...</p> <ul style="list-style-type: none">• For each UTF-16 code point, convert to uppercase by using the Unicode Default Case Conversion Algorithm, simple case conversion variant (simple case foldings), with the following notes.<2>Compare each uppercased UTF-16 code point binary value. <p><2>...</p> <p>For Windows Vista and later and for Windows Server 2008 and later, the compound file implementation conforms to the Unicode 5.0 Default Case Conversion Algorithm...</p>

*Date format: YYYY/MM/DD

[MS-CIFS]: Common Internet File System (CIFS) Protocol

This topic lists the Errata found in the MS-CIFS 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

Errata below are for Protocol Document Version [V26.0 – 2016/07/14](#).

Errata Published*	Description
2016/09/26	<p>In two sections, clarified ANDX batch processing in terms of carrying forward values and expected returns.</p> <p>In Section 2.2.4.41, SMB_COM_OPEN_ANDX (0x2D), removed the following sentence from the second paragraph: "If the command is successful, the server response MUST include a valid FID. The client MUST supply the FID in subsequent operations on the object."</p> <p>In Section 3.3.5.2.4, Receiving any Batched ("AndX") Request, changed from: When a server receives an AndX Request message, the server MUST process the batched requests sequentially.</p> <p>Changed to: When a server receives an AndX Request message, the server MUST process the batched requests sequentially. For the first operation, the identifiers for the FID, SID, and TID, if any, MUST be taken from the received operation. For every subsequent operation in the current batch, the values used for FID, SID, and TID MUST be either those in first operation or those generated by the previous operation.</p>
2016/09/26	<p>In Section 3.3.5.30, Receiving an SMB_COM_LOCKING_ANDX Request, updated the rules for byte-range locks processing.</p> <p>Changed from: Locking a range of bytes MUST fail with STATUS_LOCK_NOT_GRANTED(ERRDOS/ERRlock) if any subranges or overlapping ranges are locked, even if they are currently locked by the PID requesting the new lock.</p> <p>Changed to: Locking a range of bytes SHOULD<290> fail with STATUS_LOCK_NOT_GRANTED(ERRDOS/ERRlock) if any subranges or overlapping ranges are locked, even if they are currently locked by the PID requesting the new lock.</p> <p><290> Section 3.3.5.30: After failing the lock byte range request with STATUS_LOCK_NOT_GRANTED, if a client attempts to lock the same range of locked bytes, subranges, or overlapping ranges, Windows servers fail the lock request with</p>

Errata Published*	Description
	STATUS_FILE_LOCK_CONFLICT (ERRDOS/ERRlock).

*Date format: YYYY/MM/DD

[MS-CMRP]: Failover Cluster: Management API (ClusAPI) Protocol

This topic lists the Errata found in the MS-CMRP 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V32.0 – 2016/07/14](#).

Errata Published*	Description
2016/11/21	<p>In Section 2.2.3.43, OS_AND_OS_VERSION_INFO, in the bit table, changed the name of the field OS_(variable) to OS (variable) and changed its description from:</p> <p>OS_(variable) (4 bytes): Specifies the location where the null-terminated Unicode operating system string starts. A null-terminated string that represents the operating system version immediately follows the null termination of the operating system string.</p> <p>Changed to:</p> <p>OS (variable): Specifies the location where the null-terminated Unicode operating system string starts. A null-terminated string that represents the operating system version immediately follows the null termination of the operating system string.</p>
2016/09/26	<p>Added a new section to define the HGENERIC_RPC data type:</p> <p>Section 2.2.1.10 HGENERIC_RPC</p> <p>HGENERIC_RPC is an RPC context handle as specified in [MS-RPCE]. It represents the server context for the operations of a client. An HGENERIC_RPC is obtained as specified in section 3.1.4.2.137. ClusAPI Protocol version 2.0 servers do not support this data type.</p> <p>This type is declared as follows:</p> <pre>typedef [context_handle] void* HGENERIC_RPC;</pre>

*Date format: YYYY/MM/DD

[MS-COMA]: Component Object Model Plus (COMplus) Remote Administration Protocol

This topic lists the Errata found in the MS-COMA 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.

Errata below are for Protocol Document Version [V9.0 – 2016/07/14](#).

Errata Published*	Description
2016/12/05	<p>In Section 2.2.2.23, ActivationTypeProperty, corrected the name of a field in a Product Behavior Note.</p> <p>Changed from:</p> <p>Server validation: Servers SHOULD<28> enforce validity constraints.</p> <p><28> Section 2.2.2.23: Windows servers do not enforce constraints on values of type DefaultAuthenticationLevelProperty. Windows clients never pass invalid values of this type.</p> <p>Changed to:</p> <p>Server validation: Servers SHOULD<28> enforce validity constraints.</p> <p><28> Section 2.2.2.23: Windows servers do not enforce constraints on values of type ActivationTypeProperty. Windows clients never pass invalid values of this type.</p>

*Date format: YYYY/MM/DD

[MS-CSRA]: Certificate Services Remote Administration Protocol

This topic lists the Errata found in the MS-CSRA 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-CSSP]: Credential Security Support Provider (CredSSP) Protocol

This topic lists the Errata found in the MS-CSSP 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V13.0 – 2016/07/14](#).

Errata Published*	Description
2017/02/20	<p>In Section 4, Protocol Examples, added a new figure that shows an unencrypted dump of the TSRequest.authInfo structure and the transformed structure.</p> <p>Changed from:</p> <p>...</p> <p>Step 9: The client sends its credentials to the target server that is protected under SPNEGO and TLS encryption.</p> <p>Changed to:</p> <p>...</p> <p>Step 9: The client sends its credentials to the target server that is protected under SPNEGO and TLS encryption. The following figure shows a sample unencrypted dump (ASN.1DER encoded) of the TSRequest.authInfo structure. This is encrypted on the wire.</p> <pre>30 82 01 0f a0 03 02 01-02 a1 82 01 06 04 82 01 0..... 02 30 81 ff a0 1a 04 18-62 00 62 00 62 00 62 00 .0.....b.b.b.b. 62 00 62 00 62 00 62 00-62 00 62 00 62 00 62 00 b.b.b.b.b.b.b.b. a1 81 e0 30 81 dd a0 03-02 01 01 a2 2e 04 2c 4f ...0.....,O 00 4d 00 4e 00 49 00 4b-00 45 00 59 00 20 00 43 .M.N.I.K.E.Y. .C 00 61 00 72 00 64 00 4d-00 61 00 6e 00 20 00 33 .a.r.d.M.a.n. .3 00 78 00 32 00 31 00 20-00 30 00 a3 50 04 4e 6c .x.2.1. .0..P.Nl 00 65 00 2d 00 4d 00 53-00 53 00 6d 00 61 00 72 .e.-.M.S.S.m.a.r 00 74 00 63 00 61 00 72-00 64 00 55 00 73 00 65 .t.c.a.r.d.U.s.e 00 72 00 2d 00 38 00 62-00 64 00 61 00 30 00 31 .r.-.8.b.d.a.0.1 00 39 00 66 00 2d 00 31-00 32 00 36 00 36 00 2d .9.f.-.1.2.6.6.- 00 2d 00 35 00 33 00 32-00 36 00 38 00 a4 54 04 .-5.3.2.6.8..T. 52 4d 00 69 00 63 00 72-00 6f 00 73 00 6f 00 66 RM.i.c.r.o.s.o.f 00 74 00 20 00 42 00 61-00 73 00 65 00 20 00 53 .t. .B.a.s.e. .S 00 6d 00 61 00 72 00 74-00 20 00 43 00 61 00 72 .m.a.r.t. .C.a.r 00 64 00 20 00 43 00 72-00 79 00 70 00 74 00 6f .d. .C.r.y.p.t.o 00 20 00 50 00 72 00 6f-00 76 00 69 00 64 00 65 . .P.r.o.v.i.d.e 00 72 00</pre> <p>Figure 2: Unencrypted dump of the TSRequest.authInfo structure</p> <p>The transformed TSRequest.authinfo structure is as follows:</p>

Errata Published*	Description
	<pre> Total Size: 275 - - - - - TSCredentials - - - - - tscredentials_len: 0X10F=271 credType: 0X2=2 creds_len: 0X106=262 - - - - - TSSmartCardCreds - - - - - pin: [bbbbbbbbbbbb] csp_len: 0XE0=224 - - - - - TSCspDataDetail - - - - - keySpec: 0X1=1 cardName not present readerName: [OMNIKEY CardMan 3x21 0] containerName: [le-MSSmartcardUser-8bda019f-1266--53268] cspName: [Microsoft Base Smart Card Crypto Provider] - - - - - TSSmartCardCreds ctd - - - - - userHint not present domainHint not present Bytes Remaining: 275-275=0 </pre>
2016/12/05	<p>In Section 2.2.1.1, NegoData, changed the name of the field "NegoToken" to "negoToken" and removed the following product behavior note as it was redundant with existing text and not Windows specific.</p> <p>Deleted:</p> <p><10> Section 2.2.1.1: This contains all Kerberos- or NTLM-specific messages as negotiated by SPNEGO.</p>

*Date format: YYYY/MM/DD

[MS-CSVP]: Failover Cluster: Setup and Validation Protocol (ClusPrep)

This topic lists the Errata found in the MS-CSVP 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-DCOM]: Distributed Component Object Model (DCOM) Remote Protocol

This topic lists the Errata found in the MS-DCOM 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-DFSC]: Distributed File System (DFS) Referral Protocol

This topic lists the Errata found in [MS-DFSC] 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.

Errata below are for Protocol Document Version [V25.0 – 2016/07/14](#).

Errata Published*	Description
2016/08/15	<p>In Section 3.1.5.1, I/O Operation to Target Fails with STATUS_PATH_NOT_COVERED, the last paragraph was changed from:</p> <p>On a cache miss, it MUST issue a DFS link referral request, as specified in section 3.1.4.2, providing "LINK", the DFS root target server specified by TargetHint of ReferralCache entry corresponding to the DFS namespace, UserCredentials, MaxOutputSize, and Path as parameters. The Path parameter MUST be set to the path in the I/O operation issued to the DFS root target in step 8 of section 3.1.4.1. Process the DFS referral response as specified in section 3.1.5.4.3, which will update the ReferralCache.<9> The resulting ReferralCache entry MUST be used in further processing.</p> <p>Changed to:</p> <p>Otherwise, the client MUST obtain the file attributes of the DFS link as specified in [MS-CIFS] section 3.2.4.12 or [MS-SMB2] section 3.2.4.8 based on the protocol transport.</p> <p>If the file attributes include FILE_ATTRIBUTE_REPARSE_POINT, the client MUST issue a DFS link referral request, as specified in section 3.1.4.2, providing as parameters "LINK", the DFS root target server specified by the TargetHint of the ReferralCache entry corresponding to the DFS namespace, UserCredentials, MaxOutputSize, and Path. The Path parameter MUST be set to the path in the I/O operation issued to the DFS root target in step 8 of section 3.1.4.1. The client MUST process the DFS referral response as specified in section 3.1.5.4.3, which will update the ReferralCache.<9> The resulting ReferralCache entry, if any, MUST be used in further processing.</p>

*Date format: YYYY/MM/DD

[MS-DHCPM]: Microsoft Dynamic Host Configuration Protocol (DHCP) Server Management Protocol

This topic lists the Errata found in [MS-DHCPM] 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.

Errata below are for Protocol Document Version [V30.0 – 2016/07/14](#).

Errata Published*	Description
2017/02/20	<p>In Section 2.2.1.2.112, DHCP_STATELESS_PARAMS, updated the constant from DHCP_STATELESS_PARAMS to DHCPV6_STATELESS_PARAMS.</p> <p>Changed from:</p> <p>2.2.1.2.112 DHCP_STATELESS_PARAMS</p> <p>The DHCP_STATELESS_PARAMS structure contains stateless settings for a DHCPv6 server. This structure is used with the R_DhcpV6SetStatelessStoreParams (section 3.2.4.117) and R_DhcpV6GetStatelessStoreParams (section 3.2.4.118) methods</p> <p>Changed to:</p> <p>2.2.1.2.112 DHCPV6_STATELESS_PARAMS</p> <p>The DHCPV6_STATELESS_PARAMS structure contains stateless settings for a DHCPv6 server. This structure is used with the R_DhcpV6SetStatelessStoreParams (section 3.2.4.117) and R_DhcpV6GetStatelessStoreParams (section 3.2.4.118) methods</p>
2017/02/20	<p>In Section 2.2.1.1.25, DHCP_MAX_FREE_ADDRESSES_REQUESTED, updated the constant from DHCP_MAX_FREE_ADDRESSES_REQUIRED to DHCP_MAX_FREE_ADDRESSES_REQUESTED.</p> <p>Changed from:</p> <p>2.2.1.1.25 DHCP_MAX_FREE_ADDRESSES_REQUIRED</p> <p>The DHCP_MAX_FREE_ADDRESSES_REQUIRED constant defines the maximum number of free IPv4 or IPv6 addresses that can be retrieved from the DHCP server in one call to R_DhcpV4GetFreeIpAddress (section 3.2.4.121) or R_DhcpV6GetFreeIpAddress (section 3.2.4.122) methods.</p> <p>This constant is declared as follows:</p> <pre>#define DHCP_MAX_FREE_ADDRESSES_REQUIRED 1024</pre> <p>Changed to:</p> <p>2.2.1.1.25 DHCP_MAX_FREE_ADDRESSES_REQUESTED</p> <p>The DHCP_MAX_FREE_ADDRESSES_REQUESTED constant defines the maximum number of free IPv4 or IPv6 addresses that can be retrieved from the DHCP server in one call to R_DhcpV4GetFreeIpAddress (section 3.2.4.121) or R_DhcpV6GetFreeIpAddress (section 3.2.4.122) methods.</p> <p>This constant is declared as follows:</p> <pre>#define DHCP_MAX_FREE_ADDRESSES_REQUESTED 1024</pre>
2017/02/20	<p>In Section 6, Appendix A: Full IDL, added a line in the full IDL to match the definition in section</p>

Errata Published*	Description
	<p>2.2.1.1.15.</p> <p>Changed from:</p> <pre>import "ms-dtyp.idl"; typedef [handle] LPWSTR DHCP_SRV_HANDLE;</pre> <p>Changed to:</p> <pre>import "ms-dtyp.idl"; #define LPWSTR [string] wchar t* typedef [handle] LPWSTR DHCP_SRV_HANDLE;</pre>
2017/02/20	<p>In Section 3.1.4.20, R_DhcpDeleteClientInfo (Opnum 19), the field name was updated from ServerInfo to ClientInfo to match the description.</p> <p>Changed from:</p> <p>ServerInfo This is of type DHCP_SEARCH_INFO (section 2.2.1.2.18) structure, defining the key to be used to search the DHCPv4 client lease record that needs to be deleted on the DHCPv4 server. In case the SearchType member is DhcpClientName and there are multiple lease records with the same ClientName member, the server will delete the lease record for any of the clients with that client name.</p> <p>Changed to:</p> <p>ClientInfo This is of type DHCP_SEARCH_INFO (section 2.2.1.2.18) structure, defining the key to be used to search the DHCPv4 client lease record that needs to be deleted on the DHCPv4 server. In case the SearchType member is DhcpClientName and there are multiple lease records with the same ClientName member, the server will delete the lease record for any of the clients with that client name.</p>
2017/02/06	<p>In Section 2.2.1.2.83, DHCPV6_BIND_ELEMENT_ARRAY, updated that the Elements field of the DHCPV6_BIND_ELEMENT_ARRAY structure is an array of type DHCPV6_BIND_ELEMENT structure rather than type DHCP_BIND_ELEMENT structure.</p> <p>Changed from:</p> <p>Elements: This is a pointer to an array of type DHCP_BIND_ELEMENT (section 2.2.1.2.82) structure and length NumElements that contains information for interface bindings for a DHCPv6 server.</p> <p>Changed to:</p> <p>Elements: This is a pointer to an array of type DHCPV6_BIND_ELEMENT (section 2.2.1.2.82) structure and length NumElements that contains information for interface bindings for a DHCPv6 server.</p>

*Date format: YYYY/MM/DD

[MS-DNSP]: Domain Name Service (DNS) Server Management Protocol

This topic lists the Errata found in the MS-DNSP 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V31.0 - 2016/07/14](#).

Errata Published *	Description																
2017/03/06	<p>In Section 3.1.8.3, DNS Policy Validation, missing values were added and several other values were updated in the table in this section.</p> <p>Changed from:</p> <p>The DNS Policy configured at the server level has certain restrictions. The following table describes the valid settings:</p> <table><tr><th>DNS_RPC_POLICY_LEVEL</th><th>DNS_RPC_POLICY_TYPE allowed</th><th>DNS_RPC_POLICY_ACTION_TYPE allowed</th><th>DNS Policy Content</th></tr><tr><td>DnsPolicyServerLevel</td><td>DnsPolicyQueryProcessing</td><td>DnsPolicyDeny DnsPolicyIgnore</td><td>There MUST be no DNS Policy content specified for DNS Policy at the server level.</td></tr><tr><td>DnsPolicyServerLevel</td><td>DnsPolicyRecursion</td><td>DnsPolicyDeny DnsPolicyIgnore</td><td>There MUST be no DNS Policy content specified.</td></tr><tr><td>DnsPolicyServerLevel</td><td>DnsPolicyRecursion</td><td>DnsPolicyAllow</td><td>The DNS Policy content field MUST be populate</td></tr></table>	DNS_RPC_POLICY_LEVEL	DNS_RPC_POLICY_TYPE allowed	DNS_RPC_POLICY_ACTION_TYPE allowed	DNS Policy Content	DnsPolicyServerLevel	DnsPolicyQueryProcessing	DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified for DNS Policy at the server level.	DnsPolicyServerLevel	DnsPolicyRecursion	DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified.	DnsPolicyServerLevel	DnsPolicyRecursion	DnsPolicyAllow	The DNS Policy content field MUST be populate
DNS_RPC_POLICY_LEVEL	DNS_RPC_POLICY_TYPE allowed	DNS_RPC_POLICY_ACTION_TYPE allowed	DNS Policy Content														
DnsPolicyServerLevel	DnsPolicyQueryProcessing	DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified for DNS Policy at the server level.														
DnsPolicyServerLevel	DnsPolicyRecursion	DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified.														
DnsPolicyServerLevel	DnsPolicyRecursion	DnsPolicyAllow	The DNS Policy content field MUST be populate														

Errata Published *	Description			
				d with server scopes.
	DnsPolicyZoneLevel	DnsPolicyQueryProcessing	DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified.
	DnsPolicyZoneLevel	DnsPolicyQueryProcessing	DnsPolicyAllow	The DNS Policy content field MUST be populated with zone scopes configured for the zone.
	DnsPolicyZoneLevel		DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified.
	DnsPolicyZoneLevel		DnsPolicyAllow	The DNS Policy content field MUST be populated with zone scopes configured for the zone from which Zone Transfer will take place.
	DnsPolicyZoneLevel		DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified.
	DnsPolicyZoneLevel		DnsPolicyAllow	The DNS Policy content

Errata Published *	Description			
				field MUST be populated with zone scopes configured for the zone on which update has to happen.
	<p>Changed to:</p> <p>The DNS Policy configured at the server level has certain restrictions. The following table describes the valid settings:</p>			
	DNS_RPC_POLICY_LEVEL	DNS_RPC_POLICY_TYPE allowed	DNS_RPC_POLICY_ACTION_TYPE allowed	DNS Policy Content
	DnsPolicyZoneLevel	DnsPolicyQueryProcessing	DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified.
	DnsPolicyZoneLevel	DnsPolicyQueryProcessing	DnsPolicyAllow	The DNS Policy content field MUST be populated with zone scopes configured for the zone.
	DnsPolicyZoneLevel	DnsPolicyZoneTransfer	DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified.
	DnsPolicyServerLevel	DnsPolicyQueryProcessing	DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified for DNS Policy at

Errata Published *	Description			
				the server level.
	DnsPolicyServerLevel	DnsPolicyRecursion	DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified.
	DnsPolicyServerLevel	DnsPolicyRecursion	DnsPolicyAllow	The DNS Policy content field MUST be populated with server scopes.
	DnsPolicyServerLevel	DnsPolicyZoneTransfer	DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified.
	DnsPolicyServerLevel	DnsPolicyDynamicUpdate	DnsPolicyDeny DnsPolicyIgnore	There MUST be no DNS Policy content specified.
	DnsPolicyServerLevel	DnsRRLEntryList	DnsPolicyDeny	There MUST be no DNS Policy content specified.
2017/02/20	<p>In Section 6, Appendix A: Full IDL, updated the IDL to add *PDNS_RPC_ZONE_FLAGS to the definition of DNS_RPC_ZONE_FLAGS for consistency with the definition in section 2.2.5.2.2.</p> <p>Changed from:</p> <pre> ... //typedef struct _DnsSrvRpcZoneFlags //{ // DWORD Paused : 1; // DWORD Shutdown : 1; // DWORD Reverse : 1; // DWORD AutoCreated : 1; // DWORD DsIntegrated : 1; // DWORD Aging : 1; // DWORD Update : 2; </pre>			

Errata Published *	Description
	<pre> // DWORD ReadOnly : 1; // DWORD Unused : 23; //} //DNS_RPC_ZONE_FLAGS, *PDNS_RPC_ZONE_FLAGS; typedef DWORD DNS_RPC_ZONE_FLAGS; ... Changed to: ... //typedef struct DnssrvRpcZoneFlags //{ // DWORD Paused : 1; // DWORD Shutdown : 1; // DWORD Reverse : 1; // DWORD AutoCreated : 1; // DWORD DsIntegrated : 1; // DWORD Aging : 1; // DWORD Update : 2; // DWORD ReadOnly : 1; // DWORD Unused : 23; //} //DNS_RPC_ZONE_FLAGS, *PDNS_RPC_ZONE_FLAGS; typedef DWORD DNS_RPC_ZONE_FLAGS, *PDNS_RPC_ZONE_FLAGS; ... </pre>
2017/01/23	<p>In Section 2.2.1.2.6, DNSSRV_RPC_UNION, updated the type names in the descriptions of two pointers.</p> <p>Changed from:</p> <p>...</p> <p>ZoneInfoW2K: A pointer to a structure of type DNS_RPC_INFO_W2K (section 2.2.5.2.4). This structure is used to specify detailed DNS zone information.</p> <p>...</p> <p>AutoConfigure: A pointer to a structure of type DNS_AUTOCONFIGURE (section 2.2.8.2.1). This structure is used to request DNS server autoconfiguration.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>ZoneInfoW2K: A pointer to a structure of type DNS_RPC_ZONE_INFO_W2K (section 2.2.5.2.4.1). This structure is used to specify detailed DNS zone information.</p> <p>...</p> <p>AutoConfigure: A pointer to a structure of type DNS_RPC_AUTOCONFIGURE (section 2.2.8.2.1). This structure is used to request DNS server autoconfiguration.</p> <p>...</p>

Errata Published *	Description
	<p>In Section 2.2.5.2.3.1, DNSSRV_RPC_ZONE_LIST_W2K, updated the type names in the description of one array.</p> <p>Changed from:</p> <p>...</p> <p>ZoneArray: An array of structures of type DNS_RPC_ZONE (section 2.2.5.2.1.1). Each element of the array represents one zone.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>ZoneArray: An array of structures of type DNS_RPC_ZONE_W2K (section 2.2.5.2.1.1). Each element of the array represents one zone.</p> <p>...</p>
2016/08/29	<p>In two sections, revisions were made to the description of one field and one value to account for scenarios where virtualization instances are automatically created via the CreateVirtualizationInstance operation.</p> <p>In Section 2.2.5.2.2, DNS_RPC_ZONE_FLAGS, changed the description of the AutoCreated field from:</p> <p>...</p> <p>D (AutoCreated): If set to 1, indicates that zone was auto-created. A DNS server MAY automatically create certain zones at boot time which are flagged as "AutoCreated". Such zones are never written to persistent storage, and the DNS Server MUST NOT perform any DNS Server Management Protocol RPC operations on such zones.<38></p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>D (AutoCreated): If set to 1, indicates that zone was auto-created. A DNS server MAY automatically create certain zones at boot time or when a virtualization instance is created via the CreateVirtualizationInstance RPC operation (section 3.1.4.1), and flag these zones as "AutoCreated". Such zones are never written to persistent storage, and the DNS Server MUST NOT perform any DNS Server Management Protocol RPC operations on such zones.<38></p> <p>...</p> <p>In Section 2.2.5.2.4.1, DNS_RPC_ZONE_INFO_W2K, revised the description of the fAutoCreated value from:</p> <p>...</p> <p>fAutoCreated: A Boolean value that indicates whether this zone was autocreated by the DNS server at boot time.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>fAutoCreated: A Boolean value that indicates whether this zone was autocreated by the DNS server at boot time or when a virtualization instance is created via the CreateVirtualizationInstance RPC operation (section 3.1.4.1).</p> <p>...</p>

Errata Published *	Description
2016/08/15	<p>In several sections, made updates to address inconsistencies between the IDL and the text in those sections.</p> <p>In Section 2.2.1.1.1, DNS_RPC_TYPEID, added DNSSRV_TYPEID_ANY to the list of enumeration values, and added a description for this value ("Type is invalid.").</p> <p>Changed from:</p> <pre>... typedef enum _DnssrvRpcTypeId { DNSSRV_TYPEID_NULL = 0, DNSSRV_TYPEID_DWORD, ... }</pre> <p>Changed to:</p> <pre>... typedef enum _DnssrvRpcTypeId { DNSSRV_TYPEID_ANY = (-1), DNSSRV_TYPEID_NULL = 0, DNSSRV_TYPEID_DWORD, ... }</pre> <p>In Section 2.2.12.1, Enumerations and Constants, updated the value for MAX_RECORD_TYPES row to reflect the correct number of record types from 0x0000001D to 0x00000020.</p> <p>In Section 2.2.15.1.1.5, DNS_RPC_POLICY_TYPE, added an entry for DnsPolicyMax to the list of values in the table for this enumeration:</p> <p>DnsPolicyMax Shows the maximum DNS policies supported.</p> <p>In Section 3.1.4.17, R_DnssrvQuery4 (Opnum 16), removed the hBindingHandle parameter to match the IDL.</p> <p>Changed from:</p> <pre>... LONG R_DnssrvQuery4([in] handle_t hBindingHandle, [in] DWORD dwClientVersion, [in] DWORD dwSettingFlags, ...)</pre> <p>Changed to:</p> <pre>... LONG R_DnssrvQuery4([in] DWORD dwClientVersion, [in] DWORD dwSettingFlags, ...)</pre>

Errata Published *	Description
	<p>...</p> <p>In Section 6, Appendix A: Full ID:</p> <ul style="list-style-type: none"> ▪ Added "DNSSRV_TYPEID_ANY = (-1)" to the DnssrvRpcTypeId enumeration. ▪ Updated the value for the MAX_RECORD_TYPES definition in the DNS_ZONE_STATS_TYPE enumeration from 31 to 32. ▪ Removed the hBindingHandle parameter for the following methods in the DnsServer interface: <p>R_DnssrvOperation R_DnssrvQuery R_DnssrvComplexOperation R_DnssrvEnumRecords R_DnssrvUpdateRecord R_DnssrvQuery2 R_DnssrvComplexOperation2 R_DnssrvEnumRecords2 R_DnssrvUpdateRecord2</p>

*Date format: YYYY/MM/DD

[MS-DPWSSN]: Devices Profile for Web Services (DPWS) Size Negotiation Extension

This topic lists the Errata found in [MS-DPWSSN] 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.

Errata below are for Protocol Document Version [V5.0 – 2016/07/14](#).

Errata Published*	Description
2016/09/12	<p>In Section 6, Appendix A: Full WSDL, added quotation marks missing from the value for the xmlns:lms attribute.</p> <p>Changed from:</p> <pre><?xml version="1.0" encoding="UTF-8"?> <xs:schema targetNamespace="http://schemas.microsoft.com/windows/dpws/LargeMetadataSupport/2007/08" xmlns:lms=http://schemas.microsoft.com/windows/dpws/LargeMetadataSupport/2007/08 xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"> ...</pre> <p>Changed to:</p> <pre><?xml version="1.0" encoding="UTF-8"?> <xs:schema targetNamespace="http://schemas.microsoft.com/windows/dpws/LargeMetadataSupport/2007/08" xmlns:lms="http://schemas.microsoft.com/windows/dpws/LargeMetadataSupport/2007/08" xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"> ...</pre>

*Date format: YYYY/MM/DD

[MS-DRSR]: Directory Replication Service (DRS) Remote Protocol

This topic lists the Errata found in the MS-DRSR 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V35.0 - 2016/07/14](#).

Errata Published*	Description
2017/03/06	<p>In Section 4.1.2.3, Server Behavior of the IDL_DRSSAddSidHistory Method, updated srcCxt to srcCtx in the pseudocode.</p> <p>Changed from:</p> <pre>srcCxt := ConnectToDCWithCreds(srcDomainController,</pre> <p>Changed to:</p> <pre>srcCtx := ConnectToDCWithCreds(srcDomainController,</pre>
2017/02/06	<p>In Section 4.1.10.2.20, EXOP_ERR Codes, updated an EXOP_ERR error code from EXOP_ERR_PARAM_ERROR to EXOP_ERR_PARAM_ERR.</p> <p>Changed from:</p> <pre>EXOP_ERR_PARAM_ERROR (0x00000010)</pre> <p>Changed to:</p> <pre>EXOP_ERR_PARAM_ERR (0x00000010)</pre> <p>In Section 4.1.10.5.12, ProcessFsmoRoleRequest, added and updated code fragments for the ProcessFsmoRoleRequest procedure.</p> <p>Changed from:</p> <pre>msgOut.ulExtendedRet := EXOP_ERR_OWNER_DELETED</pre> <p>Changed to:</p> <pre>msgOut.ulExtendedRet := EXOP_ERR_FSMO_OWNER_DELETED</pre>

Errata Published*	Description
	<p>Changed from:</p> <pre> clientComputerObj := serverObj!serverReference if clientComputerObj!rIDSetReference = null then clientRidSetObj := An implementation-defined DSName in the default NC such that not ObjExists(clientRidSetObj) Create object with DSName clientRidSetObject such that rIDSet in clientRidSetObject!objectClass /* Windows Behavior: Windows sets clientRidSetObj to be a child * of clientComputerObj. */ clientComputerObj!rIDSetReference := clientRidSetObj else clientRidSetObj := clientComputerObj!rIDSetReference endif </pre> <p>Changed to:</p> <pre> clientComputerObj := serverObj!serverReference if clientComputerObj!rIDSetReferences = null then clientRidSetObj := An implementation-defined DSName in the default NC such that not ObjExists(clientRidSetObj) Create object with DSName clientRidSetObj such that rIDSet in clientRidSetObj!objectClass /* Windows Behavior: Windows sets clientRidSetObj to be a child * of clientComputerObj. */ clientComputerObj!rIDSetReferences := clientRidSetObj else clientRidSetObj := clientComputerObj!rIDSetReferences endif </pre> <p>Changed from:</p> <pre> fsmoObj!rIDAvailablePool := ridAvailLoHi clientRidSetObj!rIDAllocationPool := ridAllocLoHi msgOut.liFsmoInfo := ridAllocLoHi endif </pre> <p>Changed to:</p> <pre> fsmoObj!rIDAvailablePool := ridAvailLoHi clientRidSetObj!rIDAllocationPool := ridAllocLoHi clientRidSetObj!rIDPreviousAllocationPool := 0 clientRidSetObj!rIDNextRID := 0 /* Windows Behavior: rIDUsedPool [MS-ADA3] is not used anywhere, * but Windows always sets it to zero. */ clientRidSetObj!rIDUsedPool := 0 msgOut.liFsmoInfo := ridAllocLoHi endif </pre>

Errata Published*	Description
	<p>Changed from:</p> <pre> and RevealSecretsForUserAllowed(rodObj, fsmoObj) and (not NTDSDSA_OPT_DISABLE_OUTBOUND_REPL_SECRET in DSAObj()!options or DRS_SYNC_FORCED in msgIn.ulFlags) then scope := {fsmoObj} else scope := {} endif else if EXOP_REPL_OBJ in msgIn.ulExtendedOp if AmILHServer() = true and NTDSDSA_OPT_DISABLE_OUTBOUND_REPL_OBJ in DSAObj()!options and not DRS_SYNC_FORCED in msgIn.ulFlags then </pre> <p>Changed to:</p> <pre> and RevealSecretsForUserAllowed(rodObj, fsmoObj) and (not NTDSDSA_OPT_DISABLE_OUTBOUND_REPL in DSAObj()!options or DRS_SYNC_FORCED in msgIn.ulFlags) then scope := {fsmoObj} else scope := {} endif else if EXOP_REPL_OBJ in msgIn.ulExtendedOp if AmILHServer() = true and NTDSDSA_OPT_DISABLE_OUTBOUND_REPL in DSAObj()!options and not DRS_SYNC_FORCED in msgIn.ulFlags then </pre> <p>Changed from:</p> <pre> hDrs, o, ncRoot, msgIn.ulFlags, msgIn.ulExtendedOp, msgOut) </pre> <p>Changed to:</p> <pre> hDrs, o, GetObjectNC(msgIn.pNC^), msgIn.ulFlags, msgIn.ulExtendedOp, msgOut) </pre>

*Date format: YYYY/MM/DD

[MS-DTCO]: MSDTC Connection Manager: OleTx Transaction Protocol

This topic lists the Errata found in the MS-DTCO 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-DSCPM]: Desired State Configuration Pull Model Protocol

This topic lists the Errata found in the MS-DSCPM 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-DTYP]: Windows Data Types

This topic lists the Errata found in the MS-DTYP 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V31.0 - 2016/07/14](#).

Errata Published*	Description																																																
2017/03/06	<p>In Section 2.5.1.1, SDDL Syntax, corrected the values for the object-specific-rights-strings.</p> <p>Changed from:</p> <p>...</p> <p>it is recommended that the reader consult a specific protocol for applicable values, if any, in that protocol.</p> <table><tr><th>String</th><th>Object type</th><th>Access right</th><th>Hex value</th></tr><tr><td>...</td><td></td><td></td><td></td></tr><tr><td>"FW"</td><td>File</td><td>File Write</td><td>0x00100116</td></tr><tr><td>"FR"</td><td>File</td><td>File Read</td><td>0x00120089</td></tr><tr><td>"KA"</td><td>Registry Key</td><td>Key All Access</td><td>0x00000019</td></tr><tr><td>"KR"</td><td>Registry Key</td><td>Key Read</td><td>0x0000003F</td></tr><tr><td>"KX"</td><td>Registry Key</td><td>Key Execute</td><td>0x00000019</td></tr><tr><td>"KW"</td><td>Registry Key</td><td>Key Write</td><td>0x00000006</td></tr><tr><td>...</td><td></td><td></td><td></td></tr></table> <p>Changed to:</p> <p>it is recommended that the reader consult a specific protocol for applicable values, if any, in that protocol.</p> <table><tr><th>String</th><th>Object type</th><th>Access right</th><th>Hex value</th></tr><tr><td>...</td><td></td><td></td><td></td></tr><tr><td>"FW"</td><td>File</td><td>File Write</td><td>0x00120116</td></tr></table>	String	Object type	Access right	Hex value	...				"FW"	File	File Write	0x00100116	"FR"	File	File Read	0x00120089	"KA"	Registry Key	Key All Access	0x00000019	"KR"	Registry Key	Key Read	0x0000003F	"KX"	Registry Key	Key Execute	0x00000019	"KW"	Registry Key	Key Write	0x00000006	...				String	Object type	Access right	Hex value	...				"FW"	File	File Write	0x00120116
String	Object type	Access right	Hex value																																														
...																																																	
"FW"	File	File Write	0x00100116																																														
"FR"	File	File Read	0x00120089																																														
"KA"	Registry Key	Key All Access	0x00000019																																														
"KR"	Registry Key	Key Read	0x0000003F																																														
"KX"	Registry Key	Key Execute	0x00000019																																														
"KW"	Registry Key	Key Write	0x00000006																																														
...																																																	
String	Object type	Access right	Hex value																																														
...																																																	
"FW"	File	File Write	0x00120116																																														

Errata Published*	Description																											
	<table><tr><td>"FR"</td><td>File</td><td>File Read</td><td>0x00120089</td></tr><tr><td>"KA"</td><td>Registry Key</td><td>Key All Access</td><td>0x000F003F</td></tr><tr><td>"KR"</td><td>Registry Key</td><td>Key Read</td><td>0x00020019</td></tr><tr><td>"KX"</td><td>Registry Key</td><td>Key Execute</td><td>0x00020019</td></tr><tr><td>"KW"</td><td>Registry Key</td><td>Key Write</td><td>0x00020006</td></tr><tr><td>...</td><td></td><td></td><td></td></tr></table>				"FR"	File	File Read	0x00120089	"KA"	Registry Key	Key All Access	0x000F003F	"KR"	Registry Key	Key Read	0x00020019	"KX"	Registry Key	Key Execute	0x00020019	"KW"	Registry Key	Key Write	0x00020006	...			
"FR"	File	File Read	0x00120089																									
"KA"	Registry Key	Key All Access	0x000F003F																									
"KR"	Registry Key	Key Read	0x00020019																									
"KX"	Registry Key	Key Execute	0x00020019																									
"KW"	Registry Key	Key Write	0x00020006																									
...																												
2017/01/09	<p>In two sections, revised the descriptions for two SIDs.</p> <p>In Section 2.4.2.4, Well-Known SID Structures, changed from:</p> <table><tr><th>Constant/value</th><th>Description</th></tr><tr><td>...</td><td>...</td></tr><tr><td>RAS_SERVERS S-1-5-21-<domain>-553</td><td>A domain local group for Remote Access Services (RAS) servers. Servers in this group have Read Account Restrictions and Read Logon Information access to User objects in the Active Directory domain local group.</td></tr><tr><td>...</td><td>...</td></tr><tr><td>RDS_REMOTE_ACCESS_SERVERS S-1-5-32-575</td><td>A group that allows members use of Remote Application Services resources.</td></tr><tr><td>...</td><td>...</td></tr></table> <p>Changed to</p> <table><tr><th>Constant/value</th><th>Description</th></tr><tr><td>...</td><td>...</td></tr><tr><td>RAS_SERVERS S-1-5-21-<domain>-553</td><td>A domain local group for Remote Access Services (RAS) servers. By default, this group has no members. Servers in this group have Read Account Restrictions and Read Logon Information access to User objects in the Active Directory domain local group</td></tr><tr><td>...</td><td>...</td></tr><tr><td>RDS_REMOTE_ACCESS_SERVERS S-1-5-32-575</td><td>Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. This group needs to be populated on servers running RD Connection Broker. RD Gateway servers</td></tr></table>				Constant/value	Description	RAS_SERVERS S-1-5-21-<domain>-553	A domain local group for Remote Access Services (RAS) servers. Servers in this group have Read Account Restrictions and Read Logon Information access to User objects in the Active Directory domain local group.	RDS_REMOTE_ACCESS_SERVERS S-1-5-32-575	A group that allows members use of Remote Application Services resources.	Constant/value	Description	RAS_SERVERS S-1-5-21-<domain>-553	A domain local group for Remote Access Services (RAS) servers. By default, this group has no members. Servers in this group have Read Account Restrictions and Read Logon Information access to User objects in the Active Directory domain local group	RDS_REMOTE_ACCESS_SERVERS S-1-5-32-575	Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. This group needs to be populated on servers running RD Connection Broker. RD Gateway servers		
Constant/value	Description																											
...	...																											
RAS_SERVERS S-1-5-21-<domain>-553	A domain local group for Remote Access Services (RAS) servers. Servers in this group have Read Account Restrictions and Read Logon Information access to User objects in the Active Directory domain local group.																											
...	...																											
RDS_REMOTE_ACCESS_SERVERS S-1-5-32-575	A group that allows members use of Remote Application Services resources.																											
...	...																											
Constant/value	Description																											
...	...																											
RAS_SERVERS S-1-5-21-<domain>-553	A domain local group for Remote Access Services (RAS) servers. By default, this group has no members. Servers in this group have Read Account Restrictions and Read Logon Information access to User objects in the Active Directory domain local group																											
...	...																											
RDS_REMOTE_ACCESS_SERVERS S-1-5-32-575	Servers in this group enable users of RemoteApp programs and personal virtual desktops access to these resources. This group needs to be populated on servers running RD Connection Broker. RD Gateway servers																											

Errata Published*	Description	
		and RD Web Access servers used in the deployment need to be in this group.

	In Section 2.5.1.1, Syntax, changed from:	
	SDDL alias	Well-Known SID name

	"RA"	REMOTE ACCESS SERVERS

	Changed to:	
SDDL alias	Well-Known SID name	
...	...	
"RA"	RDS_REMOTE_ACCESS_SERVERS	
...	...	

*Date format: YYYY/MM/DD

[MS-DVRD]: Device Registration Discovery Protocol

This topic lists the Errata found in [MS-DVRD] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-DVRE]: Device Registration Enrollment Protocol

This topic lists the Errata found in the MS-DVRE 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-ECS]: Enterprise Client Synchronization Protocol

This topic lists the Errata found in the MS-ECS 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V6.0 – 2016/07/14](#).

Errata Published*	Description																																																																																																																																																																
2017/01/09	<p>In Section 2.2.2.2, QUOTA_USAGE_ENTRY, in the bit table and in the description that follows, swapped the order of the UserUsage and UserDataFreeSpace fields.</p> <p>Changed from:</p> <table><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>3</td><td>1</td></tr><tr><td colspan="32">UserUsage</td></tr><tr><td colspan="32">...</td></tr><tr><td colspan="32">UserDataFreeSpace</td></tr><tr><td colspan="32">...</td></tr></table> <p>UserUsage (8 bytes): A 64-bit unsigned integer that contains the amount of data, in bytes, in the user's share.</p> <p>UserDataFreeSpace (8 bytes): A 64-bit unsigned integer that contains the amount of available free space, in bytes, in the user's share.</p> <p>Changed to:</p>	0	1	2	3	4	5	6	7	8	9	1	1	2	3	4	5	6	7	8	9	2	1	2	3	4	5	6	7	8	9	3	1	UserUsage																																...																																UserDataFreeSpace																																...																															
0	1	2	3	4	5	6	7	8	9	1	1	2	3	4	5	6	7	8	9	2	1	2	3	4	5	6	7	8	9	3	1																																																																																																																																		
UserUsage																																																																																																																																																																	
...																																																																																																																																																																	
UserDataFreeSpace																																																																																																																																																																	
...																																																																																																																																																																	

Errata Published*	Description																																																																																																																																																																
	<table><tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>1</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>3</td><td>1</td></tr><tr><td colspan="32">UserDataFreeSpace</td></tr><tr><td colspan="32">...</td></tr><tr><td colspan="32">UserUsage</td></tr><tr><td colspan="32">...</td></tr></table> <p>UserDataFreeSpace (8 bytes): A 64-bit unsigned integer that contains the amount of available free space, in bytes, in the user's share.</p> <p>UserUsage (8 bytes): A 64-bit unsigned integer that contains the amount of data, in bytes, in the user's share.</p>	0	1	2	3	4	5	6	7	8	9	1	1	2	3	4	5	6	7	8	9	2	1	2	3	4	5	6	7	8	9	3	1	UserDataFreeSpace																																...																																UserUsage																																...																															
0	1	2	3	4	5	6	7	8	9	1	1	2	3	4	5	6	7	8	9	2	1	2	3	4	5	6	7	8	9	3	1																																																																																																																																		
UserDataFreeSpace																																																																																																																																																																	
...																																																																																																																																																																	
UserUsage																																																																																																																																																																	
...																																																																																																																																																																	

*Date format: YYYY/MM/DD

[MS-EFSR]: Encrypting File System Remote (EFSRPC) Protocol

This topic lists the Errata found in the MS-EFSR 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-EMF]: Enhanced Metafile Format

This topic lists the Errata found in the MS-EMF 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-EMFPLUS]: Enhanced Metafile Format Plus Extensions

This topic lists the Errata found in the MS-EMFPLUS 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-ERREF]: Windows Error Codes

This topic lists the Errata found in the MS-ERREF 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V16.0 – 2016/07/14](#).

Errata Published*	Description																		
2017/03/06	<p>In Section 2.2, Win32 Error Codes, added a new error code.</p> <p>Changed from:</p> <table><tr><th>Win32 Error Codes</th><th>Description</th></tr><tr><td>...</td><td>...</td></tr><tr><td>0x00000BCA ERROR_FAIL_REBOOT_INITIATED</td><td>The requested operation failed. A system reboot has been initiated to roll back changes made.</td></tr><tr><td>...</td><td>...</td></tr></table> <p>Changed to:</p> <table><tr><th>Win32 Error Codes</th><th>Description</th></tr><tr><td>...</td><td>...</td></tr><tr><td>0x00000BCA ERROR_FAIL_REBOOT_INITIATED</td><td>The requested operation failed. A system reboot has been initiated to roll back changes made.</td></tr><tr><td>0x00000BCB ERROR_PRINTER_DRIVER_DOWNLOAD_NEEDED</td><td>The specified printer driver was not found on the system and needs to be downloaded.</td></tr><tr><td>...</td><td>...</td></tr></table>	Win32 Error Codes	Description	0x00000BCA ERROR_FAIL_REBOOT_INITIATED	The requested operation failed. A system reboot has been initiated to roll back changes made.	Win32 Error Codes	Description	0x00000BCA ERROR_FAIL_REBOOT_INITIATED	The requested operation failed. A system reboot has been initiated to roll back changes made.	0x00000BCB ERROR_PRINTER_DRIVER_DOWNLOAD_NEEDED	The specified printer driver was not found on the system and needs to be downloaded.
Win32 Error Codes	Description																		
...	...																		
0x00000BCA ERROR_FAIL_REBOOT_INITIATED	The requested operation failed. A system reboot has been initiated to roll back changes made.																		
...	...																		
Win32 Error Codes	Description																		
...	...																		
0x00000BCA ERROR_FAIL_REBOOT_INITIATED	The requested operation failed. A system reboot has been initiated to roll back changes made.																		
0x00000BCB ERROR_PRINTER_DRIVER_DOWNLOAD_NEEDED	The specified printer driver was not found on the system and needs to be downloaded.																		
...	...																		

*Date format: YYYY/MM/DD

[MS-EVEN]: EventLog Remoting Protocol

This topic lists the Errata found in the MS-EVEN 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-FRS2]: Distributed File System Replication Protocol

This topic lists the Errata found in the MS-FRS2 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-FSA]: File System Algorithms

This topic lists the Errata found in the MS-FSA 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 2, 2016 - [Download](#)

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V22.0 – 2016/07/14](#)

Errata Published*	Description
2017/03/06	<p>In Section 2.1.5.11.29, FileStreamInformation, a new bullet point was added to the second list.</p> <p>Added:</p> <ul style="list-style-type: none">• If OutputBufferSize is smaller than sizeof(FILE_STREAM_INFORMATION), the operation MUST be failed with STATUS_INFO_LENGTH_MISMATCH. <p>In Section 2.1.5.14.1, FileAllocationInformation, a new bullet point was added to the second list.</p> <p>Added:</p> <ul style="list-style-type: none">• If InputBufferSize is less than the size, in bytes, of the FILE_ALLOCATION_INFORMATION structure, the operation MUST be failed with STATUS_INFO_LENGTH_MISMATCH. <p>In Section 2.1.5.14.3, FileDispositionInformation, a new bullet point was added to the first list.</p> <p>Added:</p> <ul style="list-style-type: none">• If InputBufferSize is less than the size, in bytes, of the FILE_DISPOSITION_INFORMATION structure, the operation MUST be failed with STATUS_INFO_LENGTH_MISMATCH. <p>In Section 2.1.5.14.4, FileEndOfFileInformation, a new bullet point was added to the first list.</p> <ul style="list-style-type: none">• If InputBufferSize is less than the size, in bytes, of the FILE_END_OF_FILE_INFORMATION structure, the operation MUST be failed with STATUS_INFO_LENGTH_MISMATCH. <p>In Section 2.1.5.14.6, FileLinkInformation, the first paragraph was changed from:</p> <p>InputBuffer is of type FILE_LINK_INFORMATION, as described in [MS-FSCC] section 2.4.21.<136>Open represents the pre-existing file to which a new link named in InputBuffer.FileName will be created.</p>

Errata Published*	Description
	<p>Changed to:</p> <p>InputBuffer is of type FILE_LINK_INFORMATION_TYPE_1, as described in [MS-FSCC] section 2.4.21.1, for 32-bit local clients; or of type FILE_LINK_INFORMATION_TYPE_2, as described in [MS-FSCC] section 2.4.21.2, for remote clients or 64-bit local clients. Open represents the pre-existing file to which a new link named in InputBuffer.FileName will be created.</p> <p>In Section 2.1.5.14.6, FileLinkInformation, a new bullet point was added to the first list.</p> <p>Added:</p> <ul style="list-style-type: none"> • If InputBufferSize is less than the size, in bytes, of the FILE_LINK_INFORMATION_TYPE_1 structure (for 32-bit local clients) or the FILE_LINK_INFORMATION_TYPE_2 structure (for remote clients or 64-bit local clients), the operation MUST be failed with STATUS_INFO_LENGTH_MISMATCH. <p>In Section 2.1.5.14.7, FileModeInformation, a new bullet point was added to the first list.</p> <ul style="list-style-type: none"> • If InputBufferSize is less than the size, in bytes, of the FILE_MODE_INFORMATION structure, the operation MUST be failed with STATUS_INFO_LENGTH_MISMATCH. <p>In Section 2.1.5.14.11, FileRenameInformation, the first paragraph was changed from:</p> <p>InputBuffer is of type FILE_RENAME_INFORMATION, as described in [MS-FSCC] section 2.4.34.Open.FileName is the pre-existing file name that will be changed by this operation.</p> <p>Changed to:</p> <p>InputBuffer is of type FILE_RENAME_INFORMATION_TYPE_1, as described in [MS-FSCC] section 2.4.34.1, for 32-bit local clients; or of type FILE_RENAME_INFORMATION_TYPE_2, as described in [MS-FSCC] section 2.4.34.2, for remote clients or 64-bit local clients. Open.FileName is the pre-existing file name that will be changed by this operation.</p> <p>In Section 2.1.5.14.11, FileRenameInformation, a new bullet point was added to the second list.</p> <p>Added:</p> <ul style="list-style-type: none"> • If InputBufferSize is less than the size, in bytes, of the FILE_RENAME_INFORMATION_TYPE_1 structure (for 32-bit local clients) or the FILE_RENAME_INFORMATION_TYPE_2 structure (for remote clients or 64-bit local clients), the operation MUST be failed with STATUS_INFO_LENGTH_MISMATCH. <p>In Section 2.1.5.14.13, FileShortNameInformation, a new bullet point was added to the first list.</p> <p>Added:</p> <ul style="list-style-type: none"> • If InputBufferSize is less than the size, in bytes, of the FILE_NAME_INFORMATION structure, the operation MUST be failed with STATUS_INFO_LENGTH_MISMATCH. <p>In Section 2.1.5.14.14, FileValidDataLengthInformation, a new bullet point was added to the first list.</p> <ul style="list-style-type: none"> • If InputBufferSize is less than the size, in bytes, of the FILE_VALID_DATA_LENGTH_INFORMATION structure, the operation MUST be failed with

Errata Published*	Description														
	<p>STATUS_INFO_LENGTH_MISMATCH.</p> <p>In Section 2.1.5.15.6, FileFsControlInformation, the status code in the first bullet point was changed from:</p> <p>STATUS_INVALID_INFO_CLASS</p> <p>Changed to:</p> <p>STATUS__INFO_LENGTH_MISMATCH</p>														
2017/01/09	<p>In Section 2.6, File Attributes, added a paragraph about how unsupported attributes are handled.</p> <p>Changed from:</p> <p>The following attributes are defined for files and directories. They can be used in any combination unless noted in the description of the attribute's meaning. There is no file attribute with the value 0x00000000 because a value of 0x00000000 in the FileAttributes field means that the file attributes for this file MUST NOT be changed when setting basic information for the file.</p> <p>Changed to:</p> <p>The following attributes are defined for files and directories. They can be used in any combination unless noted in the description of the attribute's meaning. There is no file attribute with the value 0x00000000 because a value of 0x00000000 in the FileAttributes field means that the file attributes for this file MUST NOT be changed when setting basic information for the file.</p> <p>Note: File systems silently ignore any attribute that is not supported by that file system. Unsupported attributes MUST NOT be persisted on the media. It is recommended that unsupported attributes be masked off when encountered.</p>														
2017/01/09	<p>In Section 2.5.1, FileFsAttributeInformation, modified the Windows Product Behavior Note about EFS support.</p> <p>Changed from:</p> <table border="1" data-bbox="386 1224 1430 1461"> <thead> <tr> <th>Value</th><th>Meaning</th></tr> </thead> <tbody> <tr> <td>...</td><td>...</td></tr> <tr> <td>FILE_SUPPORTS_ENCRYPTION 0x00020000</td><td>The file system supports the Encrypted File System (EFS).<136></td></tr> <tr> <td>...</td><td>...</td></tr> </tbody> </table> <p><136> Section 2.5.1: Windows support for a volume formatted to NTFS version 3.0 or 3.1 is required for EFS use. NTFS versions 3.0 and 3.1 are supported on Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.</p> <p>Changed to:</p> <table border="1" data-bbox="386 1650 1430 1791"> <thead> <tr> <th>Value</th><th>Meaning</th></tr> </thead> <tbody> <tr> <td>...</td><td>...</td></tr> <tr> <td>FILE_SUPPORTS_ENCRYPTION</td><td>The file system supports the Encrypted File</td></tr> </tbody> </table>	Value	Meaning	FILE_SUPPORTS_ENCRYPTION 0x00020000	The file system supports the Encrypted File System (EFS).<136>	Value	Meaning	FILE_SUPPORTS_ENCRYPTION	The file system supports the Encrypted File
Value	Meaning														
...	...														
FILE_SUPPORTS_ENCRYPTION 0x00020000	The file system supports the Encrypted File System (EFS).<136>														
...	...														
Value	Meaning														
...	...														
FILE_SUPPORTS_ENCRYPTION	The file system supports the Encrypted File														

Errata Published*	Description				
	<table border="1" data-bbox="386 224 1430 317"> <tr> <td data-bbox="386 224 911 264">0x00020000</td><td data-bbox="911 224 1430 264">System (EFS).<136></td></tr> <tr> <td data-bbox="386 264 911 317">...</td><td data-bbox="911 264 1430 317">...</td></tr> </table> <p data-bbox="370 327 1365 432"><136> Section 2.5.1: Windows support for a volume formatted to NTFS version 3.0 or 3.1 is required for EFS use. NTFS versions 3.0 and 3.1 are supported on Windows 2000 and later. Support for FAT and EXFAT was added in Windows 10 v1607 operating system and Windows Server 2016 and later.</p>	0x00020000	System (EFS).<136>
0x00020000	System (EFS).<136>				
...	...				
2017/01/09	<p data-bbox="370 453 1430 506">In Section 2.1.5.9.4, FSCTL_DUPLICATE_EXTENTS_TO_FILE, revised the pseudocode to add a new Windows Product Behavior Note to cover the situation when the source file handle is closed.</p> <p data-bbox="370 548 529 579">Changed from:</p> <p data-bbox="370 583 1252 663">If InputBuffer.FileHandle does not represent an open Handle to a DataStream with FILE_READ_DATA FILE_READ_ATTRIBUTES level access, the operation fails with STATUS_INVALID_PARAMETER.</p> <p data-bbox="370 705 501 737">Changed to:</p> <p data-bbox="370 741 1398 821">If InputBuffer.FileHandle does not represent an open Handle to a DataStream with FILE_READ_DATA FILE_READ_ATTRIBUTES level access, the operation SHOULD<70> fail with STATUS_INVALID_PARAMETER.</p> <p data-bbox="370 825 1382 877"><70> Section 2.1.5.9.4: Windows Server returns STATUS_INVALID_HANDLE if the source file handle is closed.</p>				
2017/01/09	<p data-bbox="370 894 1430 947">In Section 2.1.5.1.2, Open of an Existing File, revised the processing rules when access checks fail with STATUS_SHARING_VIOLATION.</p> <p data-bbox="370 989 529 1020">Changed from:</p> <p data-bbox="370 1031 391 1062">...</p> <ul data-bbox="370 1062 1373 1251" style="list-style-type: none"> <li data-bbox="370 1062 756 1094">• If FileTypeToOpen is DirectoryFile: <li data-bbox="370 1104 391 1136">... <li data-bbox="370 1136 1373 1188">• Perform access checks as described in section 2.1.5.1.2.1. If this fails, the request MUST be failed with the same status. <li data-bbox="370 1188 448 1220">• EndIf <li data-bbox="370 1230 391 1262">... <p data-bbox="370 1293 501 1325">Changed to:</p> <p data-bbox="370 1335 391 1367">...</p> <ul data-bbox="370 1367 1373 1608" style="list-style-type: none"> <li data-bbox="370 1367 756 1398">• If FileTypeToOpen is DirectoryFile: <li data-bbox="370 1409 391 1440">... <li data-bbox="370 1440 1373 1493">• Perform access checks as described in section 2.1.5.1.2.1. If this fails, the request MUST be failed with the same status. <li data-bbox="370 1493 846 1524">• ElseIf this fails with any other status code: <li data-bbox="370 1524 919 1556">• The request MUST be failed with the same status. <li data-bbox="370 1556 448 1587">• EndIf <li data-bbox="370 1598 391 1629">... 				
2016/12/19	<p data-bbox="370 1629 1390 1682">In section 2.1.5.9.4 FSCTL_DUPLICATE_EXTENTS_TO_FILE behavior notes have been added to the following paragraphs.</p> <p data-bbox="370 1724 529 1755">Changed from:</p> <p data-bbox="370 1759 1382 1808">The object store MUST check for byte range lock conflicts on Open.Stream using the algorithm described in section 2.1.4.10 with ByteOffset set to InputBuffer.TargetFileOffset, Length set to</p>				

Errata Published*	Description																		
	<p>InputBuffer.ByteCount, IsExclusive set to TRUE, LockIntent set to FALSE, and Open set to Open. If a conflict is detected, the operation MUST be failed with STATUS_FILE_LOCK_CONFLICT.</p> <p>The object store MUST check for byte range lock conflicts on Source using the algorithm described in section 2.1.4.10 with ByteOffset set to InputBuffer.SourceFileOffset, Length set to InputBuffer.ByteCount, IsExclusive set to FALSE, LockIntent set to FALSE, and Open set to InputBuffer.FileHandle. If a conflict is detected, the operation MUST be failed with STATUS_FILE_LOCK_CONFLICT.</p> <p>Changed to:</p> <p>The object store SHOULD<WBN1> check for byte range lock conflicts on Open.Stream using the algorithm described in section 2.1.4.10 with ByteOffset set to InputBuffer.TargetFileOffset, Length set to InputBuffer.ByteCount, IsExclusive set to TRUE, LockIntent set to FALSE, and Open set to Open. If a conflict is detected, the operation MUST be failed with STATUS_FILE_LOCK_CONFLICT.</p> <p>The object store SHOULD<WBN2> check for byte range lock conflicts on Source using the algorithm described in section 2.1.4.10 with ByteOffset set to InputBuffer.SourceFileOffset, Length set to InputBuffer.ByteCount, IsExclusive set to FALSE, LockIntent set to FALSE, and Open set to InputBuffer.FileHandle. If a conflict is detected, the operation MUST be failed with STATUS_FILE_LOCK_CONFLICT.</p> <p>WBN1: The ReFS file system in Windows Server 2016 does not check for byte range lock conflicts on Open.Stream.</p> <p>WBN2: The ReFS file system in Windows Server 2016 does not check for byte range lock conflicts on Source.</p>																		
2016/11/21	<p>In Section 2.2, Status Codes, removed status code FSCTL_SET_SHORT_NAME_BEHAVIOR.</p> <p>Changed from:</p> <p>A server SHOULD return a status of STATUS_INVALID_DEVICE_REQUEST when an FSCTL is not supported remotely or is not supported on the file system on which the file or directory handle specified by the FSCTL exists.<10><11></p> <p><11> Section 2.2: The following table lists FSCTLs that are not supported remotely and that, if received by the object store, will respond with a status code other than STATUS_INVALID_DEVICE_REQUEST, as specified in section 2.2.</p> <table><tr><th>FSCTL name</th><th>FSCTL function number</th><th>Status Code</th></tr><tr><td>...</td><td></td><td></td></tr><tr><td>FSCTL_FILE_PREFETCH</td><td>0x90120</td><td>STATUS_INVALID_PARAMETER</td></tr><tr><td>FSCTL_SET_SHORT_NAME_BEHAVIOR</td><td>0x901B4</td><td>STATUS_ACCESS_DENIED</td></tr><tr><td>...</td><td></td><td></td></tr></table> <p>Changed to:</p> <p>A server SHOULD return a status of STATUS_INVALID_DEVICE_REQUEST when an FSCTL is not supported remotely or is not supported on the file system on which the file or directory handle specified by the FSCTL exists.<10><11></p> <p><11> Section 2.2: The following table lists FSCTLs that are not supported remotely and that, if received by the object store, will respond with a status code other than STATUS_INVALID_DEVICE_REQUEST, as specified in section 2.2.</p> <table><tr><th>FSCTL name</th><th>FSCTL function number</th><th>Status Code</th></tr></table>	FSCTL name	FSCTL function number	Status Code	...			FSCTL_FILE_PREFETCH	0x90120	STATUS_INVALID_PARAMETER	FSCTL_SET_SHORT_NAME_BEHAVIOR	0x901B4	STATUS_ACCESS_DENIED	...			FSCTL name	FSCTL function number	Status Code
FSCTL name	FSCTL function number	Status Code																	
...																			
FSCTL_FILE_PREFETCH	0x90120	STATUS_INVALID_PARAMETER																	
FSCTL_SET_SHORT_NAME_BEHAVIOR	0x901B4	STATUS_ACCESS_DENIED																	
...																			
FSCTL name	FSCTL function number	Status Code																	

Errata Published*	Description											
	<table><tr><td>...</td><td></td><td></td></tr><tr><td>FSCTL_FILE_PREFETCH</td><td>0x90120</td><td>STATUS_INVALID_PARAMETER</td></tr><tr><td>...</td><td></td><td></td></tr></table>			...			FSCTL_FILE_PREFETCH	0x90120	STATUS_INVALID_PARAMETER	...		
...												
FSCTL_FILE_PREFETCH	0x90120	STATUS_INVALID_PARAMETER										
...												
2016/11/21	<p>In Section 2.1.5.9.15, FSCTL_IS_PATHNAME_VALID, changed from:</p> <p>This operation always returns STATUS_SUCCESS.</p> <p>Changed to:</p> <p>The FSCTL_IS_PATHNAME_VALID structure is defined in [MS-FSCC] section 2.3.25.</p> <p>This operation always returns STATUS_SUCCESS.</p> <p>In Section 2.1.5.9.17, FSCTL_LMR_SET_LINK_TRACKING_INFORMATION, changed from:</p> <p>This operation MUST be failed with STATUS_INVALID_DEVICE_REQUEST.</p> <p>Changed to:</p> <p>The FSCTL_LMR_SET_LINK_TRACKING_INFORMATION structure is defined in [MS-FSCC] section 2.3.27.1.</p> <p>This operation MUST be failed with STATUS_INVALID_DEVICE_REQUEST.</p>											
2016/11/07	<p>In Section 2.1.5.5.3, Directory Information Queries, the processing rules for an empty Open.QueryPattern were changed from:</p> <ul style="list-style-type: none">• If Open.QueryPattern is empty:<ul style="list-style-type: none">If FileNamePattern is empty:<ul style="list-style-type: none">Set FileNamePattern to "*".Else:<ul style="list-style-type: none">If FileNamePattern is not a valid filename component as described in [MS-FSCC] section 2.1.5, with the exceptions that wildcard characters described in section 2.1.4.3 are permitted and the strings "." and ".." are permitted, the operation MUST be failed with STATUS_OBJECT_NAME_INVALID. <p>EndIf</p> <p>Set Open.QueryPattern to FileNamePattern for use in subsequent queries.</p> <p>Else:</p> <p>FirstQuery = FALSE</p> <p>...</p> <p>Changed to:</p> <ul style="list-style-type: none">• If Open.QueryPattern is empty:<ul style="list-style-type: none">FirstQuery = TRUEElse:<ul style="list-style-type: none">FirstQuery = FALSE <p>EndIf</p>											

Errata Published*	Description
	<p>If FirstQuery is TRUE or (FileNamePattern is not empty and RestartScan is TRUE)<55> If FileNamePattern is empty: Set FileNamePattern to "*". Else: If FileNamePattern is not a valid filename component as described in [MS-FSCC] section 2.1.5, with the exceptions that wildcard characters described in section 2.1.4.3 are permitted and the strings "." and ".." are permitted, the operation MUST be failed with STATUS_OBJECT_NAME_INVALID. EndIf Set Open.QueryPattern to FileNamePattern for use in subsequent queries. Else: Set FileNamePattern to Open.QueryPattern. FirstQuery = FALSE <55> Section 2.1.5.5.3: Windows Vista operating system with Service Pack 1 (SP1), Windows Server 2008, Windows 7, and Windows Server 2008 R2 execute this portion only when FirstQuery is TRUE; the remaining conditions are ignored. This means the query pattern for a given Open cannot be changed once it is set. ...</p>
2016/11/07	<p>In Section 2.1.4.12, Algorithm to Check for an Oplock Break, the processing rules have been changed from:</p> <ul style="list-style-type: none"> • Indicate that the operation associated with WaitingOpen can continue according to the algorithm in section 2.1.4.12.1, setting OpenToRelease equal to WaitingOpen. <p>Changed to:</p> <ul style="list-style-type: none"> • Indicate that the operation associated with WaitingOpen can continues according to the algorithm in section 2.1.4.12.1, setting OpenToRelease equal to WaitingOpen. <p>In the processing rules shown below, the text in bold has been added:</p> <ul style="list-style-type: none"> • The operation that called this algorithm MUST be made cancelable by inserting it into CancelableOperations.CancelableOperationList. • Insert Open into Oplock.WaitList. • The operation that called this algorithm waits until the oplock break is acknowledged, as specified in section 2.1.5.18, or the operation is canceled. • The operation that called this algorithm MUST be made cancelable by inserting it into CancelableOperations.CancelableOperationList. • Insert Open into Oplock.WaitList. • The operation that called this algorithm waits until the oplock break is acknowledged, as specified in section 2.1.5.18, or the operation is canceled. • EndIf • EndCase • Case (READ_CACHING HANDLE_CACHING): • The operation that called this algorithm MUST be made cancelable by inserting it into

Errata Published*	Description
	CancelableOperations.CancelableOperationList. <ul style="list-style-type: none"> • Insert Open into Oplock.WaitList. • The operation that called this algorithm waits until the oplock break is acknowledged, as specified in section 2.1.5.18, or the operation is canceled.

*Date format: YYYY/MM/DD

[MS-FSCC]: File System Control Codes

This topic lists the Errata found in the MS-FSCC 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V40.0 - 2016/07/14](#).

Errata Published*	Description				
2017/02/20	In this document, Sections 2.1.5.9.16, FSCTL_LMR_GET_LINK_TRACKING_INFORMATION, and 2.1.5.17, FSCTL_LMR_SET_LINK_TRACKING_INFORMATION, were removed as those structures are not supported by SMB.				
2017/01/09	<p>Section 2.4.42, FileNotifyInformation, was located in the wrong section of the document. Created a new Section 2.7, Directory Change Notifications, and moved the information from Section 2.4.42, FileNotifyInformation, into that new section.</p> <p>Added:</p> <p>2.7 Directory Change Notifications</p> <p>The following definitions are part of the Directory Change Notification algorithm defined in [MS-FSA] section 2.1.5.10.</p> <p>2.7.1 FILE_NOTIFY_INFORMATION</p> <p>The FILE_NOTIFY_INFORMATION structure contains the changes for which the client is being notified. The structure consists of the following:</p> <p>...</p> <p>FileName (variable): A Unicode string with the name of the file that changed.</p> <p>As a consequence of this move, changed the reference in MS-FSA Section 2.1.1.9, Per NotifyEventEntry, to reference MS-FSCC section 2.7.1 instead of 2.4.42.</p> <p>In Section 5.4, NTFS Stream Names, corrected one of the NTFS Internal Stream Names from \$SII\Secure:\$SII:\$INDEX_ALLOCATION to \$SII.</p>				
2017/01/09	<p>In Section 2.3.8, FSCTL_DUPLICATE_EXTENTS_TO_FILE Reply, changed the description of error code STATUS_NOT_SUPPORTED from:</p> <table><tr><th>Error code</th><th>Meaning</th></tr><tr><td>STATUS_NOT_SUPPORTED 0xC00000BB</td><td><ul style="list-style-type: none">The source and target destination ranges overlap on the same file.Target file is sparse, while source is a non-</td></tr></table>	Error code	Meaning	STATUS_NOT_SUPPORTED 0xC00000BB	<ul style="list-style-type: none">The source and target destination ranges overlap on the same file.Target file is sparse, while source is a non-
Error code	Meaning				
STATUS_NOT_SUPPORTED 0xC00000BB	<ul style="list-style-type: none">The source and target destination ranges overlap on the same file.Target file is sparse, while source is a non-				

Errata Published*	Description						
	<table border="1" data-bbox="396 226 1430 464"> <tr> <td data-bbox="396 226 911 464"></td><td data-bbox="911 226 1430 464"> sparse file. <ul style="list-style-type: none"> • The source range is beyond the source file's allocation size. • The destination range extends beyond the target file's allocation size. The caller might need to increase the target's allocation size before using FSCTL_DUPLICATE_EXTENTS_TO_FILE. </td></tr> </table> <p>Changed to:</p> <table border="1" data-bbox="396 541 1430 787"> <tr> <th data-bbox="396 541 911 590">Error code</th><th data-bbox="911 541 1430 590">Meaning</th></tr> <tr> <td data-bbox="396 590 911 787">STATUS_NOT_SUPPORTED 0xC00000BB</td><td data-bbox="911 590 1430 787"> <ul style="list-style-type: none"> • The source and target destination ranges overlap on the same file. • Source file is sparse, while target is a non-sparse file. • The source range is beyond the source file's allocation size. </td></tr> </table>		sparse file. <ul style="list-style-type: none"> • The source range is beyond the source file's allocation size. • The destination range extends beyond the target file's allocation size. The caller might need to increase the target's allocation size before using FSCTL_DUPLICATE_EXTENTS_TO_FILE. 	Error code	Meaning	STATUS_NOT_SUPPORTED 0xC00000BB	<ul style="list-style-type: none"> • The source and target destination ranges overlap on the same file. • Source file is sparse, while target is a non-sparse file. • The source range is beyond the source file's allocation size.
	sparse file. <ul style="list-style-type: none"> • The source range is beyond the source file's allocation size. • The destination range extends beyond the target file's allocation size. The caller might need to increase the target's allocation size before using FSCTL_DUPLICATE_EXTENTS_TO_FILE. 						
Error code	Meaning						
STATUS_NOT_SUPPORTED 0xC00000BB	<ul style="list-style-type: none"> • The source and target destination ranges overlap on the same file. • Source file is sparse, while target is a non-sparse file. • The source range is beyond the source file's allocation size. 						
2016/12/19	<p>In section 2.3.8 FSCTL_DUPLICATE_EXTENTS_TO_FILE Reply, the second paragraph was changed from:</p> <p>Changed from:</p> <p>The only data item this message returns is a status code, as specified in [MS-ERREF] section 2.3. The status code returned directly by the function that processes this FSCTL MUST be STATUS_SUCCESS or one of the following.</p> <p>Changed to:</p> <p>The only data item this message returns is a status code, as specified in [MS-ERREF] section 2.3. The status code returned directly by the function that processes this FSCTL SHOULD<WBN> be STATUS_SUCCESS or one of the following.</p> <p><WBN> Windows Server returns STATUS_INVALID_HANDLE if the source file handle is closed, and STATUS_FILE_CLOSED if the target file handle is closed.</p>						
2016/08/29	<p>In Section 2.1.2.1, Reparse Tags, added a missing constant.</p> <p>Added:</p> <table border="1" data-bbox="396 1457 1414 1558"> <tr> <td data-bbox="396 1457 902 1558">IO_REPARSE_TAG_NFS 0x80000014</td><td data-bbox="902 1457 1414 1558">Used by the Network File System (NFS) component. Server-side interpretation only, not meaningful over the wire.</td></tr> </table>	IO_REPARSE_TAG_NFS 0x80000014	Used by the Network File System (NFS) component. Server-side interpretation only, not meaningful over the wire.				
IO_REPARSE_TAG_NFS 0x80000014	Used by the Network File System (NFS) component. Server-side interpretation only, not meaningful over the wire.						

*Date format: YYYY/MM/DD

[MS-FSRVP]: File Server Remote VSS Protocol

This topic lists the Errata found in the MS-FSRVP 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V10.0 - 2016/07/14](#).

Errata Published*	Description
2017/02/20	<p>In Section 3.1.4.12, DeleteShareMapping (Opnum 11), the processing rules have been changed from:</p> <p>If ShadowCopySet.Status is not "Recovered", the server MUST fail the call with FSRVP_E_BAD_STATE.</p> <p>Changed to:</p> <p>If ShadowCopySet.Status is not "Exposed" or "Recovered", the server MUST fail the call with FSRVP_E_BAD_STATE.</p>
2017/01/23	<p>In Section 3.1.4.12, DeleteShareMapping (Opnum 11), the second paragraph of the processing rules has been changed from:</p> <p>The server MUST look up the ShadowCopySet from GlobalShadowCopysetTable using the index ShadowCopySetId. If no shadow copy set is found, the server MUST fail the call with FSRVP_E_SHADOWCOPYSET_ID_MISMATCH.</p> <p>Changed to:</p> <p>The server MUST look up the ShadowCopySet from GlobalShadowCopysetTable using the index ShadowCopySetId. If no shadow copy set is found, the server MUST fail the call with FSRVP_E_OBJECT_NOT_FOUND.</p>

*Date format: YYYY/MM/DD

[MS-FSVCA]: File Set Version Comparison Algorithms

This topic lists the Errata found in the MS-FSVCA 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-GPPREF]: Group Policy: Preferences Extension Data Structure

This topic lists the Errata found in [MS-GPPREF] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-GPSB]: Group Policy: Security Protocol Extension

This topic lists the Errata found in [MS-GPSB] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-GPOL]: Group Policy: Core Protocol

This topic lists the Errata found in [MS-GPOL] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

Errata below are for Protocol Document Version [V33.0 – 2016/07/14](#).

Errata Published*	Description
2016/12/19	<p>The policy application process in Section 3.2.5.1 was modified:</p> <p>Changed from:</p> <p>Steps 3.2.5.1.3 through 3.2.5.1.7 SHOULD be performed while impersonating the policy target as specified in [MS-DTYP] section 2.7, Impersonation Abstract Interfaces. The successful completion of these steps ends with a Policy Application Notification. There is no Policy Application starting or failure notification.</p> <p>...</p> <p>Policy target impersonation proceeds as follows:</p> <ol style="list-style-type: none">1. For Computer Policy Application Mode, the Policy Source Mode MUST be set to Normal.2. The client application retrieves the primary token of the interactive user (the policy target) and passes it to the Start Impersonation abstract interface as specified in [MS-DTYP] section 2.7.1.3. The client application establishes an LDAP connection to the directory server. An LDAP bind request ([RFC2251] section 4.2, Bind Operation) is sent to the directory server with the credentials of an administrator. <p>Changed to:</p> <p>The steps in sections 3.2.5.1.3 through 3.2.5.1.7 are performed while impersonating the policy target as specified in [MS-DTYP] section 2.7, Impersonation Abstract Interfaces. The successful completion of these steps ends with a Policy Application Notification. There is no Policy Application starting or failure notification.</p> <p>...</p> <p>Policy target impersonation proceeds as follows:</p> <ol style="list-style-type: none">1. For Computer Policy Application Mode, the Policy Source Mode MUST be set to Normal.2. The client application retrieves the primary token of the interactive user (the policy target) during user policy application or retrieves the machine token of the computer (the policy target) during computer policy application. It then passes the token to the Start Impersonation abstract interface as specified in [MS-DTYP] section 2.7.1.3. The client application establishes an LDAP connection to the directory server. An LDAP bind request ([RFC2251] section 4.2, Bind Operation) is sent to the directory server with the credentials of the policy target.

*Date format: YYYY/MM/DD

[MS-GSSA]: Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG) Protocol Extension

This topic lists the Errata found in the MS-GSSA 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.

Errata below are for Protocol Document Version [V8.0 – 2016/07/14](#).

Errata Published*	Description
2016/08/29	<p>A new section, 3.1.5.4, Domain Name Compression, has been added to discuss domain name compression.</p> <p>Added:</p> <p>3.1.5.4 Domain Name Compression</p> <p>As described in [RFC1123] section 6.1.2.4, name servers MUST use compression in responses. For TSIG resource record in DNS response messages, compression is not supported.</p>

*Date format: YYYY/MM/DD

[MS-HTTPE]: Hypertext Transfer Protocol (HTTP) Extensions

This topic lists the Errata found in [MS-HTTPE] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-HVRS]: Hyper-V Remote Storage Profile

This topic lists the Errata found in [MS-HVRS] 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.

Errata below are for Protocol Document Version [V1.0 - 2016/07/14](#).

Errata Published*	Description
2016/12/19	<p>In Section 2.2.3, [MS-RSVD] Remote Shared Virtual Disk Protocol, added the following: 2.3.</p> <p>If the server doesn't support version 2 of the Remote Shared Virtual Disk Protocol [MS-RSVD]:</p> <ul style="list-style-type: none">• The backup operation of a remote shared virtual disk, including checkpoints and resilient change tracking, fails.• The replica operation of a remote shared virtual disk fails.• Resizing a remote shared virtual disk fails.

*Date format: YYYY/MM/DD

[MS-ICPR]: ICertPassage Remote Protocol

This topic lists the Errata found in the MS-ICPR 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-IKEE]: Internet Key Exchange Protocol Extensions

This topic lists the Errata found in the MS-IKEE 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-IPAMM2]: IP Address Management (IPAM) Management Protocol Version 2

This topic lists the Errata found in [MS-IPAMM2] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V6.0 - 2016/07/14](#).

Errata Published*	Description														
2017/03/06	<p>In this document, made numerous changes, including:</p> <ul style="list-style-type: none">• Correcting type name mismatches and capitalization errors.• Adding missing elements and tags.• Correcting mismatches between the code snippets in Section 2 and the IDL in the Appendix. <p>For details on the changes, see the Diff PDF document at https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-IPAMM2/[MS-IPAMM2]-170306-diff.pdf.</p>														
2017/02/06	<p>In Section 3.5.4.8.1, Enumeration Processing Logic, removed parameter IPAAuditEnumerationParameters, object type IPAAudit, as the parameter is already described correctly in section 3.9.</p> <p>Changed from:</p> <table><tr><th>Enumeration Parameter Type</th><th>Object Type</th></tr><tr><td>...</td><td>...</td></tr><tr><td>IpamProvisioningEnumerationParameters</td><td>Provisioning</td></tr><tr><td>IPAAuditEnumerationParameters</td><td>IPAAudit</td></tr><tr><td>IPBlockChildBlockEnumerationParameters</td><td>IPBlock</td></tr><tr><td>...</td><td>...</td></tr></table> <p>Changed to:</p> <table><tr><th>Enumeration Parameter Type</th><th>Object Type</th></tr></table>	Enumeration Parameter Type	Object Type	IpamProvisioningEnumerationParameters	Provisioning	IPAAuditEnumerationParameters	IPAAudit	IPBlockChildBlockEnumerationParameters	IPBlock	Enumeration Parameter Type	Object Type
Enumeration Parameter Type	Object Type														
...	...														
IpamProvisioningEnumerationParameters	Provisioning														
IPAAuditEnumerationParameters	IPAAudit														
IPBlockChildBlockEnumerationParameters	IPBlock														
...	...														
Enumeration Parameter Type	Object Type														

Errata Published*	Description																												
	<table> <tr><td data-bbox="365 258 906 300">...</td><td data-bbox="906 258 1437 300">...</td></tr> <tr><td data-bbox="365 300 906 352">IpamProvisioningEnumerationParameters</td><td data-bbox="906 300 1437 352">Provisioning</td></tr> <tr><td data-bbox="365 352 906 405">IPBlockChildBlockEnumerationParameters</td><td data-bbox="906 352 1437 405">IPBlock</td></tr> <tr><td data-bbox="365 405 906 457">...</td><td data-bbox="906 405 1437 457">...</td></tr> </table>	IpamProvisioningEnumerationParameters	Provisioning	IPBlockChildBlockEnumerationParameters	IPBlock																				
...	...																												
IpamProvisioningEnumerationParameters	Provisioning																												
IPBlockChildBlockEnumerationParameters	IPBlock																												
...	...																												
2016/12/05	<p data-bbox="349 468 1437 531">In Section 3.5.4.8.1, Enumeration Processing Logic, deleted one Enumeration Parameter Type and added 7 others as shown below (deletions shown as strikeouts, additions in bold font):</p> <table data-bbox="365 562 1437 1352"> <tr> <th data-bbox="365 562 1136 615">Enumeration Parameter Type</th><th data-bbox="1136 562 1437 615">Object Type</th></tr> <tr><td data-bbox="365 615 1136 667">...</td><td data-bbox="1136 615 1437 667"></td></tr> <tr><td data-bbox="365 667 1136 720">DhcpScopeObjectSpecificEnumerationParameters</td><td data-bbox="1136 667 1437 720">DhcpScope</td></tr> <tr><td data-bbox="365 720 1136 772">...</td><td data-bbox="1136 720 1437 772"></td></tr> <tr><td data-bbox="365 772 1136 825">DiscoverySubnetEnumerationParameters</td><td data-bbox="1136 772 1437 825">DiscoveredSubnets</td></tr> <tr><td data-bbox="365 825 1136 898">DnsConditionalForwarderEnumerationParameters</td><td data-bbox="1136 825 1437 898">DnsConditionalForwarder</td></tr> <tr><td data-bbox="365 898 1136 951">DnsResourceRecordEnumerationParameters</td><td data-bbox="1136 898 1437 951">DnsResourceRecord</td></tr> <tr><td data-bbox="365 951 1136 1003">...</td><td data-bbox="1136 951 1437 1003"></td></tr> <tr><td data-bbox="365 1003 1136 1056">UnmappedIpamIPAddressForLogicalGroupEnumerationParameters</td><td data-bbox="1136 1003 1437 1056">IPAddress</td></tr> <tr><td data-bbox="365 1056 1136 1108">DhcpScopeObjectSpecificEnumerationParameters</td><td data-bbox="1136 1056 1437 1108">DhcpScope</td></tr> <tr><td data-bbox="365 1108 1136 1161">DhcpScopeByPrefixAndServerNameEnumerationParameters</td><td data-bbox="1136 1108 1437 1161">DhcpScope</td></tr> <tr><td data-bbox="365 1161 1136 1234">DhcpSuperscopeBySuperscopeAndServerNameEnumerationParameters</td><td data-bbox="1136 1161 1437 1234">DHCPSuperscope</td></tr> <tr><td data-bbox="365 1234 1136 1308">DnsConditionalForwarderByFiltersEnumerationParameters</td><td data-bbox="1136 1234 1437 1308">DnsConditionalForwarder</td></tr> <tr><td data-bbox="365 1308 1136 1352">DnsResourceRecordFilterEnumerationParameters</td><td data-bbox="1136 1308 1437 1352">DnsResourceRecord</td></tr> </table>	Enumeration Parameter Type	Object Type	...		DhcpScopeObjectSpecificEnumerationParameters	DhcpScope	...		DiscoverySubnetEnumerationParameters	DiscoveredSubnets	DnsConditionalForwarderEnumerationParameters	DnsConditionalForwarder	DnsResourceRecordEnumerationParameters	DnsResourceRecord	...		UnmappedIpamIPAddressForLogicalGroupEnumerationParameters	IPAddress	DhcpScopeObjectSpecificEnumerationParameters	DhcpScope	DhcpScopeByPrefixAndServerNameEnumerationParameters	DhcpScope	DhcpSuperscopeBySuperscopeAndServerNameEnumerationParameters	DHCPSuperscope	DnsConditionalForwarderByFiltersEnumerationParameters	DnsConditionalForwarder	DnsResourceRecordFilterEnumerationParameters	DnsResourceRecord
Enumeration Parameter Type	Object Type																												
...																													
DhcpScopeObjectSpecificEnumerationParameters	DhcpScope																												
...																													
DiscoverySubnetEnumerationParameters	DiscoveredSubnets																												
DnsConditionalForwarderEnumerationParameters	DnsConditionalForwarder																												
DnsResourceRecordEnumerationParameters	DnsResourceRecord																												
...																													
UnmappedIpamIPAddressForLogicalGroupEnumerationParameters	IPAddress																												
DhcpScopeObjectSpecificEnumerationParameters	DhcpScope																												
DhcpScopeByPrefixAndServerNameEnumerationParameters	DhcpScope																												
DhcpSuperscopeBySuperscopeAndServerNameEnumerationParameters	DHCPSuperscope																												
DnsConditionalForwarderByFiltersEnumerationParameters	DnsConditionalForwarder																												
DnsResourceRecordFilterEnumerationParameters	DnsResourceRecord																												

*Date format: YYYY/MM/DD

[MS-IRP]: Internet Information Services (IIS) Inetinfo Remote Protocol

This topic lists the Errata found in [MS-IRP] 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.

Errata below are for Protocol Document Version [V7.0 – 2016/07/14](#).

Errata Published*	Description
2016/11/21	<p>In Section 3.1.5.1, R_InetInfoGetVersion (Opnum 0), changed MAY to SHOULD regarding the value that is returned in the pdwVersion pointer and modified the corresponding product behavior note.</p> <p>Changed from:</p> <p>The value returned in pdwVersion MAY correspond to the version of the Internet protocol servers managed by the Internet Information Services (IIS) Inetinfo Remote Protocol server.<9>.</p> <p><9> Section 3.1.5.1: The Windows implementation of R_InetInfoGetVersion returns Major Version = 5 and Minor Version = 1 for implementations of IIS released on Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2 operating system, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows Server 2016.</p> <p>Changed to:</p> <p>The value returned in pdwVersion SHOULD<9> correspond to the version of the Internet protocol servers managed by the Internet Information Services (IIS) Inetinfo Remote Protocol server.</p> <p><9> Section 3.1.5.1: The Windows implementation of R_InetInfoGetVersion does not return Major Version = 5 and Minor Version = 1 for implementations of IIS released on Windows NT 4.0, Windows 2000 Professional, and Windows 2000 Server.</p> <p>In Section 7, Appendix B: Product Behavior, changed references to the "Windows 2000 operating system" to "Windows 2000 Professional" and "Windows 2000 Server".</p>

*Date format: YYYY/MM/DD

[MS-KILE]: Kerberos Protocol Extensions

This topic lists the Errata found in [MS-KILE] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-LSAD]: Local Security Authority (Domain Policy) Remote Protocol

This topic lists the Errata found in [MS-LSAT] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-LSAT]: Local Security Authority (Translation Methods) Remote Protocol

This topic lists the Errata found in [MS-LSAT] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V27.0 - 2016/07/14](#).

Errata Published*	Description												
2017/01/23	<p>In the following product behavior notes, added Windows XP to the product version information about the second flag (0x00000002) in three structures:</p> <ul style="list-style-type: none">-- Behavior note <11> (for Section 2.2.21, LSAPR_TRANSLATED_NAME_EX)-- Behavior note <13> (for Section 2.2.23, LSAPR_TRANSLATED_SID_EX)-- Behavior note <15> (for Section 2.2.25, LSAPR_TRANSLATED_SID_EX2) <p>Changed from:</p> <table><thead><tr><th>Flag value</th><th>Windows version</th></tr></thead><tbody><tr><td>...</td><td>...</td></tr><tr><td>0x00000002</td><td>Windows Server 2003</td></tr></tbody></table> <p>Changed to:</p> <table><thead><tr><th>Flag value</th><th>Windows version</th></tr></thead><tbody><tr><td>...</td><td>...</td></tr><tr><td>0x00000002</td><td>Windows XP, Windows Server 2003</td></tr></tbody></table>	Flag value	Windows version	0x00000002	Windows Server 2003	Flag value	Windows version	0x00000002	Windows XP, Windows Server 2003
Flag value	Windows version												
...	...												
0x00000002	Windows Server 2003												
Flag value	Windows version												
...	...												
0x00000002	Windows XP, Windows Server 2003												

*Date format: YYYY/MM/DD

[MS-MDE]: Mobile Device Enrollment Protocol

This topic lists the Errata found in [MS-MDE] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-MDE2]: Mobile Device Enrollment Protocol Version 2

This topic lists the Errata found in [MS-MDE2] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-MDM]: Mobile Device Management Protocol

This topic lists the Errata found in [MS-MDM] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-MWBE]: Microsoft Web Browser Federated Sign-On Protocol Extensions

This topic lists the Errata found in [MS-MWBE] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive [here](#).

[MS-MWBF]: Microsoft Web Browser Federated Sign-On Protocol

This topic lists the Errata found in [MS-MWBF] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V11.0 – 2016/07/14](#).

Errata Published*	Description
2016/08/04 (updated) 2016/07/18	<p>In three sections, added and updated information about the prompt URI parameter regarding its existing behavior and behavior that is modified through KB/QFE 3172614.</p> <p>In Section 1.2.1, Normative References, included the following reference: [MSKB-3172614] Microsoft Corporation, "July 2016 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2", https://support.microsoft.com/en-us/kb/3172614</p> <p>In Section 2.2.3, wsignin1.0 Request Message, changed from:</p> <p>...</p> <ul style="list-style-type: none">• prompt (optional): This query parameter is used in the same way as the prompt parameter defined in [OIDCCore] section 3.1.2.1, but the only accepted value for this parameter is "login".<20> Any other values are ignored. This parameter is used to interactively prompt the end-user for re-authentication. Error handling for this parameter follows the specification of section 3.1.5.2. <p>...</p> <p><20> Section 2.2.3: The prompt parameter is not supported on Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2. Additionally, it is supported only in AD FS server with AD FS behavior level set to AD_FS_BEHAVIOR_LEVEL_2 or higher, and ignored otherwise.</p> <p>Changed to:</p> <p>...</p> <ul style="list-style-type: none">• prompt (optional): This query parameter is used in the same way as the prompt parameter defined in [OIDCCore] section 3.1.2.1, but the only accepted value for this parameter is "login".<20> Any other values are ignored. This parameter is used to interactively prompt the end-user for re-authentication. Error handling for this parameter follows the specification of section 3.1.5.2. <p>...</p> <p><20> Section 2.2.3: The prompt parameter is not supported on Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012. It is also not supported on Windows Server 2012 R2 unless [MSKB-3172614] is installed.</p> <p>In Section 3.1.5.3.4, Message Transmission, changed from:</p> <p>...</p> <p>The following are recommended best practices:</p> <ul style="list-style-type: none">• Upon forwarding the wsignin1.0 request, the resource IP/STS SHOULD use only the parameters

Errata Published*	Description
	<p>that are supported by the requestor IP/STS behavior level. The resource IP/STS can track the requestor IP/STS behavior level and choose the forwarding behavior accordingly. Behavior-level tracking is implementation specific.</p> <ul style="list-style-type: none"> • For a resource IP/STS with the <code>ad_fs_behavior_level</code> ADM element, as defined in [MS-OAPX] section 3.2.1.1 (hereafter referred to simply as the AD FS behavior level) set to <code>AD_FS_BEHAVIOR_LEVEL_2</code> or higher, if it receives the prompt parameter and knows that the requestor IP/STS AD FS behavior level is lower than <code>AD_FS_BEHAVIOR_LEVEL_2</code>, the resource IP/STS SHOULD send a <code>wsignin1.0</code> request using the protocol-specific parameters (for example, <code>wfresh</code> and <code>wauth</code>) to facilitate a fresh and interactive authentication.... <p>Changed to:</p> <p>...</p> <p>The <code>ad_fs_behavior_level</code> ADM element is defined in [MS-OAPX] section 3.2.1.1 and is hereafter referred to simply as the AD FS behavior level. [MS-OAPX] section 3.2.1.1 also includes information about how the AD FS behavior level relates to product versions. The following are recommended best practices related to the AD FS behavior level:</p> <ul style="list-style-type: none"> • Upon forwarding the <code>wsignin1.0</code> request, the resource IP/STS SHOULD use only the parameters that are supported by the requestor IP/STS AD FS behavior level. The resource IP/STS can track the requestor IP/STS AD FS behavior level and choose the forwarding behavior accordingly. Behavior-level tracking is implementation specific. • If a resource IP/STS that supports the prompt parameter receives the prompt parameter and knows that the requestor IP/STS does not support the prompt parameter, the resource IP/STS SHOULD send a <code>wsignin1.0</code> request using the protocol-specific parameters (for example, <code>wfresh</code> and <code>wauth</code>) to facilitate a fresh and interactive authentication. <p>Note Support for the prompt parameter depends on the AD FS behavior level and the product version. See section 2.2.3 for support information. If the parameter is not supported by the AD FS server, it is ignored.</p> <p>...</p>

*Date format: YYYY/MM/DD

[MS-NCT]: Network Cost Transfer Protocol

This topic lists the Errata found in the MS-NCT 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.

Errata below are for Protocol Document Version [V1.0 - 2016/07/14](#).

Errata Published*	Description																					
2017/02/20	<p>In Section 2.2.1.1, Cost Flags, added the 0x00 cost flag value to the table.</p> <p>Changed from:</p> <table><tr><th>Value</th><th>Name</th><th>Description</th></tr><tr><td>0x01</td><td>Over Data Limit</td><td>Usage has exceeded the data limit of the metered network; different network costs or conditions might apply.</td></tr><tr><td>...</td><td>...</td><td>...</td></tr></table> <p>Changed to:</p> <table><tr><th>Value</th><th>Name</th><th>Description</th></tr><tr><td>0x00</td><td>Unknown</td><td>The usage is unknown or unrestricted.</td></tr><tr><td>0x01</td><td>Over Data Limit</td><td>Usage has exceeded the data limit of the metered network; different network costs or conditions might apply.</td></tr><tr><td>...</td><td>...</td><td>...</td></tr></table>	Value	Name	Description	0x01	Over Data Limit	Usage has exceeded the data limit of the metered network; different network costs or conditions might apply.	Value	Name	Description	0x00	Unknown	The usage is unknown or unrestricted.	0x01	Over Data Limit	Usage has exceeded the data limit of the metered network; different network costs or conditions might apply.
Value	Name	Description																				
0x01	Over Data Limit	Usage has exceeded the data limit of the metered network; different network costs or conditions might apply.																				
...																				
Value	Name	Description																				
0x00	Unknown	The usage is unknown or unrestricted.																				
0x01	Over Data Limit	Usage has exceeded the data limit of the metered network; different network costs or conditions might apply.																				
...																				

*Date format: YYYY/MM/DD

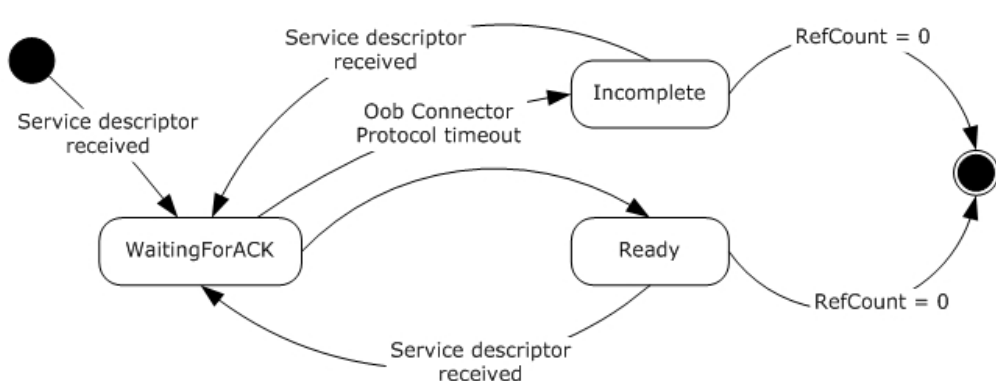
[MS-NFPB]: Near Field Proximity Bidirectional Services Protocol

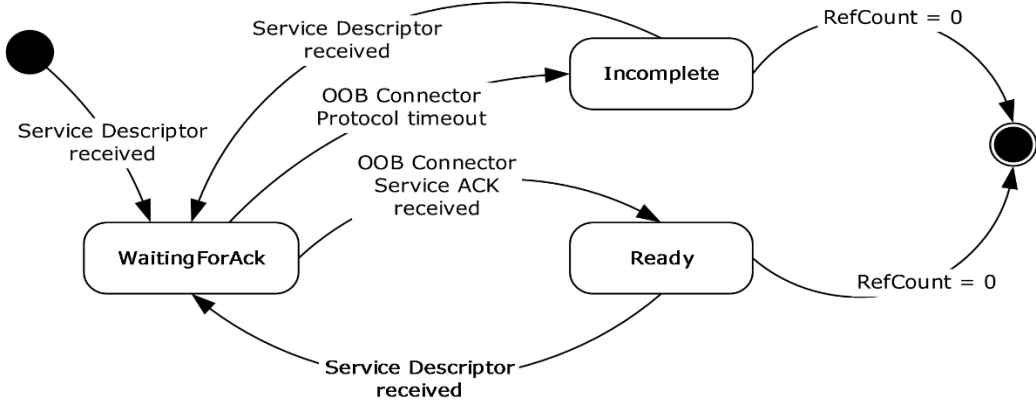
This topic lists the Errata found in [MS-NFPB] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

Errata below are for Protocol Document Version [V7.0 - 2016/07/14](#).

Errata Published *	Description
2017/02/20	<p>In Section 3.1.1.2 OOB, Connector Object, updated the OOB Connector state transitions: Connector role figure to show "WaitingForACK" transits to the state "Ready".</p> <p>Changed from:</p>  <p>Figure 4: OOB Connector state transitions: Connector role</p> <p>Changed to:</p>

Errata Published *	Description
	 <p>Figure 4: OOB Connector state transitions: Connector role</p>
2016/12/05	<p>In two sections, corrected a field name and an object name.</p> <p>In Section 2.2.3, Extension Structure, in the description for field ExtensionDataSize, changed "Extension Data" to "ExtensionData".</p> <p>In Section 2.2.12, Session Factory Service Activation Message, in the description for field ReplyChannelID, changed "SessionFactory" to "Session Factory".</p>

*Date format: YYYY/MM/DD

[MS-NFPS]: Near Field Proximity Sharing Protocol

This topic lists the Errata found in [MS-NFPS] 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.

Errata below are for Protocol Document Version [V3.0 - 2016/07/14](#).

Errata Published *	Description
2017/02/20	<p>In Section 3.2.1, Abstract Data, updated the Share sender state transitions figure to match the State table.</p> <p>Changed from:</p> <p>Figure 3: Share sender state transitions</p> <p>Changed to:</p> <p>Figure 3: Share sender state transitions</p>

*Date format: YYYY/MM/DD

[MS-NKPU]: Network Key Protector Unlock Protocol

This topic lists the Errata found in [MS-NKPU] 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.

Errata below are for Protocol Document Version [V5.0 - 2016/07/14](#).

Errata Published*	Description
2016/10/10	<p>In two sections, clarified the AES-CCM parameters for encryption in the Encrypted Buffer Suboption field.</p> <p>In Section 2.2.1.2, DHCPv6 Vendor Specific Information Option Structure, changed from:</p> <p>...</p> <p>Encrypted Buffer Suboption:</p> <p>Opt-Code (2 bytes): This field MUST be set to 2 (0x0002).</p> <p>Option-Len (2 bytes): In the client request, this field MUST be set to 256 (0x0100), which is the length of the KP ADM element data. In the server response, this field MUST be set to 32 (0x20), which is the length of the CK ADM element data encrypted with the SK ADM element content.</p> <p>Option-Data: In a client request, this field contains the KP ADM element data. In a server response, this field contains the CK ADM element data encrypted with the SK ADM element content.</p> <p>When both suboptions are present, the Certificate Thumbprint Suboption MUST come before the Encrypted Buffer Suboption.</p> <p>Changed to:</p> <p>...</p> <p>Encrypted Buffer Suboption:</p> <p>Opt-Code (2 bytes): This field MUST be set to 2 (0x0002).</p> <p>Option-Len (2 bytes): In the client request, this field MUST be set to 256 (0x0100), which is the length of the KP ADM element data. In the server response, this field MUST be set to 32 (0x20), which is the length of the CK ADM element data encrypted with the SK ADM element content.</p> <p>Option-Data: In a client request, this field contains the KP ADM element data. In a server response, this field contains the CK ADM element data that is encrypted with the SK ADM element content by using the AES-CCM [FIPS197] [RFC3610] mode of encryption without authentication data and the MAC containing the first 16 bytes of encrypted data. The nonce used is 12 bytes, all zeros, and is not transmitted.</p> <p>When both suboptions are present, the Certificate Thumbprint Suboption MUST come before the Encrypted Buffer Suboption.</p> <p>In Section 2.2.1.4, DHCPv4 Vendor Specific Information Option Structure, changed from:</p>

Errata Published*	Description
	<p>...</p> <p>Encrypted Buffer Suboption: Suboption Code (1 byte): This field MUST be set to 2 (0x02). Suboption Length (1 byte): In the client request, this field MUST be set to 128 (0x80), which is half the length of the KP ADM element data. In the server response, this field MUST be set to 32 (0x20), which is the length of the CK ADM element data encrypted with the SK ADM element content. Suboption Data: In a client request, this field contains the first 128 bytes of the KP ADM element data. In a server response, this field contains the CK ADM element data encrypted with the SK ADM element data.</p> <p>Changed to:</p> <p>...</p> <p>Encrypted Buffer Suboption: Suboption Code (1 byte): This field MUST be set to 2 (0x02). Suboption Length (1 byte): In the client request, this field MUST be set to 128 (0x80), which is half the length of the KP ADM element data. In the server response, this field MUST be set to 32 (0x20), which is the length of the CK ADM element data encrypted with the SK ADM element content. Suboption Data: In a client request, this field contains the first 128 bytes of the KP ADM element data. In a server response, this field contains the CK ADM element data that is encrypted with the SK ADM element data by using the AES-CCM [FIPS197] [RFC3610] mode of encryption without authentication data and the MAC containing the first 16 bytes of encrypted data. The nonce used is 12 bytes, all zeros, and is not transmitted.</p>

*Date format: YYYY/MM/DD

[MS-NLMP]: NT LAN Manager (NTLM) Authentication Protocol

This topic lists the Errata found in [MS-NLMP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-NNS]: .NET NegotiateStream Protocol

This topic lists the Errata found in [MS-NNS] 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.

Errata below are for Protocol Document Version [V6.0 – 2016/07/14](#).

Errata Published*	Description
2016/07/18	<p>In Section 2.2.2, Data Message, changed from:</p> <p>This section defines the structure of the data exchange messages. These messages are used to transfer application-specific data after the handshake phase is complete. The .NET NegotiateStream Protocol only frames application data using the format noted in the following table if the negotiation of security services during the handshake phase resulted in both the client and server agreeing to sign or encrypt and sign the data to be transferred. Thus, if the negotiated security context in the handshake phase results in a context that does not support message confidentiality or integrity, then the data transferred is not framed, and does not follow the format specified in this section (that is, application-supplied data is written directly to the underlying TCP stream).</p> <p>Changed to (change in bold):</p> <p>This section defines the structure of the data exchange messages. These messages are used to transfer application-specific data after the handshake phase is complete. The .NET NegotiateStream Protocol only frames application data using the format noted in the following table if the negotiation of security services during the handshake phase resulted in both the client and server agreeing to sign or encrypt and sign the data to be transferred. Thus, if the negotiated security context in the handshake phase results in a context that supports neither message confidentiality nor integrity, then the data transferred is not framed, and does not follow the format specified in this section (that is, application-supplied data is written directly to the underlying TCP stream).</p> <p>In Section 3.1.4.1, Application Invocation of the .NET NegotiateStream Protocol, changed from:</p> <p>...</p> <p>If the function returns any major_status other than GSS_S_COMPLETE, the implementation MUST notify the application of the failure without sending anything over the Underlying TCP Connection. Otherwise, the implementation MUST store the returned credential handle as the Client Credentials, and MUST set the Stream State to CreatingSecurityToken. The implementation MUST pass the Client Credentials to the GSS_Init_sec_context function ([RFC2743] section 2.2.1). The input_context_handle parameter MUST be GSS_C_NO_CONTEXT. The targ_name parameter MUST be the Target Name. The mech_type parameter MUST be the same as that passed to GSS_Acquire_cred. The deleg_req_flag MUST be true if and only if Allowed Impersonation Level is Delegation. The conf_req_flag MUST be true if and only if the Required Protection Level is EncryptAndSign. The integ_req_flag MUST be true if and only if the Required Protection Level is Sign or EncryptAndSign. The mutual_req_flag, replay_det_req_flag, and sequence_req_flag MUST be true. The anon_req_flag MUST be false. The chan_bindings parameter MUST be the Channel Binding Token. The input_token MUST be NULL, and the lifetime_req MUST be 0.</p> <p>Changed to:</p> <p>...</p> <p>If the function returns any major_status other than GSS_S_COMPLETE, the implementation MUST notify the application of the failure without sending anything over the Underlying TCP</p>

Errata Published*	Description
	<p>Connection. Otherwise, the implementation MUST store the returned credential handle as the Client Credentials, and MUST set the Stream State to CreatingSecurityToken. The implementation MUST pass the Client Credentials to the GSS_Init_sec_context function ([RFC2743] section 2.2.1). The input_context_handle parameter MUST be GSS_C_NO_CONTEXT. The targ_name parameter MUST be the Target Name. The mech_type parameter MUST be the same as that passed to GSS_Acquire_cred. The deleg_req_flag MUST be true if and only if Allowed Impersonation Level is Delegation. The conf_req_flag MUST be true if and only if the Required Protection Level is EncryptAndSign. The integ_req_flag MUST be true if and only if the Required Protection Level is Sign or EncryptAndSign. The mutual_req_flag, replay_det_req_flag, and sequence_req_flag MUST be true. The anon_req_flag MUST be false. The chan_bindings parameter MUST be the Channel Binding Token. The input_token MUST be NULL, and the lifetime_req MUST be 0.</p> <p>If the conf_avail return value is true, the integ_avail return value MUST also be true, and the Negotiated Protection Level is EncryptAndSign. If the conf_avail return value is false and the integ_avail return value is true, the Negotiated Protection Level is Sign. Otherwise, the Negotiated Protection Level is None.</p>

*Date format: YYYY/MM/DD

[MS-NRPC]: Netlogon Remote Protocol

This topic lists the Errata found in [MS-NRPC] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-OAPX]: OAuth 2.0 Protocol Extensions

This topic lists the Errata found in [MS-OAPX] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V4.0 – 2016/07/14](#).

Errata Published*	Description																								
2016/12/19	<p>Revisions have been applied to MS-OAPX, and client applicability for this protocol has been added. Please see the following sections:</p> <p>Section 1.2.1</p> <p>Added:</p> <p>[MSFT-WKPLJOIN] Microsoft Corporation, "Microsoft Workplace Join for non-Windows 10 computers", https://www.microsoft.com/en-us/download/details.aspx?id=53554</p> <p>Section 1.6</p> <p>Changed from:</p> <p>OAuth 2.0 clients that request authorization using the OAuth 2.0 protocol are required to implement the mandatory extensions defined in this protocol document.</p> <p>Changed to:</p> <p>OAuth 2.0 clients that request authorization using the OAuth 2.0 protocol are required to implement the mandatory extensions defined in this protocol document.<2></p> <p>Appendix B</p> <p>Changed from:</p> <ul style="list-style-type: none">· Windows Server 2012 R2 operating system· Windows Server 2016 operating system <p>Changed to:</p> <p>The following tables show the relationships between Microsoft product versions or supplemental software and the roles they perform.</p> <table><tr><th>Windows Client</th><th>Client role</th><th>Server role</th></tr><tr><td>Windows 7 operating system</td><td>Yes</td><td>No</td></tr><tr><td>Windows 8 operating system</td><td>Yes</td><td>No</td></tr><tr><td>Windows 8.1 operating system</td><td>Yes</td><td>No</td></tr><tr><td>Windows 10 operating system</td><td>Yes</td><td>No</td></tr></table> <table><tr><th>Windows Server</th><th>Client role</th><th>Server role</th></tr><tr><td>Windows Server 2008 operating system</td><td>Yes</td><td>No</td></tr><tr><td>Windows Server 2008 R2 operating system</td><td>Yes</td><td>No</td></tr></table>	Windows Client	Client role	Server role	Windows 7 operating system	Yes	No	Windows 8 operating system	Yes	No	Windows 8.1 operating system	Yes	No	Windows 10 operating system	Yes	No	Windows Server	Client role	Server role	Windows Server 2008 operating system	Yes	No	Windows Server 2008 R2 operating system	Yes	No
Windows Client	Client role	Server role																							
Windows 7 operating system	Yes	No																							
Windows 8 operating system	Yes	No																							
Windows 8.1 operating system	Yes	No																							
Windows 10 operating system	Yes	No																							
Windows Server	Client role	Server role																							
Windows Server 2008 operating system	Yes	No																							
Windows Server 2008 R2 operating system	Yes	No																							

Errata Published*	Description										
	Windows Server 2012 operating system	Yes	No								
	Windows Server 2012 R2 operating system	Yes	Yes								
	Windows Server 2016 operating system	Yes	Yes								
	Added: <2> Section 1.6: OAuth 2.0 clients running on Windows 8.1 and later implement these mandatory extensions by default. OAuth 2.0 clients running on Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 implement these mandatory extensions if [MSFT-WKPLJOIN] is installed. However, even with [MSFT-WKPLJOIN] installed, these products support only the resource and resource_params URI parameters. Changed from: <2> Section 2.2.2: The prompt parameter is not supported on Windows Server 2012 R2 unless [MSKB-3172614] is installed. Even with [MSKB-3172614] installed, the "none" value for the parameter is not supported on Windows Server 2012 R2. Changed to: <3> Section 2.2.2: The prompt parameter is not supported on Windows Server 2012 R2 unless [MSKB-3172614] is installed. Even with [MSKB-3172614] installed, the "none" value for the parameter is not supported on Windows Server 2012 R2. The prompt parameter is not supported on Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012.										
2016/08/04 (updated) 2016/07/18	In several sections, added and updated information about the prompt URI parameter regarding its existing behavior and behavior that is modified through KB/QFE 3172614. In Section 1.2.1, Normative References, included the following reference: [MSKB-3172614] Microsoft Corporation, "July 2016 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2", https://support.microsoft.com/en-us/kb/3172614. In Section 2.2.2, Common URI Parameters, changed from: <table><tr><th>URI parameter</th><th>Description</th></tr><tr><td>prompt</td><td>OPTIONAL. This query parameter is used in the same way as the prompt parameter defined in [OIDCCore] section 3.1.2.1. The AD FS server ignores this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher.</td></tr></table> Changed to: <table><tr><th>URI parameter</th><th>Description</th></tr><tr><td>prompt</td><td>OPTIONAL. This query parameter is used in the same way as the prompt parameter defined in [OIDCCore] section 3.1.2.1, but the only accepted values for this parameter are "none" and "login". This parameter and the accepted values specified above SHOULD<2> be supported for all values of ad_fs_behavior_level.</td></tr></table> <2> Section 2.2.2: The prompt parameter is not supported on Windows Server 2012 R2 unless [MSKB-3172614] is installed. Even with [MSKB-3172614] installed, the "none" value for the			URI parameter	Description	prompt	OPTIONAL. This query parameter is used in the same way as the prompt parameter defined in [OIDCCore] section 3.1.2.1. The AD FS server ignores this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher.	URI parameter	Description	prompt	OPTIONAL. This query parameter is used in the same way as the prompt parameter defined in [OIDCCore] section 3.1.2.1, but the only accepted values for this parameter are "none" and "login". This parameter and the accepted values specified above SHOULD<2> be supported for all values of ad_fs_behavior_level.
URI parameter	Description										
prompt	OPTIONAL. This query parameter is used in the same way as the prompt parameter defined in [OIDCCore] section 3.1.2.1. The AD FS server ignores this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher.										
URI parameter	Description										
prompt	OPTIONAL. This query parameter is used in the same way as the prompt parameter defined in [OIDCCore] section 3.1.2.1, but the only accepted values for this parameter are "none" and "login". This parameter and the accepted values specified above SHOULD<2> be supported for all values of ad_fs_behavior_level.										

Errata Published*	Description
	<p>parameter is not supported on Windows Server 2012 R2.</p> <p>In Section 2.2.2.7, prompt, changed from:</p> <p>...</p> <p>The prompt query parameter is OPTIONAL, and can be specified by the client role of the OAuth 2.0 Protocol Extensions. This parameter has the same behavior as the prompt parameter defined in [OIDCCore] section 3.1.2.1, but can be specified regardless of whether the client role also requests the "openid" scope.</p> <p>The AD FS server ignores this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>The prompt query parameter is OPTIONAL, and can be specified by the client role of the OAuth 2.0 Protocol Extensions. This parameter has the same behavior as the prompt parameter defined in [OIDCCore] section 3.1.2.1 (see section 2.2.2 for exceptions and support information), but can be specified regardless of whether the client role also requests the "openid" scope.</p> <p>...</p> <p>In Section 3.2.5.1.1, GET, changed from:</p> <p>...</p> <p>prompt: OPTIONAL. The client can choose to specify this optional query parameter. It is used in the same way as the prompt parameter defined in [OIDCCore] section 3.1.2.1.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>prompt: OPTIONAL. The client can choose to specify this optional query parameter. It is used in the same way as the prompt parameter defined in [OIDCCore] section 3.1.2.1.</p> <p>Note Support for the prompt parameter depends on the AD FS server's ad_fs_behavior_level and the product version. See section 2.2.2 for support information.</p> <p>...</p> <p>In Section 3.2.5.1.1.3, Processing Details, changed from:</p> <p>...</p> <ul style="list-style-type: none"> • If the AD FS server's ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher and the OAuth 2.0 client provided a value of "none" or "login" for the prompt query parameter, the AD FS server follows the behavior described for the prompt parameter in [OIDCCore] section 3.1.2.1. <p>...</p> <p>Changed to:</p> <p>...</p> <ul style="list-style-type: none"> • If the prompt query parameter is supported and the OAuth 2.0 client provided a value of "none" or "login" for the prompt query parameter, the AD FS server follows the behavior described for the prompt parameter in [OIDCCore] section 3.1.2.1. <p>Note Support for the prompt parameter depends on the AD FS server's ad_fs_behavior_level and the product version. See section 2.2.2 for support information.</p> <p>...</p> <p>In Section 4.10, Authorization Code Request with prompt Parameter, changed from:</p>

Errata Published*	Description
	<p>Refer to [RFC6749] section 4.1.1 (Authorization Request). For more information on the prompt parameter, see [OIDCCore] section 3.1.2.1.</p> <p>...</p> <p>Changed to:</p> <p>Refer to [RFC6749] section 4.1.1 (Authorization Request). For more information on the prompt parameter, see section 2.2.2 and [OIDCCore] section 3.1.2.1.</p> <p>...</p>

* Date format: YYYY/MM/DD

[MS-OAPXBC]: OAuth 2.0 Protocol Extensions for Broker Clients

This topic lists the Errata found in [MS-OAPXBC] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

September 26, 2016 - [Download](#)

[MS-OTPC]: One-Time Password Certificate Enrollment Protocol

This topic lists the Errata found in [MS-OTPC] 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.

Errata below are for Protocol Document Version [V4.0 - 2016/07/14](#).

Errata Published*	Description
2016/08/15	<p>In Section 2.2.3, SignCert Response, revised the below code snippet to match the IDL:</p> <pre><xs:complexType name="SignCertResponse"> <xs:sequence> <xs:element name="IssuingCA" type="xs:anyURI" minOccurs="0" maxOccurs="unbounded" /> </xs:sequence> <xs:attribute name="statusCode" type="otpcep:SignCertStatusCode" use="required" /> <xs:attribute name="SignedCertRequest" type="otpcep:CertificateBase64Binary" use="optional" /> </xs:complexType></pre> <p>In Section 3.2.5.1, Processing A SignCert Request Message, specified that the SignedCertRequest and IssuingCA attributes are not set on failure. Also specified that Password Authentication Protocol [RFC1334] over RADIUM is used to validate OTP credentials.</p>

*Date format: YYYY/MM/DD

[MS-PEAP]: Protected Extensible Authentication Protocol (PEAP)

This topic lists the Errata found in [MS-PEAP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-PSRDP]: PowerShell Remote Debugging Protocol

This topic lists the Errata found in [MS-PSRDP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-PSRP]: PowerShell Remoting Protocol

This topic lists the Errata found in [MS-PSRP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-RA]: Remote Assistance Protocol

This topic lists the Errata found in [MS-RA] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-RAI]: Remote Assistance Initiation Protocol

This topic lists the Errata found in [MS-RAI] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-RDPBCGR]: Remote Desktop Protocol: Basic Connectivity and Graphics Remoting

This topic lists the Errata found in [MS-RDPBCGR] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V43.0 – 2016/10/13](#).

Errata Published*	Description
2017/01/23	<p>In this document:</p> <ol style="list-style-type: none">1) Clarified that Redirection PDU has to contain a variable-length routing token in Section 1.3.8, Server Redirection.2) Added the PROTOCOL_RDSTLS flag to the requestedProtocols field table in Section 2.2.1.1.1, RDP Negotiation Request (RDP_NEG_REQ), and added the PROTOCOL_RDSTLS value to the selectedProtocol field table in Section 2.2.1.2.1, RDP Negotiation Response (RDP_NEG_RSP).3) Added RedirectionGuidLength, RedirectionGuid, TargetCertificateLength, and TargetCertificate fields; and added LB_PASSWORD_IS_PK_ENCRYPTED, LB_REDIRECTION_GUID, and LB_TARGET_CERTIFICATE to the RedirFlags field table in Section 2.2.13.1, Server Redirection Packet (RDP_SERVER_REDIRECTION_PACKET).4) Added the RDSTLS external security protocol to Section 5.4, Enhanced RDP Security.5) Added the following new sections:<ul style="list-style-type: none">1.3.8.1 RDSTLS2.2.17 RDSTLS PDUs<ul style="list-style-type: none">2.2.17.1 RDSTLS Capabilities PDU2.2.17.2 RDSTLS Authentication Request PDU with Password Credentials2.2.17.3 RDSTLS Authentication Request PDU with Auto-Reconnect Cookie2.2.17.4 RDSTLS Authentication Response PDU5.4.5.3 RDSTLS Security<ul style="list-style-type: none">5.4.5.3.1 RDSTLS Connection Sequence <p>For details on these changes, see the [MS-RDPBCGR] DIFF doc in PDF format here.</p>
2017/01/09	<p>In this document:</p> <ul style="list-style-type: none">• Added the normative reference [ITUX691] to Section 1.2.1, Normative References.• Clarified how MCS Send Data Request and MCS Send Data Indication structures avoid implementing ASN.1 PER extended size determinant encoding in Section 2.2, Message Syntax.• Clarified the overall PDU length in the length1 and length2 field descriptions in the following sections: 2.2.8.1.2, Client Fast-Path Input Event PDU (TS_FP_INPUT_PDU) and 2.2.9.1.2, Server Fast-Path Update PDU (TS_FP_UPDATE_PDU).

Errata Published*	Description
	<ul style="list-style-type: none"> Replaced instances of "secFlags" field with "flags" field in the following sections: <ul style="list-style-type: none"> 2.2.8.1.2 Client Fast-Path Input Event PDU (TS_FP_INPUT_PDU) 2.2.9.1.2 Server Fast-Path Update PDU (TS_FP_UPDATE_PDU) 3.2.5.8.1.2 Sending Fast-Path Input Event PDU 3.2.5.9.3 Processing Fast-Path Update PDU 3.3.5.8.1.2 Processing Fast-Path Input Event PDU 3.3.5.9.3 Sending Fast-Path Update PDU 4.7 Annotated Fast-Path Input Event PDU <p>In Section 1.2.1, Normative References, changed from:</p> <p>[International] Dr. International, "Developing International Software (2nd Edition)", Microsoft Press, 2003, ISBN: 0735615837.</p> <p>[MS-CSSP] Microsoft Corporation, "Credential Security Support Provider (CredSSP) Protocol". ...</p> <p>Changed to:</p> <p>[International] Dr. International, "Developing International Software (2nd Edition)", Microsoft Press, 2003, ISBN: 0735615837.</p> <p>[ITUX691] ITU-T, "ASN.1 Encoding Rules: Specification of Packed Encoding Rules (PER)", Recommendation X.691, July 2002, http://www.itu.int/ITU-T/studygroups/com17/languages/X.691-0207.pdf</p> <p>[MS-CSSP] Microsoft Corporation, "Credential Security Support Provider (CredSSP) Protocol". ...</p> <p>In Section 2.2, Message Syntax, changed from:</p> <p>...</p> <p>Version 2 MCS Encoding Rules (defined in [T125] section 9) are used when encoding MCS structures defined in [T125].</p> <p>Changed to:</p> <p>...</p> <p>Version 2 MCS Encoding Rules (defined in [T125] section 9) are used when encoding MCS structures defined in [T125]. The MCS Send Data Request ([T125] section 11.32) and MCS Send Data Indication ([T125] section 11.33) structures MUST be restricted to 16,383 or fewer bytes in length to avoid implementing ASN.1 Packed Encoding Rules (PER) extended size determinant encoding ([ITUX691] section 10.9.3, excluding 10.9.3.8).</p> <p>In Section 2.2.8.1.2, Client Fast-Path Input Event PDU (TS_FP_INPUT_PDU), changed from:</p> <p>....</p> <p>fpInputHeader (1 byte): An 8-bit, unsigned integer. One-byte, bit-packed header. This byte coincides with the first byte of the TPKT Header ([T123] section 8). Three pieces of information are collapsed into this byte:</p> <ul style="list-style-type: none"> Security flags Number of events in the fast-path input PDU Action code

Errata Published*	Description
	<p>The format of the fpInputHeader byte is described by the following bitmask diagram.</p> <pre> 0 1 2 3 4 5 6 7 8 9 1 0 1 2 3 4 5 6 7 8 9 2 0 1 2 3 4 5 6 7 8 9 3 0 1 action numEvents secFlags ... secFlags (2 bits): A 2-bit, unsigned integer that contains the flags describing the cryptographic parameters of the PDU. ... length1 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the size of the PDU is in the range 1 to 127 bytes and the length1 field contains the overall PDU length (the length2 field is not present in this case). However, if the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). length2 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the length2 field is not present. If the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). ... Changed to: fpInputHeader (1 byte): An 8-bit, unsigned integer. One-byte, bit-packed header. This byte coincides with the first byte of the TPKT Header ([T123] section 8). Three pieces of information are collapsed into this byte: <ul style="list-style-type: none"> • Security flags • Number of events in the fast-path input PDU • Action code The format of the fpInputHeader byte is described by the following bitmask diagram. <pre> 0 1 2 3 4 5 6 7 8 9 1 0 1 2 3 4 5 6 7 8 9 2 0 1 2 3 4 5 6 7 8 9 3 0 1 action numEvents flags ... flags (2 bits): A 2-bit, unsigned integer that contains the flags describing the cryptographic parameters of the PDU. ... length1 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the size of the PDU is in the range 1 to 127 bytes and the length1 field contains the overall PDU length (the length2 field is not present in this case). However, if the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). The overall PDU length SHOULD be less than or equal to 16,383 bytes. length2 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the length2 field is not present. If the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits </pre> </pre>

Errata Published*	Description
	<p>of the length2 field, in big-endian order (the length2 field contains the low-order bits). The overall PDU length SHOULD be less than or equal to 16,383 bytes.</p> <p>In Section 2.2.9.1.2, Server Fast-Path Update PDU (TS_FP_UPDATE_PDU), changed from:</p> <p>...</p> <p>fpOutputHeader (1 byte): An 8-bit, unsigned integer. One-byte, bit-packed header. This byte coincides with the first byte of the TPKT Header ([T123] section 8). Two pieces of information are collapsed into this byte:</p> <ul style="list-style-type: none"> • Security flags • Action code <p>The format of the fpOutputHeader byte is described by the following bitmask diagram.</p> <pre> 0 1 2 3 4 5 6 7 8 9 1 0 1 2 3 4 5 6 7 8 9 2 0 1 2 3 4 5 6 7 8 9 3 0 1 action reserved secFlags ... secFlags (2 bits): A 2-bit, unsigned integer that contains flags describing the cryptographic parameters of the PDU. ... length1 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the size of the PDU is in the range 1 to 127 bytes and the length1 field contains the overall PDU length (the length2 field is not present in this case). However, if the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). length2 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the length2 field is not present. If the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). ... Changed to: ... fpOutputHeader (1 byte): An 8-bit, unsigned integer. One-byte, bit-packed header. This byte coincides with the first byte of the TPKT Header ([T123] section 8). Two pieces of information are collapsed into this byte: <ul style="list-style-type: none"> • Security flags • Action code <p>The format of the fpOutputHeader byte is described by the following bitmask diagram.</p> <pre> 0 1 2 3 4 5 6 7 8 9 1 0 1 2 3 4 5 6 7 8 9 2 0 1 2 3 4 5 6 7 8 9 3 0 1 action reserved flags ... flags (2 bits): A 2-bit, unsigned integer that contains flags describing the cryptographic parameters of the PDU. ... length1 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not </pre> </pre>

Errata Published*	Description
	<p>set, then the size of the PDU is in the range 1 to 127 bytes and the length1 field contains the overall PDU length (the length2 field is not present in this case). However, if the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). The overall PDU length SHOULD be less than or equal to 16,383 bytes.</p> <p>length2 (1 byte): An 8-bit, unsigned integer. If the most significant bit of the length1 field is not set, then the length2 field is not present. If the most significant bit of the length1 field is set, then the overall PDU length is given by the low 7 bits of the length1 field concatenated with the 8 bits of the length2 field, in big-endian order (the length2 field contains the low-order bits). The overall PDU length SHOULD be less than or equal to 16,383 bytes.</p> <p>...</p> <p>In Section 3.2.5.8.1.2, Sending Fast-Path Input Event PDU, changed from:</p> <p>...</p> <p>If Standard RDP Security mechanisms (section 5.3) are in effect, the PDU data following the optional dataSignature field can be encrypted and signed (depending on the values of the Encryption Level (section 5.3.1) and Encryption Method selected by the server as part of the negotiation described in section 5.3.2), using the methods and techniques described in section 5.3.6. If the data is to be encrypted, the embedded secFlags field of the fpInputHeader field MUST contain the FASTPATH_INPUT_ENCRYPTED (2) flag.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>If Standard RDP Security mechanisms (section 5.3) are in effect, the PDU data following the optional dataSignature field can be encrypted and signed (depending on the values of the Encryption Level (section 5.3.1) and Encryption Method selected by the server as part of the negotiation described in section 5.3.2), using the methods and techniques described in section 5.3.6. If the data is to be encrypted, the embedded flags field of the fpInputHeader field MUST contain the FASTPATH_INPUT_ENCRYPTED (2) flag.</p> <p>...</p> <p>In Section 3.2.5.9.3, Processing Fast-Path Update PDU, changed from:</p> <p>...</p> <p>If the embedded secFlags field of the fpOutputHeader field contains the FASTPATH_OUTPUT_ENCRYPTED (2) flag, then the data following the optional dataSignature field (which in this case MUST be present) MUST be verified and decrypted using the methods and techniques described in section 5.3.6. If the MAC signature is incorrect or the data cannot be decrypted correctly, the connection SHOULD be dropped. If Enhanced RDP Security is in effect and the FASTPATH_OUTPUT_ENCRYPTED (2) flag is present the connection SHOULD be dropped because double-encryption is not used within RDP in the presence of an External Security Protocol provider.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>If the embedded flags field of the fpOutputHeader field contains the FASTPATH_OUTPUT_ENCRYPTED (2) flag, then the data following the optional dataSignature field (which in this case MUST be present) MUST be verified and decrypted using the methods and techniques described in section 5.3.6. If the MAC signature is incorrect or the data cannot be decrypted correctly, the connection SHOULD be dropped. If Enhanced RDP Security is in effect and the FASTPATH_OUTPUT_ENCRYPTED (2) flag is present the connection SHOULD be dropped because double-encryption is not used within RDP in the presence of an External Security Protocol</p>

Errata Published*	Description
	<p>provider.</p> <p>...</p> <p>In Section 3.3.5.8.1.2, Processing Fast-Path Input Event PDU, changed from:</p> <p>...</p> <p>If the embedded secFlags field of the fpInputHeader field contains the FASTPATH_INPUT_ENCRYPTED (2) flag, then the data following the optional dataSignature field (which in this case MUST be present) MUST be verified and decrypted using the methods and techniques described in section 5.3.6. If the MAC signature is incorrect or the data cannot be decrypted correctly, the connection SHOULD be dropped. If Enhanced RDP Security is in effect and the FASTPATH_INPUT_ENCRYPTED (2) flag is present the connection SHOULD be dropped because double-encryption is not used within RDP in the presence of an External Security Protocol Provider.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>If the embedded flags field of the fpInputHeader field contains the FASTPATH_INPUT_ENCRYPTED (2) flag, then the data following the optional dataSignature field (which in this case MUST be present) MUST be verified and decrypted using the methods and techniques described in section 5.3.6. If the MAC signature is incorrect or the data cannot be decrypted correctly, the connection SHOULD be dropped. If Enhanced RDP Security is in effect and the FASTPATH_INPUT_ENCRYPTED (2) flag is present the connection SHOULD be dropped because double-encryption is not used within RDP in the presence of an External Security Protocol Provider.</p> <p>...</p> <p>In Section 3.3.5.9.3, Sending Fast-Path Update PDU, changed from:</p> <p>...</p> <p>If Standard RDP Security mechanisms (section 5.3) are in effect, the PDU data following the optional dataSignature field can be encrypted and signed (depending on the values of the Encryption Level and Encryption Method selected by the server as part of the negotiation described in section 5.3.2) using the methods and techniques described in section 5.3.6. If the data is to be encrypted, the embedded secFlags field of the fpOutputHeader field MUST contain the FASTPATH_OUTPUT_ENCRYPTED (2) flag.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>If Standard RDP Security mechanisms (section 5.3) are in effect, the PDU data following the optional dataSignature field can be encrypted and signed (depending on the values of the Encryption Level and Encryption Method selected by the server as part of the negotiation described in section 5.3.2) using the methods and techniques described in section 5.3.6. If the data is to be encrypted, the embedded flags field of the fpOutputHeader field MUST contain the FASTPATH_OUTPUT_ENCRYPTED (2) flag.</p> <p>...</p> <p>In Section 4.7, Annotated Fast-Path Input Event PDU, changed from:</p> <p>The following is an annotated dump of a Fast-Path Input Event PDU (section 2.2.8.1.2) that was sent from a Microsoft RDP 5.1 client to a Microsoft RDP 5.1 server.</p>

Errata Published*	Description
	<pre> 00000000 c4 11 30 35 6b 5b b5 34 c8 47 26 18 5e 76 0e de ..05k[.4.G&.^v.. 00000010 28 (c4 -> TS_FP_INPUT_PDU::fpInputHeader = 0xc4 Binary of 0xc4 = 11 0001 00 action = FASTPATH_INPUT_ACTION_FASTPATH (0) numEvents = 1 secFlags = 0x3 0x3 = 0x1 0x2 = FASTPATH_INPUT_SECURE_CHECKSUM FASTPATH_INPUT_ENCRYPTED ... Changed to: The following is an annotated dump of a Fast-Path Input Event PDU (section 2.2.8.1.2) that was sent from a Microsoft RDP 5.1 client to a Microsoft RDP 5.1 server. 00000000 c4 11 30 35 6b 5b b5 34 c8 47 26 18 5e 76 0e de ..05k[.4.G&.^v.. 00000010 28 (c4 -> TS_FP_INPUT_PDU::fpInputHeader = 0xc4 Binary of 0xc4 = 11 0001 00 action = FASTPATH_INPUT_ACTION_FASTPATH (0) numEvents = 1 flags = 0x3 0x3 = 0x1 0x2 = FASTPATH_INPUT_SECURE_CHECKSUM FASTPATH_INPUT_ENCRYPTED ... </pre>
2016/10/13	<p>In this document:</p> <ul style="list-style-type: none"> • Added RDP version 10.2 to multiple sections and product behavior notes. • Clarified that only RDP 8.0 and 8.1 servers support the RDP-UDP FEC lossy transport. • Added the INFO_RESERVED1 flag to the flags field table. • Updated the meaning for flag NEGRSP_FLAG_RESERVED in the flags field table. • Updated the meaning for flags PERF_RESERVED1 and PERF_RESERVED2 in the performance flags field table. <p>For details on these changes, see the [MS-RDPBCGR] DIFF doc in PDF format here.</p>

*Date format: YYYY/MM/DD

[MS-RDPEA]: Remote Desktop Protocol: Audio Output Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEA] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-RDPECLIP]: Remote Desktop Protocol: Clipboard Virtual Channel Extension

This topic lists the Errata found in [MS-RDPECLIP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-RDPEDYC]: Remote Desktop Protocol: Dynamic Channel Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEDYC] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

Errata below are for Protocol Document Version [V15.0 – 2016/07/14](#).

Errata Published*	Description
2016/11/21	<p>In Section 1.7, Versioning and Capability Negotiation, clarified that there are three versions of the Remote Desktop Protocol: Dynamic Channel Virtual Channel Extension.</p> <p>Changed from:</p> <p>...</p> <p>There are two versions of the Remote Desktop Protocol: Dynamic Channel Virtual Channel Extension.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>There are three versions of the Remote Desktop Protocol: Dynamic Channel Virtual Channel Extension.</p> <p>...</p> <p>In Section 2.2.5.1, Soft-Sync Request PDU (DYNVC_SOFT_SYNC_REQUEST), added Length, Flags, and NumberOfTunnels fields to the Length definition.</p> <p>Changed from:</p> <p>...</p> <p>Length (4 bytes): A 32-bit, unsigned integer indicating the total size, in bytes, of SoftSyncChannelLists field.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>Length (4 bytes): A 32-bit, unsigned integer indicating the total size, in bytes, of the Length, Flags, NumberOfTunnels, and SoftSyncChannelLists fields.</p> <p>...</p>

*Date format: YYYY/MM/DD

[MS-RDPEFS]: Remote Desktop Protocol: File System Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEFS] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

Errata below are for Protocol Document Version [V23.0 – 2016/07/14](#).

Errata Published*	Description
2016/09/26	<p>In Section 2.2.3.4.2, Client Drive Close Response (DR_DRIVE_CLOSE_RSP), updated the size of the DeviceCloseResponse field from 21 bytes to 20 bytes and added the 1 byte Padding field.</p> <p>Changed from: DeviceCloseResponse (21 bytes):</p> <p>Changed to: DeviceCloseResponse (20 bytes):</p> <p>Included the following field: Padding (1 byte): An 8-bit unsigned integer that is intended to allow the client minor flexibility in determining the overall packet length. This field is unused and MUST be ignored.</p>
2016/09/26	<p>In Section 2.2.2.3, Client Announce Reply (DR_CORE_CLIENT_ANNOUNCE_RSP), changed ClientID to ClientId in the ClientId field description.</p> <p>Changed from: ... ClientID (4 bytes): A 32-bit unsigned integer that the client MUST set to either the ClientID field,...</p> <p>Changed to: ... ClientId (4 bytes): A 32-bit unsigned integer that the client MUST set to either the ClientId field,...</p>
2016/08/15	<p>In Section 2.2.1.3, Device Announce Header (DEVICE_ANNOUNCE), clarified that the maximum device name length should be 7 characters to account for the null terminator in the PreferredDosName field description.</p>

Errata Published*	Description
	<p>Changed from:</p> <p>...</p> <p>PreferredDosName (8 bytes): A string of ASCII characters with a maximum length of eight characters that represent the name of the device as it appears on the client. This field MUST not be null-terminated if the device name is 8 characters long. The following characters are considered invalid for the PreferredDosName field:</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>PreferredDosName (8 bytes): A string of ASCII characters (with a maximum length of eight characters) that represents the name of the device as it appears on the client. This field MUST be null-terminated, so the maximum device name is 7 characters long. The following characters are considered invalid for the PreferredDosName field:</p> <p>...</p>

*Date format: YYYY/MM/DD

[MS-RDPEGDI]: Remote Desktop Protocol: Graphics Device Interface (GDI) Acceleration Extensions

This topic lists the Errata found in [MS-RDPEGDI] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-RDPEGFX]: Remote Desktop Protocol: Graphics Pipeline Extension

This topic lists the Errata found in [MS-RDPEGFX] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V42.0 - 2016/07/14](#).

Errata Published*	Description
2017/02/20	<p>In Section 3.3.5.2, Processing an RDPGFX_WIRE_TO_SURFACE_PDU_2 message, added a note.</p> <p>Changed from:</p> <p>...The bitmap SHOULD be copied to the target surface using a SRCCOPY ROP3 operation ([MS-RDPEGDI] section 2.2.2.2.1.1.1.7) once enough data has been decoded to render a discernible image and SHOULD then continue to be updated as subsequent RDPGFX_WIRE_TO_SURFACE_PDU_2 messages are processed.</p> <p>Changed to:</p> <p>...The bitmap SHOULD be copied to the target surface using a SRCCOPY ROP3 operation ([MS-RDPEGDI] section 2.2.2.2.1.1.1.7) once enough data has been decoded to render a discernible image and SHOULD then continue to be updated as subsequent RDPGFX_WIRE_TO_SURFACE_PDU_2 messages are processed. Note that if the type (specified in the blockType field) of the current RFX_PROGRESSIONIVE_DATABLOCK structure (section 2.2.4.2.1) of an RFX_PROGRESSIONIVE_BITMAP_STREAM (section 2.2.4.2) is WBT_TILE_PROGRESSIONIVE_UPGRADE (0xCCC7), then the codecContextId field in the Codec Contexts (section 3.3.1.1) ADM element MUST be known.</p>
2016/09/26	<p>In Section 4.1.1.2, Example 2, updated the Hex value 4C to 0 for the value 0 of the field runLengthFactor1 in the decoding of the sixteenth RLEX_SEGMENT.</p> <p>Changed from:</p> <p>4c -> CLEARCODEC_SUBCODEC_RLEX_SEGMENT::runLengthFactor1 = 0</p> <p>Changed to:</p> <p>0 -> CLEARCODEC_SUBCODEC_RLEX_SEGMENT::runLengthFactor1 = 0</p>

*Date format: YYYY/MM/DD

[MS-RDPEGT]: Remote Desktop Protocol Geometry Tracking Virtual Channel Protocol Extension

This topic lists the Errata found in [MS-RDPEGFT] 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.

Errata below are for Protocol Document Version [V5.0 – 2016/07/14](#).

Errata Published*	Description
2017/03/06	<p>In Section 2.2.1.1, MAPPED_GEOMETRY_PACKET Structure, described what happens when the nCount field is zero and the rectangles do not intersect with the rectangle specified in the rcBound field in the pGeometryBuffer description.</p> <p>Changed from:</p> <p>...</p> <p>pGeometryBuffer (variable): Array of UINT8 ([MS-DTYP] section 2.2.47). This field contains a RGNDATA structure, as specified in [MSDN-WindowsGDI]. The rectangles in this structure are relative to the tracked rectangle, and represent the parts of the tracked rectangle that are visible. If window tracking mode is not in effect, the rcBound field in the RGNDATA structure MUST be ignored. The total number of bytes in this field is set in the cbGeometryBuffer field.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>pGeometryBuffer (variable): Array of UINT8 ([MS-DTYP] section 2.2.47). This field contains a RGNDATA structure, as specified in [MSDN-WindowsGDI]. The rectangles in this structure are relative to the tracked rectangle, and represent the parts of the tracked rectangle that are visible. If window tracking mode is not in effect, the rcBound field in the RGNDATA structure MUST be ignored. If the nCount field of the RGNDATA structure is zero, or the rectangles in the RGNDATA buffer field do not intersect with the rectangle specified in the rcBound field, then the RGNDATA structure MUST be ignored. The total number of bytes in this field is set in the cbGeometryBuffer field.</p> <p>...</p>

*Date format: YYYY/MM/DD

[MS-RDPEI]: Remote Desktop Protocol: Input Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEI] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-RDPEMC]: Remote Desktop Protocol: Multiparty Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEMC] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-RDPEMT]: Remote Desktop Protocol: Multitransport Extension

This topic lists the Errata found in [MS-RDPEMT] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 2, 2016 - [Download](#)

[MS-RDPEPC]: Remote Desktop Protocol: Print Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEPC] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V8.0 - 2016/07/14](#).

Errata Published*	Description
2016/11/07	<p>In Section 1.2.1, Normative References, added a reference to protocol [MS-RDPEXPS] and in Section 3.1.1.2, XPS Mode, added a dependency to reference [MS-RDPEXPS] when redirection of XPS data is used.</p> <p>In Section 1.2.1, Normative References, changed from:</p> <p>...</p> <p>[MS-RDPESP] Microsoft Corporation, "Remote Desktop Protocol: Serial and Parallel Port Virtual Channel Extension".</p> <p>[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.rfc-editor.org/rfc/rfc2119.txt</p> <p>Changed to:</p> <p>...</p> <p>[MS-RDPESP] Microsoft Corporation, "Remote Desktop Protocol: Serial and Parallel Port Virtual Channel Extension".</p> <p>[MS-RDPEXPS] Microsoft Corporation, "Remote Desktop Protocol: XML Paper Specification (XPS) Print Virtual Channel Extension".</p> <p>[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.rfc-editor.org/rfc/rfc2119.txt</p> <p>In Section 3.1.1.2, XPS Mode, changed from:</p> <p>When a client redirects printers, it adds a special flag (RDPDR_PRINTER_ANNOUNCE_FLAG_XPSFORMAT) if the client can handle the XPS format for the given printer. For these printers, the server MAY<2> choose to use either the XPS format or the printer driver-specific format. The server MUST notify the client with the message DR_PRN_USING_XPS (section 2.2.2.2) if it chooses to use the XPS format. When this type of message is received, the client marks the printer in XPS mode.</p>

Errata Published*	Description
	<p>Changed to:</p> <p>When a client redirects printers, it adds a special flag (RDPDR_PRINTER_ANNOUNCE_FLAG_XPSFORMAT) if the client can handle the XPS format for the given printer. For these printers, the server MAY choose to use either the XPS format or the printer driver-specific format. The server MUST notify the client with the message DR_PRN_USING_XPS (section 2.2.2.2) if it chooses to use the XPS format. When this type of message is received, the client marks the printer in XPS mode. Redirection of XPS data using the Remote Desktop Protocol: XML Paper Specification (XPS) Print Virtual Channel Extension is described in [MS-RDPEXPS].</p>
2016/08/15	<p>In Section 2.2.2.1, Client Device List Announce Request (DR_PRN_DEVICE_ANNOUNCE), updated the PreferredDosName field description to indicate mandatory usage of the "PRN" prefix.</p> <p>Changed from:</p> <p>...</p> <p>PreferredDosName (8 bytes): This field is defined in [MS-RDPEFS] section 2.2.1.3. The PreferredDosName field MUST be set to the port name on which the printer is installed.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>PreferredDosName (8 bytes): This field is defined in [MS-RDPEFS] section 2.2.1.3. The PreferredDosName field MUST be set to the port name on which the printer is installed. The first 3 characters MUST be "PRN" and the remainder MUST be digits.</p> <p>...</p>

*Date format: YYYY/MM/DD

[MS-RDPEPNP]: Remote Desktop Protocol: Plug and Play Devices Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEPNP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-RDPERP]: Remote Desktop Protocol: Remote Programs Virtual Channel Extension

This topic lists the Errata found in [MS-RDPERP] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 2, 2016 - [Download](#)

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V22.0 - 2016/07/14](#).

Errata Published*	Description
2016/09/26	<p>In Section 1.5, Prerequisites/Preconditions, clarified that the CHANNEL_FLAG_SHOW_PROTOCOL (0x00000010) has to be set in the flags field of the Channel PDU Header in order for it to be visible for all data that flows over the RAIL virtual channel.</p> <p>Changed from:</p> <p>The Remote Programs Extensions for Remote Desktop Protocol has the assumption to operate in a fully operational RDP connection. A fully operational RDP connection is a connection that has passed the Connection Finalization phase, as specified in [MS-RDPBCGR] section 1.3.1.1.</p> <p>Changed to:</p> <p>The Remote Programs Extensions for Remote Desktop Protocol has the assumption to operate in a fully operational RDP connection. A fully operational RDP connection is a connection that has passed the Connection Finalization phase, as specified in [MS-RDPBCGR] section 1.3.1.1.</p> <p>The RAIL server endpoint expects that the Channel PDU Header ([MS-RDPBCGR] section 2.2.6.1.1) is visible for all data that flows over the RAIL virtual channel (sections 1.3.1 and 2.2.2). To ensure that this condition is met, the CHANNEL_FLAG_SHOW_PROTOCOL (0x00000010) flag has to be set in the flags field of the Channel PDU Header.</p> <p>In Section 2.2.2, Static Virtual Channel Protocol, clarified that the RAIL Static Virtual Channel is named "RAIL".</p> <p>Changed from:</p> <p>The RAIL Static Virtual Channel is responsible...</p> <p>Changed to:</p>

Errata Published*	Description
	The RAIL Static Virtual Channel (named "RAIL") is responsible...
2016/09/26	<p>In Section 4.3.2, TS_RAIL_ORDER_EXEC_RESULT, changed RAIL_ORDER_EXEC_RESULT to TS_RAIL_ORDER_EXEC_RESULT.</p> <p>Changed from:</p> <p>The following is a network capture of the Server Execute Result PDU</p> <p>(RAIL_ORDER_EXEC_RESULT, as specified in 2.2.2.3.2).</p> <p>...</p> <p>80 00 -> TS_RAIL_PDU_HEADER::orderType = RAIL_ORDER_EXEC_RESULT(128) (2 Bytes)</p> <p>...</p> <p>Changed to:</p> <p>The following is a network capture of the Server Execute Result PDU</p> <p>(TS_RAIL_ORDER_EXEC_RESULT, as specified in 2.2.2.3.2).</p> <p>...</p> <p>80 00 -> TS_RAIL_PDU_HEADER::orderType = TS_RAIL_ORDER_EXEC_RESULT(128) (2 Bytes)</p> <p>...</p>
2016/09/26	<p>In Section 3.2.5.1.6, Processing Window Information Orders, clarified how the client will process the server window events of registration, deregistration, and updates on the edge of an application desktop toolbar.</p> <p>Changed from:</p> <p>Window Information Orders (section 2.2.1.3.1) inform the client of the following types of window events on the server:</p> <p>...</p> <ul style="list-style-type: none"> • Registration of a new or existing window as an application desktop toolbar. • Deregistration of an existing application desktop toolbar. <p>...</p> <p>Upon receipt of a Window Information Order for a deleted window, as specified in section 2.2.1.3.1.2.4, the client SHOULD locate the local RAIL window that corresponds to the WindowId reported in the Hdr field and destroy it. If no such window can be found, the client SHOULD ignore the order.</p> <p>Changed to:</p> <p>Window Information Orders (section 2.2.1.3.1) inform the client of the following types of window events on the server:</p> <p>...</p> <ul style="list-style-type: none"> • Registration of a new or existing window as an application desktop toolbar. • Deregistration of an existing application desktop toolbar.

Errata Published*	Description
	<ul style="list-style-type: none"> • Updates on the edge to which the application desktop toolbar window is anchored. <p>...</p> <p>Upon receipt of a Window Information Order for a deleted window, as specified in section 2.2.1.3.1.2.4, the client SHOULD locate the local RAIL window that corresponds to the WindowId reported in the Hdr field and destroy it. If no such window can be found, the client SHOULD ignore the order.</p> <p>Upon receipt of a Window Information Order for the registration of a window as an application desktop toolbar, the client SHOULD locate the local RAIL window that corresponds to the WindowId reported in the Hdr field and register it as an application desktop toolbar. If no such window can be found, the client SHOULD ignore the order.</p> <p>Upon receipt of a Window Information Order for the deregistration of an application desktop toolbar window, the client SHOULD locate the local RAIL window that corresponds to the WindowId reported in the Hdr field and deregister the application desktop toolbar window. If no such window can be found, the client SHOULD ignore the order.</p> <p>Upon receipt of a Window Information Order for the edge of an application desktop toolbar window, the client SHOULD locate the local RAIL window that corresponds to the WindowId reported in the Hdr field and update the edge to which the window is anchored. If no such window can be found, the client SHOULD ignore the order.</p>
2016/09/26	<p>Added two Window Information Orders to match the client behavior in Section 3.3.5.1.6, Constructing Window Information Orders, and removed two Notification Icon Orders to match the client behavior in Section 3.3.5.1.7, Constructing Notification Icon Orders.</p> <p>In Section 3.3.5.1.6, Constructing Window Information Orders, changed from:</p> <p>The server generates Window Information Orders to inform the client of the following types of window events on the server:</p> <ul style="list-style-type: none"> • Creation of a new window. • Updates on window properties for a new or existing window. • Updates on icons for a new or existing window. • Deletion of an existing window. <p>...</p> <p>Changed to:</p> <p>The server generates Window Information Orders to inform the client of the following types of window events on the server:</p> <ul style="list-style-type: none"> • Creation of a new window. • Updates on window properties for a new or existing window. • Updates on icons for a new or existing window. • Deletion of an existing window. • Registration of a new or existing window as an application desktop toolbar. • Deregistration of an existing application desktop toolbar. <p>...</p>

Errata Published*	Description
	<p>In Section 3.3.5.1.7, Constructing Notification Icon Orders, changed from:</p> <p>The server generates Notification Icon Information Orders to inform the client of the following types of notification icon events on the server.</p> <ul style="list-style-type: none"> • Creation of a new notification icon. • Updates on properties for a new or existing notification icon. • Deletion of an existing notification icon. • Registration of a new or existing window as an application desktop toolbar. • Deregistration of an existing application desktop toolbar. <p>...</p> <p>Changed to:</p> <p>The server generates Notification Icon Information Orders to inform the client of the following types of notification icon events on the server.</p> <ul style="list-style-type: none"> • Creation of a new notification icon. • Updates on properties for a new or existing notification icon. • Deletion of an existing notification icon. <p>...</p>

*Date format: YYYY/MM/DD

[MS-RDPESC]: Remote Desktop Protocol: Smart Card Virtual Channel Extension

This topic lists the Errata found in [MS-RDPESC] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

Errata below are for Protocol Document Version [V11.0.1 – 2016/07/14](#).

Errata Published *	Description
2016/09/26	<p>Multiple changes in various sections:</p> <ul style="list-style-type: none">• Added the dialect SCREDIR_VERSION_WINDOWS_8 to the protocol versions and the behavior note along with the build numbers for SCREDIR_VERSION_XP, SCREDIR_VERSION_LONGHORN, and SCREDIR_VERSION_WINDOWS_8 in Section 1.7, Versioning and Capability Negotiation.• Updated the function number for SCARD_IOCTL_RELEASETARTEDEVENT IOCTL to 57 and updated the behavior note to include Windows 7 and Windows Server 2008 R2 in Section 3.1.4, Message Processing Events and Sequencing Rules. <p>In Section 1.7, Versioning and Capability Negotiation, changed from:</p> <p>This document covers versioning issues in the following areas:</p> <ul style="list-style-type: none">• Protocol Versions: Smart Card Redirection supports the explicit dialects "SCREDIR_VERSION_XP" and "SCREDIR_VERSION_LONGHORN". <p>Multiple versions of the Smart Card Redirection Protocol exist. It was introduced in Remote Desktop Protocol version 5.1 and extended by adding additional calls in Remote Desktop Protocol version 6.0. The version of the protocol is determined on the server by querying the value of the TS client build number.</p> <ul style="list-style-type: none">• Capability Negotiation: The Smart Card Redirection protocol does not support negotiation of the dialect to use. Instead, an implementation is configured with the dialect to use. <p>The dialect used is determined by the TS client's build number. The TS server determines the dialect to use by analyzing the client build number on device announce.<1> If the build number is at least 4,034, SCREDIR_VERSION_LONGHORN is assumed; otherwise, SCREDIR_VERSION_XP is to be used.</p> <p>Changed to:</p> <p>This document covers versioning issues in the following areas:</p>

Errata Published *	Description																																								
	<ul style="list-style-type: none">• Protocol Versions: Smart Card Redirection supports the dialects SCREDIR_VERSION_XP (1), SCREDIR_VERSION_LONGHORN (2), and SCREDIR_VERSION_WINDOWS_8 (3).• Capability Negotiation: The Smart Card Redirection protocol does not support negotiation of the dialect to use. Instead, an implementation is configured with the dialect to use. <p>The TS server determines the dialect to use by analyzing the client build number on device announce as specified in [MS-RDPBCGR] section 2.2.1.3.2 using the following mapping.<1></p> <table><tr><th>Build Number</th><th>Dialect</th></tr><tr><td>>= 7865</td><td>SCREDIR_VERSION_WINDOWS_8 (3)</td></tr><tr><td>>= 4034 and < 7865</td><td>SCREDIR_VERSION_LONGHORN (2)</td></tr><tr><td>< 4034</td><td>SCREDIR_VERSION_XP (1)</td></tr></table> <p>In Section 3.1.4, Message Processing Events and Sequencing Rules, changed from:</p> <p>...</p> <table><tr><th>Function number</th><th>Value for IoControlCode</th><th>IRP_MJ_DEVICE_CONTROL request</th><th>Input packet, Output packet</th></tr><tr><td>56</td><td>0x000900E0</td><td>SCARD_IOCTL_ACCESSSTARTEDEVENT</td><td>ScardAccessStartedEvent_Call (section 2.2.2.30), Long_Return (section 2.2.3.3)</td></tr><tr><td>58</td><td>0x000900E8</td><td>SCARD_IOCTL_LOCATECARDSBYATRA</td><td>LocateCardsByATRA_Call (section 2.2.2.23), LocateCards_Return (section 2.2.3.5)</td></tr><tr><td>...</td><td></td><td></td><td></td></tr><tr><td>64</td><td>0x00090100</td><td>SCARD_IOCTL_GETTRANSMITCOUNT</td><td>GetTransmitCount_Call (section 2.2.2.29), GetTransmitCount_Return (section 2.2.3.13)</td></tr><tr><td>66</td><td>0x000900E4</td><td>SCARD_IOCTL_RELEASETARTEDEVENT</td><td>Not used.</td></tr><tr><td>67</td><td>0x00090104</td><td>SCARD_IOCTL_GETREADERICON</td><td>GetReaderIcon_Call (section 2.2.2.31), GetReaderIcon_Return (section 2.2.3.14)</td></tr><tr><td>68</td><td>0x00090108</td><td>SCARD_IOCTL_GETDEVICETYPEID</td><td>GetDeviceTypeId_Call (section 2.2.2.32), GetDeviceTypeId_Return</td></tr></table>	Build Number	Dialect	>= 7865	SCREDIR_VERSION_WINDOWS_8 (3)	>= 4034 and < 7865	SCREDIR_VERSION_LONGHORN (2)	< 4034	SCREDIR_VERSION_XP (1)	Function number	Value for IoControlCode	IRP_MJ_DEVICE_CONTROL request	Input packet, Output packet	56	0x000900E0	SCARD_IOCTL_ACCESSSTARTEDEVENT	ScardAccessStartedEvent_Call (section 2.2.2.30), Long_Return (section 2.2.3.3)	58	0x000900E8	SCARD_IOCTL_LOCATECARDSBYATRA	LocateCardsByATRA_Call (section 2.2.2.23), LocateCards_Return (section 2.2.3.5)	...				64	0x00090100	SCARD_IOCTL_GETTRANSMITCOUNT	GetTransmitCount_Call (section 2.2.2.29), GetTransmitCount_Return (section 2.2.3.13)	66	0x000900E4	SCARD_IOCTL_RELEASETARTEDEVENT	Not used.	67	0x00090104	SCARD_IOCTL_GETREADERICON	GetReaderIcon_Call (section 2.2.2.31), GetReaderIcon_Return (section 2.2.3.14)	68	0x00090108	SCARD_IOCTL_GETDEVICETYPEID	GetDeviceTypeId_Call (section 2.2.2.32), GetDeviceTypeId_Return
Build Number	Dialect																																								
>= 7865	SCREDIR_VERSION_WINDOWS_8 (3)																																								
>= 4034 and < 7865	SCREDIR_VERSION_LONGHORN (2)																																								
< 4034	SCREDIR_VERSION_XP (1)																																								
Function number	Value for IoControlCode	IRP_MJ_DEVICE_CONTROL request	Input packet, Output packet																																						
56	0x000900E0	SCARD_IOCTL_ACCESSSTARTEDEVENT	ScardAccessStartedEvent_Call (section 2.2.2.30), Long_Return (section 2.2.3.3)																																						
58	0x000900E8	SCARD_IOCTL_LOCATECARDSBYATRA	LocateCardsByATRA_Call (section 2.2.2.23), LocateCards_Return (section 2.2.3.5)																																						
...																																									
64	0x00090100	SCARD_IOCTL_GETTRANSMITCOUNT	GetTransmitCount_Call (section 2.2.2.29), GetTransmitCount_Return (section 2.2.3.13)																																						
66	0x000900E4	SCARD_IOCTL_RELEASETARTEDEVENT	Not used.																																						
67	0x00090104	SCARD_IOCTL_GETREADERICON	GetReaderIcon_Call (section 2.2.2.31), GetReaderIcon_Return (section 2.2.3.14)																																						
68	0x00090108	SCARD_IOCTL_GETDEVICETYPEID	GetDeviceTypeId_Call (section 2.2.2.32), GetDeviceTypeId_Return																																						

Errata Published *	Description			
				(section 2.2.3.15)
	Changed to:			
	...			
	Function number	Value for IoControlCode	IRP_MJ_DEVICE_CONTROL request	Input packet, Output packet
	56	0x000900E0	SCARD_IOCTL_ACCESSSTARTEDEVENT	ScardAccessStartedEvent_Call (section 2.2.2.30), Long_Return (section 2.2.3.3)
	57	0x000900E4	SCARD_IOCTL_RELEASETARTEDEVENT	Not used.
	58	0x000900E8	SCARD_IOCTL_LOCATECARDSBYATRA	LocateCardsByATRA_Call (section 2.2.2.23), LocateCards_Return (section 2.2.3.5)
	...			
	64	0x00090100	SCARD_IOCTL_GETTRANSMITCOUNT	GetTransmitCount_Call (section 2.2.2.29), GetTransmitCount_Return (section 2.2.3.13)
	65	0x00090104	SCARD_IOCTL_GETREADERICON	GetReaderIcon_Call (section 2.2.2.31), GetReaderIcon_Return (section 2.2.3.14)
	66	0x00090108	SCARD_IOCTL_GETDEVICETYPEID	GetDeviceTypeId_Call (section 2.2.2.32), GetDeviceTypeId_Return (section 2.2.3.15)
	In Section 7, Appendix B: Product Behavior, changed from:			
	<1> Section 1.7: The Windows XP and Windows Server 2003 versions always use SCREDIR_VERSION_XP. Windows Vista and Windows Server 2008 are always SCREDIR_VERSION_LONGHORN.			
	<2> Section 3.1.4: Windows XP and Windows Server 2003 implement function numbers 5 through 58. Windows Vista and Windows Server 2008 implement function numbers 5 through 64.			
	Changed to:			
	<1> Section 1.7: The Windows XP and Windows Server 2003 versions always use SCREDIR_VERSION_XP. Windows Vista and Windows Server 2008 are always SCREDIR_VERSION_LONGHORN. All other versions use SCREDIR_VERSION_WINDOWS_8.			
	<2> Section 3.1.4: Windows XP and Windows Server 2003 implement function numbers 5 through 58. Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 implement			

Errata Published *	Description
	function numbers 5 through 64. All other versions implement 5 through 66.

*Date format: YYYY/MM/DD

[MS-RDPESP]: Remote Desktop Protocol: Serial and Parallel Port Virtual Channel Extension

This topic lists the Errata found in [MS-RDPESP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-RDPEUDP]: Remote Desktop Protocol: UDP Transport Extension

This topic lists the Errata found in [MS-RDPEUDP] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

March 2, 2016 - [Download](#)

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

Errata below are for Protocol Document Version [V9.0 - 2016/07/14](#).

Errata Published*	Description
2016/11/07 (updates errata entry originally published on 2016/08/15; additions to the original entry in bold , deletions in strikeout)	<p>In Section 2.2.2.2, RDPUDP_FEC_PAYLOAD_HEADER Structure, changed from:</p> <p>...</p> <p>uRange (1 byte): An unsigned 8-bit value that, when added to snSourceStart, yields the range of packets that are contained in the FEC payload.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>uRange (1 byte): An unsigned 8-bit value that, when added to snSourceStart, yields the last sequence number of a Source Packet that is contained in the FEC payload.</p> <p>...</p> <p>In Section 3.1.5.1.5, ACK and FEC Packets Data, changed from:</p> <p>...</p> <p>• The uRange variable MUST be set to the number of datagrams included in this FEC operation.</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>• The uRange variable MUST be set to the Source sequence number of the last datagram included in the FEC range minus snSourceStart.</p> <p>...</p> <p>In Section 3.1.1.6.1.3, Logarithms and Exponents, clarified the modulo operation and indented the first line of syntax in the pseudo-code examples</p> <p>Changed from:</p> <p>...</p>

Errata Published*	Description
	<p>Pseudo-code example:</p> <pre> reduction = 0x1d; m_ffExp2Poly[0] = 0x01; for (i = 1; i < m_fieldSize - 1; i++) ... Where m_fieldSize is 256 for GF(28) Logarithms are the inverse of exponents, and can be easily calculated by reversing the previous operation as shown in the following pseudo-code example: m_ffPoly2Exp[0] = 2 * m_fieldSize; // no exponential representation, doesn't exist for (i = 0; i < m_fieldSize - 1; i++) ... Changed to: ... Pseudo-code example: reduction = 0x1d; m_ffExp2Poly[0] = 0x01; for (i = 1; i < m_fieldSize - 1; i++) ... Where m_fieldSize is 256 for GF(28). Note that m_ffExp2Poly is modulo m_fieldSize - 1. In other words, m_ffExp2Poly[n] = m_ffExp2Poly[n + m_fieldSize - 1]. The pseudo-code in this document makes the assumption that m_ffExp2Poly is defined for at least m_fieldSize * 2 elements. Logarithms are the inverse of exponents, and can be easily calculated by reversing the previous operation as shown in the following pseudo-code example: m_ffPoly2Exp[0] = 2 * m_fieldSize; // no exponential representation, doesn't exist for (i = 0; i < m_fieldSize - 1; i++) ... In Section 3.1.1.6.4, Selecting the Coefficients Matrix, replaced the source sequence number 0xf with 0xff in the Matrix coefficient calculation figure and in the pseudo-code. Changed from: If the Source sequence numbers (section 3.1.1.2) for packets S1, S2, S3 ... Sn are s1, s2, s3 ... sn, the coefficient matrix is calculated as follows. Figure 12: Matrix coefficient calculation ... Only the last byte of the Source sequence number is used in calculating the coefficient. The fecIndex field described in the following pseudo-code example is equivalent to the uFecIndex field, as specified in section 2.2.2.2. The value of the </pre>

Errata Published*	Description
	<p>fecIndex field is updated using the following code prior to every call for encoding an FEC Packet:</p> <pre> if ((sn&0xf) >= (s1 &0xf) && ((fecIndex >= (s1 &0xf)) && (fecIndex <= (sn&0xf))) (sn&0xf) < (s1 &0xf) && ((fecIndex >= (s1 &0xf)) (fecIndex <= (sn&0xf)))) fecIndex = (sn+1) & 0xf; </pre> <p>Pseudo-code example:</p> <pre> ... for (int i=0; i < cLength; i++, ucOrigStart++) { BYTE e = Div(1, (*pucFecIndex)^ucOrigStart); pbCoEfficientArray[i] = (BYTE)m_ffPoly2Exp[e]; } ... for (int i=0; i < cLength; i++, ucOrigStart++) { BYTE e = Div(1, fecIndex^ucOrigStart); pbCoefficientArray[i] = (BYTE)m_ffPoly2Exp[e]; } ... </pre> <p>Changed to:</p> <p>If the Source sequence numbers (section 3.1.1.2) for packets S1, S2, S3 ... Sn are s1, s2, s3 ... sn, the coefficient matrix is calculated as follows.</p> <p>...</p> <p>Figure 12: Matrix coefficient calculation</p> <p>...</p> <p>Only the last byte of the Source sequence number is used in calculating the coefficient. The fecIndex field described in the following pseudo-code example is equivalent to the uFecIndex field, as specified in section 2.2.2.2. The value of the fecIndex field is updated using the following code prior to every call for encoding an FEC Packet:</p> <pre> if ((sn & 0xff) >= (s1 & 0xff) && ((fecIndex >= (s1 & 0xff)) && (fecIndex <= (sn & 0xff))) (sn & 0xff) < (s1 & 0xff) && ((fecIndex >= (s1 & 0xff)) (fecIndex <= (sn & 0xff)))) fecIndex = (sn + 1) & 0xff; </pre> <p>Pseudo-code example:</p> <pre> ... for (int i=0; i < cLength; i++, ucOrigStart++) { pbCoEfficientArray[i] = (BYTE)Div(1, (*pucFecIndex)^(ucOrigStart & 0xff)); } ... for (int i=0; i < cLength; i++, ucOrigStart++) </pre>

Errata Published*	Description																					
	<pre>{ pbCoefficientArray[i] = (BYTE)Div(1, fecIndex^(ucOrigStart & 0xff)); } ... In Section 4.2.2.1, Payload of an FEC Packet, updated the FEC Payload table values and the CoEff Array packet value. Changed from: The following is an example of an FEC Packet network payload.</pre> <table><tr><th>Sequence number</th><th>Size</th><th>Value</th></tr><tr><td>...</td><td>...</td><td>...</td></tr><tr><td>FEC Payload</td><td></td><td>0 66 208 168 239 37 29 238 180 193 24 58 66 252 233 126 172 211 135 31 206 27</td></tr><tr><td>...</td><td>...</td><td>...</td></tr></table> <p>The following are FEC encoding internals; these packets are not transferred on the wire:</p> <ul style="list-style-type: none">• CoEff Array [0 254 230 253 205] <p>...</p> <ul style="list-style-type: none">• RDPUDP_FEC_PAYLOAD_HEADER:: uRange = 5 <p>...</p> <p>Changed to:</p> <p>The following is an example of an FEC Packet network payload.</p> <table><tr><th>Sequence number</th><th>Size</th><th>Value</th></tr><tr><td>...</td><td>...</td><td>...</td></tr><tr><td>FEC Payload</td><td></td><td>0 203 146 55 209 198 69 147 95 141 120 66 86 91 174 141 153 99 169 49 31 14</td></tr></table> <p>The following are FEC encoding internals; these packets are not transferred on the wire:</p> <ul style="list-style-type: none">• CoEff Array [1 142 244 71 167] <p>...</p> <ul style="list-style-type: none">• RDPUDP_FEC_PAYLOAD_HEADER:: uRange = 5• RDPUDP_FEC_PAYLOAD_HEADER:: uRange = 4 <p>...</p>	Sequence number	Size	Value	FEC Payload		0 66 208 168 239 37 29 238 180 193 24 58 66 252 233 126 172 211 135 31 206 27	Sequence number	Size	Value	FEC Payload		0 203 146 55 209 198 69 147 95 141 120 66 86 91 174 141 153 99 169 49 31 14
Sequence number	Size	Value																				
...																				
FEC Payload		0 66 208 168 239 37 29 238 180 193 24 58 66 252 233 126 172 211 135 31 206 27																				
...																				
Sequence number	Size	Value																				
...																				
FEC Payload		0 203 146 55 209 198 69 147 95 141 120 66 86 91 174 141 153 99 169 49 31 14																				

*Date format: YYYY/MM/DD

[MS-RDPEV]: Remote Desktop Protocol: Video Redirection Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEV] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-RDPEVOR]: Remote Desktop Protocol: Video Optimized Remoting Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEVOR] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V8.0 – 2016/07/14](#).

Errata Published*	Description
2017/01/09	<p>Moved the description of effective utilization of transport from Section 2.1, Transport, to Section 1.5, Prerequisites/Preconditions.</p> <p>In Section 1.5, Prerequisites/Preconditions, changed from:</p> <p>...</p> <p>The Remote Desktop Protocol: Video Optimized Remoting Virtual Channel is dependent on the Microsoft::Windows::RDS::Graphics protocol, as defined in [MS-RDPEGFX]. The graphics channel MUST be opened before the Video Optimized Remoting Virtual channel is opened.</p> <p>This protocol is message-based. It assumes preservation of the packet as a whole and does not allow for fragmentation. Some messages can be lost and are described in section 2.</p> <p>Changed to:</p> <p>...</p> <p>The Remote Desktop Protocol: Video Optimized Remoting Virtual Channel is dependent on the Microsoft::Windows::RDS::Graphics protocol, as defined in [MS-RDPEGFX]. The graphics channel MUST be opened before the Video Optimized Remoting Virtual channel is opened.</p> <p>To ensure high-quality graphics content and effective utilization of the transport, continuous network characteristics detection SHOULD be enabled (as specified in [MS-RDPBCGR] sections 1.3.9 and 2.2.14) and the client SHOULD send the Client Multitransport Channel Data ([MS-RDPBCGR] section 2.2.1.3.8) to the server.</p> <p>This protocol is message-based. It assumes preservation of the packet as a whole and does not allow for fragmentation. Some messages can be lost and are described in section 2.</p> <p>In Section 2.1, Transport, changed from:</p> <p>...</p> <p>All PDUs except TSMM_VIDEO_DATA flow on the control channel, whereas TSMM_VIDEO_DATA flows on the data channel.</p>

Errata Published*	Description
	<p>To ensure that the transport is utilized effectively, continuous network characteristics detection SHOULD be enabled (as specified in [MS-RDPBCGR] sections 1.3.9 and 2.2.14) and the client SHOULD send the Client Multitransport Channel Data ([MS-RDPBCGR] section 2.2.1.3.8) to the server.</p> <p>Changed to:</p> <p>...</p> <p>All PDUs except TSMM_VIDEO_DATA flow on the control channel, whereas TSMM_VIDEO_DATA flows on the data channel.</p>

*Date format: YYYY/MM/DD

[MS-RDPEXPS]: Remote Desktop Protocol: XML Paper Specification (XPS) Print Virtual Channel Extension

This topic lists the Errata found in [MS-RDPEXPS] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-RDPRFX]: Remote Desktop Protocol: RemoteFX Codec Extension

This topic lists the Errata found in [MS-RDPRFX] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

Errata below are for Protocol Document Version [V17.0 – 2016/07/14](#).

Errata Published*	Description
2016/08/15	<p>In Section 3.1.8.2.5, Color Conversion (YCbCr to RGB), updated the figure with new color conversion (YCbCr to RGB) values: -3.43730 changed to -0.343730; 0.0 in the lower right element changed to 0.000013.</p> <p>Changed from:</p> $[RGB] = [YCbCr] \begin{bmatrix} 1.0 & 1.0 & 1.0 \\ 0.0 & -3.43730 & 1.769905 \\ 1.402525 & -0.71440 & 0.0 \end{bmatrix}$ <p>Changed to:</p> $[RGB] = [YCbCr] \begin{bmatrix} 1.0 & 1.0 & 1.0 \\ 0.0 & -0.343730 & 1.769905 \\ 1.402525 & -0.714401 & 0.000013 \end{bmatrix}$

*Date format: YYYY/MM/DD

[MS-RMPR]: Rights Management Services (RMS): Client-to-Server Protocol

This topic lists the Errata found in [MS-RMPR] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V35.0 – 2016/07/14](#).

Errata Published*	Description
2016/10/24	<p>In Section 3.1.4.4, Service Connection Point, added missing versions of Windows Server.</p> <p>Changed from:</p> <p>To facilitate the discovery of an RMS server, a service connection point (SCP) MAY<33> be defined in Active Directory. RMS clients and servers MAY<34> use the SCP to locate an RMS server that is capable of servicing requests for that directory. ...</p> <p><34> Section 3.1.4.4: Windows RMS clients will search Active Directory for the SCP unless one of the following registry keys is present.</p> <ul style="list-style-type: none">• "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\Activation" can be used to specify the location of the certification service, http(s)://servername/_wmcs/certification.• "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\EnterprisePublishing" can be used to specify the location of the licensing service, http(s)://servername/_wmcs/licensing. <p>In addition applications can specify an alternate service URL when invoking Windows APIs that would normally search Active Directory for the SCP.</p> <p>Windows RMS servers will search Active Directory for the SCP unless the GICURL value of one of the following registry keys contains the location of the certification service, http(s)://servername/_wmcs/certification.</p> <ul style="list-style-type: none">• For RMS 1.0 SP2 or earlier, the registry key is "HKEY_LOCAL_MACHINE\Software\Microsoft\DRMS\1.0".• For Windows Server 2008, the registry key is "HKEY_LOCAL_MACHINE\Software\Microsoft\DRMS\2.0".• For Windows Server 2008 R2, the registry key is "HKEY_LOCAL_MACHINE\Software\Microsoft\DRMS". <p>Changed to:</p> <p>To facilitate the discovery of an RMS server, a service connection point (SCP) MAY<31> be defined in Active Directory. RMS clients and servers MAY<32> use the SCP to locate an RMS server that is capable of servicing requests for that directory. ...</p>

Errata Published*	Description
	<p><32> Section 3.1.4.4: Windows RMS clients search Active Directory for the SCP unless one of the following registry keys is present.</p> <ul style="list-style-type: none"> • "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\Activation" can be used to specify the location of the certification service, http(s)://servername/_wmcs/certification. • "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSDRM\ServiceLocation\EnterprisePublishing" can be used to specify the location of the licensing service, http(s)://servername/_wmcs/licensing. <p>In addition, applications can specify an alternate service URL when invoking Windows APIs that would normally search Active Directory for the SCP.</p> <p>Windows RMS servers search Active Directory for the SCP unless the GICURL value of one of the following registry keys contains the location of the certification service, http(s)://servername/_wmcs/certification.</p> <ul style="list-style-type: none"> • For RMS 1.0 SP2 or earlier, the registry key is "HKEY_LOCAL_MACHINE\Software\Microsoft\DRMS\1.0". • For Windows Server 2008, the registry key is "HKEY_LOCAL_MACHINE\Software\Microsoft\DRMS\2.0". • For Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016, the registry key is "HKEY_LOCAL_MACHINE\Software\Microsoft\DRMS".
2016/08/01	<p>In several places in Section 2, added double quotation marks around element attribute values.</p> <p>In Section 2.2.9.7.5, OWNER, changed from:</p> <pre><ID type=[[- type -]] /></pre> <p>Changed to:</p> <pre><ID type="[[- type -]]" /></pre> <p>In Section 2.2.9.8, Encrypted Rights Data, changed from:</p> <pre><BODY type=[[- erdtype -]] ></pre> <p>Changed to:</p> <pre><BODY type="[[- erdtype -]]" ></pre> <p>In Section 2.2.9.8.5.1, METADATA, changed from:</p> <pre><ID type=[[- type -]] /></pre> <p>Changed to:</p> <pre><ID type="[[- type -]]" /></pre> <p>In Section 2.2.9.8.5.3, RIGHT, changed from:</p> <pre><RIGHT name=[[- rightname -]] ></pre> <p>Changed to:</p> <pre><RIGHT name="[[- rightname -]]" ></pre>

Errata Published*	Description
	<p>In Section 2.2.9.9.5, OWNER, changed from:</p> <pre><ID type=[[- type -]] /></pre> <p>Changed to:</p> <pre><ID type="[- type -]" /></pre> <p>In Section 2.2.9.9.6, RIGHT, changed from:</p> <pre><RIGHT name=[[- rightname -]] ></pre> <p>Changed to:</p> <pre><RIGHT name="[- rightname -]" ></pre> <p>In Section 2.2.9.10.4.2.1, RIGHT, changed from:</p> <pre><RIGHT name=[[- rightname -]] ></pre> <p>Changed to:</p> <pre><RIGHT name="[- rightname -]" ></pre>

*Date format: YYYY/MM/DD

[MS-RMSOD]: Rights Management Services Protocols Overview

This topic lists the Errata found in [MS-RMSOD] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

Errata below are for Protocol Document Version [V8.0 – 2016/09/26](#).

Errata Published*	Description
2017/03/06	<p>In Section 3.4, Example 4: Consuming Protected Content, added a note explaining that the Certify and FindService LocationsForUser are interchangeable.</p> <p>Added:</p> <p>Note In the preceding diagram, the Certify and FindServiceLocationsForUser calls are interchangeable. It is possible to call FindServiceLocationsForUser (to get the service location for GetClientLicensorCert) before calling Certify as long as both requests are completed before calling AcquireLicense.</p> <p>In Section 3.4.1.1, Activate the Computer, added the following text:</p> <p>In this example, activating the computer for client bootstrapping is the same as in Example 2. See section 3.2.1.1 for more details.</p> <p>Added a new section for finding service locations.</p> <p>Added:</p> <p>3.4.1.3 Find Service Locations</p> <p>In this example, finding service locations for client bootstrapping is the same as in Example 2. See section 3.2.1.2 for details.</p>

*Date format: YYYY/MM/DD

[MS-RPCE]: Remote Procedure Call Protocol Extensions

This topic lists the Errata found in the MS-RPCE 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.

Errata below are for Protocol Document Version [V28.0 - 2016/07/14](#).

Errata Published*	Description
2017/01/23	<p>In Section 2.2.1.2.5, ept_map Method, the description of the obj field has been changed from:</p> <p>obj: Optionally specifies an object UUID. A value of NULL indicates that no object UUID is specified.</p> <p>Changed to:</p> <p>obj: Optionally specifies an object UUID. A value of NULL indicates that no object UUID is specified. Interfaces registered with a NULL object UUID will match any object UUID supplied here.</p>

*Date format: YYYY/MM/DD

[MS-RPCH]: Remote Procedure Call over HTTP Protocol

This topic lists the Errata found in [MS-RPCH] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-RPRN]: Print System Remote Protocol

This topic lists the Errata found in [MS-RPRN] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-RRASM]: Routing and Remote Access Server (RRAS) Management Protocol

This topic lists the Errata found in [MS-RRASM] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-RSMC]: Remote Session Monitoring and Control Protocol

This topic lists the Errata found in [MS-RSMC] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V3.0 – 2016/07/14](#).

Errata Published*	Description
2017/01/09	<p>In this document:</p> <ul style="list-style-type: none">• Replaced "InputMessage" with "OutputMessage" in the WSDL message names in Sections 3.6.4.13.1.2, IMultiPointServer_Shutdown_OutputMessage Message, and 3.7.4.10.1.2, IMultiPointSession_GetThumbnailBits_OutputMessage Message• Updated section titles from 'GetSessionFlagsSession' to 'GetSessionFlags' in Section 3.7.4.12.2.1, GetSessionFlags, and 'GetSessionFlagsSessionResponse' to 'GetSessionFlagsResponse' in Section 3.7.4.12.2.2, GetSessionFlagsResponse. <p>In Section 3.6.4.13.1.2, IMultiPointServer_Shutdown_OutputMessage Message, changed from:</p> <p>A WSDL message containing the request for the Shutdown WSDL operation.</p> <p>The SOAP action value is:</p> <pre>http://MultiPoint/RemoteManagement/IMultiPointServer/Shutdown <wsdl:message name="IMultiPointServer_Shutdown_InputMessage"> <wsdl:part name="Shutdown" element="tns:Shutdown"/> </wsdl:message></pre> <p>Changed to:</p> <p>A WSDL message containing the request for the Shutdown WSDL operation.</p> <p>The SOAP action value is:</p> <pre>http://MultiPoint/RemoteManagement/IMultiPointServer/Shutdown <wsdl:message name="IMultiPointServer_Shutdown_OutputMessage"> <wsdl:part name="Shutdown" element="tns:Shutdown"/> </wsdl:message></pre>

Errata Published*	Description
	<p>In Section 3.7.4.10.1.2, IMultiPointSession_GetThumbnailBits_OutputMessage Message, changed from:</p> <p>A WSDL message containing the request for the GetThumbnailBits WSDL operation.</p> <p>The SOAP action value is:</p> <p>http://MultiPoint/RemoteManagement/IMultiPointSession/GetThumbnailBits <wsdl:message name="IMultiPointSession_GetThumbnailBits_InputMessage"> <wsdl:part name="GetThumbnailBits" element="tns:GetThumbnailBits"/> </wsdl:message></p> <p>Changed to:</p> <p>A WSDL message containing the request for the GetThumbnailBits WSDL operation.</p> <p>The SOAP action value is:</p> <p>http://MultiPoint/RemoteManagement/IMultiPointSession/GetThumbnailBits <wsdl:message name="IMultiPointSession_GetThumbnailBits_OutputMessage"> <wsdl:part name="GetThumbnailBits" element="tns:GetThumbnailBits"/> </wsdl:message></p> <p>Updated the title of Section 3.7.4.12.2.1, GetSessionFlagsSession, to 3.7.4.12.2.1, GetSessionFlags.</p> <p>Updated the title of Section 3.7.4.12.2.2, GetSessionFlagsSessionResponse, to 3.7.4.12.2.2 GetSessionFlagsResponse.</p>

*Date format: YYYY/MM/DD

[MS-RSVD]: Remote Shared Virtual Disk Protocol

This topic lists the Errata found in [MS-RSVD] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

September 26, 2016 - [Download](#)

Errata below are for Protocol Document Version [V9.0 – 2016/09/26](#).

Errata Published*	Description
2016/11/07	<p>In Section 2.2.3, Error Code, the description for STATUS_SVHDX_VERSION_MISMATCH has been changed from:</p> <p>Protocol version in request is not equal to 1.</p> <p>Changed to:</p> <p>Protocol version in request is not equal to 0x00000001 or 0x00000002.</p>
2016/11/07	<p>In Section 2.2.4.16, SVHDX_SHARED_VIRTUAL_DISK_SUPPORT_RESPONSE Structure, the constant SharedVirtualDiskCDPSnapshotsSupported has been renamed SharedVirtualDiskSnapshotsSupported and the description changed from:</p> <p>The server supports shared virtual disks and continuous data protection (log-based) snapshots.</p> <p>Changed to:</p> <p>The server supports shared virtual disks and all snapshot types defined in section 2.2.6.</p> <p>In Section 3.1.4.11, Application Requests Querying Shared Virtual Disk Support, the second paragraph has been changed from:</p> <p>The client MUST call the interface specified in [MS-SMB2] section 3.2.4.20.11, supplying the following input parameters:</p> <p>Changed to:</p> <p>The client MUST send an SVHDX_SHARED_VIRTUAL_DISK_SUPPORT_REQUEST structure,</p>

Errata Published*	Description
	<p>specified in section 2.2.4.15, by calling the interface specified in [MS-SMB2] section 3.2.4.20.11, supplying the following input parameters:</p> <p>In Section 3.2.5.6, Receiving a Query Shared Virtual Disk Support Request, the following paragraphs were changed from:</p> <p>If IsSVHDXSupported is TRUE, the server MUST set SharedVirtualDiskSupport to 1. Otherwise, the server SHOULD<19> set SharedVirtualDiskSupport to 0.</p> <p>If ServerServiceVersion is equal to RSVD Protocol version 1(0x00000001), the server MUST set SharedVirtualDiskSupport to SharedVirtualDisksSupported. If ServerServiceVersion is equal to RSVD Protocol version 2(0x00000002), the server MUST set SharedVirtualDiskSupport to SharedVirtualDiskCDPSnapshotsSupported. Otherwise, the server MUST fail the request with STATUS_INVALID_PARAMETER.</p> <p>The server MUST search the OpenTable where Open.FileName matches the file name.</p> <p>If no Open is found, the server MUST set SharedVirtualDiskHandleState to HandleStateNone.</p> <p>If any Open is found for which Open.LocalOpen matches the application-provided handle, the server MUST set SharedVirtualDiskHandleState to HandleStateShared.</p> <p>Otherwise, the server MUST set SharedVirtualDiskHandleState to HandleStateFileShared.</p> <p><19> Section 3.2.5.6: Windows Server 2012 R2 always sets SharedVirtualDiskSupport to 1.</p> <p>Changed to:</p> <p>The server MUST construct an SVHDX_SHARED_VIRTUAL_DISK_SUPPORT_RESPONSE structure, as specified in section 2.2.4.16, with the following values:</p> <ul style="list-style-type: none"> • If ServerServiceVersion is equal to RSVD Protocol version 1(0x00000001), the server MUST set the SharedVirtualDiskSupport field of the response to SharedVirtualDisksSupported. If ServerServiceVersion is equal to RSVD Protocol version 2(0x00000002), the server MUST set the SharedVirtualDiskSupport field of the response to SharedVirtualDiskSnapshotsSupported. • The server MUST search the OpenTable where Open.FileName matches the file name. If no Open is found, the server MUST set the SharedVirtualDiskHandleState field of the response to HandleStateNone. If any Open is found for which Open.LocalOpen matches the application-provided handle, the server MUST set the SharedVirtualDiskHandleState field of the response to HandleStateShared. Otherwise, the server MUST set the SharedVirtualDiskHandleState field of the response to HandleStateFileShared.
2016/11/07	<p>In Section 3.2.5.1, Receiving an Open Request, the fourth paragraph has been changed from:</p> <p>If ServerServiceVersion is RSVD Protocol version 1 and if the first 4 bytes, interpreted as little-endian, of the received context is not 0x00000001, the server MUST fail the request with STATUS_INVALID_PARAMETER.</p> <p>Changed to:</p>

Errata Published*	Description
	<p>If ServerServiceVersion is RSVD Protocol version 1 and if the first 4 bytes, interpreted as little-endian, of the received context is not 0x00000001, the server SHOULD<8> fail the request with STATUS_INVALID_PARAMETER.</p> <p><8> Section 3.2.5.1: Windows Server 2012 R2 without [MSKB-3025091] fail the operation with status code zero (0x00000000).</p> <p>The 11th paragraph has been changed from:</p> <p>If ServerServiceVersion is RSVD Protocol version 1 the server MUST construct a SVHDX_OPEN_DEVICE_CONTEXT_RESPONSE structure by setting all the fields to their respective values received in the request, and the server SHOULD<11> return the constructed SVHDX_OPEN_DEVICE_CONTEXT_RESPONSE and STATUS_SUCCESS to the client.</p> <p>Changed to:</p> <p>If ServerServiceVersion is RSVD Protocol version 1 and the first 4 bytes, interpreted as little-endian, of the received context is 0x00000001, the server MUST construct a SVHDX_OPEN_DEVICE_CONTEXT_RESPONSE structure by setting all the fields to their respective values received in the request, and the server SHOULD<11> return the constructed SVHDX_OPEN_DEVICE_CONTEXT_RESPONSE and STATUS_SUCCESS to the client.</p>

*Date format: YYYY/MM/DD

[MS-SAMR]: Security Account Manager (SAM) Remote Protocol (Client-to-Server)

This topic lists the Errata found in [MS-SAMR] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V37.0 – 2016/07/14](#).

Errata Published*	Description										
2017/01/23	<p>In Section 3.1.4.2, Default Accounts, added Windows 2000 Server to the product version information about the Group Policy Creator Owners group.</p> <p>Changed from:</p> <p>The following accounts MUST be present in a server's database.<36></p> <p><36> Section 3.1.4.2: The following tables list the Windows versions in which various accounts were introduced.</p> <p>...</p> <p>DC configuration, group accounts.</p> <table><tr><th>Name</th><th>Revision introduced</th></tr><tr><td>...</td><td>...</td></tr><tr><td>Group Policy Creator Owners</td><td>Windows XP</td></tr><tr><td>...</td><td>...</td></tr></table> <p>-----</p> <p>Changed to:</p> <p>The following accounts MUST be present in a server's database.<36></p> <p><36> Section 3.1.4.2: The following tables list the Windows versions in which various accounts were introduced.</p> <p>...</p> <p>DC configuration, group accounts.</p> <table><tr><th>Name</th><th>Revision introduced</th></tr></table>	Name	Revision introduced	Group Policy Creator Owners	Windows XP	Name	Revision introduced
Name	Revision introduced										
...	...										
Group Policy Creator Owners	Windows XP										
...	...										
Name	Revision introduced										

Errata Published*	Description						
	<table border="1"> <tr> <td data-bbox="402 226 922 279">...</td><td data-bbox="922 226 1429 279">...</td></tr> <tr> <td data-bbox="402 279 922 363">Group Policy Creator Owners</td><td data-bbox="922 279 1429 363">Windows 2000 Server Windows XP</td></tr> <tr> <td data-bbox="402 363 922 415">...</td><td data-bbox="922 363 1429 415">...</td></tr> </table> <p>-----</p>	Group Policy Creator Owners	Windows 2000 Server Windows XP
...	...						
Group Policy Creator Owners	Windows 2000 Server Windows XP						
...	...						
2016/08/01	<p>Updated three sections with additional information about USER_PROPERTY elements.</p> <p>In Section 2.2.10.1, USER_PROPERTIES, changed from:</p> <p>PropertyCount (2 bytes): The number of USER_PROPERTY elements in the UserProperties field.</p> <p>Changed to:</p> <p>PropertyCount (2 bytes): The number of USER_PROPERTY elements in the UserProperties field. When there are zero USER_PROPERTY elements in the UserProperties field, this field MUST be omitted; the resultant USER_PROPERTIES structure has a constant size of 0x6F bytes.</p> <p>In Section 3.1.1.8.10, userAccountControl, changed from:</p> <p>...</p> <p>6. If the UF_SMARTCARD_REQUIRED bit is set and is NOT present in the previous value, the dBCSPwd and unicodePwd attributes MUST be updated with 16 bytes of random bytes, and the supplementalCredentials attribute MUST be removed.</p> <p>Changed to:</p> <p>...</p> <p>6. If the UF_SMARTCARD_REQUIRED bit is set and is NOT present in the previous value, the dBCSPwd and unicodePwd attributes MUST be updated with 16 bytes of random bytes, and all USER_PROPERTY elements MUST be removed from the supplementalCredentials attribute.</p> <p>In Section 3.1.1.8.11.1.1, USER_PROPERTIES Processing, included the following paragraph in the section:</p> <p>When the last property-value pair is removed, the PropertyCount field is no longer included in the USER_PROPERTIES structure. In this state, the absence of any user properties MUST be inferred from the structure's total length (0x6F bytes).</p>						

*Date format: YYYY/MM/DD

[MS-SFMWA]: Server and File Management Web APIs

This topic lists the Errata found in [MS-SFMWA] 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.

Errata below are for Protocol Document Version [V1.0 - 2016/07/14](#).

Errata Published*	Description
2017/03/06	<p>In Section 3.3.5.1.1, GET, updated the example URI to include a more complete definition of how it should be constructed.</p> <p>Changed from:</p> <p>...</p> <p>items/index/{index}/count/{count}?path={path}&filter={filter}&sortByfield={sortByfield}&ascending={ascending}</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>https://<ServerName>/services/builtin/fileoperationservice.svc/items/index/{index}/count/{count}?path={path}&filter={filter}&sortByfield={sortByfield}&ascending={ascending}</p> <p>...</p> <p>In Section 3.3.5.2.1, GET, updated the example URI to include a more complete definition of how it should be constructed.</p> <p>Changed from:</p> <p>...</p> <p>items/index/{index}/count/{count}/search?query={query}&sortByfield={sortByfield}&ascending={ascending}&scope={scope}&timeoutseconds={timeoutseconds}</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>https://<ServerName>/services/builtin/fileoperationservice.svc/items/index/{index}/count/{count}/search?query={query}&sortByfield={sortByfield}&ascending={ascending}&scope={scope}&timeoutseconds={timeoutseconds}</p> <p>...</p> <p>In Section 3.3.5.3.1, GET, updated the example URI to include a more complete definition of how it should be constructed.</p> <p>Changed from:</p> <p>...</p>

Errata Published*	Description
	<p>folder/newsubfoldername?path={path}&language={language}</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>https://<ServerName>/services/builtin/fileoperationservice.svc/folder/newsubfoldername?path={path}&language={language}</p> <p>...</p>
2017/03/06	<p>In Section 3.15.5.2, /notification/unsubscribe?deviceid={deviceid}, added a description for deviceid.</p> <p>Changed from:</p> <p>deviceid:</p> <p>...</p> <p>Changed to:</p> <p>deviceid: The ID of the device.</p> <p>...</p>
2017/03/06	<p>In Sections 2.2.3.30 and 2.2.3.31, updated the code fragments to reflect that these flags have a Boolean value.</p> <p>In Section 2.2.3.30, overwrite, changed from:</p> <p>String = *(%x20-7E) overwrite = String</p> <p>-----</p> <p>Changed to:</p> <p>overwrite = TRUE FALSE</p> <p>In Section 2.2.3.31, overwritepermissions, changed from:</p> <p>String = *(%x20-7E) overwritepermissions = String</p> <p>Changed to:</p> <p>overwritepermissions = TRUE FALSE</p>
2017/03/06	<p>In Sections 2.2.4.2 through 2.2.4.23, updated the element restriction attributes (the minOccurs values) in the code fragments.</p> <p>For example, in Section 2.2.4.3, ArrayOfConnectionInfo, changed the minOccurs value for this complex type from 1 to 0.</p>

Errata Published*	Description																								
	<p>Changed from:</p> <pre><xs:element minOccurs="1" maxOccurs="unbounded" name="ConnectionInfo" nillable="true" type="tnsl:ConnectionInfo"/></pre> <p>Changed to:</p> <pre><xs:element minOccurs="0" maxOccurs="unbounded" name="ConnectionInfo" nillable="true" type="tnsl:ConnectionInfo"/></pre>																								
2017/02/20	<p>In Section 7, Appendix B: Full Xml Schema, changed the namespace prefix for http://schemas.microsoft.com/Message from "q6, q7" to "tns10".</p> <p>Changed from:</p> <table><tr><th>Schema name</th><th>Prefix</th><th>Section</th></tr><tr><td>...</td><td>...</td><td>...</td></tr><tr><td>http://schemas.microsoft.com/Message</td><td>q6, q7</td><td>7.9</td></tr><tr><td>...</td><td>..</td><td>...</td></tr></table> <p>Changed to:</p> <table><tr><th>Schema name</th><th>Prefix</th><th>Section</th></tr><tr><td>...</td><td>...</td><td>...</td></tr><tr><td>http://schemas.microsoft.com/Message</td><td>tns10</td><td>7.9</td></tr><tr><td>...</td><td>...</td><td>...</td></tr></table>	Schema name	Prefix	Section	http://schemas.microsoft.com/Message	q6, q7	7.9	Schema name	Prefix	Section	http://schemas.microsoft.com/Message	tns10	7.9
Schema name	Prefix	Section																							
...																							
http://schemas.microsoft.com/Message	q6, q7	7.9																							
...																							
Schema name	Prefix	Section																							
...																							
http://schemas.microsoft.com/Message	tns10	7.9																							
...																							
2017/02/20	<p>Throughout Section 2.2.4, Complex Types, changed the type from DateTime to xs:dateTime in 11 complex type definitions.</p> <p>In Section 2.2.4.1, AlertInfo, changed from:</p> <pre>...</pre> <pre><xs:element minOccurs="0" maxOccurs="1" name="DateAndTime" type="DateTime"/></pre> <pre>...</pre> <p>Changed to:</p> <pre>...</pre> <pre><xs:element minOccurs="0" maxOccurs="1" name="DateAndTime"</pre>																								

Errata Published*	Description
	<pre> type="xs:dateTime"/> ... In Section 2.2.4.26, ConnectionInfo, changed from: ... <xs:element minOccurs="0" maxOccurs="1" name="EndTime" type="DateTime"/> <xs:element minOccurs="0" maxOccurs="1" name="ServiceType" nillable="true" type="xs:string"/> <xs:element minOccurs="0" maxOccurs="1" name="StartTime" type="DateTime"/> ... ----- Changed to: ... <xs:element minOccurs="0" maxOccurs="1" name="EndTime" type="xs:dateTime"/> <xs:element minOccurs="0" maxOccurs="1" name="ServiceType" nillable="true" type="xs:string"/> <xs:element minOccurs="0" maxOccurs="1" name="StartTime" type="xs:dateTime"/> ... In Section 2.2.4.32, ItemInfo, changed from: ... <xs:element minOccurs="0" maxOccurs="1" name="CreateTime" type="DateTime"/> <xs:element minOccurs="0" maxOccurs="1" name="CreateTimeUtc" type="DateTime"/> <xs:element minOccurs="0" maxOccurs="1" name="IsDirectory" type="xs:boolean"/> <xs:element minOccurs="0" maxOccurs="1" name="ModifiedTime" type="DateTime"/> <xs:element minOccurs="0" maxOccurs="1" name="ModifiedTimeUtc" type="DateTime"/> ... Changed to: ... <xs:element minOccurs="0" maxOccurs="1" name="CreateTime" type="xs:dateTime"/> <xs:element minOccurs="0" maxOccurs="1" name="CreateTimeUtc" type="xs:dateTime"/> <xs:element minOccurs="0" maxOccurs="1" name="IsDirectory" type="xs:boolean"/> <xs:element minOccurs="0" maxOccurs="1" name="ModifiedTime" type="xs:dateTime"/> <xs:element minOccurs="0" maxOccurs="1" name="ModifiedTimeUtc" type="xs:dateTime"/> ... In Section 2.2.4.47, MSOLicenseSubscription, changed from: </pre>

Errata Published*	Description
	<p>...</p> <pre><xs:element minOccurs="0" maxOccurs="1" name="BillingExpirationTime" type="DateTime"/></pre> <p>...</p> <p>Changed to:</p> <p>...</p> <pre><xs:element minOccurs="0" maxOccurs="1" name="BillingExpirationTime" type="xs:dateTime"/></pre> <p>...</p> <p>In Section 2.2.4.51, PartialCollection_Of_AlertInfo, changed from:</p> <p>...</p> <pre><xs:element minOccurs="0" maxOccurs="1" name="CollectionModified" type="DateTime"/></pre> <p>...</p> <p>Changed to:</p> <p>...</p> <pre><xs:element minOccurs="0" maxOccurs="1" name="CollectionModified" type="xs:dateTime"/></pre> <p>...</p> <p>In Section 2.2.4.52, PartialCollection_Of_ConnectionInfo, changed from:</p> <p>...</p> <pre><xs:element minOccurs="0" maxOccurs="1" name="CollectionModified" type="DateTime"/></pre> <p>...</p> <p>Changed to:</p> <p>...</p> <pre><xs:element minOccurs="0" maxOccurs="1" name="CollectionModified" type="xs:dateTime"/></pre> <p>...</p> <p>In Section 2.2.4.53, PartialCollection_Of_DeviceInfo, changed from:</p> <p>...</p> <pre><xs:element minOccurs="0" maxOccurs="1" name="CollectionModified"</pre>

Errata Published*	Description
	<pre> type="DateTime"/> ... Changed to: ... <xs:element minOccurs="0" maxOccurs="1" name="CollectionModified" type="xs:dateTime"/> ... In Section 2.2.4.54, PartialCollection_Of_DriveInfo, changed from: ... <xs:element minOccurs="0" maxOccurs="1" name="CollectionModified" type="DateTime"/> ... Changed to: ... <xs:element minOccurs="0" maxOccurs="1" name="CollectionModified" type="xs:dateTime"/> ... In Section 2.2.4.55 PartialCollection_Of_FolderInfo, changed from: ... <xs:element minOccurs="0" maxOccurs="1" name="CollectionModified" type="DateTime"/> ... Changed to: ... <xs:element minOccurs="0" maxOccurs="1" name="CollectionModified" type="xs:dateTime"/> ... In Section 2.2.4.56 PartialCollection_Of_UserInfo, changed from: ... <xs:element minOccurs="0" maxOccurs="1" name="CollectionModified" type="DateTime"/> </pre>

Errata Published*	Description
	<p>...</p> <p>Changed to:</p> <p>...</p> <pre><xs:element minOccurs="0" maxOccurs="1" name="CollectionModified" type="xs:dateTime"/></pre> <p>...</p> <p>In Section 2.2.4.64, ServerInfo, changed from:</p> <p>...</p> <pre><xs:element minOccurs="0" maxOccurs="1" name="ServerUtcNow" type="DateTime"/></pre> <p>...</p> <p>Changed to:</p> <p>...</p> <pre><xs:element minOccurs="0" maxOccurs="1" name="ServerUtcNow" type="xs:dateTime"/></pre> <p>...</p>
2017 /02/ 20	<p>In Section 2.2.4.50, MSOUser, added the missing FirstName and LastName attributes to the definition of the MSOUser complex type.</p> <p>Changed from:</p> <p>...</p> <pre><xs:complexType name="MSOUser"> <xs:sequence> <xs:element minOccurs="0" name="Activated" type="xs:boolean" /> <xs:element minOccurs="0" name="Licenses" nillable="true" xmlns:q1="http://schemas.datacontract.org/2004/07/System.Collections.ObjectModel" type="q1:ReadOnlyCollectionOfMSOLicensePGX Pb6b" /> <xs:element minOccurs="0" name="LocalUserName" nillable="true" type="xs:string" /> <xs:element minOccurs="0" name="ObjectId" type="ser:guid" /> <xs:element minOccurs="0" name="UserPrincipalName" nillable="true" type="xs:string" /> </xs:sequence> </xs:complexType></pre> <p>...</p> <p>Changed to:</p> <p>...</p> <pre><xs:complexType name="MSOUser"> <xs:sequence></pre>

Errata Published*	Description
	<pre> <xs:element minOccurs="0" name="Activated" type="xs:boolean" /> <xs:element minOccurs="0" maxOccurs="1" name="FirstName" nillable="true" type="xs:string"/> <xs:element minOccurs="0" maxOccurs="1" name="LastName" nillable="true" type="xs:string"/> <xs:element minOccurs="0" name="Licenses" nillable="true" xmlns:q1="http://schemas.datacontract.org/2004/07/System.Collections.ObjectModel" type="q1:ReadOnlyCollectionOfMSOLicensePGX_Pb6b" /> <xs:element minOccurs="0" name="LocalUserName" nillable="true" type="xs:string" /> <xs:element minOccurs="0" name="ObjectId" type="ser:guid" /> <xs:element minOccurs="0" name="UserPrincipalName" nillable="true" type="xs:string" /> </xs:sequence> </xs:complexType> </pre> <p>...</p>

*Date format: YYYY/MM/DD

[MS-SMB]: Server Message Block (SMB) Protocol

This topic lists the Errata found in [MS-SMB] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

Errata below are for Protocol Document Version [V45.0 – 2016/07/14](#).

Errata Published*	Description
2017/01/09	<p>In Section 3.3.1.1, Global, added:</p> <p>Server.Snapshotlist: The list of available snapshots.</p> <p>In Section 3.3.3, Initialization, added:</p> <p>Server.Snapshotlist MUST be set to zero.</p> <p>In Section 3.3.5.11.1.1, Receiving an FSCTL_SRV_ENUMERATE_SNAPSHOTS Function Code, the second sentence was changed to:</p> <p>The server SHOULD<135> refresh the Server.Snapshotlist and return an enumeration of available previous versions, as specified in section 2.2.7.2.2.</p> <p>FSCTL_ENUMERATE_SNAPSHOTS was changed to FSCTL_SRV_ENUMERATE_SNAPSHOTS.</p> <p>In Section 6, Appendix A: Product Behavior, a PBN was added:</p> <p><135> Section 3.3.5.11.1.1: If MaxDataCount is not 0x10, Windows servers do not refresh the Server.Snapshotlist.</p>
2016/11/07	<p>In Section 3.3.5.11.2, Receiving an NT_TRANS_QUERY_QUOTA Request, the second paragraph has been changed from:</p> <p>The server MUST return as much of the available quota information that is able to fit in the maximum response buffer size denoted by MaxDataCount. If the entire quota information cannot fit in the response buffer, then the server MUST return a status of STATUS_BUFFER_TOO_SMALL. Otherwise, the server MUST return STATUS_SUCCESS. The format of the request determines which entries need to be returned, as specified in section 2.2.7.5.1. The server MUST place the quota information in the response, as specified in section 2.2.7.5.2, and send the response back to the client.</p>

Errata Published*	Description								
	<p>Changed to:</p> <p>The format of the request determines which entries need to be returned, as specified in section 2.2.7.5.1. The server MUST place the quota information in the response, as specified in section 2.2.7.5.2, and send the response back to the client.</p>								
2016/10/24	<p>In various sections, added information on a missing flag and field.</p> <p>In Section 2.2.4.9.1, Client Request Extensions, made two changes.</p> <p>Added the following bullet point:</p> <ul style="list-style-type: none"> • An additional flag bit is added to the CreateOptions field. The additional flag, FILE_OPEN_REPARSE_POINT, is used to open a reparse point file itself. <p>Added a definition for the CreateOptions field:</p> <p>CreateOptions (4 bytes): A 32-bit field containing flag options for creating a file or directory. In addition to the flags specified in [MS-CIFS] section 2.2.4.64, the following modifications and extensions apply to the CreateOptions field. FILE_OPEN_REPARSE_POINT is a new flag to SMB. The CreateOptions field MUST be set to 0x00000000 or to a combination of the flags specified in the [MS-CIFS] section 2.2.4.64 CreateOptions table and the following table. Unused bit fields SHOULD be set to 0 when sent and MUST be ignored on receipt. Server implementations SHOULD reserve all bits not specified in the [MS-CIFS] section 2.2.4.64 CreateOptions table and the following table.</p> <table data-bbox="394 869 1430 1050"> <tr> <th>Name and bitmask</th><th>Meaning</th></tr> <tr> <td>FILE_OPEN_REPARSE_POINT 0x00200000</td><td>If the file or directory being opened is a reparse point, open the reparse point itself rather than the target that the reparse point references.</td></tr> </table> <p>In Section 2.2.7.1.1, Client Request Extensions, made two changes.</p> <p>Added the following bullet point:</p> <ul style="list-style-type: none"> • An additional flag bit is added to the CreateOptions field. The additional flag, FILE_OPEN_REPARSE_POINT, is used to open a reparse point file itself. <p>Added a definition for the CreateOptions field:</p> <p>CreateOptions (4 bytes): A 32-bit field containing flag options for creating a file or directory. In addition to the flags specified in [MS-CIFS] section 2.2.4.64, the following modifications and extensions apply to the CreateOptions field. FILE_OPEN_REPARSE_POINT is a new flag to SMB. The CreateOptions field MUST be set to 0x00000000 or to a combination of the flags specified in the [MS-CIFS] section 2.2.4.64 CreateOptions table and the following table. Unused bit fields SHOULD be set to 0 when sent and MUST be ignored on receipt. Server implementations SHOULD reserve all bits not specified in the [MS-CIFS] section 2.2.4.64 CreateOptions table and the following table.</p> <table data-bbox="394 1501 1430 1682"> <tr> <th>Name and bitmask</th><th>Meaning</th></tr> <tr> <td>FILE_OPEN_REPARSE_POINT 0x00200000</td><td>If the file or directory being opened is a reparse point, open the reparse point itself rather than the target that the reparse point references.</td></tr> </table> <p>In Section 2.2.7.1.2, Server Response Extensions, added the following sentence:</p>	Name and bitmask	Meaning	FILE_OPEN_REPARSE_POINT 0x00200000	If the file or directory being opened is a reparse point, open the reparse point itself rather than the target that the reparse point references.	Name and bitmask	Meaning	FILE_OPEN_REPARSE_POINT 0x00200000	If the file or directory being opened is a reparse point, open the reparse point itself rather than the target that the reparse point references.
Name and bitmask	Meaning								
FILE_OPEN_REPARSE_POINT 0x00200000	If the file or directory being opened is a reparse point, open the reparse point itself rather than the target that the reparse point references.								
Name and bitmask	Meaning								
FILE_OPEN_REPARSE_POINT 0x00200000	If the file or directory being opened is a reparse point, open the reparse point itself rather than the target that the reparse point references.								

Errata Published*	Description
	<p>If the FILE_OPEN_REPARSE_POINT flag bit is set in CreateOptions, and there is a symbolic link error, the server MUST return STATUS_STOPPED_ON_SYMLINK to the client.</p> <p>In Section 3.3.5.5, Receiving an SMB_COM_NT_CREATE_ANDX Request, added the following paragraphs:</p> <p>If any intermediate component of the path specified in the create request is a symbolic link, the server MUST return an error as specified in section 2.2.7.1.2. Symbolic links MUST NOT be evaluated by the server.</p> <p>If the final component of the path is a symbolic link, the server behavior depends on whether the flag FILE_OPEN_REPARSE_POINT is specified in the CreateOptions field of the request. If FILE_OPEN_REPARSE_POINT is specified, the server MUST open the underlying file or directory and return a handle to it. Otherwise, the server MUST return an error as specified in section 2.2.7.1.2.</p>

*Date format: YYYY/MM/DD

[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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

September 26, 2016 - [Download](#)

Errata below are for Protocol Document Version [V50.0 – 2016/09/26](#).

Errata Published*	Description
2017/02/20	<p>In Section 2.2.24.1, Oplock Break Acknowledgment. Section 2.2.24.2, Lease Break Acknowledgment, and Section 2.2.26, SMB2 LOCK Request, the following was added to the first paragraph:</p> <p>This message is composed of an SMB2 header, as specified in section 2.2.1, followed by this acknowledgement structure.</p>
2017/01/09	<p>In Section 3.2.4.24, Application Requests Canceling an Operation, the SessionId field initialization was changed to:</p> <p>The SessionId field MUST be set to the session identifier that is previously used for the request being canceled. If the session identified by SessionId has Session.SigningRequired equal to TRUE, the client sets SMB2_FLAGS_SIGNED to TRUE in the Flags field. The SMB2 CANCEL Request MUST be initialized to the default values, as specified in 2.2.30.</p> <p>In Section 3.3.5.16, Receiving an SMB2 CANCEL Request, the following paragraph was added:</p> <p>If SMB2_FLAGS_SIGNED bit is set in the Flags field of the SMB2 header of the cancel request, the server MUST verify the session, as specified in section 3.3.5.2.9.</p> <p>In Section 6, Appendix A Product Behavior, Product Behavior Note 145 associated with the change in Section 3.2.4.24 was removed.</p>
2017/01/09	<p>In Section 3.2.5.1.1, Decrypting the Message, the third bullet point was changed from:</p> <p>The client MUST look up the session in the Connection.SessionTable using the SessionId in the SMB2 TRANSFORM_HEADER of the response. If the session is not found, the response MUST be discarded as invalid.</p> <p>Changed to:</p>

Errata Published*	Description
	<p>The client MUST look up the session in the Connection.SessionTable using the SessionId in the SMB2 TRANSFORM_HEADER of the response. If the session is not found, the response MUST be discarded.</p> <p>A new bullet point was added:</p> <p>If the NextCommand field in the first SMB2 header of the message is equal to 0 and SessionId of the first SMB2 header is not equal to the SessionId field in SMB2 TRANSFORM_HEADER of response, the client MUST discard the message.</p> <p>In Section 3.2.5.1.9, Handling Compounded Responses, the following additions were made.</p> <p>For the first response:</p> <ul style="list-style-type: none"> • If SMB2_FLAGS_RELATED_OPERATIONS is set in the Flags field of the SMB2 header of response, the client SHOULD<152> discard the message. • If the SessionId field of SMB2 header is not equal to the SessionId field in SMB2 TRANSFORM_HEADER of response, the client MUST discard the message. <p>For each subsequent response:</p> <ul style="list-style-type: none"> • If SMB2_FLAGS_RELATED_OPERATIONS is not set in the Flags field of the SMB2 header of the response, the client SHOULD<153> discard the message. • If the SessionId field of SMB2 header is not equal to the SessionId field in the SMB2 TRANSFORM_HEADER of response, the client MUST discard the message. <p><152> Section 3.2.5.1.9: Windows 8, Windows Server 2012, Windows 8.1 and Windows Server 2012 R2 ignore this flag.</p> <p><153> Section 3.2.5.1.9: Windows 8, Windows Server 2012, Windows 8.1 and Windows Server 2012 R2 discard the message if SMB2_FLAGS_RELATED_OPERATIONS is set in the Flags field of the SMB2 header of the response.</p> <p>In Section 3.3.5.2.7.2, Handling Compounded Related Requests, the last paragraph was changed from:</p> <p>When all operations are complete, the responses SHOULD be compounded into a single response to return to the client. If the responses are compounded, the server MUST set SMB2_FLAGS_RELATED_OPERATIONS in the Flags field of the SMB2 header of all responses except the first one. This indicates that the response was part of a compounded chain.</p> <p>Changed to:</p> <p>When all operations are complete, the responses SHOULD be compounded into a single response to return to the client. If the responses are compounded, the server SHOULD set SMB2_FLAGS_RELATED_OPERATIONS in the Flags field of the SMB2 header of all responses except the first one. This indicates that the response was part of a compounded chain.</p>
2016/12/19	<p>In Section 3.3.5.15.6, Handling a Server-Side Data Copy Request, changed the field name OutputCount to MaxOutputResponse.</p> <p>Changed from:</p>

Errata Published*	Description
	<p>...</p> <p>If the OutputCount value in the SMB2 IOCTL Request is less than the size of the SRV_COPYCHUNK_RESPONSE structure, the server MUST fail the SMB2 IOCTL Request with STATUS_INVALID_PARAMETER.</p> <p>If the OutputCount value in the SMB2 IOCTL Request is greater than or equal to the size of the SRV_COPYCHUNK_RESPONSE structure and any of the following are true, the server MUST send an SMB2 IOCTL Response as specified in section 3.3.5.15.6.2:</p> <p>...</p> <p>Changed to:</p> <p>...</p> <p>If the MaxOutputResponse value in the SMB2 IOCTL Request is less than the size of the SRV_COPYCHUNK_RESPONSE structure, the server MUST fail the SMB2 IOCTL Request with STATUS_INVALID_PARAMETER.</p> <p>If the MaxOutputResponse value in the SMB2 IOCTL Request is greater than or equal to the size of the SRV_COPYCHUNK_RESPONSE structure and any of the following are true, the server MUST send an SMB2 IOCTL Response as specified in section 3.3.5.15.6.2:</p> <p>...</p>
2016/11/21	<p>In two sections, modified the processing rules for change notifications.</p> <p>In Section 3.3.1.3, Algorithm for Change Notifications in an Object Store, changed from:</p> <p>...</p> <ul style="list-style-type: none"> • If a change notification request is pending on a directory AND a change occurs to the directory contents matching the events to be monitored as specified in CompletionFilter, the server MUST copy the results into the buffer of the Change Notification response. The server MAY choose to aggregate one or more changes indicated by the underlying object store into a single response. The server MUST construct a SMB2 CHANGE_NOTIFY Response as specified in section 2.2.36. The server MUST then return the results to the client. • The server SHOULD try to fit in the maximum number of events that match the CompletionFilter of the request before completing the request. • If a client issues multiple change notification requests on the same open to a directory, the server MUST queue the requests and complete them on a First In, First Out (FIFO) basis when changes are indicated by the underlying object store. • If the client requested that an entire tree be watched, the server MUST monitor all objects beneath the directory on which the operation was issued, instead of simply the immediate children of that directory. • Change notification information that is returned to the user MUST conform to the syntax specified in section 2.4.42. <p>Changed to:</p> <p>...</p> <ul style="list-style-type: none"> • The algorithm MUST perform the change notification processing based on the CompletionFilter and SMB2_WATCH_TREE flag in the Flags field of the first CHANGE_NOTIFY request on an Open.LocalOpen. The algorithm MUST ignore the CompletionFilter and SMB2_WATCH_TREE flag in all further requests on the same open.

Errata Published*	Description										
	<ul style="list-style-type: none"> • If the client sets the SMB2_WATCH_TREE flag in the Flags field of the first request on an Open.LocalOpen, indicating that an entire tree is being watched, the algorithm MUST monitor all objects beneath the directory on which the operation was issued, instead of simply the immediate children objects of that directory. • If a client issues multiple change notification requests on the same open to a directory, the server MUST queue the requests and complete them on a First In, First Out (FIFO) basis when changes are indicated by the underlying object store. • If a change notification request is pending on a directory and a change occurs to the directory contents matching the events to be monitored as specified by the CompletionFilter, the server MUST copy the results into the Buffer field of the CHANGE_NOTIFY response. The server SHOULD send the maximum number of events that match the CompletionFilter of the first CHANGE_NOTIFY request indicated by the underlying object store into a single response up to the maximum of the OutputBufferLength field. The server MUST construct the response in the format specified in section 2.2.36 and the change notification information in the format specified in [MS-FSCC] section 2.4.42. The server MUST then return the results to the client. <p>In Section 3.3.5.19, Receiving an SMB2 CHANGE_NOTIFY Request, changed from:</p> <p>Change notification processing in the object store MUST be handled as specified in section 3.3.1.3. It is also outlined in [MS-CIFS] section 3.3.5.9.4.</p> <p>Changed to:</p> <p>The server MUST process a change notification request in the object store as specified by the algorithm in section 3.3.1.3.</p>										
2016/11/07	<p>In Section 2.2.33, SMB2 QUERY_DIRECTORY Request, the values in the Flags field have been changed from:</p> <table border="1" data-bbox="391 1167 1430 1713"> <thead> <tr> <th>Value</th><th>Meaning</th></tr> </thead> <tbody> <tr> <td>SMB2_RESTART_SCANS 0x01</td><td>The server MUST restart the enumeration from the beginning, but the search pattern is not changed.</td></tr> <tr> <td>SMB2_RETURN_SINGLE_ENTRY 0x02</td><td>The server MUST only return the first entry of the search results.</td></tr> <tr> <td>SMB2_INDEX_SPECIFIED 0x04</td><td>The server SHOULD<64> return entries beginning at the byte number specified by FileIndex.</td></tr> <tr> <td>SMB2_REOPEN 0x10</td><td>The server MUST restart the enumeration from the beginning, and the search pattern MUST be changed to the provided value. This often involves silently closing and reopening the directory on the server side. SMB2_REOPEN implies SMB2_RESTART_SCANS as well.</td></tr> </tbody> </table>	Value	Meaning	SMB2_RESTART_SCANS 0x01	The server MUST restart the enumeration from the beginning, but the search pattern is not changed.	SMB2_RETURN_SINGLE_ENTRY 0x02	The server MUST only return the first entry of the search results.	SMB2_INDEX_SPECIFIED 0x04	The server SHOULD<64> return entries beginning at the byte number specified by FileIndex.	SMB2_REOPEN 0x10	The server MUST restart the enumeration from the beginning, and the search pattern MUST be changed to the provided value. This often involves silently closing and reopening the directory on the server side. SMB2_REOPEN implies SMB2_RESTART_SCANS as well.
Value	Meaning										
SMB2_RESTART_SCANS 0x01	The server MUST restart the enumeration from the beginning, but the search pattern is not changed.										
SMB2_RETURN_SINGLE_ENTRY 0x02	The server MUST only return the first entry of the search results.										
SMB2_INDEX_SPECIFIED 0x04	The server SHOULD<64> return entries beginning at the byte number specified by FileIndex.										
SMB2_REOPEN 0x10	The server MUST restart the enumeration from the beginning, and the search pattern MUST be changed to the provided value. This often involves silently closing and reopening the directory on the server side. SMB2_REOPEN implies SMB2_RESTART_SCANS as well.										

Errata Published*	Description										
	<p>Changed to:</p> <table border="1" data-bbox="391 459 1430 903"> <thead> <tr> <th>Value</th><th>Meaning</th></tr> </thead> <tbody> <tr> <td>SMB2_RESTART_SCANS 0x01</td><td>The server MUST restart the enumeration from the beginning as specified in section 3.3.5.18.</td></tr> <tr> <td>SMB2_RETURN_SINGLE_ENTRY 0x02</td><td>The server MUST only return the first entry of the search results.</td></tr> <tr> <td>SMB2_INDEX_SPECIFIED 0x04</td><td>The server SHOULD<64> return entries beginning at the byte number specified by FileIndex.</td></tr> <tr> <td>SMB2_REOPEN 0x10</td><td>The server MUST restart the enumeration from the beginning, and the search pattern MUST be changed to the provided value.</td></tr> </tbody> </table> <p>In Section 3.3.1.10, Per Open, the following was removed:</p> <ul style="list-style-type: none"> • Open.EnumerationLocation: For directories, this value indicates the current location in a directory enumeration and allows for the continuing of an enumeration across multiple requests. For files, this value is unused. • Open.EnumerationSearchPattern: For directories, this value holds the search pattern that is used in directory enumeration and allows for the continuing of an enumeration across multiple requests. For files, this value is unused. <p>In Section 3.3.5.9, Receiving an SMB2 CREATE Request, the following was removed:</p> <ul style="list-style-type: none"> • Open.EnumerationLocation is set to 0. • Open.EnumerationSearchPattern is set to an empty string. <p>In Section 3.3.5.18, Receiving an SMB2 QUERY_DIRECTORY Request, the following was changed from:</p> <p>If any other information class is specified in the FileInformationClass field of the SMB2 QUERY_DIRECTORY Request, the server MUST fail the operation with STATUS_INVALID_INFO_CLASS. If the information class requested is not supported by the server, the server MUST fail the request with STATUS_NOT_SUPPORTED.</p> <p>If SMB2_REOPEN is set in the Flags field of the SMB2 QUERY_DIRECTORY Request, the server SHOULD<343> set Open.EnumerationLocation to 0 and Open.EnumerationSearchPattern to an empty string.</p> <p>If SMB2_RESTART_SCANS is set in the Flags field of the SMB2 QUERY_DIRECTORY Request, the</p>	Value	Meaning	SMB2_RESTART_SCANS 0x01	The server MUST restart the enumeration from the beginning as specified in section 3.3.5.18.	SMB2_RETURN_SINGLE_ENTRY 0x02	The server MUST only return the first entry of the search results.	SMB2_INDEX_SPECIFIED 0x04	The server SHOULD<64> return entries beginning at the byte number specified by FileIndex.	SMB2_REOPEN 0x10	The server MUST restart the enumeration from the beginning, and the search pattern MUST be changed to the provided value.
Value	Meaning										
SMB2_RESTART_SCANS 0x01	The server MUST restart the enumeration from the beginning as specified in section 3.3.5.18.										
SMB2_RETURN_SINGLE_ENTRY 0x02	The server MUST only return the first entry of the search results.										
SMB2_INDEX_SPECIFIED 0x04	The server SHOULD<64> return entries beginning at the byte number specified by FileIndex.										
SMB2_REOPEN 0x10	The server MUST restart the enumeration from the beginning, and the search pattern MUST be changed to the provided value.										

Errata Published*	Description
	<p>server MUST set Open.EnumerationLocation to 0.</p> <p>If Open.EnumerationLocation is 0 and Open.EnumerationSearchPattern is an empty string, then Open.EnumerationSearchPattern MUST be set to the search pattern specified in the SMB2 QUERY_DIRECTORY by FileNameOffset and FileNameLength. If FileNameLength is 0, the server SHOULD<344> set Open.EnumerationSearchPattern as "*" to search all entries.</p> <p>If SMB2_INDEX_SPECIFIED is set in the Flags field of the SMB2 QUERY_DIRECTORY Request and the underlying object store supports resuming enumerations by index number, the server MUST set Open.EnumerationLocation to the FileIndex received in the SMB2 QUERY_DIRECTORY Request. An underlying store MAY<345> choose to support resuming enumerations by index number.</p> <p>If SMB2_INDEX_SPECIFIED is set and FileNameLength is not zero, the server MUST set Open.EnumerationSearchPattern to the search pattern specified in the request by FileNameOffset and FileNameLength.</p> <p>The server MUST now enumerate the files and directories that are contained within the directory specified by Open.LocalOpen, starting at the index Open.EnumerationLocation.<346> Each entry MUST be formed as specified in [MS-FSCC] section 2.4. The server MUST fill in entries up to the OutputBufferLength received in the client request. The server MUST only include entries that match Open.EnumerationSearchPattern. For an explanation of wildcard evaluation for search patterns, see [MS-CIFS] section 2.2.1.1.3. If SMB2_RETURN_SINGLE_ENTRY is set in the Flags field of the request, the server MUST return only a single entry.</p> <p>If TreeConnect.Share.DoAccessBasedDirectoryEnumeration is TRUE and the object store supports security, the server MUST also exclude entries for which the user represented by Session.SecurityContext does not have FILE_READ_DATA or FILE_LIST_DIRECTORY access.</p> <p>After populating the buffer, the server MUST set Open.EnumerationLocation to the location of the next enumeration entry after the last one that was returned in the buffer. If there are no remaining entries, the server MUST set Open.EnumerationLocation to an invalid value indicating that the enumeration is complete.</p> <p>If an error is encountered, the server MUST fail the request with the error code received from the underlying object store by sending an error response as specified in section 2.2.2.</p> <p>If there are no entries to return and this was the initial query (Open.EnumerationLocation was zero before querying the object store), the server MUST fail the request with STATUS_NO_SUCH_FILE.</p> <p>If there are no entries to return and this was not the initial query (Open.EnumerationLocation was not zero before querying the object store), the server MUST fail the request with STATUS_NO_MORE_FILES.</p> <p><341> Section 3.3.5.18: The Windows SMB2 server implementation closes and reopens the directory handle in order to "reset" the enumeration state. So any outstanding operations on the directory handle will be failed with a STATUS_FILE_CLOSED error.</p> <p><342> Section 3.3.5.18: If the length of the received data is less than the size of SMB2 header (0x40) plus size of SMB2 QUERY_DIRECTORY request (0x21), Windows servers fail the request with STATUS_INVALID_PARAMETER. Otherwise, if FileNameLength is 0 and the underlying file system is NTFS, Windows servers fail the request with STATUS_OBJECT_NAME_INVALID.</p> <p><343> Section 3.3.5.18: Windows-based servers do not support resuming an enumeration at a specified FileIndex. The server will ignore this flag.</p> <p><346> Section 3.3.5.18: Windows performs directory query information requests via the corresponding interfaces in [MS-FSA] section 2.1.5.5.3:</p> <ul style="list-style-type: none"> • FileBothDirectoryInformation: [MS-FSA] section 2.1.5.5.3.1. • FileDirectoryInformation: [MS-FSA] section 2.1.5.5.3.2. • FileFullDirectoryInformation: [MS-FSA] section 2.1.5.5.3.3. • FileIdBothDirectoryInformation: [MS-FSA] section 2.1.5.5.3.4. • FileIdFullDirectoryInformation: [MS-FSA] section 2.1.5.5.3.5. • FileNamesInformation: [MS-FSA] section 2.1.5.5.3.6. <p><347> Section 3.3.5.19: Windows Vista SP1 and Windows Server 2008 limit OutputBufferLength size to 256 KB.</p>

Errata Published*	Description
	<p>Changed to:</p> <p>If any other information class is specified in the FileInformationClass field of the SMB2 QUERY_DIRECTORY Request, the server MUST fail the operation with STATUS_INVALID_INFO_CLASS. If the information class requested is not supported by the server, the server MUST fail the request with STATUS_NOT_SUPPORTED.</p> <p>If SMB2_RESTART_SCANS or SMB2_REOPEN is set in the Flags field of the SMB2 QUERY_DIRECTORY Request, the server MUST restart the scan with the search pattern specified, in an implementation-specific manner<341>.</p> <p>If SMB2_RETURN_SINGLE_ENTRY is set in the Flags field of the request, the server MUST return only a single entry.</p> <p>The server MUST invoke the query directory procedure from the underlying object store in an implementation-specific manner<342>.</p> <p>An Underlying object store MAY<343> choose to support resuming enumerations by index number, if SMB2_INDEX_SPECIFIED is set in the Flags field and an index number is specified in the FileIndex field of the SMB2 QUERY_DIRECTORY Request.</p> <p>If TreeConnect.Share.DoAccessBasedDirectoryEnumeration is TRUE and the object store supports security, the server MUST also exclude entries for which the user represented by Session.SecurityContext does not have FILE_READ_DATA or FILE_LIST_DIRECTORY access.</p> <p><341> Section 3.3.5.18: Windows Vista SP1, Windows Server 2008, Windows 7, and Windows Server 2008 R2 close and reopen the directory handle prior to processing the request.</p> <p><342> Section 3.3.5.18: Windows-based servers perform query directory requests, as specified in [MS-FSA] section 2.1.5.5 with the following input parameters:</p> <ul style="list-style-type: none"> • Open is set to Open.LocalOpen. • FileInformationClass is set to the InformationClass that is received in the SMB2 QUERY_DIRECTORY Request. • OutputBufferSize is set to the OutputBufferLength that is received in the SMB2 QUERY_DIRECTORY Request. • If SMB2_RESTART_SCANS or SMB2_REOPEN is set in the Flags field of the SMB2 QUERY_DIRECTORY Request, RestartScan is set to TRUE. • If SMB2_RETURN_SINGLE_ENTRY is set in the Flags field of the request, ReturnSingleEntry is set to TRUE. • FileIndex is set to FileIndex received in the SMB2 QUERY_DIRECTORY Request. • FileNamePattern is set to the search pattern specified in the SMB2 QUERY_DIRECTORY by FileNameOffset and FileNameLength. <p><343> Section 3.3.5.18: Windows-based servers do not support resuming an enumeration at a specified FileIndex. The server will ignore this flag.</p> <p><344> Section 3.3.5.19: Windows Vista SP1 and Windows Server 2008 limit OutputBufferLength size to 256 KB.</p>
2016/10/10	<p>In two sections, revised the description of SessionId.</p> <p>In Section 2.2.1.1, SMB2 Packet Header – ASYNC, changed from:</p> <p>SessionId (8 bytes): Uniquely identifies the established session for the command. This MUST be 0 for requests that do not have an associated user context. This MUST be 0 for the first SMB2 SESSION_SETUP Request for a specified security principal. The following SMB 2 Protocol commands do not require the SessionId to be set to a nonzero value received from a previous SMB2 SESSION_SETUP Response. The client MUST set the SessionId to 0, and the server SHOULD<2> ignore this value for the following commands:</p> <ul style="list-style-type: none"> • SMB2 NEGOTIATE request • SMB2 NEGOTIATE response

Errata Published*	Description
	<p>Changed to:</p> <p>SessionId (8 bytes): Uniquely identifies the established session for the command. This field MUST be set to 0 for an SMB2_NEGOTIATE request (section 2.2.3) and for an SMB2_NEGOTIATE response (section 2.2.4).</p> <p>In Section 2.2.1.2, SMB2 Packet Header – SYNC, changed from:</p> <p>SessionId (8 bytes): Uniquely identifies the established session for the command. This MUST be 0 for requests that do not have a user context that is associated with them. This MUST be 0 for the first SMB2 SESSION_SETUP Request for a specified security principal. The following SMB 2 Protocol commands do not require the SessionId to be set to a nonzero value received from a previous SMB2 SESSION_SETUP Response. The client MUST set SessionId to 0, and the server SHOULD<5> ignore this value for the following commands:</p> <ul style="list-style-type: none"> • SMB2 NEGOTIATE Request • SMB2 NEGOTIATE Response <p>Changed to:</p> <p>SessionId (8 bytes): Uniquely identifies the established session for the command. This field MUST be set to 0 for an SMB2_NEGOTIATE request (section 2.2.3) and for an SMB2_NEGOTIATE response (section 2.2.4).</p>

*Date format: YYYY/MM/DD

[MS-SMBD]: SMB2 Remote Direct Memory Access (RDMA) Transport Protocol

This topic lists the Errata found in [MS-SMBD] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-SPNG]: Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) Extension

This topic lists the Errata found in [MS-SPNG] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-SQOS]: Storage Quality of Service Protocol

This topic lists the Errata found in [MS-SQOS] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-SSTP]: Secure Socket Tunneling Protocol (SSTP)

This topic lists the Errata found in [MS-SSTP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-SWN]: Service Witness Protocol

This topic lists the Errata found in [MS-SWN] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-TCC]: Tethering Control Channel Protocol

This topic lists the Errata found in [MS-TCC] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-TDS]: Tabular Data Stream Protocol

This topic lists the Errata found in [MS-TDS] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

Errata below are for Protocol Document Version [V19.0 – 2016/07/14](#).

Errata Published*	Description
2017/01/23	<p>In Section 2.2.5.5.4, SQL_VARIANT Values, the first sentence of the final paragraph is changed from:</p> <p>Note T data types cannot be NULL when inside a sql_variant.</p> <p>Changed to:</p> <p>Note Data types cannot be NULL when inside a sql_variant.</p> <p>In the first table in Section 2.2.6.4, LOGIN7, a product behavior note is added to the description of the OptionFlags2 parameter. The third bullet is changed from:</p> <ul style="list-style-type: none">• fODBC: Set if the client is the ODBC driver. This causes the server to set ANSI_DEFAULTS to ON, CURSOR_CLOSE_ON_COMMIT and IMPLICIT_TRANSACTIONS to OFF, TEXTSIZE to 0x7FFFFFFF (2GB) (TDS 7.2 and earlier), TEXTSIZE to infinite (introduced in TDS 7.3), and ROWCOUNT to infinite. <p>Changed to:</p> <ul style="list-style-type: none">• fODBC: Set if the client is the ODBC driver. This causes the server to set ANSI_DEFAULTS to ON, CURSOR_CLOSE_ON_COMMIT and IMPLICIT_TRANSACTIONS to OFF, TEXTSIZE to 0x7FFFFFFF (2GB) (TDS 7.2 and earlier), TEXTSIZE to infinite (introduced in TDS 7.3), and ROWCOUNT to infinite.<24> <p><24> Section 2.2.6.4: ANSI_DEFAULTS, CURSOR_CLOSE_ON_COMMIT, IMPLICIT_TRANSACTIONS, and ROWCOUNT are supported only by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014.</p> <p>In the second table in Section 2.2.6.4, LOGIN7, the FeatureId in the first row is changed from:</p> <p>%0x01 (SESSIONRECOVERY)</p> <p>Changed to:</p> <p>%0x01 (SESSIONRECOVERY)</p>

Errata Published*	Description
	<p>(introduced in TDS 7.4)</p> <p>Also in the second table in Section 2.2.6.4, LOGIN7, the FeatureData Description for %0x04 (COLUMNENCRYPTION) is changed. The last two paragraphs are changed from:</p> <p>COLUMNENCRYPTION_VERSION: This field describes the cryptographic protocol version that the client understands.</p> <p>Length: This field is the length of the COLUMNENCRYPTION_VERSION.</p> <p>Changed to:</p> <p>COLUMNENCRYPTION_VERSION: This field describes the cryptographic protocol version that the client understands. The value of COLUMNENCRYPTION_VERSION is 1.</p> <p>In Section 2.2.6.6, RPC Request, the following line of code is deleted:</p> <pre>CekHash</pre> <p>and replaced with the following lines:</p> <pre>DatabaseId CekId CekVersion CekMDVersion</pre> <p>The following line of code is changed from:</p> <pre>ParamCipherInfo</pre> <p>Changed to:</p> <pre>[ParamCipherInfo]</pre> <p>In the table in Section 2.2.6.6, RPC Request, the description of the OptionFlags parameter is changed and a product behavior note is added. The second bullet is changed from:</p> <ul style="list-style-type: none"> • fNoMetaData: 1 if the client has already cached the metadata for the result set from previous calls to the same RPC, and wants the server to avoid sending metadata by using NoMetaData (see COLMETADATA section 2.2.7.4). <p>Changed to:</p> <ul style="list-style-type: none"> • fNoMetaData: The server sends NoMetaData only if fNoMetadata is set to 1 in the request (see COLMETADATA section 2.2.7.4).<31> <p><31> Section 2.2.6.6: The option to have NoMetaData returned is not supported by SQL Server 2016.</p> <p>Also in the table in Section 2.2.6.6, RPC Request, the name of the "EmcryptionAlgo" parameter is changed to "EncryptionAlgo" and the name of the "EncryptionName" parameter is changed to "EncryptionType".</p> <p>Also in the table in Section 2.2.6.6, RPC Request, the description of the NormVersion parameter is changed from:</p> <p>The normalization version to which plaintext data MUST be normalized. Version numbering starts at 0x01.</p>

Errata Published*	Description																		
	<p>Changed to:</p> <p>Reserved for future use. The value MUST be set to 1.</p> <p>Also in the table in Section 2.2.6.6, RPC Request, the following row is deleted:</p> <table border="1" data-bbox="375 443 1214 552"> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td>...</td><td>...</td></tr> <tr> <td>CekHash</td><td>The hash of encryption key as reported by stored procedure sp_describe_parameter_encryption.</td></tr> </table> <p>And the following rows are added:</p> <table border="1" data-bbox="375 653 1214 842"> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td>...</td><td>...</td></tr> <tr> <td>DatabaseId</td><td>A 4 byte integer value that represents the database ID where the column encryption key is stored.</td></tr> <tr> <td>CekId</td><td>An identifier for the column encryption key.</td></tr> <tr> <td>CekVersion</td><td>The key version of the column encryption key.</td></tr> <tr> <td>CekMDVersion</td><td>The metadata version for the column encryption key.</td></tr> </table> <p>Also in the table in Section 2.2.6.6, RPC Request, the description of the ParamCipherInfo parameter is changed from:</p> <p>Describes the parameter encryption information when that information is transparently encrypted. It defines the original TYPE_INFO of the data that is encrypted, the encryption algorithm that is used, and the normalization version, and hash of the encryption key that is used. This field MUST be sent only when fEncrypted is set to 1.</p> <p>Changed to:</p> <p>Describes the parameter encryption information when the parameter is transparently encrypted. It defines the original TYPE_INFO of the data that is encrypted, the encryption algorithm that is used, the normalization version, the id of the database containing the column encryption key used for encryption, the id of the column encryption key, the version of the column encryption key and the version of the column encryption key metadata. These fields MUST be sent only when fEncrypted is set to 1.</p> <p>In the table in Section 2.2.7.1, ALTMETADATA, a product behavior note is added to the description of the TokenType parameter. The description is changed from:</p> <p>ALTMETADATA_TOKEN</p> <p>Changed to:</p> <p>ALTMETADATA_TOKEN<33></p> <p><33> Section 2.2.7.1: ALTMETADATA_TOKEN is supported only by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, and SQL Server 2008 R2.</p> <p>In the table in Section 2.2.7.2, ALTROW, a product behavior note is added to the description of</p>	Parameter	Description	CekHash	The hash of encryption key as reported by stored procedure sp_describe_parameter_encryption.	Parameter	Description	DatabaseId	A 4 byte integer value that represents the database ID where the column encryption key is stored.	CekId	An identifier for the column encryption key.	CekVersion	The key version of the column encryption key.	CekMDVersion	The metadata version for the column encryption key.
Parameter	Description																		
...	...																		
CekHash	The hash of encryption key as reported by stored procedure sp_describe_parameter_encryption.																		
Parameter	Description																		
...	...																		
DatabaseId	A 4 byte integer value that represents the database ID where the column encryption key is stored.																		
CekId	An identifier for the column encryption key.																		
CekVersion	The key version of the column encryption key.																		
CekMDVersion	The metadata version for the column encryption key.																		

Errata Published*	Description				
	<p>the TokenType parameter. The description is changed from:</p> <p>ALTROW_TOKEN</p> <p>Changed to:</p> <p>ALTROW_TOKEN<34></p> <p><34> Section 2.2.7.2: ALTROW_TOKEN is supported only by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, and SQL Server 2008 R2.</p> <p>In Section 2.2.7.4, COLMETADATA, the following line of code is changed from:</p> <pre>(usReserved / (FRESERVEDBIT fSparseColumnSet fEncrypted usReserved3)</pre> <p>Changed to:</p> <pre>(usReserved / (FRESERVEDBIT fSparseColumnSet fEncrypted usReserved3))</pre> <p>Also in Section 2.2.7.4, COLMETADATA, the following line of code is changed from:</p> <pre>CryptoMetaData</pre> <p>Changed to:</p> <pre>[CryptoMetaData]</pre> <p>In the table in Section 2.2.7.4, COLMETADATA, added a product behavior note and the following rows are changed from:</p> <table border="1" data-bbox="375 1409 1214 1497"> <tr> <th data-bbox="375 1409 586 1451">Parameter</th><th data-bbox="586 1409 1214 1451">Description</th></tr> <tr> <td data-bbox="375 1451 586 1497">...</td><td data-bbox="586 1451 1214 1497">...</td></tr> </table>	Parameter	Description
Parameter	Description				
...	...				

Errata Published*	Description																				
	<table border="1" data-bbox="375 226 1214 835"> <tr> <td data-bbox="375 226 586 569">EncryptionAlgo</td><td data-bbox="586 226 1214 569"> <p>A byte that describes the encryption algorithm that is used.</p> <p>If EncryptionAlgo is set to 0, a custom encryption algorithm is used and AlgoName MUST be sent. AlgoName is populated with the name of the custom encryption algorithm.</p> <p>For all EncryptionAlgo values other than 0, AlgoName MUST NOT be sent.</p> <p>If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4.</p> </td></tr> <tr> <td data-bbox="375 569 586 625">AlgoName</td><td data-bbox="586 569 1214 625">Algorithm name literal that is used to encrypt the plaintext value.</td></tr> <tr> <td data-bbox="375 625 586 653">...</td><td data-bbox="586 625 1214 653">...</td></tr> <tr> <td data-bbox="375 653 586 835">NoMetaData</td><td data-bbox="586 653 1214 835"> <p>This notifies client that no metadata will follow the COLMETADATA token. Client notifies the server that it has already cached the metadata from previous request, by setting fNoMetadata to 1 in RPC Request (section 2.2.6.6). The server SHOULD not send NoMetaData unless fNoMetadata is set to 1 in the request.</p> </td></tr> </table> <p>Changed to:</p> <table border="1" data-bbox="375 932 1214 1457"> <tr> <th data-bbox="375 932 586 980">Parameter</th><th data-bbox="586 932 1214 980">Description</th></tr> <tr> <td data-bbox="375 980 586 1016">...</td><td data-bbox="586 980 1214 1016">...</td></tr> <tr> <td data-bbox="375 1016 586 1220">EncryptionAlgo</td><td data-bbox="586 1016 1214 1220"> <p>A byte that describes the encryption algorithm that is used.</p> <p>If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4. Other values are reserved for future use.</p> </td></tr> <tr> <td data-bbox="375 1220 586 1255">AlgoName</td><td data-bbox="586 1220 1214 1255">Reserved for future use.</td></tr> <tr> <td data-bbox="375 1255 586 1283">...</td><td data-bbox="586 1255 1214 1283">...</td></tr> <tr> <td data-bbox="375 1283 586 1457">NoMetaData</td><td data-bbox="586 1283 1214 1457"> <p>This notifies client that no metadata will follow the COLMETADATA token. Client notifies the server that it has already cached the metadata from previous request, by setting fNoMetadata to 1 in RPC Request (section 2.2.6.6). The server sends NoMetaData only if fNoMetadata is set to 1 in the request.<36></p> </td></tr> </table> <p><36> Section 2.2.7.4: The option to have NoMetaData returned is not supported by SQL Server 2016.</p> <p>In Section 2.2.7.8, ENVCHANGE, the last paragraph is changed from:</p> <ul style="list-style-type: none"> ENVCHANGE type 20 MAY be sent back to a client running TDS 7.4 or later whether or not the fReadOnlyIntent bit is set in the preceding LOGIN7 record. Type 20 MAY be sent to a TDS client running TDS 7.1 to 7.3 but only when the fReadOnlyIntent bit is set in the preceding LOGIN7 record. 	EncryptionAlgo	<p>A byte that describes the encryption algorithm that is used.</p> <p>If EncryptionAlgo is set to 0, a custom encryption algorithm is used and AlgoName MUST be sent. AlgoName is populated with the name of the custom encryption algorithm.</p> <p>For all EncryptionAlgo values other than 0, AlgoName MUST NOT be sent.</p> <p>If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4.</p>	AlgoName	Algorithm name literal that is used to encrypt the plaintext value.	NoMetaData	<p>This notifies client that no metadata will follow the COLMETADATA token. Client notifies the server that it has already cached the metadata from previous request, by setting fNoMetadata to 1 in RPC Request (section 2.2.6.6). The server SHOULD not send NoMetaData unless fNoMetadata is set to 1 in the request.</p>	Parameter	Description	EncryptionAlgo	<p>A byte that describes the encryption algorithm that is used.</p> <p>If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4. Other values are reserved for future use.</p>	AlgoName	Reserved for future use.	NoMetaData	<p>This notifies client that no metadata will follow the COLMETADATA token. Client notifies the server that it has already cached the metadata from previous request, by setting fNoMetadata to 1 in RPC Request (section 2.2.6.6). The server sends NoMetaData only if fNoMetadata is set to 1 in the request.<36></p>
EncryptionAlgo	<p>A byte that describes the encryption algorithm that is used.</p> <p>If EncryptionAlgo is set to 0, a custom encryption algorithm is used and AlgoName MUST be sent. AlgoName is populated with the name of the custom encryption algorithm.</p> <p>For all EncryptionAlgo values other than 0, AlgoName MUST NOT be sent.</p> <p>If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4.</p>																				
AlgoName	Algorithm name literal that is used to encrypt the plaintext value.																				
...	...																				
NoMetaData	<p>This notifies client that no metadata will follow the COLMETADATA token. Client notifies the server that it has already cached the metadata from previous request, by setting fNoMetadata to 1 in RPC Request (section 2.2.6.6). The server SHOULD not send NoMetaData unless fNoMetadata is set to 1 in the request.</p>																				
Parameter	Description																				
...	...																				
EncryptionAlgo	<p>A byte that describes the encryption algorithm that is used.</p> <p>If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4. Other values are reserved for future use.</p>																				
AlgoName	Reserved for future use.																				
...	...																				
NoMetaData	<p>This notifies client that no metadata will follow the COLMETADATA token. Client notifies the server that it has already cached the metadata from previous request, by setting fNoMetadata to 1 in RPC Request (section 2.2.6.6). The server sends NoMetaData only if fNoMetadata is set to 1 in the request.<36></p>																				

Errata Published*	Description						
	<p>Changed to:</p> <ul style="list-style-type: none"> ENVCHANGE type 20 can be sent back to a client running TDS 7.4 or later regardless of whether the fReadOnlyIntent bit is set in the preceding LOGIN7 record. If a client is running TDS 7.1 to 7.3, type 20 can be sent only if the fReadOnlyIntent bit is set in the preceding LOGIN7 record. <p>In the second table in Section 2.2.7.10, FEATUREEXTACK, the FeatureId in the second row is changed from:</p> <p>%0x01 (SESSIONRECOVERY)</p> <p>Changed to:</p> <p>%0x01 (SESSIONRECOVERY) (introduced in TDS 7.4)</p> <p>Also in the second table in Section 2.2.7.10, FEATUREEXTACK, the following row with product behavior note is added:</p> <table border="1" data-bbox="375 961 1346 1512"> <thead> <tr> <th>FeatureId</th><th>FeatureExtData Description</th></tr> </thead> <tbody> <tr> <td>...</td><td>...</td></tr> <tr> <td>%0x04 (COLUMNENCRYPTION)<46> (introduced in TDS 7.4)</td><td> <p>Presence of COLUMNENCRYPTION FeatureExt indicates that the client is capable of performing cryptographic operations on data. The feature data is described as follows:</p> <pre> Length = DWORD COLUMNENCRYPTION_VERSION = BYTE FeatureData = Length COLUMNENCRYPTION_VERSION COLUMNENCRYPTION_VERSION: This field describes the cryptographic protocol version that the client understands. The value of COLUMNENCRYPTION_VERSION is 1. </pre> </td></tr> </tbody> </table> <p><46> Section 2.2.7.10: Column encryption is not supported by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014.</p> <p>In Section 2.2.7.18, RETURNVALUE, the following line of code is changed from:</p>	FeatureId	FeatureExtData Description	%0x04 (COLUMNENCRYPTION)<46> (introduced in TDS 7.4)	<p>Presence of COLUMNENCRYPTION FeatureExt indicates that the client is capable of performing cryptographic operations on data. The feature data is described as follows:</p> <pre> Length = DWORD COLUMNENCRYPTION_VERSION = BYTE FeatureData = Length COLUMNENCRYPTION_VERSION COLUMNENCRYPTION_VERSION: This field describes the cryptographic protocol version that the client understands. The value of COLUMNENCRYPTION_VERSION is 1. </pre>
FeatureId	FeatureExtData Description						
...	...						
%0x04 (COLUMNENCRYPTION)<46> (introduced in TDS 7.4)	<p>Presence of COLUMNENCRYPTION FeatureExt indicates that the client is capable of performing cryptographic operations on data. The feature data is described as follows:</p> <pre> Length = DWORD COLUMNENCRYPTION_VERSION = BYTE FeatureData = Length COLUMNENCRYPTION_VERSION COLUMNENCRYPTION_VERSION: This field describes the cryptographic protocol version that the client understands. The value of COLUMNENCRYPTION_VERSION is 1. </pre>						

Errata Published*	Description
	<p>(usReserved / (usReserved2 fEncrypted usReserved3))</p> <p>Changed to:</p> <p>(usReserved / (usReserved2 fEncrypted usReserved3))</p> <p>In the table in Section 2.2.7.18, RETURNVALUE, the description of the EncryptionAlgo parameter is changed from:</p> <p>A byte that describes the encryption algorithm that is used. If EncryptionAlgo is set to 0, a custom encryption algorithm is used and AlgoName MUST be sent. AlgoName is populated with the name of the custom encryption algorithm. For all EncryptionAlgo values other than 0, AlgoName MUST NOT be sent. If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4.</p> <p>Changed to:</p> <p>A byte that describes the encryption algorithm that is used. AlgoName is populated with the name of the custom encryption algorithm. For all EncryptionAlgo values other than 0, AlgoName MUST NOT be sent. If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4.</p>
2016/08/29	<p>In Section 6, Appendix A: Product Behavior, product behavior notes <21>, <25>, <30>, and <31> are updated as follows.</p> <p>Note <21> is changed from:</p> <p><21> Section 2.2.5.7: Column encryption is not supported by SQL Server.</p> <p>Changed to:</p> <p><21> Section 2.2.5.7: Column encryption is not supported by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014.</p> <p>Note <25> is changed from:</p> <p><25> Section 2.2.6.4: Column encryption is not supported by SQL Server.</p> <p>Changed to:</p> <p><25> Section 2.2.6.4: Column encryption is not supported by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014.</p> <p>Note <30> is changed from:</p> <p><30> Section 2.2.6.6: Column encryption is not supported by SQL Server.</p> <p>Changed to:</p> <p><30> Section 2.2.6.6: Column encryption is not supported by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014.</p> <p>Note <31> is changed from:</p> <p><31> Section 2.2.7.4: Column encryption is not supported by SQL Server.</p> <p>Changed to:</p> <p><31> Section 2.2.7.4: Column encryption is not supported by SQL Server 7.0, SQL Server 2000,</p>

Errata Published*	Description
	SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014.

*Date format: YYYY/MM/DD

[MS-TLSP]: Transport Layer Security (TLS) Profile

This topic lists the Errata found in [MS-TLSP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-TPMVSC]: Trusted Platform Module (TPM) Virtual Smart Card Management Protocol

This topic lists the Errata found in [MS-TPMVSC] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-TSCH]: Task Scheduler Service Remoting Protocol

This topic lists the Errata found in [MS-TSCH] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-TSGU]: Terminal Services Gateway Server Protocol

This topic lists the Errata found in [MS-TSGU] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V36.0 - 2016/07/14](#).

Errata Published*	Description
2016/09/12	<p>In several sections, updated the msgBytes range in the TSG_PACKET_STRING_MESSAGE structure.</p> <p>In Section 2.2.9.2.1.9.1.1, TSG_PACKET_STRING_MESSAGE, changed from:</p> <p>The TSG_PACKET_STRING_MESSAGE structure contains either the Consent Signing Message or the Administrative Message that is being sent from the RDG server to the client.</p> <pre>typedef struct _TSG_PACKET_STRING_MESSAGE { long isDisplayMandatory; long isConsentMandatory; [range(0,n)] unsigned long msgBytes; ... }</pre> <p>Changed to:</p> <p>The TSG_PACKET_STRING_MESSAGE structure contains either the Consent Signing Message or the Administrative Message that is being sent from the RDG server to the client.</p> <pre>typedef struct _TSG_PACKET_STRING_MESSAGE { long isDisplayMandatory; long isConsentMandatory; [range(0,65536)] unsigned long msgBytes; ... }</pre> <p>In Section 4.1.1, Normal Scenario, changed from:</p> <p>...</p> <p>Where the servicemessage is set as follows.</p> <pre>typedef struct _TSG_PACKET_STRING_MESSAGE</pre>

Errata Published*	Description
	<pre> { long isDisplayMandatory = 1; long isConsentMandatory = 1; [range(0, 12288)] unsigned long msgBytes = 4; ... Changed to: ... Where the servicemessage is set as follows. typedef struct _TSG_PACKET_STRING_MESSAGE { long isDisplayMandatory = 1; long isConsentMandatory = 1; [range(0, 65536)] unsigned long msgBytes = 4; ... In Section 4.1.2, Pluggable Authentication Scenario with Consent Message Returned, changed from: ... Where the consentMessage is set as follows. typedef struct _TSG_PACKET_STRING_MESSAGE { long isDisplayMandatory = 1; long isConsentMandatory = 1; [range(0, 12288)] unsigned long msgBytes = 7; ... Changed to: ... Where the consentMessage is set as follows. typedef struct _TSG_PACKET_STRING_MESSAGE { long isDisplayMandatory = 1; long isConsentMandatory = 1; [range(0, 65536)] unsigned long msgBytes = 7; ... In Section 6, Appendix A: Full IDL, changed from: ... typedef struct _TSG_PACKET_STRING_MESSAGE { long isDisplayMandatory; long isConsentMandatory; </pre>

Errata Published*	Description
	<pre> [range(0,12288)] unsigned long msgBytes; ... Changed to: ... typedef struct _TSG_PACKET_STRING_MESSAGE { long isDisplayMandatory; long isConsentMandatory; [range(0,65536)] unsigned long msgBytes; ... </pre>

*Date format: YYYY/MM/DD

[MS-TSTS]: Terminal Services Terminal Server Runtime Interface Protocol

This topic lists the Errata found in [MS-TSTS] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-UAMG]: Update Agent Management Protocol

This topic lists the Errata found in [MS-UAMG] 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.

[RSS](#)
[Atom](#)

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

Errata below are for Protocol Document Version [V8.0 - 2016/07/14](#).

Errata Published*	Description
2016/10/10	<p>In Section 6, Appendix A, Full IDL, removed the code for the ISearchJob interface.</p> <p>Removed:</p> <pre>[object, oleautomation, dual, nonextensible, uuid(7366ea16-7a1a-4ea2-b042-973d3e9cd99b), pointer_default(unique),] interface ISearchJob : IDispatch { [id(0x60020001), propget] HRESULT AsyncState([out, retval] VARIANT* retval); [id(0x60020002), propget] HRESULT IsCompleted([out, retval] VARIANT_BOOL* retval); [id(0x60020003),] HRESULT Cleanup(); [id(0x60020004),] HRESULT RequestAbort(); }</pre>

*Date format: YYYY/MM/DD

[MS-UCODEREF]: Windows Protocols Unicode Reference

This topic lists the Errata found in [MS-UCODEREF] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-VHDX]: Virtual Hard Disk v2 (VHDX) File Format

This topic lists the Errata found in [MS-VHDX] 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.

Errata below are for Protocol Document Version [V1.0 - 2016/07/14](#).

Errata Published*	Description
2016/11/21	<p>In two sections, updated a field name.</p> <p>In Section 2.6.2, Known Metadata Items, changed from:</p> <p>Page 83 Data BECA12AB-B2E6-4523-93EF-C309E000C746 False True True</p> <p>Changed to:</p> <p>Virtual Disk ID BECA12AB-B2E6-4523-93EF-C309E000C746 False True True</p> <p>Changed the title of Section 3.5.2.3, Page 83 Data, to 3.5.2.3, Virtual Disk Id, and in that section changed the description of the field from:</p> <p>Page83Data (16 bytes): A GUID field. This item SHOULD be set to a value that is unique across all small computer system interface (SCSI) devices that properly support page 0x83.</p> <p>Changed to:</p> <p>VirtualDiskId (16 bytes): A GUID that specifies the identification of the disk.</p>
2016/09/26	<p>In Section 2.4, Blocks, updated a field name and a block size.</p> <p>Changed from:</p> <p>Payload blocks are the size of the BlockSize field defined by the VHDX file parameter field.</p> <p>...</p> <p>The number of sectors that can be described in each sector bitmap block is 223, so the number of bytes described by a single sector bitmap block is 223 times the logical sector size (see section 2.6.2.4 for more information on LogicalSectorSize).</p> <p>Changed to:</p> <p>Payload blocks are the size of the BlockSize field defined by the VHDX file File Parameters field.</p> <p>...</p> <p>The number of sectors that can be described in each sector bitmap block is 2²³, so the number of bytes described by a single sector bitmap block is 2²³ times the logical sector size (see section 2.6.2.4 for more information on LogicalSectorSize).</p>

*Date format: YYYY/MM/DD

[MS-W32T]: W32Time Remote Protocol

This topic lists the Errata found in [MS-W32T] 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.

Errata below are for Protocol Document Version [V17.0 - 2016/07/14](#).

Errata Published*	Description
2017/02/06	<p>In this document:</p> <ul style="list-style-type: none">• Changed the prescriptive language for ulFlags from "SHOULD" to "MUST".• Removed the resulting unnecessary product behavior notes.• Added a product to the list of products that do not support a method. <p>In Section 3.2.5.3, W32TimeQueryProviderStatus (Opnum 2), the description for ulFlags has been changed from:</p> <p>ulFlags: Reserved. This parameter SHOULD be set to zero and SHOULD be ignored on receipt.<40></p> <p>Changed to:</p> <p>ulFlags: Reserved. This parameter MUST be set to zero and MUST be ignored on receipt.</p> <p>In Section 3.2.5.5, W32TimeQueryProviderConfiguration (Opnum 4), the description for ulFlags has been changed from:</p> <p>ulFlags: Reserved. This parameter SHOULD be set to zero and SHOULD be ignored on receipt.<46></p> <p>Changed to:</p> <p>ulFlags: Reserved. This parameter MUST be set to zero and MUST be ignored on receipt.</p> <p>In Section 7, Appendix B: Product Behavior, behavior note <45> (now <44>) (for section 3.2.5.5), which has been changed from:</p> <p>The RPC method W32TimeQueryProviderConfiguration is not supported in Windows 2000 or Windows XP.</p> <p>Changed to:</p> <p>The RPC method W32TimeQueryProviderConfiguration is not supported in Windows 2000, Windows XP, or Windows Server 2003.</p>

*Date format: YYYY/MM/DD

[MS-WCCE]: Windows Client Certificate Enrollment Protocol

This topic lists the Errata found in [MS-WCCE] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-WCFESAN]: WCF-Based Encrypted Server Administration and Notification Protocol

This topic lists the Errata found in [MS-WCFESAN] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-WDSMT]: Windows Deployment Services Multicast Transport Protocol

This topic lists the Errata found in [MS-WDSMT] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-WFDAA]: Wi-Fi Direct (WFD) Application to Application Protocol

This topic lists the Errata found in [MS-WFDAA] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

Errata below are for Protocol Document Version [V5.0 – 2016/07/14](#).

Errata Published*	Description
2017/02/06	<p>In three sections, added bytes as the size units for the cbLength and cbLength1 fields.</p> <p>In Section 2.2.2, AppWFDConnectionIE Message, changed from:</p> <p>cbLength1 (2 bytes): This field indicates the remaining size of the message.</p> <p>Changed to:</p> <p>cbLength1 (2 bytes): This field indicates the remaining size of the message in bytes.</p> <p>In Section 2.2.3, AppWFDDiscoveryMetadataIE Message, changed from:</p> <p>cbLength (1 byte): This field indicates the remaining size of the message.</p> <p>cbLength1 (2 bytes): This field indicates the remaining size of the message.</p> <p>Changed to:</p> <p>cbLength (1 byte): This field indicates the remaining size of the message in bytes.</p> <p>cbLength1 (2 bytes): This field indicates the remaining size of the message in bytes.</p> <p>In Section 2.2.4, AppWFDDiscoveryPrimaryIE Message, changed from:</p> <p>cbLength (1 byte): This field indicates the remaining size of the message.</p> <p>cbLength1 (2 bytes): This field indicates the remaining size of the message.</p> <p>Changed to:</p> <p>cbLength (1 byte): This field indicates the remaining size of the message in bytes.</p> <p>cbLength1 (2 bytes): This field indicates the remaining size of the message in bytes.</p>

*Date format: YYYY/MM/DD

[MS-WFDPE]: Wi-Fi Display Protocol Extension

This topic lists the Errata found in [MS-WFDPE] 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

Errata below are for Protocol Document Version [V3.0 – 2016/07/14](#).

Errata Published*	Description
2017/01/09	<p>In Section 2.7.1.1, wfdx_video_formats, the ABNF syntax for wfdx_video_formats was updated, and H.264 codec was changed to H.264-codec.</p> <p>Changed from:</p> <p>The ABNF syntax is as follows:</p> <pre>wfdx-video-formats = "wfdx_video_formats:" SP sink-video-list CRLF sink-video-list = "none" / (native SP preferred-display-mode-supported SP codec); native = 4*4HEXDIG; preferred-display-mode-supported = 2*2HEXDIG; 0-not supported, 1-supported, 2-255 reserved H.264 codec = profile SP level SP misc-params SP max-hres SP max-vres*(",", " SP H.264-codec)</pre> <p>Changed to:</p> <p>The ABNF syntax is as follows:</p> <pre>wfdx-video-formats = "wfdx_video_formats:" SP sink-video-list CRLF sink-video-list = "none" / (native SP preferred-display-mode-supported SP H.264-codec); native = 4*4HEXDIG; preferred-display-mode-supported = 2*2HEXDIG; 0-not supported, 1-supported, 2-255 reserved H.264-codec = profile SP level SP misc-params SP max-hres SP max-vres*(",", " SP H.264-codec)</pre>
2017/01/09	<p>In Section 3, Structure Examples, updated the wfdx-video-formats parameter value in the M3 response example.</p>

Errata Published*	Description
	<p>Changed from:</p> <p>The following is an example of an M3 response for extended video formats using the wfdx-video-formats parameter (section 2.7.1.1).</p> <pre> RTSP/1.0 200 OK CSeq: 2 Content-Type: text/parameters Content-length: 228 wfd audio codecs: LPCM 00000003 00, AAC 00000001 00, AC3 00000000 00 wfdx_video_formats: 0040 00 0001 0001 0000500001 0010000000 00000000 00 0000 0000 11 none none wfd_client_rtp_ports: RTP/AVP/UDP;unicast 19000 0 mode=play </pre> <p>Changed to:</p> <p>The following is an example of an M3 response for extended video formats using the wfdx-video-formats parameter (section 2.7.1.1).</p> <pre> RTSP/1.0 200 OK CSeq: 2 Content-Type: text/parameters Content-length: 228 wfd_audio_codecs: LPCM 00000003 00, AAC 00000001 00, AC3 00000000 00 wfdx_video_formats: 40 00 0001 0001 0000500001 0010000000 00000000 00 0000 0000 11 none none wfd_client_rtp_ports: RTP/AVP/UDP;unicast 19000 0 mode=play </pre>
2016/11/07	<p>In Section 2.7.1.1, wfdx_video_formats, the parameter names in the ABNF syntax for min-slice-size and frame-rate-control-support were updated.</p> <p>Changed from:</p> <p>The ABNF syntax is as follows:</p> <pre> wfdx-video-formats = "wfdx_video_formats:" SP sink-video-list CRLF sink-video-list = "none" / (native SP preferred-display-mode-supported SP codec); native = 4*4HEXDIG; preferred-display-mode-supported = 2*2HEXDIG; 0-not supported, 1-supported, 2-255 reserved H.264 codec = profile SP level SP misc-params SP max-hres SP max- vres*("," SP H.264-codec) profile = 4*4HEXDIG; level = 4*4HEXDIG; max-hres = "none" / (4*4HEXDIG); max-vres = "none" / (4*4HEXDIG); misc-params = CEA-Support SP VESA-Support SP HH-Support SP latency SP min-slicesize SP slice-enc-params SP frame-rate-controlsupport </pre> <p>...</p>

Errata Published*	Description
	<p>Changed to:</p> <p>The ABNF syntax is as follows:</p> <pre> wfdx-video-formats = "wfdx_video_formats:" SP sink-video-list CRLF sink-video-list = "none" / (native SP preferred-display-mode-supported SP codec); native = 4*4HEXDIG; preferred-display-mode-supported = 2*2HEXDIG; 0-not supported, 1-supported, 2-255 reserved H.264 codec = profile SP level SP misc-params SP max-hres SP max- vres*("," SP H.264-codec) profile = 4*4HEXDIG; level = 4*4HEXDIG; max-hres = "none" / (4*4HEXDIG); max-vres = "none" / (4*4HEXDIG); misc-params = CEA-Support SP VESA-Support SP HH-Support SP latency SP min-slice-size SP slice-enc-params SP frame-rate-control-support </pre> <p>...</p>

*Date format: YYYY/MM/DD

[MS-WKST]: Workstation Service Remote Protocol

This topic lists the Errata found in [MS-WKST] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

[MS-WPO]: Windows Protocols Overview

This topic lists the Errata found in [MS-WPO] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-WMF]: Windows Metafile Format

This topic lists the Errata found in [MS-WMF] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-WSDS]: WS-Enumeration Directory Services Protocol Extensions

This topic lists the Errata found in [MS-WSDS] 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.

Errata below are for Protocol Document Version [V9.0 - 2016/07/14](#).

Errata Published*	Description
2016/08/15	<p>In Section 3, Protocol Details, updated that the server implementation of this protocol can limit the maximum validity of an enumeration context by including the following note at the end of the section:</p> <p>Note The server implementation of the WS-Enumeration: Directory Services Protocol Extensions MAY<2> limit the maximum validity of an enumeration context. This limit, if implemented, applies across the Renew operation (section 3.1.4.3).</p> <p><2> Section 3: Microsoft implementations of WS-Enumeration: Directory Services Protocol Extensions limit the validity of an enumeration context to 30 minutes by default (defined as MaxEnumContextExpiration in the configuration settings).</p>
2016/08/15	<p>In several sections, added that an optional ad:controls element can also be passed to the pull request.</p> <p>In Section 1.2.1, Normative References, included the following reference: [MS-WSPELD] Microsoft Corporation, "WS-Transfer and WS-Enumeration Protocol Extension for Lightweight Directory Access Protocol v3 Controls</p> <p>In Section 3.1.4.2, wsen:Pull, included the following paragraph at the end of the section: An optional ad:controls element can also be passed to the pull request, according to the requirements in [MS-WSPELD] section 2.2.3.1.</p> <p>In Section 7, Appendix B: Schema, changed from:</p> <pre>.Section <!-- Pull request --> ..Pull (element) .</pre> <p>Changed to:</p> <pre><!--. . . .Other elements from [MS-WSPELD] schema in Appendix B: .. ad:Controls (element) . . .--></pre>

Errata Published*	Description
	<pre> <!--Extended PULL [WSENUM] request--> <xsd:element name="Pull"> <xsd:complexType> <xsd:sequence> <xsd:element name="EnumerationContext" type="tns:EnumerationContextType" /> <xsd:element name="MaxTime" type="tns:PositiveDurationType" minOccurs="0" /> <xsd:element name="MaxElements" type="xsd:positiveInteger" minOccurs="0" /> <xsd:element name="MaxCharacters" type="xsd:positiveInteger" minOccurs="0" /> <xsd:element ref="ad:Controls" minOccurs="0" maxOccurs="1" /> </xsd:sequence> </xsd:complexType> </xsd:element> </pre>
2016/08/01	<p>In Section 7, Appendix B: Schema, updated the schema with adddata elements and changed instances of <xs: to <xsd:.</p> <p>Changed from:</p> <pre> <xsd:schema xmlns:ad="http://schemas.microsoft.com/2008/1/ActiveDirectory" attributeFormDefault="unqualified" elementFormDefault="qualified" targetNamespace="http://schemas.microsoft.com/2008/1/ActiveDirectory" xmlns:xsd="http://www.w3.org/2001/XMLSchema"> </pre> <p>Changed to:</p> <pre> <xsd:schema xmlns:ad="http://schemas.microsoft.com/2008/1/ActiveDirectory" xmlns:addata="http://schemas.microsoft.com/2008/1/ActiveDirectory/Data" attributeFormDefault="unqualified" elementFormDefault="qualified" targetNamespace="http://schemas.microsoft.com/2008/1/ActiveDirectory" xmlns:xsd="http://www.w3.org/2001/XMLSchema"> </pre> <p>Changed from:</p> <pre> <xsd:schema targetNamespace="http://schemas.xmlsoap.org/ws/2004/09/enumeration" xmlns:wse="http://schemas.xmlsoap.org/ws/2004/09/enumeration" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:xsd="http://www.w3.org/2001/XMLSchema" </pre>

Errata Published*	Description
	<pre> xmlns:adlq="http://schemas.microsoft.com/2008/1/ActiveDirectory/Dialect/LdapQuery" xmlns:ad="http://schemas.microsoft.com/2008/1/ActiveDirectory" elementFormDefault="qualified" blockDefault="#all"> Changed to: <xsd:schema targetNamespace="http://schemas.xmlsoap.org/ws/2004/09/enumeration" xmlns:wsen="http://schemas.xmlsoap.org/ws/2004/09/enumeration" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:adlq="http://schemas.microsoft.com/2008/1/ActiveDirectory/Dialect/LdapQuery" xmlns:ad="http://schemas.microsoft.com/2008/1/ActiveDirectory" xmlns:addata="http://schemas.microsoft.com/2008/1/ActiveDirectory/Data" elementFormDefault="qualified" blockDefault="#all"> Changed from: <xs:complexType name="FilterType"> <xs:sequence> <xs:element minOccurs="0" maxOccurs="1" ref="adlq:LdapQuery" /> </xs:sequence> <xs:attribute name="Dialect" fixed="http://schemas.microsoft.com/2008/1/ActiveDirectory/Dialect/LdapQuery"/> </xs:complexType> Changed to: <xsd:complexType name="FilterType"> <xsd:sequence> <xsd:element minOccurs="0" maxOccurs="1" ref="adlq:LdapQuery" /> </xsd:sequence> <xsd:attribute name="Dialect" fixed="http://schemas.microsoft.com/2008/1/ActiveDirectory/Dialect/LdapQuery"/> </xsd:complexType> Changed from: <xs:element name="Filter" type="wsen:FilterType" minOccurs="0" maxOccurs="1" /> Changed to: <xsd:element name="Filter" type="wsen:FilterType" minOccurs="0" maxOccurs="1" /> </pre>

*Date format: YYYY/MM/DD

[MS-WSMV]: Web Services Management Protocol Extensions for Windows Vista

This topic lists the Errata found in [MS-WSMV] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-WSP]: Windows Search Protocol

This topic lists the Errata found in [MS-WSP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

[MS-WSTEP]: WS-Trust X.509v3 Token Enrollment Extensions

This topic lists the Errata found in [MS-WSTEP] 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.

Errata below are for Protocol Document Version [V9.0 – 2016/07/14](#).

Errata Published*	Description
2017/02/06	<p>In Section 3.1.4.1.3.3, wst:RequestSecurityTokenType, removed the wstep:PreferredLanguage attribute.</p> <p>Changed from:</p> <p>wstep:RequestID: An instance of wstep:RequestID as specified in section 3.1.4.1.2.4.</p> <p>WSTEP extends <wst:RequestSecurityTokenType> with an additional attribute: <xs:attribute name="PreferredLanguage" type="xs:language" use="optional" /> Only the attribute specified below is used in WSTEP. Any attribute received that is not specified below SHOULD be ignored. wstep:PreferredLanguage: The wstep:PreferredLanguage attribute defines the preferred language to be used in a server response.</p> <p>Changed to:</p> <p>wstep:RequestID: An instance of wstep:RequestID as specified in section 3.1.4.1.2.4.</p> <p>In Section, Appendix A: Full WSDL, changed from:</p> <pre><xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:wstep="http://schemas.microsoft.com/windows/pki/2009/01/enrollment" targetNamespace="http://schemas.microsoft.com/windows/pki/2009/01/enrollment" elementFormDefault="qualified"> <xs:import namespace="http://www.w3.org/XML/1998/namespace" schemaLocation="http://www.w3.org/2001/xml.xsd" /> <xs:element name="DispositionMessage" type="wstep:DispositionMessageType" nillable="true" /> <xs:complexType name="DispositionMessageType"> <xs:simpleContent> <xs:extension base="xs:string"> <xs:attribute ref="xml:lang" use="optional" /> </xs:extension> </xs:simpleContent> </xs:complexType> <xs:element name="CertificateEnrollmentWSDetail" nillable="true" type="wstep:CertificateEnrollmentWSDetailType" /> <xs:complexType name="CertificateEnrollmentWSDetailType"> <xs:sequence> <xs:element minOccurs="0" maxOccurs="1" name="BinaryResponse"</pre>

Errata Published*	Description
	<pre> nillable="true" type="xs:string" /> <xs:element minOccurs="0" maxOccurs="1" name="ErrorCode" nillable="true" type="xs:int" /> <xs:element minOccurs="0" maxOccurs="1" name="InvalidRequest" nillable="true" type="xs:boolean" /> <xs:element minOccurs="0" maxOccurs="1" name="RequestID" type="xs:string" nillable="true" /> </xs:sequence> </xs:complexType> <xs:element name="RequestID" type="xs:string" nillable="true" /> <xs:attribute name="PreferredLanguage" type="xml:language" use="optional"/> </xs:schema> Changed to: <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:wstep="http://schemas.microsoft.com/windows/pki/2009/01/enrollment" targetNamespace="http://schemas.microsoft.com/windows/pki/2009/01/enrollment" elementFormDefault="qualified"> <xs:import namespace="http://www.w3.org/XML/1998/namespace" schemaLocation="http://www.w3.org/2001/xml.xsd" /> <xs:element name="DispositionMessage" type="wstep:DispositionMessageType" nillable="true" /> <xs:complexType name="DispositionMessageType"> <xs:simpleContent> <xs:extension base="xs:string"> <xs:attribute ref="xml:lang" use="optional" /> </xs:extension> </xs:simpleContent> </xs:complexType> <xs:element name="CertificateEnrollmentWSDetail" nillable="true" type="wstep:CertificateEnrollmentWSDetailType" /> <xs:complexType name="CertificateEnrollmentWSDetailType"> <xs:sequence> <xs:element minOccurs="0" maxOccurs="1" name="BinaryResponse" nillable="true" type="xs:string" /> <xs:element minOccurs="0" maxOccurs="1" name="ErrorCode" nillable="true" type="xs:int" /> <xs:element minOccurs="0" maxOccurs="1" name="InvalidRequest" nillable="true" type="xs:boolean" /> <xs:element minOccurs="0" maxOccurs="1" name="RequestID" type="xs:string" nillable="true" /> </xs:sequence> </xs:complexType> <xs:element name="RequestID" type="xs:string" nillable="true" /> </xs:schema> </pre>

*Date format: YYYY/MM/DD

[MS-WSUSAR]: Windows Server Update Services: Administrative API Remoting Protocol

This topic lists the Errata found in the MS-WSUSAR 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V3.0 – 2016/07/14](#).

Errata Published*	Description
2017/02/20	<p>In Section 2.2.3.1, UpdateSearch Element, updated the element name UpdateSearch to UpdateScope.</p> <p>Changed from:</p> <p>2.2.3.1 UpdateSearch Element</p> <p>The UpdateSearch element is the top level node for the update search scope XML fragment...</p> <p>Changed to:</p> <p>2.2.3.1 UpdateScope Element</p> <p>The UpdateScope element is the top level node for the update search scope XML fragment...</p>
2017/02/20	<p>In Section 2.2.3.1, UpdateScope Element, revised the XML fragment to eliminate the duplicate UpdateTypes attribute.</p> <p>Changed from:</p> <pre><UpdateScope ApprovedStates="[integer]" FromArrivalDate="[datetime]" ToArrivalDate="[datetime]" UpdateTypes="[integer]" IncludedInstallationStates="[integer]" ExcludedInstallationStates="[integer]" ... UpdateApprovalActions="[integer]" ApprovedComputerTargetGroups="[string]" UpdateTypes="[integer]" ExcludeOptionalUpdates="[bool]" > <UpdateApprovalScope>...</UpdateApprovalScope> </UpdateScope></pre> <p>Changed to:</p> <pre><UpdateScope ApprovedStates="[integer]"</pre>

Errata Published*	Description
	<pre> FromArrivalDate="[datetime]" ToArrivalDate="[datetime]" UpdateTypes="[integer]" IncludedInstallationStates="[integer]" ExcludedInstallationStates="[integer]" ... UpdateApprovalActions="[integer]" ApprovedComputerTargetGroups="[string]" ExcludeOptionalUpdates="[bool]" > <UpdateApprovalScope>...</UpdateApprovalScope> </UpdateScope> </pre>
2017/02/20	<p>In Section 2.2.3.1.15, ApprovedComputerTargetGroups Attribute, in the escaped example, changed "GUIDID" to "GUID".</p> <p>Changed from:</p> <p>Because this is an attribute, the XML fragment has to be escaped, for example:</p> <pre> ApprovedComputerTargetGroups = "&lt;root&gt;&lt;TargetGroupID &gt;GUIDID&lt;/TargetGroupID &gt;&lt;/root&gt;," </pre> <p>Changed to:</p> <p>Because this is an attribute, the XML fragment has to be escaped, for example:</p> <pre> ApprovedComputerTargetGroups = "&lt;root&gt;&lt;TargetGroupID &gt;GUID&lt;/TargetGroupID &gt;&lt;/root&gt;," </pre> <p>In Section 2.2.3.2.9, ComputerTargetGroups Attribute, in the escaped example, changed "GUIDID" to "GUID".</p> <p>Changed from:</p> <p>Because this is an attribute, the XML fragment has to be escaped, for example:</p> <pre> ComputerTargetGroups = "&lt;root&gt;&lt;TargetGroupID &gt;GUIDID&lt;/TargetGroupID &gt;&lt;/root&gt;," </pre> <p>Changed to:</p> <p>Because this is an attribute, the XML fragment has to be escaped, for example:</p> <pre> ComputerTargetGroups = "&lt;root&gt;&lt;TargetGroupID &gt;GUID&lt;/TargetGroupID &gt;&lt;/root&gt;," </pre>
2017/02/20	In Section 2.2.3.2.2, RequestedTargetGroupNames Attribute, in the escaped example, added

Errata Published*	Description
	<p>"&quot;&lt;".</p> <p>Changed from:</p> <p>Because this is an attribute, the XML fragment has to be escaped, for example:</p> <pre>RequestedTargetGroupNames = "&lt;root&gt;&lt;RequestedTargetGroup Name=&quot;Target Group Name&lt;/RequestedTargetGroup&gt;...&lt;/root&gt;"</pre> <p>Changed to:</p> <p>Because this is an attribute, the XML fragment has to be escaped, for example:</p> <pre>RequestedTargetGroupNames = "&lt;root&gt;&lt;RequestedTargetGroup Name=&quot;Target Group Name=&quot;&gt;&lt;/RequestedTargetGroup&gt;...&lt;/root&gt;"</pre>
2017/02/20	<p>In Section 2.2.4.11, EmailNotificationConfigurationRow, added the complexType element to the first line of the XML definition.</p> <p>Changed from:</p> <pre><xsd: name="EmailNotificationConfigurationRow"> <xsd:sequence> ...</pre> <p>Changed to:</p> <pre><xsd:complexType name="EmailNotificationConfigurationRow"> <xsd:sequence> ...</pre>
2017/02/20	<p>In Section 3.1.4.82, GetDynamicCategories, added the </wsdl:operation> tag to the end of the XML definition.</p> <p>Changed from:</p> <pre>... name="ApiRemotingSoap_GetDynamicCategories_OutputMessage" message="tns:ApiRemotingSoap_GetDynamicCategories_OutputMessage"/></pre> <p>Changed to:</p> <pre>... name="ApiRemotingSoap_GetDynamicCategories_OutputMessage" message="tns:ApiRemotingSoap_GetDynamicCategories_OutputMessage"/></pre>

Errata Published*	Description
	</wsdl:operation>
2017/02/20	<p>In Section 3.1.4.76.3.1, SignCabExForPublishingWithTimeStampOptionRequestBody, in the description of the filePath field, changed the capitalization of the field name from filepath to filePath.</p> <p>Changed from: filePath: This field MUST be present. It specifies the path to the file to publish. If the filepath field is NULL, the server MUST send a SOAP fault as specified in section 3.1.4.1.</p> <p>Changed to: filePath: This field MUST be present. It specifies the path to the file to publish. If the filePath field is NULL, the server MUST send a SOAP fault as specified in section 3.1.4.1.</p>

*Date format: YYYY/MM/DD

[MS-WSUSSS]: Windows Update Services: Server-Server Protocol

This topic lists the Errata found in the MS-WSUSSS 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.

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - [Download](#)

Errata below are for Protocol Document Version [V3.0 – 2016/07/14](#).

Errata Published*	Description
2017/02/20	<p>In Section 2.2.4.1, ArrayOfAuthorizationCookie, changed the namespace for the type attribute in the XML definition from "s1" to "tns".</p> <p>Changed from:</p> <p>...</p> <pre><s:element minOccurs="0" maxOccurs="unbounded" name="AuthorizationCookie" nillable="true" type="s1:AuthorizationCookie" /></pre> <p>...</p> <p>Changed to:</p> <p>...</p> <pre><s:element minOccurs="0" maxOccurs="unbounded" name="AuthorizationCookie" nillable="true" type="tns:AuthorizationCookie" /></pre> <p>...</p> <p>In Section 2.2.4.3, ArrayOfGuid, changed the namespace for the type attribute in the XML definition from "s2" to "s1".</p> <p>Changed from:</p> <p>...</p> <pre><s:element minOccurs="0" maxOccurs="unbounded" name="guid" type="s2:guid" /></pre>

Errata Published*	Description
	<p>...</p> <p>Changed to:</p> <p>...</p> <pre><s:element minOccurs="0" maxOccurs="unbounded" name="guid" type="s1:guid" /></pre> <p>...</p> <p>In Section 2.2.4.6, ArrayOfUpdateIdentity, changed the namespace for the type attribute in the XML definition from "s1" to "tns".</p> <p>Changed from:</p> <p>...</p> <pre><s:element minOccurs="0" maxOccurs="unbounded" name="UpdateIdentity" nillable="true" type="s1:UpdateIdentity" /></pre> <p>...</p> <p>Changed to:</p> <p>...</p> <pre><s:element minOccurs="0" maxOccurs="unbounded" name="UpdateIdentity" nillable="true" type="tns:UpdateIdentity" /></pre> <p>...</p> <p>In Section 2.2.4.9, UpdateIdentity, changed the namespace for the type attribute in the XML definition from "s2" to "s1".</p> <p>Changed from:</p> <p>...</p> <pre><s:element minOccurs="1" maxOccurs="1" name="UpdateID" type="s2:guid" /></pre> <p>...</p> <p>Changed to:</p> <p>...</p> <pre><s:element minOccurs="1" maxOccurs="1" name="UpdateID"</pre>

Errata Published*	Description
	<pre> type="s1:guid" /> ... In Section 3.1.4.1.2.2, GetAuthConfigResponse, changed the namespace for the type attribute in the XML definition from "s1" to "tns". Changed from: ... <s:element minOccurs="0" maxOccurs="1" name="GetAuthConfigResult" type="s1:ServerAuthConfig" /> ... Changed to: ... <s:element minOccurs="0" maxOccurs="1" name="GetAuthConfigResult" type="tns:ServerAuthConfig" /> ... In Section 3.1.4.1.3.1, ServerAuthConfig, changed the namespace for the type attribute in the XML definition from "s1" to "tns". Changed from: ... <s:element minOccurs="0" maxOccurs="1" name="AuthInfo" type="s1:ArrayOfAuthPlugInInfo" /> ... Changed to: ... <s:element minOccurs="0" maxOccurs="1" name="AuthInfo" type="tns:ArrayOfAuthPlugInInfo" /> ... In Section 3.1.4.1.3.2, ArrayOfAuthPlugInInfo, changed the namespace for the type attribute in the XML definition from "s1" to "tns". </pre>

Errata Published*	Description
	<p>Changed from:</p> <p>...</p> <pre><s:element minOccurs="0" maxOccurs="unbounded" name="AuthPlugInInfo" nillable="true" type="s1:AuthPlugInInfo" /></pre> <p>...</p> <p>Changed to:</p> <p>...</p> <pre><s:element minOccurs="0" maxOccurs="unbounded" name="AuthPlugInInfo" nillable="true" type="tns:AuthPlugInInfo" /></pre> <p>...</p>
2017/02/20	<p>In Section 3.1.4.2.2.1, GetAuthorizationCookie, corrected the code snippet.</p> <p>Changed from:</p> <pre><s:element name="GetAuthorizationCookie"> <s:complexType> <s:sequence> <s:element minOccurs="0" maxOccurs="1" name="accountName" type="s:string" /> <s:element minOccurs="0" maxOccurs="1" name="accountGuid" type="s:string" /> <s:element minOccurs="0" maxOccurs="1" name="programKeys" type="tns:ArrayOfGuid" /> </s:sequence> </s:complexType> </s:element></pre> <p>Changed to (change in bold):</p> <pre><s:element name="GetAuthorizationCookie"> <s:complexType> <s:sequence> <s:element minOccurs="0" maxOccurs="1" name="accountName" type="s:string" /> <s:element minOccurs="0" maxOccurs="1" name="accountGuid" type="s:string" /> <s:element minOccurs="0" maxOccurs="1" name="programKeys" type="tns:ArrayOfGuid" /> </s:sequence> </s:complexType> </s:element></pre>

Errata Published*	Description
	<p>In Section 3.1.4.7.2.2, GetDriverIdListResponse, corrected the code snippet.</p> <p>Changed from:</p> <pre> <s:element name="GetDriverIdListResponse"> <s:complexType> <s:sequence> <s:element minOccurs="0" maxOccurs="1" name="GetDriverIdListResult" type="tns:DriverSetAndRevisionIdList" /> </s:sequence> </s:complexType> </s:element> </pre> <p>Changed to (change in bold):</p> <pre> <s:element name="GetDriverIdListResponse"> <s:complexType> <s:sequence> <s:element minOccurs="0" maxOccurs="1" name="GetDriverIdListResult" type="tns:DriverSetAndRevisionIdList" /> </s:sequence> </s:complexType> </s:element> </pre>

*Date format: YYYY/MM/DD

[MS-WUSP]: Windows Update Services: Client-Server Protocol

This topic lists the Errata found in [MS-WMF] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

[MS-XCEP]: X.509 Certificate Enrollment Policy Protocol

This topic lists the Errata found in [MS-XCEP] 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.

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)