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.

RSS
Atom

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 Docs.Microsoft.Com [DMC]) and provide links to archived Errata (i.e., Errata already released with the documents on DMC).

Protocols Documents with Active Errata

[MC-NBFX]: .NET Binary Format XML Data Structure

[MC-NMF]: .NET Message Framing Protocol

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

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

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

[MS-ADSC]: Active Directory Schema Classes

[MS-ADTS]: Active Directory Technical Specification

[MS-AZOD]: Authorization Protocols Overview

[MS-BKUP]: Microsoft NT Backup File Structure

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

[MS-CRTD]: Certificate Templates Structure

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

[MS-DHCPE]: Dynamic Host Configuration Protocol (DHCP) Extensions

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

[MS-DTYP]: Windows Data Types

[MS-EMF]: Enhanced Metafile Format

Copyright © 2020 Microsoft Corporation

[MS-EMFPLUS]: Enhanced Metafile Format Plus Extensions

[MS-EMFSPOOL]: Enhanced Metafile Spool Format

[MS-ERREF]: Windows Error Codes

[MS-EVEN]: EventLog Remoting Protocol

[MS-FSCC]: File System Control Codes

[MS-FRS2]: Distributed File System Replication Protocol

[MS-GPOL]: Group Policy: Core Protocol

[MS-GPWL]: Group Policy: Wireless/Wired Protocol Extension

[MS-IKEE]: Internet Key Exchange Protocol Extensions

[MS-KILE]: Kerberos Protocol Extensions

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

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

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

[MS-MDM]: Mobile Device Management Protocol

[MS-NCNBI]: Network Controller Northbound Interface Specification

[MS-NNS]: .NET NegotiateStream Protocol

[MS-NRBF]: .NET Remoting: Binary Format Data Structure

[MS-NRPC]: Netlogon Remote Protocol

[MS-OCSPA]: Microsoft OCSP Administration Protocol

[MS-OLEPS]: Object Linking and Embedding (OLE) Property Set Data Structures

[MS-PAR]: Print System Asynchronous Remote Protocol

[MS-RAI]: Remote Assistance Initiation Protocol

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

[MS-RDPECAM]: Remote Desktop Protocol: Video Capture Virtual Channel Extension

[MS-RDPEDISP]: Remote Desktop Protocol: Display Update Virtual Channel Extension

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

[MS-RDPELE]: Remote Desktop Protocol: Licensing Extension

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

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

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

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

Copyright © 2020 Microsoft Corporation

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

[MS-RPCE]: Remote Procedure Call Protocol Extensions

[MS-RPRN]: Print System Remote Protocol

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

[MS-RRP]: Windows Remote Registry Protocol

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

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

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

[MS-SSTR]: Smooth Streaming Protocol

[MS-SWN]: Service Witness Protocol

[MS-TSGU]: Terminal Services Gateway Server Protocol

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

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

[MS-WKST]: Workstation Service Remote Protocol

[MS-WMF]: Windows Metafile Format

[MS-WMIO]: Windows Management Instrumentation Encoding Version 1.0 Protocol

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

[MS-WSP]: Windows Search Protocol

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

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

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

Errata Archives

June 30, 2015 - Download

October 16, 2015 - Download

March 2, 2016 - Download

July 18, 2016 - Download

September 26, 2016 - Download

March 20, 2017 - Download

June 1, 2017 - Download

August 21, 2017 - Download

September 15, 2017 - Download

Copyright © 2020 Microsoft Corporation

December 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

March 13, 2019 - Download

June 24, 2019 – Download

September 23, 2019 - Download

October 14, 2019 - Download

March 4, 2020 - Download

June 15, 2020 - Download

August 24, 2020 – Download

September 29, 2020 – Download

November 23, 2020 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[MC-NBFX]: .NET Binary Format XML Data Structure

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

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

RSS
Atom

Errata below are for Protocol Document Version V8.0 – 2019/03/13.

Errata Published*	Description
2019/12/09	In Section 2.2.3.30, QNameDictionaryTextRecord(0xBC), the length of the Name field was changed from 3 bytes to variable: Changed from: Name (3 bytes) Changed to: Name (variable) The packet diagram for the message was also changed to reflect the length.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MC-NMF]: .NET Message Framing Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V9.0 – 2018/03/16.

Errata Published*	Description
2018/07/02	In Section 2.2.6, Preamble Message, the field descriptions have been modified as follows and have been moved to follow the packet diagram. Changed from: The VersionRecord MUST be formatted as specified in section 2.2.3.1. The ModeRecord MUST be formatted as specified in section 2.2.3.2. The ViaRecord MUST be formatted as specified in section 2.2.3.3. The EnvelopeEncodingRecord MUST be formatted as specified in section 2.2.3.4 Changed to: VersionRecord (3 bytes): This field MUST be formatted as specified in section 2.2.3.1. ModeRecord (2 bytes): This field MUST be formatted as specified in section 2.2.3.2. ViaRecord (variable): This field MUST be formatted as specified in section 2.2.3.3. EnvelopeEncodingRecord (variable): This field MUST be formatted as specified in section 2.2.3.4

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MC-PRCR]: Peer Channel Custom Resolver Protocol

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

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

RSS
Atom

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:

September 15, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 V15.0 – 2018/09/12.

Errata Published*	Description
2018/12/17	In Section 1.2.1, Normative References, the following reference has been deleted: [RFC4346] Dierks, T., and Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006, http://www.ietf.org/rfc/rfc4346.txt In Section 2.1, Endpoints, changed from: The ADWS protocol set uses two types of authentication. Each endpoint (except for the "mex" endpoint) supports one or the other. The forms of authentication are: • Windows Integrated: These endpoints use Transport Layer Security (TLS) [RFC4346] to protect the TCP transport. Integrated Windows authentication using the .Net Negotiate Stream protocol [MS-NNS] is used to authenticate the client to the server at the transport layer and to negotiate the session key used for TLS. Changed to: The ADWS protocol set uses two types of authentication. Each endpoint (except for the "mex" endpoint) supports one or the other. The forms of authentication are: • Windows Integrated: These endpoints use integrated Windows authentication with the .Net Negotiate Stream protocol [MS-NNS] to authenticate the client and provide message security at the transport layer.

* Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

September 15, 2017 - Download

September 12, 2018 - Download

Errata below are for Protocol Document Version V7.0 – 2018/09/12.

Errata Published*	Description
2019/05/27	In the sections listed below, the enum Certificate Type values have been changed from string to integer: Section 2.2.2.12, Port Type Section 2.2.2.14, TLS Query Behavior Section 2.2.2.15, Certificate Validation Section 2.2.2.16, Certificate Type Section 2.2.2.17, Error Type Section 3.10.5.1.1.3, Processing Details Section 3.10.5.1.1.3, Processing Details Section 3.11.5, Message Processing Events and Sequencing Rules Section 3.11.5.1, End-user X509 Certificate Success Processing Section 3.11.5.2, End-user X509 Certificate Common Processing Section 6, Appendix A: Full JSON Schema For details on the above changes, see the PDF doc here.
2019/05/27	In Section 3.10.5.1.1.2, Response Body, changed from: No response body is returned. Changed to: The response from the server MUST be returned to the client.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 – 2018/09/12.

Errata Published*	Description
2019/11/25	In Section 3.1.4.1.1.3, GetFsTrustInformationSoapOut, and Section 6, Appendix: Full WSDL, the value of minOccurs was changed from 1 to 0. Changed from: `<s:complexType name="VersionInformation"> <s:sequence> <s:element minOccurs="1" maxOccurs="1" name="SoftwareVersion" type="s:long" /> <s:element minOccurs="1" maxOccurs="1" name="Guid" type="s1:guid" /> <s:element minOccurs="1" maxOccurs="1" name="Version" type="s:long" /> </s:sequence>` Changed to: `<s:complexType name="VersionInformation"> <s:sequence> <s:element minOccurs="0" maxOccurs="1" name="SoftwareVersion" type="s:long" /> <s:element minOccurs="0" maxOccurs="1" name="Guid" type="s1:guid" /> <s:element minOccurs="0" maxOccurs="1" name="Version" type="s:long" /> </s:sequence>`

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-ADLS]: Active Directory Lightweight Directory Services Schema

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

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

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 – 2018/03/16.

Errata Published*	Description

2019/09/16	In Section 2.243, Class samDomain, changed from:
	
	`(OA;CIOI;RPWP;3f78c3e5-f79a-46bd-a0b8-9d18116ddc79;;PS)`
	`S:(AU;SA;WDWOWP;;;WD)(AU;SA;CR;;;BA)(AU;SA;CR;;;DU)`
	
	Changed to:
	
	`(OA;CIOI;RPWP;3f78c3e5-f79a-46bd-a0b8-9d18116ddc79;;PS)`
	`(OA;CIIO;SW;9b026da6-0d3c-465c-8bee-5199d7165cba;bf967a86-0de6-11d0-a285-00aa003049e2;PS)`
	`(OA;CIIO;SW;9b026da6-0d3c-465c-8bee-5199d7165cba;bf967a86-0de6-11d0-a285-00aa003049e2;CO)`
	`S:(AU;SA;WDWOWP;;;WD)(AU;SA;CR;;;BA)(AU;SA;CR;;;DU)`

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

March 20, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

March 13, 2019 - Download

March 4, 2020 - Download

August 24, 2020 – Download

Errata below are for Protocol Document Version V52.0 - 2020/08/26

Errata Published*	Description
2021/01/11	In Section 2.2.20.4 CUSTOM_KEY_INFORMATION, clarified description of the 'FekKeyVersion' field. Changed from: FekKeyVersion (1 byte): An 8-bit unsigned integer that specifies the version of the File Encryption Key (FEK). This field must be set to 1. Changed to: FekKeyVersion (1 byte): An 8-bit unsigned integer that specifies the version of the buffer stored in KEY_USAGE_FEK (section 2.2.20.5.3). This field must be set to 1.
2020/11/10	Added new Section 5.1.1.6 Authentication Expiration, to clarify the conditions under which a DC uses the expiry time of a connection to initiate disconnection of such a connection, and in the specific case of a new LDAP request on an existing connection with an elapsed expiry time, to subsequently send a Notice of Disconnection; as specified by the included ASN.1 definition. Changed to:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	5.1.1.6 Authentication Expiration If the authentication method used to establish a connection specifies an expiry time, the DC MUST associate the expiry time with the connection. The expiry time is then used as follows: A DC MUST disconnect connections having expiry times in a given period of time following the expiry time. Although the protocol places no boundary or other requirement on the length of the given time period, it is recommended that implementations minimize the length of the time period to improve client usability of the directory. ...
2020/09/14	In Section 3.1.1.5.3.3 Processing Specifics, specified the server operations that MUST occur whenever an msDS-AdditionalDnsHostName attribute is added or when one is removed. Added new Normative Reference: [MSKB-4505903]. Changed from: "If any of the operations above fail, then the modify returns unwillingToPerform. This processing rule is not supported by ADAM RTW DCs." Changed to: "If any of the operations above fail, then the modify returns unwillingToPerform. This processing rule is not supported by ADAM RTW DCs. In AD DS, if the msDS-AdditionalDnsHostName attribute is modified, additional operations are performed as follows. These steps assume the value(s) added or deleted are in the form anyDnsLabel.suffix: For each msDS-AdditionalDnsHostName attribute value that is being added, the server MUST add a value to the msDS-AdditionalSamAccountName attribute in the format 'anyDnsLabel$'. Windows Server 2016, Windows Server 2019, and Windows Server v1903 operating system without [MSKB-4505903] installed, will add the 'anyDnsLabel$' value to the msDS-AdditionalDnsHostName attribute. For each msDS-AdditionalDnsHostName value that is being removed, the server MUST check for a corresponding 'anyDnsLabel$' value in the msDS-AdditionalSamAccountName attribute, and if found, remove it.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 V4.0 - 2018/11/05

Errata Published*	Description
2021/01/11	In Section 1.1.1.3, Security Descriptor, the language describing how access is granted or denied has been updated. Changed from: "If an explicit deny is found, access is denied. Explicit deny ACEs are always applied, even if conflicting allow ACEs exist. Explicit allow ACEs are examined, as are inherited deny and allow ACEs. The ACEs that apply to the user are accumulated. Inherited deny ACEs overrule inherited allow ACEs but are overruled themselves by explicit allow permissions. If none of the user SIDs or group SIDs in the access token match the DACL, the user is denied access implicitly." Changed to: "The access check algorithm processes ACEs in the order in which they are present within the DACL in order to determine the appropriate access. A matching allow ACE will grant access for any access mask bits present in the ACE, while a matching deny ACE will deny access for any access mask bits in the ACE not already granted by an allow ACE (preventing those bits from being granted by a later allow ACE). As soon as access is granted by any one or more allow ACEs, processing will stop and access will be granted. If a specific desired access bit is denied by a deny ACE (and has not been already granted by an allow ACE) then processing will stop and access will be denied. Thus the recommendation is to always place deny ACEs at the beginning of the ACL followed by allow ACEs, if the deny ACEs should take precedence over the allow ACEs. If none of the user SIDs or group SIDs in the access token match the DACL, the user is denied access implicitly."

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[MS-BKUP]: Microsoft NT Backup File Structure

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

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

RSS
Atom

Errata below are for Protocol Document Version V9.0 – 2018/09/12.

Errata Published*	Description
2020/04/27	In Section 2.13.1, Creating an NT Backup File, a new paragraph was added to the end of the section. Added: If F has any ghosted extents, the NT backup file MUST generate one GHOSTED_EXTENT backup stream structure. During restore the GHOSTED_EXTENT backup stream structure is presented to the filesystem to recreate the file ghosted extent state. The following new sections were added: 2.12 FileSystem Ghosted Extents Functionality Hierarchical Storage Management (HSM) solutions on top of a filesystem remove cold data and move it to the next storage tier. This movement creates sparse holes in file system data, and HSM solutions have to maintain mappings between those sparse holes and location of the data in the new tier. An implementation of the Ghosted extents feature helps this process by maintaining some token in the sparse holes, on behalf of the HSM solution. This obviates the need for the HSM solution to maintain its own mappings. When a file with such tokens, hereby referred to as ghosted extents, are backed up, the backup process should store the tokens and their locations in the backup stream state. On restore those tokens should be reinserted in the data stream in exactly the same locations to recreate the original file state. The method to query the tokens, serialize the tokens, and restore the tokens is file system implementation specific. 2.12.1 Ghosted Extents Stream Structure A ghosted extent stream structure represents ghosted extents in the DATA backup stream. Ghosted extents are a kind of sparse extents, which store a GUID representing the owner of the extent and some variable-sized metadata. The structure of the data portion of this backup stream for a specific implementation is as follows: 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

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Count TotalCount Data (variable) ... Count (4 bytes): The number of extents in the Data portion. TotalCount (4 bytes): The total number of ghosted extents in the stream. Data (Variable): The data portion of the above structure contains a variable number of extents. The number of extents is given by Count. The structure of each Extent is described below: 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 Offset ... Length ... Guid ... ... NextOffset Size Data (variable) ...

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Offset (8 bytes): The logical byte offset in the DATA backup stream where the ghosted extent starts. Length (8 bytes): The logical length of the ghosted extent. GUID (16 bytes): The GUID identifier of the owner for the ghosted extent. NextOffset (4 bytes): Offset to the next Extent structure. Size (4 bytes): Size of the metadata of the ghosted extent. Data (variable): Metadata of the ghosted extent.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[MS-CDP]: Connected Devices Platform Protocol Version 3

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

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

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

March 16, 2018 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

March 4, 2020 - Download

September 29, 2020 – Download

Errata below are for Protocol Document Version V30.0 - 2020/10/01

Errata Published*	Description
2021/01/11	In Section 6 Appendix A: Product Behavior, the following behavior notes have been updated: Changed from: <245> Section 3.3.5.5 ... AccessMode.SharingMode ShareAccess 0 Compatibility mode (see below) 1 0x0L (don't share, exclusive use) 2 FILE_SHARE_READ 3 FILE_SHARE_WRITE 4 FILE_SHARE_READ | FILE_SHARE_WRITE 0xFF FCB mode (see below)

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	• For Compatibility mode, special filename suffixes (after the '.' in the filename) are mapped to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM, "COM". All other file names are mapped to SharingMode 3. • For FCB mode, if the file is already open on the server, the current sharing mode of the existing Open is preserved and a FID for the file is returned. If the file is not already open on the server, the server attempts to open the file using SharingMode 1. ... Changed to: ... AccessMode.SharingMode ShareAccess 0 Compatibility mode (see below) 1 0x0L (don't share, exclusive use) 2 FILE_SHARE_READ 3 FILE_SHARE_WRITE 4 FILE_SHARE_READ | FILE_SHARE_WRITE • For Compatibility mode, special filename suffixes (after the '.' in the filename) are mapped to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM, "COM". All other file names are mapped to SharingMode 3. • If AccessMode field in the request is 0xFF, and the file is already open on the server, the current sharing mode of the existing Open is preserved and a FID for the file is returned. If the file is not already open on the server, the server attempts to open the file using SharingMode 1. ... Changed from: <297> Section 3.3.5.35 ... AccessMode.SharingMode ShareAccess 0 Compatibility mode (see below) 1 0x0L (don't share, exclusive use)

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	2 FILE_SHARE_READ 3 FILE_SHARE_WRITE 4 FILE_SHARE_READ | FILE_SHARE_WRITE 0xFF FCB mode (see below) ● For Compatibility mode, special filename suffixes (after the '.' in the filename) are mapped to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM", and "COM". All other file names are mapped to SharingMode 3. ● For FCB mode, if the file is already open on the server, the current sharing mode of the existing Open is preserved, and a FID for the file is returned. If the file is not already open on the server, the server attempts to open the file using SharingMode 1. ... Changed to: ... AccessMode.SharingMode ShareAccess 0 Compatibility mode (see below) 1 0x0L (don't share, exclusive use) 2 FILE_SHARE_READ 3 FILE_SHARE_WRITE 4 FILE_SHARE_READ | FILE_SHARE_WRITE ● For Compatibility mode, special filename suffixes (after the '.' in the filename) are mapped to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM", and "COM". All other file names are mapped to SharingMode 3. ● If AccessMode field in the request is 0xFF, and the file is already open on the server, the current sharing mode of the existing Open is preserved, and a FID for the file is returned. If the file is not already open on the server, the server attempts to open the file using SharingMode 1. ... Changed from: <339> Section 3.3.5.58.2

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	... AccessMode.SharingMode ShareAccess 0 Compatibility mode (see following) 1 0x0L (don't share, exclusive use) 2 FILE_SHARE_READ 3 FILE_SHARE_WRITE 4 FILE_SHARE_READ | FILE_SHARE_WRITE 0xFF FCB mode (see following) ● For Compatibility mode, special filename suffixes (after the "." in the filename) are mapped to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM", "COM". All other file names are mapped to SharingMode 3. ● For FCB mode, if the file is already open on the server, the current sharing mode of the existing Open is preserved, and a FID for the file is returned. If the file is not already open on the server, the server attempts to open the file using SharingMode 1. ... Changed To: ... AccessMode.SharingMode ShareAccess 0 Compatibility mode (see following) 1 0x0L (don't share, exclusive use) 2 FILE_SHARE_READ 3 FILE_SHARE_WRITE 4 FILE_SHARE_READ | FILE_SHARE_WRITE ● For Compatibility mode, special filename suffixes (after the "." in the filename) are mapped to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM", "COM". All other file names are mapped to SharingMode 3. ● If AccessMode field in the request is 0xFF, and the file is already open on the server, the current sharing mode of the existing Open is preserved, and a FID for the file is returned. If

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	the file is not already open on the server, the server attempts to open the file using SharingMode 1. ...

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

March 4, 2020 - Download

August 24, 2020 – Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[MS-CRTD]: Certificate Templates Structure

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

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

RSS
Atom

Errata below are for Protocol Document Version V24.0 – 2018/09/12.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2020/11/10</td><td>In Section 2.28 msPKI-Certificate-Name-Flag Attribute, added flag 'CT_FLAG_SUBJECT_ALT_REQUIRE_SPN' and description to the table in this section; for adding the UPN attribute to an issued certificate.

Changed from:

<table>
<tr><th>Flag</th><th>Client processing</th></tr>
<tr><td>0x00400000
CT_FLAG_SUBJECT_ALT_REQUIRE_DOMAIN_DNS</td><td>This flag instructs the CA to add the value of the requester's FQDN (2) and NetBIOS name to the Subject Alternative Name extension of the issued certificate (1).</td></tr>
<tr><td>0x01000000
CT_FLAG_SUBJECT_ALT_REQUIRE_DIRECTORY_GUID</td><td>This flag instructs the CA to add the value of the objectGUIDattribute (2) from the requestor's user object (2) in Active Directory to the Subject Alternative Name extension of the issued certificate (1).</td></tr>
</table>

Changed to:

<table>
<tr><th>Flag</th><th>Client processing</th></tr>
<tr><td>0x00400000
CT_FLAG_SUBJECT_ALT_REQUIRE_DOMAIN_DNS</td><td>This flag instructs the CA to add the value of the requester's FQDN (2) and NetBIOS name to the Subject Alternative Name extension of the issued certificate (1).</td></tr>
<tr><td>0x00800000
CT_FLAG_SUBJECT_ALT_REQUIRE_SPN</td><td>This flag instructs the CA to add the value of the UPN attribute (2) from the requestor's user object (2) in Active Directory to the Subject Alternative Name extension of the issued certificate (1).</td></tr>
</table>
</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>0x01000000
CT_FLAG_SUBJECT_ALT_REQUIRE_DIRECTORY_GUID</td><td>This flag instructs the CA to add the value of the objectGUIDattribute (2) from the requestor's user object (2) in Active Directory to the Subject Alternative Name extension of the issued certificate (1).</td></tr>
</table>
</td></tr>
<tr><td>2019/12/16</td><td>
In Section 2.26, msPKI-Enrollment-Flag Attribute, added missing 'CT_FLAG_SKIP_AUTO_RENEWAL' flag and description to the enrollment flags table.

Changed from:

<table>
<tr><td>0x00020000
CT_FLAG_ISSUANCE_POLICIES_FROM_REQUEST</td><td>This flag indicates that the certificate issuance policies to be included in the issued certificate come from the request rather than from the template. The template contains a list of all of the issuance policies that the request is allowed to specify; if the request contains policies that are not listed in the template, then the request is rejected. For the processing rules of this flag, see [MS-WCCE] section 3.2.2.6.2.1.4.5.8.<33></td></tr>
</table>

Changed to:

<table>
<tr><td>0x00020000
CT_FLAG_ISSUANCE_POLICIES_FROM_REQUEST</td><td>This flag indicates that the certificate issuance policies to be included in the issued certificate come from the request rather than from the template. The template contains a list of all of the issuance policies that the request is allowed to specify; if the request contains policies that are not listed in the template, then the request is rejected. For the processing rules of this flag, see [MS-WCCE] section 3.2.2.6.2.1.4.5.8.<33></td></tr>
<tr><td>0x00040000
CT_FLAG_SKIP_AUTO_RENEWAL</td><td>This flag indicates that the certificate should not be auto-renewed, although it has a valid template.</td></tr>
</table>

In Section 2.27, msPKI-Private-Key-Flag Attribute, added missing 'CT_FLAG_HELLO_LOGON_KEY' flag and description to the private key flags table.
</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>Changed from:

<table><tr><td>0x00000800 *
CT_FLAG_EK_VALIDATE_KEY</td><td>This flag indicates that attestation based on the hardware key of the TPM is to be performed. For more details, see [MS-WCCE] section 3.2.2.6.2.1.4.5.7.</td></tr></table>
Changed to:

<table><tr><td>0x00000800 *
CT_FLAG_EK_VALIDATE_KEY</td><td>This flag indicates that attestation based on the hardware key of the TPM is to be performed. For more details, see [MS-WCCE] section 3.2.2.6.2.1.4.5.7.</td></tr><tr><td>0x00200000 *
CT_FLAG_HELLO_LOGON_KEY</td><td>This flag indicates that the key is used for Windows Hello logon. For more details, see [MS-WCCE] section 3.2.2.6.2.1.4.5.7.</td></tr></table></td></tr>
</table>

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

September 12, 2018 - Download

September 29, 2020 – Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

September 29, 2020 – Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

August 24, 2020 – Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

September 12, 2018 - Download

Errata below are for Protocol Document Version V28.0 – 2018/09/12.

Errata Published*	Description
2018/10/29	In Section 3.1.4.2, Sending a DFS Referral Request to the Server, the following has been changed from: The client MUST query the DFS referral, as specified in [MS-CIFS] section 3.4.4.9, by passing ClientGenericContext, HostName, UserCredentials, MaxOutputSize, the REQ_GET_DFS_REFERRAL_EX or REQ_GET_DFS_REFERRAL structure as the input buffer, and the FSCTL code set to FSCTL_DFS_GET_REFERRALS or FSCTL_DFS_GET_REFERRALS_EX based on the input buffer. Changed to: The client MUST query the DFS referral, as specified in [MS-CIFS] section 3.4.4.9, by passing ClientGenericContext, HostName, UserCredentials, MaxOutputSize, the REQ_GET_DFS_REFERRAL_EX or REQ_GET_DFS_REFERRAL structure as the input buffer, and the FSCTL code set to FSCTL_DFS_GET_REFERRALS, if the input buffer is an REQ_GET_DFS_REFERRAL, or FSCTL_DFS_GET_REFERRALS_EX, if the input buffer is an REQ_GET_DFS_REFERRAL_EX.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-DHCPE]: Dynamic Host Configuration Protocol (DHCP) Extensions

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

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

RSS
Atom

Errata below are for Protocol Document Version V24.0 – 2018/09/12.

Errata Published*	Description
2019/12/16	In Section 3.1.5.2, Receiving a DHCPACK, added alternate processing for none or two route options. Changed from: If it contains a Microsoft Classless Static Route Option, the client MUST first check whether the option conforms to the syntax specified in section 2.2.8. If any of the parameters in this DHCPv4 option are invalid or incomplete, the DHCPv4 client MUST silently discard the complete DHCPv4 message and start the initialization process again. Otherwise, the specified routes MUST be inserted into the routing table in the TCP/IP stack. Changed to: If it contains a Microsoft Classless Static Route Option, the client MUST first check whether the option conforms to the syntax specified in section 2.2.8. If any of the parameters in this DHCPv4 option are invalid or incomplete, the DHCPv4 client MUST silently discard the complete DHCPv4 message and start the initialization process again. Otherwise, if the DHCPACK does not contain a Classless Static Route Option (121), the specified routes MUST be inserted into the routing table in the TCP/IP stack. If it contains both a Microsoft Classless Static Route Option (249) and a Classless Static Route Option (121) then the client MUST select either (in any implementation-specific way[27]) set of routes as the routes to be added into the routing table in the TCP/IP stack. <27> Section 3.1.5.2: All versions of Windows Vista and Windows Server 2008 and later will insert the last option in the message.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

September 15, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

September 12, 2018 - Download

August 24, 2020 – Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

Errata below are for Protocol Document Version V40.0 – 2019/09/12.

Errata Published*	Description

2019/10/16	In Section 4.1.1.2.3, CreateNtdsData, the pseudocode for creating an nTDSDSA object has been updated by including a check if attributes meet correct order for creating the NtdsDsa object, and if not, setting the ERROR_DS_NO_CROSSREF_FOR_NC error and returning 'false'.
	
	Changed from:
	
	.. if not accessAllowed then
	SetErrorData(SV_PROBLEM_DIR_ERROR, serviceError,
	ERROR_ACCESS_DENIED, pmsgOut, ver)
	return false
	endif
	
	/* Check for the functional level compliance. The functional level.."
	
	Changed to:
	.. if not accessAllowed then
	SetErrorData(SV_PROBLEM_DIR_ERROR, serviceError,
	ERROR_ACCESS_DENIED, pmsgOut, ver)
	return false
	endif
	
	correctOrder := DoAttributesSatisfyPreCheckForCreateNtdsDsa (entList)
	
	if not correctOrder then

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	SetErrorData(SV_PROBLEM_DIR_ERROR, serviceError, ERROR_DS_NO_CROSSREF_FOR_NC, pmsgOut, ver) return false endif /* Check for the functional level compliance. The functional level.." Also, in Section 4.1.1.2.11, DoAttributesSatisfyPreCheckForCreateNtdsDsa, new content has been added to describe the new procedure above added in section 4.1.1.2.3.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

December 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

December 1, 2017 - Download

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

Errata below are for Protocol Document Version V35.0 – 2018/09/12

Errata Published*	Description
2021/01/25	In Section 2.4.4.1, ACE_HEADER, revised the description of the INHERITED_ACE flag to indicate it is not set automatically. Changed from: Used to indicate that the ACE was inherited. Set this bit in the child object if the child object has the same DACL as the parent object.<54> Changed to: Used to indicate that the ACE was inherited.<54> See section 2.5.3.5 for processing rules for setting this flag. Added new section 2.5.3.5, Setting the INHERITED_ACE Flag: ACEs are usually contained in ACLs (see section 2.4.5) with the INHERITED_ACE flag in an ACE set as part of comparing the ACEs in a parent ACL and a child ACL. If an ACE is present in both the parent ACL and the child ACL, the INHERITED_ACE flag is set in the child ACE if the ACEs are equal: ▪ If either ACE is NULL, the ACEs are not equal. ▪ If the AceType of the ACEs are different, they are not equal. ▪ If the parent AceFlags anded with not INHERITED_ACE are not equal to the child AceFlags, it is a special case where there may be an additional ACE that was created:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	▪ If the ACE is a child of a container, parent flags are set, there is a following ACE, the child ACE flags are not set, and INHERIT_ONLY is set in the parent ACE, then for ▪ ACCESS_ALLOWED_ACE_TYPE, ACCESS_DENIED_ACE_TYPE, SYSTEM_AUDIT_ACE_TYPE, SYSTEM_ALARM_ACE_TYPE, skip the current ACE if the masks are equal in the parent ACE and the next child ACE, and their SIDs are equal, and compare this next ACE to the parent ACE. ▪ Otherwise, the ACEs are not equal. ▪ If the parent and child flags are not equal, the ACEs are not equal. ▪ If the ACE_TYPE_OBJECT_PRESENT is set in the parent ACE, but the parent and child ACE GUIDs are not equal, the ACEs are not equal. ▪ If the ACE_INHERITED_OBJECT_TYPE_PRESENT is set in the parent ACE, but the parent and child ACE GUIDs are not equal, the ACEs are not equal. ▪ If ACCESS_ALLOWED_COMPOUND_ACE_TYPE is set in the parent ACE, but the compound ACE types are not equal in the parent and child ACEs, the ACEs are not equal. ▪ If either the parent or child ACE SIDs are not valid, or the two are not equal, the ACEs are not equal. ▪ If the parent and child ACE access masks are not equal, the ACEs are not equal.
2020/03/02	In Section 2.5.3.2, Access Check Algorithms Pseudocode, the pseudocode confirming that the object owner is always granted READ_CONTROL and WRITE_DAC has been corrected as follows: Changed from: Set GrantedAccess to GrantedAccess or READ_CONTROL or WRITE_OWNER Changed to: Set GrantedAccess to GrantedAccess or READ_CONTROL or WRITE_DAC
2019/11/11	In Section 2.4.2.4, Well-Known SID Structures, the description of the table entry for AUTHENTICATED_USERS has been updated for clarity, and an associated behavior note added: Changed from: A group that includes all users whose identities were authenticated when they logged on. Changed to: A group that includes all users whose identities were authenticated when they logged on. Users authenticated as Guest or Anonymous are not members of this group.<11> <11> Windows server versions earlier than Windows Server 2003 and client versions earlier than Windows XP SP2 included the Guest account in the Authenticated Users group.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[MS-DVRJ]: Device Registration Join Protocol

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

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

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

August 24, 2020 – Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Errata below are for Protocol Document Version V14.0 – 2018/09/12

Errata Published*	Description
2021/03/08	In Section 2.3.7.3, EMR_CREATECOLORSPACEW Record, clarified the semantics of the cbData value: Changed from: Data (variable, optional): An array of bytes that specifies color profile data. Changed to: Data (variable, optional): An array of bytes that specifiescolor profiledata. When cbData is zero, this field is optional and is ignored.
2021/03/08	In Section 2.3.6.1, EMR_DRAWESCAPE Record, changed cross-reference: Changed from: Type (4 bytes): An unsigned integer that identifies this record type from the EmrComment enumeration (section 2.1.10). It MUST be EMR_DRAWESCAPE, which is 0x00000069. Changed to: Type (4 bytes): An unsigned integer that identifies this record type from the RecordType enumeration (section 2.1.1). It MUST be EMR_DRAWESCAPE, which is 0x00000069. In Section 2.3.6.2, EMR_EXTESCAPE Record, changed cross-reference: Changed from: Type (4 bytes): An unsigned integer that identifies this record type from the EmrComment enumeration (section 2.1.10). This value is 0x0000006A. Changed to:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Type (4 bytes): An unsigned integer that identifies this record type from the RecordType enumeration (section 2.1.1). This value is 0x0000006A. In Section 2.3.6.3, EMR_NAMEDESCAPE Record, changed cross-reference: Changed from: Type (4 bytes): An unsigned integer that identifies this record type from the EmrComment enumeration (section 2.1.10). It MUST be EMR_NAMEDESCAPE, which is 0x0000006E. Changed to: Type (4 bytes): An unsigned integer that identifies this record type from the RecordType enumeration (section 2.1.1). It MUST be EMR_NAMEDESCAPE, which is 0x0000006E.
2021/02/08	In Section 2.3, EMF Records, added information about ignoring data beyond the defined length of an EMF record: Changed from: All EMF records MUST be multiples of 4 bytes in length; hence, each record starts on a 32-bit offset from the start of the metafile. To ensure each subsequent record also starts on a 32-bit boundary, an AlignmentPadding field is used, if necessary. The contents of AlignmentPadding fields are indeterminate and MUST be ignored. In general, such fields are shown only in the generic definitions of record categories. Changed to: All EMF records MUST be multiples of 4 bytes in length; hence, each record starts on a 32-bit offset from the start of the metafile. To ensure each subsequent record also starts on a 32-bit boundary, an AlignmentPadding field is used, if necessary. The contents of AlignmentPadding fields are indeterminate and MUST be ignored. In general, such fields are shown only in the generic definitions of record categories. To ensure maximum compatibility, implementations need to allow for record truncation for unused fields at the end of an EMF record. If there are extra data at the end of the record undocumented by this specification, these data MUST be ignored.
2021/02/08	In Section 2.3.5.17, EMR_POLYBEZIER16 Record, removed the Start field which does not exist in the record: Changed from: Bounds (16 bytes): A RectL object ([MS-WMF] section 2.2.2.19), which specifies the inclusive-inclusive bounding rectangle in logical units. Start (8 bytes): A PointL object ([MS-WMF] section 2.2.2.15), which specifies the coordinates, in logical units, of the first radial ending point.Count (4 bytes): An unsigned integer that specifies the total number of points. This value MUST be one more than three times the number of curves to be drawn because each Bezier curve requires two control points and an endpoint, and the initial curve requires an additional starting point Changed to:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Bounds (16 bytes): A RectL object ([MS-WMF] section 2.2.2.19), which specifies the inclusive-inclusive bounding rectangle in logical units. Count (4 bytes): An unsigned integer that specifies the total number of points. This value MUST be one more than three times the number of curves to be drawn because each Bezier curve requires two control points and an endpoint, and the initial curve requires an additional starting point

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

March 4, 2020 - Download

Errata below are for Protocol Document Version V17.0 – 2020/03/04.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2020/07/06</td><td>In Section 2.2.3.4, ColorCurveEffect Object, added midtone adjustment range to AdjustmentIntensity field.

Changed from:

Shadow adjustment range:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>-100 ≤ value < 0</td><td>As the value decreases, the dark areas of the image SHOULD appear darker.</td></tr>
<tr><td>0</td><td>A value of 0 specifies that the shadow MUST NOT change.</td></tr>
<tr><td>0 < value ≤ 100</td><td>As the value increases, the dark areas of the image SHOULD appear lighter.</td></tr>
</table>
Changed to:

Shadow adjustment range:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>-100 ≤ value < 0</td><td>As the value decreases, the dark areas of the image SHOULD appear darker.</td></tr>
<tr><td>0</td><td>A value of 0 specifies that the shadow MUST NOT change.</td></tr>
<tr><td>0 < value ≤ 100</td><td>As the value increases, the dark areas of the image SHOULD appear lighter.</td></tr>
</table>
Midtone adjustment range:</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

Errata Published*	Description

Value	Meaning
- 100 ≤ value < 0	As the value decreases, the midtones of the image SHOULD appear darker.
0	A value of 0 specifies that the midtone MUST NOT change.
0 < value ≤ 100	As the value increases, the midtones of the image SHOULD appear lighter.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-EMFSPOOL]: Enhanced Metafile Spool Format

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

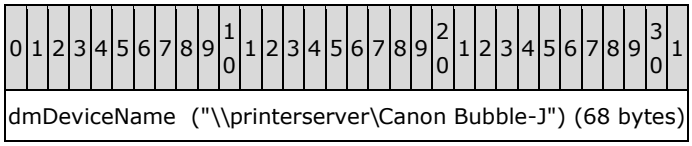
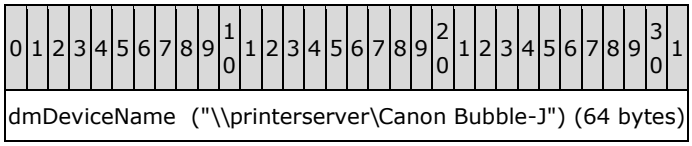
Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS
Atom

Errata below are for Protocol Document Version V10.0 – 2018/09/12

Errata Published*	Description
2021/02/22	In Section 3.2.1, EMFSPOOL Header Example, revised the hexadecimal dump and information about the alignment and values of the extraDataDocName and extraDataOutputDevice fields. Changed from: 00000050:00 00 00 Changed to: 00000050:00 00 00 00 Changed from: extraDataOutputDevice ("net02:") Changed to: extraDataOutputDevice ("Ne02:") Changed from: extraDataDocName: Variable-size storage area for document name, 4-byte aligned. extraDataOutputDevice: Variable-size storage area for output device (2) name, 4-byte aligned. Changed to: extraDataDocName: Variable-size storage area for document name. extraDataOutputDevice: Variable-size storage area for output device (2) name. Padding bytes will be added following this storage area to align the entire header record on a 4-byte boundary.
2021/02/22	In Section 3.2.4, EMRI_DEVMODE Example 1, revised the hex output and the length of the dmDeviceName field.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Changed from: 00064B00:00 00 00 00 00 00 00 00 00 00 00 00 Changed to: 00064B00:00 00 00 00 Changed from:  Changed to:  Changed from: dmDeviceName (68 bytes): "\\printerserver\Canon Bubble-J" is the text name of the printer. Changed to: dmDeviceName (64bytes): "\\printerserver\Canon Bubble-J" is the text name of the printer. In Section 3.2.4, EMRI_DEVMODE Example 1, revised the length of the dmFormName field: Changed from: dmYResolution (0xFFFD) | dmTTOption (0x0002) dmCollate (0x0001) | dmFormName ("Letter") (68 bytes) Changed to: dmYResolution (0xFFFD) | dmTTOption (0x0002) dmCollate (0x0001) | dmFormName ("Letter") (64 bytes)

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>Changed from:

dmFormName (68 bytes): "Letter" specifies the name of the printer form, padded with nulls to fit into a 32-character Unicode.

Changed to:

dmFormName (64 bytes): "Letter" specifies the name of the printer form, padded with nulls to fit into a 32-character Unicode.

In Section 3.2.4, EMRI_DEVMODE Example 1, revised the length of the dmDriverExtraData field:

Changed from:

<table><tr><td>reserved8 (0x00000000)</td></tr><tr><td>dmDriverExtraData (116 bytes)</td></tr></table>
Changed to:

<table><tr><td>reserved8 (0x00000000)</td></tr><tr><td>dmDriverExtraData (868 bytes)</td></tr></table>
Changed from:

dmDriverExtraData (116 bytes): Private, printer driver-specific data.

Changed to:

dmDriverExtraData (868 bytes): Private, printer driver-specific data.</td></tr>
</table>

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

Errata below are for Protocol Document Version V19.0 – 2018/09/12.

Errata Published*	Description
2021/01/25	In Section 2.2, Win32 Error Codes, added ERROR_PRINTER_NOT_SHAREABLE error code. Changed from: 0x00000BCB ERROR_PRINTER_DRIVER_DOWNLOAD_NEEDED The specified printer driver was not found on the system and needs to be downloaded. 0x00000F6E ERROR_IO_REISSUE_AS_CACHED Reissue the given operation as a cached I/O operation. Changed to: 0x00000BCB ERROR_PRINTER_DRIVER_DOWNLOAD_NEEDED The specified printer driver was not found on the system and needs to be downloaded. 0x00000BCE ERROR_PRINTER_NOT_SHAREABLEThe specified printer cannot be shared. 0x00000F6E ERROR_IO_REISSUE_AS_CACHED Reissue the given operation as a cached I/O operation.
2019/08/05	In the Section 1.1, Glossary, the entry for the term message identifier, which is at odds with the definition in Section 2.2, has been removed.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 V22.0 – 2018/09/12.

Errata Published*	Description
2019/09/02	In Section 2.2.6, Handles, the section name has been changed to reflect the name of the type it describes. Changed from: 2.2.6 Handles Changed to: 2.2.6 IELF_HANDLE In Section 3.1.4.7, ElfrReadELW (Opnum 10), the name of the EVENTLOG_BACKWARDS_READ flag contained a misspelling in one place. Changed from: … If neither of the two flags are set, the server will treat it as if the EVENTLOG_BACKWORDS_READ flag is set. ... Changed to: … If neither of the two flags are set, the server will treat it as if the EVENTLOG_BACKWARDS_READ flag is set. ...

Copyright © 2020 Microsoft Corporation

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-EVEN6]: EventLog Remoting Protocol Version 6.0

This topic lists the Errata found in the MS-EVEN6 document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

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

RSS
Atom

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:

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[MS-FASP]: Firewall and Advanced Security Protocol

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

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

RSS
Atom

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

March 13, 2019 - Download

Copyright © 2020 Microsoft Corporation

[MS-FAX]: Fax Server and Client Remote Protocol

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

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

RSS
Atom

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:

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 V28.0 – 2018/09/12.

Errata Published*	Description
2019/02/19	In Section 1.2.1, Normative References, the following reference has been added: [MS-XCA] Microsoft Corporation, "Xpress Compression Algorithm". In Section 2.2.1.4.15, XPRESS Block, the Block Data field has been changed from: If the value of the Block Compressed Size field is less than the value of the Block Uncompressed Size field, then the data has been compressed. For more information about decompressing compressed data, see section 3.1.1.1.3.9. Changed to: If the value of the Block Compressed Size field is less than the value of the Block Uncompressed Size field, then the data has been compressed. For more information about decompressing compressed data, see section 3.1.1.2. In Section 3.1.1.1, Compression, the following was changed from: Many of the FrsTransport methods use compression to reduce the amount of data that is returned to the client. This section describes algorithms and a conceptual model of possible data organization that an implementation maintains in order to decompress compressed data. The described organization is provided to facilitate the explanation of how the algorithm behaves. Error checking and handling has been omitted from all algorithms in the interests of clarity. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with what is described in this document. Changed to: Many of the FrsTransport methods use the LZ77+Huffman Compression algorithm, specified in [MS-XCA] section 2.1, to compress data. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with what is described in this document.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	The following sections have been removed and replaced with links to MS-XCA: 3.1.1.1.1 Pseudocode Conventions 3.1.1.1.2 Data Structures 3.1.1.1.2.1 PREFIX_CODE_NODE 3.1.1.1.2.2 PREFIX_CODE_SYMBOL 3.1.1.1.2.3 BITSTRING 3.1.1.1.3 Procedures 3.1.1.1.3.1 PrefixCodeTreeRebuild 3.1.1.1.3.2 PrefixCodeTreeAddLeaf 3.1.1.1.3.3 SortSymbols 3.1.1.1.3.4 CompareSymbols 3.1.1.1.3.5 BitstringInit 3.1.1.1.3.6 BitstringLookup 3.1.1.1.3.7 BitstreamSkip 3.1.1.1.3.8 PrefixCodeTreeDecodeSymbol A new section, 3.1.1.2, Decompression, has been added: FrsTransport methods that compress data will always return information specifying the size of the original data. It is the caller's responsibility to determine whether the returned data is compressed. If the size of the compressed data buffer that is returned by the server in bytes is equal to the size in bytes of the original uncompressed data, then the buffer returned by the server contains uncompressed data. In Section 3.2.4.1.7, RequestRecords (Opnum 6), the description of the compressedRecords field has been changed from: compressedRecords: The data records, compressed using the DFS-R compression algorithm specified in section 3.1.1.1. The compressedRecords bytes correspond to an array of FRS_ID_GVSN entries. DFS-R uses custom marshaling in this RPC call to compress the set of transmitted records. The size of the FRS_ID_GVSN array is given by the numRecords parameter. The decompression algorithm specified in section 3.1.1.1.3.9 can be used to decompress the received data into a buffer of sizeof(FRS_ID_GVSN)*numRecords bytes, which can be re-interpreted as an array of FRS_ID_GVSN entries. Changed to: compressedRecords: The data records, compressed using the algorithm specified in section 3.1.1.1. The compressedRecords bytes correspond to an array of FRS_ID_GVSN entries. DFS-R uses custom marshaling in this RPC call to compress the set of transmitted records. The size of the FRS_ID_GVSN array is given by the numRecords parameter. The decompression algorithm specified in section 3.1.1.1 can be used to decompress the received data into a buffer of sizeof(FRS_ID_GVSN)*numRecords bytes, which can be re-interpreted as an array of FRS_ID_GVSN entries. In Section 3.2.4.1.14, InitializeFileTransferAsync (Opnum 13), changed from: 2. An encapsulation of the marshaled file data stream using the compressed data format (as specified in section 3.2.4.1.14.2) generated by the DFS-R compression

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	algorithm specified in section 3.1.1.1. Even if the marshaled file data stream is not compressed by the server, it is still encapsulated using the compressed data format. Changed to: 2. An encapsulation of the marshaled file data stream using the compressed data format (as specified in section 3.2.4.1.14.2) generated by the compression algorithm specified in section 3.1.1.1. Even if the marshaled file data stream is not compressed by the server, it is still encapsulated using the compressed data format.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

June 24, 2019 – Download

March 4, 2020 - Download

August 24, 2020 – Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

September 23, 2019 - Download

March 4, 2020 - Download

August 24, 2020 – Download

Errata below are for Protocol Document Version V48.0 - 2020/08/26

Errata Published*	Description
2021/01/25	In Section 2.3 FSCTL Structures, the value for FSCTL_MARK_HANDLE was added to the table. Changed from: FSCTL_LMR_SET_LINK_TRACKING_INFORMATION 0X1400EC FSCTL_OFFLOAD_READ 0X94264 Changed to: FSCTL_LMR_SET_LINK_TRACKING_INFORMATION 0X1400EC FSCTL_MARK_HANDLE 0x900fc FSCTL_OFFLOAD_READ 0X94264
2021/01/11	In the following section updated the processing rules for when the directory is the volume root. Section 2.4.8 FileBothDirectoryInformation Section 2.4.10 FileDirectoryInformation Section 2.4.14 FileFullDirectoryInformation Section 2.4.17 FileIdBothDirectoryInformation

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Section 2.4.18 FileIdFullDirectoryInformation Section 2.4.19 FileIdGlobalTxDirectoryInformation Section 2.4.26 FileNamesInformation For more details, please see the diff file.
2020/11/23	In Section 2.6 File Attributes, the following attributes have been added. Changed to: Value Meaning FILE_ATTRIBUTE_RECALL_ON_OPEN 0x00040000 This attribute appears only in directory enumeration classes (FILE_DIRECTORY_INFORMATION, FILE_BOTH_DIR_INFORMATION, etc.). When this attribute is set, it means that the file or directory has no physical representation on the local system; the item is virtual. Opening the item will be more expensive than usual because it will cause at least some of the file or directory content to be fetched from a remote store. This attribute can only be set by kernel-mode components. This attribute is for use with hierarchical storage management software.<162> FILE_ATTRIBUTE_PINNED 0x00080000 This attribute indicates user intent that the file or directory should be kept fully present locally even when not being actively accessed. This attribute is for use with hierarchical storage management software.<163> FILE_ATTRIBUTE_UNPINNED 0x00100000 This attribute indicates that the file or directory should not be kept fully present locally except when being actively accessed. This attribute is for use with hierarchical storage management software.<164> FILE_ATTRIBUTE_RECALL_ON_DATA_ACCESS 0x00400000 When this attribute is set, it means that the file or directory is not fully present locally. For a file this means that not all of its data is on local storage (for example, it may be sparse with some data still in remote storage). For a directory it means that some of the directory contents are being virtualized from another location. Reading the file or enumerating the directory will be more expensive than usual because it will cause at least some of the file or directory content to be fetched from a remote store. Only kernel-mode callers can set this attribute. This attribute is for use with hierarchical storage management software.<165> <162> Section 2.6: Only NTFS and ReFS support this attribute. <163> Section 2.6: Only NTFS and ReFS support this attribute. <164> Section 2.6: Only NTFS and ReFS support this attribute.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	<165> Section 2.6: Only NTFS and ReFS support this attribute.
2020/11/23	In Section 2.4.34 FileRenameInformation, the description of STATUS_INVALID_PARAMETER and STATUS_ACCESS_DENIED have been updated. Changed from: STATUS_INVALID_PARAMETER: An invalid parameter was passed for FileName or FileNameLength, or the target file was open, or the RootDirectory field value was nonzero for a network operation. STATUS_ACCESS_DENIED: The handle was not opened with delete access. Changed to: STATUS_INVALID_PARAMETER: An invalid parameter was passed for FileName or FileNameLength, or the RootDirectory field value was nonzero for a network operation. STATUS_ACCESS_DENIED: The handle was not opened with delete access, or the target file was open and ReplaceIfExists is nonzero.
2020/08/31	In MS-FSCC Section 2.4.34.2 FileRenameInformation for SMB2, the Padding field was added to the end of the packet: Changed from: FileName (variable): A sequence of Unicode characters containing the new name of the file. When working with this field, use FileNameLength to determine the length of the file name rather than assuming the presence of a trailing null delimiter. Changed to: FileName (variable): A sequence of Unicode characters containing the new name of the file. When working with this field, use FileNameLength to determine the length of the file name rather than assuming the presence of a trailing null delimiter. Padding (variable): Length of this field MUST be the number of bytes required to make the size of this structure at least 24. This field MAY be set to 0 and MUST be ignored on receipt.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Errata below are for Protocol Document Version V36.1 – 2019/03/15.

Errata Published*	Description
2019/05/27	In Section 2.2.4, GPO Search, changed from: The gpt.ini file MUST be encoded in UTF-8 and is described with the following Augmented Backus-Naur Form (ABNF), as specified in [RFC4234]. Changed to: The gpt.ini file MUST be encoded in ANSI and is described with the following Augmented Backus-Naur Form (ABNF), as specified in [RFC4234].

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-GPWL]: Group Policy: Wireless/Wired Protocol Extension

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

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

RSS
Atom

Errata below are for Protocol Document Version V27.0 – 2020/03/04.

Errata Published*	Description
2020/06/22	In Section 2.2.1.2.1, Message Syntax for XML-Based Wireless Profiles, added values and enumerations to phyType. Changed from: autoSwitch: If the connection to a more preferred network is attempted when already connected to a network. A more preferred network is one that is ordered higher in a list of preferred wireless networks. phyType: The IEEE 802.11 physical type that a domain client uses while connected to this wireless network. authentication: The type of 802.11 authentication the domain clients uses for connecting to the WLAN. This value MUST be one of the following: … Changed to: autoSwitch: If the connection to a more preferred network is attempted when already connected to a network. A more preferred network is one that is ordered higher in a list of preferred wireless networks. phyType: The IEEE 802.11 physical type that a domain client uses while connected to this wireless network. This value MUST be one of the following: ▪ a: refers to LAN protocol IEEE 802.11a-1999 ▪ b: refers to LAN protocol IEEE 802.11b-1999 ▪ g: refers to LAN protocol IEEE 802.11g-2003 ▪ n: refers to LAN protocol IEEE 802.11n-2009 ▪ ac: refers to LAN protocol IEEE 802.11ac-2013 ▪ ax: refers to LAN protocol IEEE 802.11ax authentication: The type of 802.11 authentication the domain clients uses for connecting to the WLAN. This value MUST be one of the following:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description

	…
	
	In Section 6.3.1, Wireless LAN Profile v1 Schema, added values to phyType.
	
	Changed from:
	
	`<xs:element name="phyType" minOccurs="0" maxOccurs="4">`
	`<xs:simpleType>`
	`<xs:restriction base="xs:string">`
	`<xs:enumeration value="a" />`
	`<xs:enumeration value="b" />`
	`<xs:enumeration value="g" />`
	`<!-- this value is reserved for future use -->`
	`<xs:enumeration value="n" />`
	`<xs:enumeration value="ac" />`
	`</xs:restriction>`
	`</xs:simpleType>`
	`</xs:element>`
	
	Changed to:
	
	`<xs:element name="phyType" minOccurs="0" maxOccurs="6">`
	`<xs:simpleType>`
	`<xs:restriction base="xs:string">`
	`<xs:enumeration value="a" />`
	`\<xs:enumeration value="b" />`
	`\<xs:enumeration value="g" />`
	`<xs:enumeration value="n" />`
	`<xs:enumeration value="ac" />`
	`<xs:enumeration value="ax" />`
	`</xs:restriction>`
	`</xs:simpleType>`

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	</xs:element>

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[MS-HGSA]: Host Guardian Service: Attestation Protocol

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

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

RSS
Atom

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 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

June 24, 2019 – Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 20, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 15, 2017 - Download

Errata below are for Protocol Document Version V27.0 – 2018/09/12.

Errata Published*	Description
2019/10/28	In Section 2.2.8, Configuration Attribute (IKEv2) Packet, changed from: Length (2 bytes): The length of the data in the value field. Changed to: Length (2 bytes): The length of the data in the Value field. In Section 2.2.11.2, Encrypted Fragment Payload, changed from: Next_Payload (1 byte): In the very first fragment (with Fragment Number equal to 1), this field MUST be set to the payload type of the first inner payload. In the remainder of the Fragment messages (with Fragment Number greater than 1), this field MUST be set to zero. Changed to: Next_Payload (1 byte): In the very first fragment (with Fragment_Number equal to 1), this field MUST be set to the payload type of the first inner payload. In the remainder of the Fragment messages (with Fragment_Number greater than 1), this field MUST be set to zero. In Section 3.3.1, Abstract Data Model, references have been added o disambiguate which fields in section 2.2.3.1 set the values of the ADM elements: Fragment ID, Fragment Number, Flag, and Fragment Data. Changed from: Fragment queue: A queue holding the fragments that correspond to incomplete IKE messages, indexed by the Fragment ID. Each entry in the queue MUST contain: -- The Fragment ID -- The Fragment Number -- A Flag that indicates whether this fragment is the last one (that is, the LAST_FRAGMENT bit is set in the Fragment payload).

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	-- The Fragment Data For definitions of the previous values, see section 2.2.3.1. Flow state table: The following information MUST be maintained. Changed to: Fragment queue: A queue holding the fragments that correspond to incomplete IKE messages, indexed by the Fragment ID. Each entry in the queue MUST contain: -- The Fragment ID, which is set to the Fragment_ID field in section 2.2.3.1. -- The Fragment Number, which is set to the Fragment_Number field in section 2.2.3.1. -- A Flag that is set to the Flags field in section 2.2.3.1 to indicates whether this fragment is the last one (that is, the LAST_FRAGMENT bit is set in the Fragment payload). -- The Fragment Data, which is set to the Fragment_Data field in section 2.2.3.1. Flow state table: The following information MUST be maintained. In Section 3.3.2, Timers, the second bullet point has been changed from: When the fragmentation reassembly timer fires, the delay MUST NOT exceed 90 seconds.<17> Changed to: When the fragment reassembly timer fires, the delay MUST NOT exceed 90 seconds.<17> In Section 3.3.5.3, Receiving Other IKE Messages, the action taken by the Receiver upon receipt of an IKE message (to discard such a message when a Fragment payload is present and it is not the only payload in the message) has been clarified. Changed from: On receipt of an IKE message, the host MUST check if the message contains a Fragment payload. If a Fragment payload is present, this payload MUST be the only payload in the message. If not, the host MUST silently discard the message. Changed to: On receipt of an IKE message, the host MUST check if the message contains a Fragment payload. If a Fragment payload is present, and the payload is not the only payload in the message, the host MUST silently discard the message' In Section 3.3.5.3, Receiving Other IKE Messages, text has been changed to clarify from where to retrieve the Fragment ID. Changed from: Retrieve the Fragment ID from the Fragment payload.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Changed to: Retrieve the Fragment ID from the Fragment_ID field in the Fragment payload. In Section 3.3.5.3, Receiving Other IKE Messages, text has been changed to clarify how fragments not of the same Fragment Number are added to the Fragment queue in the corresponding entry of the MMSAD. Changed from: If the queue for this Fragment ID already contains a fragment with the same Fragment Number, the host MUST silently discard the message. If not, the host MUST queue the Fragment payload's fields in the corresponding entry of the MMSAD, indexed by the Fragment Id Changed to: If the queue for this Fragment ID already contains a fragment with the same Fragment Number, the host MUST silently discard the message. If not, the host MUST add an entry to the Fragment queue in the corresponding entry of the MMSAD, with the queue entry fields initialized based on the associated fields of the Fragment payload. In Section 3.3.5.3, Receiving Other IKE Messages, changed from: The host MUST then check whether all Fragment payloads for this Fragment ID have been received (that is, whether Fragment payloads that have a Fragment number from 1 to n.. Changed to: The host MUST then check whether all Fragment payloads for this Fragment ID have been received (that is, whether Fragment payloads that have a Fragment Number from 1 to n.. In Section 3.3.5.3, Receiving Other IKE Messages, text has been changed to clarify the error condition where the host MUST discard all Fragment payloads for a specific Fragment ID. Changed from: A Fragment payload has been received with a Fragment number greater than the Fragment number of the fragment with the Flags field set to LAST_FRAGMENT.' Changed to: A Fragment payload has been received with a Fragment Number greater than the Fragment Number of an entry in the Fragment queue with the Flags field set to LAST_FRAGMENT. In Section 3.3.5.3, Receiving Other IKE Messages, changed from: Fragment payloads (without the Fragment payload header) in the order of their Fragment number. Changed to:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Fragment payloads (without the Fragment payload header) in the order of their Fragment Number. In Section 3.15.1, Abstract Data Model, references have been added to disambiguate which fields in section 2.2.3.1 set the values of the ADM elements: Fragment ID, Fragment Number, and Fragment Data. Changed from: Fragment queue: A queue holding the fragments that correspond to incomplete IKE messages, indexed by the Fragment ID. Each entry in the queue MUST contain the following: Fragment ID, which is the Message ID Fragment Number Total Fragments Fragment Data Flow state table: The following information MUST be maintained. Changed to: Fragment queue: A queue holding the fragments that correspond to incomplete IKE messages, indexed by the Fragment ID. Each entry in the queue MUST contain the following: Fragment ID, which is the Message ID, is set to the Fragment_ID field in section 2.2.3.1. Fragment Number, which is set to the Fragment_Number field in section 2.2.3.1. Total Fragments Fragment Data, which is set to the Fragment_Data field in section 2.2.3.1. Flow state table: The following information MUST be maintained.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[MS-IPHTTPS]: IP over HTTPS (IP-HTTPS) Tunneling Protocol

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

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

RSS
Atom

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:

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

March 4, 2020 - Download

August 24, 2020 – Download

Errata below are for Protocol Document Version V36.0 - 2020/08/26

Errata Published*	Description
2021/01/11	In Section 3.2.5.3 Locate a DS_BEHAVIOR_WIN2012 DC, added reference to DS_BEHAVIOR_WIN2012 definition. Changed from: When a DS_BEHAVIOR_WIN2012 Domain Controller (DC) is required, DsrGetDcNameEx2 method ([MS-NRPC] section 3.5.4.3.1) is called where: Changed to: When a DS_BEHAVIOR_WIN2012 ([MS-ADTS] section 3.1.1.3.2.25) Domain Controller (DC) is required, DsrGetDcNameEx2 method ([MS-NRPC] section 3.5.4.3.1) is called where: In Section 3.4.5.6 GSS_GetMICEx() Call, added RFC reference for the GSS_GetMIC call. Changed from: This call is identical to GSS_GetMIC, except that it supports multiple input buffers. Changed to: This call is identical to GSS_GetMIC ([RFC2743] section 2.3.1), except that it supports multiple input buffers. In Section 3.4.5.7 GSS_VerifyMICEx() Call, added RFC reference for the GSS_VerifyMIC call. Changed from: This call is identical to GSS_VerifyMIC, except that it supports multiple input buffers. Changed to:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	This call is identical to GSS_VerifyMIC ([RFC2743] section 2.3.2), except that it supports multiple input buffers. In Section 3.3.1 Abstract Data Model, added reference to the POLICY_KERBEROS_VALIDATE_CLIENT definition. Changed from: AuthenticationOptions: A 32-bit unsigned integer containing the POLICY_KERBEROS_VALIDATE_CLIENT flag. Changed to: AuthenticationOptions: A 32-bit unsigned integer containing the POLICY_KERBEROS_VALIDATE_CLIENT flag ([MS-LSAD] section 2.2.4.19). In Section 3.3.5.6.3 Check Account Policy for Every TGT Request, added section reference for AuthenticationOptions for the POLICY_KERBEROS_VALIDATE_CLIENT bit. Changed from: If the POLICY_KERBEROS_VALIDATE_CLIENT bit is set in the AuthenticationOptions setting on the KDC, then KILE will enforce revocation on the KDCs and the KDC MUST verify that the account and return the following errors: Changed to: If the POLICY_KERBEROS_VALIDATE_CLIENT bit is set in the AuthenticationOptions setting (section 3.3.1) on the KDC, then KILE will enforce revocation on the KDCs and the KDC MUST verify that the account and return the following errors: In Section 3.3.5.7.1 Check Account Policy for Every Session Ticket Request, added section reference for AuthenticationOptions and the POLICY_KERBEROS_VALIDATE_CLIENT bit. Changed from: If the POLICY_KERBEROS_VALIDATE_CLIENT bit is set in the AuthenticationOptions setting on the KDC, … Changed to: If the POLICY_KERBEROS_VALIDATE_CLIENT bit is set in the AuthenticationOptions setting (section 3.3.1) on the KDC, …
2021/01/11	In Section 3.3.1.1 Account Database Extensions, Added illustrative KDC pseudo variable definitions with references. Changed from: ● AssignedSilo: A link to the silo. KILE implementations that use Active Directory for the account database use the msDS-AssignedAuthNPolicySilo attribute ([MS-ADA2] section 2.218). ● DelegationNotAllowed: A Boolean setting to prevent PROXIABLE or FORWARDABLE ticket flags ([RFC4120] sections 2.5 and 2.6) in tickets for the principal. KILE implementations that use Active Directory for the account database use the userAccountControl attribute ([MS-ADTS] section 2.2.16) ND flag. The default is FALSE. Changed to:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	• AssignedSilo: A link to the silo. KILE implementations that use Active Directory for the account database use the msDS-AssignedAuthNPolicySilo attribute ([MS-ADA2] section 2.218). • Illustrative KDC pseudo variables • BelongsToSilo: A KDC pseudo variable that is a Boolean variable used for illustrative purposes in the processing instructions of section 3.3.5.4 and section 3.3.5.5. The value of BelongsToSilo is not persisted across client requests. The KDC sets BelongsToSilo value based on processing rules in section 3.3.5.4 to determine an account's Authentication Policy Silo membership. If TRUE, then the account belongs to an AssignedSilo. If BelongsToSilo is FALSE, and AssignedPolicy is not NULL, the account belongs to an AssignedPolicy. • The KDC sets the following pseudo variables based on processing rules in section 3.3.5.5, for account types (<acctype>): User ([MS-ADSC] section 2.268), Service (ManagedServiceAccount [MS-ADSC] section 2.141), or Computer ([MS-ADSC] section 2.21): • PolicyName: A pseudo variable for the KDC's counterpart of the relative distinguished name (RDN) in msDS-<acctype>AuthNPolicy.RDN ([MS-ADA2] section 2.216). The KDC sets the value to one of the following: • AssignedSilo.msDS-<acctype>AuthNPolicy.RDN ([MS-ADSC] section 2.121), • AssignedPolicy.RDN ([MS-ADSC] section 2.120), or • NULL. • Enforced: A pseudo variable for a Boolean variable that is the KDC's counterpart of msDS-AuthNPolicyEnforced ([MS-ADA2] section 2.222). The KDC sets the value to either of the folowing: • AssignedSilo.msDS-AuthNPolicyEnforced ([MS-ADSC] section 2.121), or • FALSE. • TGTLifetime: A pseudo variable for the KDC's counterpart of msDS-<acctype>TGTLifetime ([MS-ADA2] section 2.489 User, section 2.456 Service, and section 2.289 Computer), used in msDS-AuthNPolicy ([MS-ADSC] section 2.120). The KDC sets the value to either of the following: • AssignedSilo.msDS-<acctype>AuthNPolicy.msDS-<acctype>TGTLifetime, or • AssignedPolicy.msDS-<acctype>AuthNPolicy.msDS-<acctype>TGTLifetime. • AllowedToAuthenticateTo: A pseudo variable for the KDC's counterpart of msDS-<acctype>AllowedToAuthenticateTo ([MS-ADA2] section 2.485), used in msDS-AuthNPolicy [MS-ADSC] section 2.120). The KDC sets the value to either of the following: • AssignedSilo.msDS-<acctype>AuthNPolicy.msDS-<acctype>AllowedToAuthenticateTo, or • AssignedPolicy.msDS-<acctype>AuthNPolicy.msDS-<acctype>AllowedToAuthenticateTo • AllowedToAuthenticateFrom: A pseudo variable for the KDC's counterpart of msDS-<User/Service>AuthNPolicy.msDS-<User/Service>AllowedToAuthenticateFrom ([MS-ADA2] section 2.484 User, and section 2.452 Service, used in [MS-ADSC] section 2.120). The KDC sets the value to one of the following: • AssignedSilo.msDS-<User/Service>AuthNPolicy.msDS-<User/Service>AllowedToAuthenticateFrom, • AssignedPolicy.msDS-<User/Service>UserAuthNPolicy.msDS-<User/Service>AllowedToAuthenticateFrom, or • NULL • DelegationNotAllowed: A Boolean setting to prevent PROXIABLE or FORWARDABLE ticket flags ([RFC4120] sections 2.5 and 2.6) in tickets for the principal. KILE implementations that use Active Directory for the account database use the userAccountControl attribute ([MS-ADTS]section 2.2.16) ND flag. The default is FALSE. In Section 3.3.5.4 Determining Authentication Policy Silo Membership, added section reference for KDC pseudo variable definitions.

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>Changed from:

If domainControllerFunctionality returns a value < 6 ([MS-ADTS] section 3.1.1.3.2.25), the KDC SHOULD set BelongsToSilo to FALSE.

Changed to:

If domainControllerFunctionality returns a value < 6 ([MS-ADTS] section 3.1.1.3.2.25), the KDC SHOULD set BelongsToSilo to FALSE. See section 3.3.1.1 for the following KDC pseudo variable definitions.

In Section 3.3.5.5 Determining Authentication Policy Settings, added section reference for KDC pseudo variable definitions.

Changed from:

If domainControllerFunctionality returns a value < 6 ([MS-ADTS] section 3.1.1.3.2.25), the KDC SHOULD set PolicyName to NULL.

Changed to:

If domainControllerFunctionality returns a value < 6 ([MS-ADTS] section 3.1.1.3.2.25), the KDC SHOULD set PolicyName to NULL. See section 3.3.1.1 for the following KDC pseudo variable definitions</td></tr>
<tr><td>2021/01/11</td><td>In section 2.2.2 KERB-ERROR-DATA, adjusted capitalization of Data-value to data-value as defined in the structure.

Changed from:

data-type: This value is as follows.
<table><tr><th>Integer Value</th><th>Meaning</th></tr><tr><td>. . .</td><td></td></tr><tr><td>3
KERB_ERR_TYPE_EXTENDED</td><td>The Data-value field contains extended, implementation-specific error information.</td></tr></table>
Changed to:

data-type: This value is as follows.
<table><tr><th>Integer Value</th><th>Meaning</th></tr><tr><td>. . .</td><td></td></tr><tr><td>3
KERB_ERR_TYPE_EXTENDED</td><td>The data-value field contains extended, implementation-specific error information.</td></tr></table></td></tr>
</table>

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	In section 3.3.5.6.4.1 KERB_VALIDATION_INFO Structure, adjusted capitalization of UserID to UserId to match structure. Changed from: ● The UserID field is set to the Buffer.SAMPR_USER_ALL_INFORMATION.UserId field ([MS-SAMR] section 2.2.7.1) of the SamrQueryInformationUser2 ([MS-SAMR] section 3.1.5.5.5) response message. Changed to: ● The UserId field is set to the Buffer.SAMPR_USER_ALL_INFORMATION.UserId field ([MS-SAMR] section 2.2.7.1) of the SamrQueryInformationUser2 ([MS-SAMR] section 3.1.5.5.5) response message. In Section 3.3.5.7.4 Compound Identity, Renamed UserID to UserId, DomainCount to DomainGroupCount, and added reference to DOMAIN_GROUP_MEMBERSHIP structure. Changed from: The KDC populates the following PAC_DEVICE_INFO structure ([MS-PAC] section 2.12) fields by using the following fields from the KERB_VALIDATION_INFO structure from the computer's TGT: ● UserID: from the UserID field ● . . . The non-account domain fields MUST be initialized as follows: ● . . . ● DomainCount field set to zero ● DomainGroup field is NULL . . . For the rest of the ExtraSids.Sid, DomainGroup is used: ● The DomainCount field contains the number of domains with DomainGroup populated. ● The DomainGroup field is populated for each domain where: Changed to: The KDC populates the following PAC_DEVICE_INFO structure ([MS-PAC] section 2.12) fields by using the following fields from the KERB_VALIDATION_INFO structure from the computer's TGT: ● UserId: from the UserId field ● . . . The non-account domain fields MUST be initialized as follows: ● . . . ● DomainGroupCount field set to zero ● DomainGroup field is NULL

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	. . . For the rest of the ExtraSids.Sid, DomainGroup is used: ● The DomainGroupCount field contains the number of domains with DomainGroup populated.The DomainGroup field is populated for each DOMAIN_GROUP_MEMBERSHIP structure ([MS-PAC] section 2.2.3) domain where:

2020/10/26	In Section 3.4.5.4.1 Kerberos Binding of GSS_WrapEx(), updated the H1 HMAC algorithm.
	
	Changed from:
	
	`where`
	
	`(C1, newIV) = E(Ke, conf | plaintext | pad, oldstate.ivec)`
	
	`H1 = HMAC(Ki, conf | plaintext+encrypted-data | pad)`
	
	Changed to:
	
	`where`
	
	`(C1, newIV) = E(Ke, conf | plaintext | pad, oldstate.ivec)`
	`H1 = HMAC(Ki, conf | plaintext | pad)`

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-KPP]: Key Provisioning Protocol

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

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

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[MS-KPS]: Key Protection Service Protocol

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

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

RSS
Atom

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 1, 2017 - Download

September 15, 2017 - Download

Copyright © 2020 Microsoft Corporation

[MS-LCID]: Windows Language Code Identifier (LCID) Reference

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

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

RSS
Atom

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:

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

March 13, 2019 - Download

Copyright © 2020 Microsoft Corporation

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

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

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

RSS
Atom

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

June 1, 2017 - Download

March 16, 2018 - Download

Errata below are for Protocol Document Version V43.0 – 2019/09/12.

Errata Published*	Description

2021/01/25	In Section 2.2.7.22 LSA_FOREST_TRUST_RECORD_TYPE, updated 'LSA_FOREST_TRUST_RECORD_TYPE' by adding enum element and value "ForestTrustRecordTypeLast = ForestTrustDomainInfo" to the type definition; also added description for 'ForestTrustRecordTypeLast' enum element to the definition list.
	
	Changed from:
	
	`typedef enum _LSA_FOREST_TRUST_RECORD_TYPE{`
	`ForestTrustTopLevelName = 0,`
	`ForestTrustTopLevelNameEx = 1,`
	`ForestTrustDomainInfo = 2`
	`} LSA_FOREST_TRUST_RECORD_TYPE;`
	
	....
	
	ForestTrustDomainInfo: This field specifies a record containing identification and name information.
	
	Changed to:
	
	`typedef enum _LSA_FOREST_TRUST_RECORD_TYPE{`
	`ForestTrustTopLevelName = 0,`
	`ForestTrustTopLevelNameEx = 1,`
	`ForestTrustDomainInfo = 2,`
	`ForestTrustRecordTypeLast = ForestTrustDomainInfo`
	`} LSA_FOREST_TRUST_RECORD_TYPE;`
	
	....

Copyright © 2020 Microsoft Corporation

Errata Published*	Description

	ForestTrustDomainInfo: This field specifies a record containing identification and name information.
	
	ForestTrustRecordTypeLast: The highest record value for this type is equal to the ForestTrustDomainInfo enum value (2)."
	
	In Section 6 Appendix A: Full IDL
	
	Changed from:
	
	`typedef enum _LSA_FOREST_TRUST_RECORD_TYPE {`
	`  ForestTrustTopLevelName = 0,`
	`  ForestTrustTopLevelNameEx = 1,`
	`  ForestTrustDomainInfo = 2`
	`} LSA_FOREST_TRUST_RECORD_TYPE;`
	
	Changed to:
	
	`typedef enum _LSA_FOREST_TRUST_RECORD_TYPE {`
	`  ForestTrustTopLevelName = 0,`
	`  ForestTrustTopLevelNameEx = 1,`
	`  ForestTrustDomainInfo = 2,`
	`  ForestTrustRecordTypeLast = ForestTrustDomainInfo`
	`} LSA_FOREST_TRUST_RECORD_TYPE;`

2019/10/16	In Section 2.2.4.4, LSAPR_POLICY_AUDIT_EVENTS_INFO: Changed from: MaximumAuditingEventCount Changed to: MaximumAuditEventCount

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

July 18, 2016 - Download

June 1, 2017 - Download

June 1, 2017 - Download

September 15, 2017 - Download

Errata below are for Protocol Document Version V30.0 - 2018/09/12

Errata Published*	Description
2020/09/28	In Section 3.1.1.1.2 Configurable Translation Database and Corresponding View, clarified the process to map the Security Principal SID from the ServiceName rather than the DisplayName. Changed from: The mapping rules are defined as follows: • Domain DNS Name, Additional Security Principal Name, User Principal Name, Default User Principal Names, and Security Principal SID History columns are left empty. • Security Principal SID is mapped from DisplayName in [MS-SCMR] section 3.1.1 using the following method: • Convert the DisplayName field to the uppercase, UTF-16 representation. • Take the SHA1 hash of the name: • Hash[0] denoting the first 4 bytes of the resulting hash as an unsigned integer. • Hash[1] denoting the second 4 bytes of the resulting hash as an unsigned integer. • And so on. • Create the SID using the following mapping: • S-1-5-80-hash[0]-hash[1]-hash[2]-hash[3]-hash[4] • Security Principal Name is mapped from DisplayName in [MS-SCMR] section 3.1.1. • Security Principal Type is mapped to SidTypeWellKnownGroup. Changed to: The mapping rules are defined as follows: • For all these entries:Domain DNS Name, Additional Security Principal Name, User Principal Name, Default User Principal Names, and Security Principal SID; the History columns are left empty.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	• For the "NT SERVICE" domain entry, the mapping rules are defined as follows: • Security Principal Name is "NT SERVICE" • Service Principal SID is S-1-5-80 • Security Principal Type is SidTypeDomain • For each service definition entry, the mapping rules are defined as follows: • Security Principal Name is mapped from the ServiceName in [MS-SCMR] section 3.1.1. • Security Principal SID is mapped from the ServiceName in [MS-SCMR] section 3.1.1 using the following method: • Convert the ServiceName field to the uppercase, UTF-16 representation. • Take the SHA1 hash of the name: • Hash[0] denoting the first 4 bytes of the resulting hash as an unsigned integer. • Hash[1] denoting the second 4 bytes of the resulting hash as an unsigned integer. • And so on. • Create the SID using the following mapping: • S-1-5-80-hash[0]-hash[1]-hash[2]-hash[3]-hash[4] • Security Principal Type is mapped to SidTypeWellKnownGroup.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

September 15, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

Errata below are for Protocol Document Version V9.0 - 2019/03/13

Errata Published*	Description
2020/09/28	In Section 2.2.9.1, XML Provisioning Schema, the first example of XML code has been augmented with a second example showing the device context as well as the user context illustrated in the first example, and the surrounding language changed to reflect the two examples. See the attached diff pdf file for details. Changed from: The following schema is an example of the XML required for the provisioning document. The explanation for each field in the document appears inline in the example as XML comments. ... Changed to: The following schemas are examples of the XML required for the provisioning document. The explanation for each field in the document appears inline in the example as XML comments. The following XML is a provisioning example for Mobile Device Management (MDM) in user context. ... The following XML is a provisioning example for Mobile Device Management (MDM) in device context. ...

Copyright © 2020 Microsoft Corporation

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

December 1, 2017 - Download

Errata below are for Protocol Document Version V10.0 - 2020/08/26

Errata Published*	Description

2020/10/12	In Section 2.1, Transport, details were added about support for an additional encoding type beyond the default type.
	
	Changed from:
	
	MDM, both as defined in this document and the OMA-DM protocol [OMA-DMP1.2.1], uses HTTP (as specified in [RFC2616]) as the transport layer. HTTP operations are performed on resources identified by a URI. MDM extends the resource addressing rules used by HTTP for URI formatting as specified in section 2.2.3.
	
	Changed to:
	
	MDM, both as defined in this document and the OMA-DM protocol [OMA-DMP1.2.1], uses HTTP (as specified in [RFC2616]) as the transport layer. MDM, in compliance with [OMA-SyncML-HTTPBnd], supports both “application/vnd.syncml.dm+xml” (default) and “application/vnd.syncml.dm+wbxml” encoding types. The server can be configured with the DMAcc Configuration Service Provider’s Microsoft/DefaultEncoding, as described in [DMC-DMAcc-CSP]. HTTP operations are performed on resources identified by a URI. MDM extends the resource addressing rules used by HTTP for URI formatting as specified in section 2.2.3.
	
	In Section 4, Examples, an unneeded XML header line in the middle of the example was deleted.
	
	Changed from:
	
	// The server responds with the required Status command for the SyncHdr and
	// Status commands for the requested Alert and Replace commands. The server
	// requests more information from the client with a series of Get commands
	.
	<?xml version="1.0" encoding="utf-8" ?>

Copyright © 2020 Microsoft Corporation

Errata Published*	Description

	<SyncML xmlns="SYNCML:SYNCML1.2">
	
	Changed to:
	
	// The server responds with the required Status command for the SyncHdr and
	// Status commands for the requested Alert and Replace commands. The server
	// requests more information from the client with a series of Get commands
	<SyncML xmlns="SYNCML:SYNCML1.2">

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-MICE]: Miracast over infrastructure Connection Establishment Protocol

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

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

RSS
Atom

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:

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[MS-MSSOD]: Media Streaming Server Protocols Overview

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

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

RSS
Atom

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

December 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 following ERRATA archive:

June 30, 2015 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[MS-NCNBI]: Network Controller Northbound Interface Specification

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

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

RSS
Atom

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

March 16, 2018 - Download

September 12, 2018 - Download

Errata below are for Protocol Document Version V6.0 – 2018/09/12.

Errata Published*	Description
2018/12/17	In several sections throughout this document, missing element Type designations have been added to existing element or header tables. For example, in Section 2.2.1.2, Request Headers, the text in **bold** has been added to the existing table as shown below.

Header	Section	Type	Description
Content-Type	2.2.1.1	**Required or Optional Required for PUT, must be "application/json; charset=UTF-8". Optional for GET or Delete**	The content type of the payload.

In the following sections, the added Type designations are shown in **bold**.

2.2.2, Common JSON Elements

resourceId	**Optional or Required When optional for ancestor resource, then required for descendant resource. See section 2.2.3.**
resourceRef	**Read-only Optional or Required See section 1.3.3.2.**
properties.etag	**Read-only**

Copyright © 2020 Microsoft Corporation

Errata Published*	Description

properties.provisioningState	**Read-only**

3.1.5.1 accessControlLists

configurationState.id	**Optional Read-only**
virtualNetworkInterfaceErrors	**Optional Read-only**

3.1.5.5.3 frontendIPConfigurations

configurationState.vipEndpointStates	**Read-only**
configurationState.vipEndpointStates.vipEndpoint	**Read-only**
configurationState.vipEndpointStates.dipEndpointStates	**Read-only**
configurationState.vipEndpointStates.dipEndpointStates.dipEndpoint	**Read-only**
configurationState.vipEndpointStates.dipEndpointStates.hostIPAddress	**Read-only**
configurationState.vipEndpointStates.dipEndpointStates.hostId	**Read-only**
configurationState.vipEndpointStates.dipEndpointStates.AdapterId	**Read-only**
configurationState.vipEndpointStates.dipEndpointStates.ProbeRule	**Read-only**

3.1.5.11 networkInterfaces

dnsSettings	**Optional**
dnsSettings.dnsServers	**Optional**
ipConfigurations	**Read-only**
isHostVirtualNetworkInterface	**Optional FALSE is default. Cannot be changed after creation.**
internalDnsNameLabel	**Optional**
isPrimary	**Optional TRUE is default.**
isMultitenantStack	**Optional**
privateMacAddress	**Optional**
privateMacAllocationMethod	**Required**
serviceInsertionElements	**Optional Read-only**

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	3.1.5.14 publicIPAddresses dnsSettings — **Optional** 3.1.5.15 servers connections — **Required** connections.credential — **Required** connections.credentialType — **Required** connections.managementAddresses — **Required** certificate — **Optional or Required Required only if the certificate used by the server is self-signed.** 3.1.5.18 virtualNetworks configurationState.id — **Optional Read-only** configurationState.hostErrors — **Optional Read-only** 3.1.5.18.3 virtualNetworkPeerings remoteVirtualNetwork — **Required** 3.1.5.21 virtualServers connections.credential — **Optional** connections.credentialType — **Optional** connections.managementAddresses — **Optional** In Section 3.1.5.26, changed from:

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>HTTP method</td><td>Description</td></tr>
<tr><td>PUT</td><td>Create a new virtualNetworkManager resource or update an existing VirtualGateways resource.</td></tr>
<tr><td>GET</td><td>Get one virtualNetworkManager resource</td></tr>
</table>

Changed to:
<table>
<tr><td>HTTP method</td><td>Description</td></tr>
<tr><td>PUT</td><td>Update the virtualNetworkManager singleton resource.</td></tr>
<tr><td>GET</td><td>Get the virtualNetworkManager resource.</td></tr>
</table>
</td></tr>
</table>

* Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

December 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

September 23, 2019 - Download

September 29, 2020 – Download

Copyright © 2020 Microsoft Corporation

[MS-NMFMB]: .NET Message Framing MSMQ Binding Protocol

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

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

RSS
Atom

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:

December 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Errata below are for Protocol Document Version V7.0 – 2017/12/01.

Errata Published*	Description
2019/02/19	In Section 2.2.2, Data Message, the maximum size of the PayloadSize field has been changed from '0x0000FC00' to '0x0000FC30', to accommodate for both the application data size and the size increase that occurs when this protocol signs or encrypts the data to be transferred. Changed from: PayloadSize (4 bytes): The unsigned size, in bytes, of the Payload field. The maximum value for this field is 0x0000FC00 (that is, 63K, or 64,512). Changed to: PayloadSize (4 bytes): The unsigned size, in bytes, of the Payload field. The maximum value for this field is 0x0000FC30 (64,560).

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-NRBF]: .NET Remoting: Binary Format Data Structure

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

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

RSS
Atom

Errata below are for Protocol Document Version V12.0 – 2019/03/13.

Errata Published*	Description
2019/10/28	In Section 3.0, Structure Examples, in the logical Request message for dotNET_Framework 1.1, changed the BinaryMethodCall value from: BinaryMethodCall: RecordTypeEnum: BinaryMethodCall (0x21) MessageEnum: 00000014 Changed to: BinaryMethodCall: RecordTypeEnum: BinaryMethodCall (0x15) MessageEnum: 00000014

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 23, 2019 - Download

August 24, 2020 – Download

Errata below are for Protocol Document Version V37.0 - 2020/08/26

Errata Published*	Description
2021/01/11	The following sections were adjusted for element capitalization, added structure reference, clarified pseudocode, 8-bit CFB mode, product note 84 the visible SEC_E_OUT_OF_SEQUENCE return value, query spelling, and XOR'ing session key bytes. 2.2.1.6.2 DS_DOMAIN_TRUSTSW 3.1.1 Abstract Data Model 3.1.4.3.2 Strong-key Session-Key 3.1.4.5 Netlogon Authenticator Computation and Verification 3.3.4.2.1 Generating a Client Netlogon Signature Token 3.3.4.2.2 Receiving a Client Netlogon Signature Token 3.4.6.1 Timer Expiry on domainControllerCacheTimer 3.5.1 Abstract Data Model 3.5.4.3.1 DsrGetDcNameEx2 (Opnum 34) 3.5.4.9.1 NetrLogonControl2Ex (Opnum 18) 4.1 NetrLogonSamLogon with Secure Channel For more details, please see the diff file.
2020/10/26	In Section 3.1.4.6 Calling Methods Requiring Session-Key Establishment, added a reference to product note 74 and clarified product notes 74 and 76. Changed from: <74> Section 3.1.4.6: Whenever a Windows 7 client or later creates a secure channel with a Windows Server 2008 server or later, the server will enforce that clients are using RPC Integrity and Confidentiality to secure the connection. <76> Section 3.1.4.6: Windows NT, Windows 2000, Windows Server 2003, and Windows Server 2008 allow the call to succeed.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Changed to: 1.2.2 Informative References . . . [MSFT-CVE-2020-1472] Microsoft Corporation, "CVE-2020-1472 | Netlogon Elevation of Privilege Vulnerability", 08/11/2020, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472 . . . <74> Section 3.1.4.6: Windows XP and later clients will request secure RPC. Windows Server 2008 R2 operating system and later will enforce that clients are using RPC Integrity and Confidentiality to secure the connection. For more information, see [MSFT-CVE-2020-1472]. <76> Section 3.1.4.6: Windows NT, Windows 2000, Windows Server 2003, and Windows Server 2008 MS-NRPC servers do not support enforcing that clients are using RPC Integrity and Confidentiality to secure the connection.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-NSPI]: Name Service Provider Interface (NSPI) Protocol

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

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

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[MS-OCSPA]: Microsoft OCSP Administration Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V11.0 – 2018/09/12.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2020/07/06</td><td>In Section 3.2.4.1.3 GetCAConfigInformation (Opnum 5), added 'ReminderDuration' and 'RefreshTimeout' properties along with associated processing rules to first and second tables in the indicated section, respectively.

Changed from:

<table>
<tr><th>Property name</th><th>Processing rule</th></tr>
<tr><td>SigningCertificate</td><td>The vt member of the VARIANT MUST be set to VT_ARRAY|VT_UI1, and the pArray member MUST reference a single dimension safearray. The number of elements of the safearray referenced by pArray MUST be equal to the length in bytes of the ASN.1 DER encoding of the signing certificate used by the responder to sign OCSP responses for this revocation configuration.</td></tr>
</table>

Changed to:

<table>
<tr><th>Property name</th><th>Processing rule</th></tr>
<tr><td>ReminderDuration</td><td>The vt member of the VARIANT MUST be set to VT_I4, and the lVal member MUST be a DWORD value denoting the percentage of the signing certificate’s lifetime, after which, if the signing certificate is not renewed, a warning event will be logged.</td></tr>
<tr><td>SigningCertificate</td><td>The vt member of the VARIANT MUST be set to VT_ARRAY|VT_UI1, and the pArray member MUST reference a single dimension safearray. The number of elements of the safearray referenced by pArray MUST be equal to the length in bytes of the ASN.1 DER encoding of the signing certificate used by the responder to sign OCSP responses for this revocation configuration.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
Changed from:
<table>
<tr><th>Property name</th><th>Processing rules</th></tr>
<tr><td>RevocationErrorCode</td><td>The vt member of the VARIANT MUST be set to VT_I4, and the lVal member MUST be the HRESULT DWORD value denoting the status of this revocation provider. A value of 0 means that the revocation provider can provide certificate revocation status for certificates issued by the certificate authority configured for the revocation configuration. See [MS-ERREF] for a list of the possible error codes.</td></tr>
</table>
Changed to:
<table>
<tr><th>Property name</th><th>Processing rules</th></tr>
<tr><td>RefreshTimeout</td><td>The vt member of the VARIANT MUST be set to VT_I4, and the lVal member MUST be the time-out value in milliseconds associated with refreshing the CRL information.</td></tr>
<tr><td>RevocationErrorCode</td><td>The vt member of the VARIANT MUST be set to VT_I4, and the lVal member MUST be the HRESULT DWORD value denoting the status of this revocation provider. A value of 0 means that the revocation provider can provide certificate revocation status for certificates issued by the certificate authority configured for the revocation configuration. See [MS-ERREF] for a list of the possible error codes.</td></tr>
</table>
</td></tr>
</table>

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-OIDCE]: OpenID Connect 1.0 Protocol Extensions

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

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

RSS
Atom

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 1, 2017 - Download

December 1, 2017 - Download

March 16, 2018 - Download

Copyright © 2020 Microsoft Corporation

[MS-OLEDS]: Object Linking and Embedding (OLE) Data Structures

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

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

RSS
Atom

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:

December 1, 2017 - Download

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[MS-OLEPS]: Object Linking and Embedding (OLE) Property Set Data Structures

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

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

RSS
Atom

Errata below are for Protocol Document Version V6.0 – 2019/03/15.

Errata Published*	Description
2020/12/07	In Section 3.2.2.1 "CONTENTS" Stream, the following values were updated in the Stream contents table. The value at 0x0BA was changed from: 33 Change to: 43 The value at 0x108 was changed from: 09 Change to: 0A The value at 0x1A0 was changed from: 49 Change to: 06 In Section 3.2.2.1.4 Dictionary, the following value was updated in the Stream contents table. The value at 0x01A was changed from: 33 Change to:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	43 In Section 3.2.2.1.4.1 Dictionary Entry 0, the following value was updated in the Stream contents table. The value at 0x006 was changed from: 33 Change to: 43
2020/12/07	In Section 3.1 SummaryInformation Property Set the Stream, contents table was updated for 0x0D4 Changed from: 10 Changed to: 0F In Section 3.1.2 PIDSI_TITLE, the description of the Size field has been updated. Changed from: Size (4 bytes at offset 212): 0x0000000F (decimal 15). Changed to: Size (4 bytes at offset 212): 0x0000001F (decimal 15). In Section 3.1.8 PIDSI_LASTAUTHOR, the description of the Property offset field has been updated. Changed from: Property offset: 0x00000030 + 0x000000A0 = 0x000000D0 (decimal 300) Changed to: Property offset: 0x00000030 + 0x000000FC = 0x0000012C (decimal 300) In Section 3.1.10 PIDSI_APPNAME, the description of Property identifier and Property offset have been updated.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Changed from: Property identifier: 0x00000010 Property offset: 0x00000030 + 0x0000011C = 0x000000D0 (decimal 332) Changed to: Property identifier: 0x00000012 Property offset: 0x00000030 + 0x000000A0 = 0x0000014C (decimal 332) In Section 3.1.11 PIDSI_EDITTIME, the description of Property identifier has been updated. Changed from: 0x00000011 Changed to: 0x0000000A

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

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

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

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

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[MS-PAC]: Privilege Attribute Certificate Data Structure

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

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

RSS
Atom

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:

November 23, 2020 - Download

Copyright © 2020 Microsoft Corporation

[MS-PAR]: Print System Asynchronous Remote Protocol

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

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

RSS
Atom

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

June 1, 2017 - Download

Errata below are for Protocol Document Version V15.0 – 2018/09/12.

Errata Published*	Description
2018/12/10	In Section 3.1.4.2.7, RpcAsyncInstallPrinterDriverFromPackage (Opnum 62), changed from: The print server SHOULD<10> perform the following additional validation steps: … • Validate that, if the printer driver specified by the client is a derived printer driver, either the class printer driver on which the derived printer driver depends is already installed on the print server, or a driver package containing the class printer driver is installed in the print server's driver store, or the print server can locate a driver package containing the class printer driver through some other implementation-specific mechanism;<11> otherwise, the server returns ERROR_UNKNOWN_PRINTER_DRIVER. Changed to: The print server SHOULD<10> perform the following additional validation steps: … • Validate that, if the printer driver specified by the client is a derived printer driver, either the class printer driver on which the derived printer driver depends is already installed on the print server, or a driver package containing the class printer driver is installed in the print server's driver store, or the print server can locate a driver package containing the class printer driver through some other implementation-specific mechanism;<11> otherwise, the server returns ERROR_UNKNOWN_PRINTER_DRIVER. This HRESULT error code is constructed by using the HRESULT From WIN32 Error Code Macro ([MS-ERREF] section 2.1.2) on the 16-bit Win32 value for this error ([MS-ERREF] section 2.2).

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[MS-PKAP]: Public Key Authentication Protocol

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

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

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 V9.0 – 2018/09/12.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2019/06/24</td><td>In Section 2.2.2, Remote Assistance Connection String 2, details for the URI attribute have been added for the Listener node.

Changed from:

...

3. The Transport Node has Listener child Nodes that give information about the Server IP and port. This Listener node <L> has the following attributes.

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>P</td><td>Port: The dynamic port on which the Remote Assistance connection could happen.</td></tr>
<tr><td>N</td><td>Server Name: The name/IP address of the server, that is, the novice computer.</td></tr>
</table>
...

Changed to:

...

3. The Transport Node has Listener child Nodes that give information about the Server IP and port. This Listener node <L> has the following attributes.</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>P</td><td>Port: The dynamic port on which the Remote Assistance connection could happen.</td></tr><tr><td>N</td><td>Server Name: The name/IP address of the server, that is, the novice computer.</td></tr><tr><td>U</td><td>URI: The full URI if websocket listener is enabled. The U (URI) is used instead of the P (port) attribute. N (server name) attribute is still included.</td></tr></table> ...

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-RDPADRV]: Remote Desktop Protocol Audio Level and Drive Letter Persistence Virtual Channel Extension

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

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

RSS
Atom

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:

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

March 20, 2017 - Download

June 1, 2017 - Download

December 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

March 13, 2019 - Download

September 23, 2019 - Download

March 4, 2020 - Download

August 24, 2020 – Download

Errata below are for Protocol Document Version V53.0 - 2020/08/26

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2020/12/07</td><td>In Section 2.2.1.3.2 Client Core Data (TS_UD_CS_CORE), added two additional values to the version field.

Changed from:

version (4 bytes): A 32-bit, unsigned integer. Client version number for the RDP. The major version number is stored in the high 2 bytes, while the minor version number is stored in the low 2 bytes.
<table>
<tr><td>Value</td><td>Meaning</td></tr>
<tr><td>0x00080001</td><td>RDP 4.0 servers</td></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>0x0008000C</td><td>RDP 10.7 servers</td></tr>
</table>
</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
Changed to:

version (4 bytes): A 32-bit, unsigned integer. Client version number for the RDP. The major version number is stored in the high 2 bytes, while the minor version number is stored in the low 2 bytes.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00080001</td><td>RDP 4.0 servers</td></tr>
<tr><td>0x00080004</td><td>RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 servers</td></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>0x0008000C</td><td>RDP 10.7 servers</td></tr>
<tr><td>0x0008000D</td><td>RDP 10.8 servers</td></tr>
<tr><td>0x0008000E</td><td>RDP 10.9 servers</td></tr>
</table>

In Section 2.2.1.4.2 Server Core Data (TS_UD_SC_CORE), added the same two additional values to the version field.

Changed from:

version (4 bytes): A 32-bit, unsigned integer. The server version number for the RDP. The major version number is stored in the high two bytes, while the minor version number is stored in the low two bytes.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00080001</td><td>RDP 4.0 servers</td></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>0x0008000C</td><td>RDP 10.7 servers</td></tr>
</table>

Changed to:

version (4 bytes): A 32-bit, unsigned integer. The server version number for the RDP. The major version number is stored in the high two bytes, while the minor version number is stored in the low two bytes.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00080001</td><td>RDP 4.0 servers</td></tr>
<tr><td>0x00080004</td><td>RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 servers</td></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>0x0008000C</td><td>RDP 10.7 servers</td></tr>
<tr><td>0x0008000D</td><td>RDP 10.8 servers</td></tr>
<tr><td>0x0008000E</td><td>RDP 10.9 servers</td></tr>
</table>
</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2020/11/10</td><td>In Section 2.2.5.1.1 Set Error Info PDU Data (TS_SET_ERROR_INFO_PDU), added two additional protocol-independent error codes to the TS_SET_ERROR_INFO_PDU structure.

Changed from:

errorInfo (4 bytes): A 32-bit, unsigned integer. Error code.
Protocol-independent codes:
<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>ERRINFO_NONE
0x00000000</td><td>No error has occurred. This code SHOULD be ignored.</td></tr><tr><td>…</td><td>…</td></tr></table>
Changed to:

errorInfo (4 bytes): A 32-bit, unsigned integer. Error code.
Protocol-independent codes:
<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>ERRINFO_NONE
0x00000000</td><td>No error has occurred. This code SHOULD be ignored.</td></tr><tr><td>…</td><td>…</td></tr><tr><td>ERRINFO_SERVER_SHUTDOWN
0x00000019</td><td>The remote server is busy shutting down.</td></tr><tr><td>ERRINFO_SERVER_REBOOT
0x0000001A</td><td>The remote server is busy rebooting.</td></tr></table></td></tr>
</table>

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[MS-RDPEAR]: Remote Desktop Protocol Authentication Redirection Virtual Channel

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

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

RSS
Atom

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:

September 15, 2017 - Download

September 29, 2020 – Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[MS-RDPECAM]: Remote Desktop Protocol: Video Capture Virtual Channel Extension

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

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

RSS
Atom

Errata below are for Protocol Document Version V1.0 – 2018/09/12.

Errata Published*	Description
2019/02/19	In Section 4.6.2, Property List Response, an annotated dump of a Property List Response (section 2.2.3.17) has been added. Added: The following is an annotated dump of a Property List Response (section 2.2.3.17). 00000000 02 15 01 02 03 00 00 00 00 fa 00 00 00 05 00 00 .... 00000010 00 00 00 00 00 02 02 01 00 00 00 00 ff 00 00 00 .... 00000020 01 00 00 00 80 00 00 00 .... 02->SHARED_MSG_HEADER::Version = 2 15->SHARED_MSG_HEADER::MessageId = PropertyListResponse(21) 01->PropertyDescription[0]::PropertySet = CameraControl(1) 02->PropertyDescription[0]::PropertyId = Focus(2) 03->PropertyDescription[0]::Capabilities = Manual and Auto(1 + 2) 00 00 00 00->PropertyDescription[0]::MinValue = 0 fa 00 00 00->PropertyDescription[0]::MaxValue = 250 05 00 00 00->PropertyDescription[0]::Step = 5 00 00 00 00->PropertyDescription[0]::DefaultValue = 0 02->PropertyDescription[1]::PropertySet = VideoProcAmp(2) 02->PropertyDescription[1]::PropertyId = Brightness(2) 01->PropertyDescription[1]::Capabilities = Manual(1) 00 00 00 00->PropertyDescription[1]::MinValue = 0 ff 00 00 00->PropertyDescription[1]::MaxValue = 255 01 00 00 00->PropertyDescription[1]::Step = 1 80 00 00 00->PropertyDescription[1]::DefaultValue = 128
2019/02/19	In Section 2.2.1, Shared Message Header (SHARED_MSG_HEADER), updated values to hexadecimal format for consistency in the MessageId field table. Changed from: ... MessageId (1 byte): An 8-bit unsigned integer that specifies the type of the message. Value / Meaning SuccessResponse 1 / A Success Response (section 2.2.3.1) message.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description	
	ErrorResponse 2	An Error Response (section 2.2.3.2) message.
	SelectVersionRequest 3	A Select Version Request (section 2.2.2.1) message.
	SelectVersionResponse 4	A Select Version Response (section 2.2.2.2) message.
	DeviceAddedNotification 5	A Device Added Notification (section 2.2.2.3) message.
	DeviceRemovedNotification 6	A Device Removed Notification (section 2.2.2.4) message.
	ActivateDeviceRequest 7	An Activate Device Request (section 2.2.3.3) message.
	DeactivateDeviceRequest 8	A Deactivate Device Request (section 2.2.3.4) message.
	StreamListRequest 9	A Stream List Request (section 2.2.3.5) message.
	StreamListResponse 10	A Stream List Response (section 2.2.3.6) message.
	MediaTypeListRequest 11	A Media Type List Request (section 2.2.3.7) message.
	MediaTypeListResponse 12	A Media Type List Response (section 2.2.3.8) message.
	CurrentMediaTypeRequest 13	A Current Media Type Request (section 2.2.3.9) message.
	CurrentMediaTypeResponse 14	A Current Media Type Response (section 2.2.3.10) message.
	StartStreamsRequest 15	A Start Streams Request (section 2.2.3.11) message.
	StopStreamsRequest 16	A Stop Streams Request (section 2.2.3.12) message.
	SampleRequest 17	A Sample Request (section 2.2.3.13) message.
	SampleResponse 18	A Sample Response (section 2.2.3.14) message.
	SampleErrorResponse 19	A Sample Error Response (section 2.2.3.15) message.
	PropertyListRequest 20	A Property List Request (section 2.2.3.16) message. This message is supported only by version 2 of the protocol.
	PropertyListResponse 21	A Property List Response (section 2.2.3.17) message. This message is

Copyright © 2020 Microsoft Corporation

Errata Published*	Description

	supported only by version 2 of the protocol.
PropertyValueRequest 22	A Property Value Request (section 2.2.3.18) message. This message is supported only by version 2 of the protocol.
PropertyValueResponse 23	A Property Value Response (section 2.2.3.19) message. This message is supported only by version 2 of the protocol.
SetPropertyValueRequest 24	A Set Property Value Request (section 2.2.3.20) message. This message is supported only by version 2 of the protocol.

Changed to:

...

MessageId (1 byte): An 8-bit unsigned integer that specifies the type of the message.

Value	Meaning
SuccessResponse 0x01	A Success Response (section 2.2.3.1) message.
ErrorResponse 0x02	An Error Response (section 2.2.3.2) message.
SelectVersionRequest 0x03	A Select Version Request (section 2.2.2.1) message.
SelectVersionResponse 0x04	A Select Version Response (section 2.2.2.2) message.
DeviceAddedNotification 0x05	A Device Added Notification (section 2.2.2.3) message.
DeviceRemovedNotification 0x06	A Device Removed Notification (section 2.2.2.4) message.
ActivateDeviceRequest 0x07	An Activate Device Request (section 2.2.3.3) message.
DeactivateDeviceRequest 0x08	A Deactivate Device Request (section 2.2.3.4) message.
StreamListRequest 0x09	A Stream List Request (section 2.2.3.5) message.
StreamListResponse 0x0A	A Stream List Response (section 2.2.3.6) message.
MediaTypeListRequest 0x0B	A Media Type List Request (section 2.2.3.7) message.
MediaTypeListResponse 0x0C	A Media Type List Response (section 2.2.3.8) message.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description

CurrentMediaTypeRequest 0x0D	A Current Media Type Request (section 2.2.3.9) message.
CurrentMediaTypeResponse 0x0E	A Current Media Type Response (section 2.2.3.10) message.
StartStreamsRequest 0x0F	A Start Streams Request (section 2.2.3.11) message.
StopStreamsRequest 0x10	A Stop Streams Request (section 2.2.3.12) message.
SampleRequest 0x11	A Sample Request (section 2.2.3.13) message.
SampleResponse 0x12	A Sample Response (section 2.2.3.14) message.
SampleErrorResponse 0x13	A Sample Error Response (section 2.2.3.15) message.
PropertyListRequest 0x14	A Property List Request (section 2.2.3.16) message. This message is supported only by version 2 of the protocol.
PropertyListResponse 0x15	A Property List Response (section 2.2.3.17) message. This message is supported only by version 2 of the protocol.
PropertyValueRequest 0x16	A Property Value Request (section 2.2.3.18) message. This message is supported only by version 2 of the protocol.
PropertyValueResponse 0x17	A Property Value Response (section 2.2.3.19) message. This message is supported only by version 2 of the protocol.
SetPropertyValueRequest 0x18	A Set Property Value Request (section 2.2.3.20) message. This message is supported only by version 2 of the protocol.

In Section 2.2.3.2, Error Response, updated values to hexadecimal format for consistency in the ErrorCode field table.

Changed from:

...

ErrorCode (4 bytes): A 32-bit unsigned integer containing an error code.

Value	Meaning
UnexpectedError 1	An unexpected error occurred.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description

InvalidMessage 2	An invalid message was received. Either the message is malformed, or the protocol version or message type is unexpected.
NotInitialized 3	The object MUST be initialized before the requested operation can be carried out. This error could be returned, for example, when attempting to communicate with a deactivated camera device.
InvalidRequest 4	The request is invalid in the current state.
InvalidStreamNumber 5	The provided stream number was invalid.
InvalidMediaType 6	The data specified for the stream format is invalid, inconsistent, or not supported.
OutOfMemory 7	The client ran out of memory.
ItemNotFound 8	The device does not support the requested property. This error code is generated only by version 2 of the protocol.
SetNotFound 9	The device does not support the requested property set. This error code is generated only by version 2 of the protocol.
OperationNotSupported 10	The requested operation is not supported. This error code is generated only by version 2 of the protocol.

Changed to:

...

ErrorCode (4 bytes): A 32-bit unsigned integer containing an error code.

Value	Meaning
UnexpectedError 0x00000001	An unexpected error occurred.
InvalidMessage 0x00000002	An invalid message was received. Either the message is malformed, or the protocol version or message type is unexpected.
NotInitialized 0x00000003	The object MUST be initialized before the requested operation can be carried out. This error could be returned, for example, when attempting to communicate with a deactivated camera device.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description

InvalidRequest 0x00000004	The request is invalid in the current state.
InvalidStreamNumber 0x00000005	The provided stream number was invalid.
InvalidMediaType 0x00000006	The data specified for the stream format is invalid, inconsistent, or not supported.
OutOfMemory 0x00000007	The client ran out of memory.
ItemNotFound 0x00000008	The device does not support the requested property. This error code is generated only by version 2 of the protocol.
SetNotFound 0x00000009	The device does not support the requested property set. This error code is generated only by version 2 of the protocol.
OperationNotSupported 0x0000000A	The requested operation is not supported. This error code is generated only by version 2 of the protocol.

In Section 2.2.3.6.1, STREAM_DESCRIPTION, updated the value to hexadecimal format for consistency in the StreamCategory field table.

Changed from:

...

StreamCategory (1 byte): An 8-bit unsigned integer that specifies the category of the stream.

Value	Meaning
Capture 1	Capture category streams provide a stream of compressed or uncompressed digital video.

Changed to:

...

StreamCategory (1 byte): An 8-bit unsigned integer that specifies the category of the stream.

Value	Meaning
Capture 0x01	Capture category streams provide a stream of compressed or uncompressed digital video.

In Section 2.2.3.8.1, MEDIA_TYPE_DESCRIPTION, updated values to hexadecimal format for consistency in the Format field table.

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
Changed from:
...
Format (1 byte): An 8-bit unsigned integer that specifies the stream codec.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>H264 1</td><td>H.264 video as described in [ITU-H.264-201704]. Media samples contain H.264 bitstream data with start codes and interleaved sequence parameter set/picture parameter set (SPS/PPS) packets. Each sample contains one complete picture, either one field or one frame.</td></tr>
<tr><td>MJPG 2</td><td>Motion JPEG. Motion JPEG is a video compression format in which each video frame of a digital video sequence is independently compressed as a JPEG image.</td></tr>
<tr><td>YUY2 3</td><td>YUY2 video as specified in [MSDN-YUVFormats].</td></tr>
<tr><td>NV12 4</td><td>NV12 video as described in [MSDN-YUVFormats].</td></tr>
<tr><td>I420 5</td><td>I420 video. Identical to YV12 as described in [MSDN-YUVFormats] except that the order of the U and V planes is reversed.</td></tr>
<tr><td>RGB24 6</td><td>RGB, 24 bits per pixel.</td></tr>
<tr><td>RGB32 7</td><td>RGB, 32 bits per pixel.</td></tr>
</table>
...

Changed to:
...
Format (1 byte): An 8-bit unsigned integer that specifies the stream codec.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>H264 0x01</td><td>H.264 video as described in [ITU-H.264-201704]. Media samples contain H.264 bitstream data with start codes and interleaved sequence parameter set/picture parameter set (SPS/PPS) packets. Each sample contains one complete picture, either one field or one frame.</td></tr>
<tr><td>MJPG 0x02</td><td>Motion JPEG. Motion JPEG is a video compression format in which each video frame of a digital video sequence is independently compressed as a JPEG image.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

Errata Published*	Description

YUY2 0x03	YUY2 video as specified in [MSDN-YUVFormats].
NV12 0x04	NV12 video as described in [MSDN-YUVFormats].
I420 0x05	I420 video. Identical to YV12 as described in [MSDN-YUVFormats] except that the order of the U and V planes is reversed.
RGB24 0x06	RGB, 24 bits per pixel.
RGB32 0x07	RGB, 32 bits per pixel.

...

In Section 2.2.3.17.1, PROPERTY_DESCRIPTION, updated values to hexadecimal format for consistency in the PropertySet and PropertyId field tables.

Changed from:

...

PropertySet (1 byte): An 8-bit unsigned integer that specifies the property set.

Value	Meaning
CameraControl 1	This property set category controls camera device settings.
VideoProcAmp 2	This property set controls devices that can adjust the image color attributes of analog or digital signals.

PropertyId (1 byte): An 8-bit unsigned integer that contains the identifier of the property within the property set specified by the PropertySet field.

CameraControl properties:

Value	Meaning
Exposure 1	This property controls the exposure time of the device.
Focus 2	This property controls the focus setting of the device.
Pan 3	This property controls the pan setting of the device.
Roll 4	This property controls the roll setting of the device.
Tilt 5	This property controls the tilt setting of the device.
Zoom 6	This property controls the zoom setting of the device.

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
VideoProcAmp properties:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>BacklightCompensation 1</td><td>This property controls the backlight compensation setting of the device. This value MUST be either 0 or 1. The value 0 indicates that backlight compensation is disabled. The value 1 indicates that backlight compensation is enabled.</td></tr>
<tr><td>Brightness 2</td><td>This property controls the brightness setting of the device.</td></tr>
<tr><td>Contrast 3</td><td>This property controls the contrast setting of the device.</td></tr>
<tr><td>Hue 4</td><td>This property controls the hue setting of the device.</td></tr>
<tr><td>WhiteBalance 5</td><td>This property controls the white balance setting of the device.</td></tr>
</table>
...

Changed to:
...
PropertySet (1 byte): An 8-bit unsigned integer that specifies the property set.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>CameraControl 0x01</td><td>This property set category controls camera device settings.</td></tr>
<tr><td>VideoProcAmp 0x02</td><td>This property set controls devices that can adjust the image color attributes of analog or digital signals.</td></tr>
</table>
PropertyId (1 byte): An 8-bit unsigned integer that contains the identifier of the property within the property set specified by the PropertySet field.
CameraControl properties:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>Exposure 0x01</td><td>This property controls the exposure time of the device.</td></tr>
<tr><td>Focus 0x02</td><td>This property controls the focus setting of the device.</td></tr>
<tr><td>Pan 0x03</td><td>This property controls the pan setting of the device.</td></tr>
<tr><td>Roll 0x04</td><td>This property controls the roll setting of the device.</td></tr>
<tr><td>Tilt 0x05</td><td>This property controls the tilt setting of the device.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

Errata Published*	Description

Zoom 0x06	This property controls the zoom setting of the device.

VideoProcAmp properties:

Value	Meaning
BacklightCompensation 0x01	This property controls the backlight compensation setting of the device. This value MUST be either 0 or 1. The value 0 indicates that backlight compensation is disabled. The value 1 indicates that backlight compensation is enabled.
Brightness 0x02	This property controls the brightness setting of the device.
Contrast 0x03	This property controls the contrast setting of the device.
Hue 0x04	This property controls the hue setting of the device.
WhiteBalance 0x05	This property controls the white balance setting of the device.

...

In Section 2.2.3.19.1, PROPERTY_VALUE, updated values to hexadecimal format for consistency in the Mode field table.

Changed from:

...

Mode (1 byte): An 8-bit unsigned integer that specifies how the property was set.

Value	Meaning
Manual 1	The value was set manually.
Auto 2	The value was set automatically.

...

Changed to:

...

Mode (1 byte): An 8-bit unsigned integer that specifies how the property was set.

Value	Meaning
Manual 0x01	The value was set manually.
Auto 0x02	The value was set automatically.

...

Copyright © 2020 Microsoft Corporation

Errata Published*	Description

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-RDPEDISP]: Remote Desktop Protocol: Display Update Virtual Channel Extension

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

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

RSS
Atom

Errata below are for Protocol Document Version V7.0 – 2018/09/12.

Errata Published*	Description
2019/08/19	In Section 1, Introduction, changed the source of the display configuration changes from server to client. Changed from: This document specifies the Remote Desktop Protocol: Display Control Channel Extension to the Remote Desktop Protocol: Basic Connectivity and Graphics Remoting, as specified in [MS-RDPBCGR] sections 1 to 5. This control protocol is used by the server to request display configuration changes in a remote session. Display configuration changes include the addition, removal and repositioning of monitors, resolution updates, and orientation updates. Changed to: This document specifies the Remote Desktop Protocol: Display Control Channel Extension to the Remote Desktop Protocol: Basic Connectivity and Graphics Remoting, as specified in [MS-RDPBCGR] sections 1 to 5. This control protocol is used by the client to request display configuration changes in a remote session. Display configuration changes include the addition, removal and repositioning of monitors, resolution updates, and orientation updates.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

March 20, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

August 24, 2020 – Download

Errata below are for Protocol Document Version V14.0 - 2020/08/26

Errata Published*	Description
2021/01/11	In Section 2.2.1.5 RDPGFX_HEADER, corrected an error in the cmdId value RDPGFX_CAPS_CONFIRM_PDU. Changed from: RDP_CAPS_CONFIRM_PDU (section 2.2.2.19) Changed to: RDPGFX_CAPS_CONFIRM_PDU (section 2.2.2.19)
2020/10/26	In Section 2.2.2.23 RDPGFX_MAP_SURFACE_TO_SCALED_WINDOW_PDU, corrected prescriptive language regarding mapping a surface to a RAIL window. Changed from: The RDPGFX_MAP_SURFACE_TO_SCALED_WINDOW_PDU message is sent by the server to instruct the client to map a surface to a RAIL window on the client, including a target width and height to which the surface should be scaled. Changed to: The RDPGFX_MAP_SURFACE_TO_SCALED_WINDOW_PDU message is sent by the server to instruct the client to map a surface to a RAIL window on the client, including a target width and height to which the surface MUST be scaled.

Copyright © 2020 Microsoft Corporation

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[MS-RDPELE]: Remote Desktop Protocol: Licensing Extension

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

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

RSS
Atom

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

September 12, 2018 - Download

March 4, 2020 - Download

August 24, 2020 – Download

Errata below are for Protocol Document Version V15.1 - 2020/08/26

Errata Published*	Description
2021/01/11	In Section 2.2.2.9.1 Licensed Product Info (LICENSED_PRODUCT_INFO), corrected OID_LICENSED_PRODUCT_INFO to szOID_PKIX_LICENSED_PRODUCT_INFO. Changed from: The certificate extension with OID "1.3.6.1.4.1.311.18.5" (OID_LICENSED_PRODUCT_INFO) contains product information specific to a license issued to a client and is encoded by the Licensed Product Info structure. Changed to: The certificate extension with OID "1.3.6.1.4.1.311.18.5" (szOID_PKIX_LICENSED_PRODUCT_INFO) contains product information specific to a license issued to a client and is encoded by the Licensed Product Info structure. In Section 2.2.2.9.2 MS License Server Info, corrected OID_MS_LICENSE_SERVER_INFO to szOID_PKIX_LICENSED_PRODUCT_INFO. Changed from: The certificate extension with OID "1.3.6.1.4.1.311.18.6" (OID_MS_LICENSE_SERVER_INFO) contains information about the license server that issued a license and is encoded by the MS License Server Info Version 1 (section 2.2.2.9.2.1) and Version 2 (section 2.2.2.9.2.2) structures. Changed to: The certificate extension with OID "1.3.6.1.4.1.311.18.6" (szOID_PKIX_MS_LICENSE_SERVER_INFO) contains information about the license server that issued a license and is encoded by the MS License Server Info Version 1 (section 2.2.2.9.2.1) and Version 2 (section 2.2.2.9.2.2) structures.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

March 2, 2016 - Download

Errata below are for Protocol Document Version V10.0 – 2018/09/12.

Errata Published*	Description
2019/03/18	In Section 1.3, Overview, clarified that a port number is not specified in an Initiate Multitransport Request PDU. Changed from: The Initiate Multitransport Request PDU contains information that uniquely identifies the multitransport connection; it contains a request ID and a cookie, a protocol identifier that identifies the type of multitransport connection that the client attempts to establish, and a port number that identifies the port on which the server is listening. When the client receives the Initiate Multitransport Request PDU, it attempts to establish a secure multitransport connection with the server. Changed to: The Initiate Multitransport Request PDU contains information that uniquely identifies the multitransport connection; it contains a request ID, a cookie, and a protocol identifier that identifies the type of multitransport connection that the client attempts to establish. When the client receives the Initiate Multitransport Request PDU, it attempts to establish a secure multitransport connection with the server.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

July 18, 2016 - Download

June 1, 2017 - Download

Errata below are for Protocol Document Version V10.0 – 2018/09/12.

Errata Published*	Description
2019/07/08	In Section 2.2.2.1, Client Device List Announce Request (DR_PRN_DEVICE_ANNOUNCE), added the section number that describes XPS mode to the RDPDR_PRINTER_ANNOUNCE_FLAG_XPSFORMAT value meaning in the Flags field table. Changed from: ... Flags (4 bytes): A 32-bit unsigned integer that indicates the properties of the client printer queue. This bit field MUST be a valid combination of any of the following values. Value / Meaning ... / ,,, RDPDR_PRINTER_ANNOUNCE_FLAG_XPSFORMAT 0x00000010 / This client/printer supports XML Paper Specification (XPS) format. ... / ,,, Changed to: ... Flags (4 bytes): A 32-bit unsigned integer that indicates the properties of the client printer queue. This bit field MUST be a valid combination of any of the following values. Value / Meaning ... / … RDPDR_PRINTER_ANNOUNCE_FLAG_XPSFORMAT 0x00000010 / This client/printer supports XML Paper Specification (XPS) format (section 3.1.1.2).

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	… …

In Section 2.2.2.2, Server Printer Set XPS Mode (DR_PRN_USING_XPS), added that the DR_PRN_USING_XPS message indicates to the client that future printer write request messages will use the XPS format.

Changed from:

This message is sent from server to client to set the device in XPS mode (see section 3.1.1.2).

...

Changed to:

This message is sent from server to client to set the device in XPS mode (see section 3.1.1.2) and indicate to the client that future Printer Write Request (section 2.2.2.9) messages will use the XPS format.

...

In Section 3.1.1.2, XPS Mode, added the section number that describes the server behavior if it chooses to use the XPS format.

Changed from:

...

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.

...

Changed to:

...

The server MUST notify the client with the DR_PRN_USING_XPS (section 2.2.2.2) message as described in section 3.3.5.1.2 if it chooses to use the XPS format.

...

In Section 3.3.5.1.2, Sending a Printer Set XPS Mode Message, clarified the server Printer Write Request message section number.

Changed from:

...

If the server chooses to send print data in XPS format, the server MUST send this message to the client prior to sending any data in the write request messages (section 2.2.2.1).

Changed to:

...

If the server chooses to send print data in XPS format, the server MUST send this message to the client prior to sending any data in the Printer Write Request (section 2.2.2.9) message.

Copyright © 2020 Microsoft Corporation

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

September 23, 2019 - Download

March 4, 2020 - Download

Errata below are for Protocol Document Version V29.0 – 2020/03/04.

Errata Published*	Description

2020/07/06	In Section 4.1.1.1 New or Existing Windows, added the 'TS_WINDOW_ORDER_HEADER' prefix to 'WindowId'.
	Changed from:
	
	`2e -> TS_WINDOW_ORDER_HEADER::Header (1 Byte)`
	`81 00 -> TS_WINDOW_ORDER_HEADER::OrderSize (2 Bytes)`
	`9e df 08 19 -> TS_WINDOW_ORDER_HEADER::FieldsPresentFlags (4 Bytes)`
	`58 01 12 00 -> WindowId`
	`00 00 00 00 -> OwnerWindowId`
	`00 00 cf 14 -> Style`
	`00 01 00 00 -> ExtendedStyle`
	`05 -> ShowState`
	
	Changed to:
	
	`2e -> TS_WINDOW_ORDER_HEADER::Header (1 Byte)`
	`81 00 -> TS_WINDOW_ORDER_HEADER::OrderSize (2 Bytes)`
	`9e df 08 19 -> TS_WINDOW_ORDER_HEADER::FieldsPresentFlags (4 Bytes)`
	`58 01 12 00 -> TS_WINDOW_ORDER_HEADER::WindowId (4 Bytes)`
	`00 00 00 00 -> OwnerWindowId`

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	00 00 cf 14 -> Style 00 01 00 00 -> ExtendedStyle 05 -> ShowState In Section 4.1.1.2 Deleted Window, added the 'TS_WINDOW_ORDER_HEADER' prefix to 'WindowId'. Changed from: 00000000 2e 0b 00 00 00 00 21 24 00 03 00......!$... 2e -> TS_WINDOW_ORDER_HEADER::Header (1 Byte) 0b 00 -> TS_WINDOW_ORDER_HEADER::OrderSize (2 Bytes) 00 00 00 21 -> TS_WINDOW_ORDER_HEADER::FieldsPresentFlags (4 Bytes) (WINDOW_ORDER_TYPE_WINDOW \| WINDOW_ORDER_STATE_DELETED) 24 00 03 00 -> WindowId (4 Bytes) Changed to: 00000000 2e 0b 00 00 00 00 21 24 00 03 00......!$... 2e -> TS_WINDOW_ORDER_HEADER::Header (1 Byte) 0b 00 -> TS_WINDOW_ORDER_HEADER::OrderSize (2 Bytes) 00 00 00 21 -> TS_WINDOW_ORDER_HEADER::FieldsPresentFlags (4 Bytes) (WINDOW_ORDER_TYPE_WINDOW | WINDOW_ORDER_STATE_DELETED) 24 00 03 00 -> TS_WINDOW_ORDER_HEADER::WindowId (4 Bytes) In Section 4.4.1 S_RAIL_ORDER_SYSPARAM, added the 'TS_HIGHCONTRAST::' prefix to 'Flags', 'ColorSchemeLength', and 'ColorSchema'. Changed from: 03 00 -> TS_RAIL_PDU_HEADER::orderType = TS_RAIL_ORDER_SYSPARAM(3) (2 Bytes) 12 00 -> TS_RAIL_PDU_HEADER::orderLength = 18 (2 Bytes) 43 00 00 00 -> SystemParam: SPI_SETHIGHCONTRAST (4 Bytes) 7e 00 00 00 -> Flags: 0x7e (4 Bytes) 02 00 00 00 -> ColorSchemeLength: 2 (4 Bytes) 00 00 -> ColorScheme: 0 (2 Bytes) Changed to:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	03 00 -> TS_RAIL_PDU_HEADER::orderType = TS_RAIL_ORDER_SYSPARAM(3) (2 Bytes) 12 00 -> TS_RAIL_PDU_HEADER::orderLength = 18 (2 Bytes) 43 00 00 00 -> SystemParam: SPI_SETHIGHCONTRAST (4 Bytes) 7e 00 00 00 -> TS_HIGHCONTRAST::Flags: 0x7e (4 Bytes) 02 00 00 00 -> TS-HIGHCONTRAST::ColorSchemeLength: 2 (4 Bytes) 00 00 -> TS_HIGHCONTRAST::ColorScheme: 0 (2 Bytes)
2020/07/06	In Section 2.2.1.3.1.2.1 New or Existing Window, removed the extraneous space from 'FIELD_ RESIZE' Changed from: WindowRightResizeMargin (4 bytes): An unsigned 32-bit integer specifying the width of the transparent hit-testable margin along the right edge of the window. Any mouse, pen or touch input within this margin SHOULD be sent to the server. This field is present only if the WINDOW_ORDER_FIELD_ RESIZE_MARGIN_X flag is set in the FieldsPresentFlags field of TS_WINDOW_ORDER_HEADER. Resize margins SHOULD be used to extend the window geometry (defined by the WindowOffsetX, WindowOffsetY, WindowWidth and WindowHeight fields) and are not included in the window boundaries. WindowTopResizeMargin (4 bytes): An unsigned 32-bit integer specifying the height of the transparent hit-testable margin along the top edge of the window. Any mouse, pen or touch input within this margin SHOULD be sent to the server. This field is present only if the WINDOW_ORDER_FIELD_ RESIZE_MARGIN_Y flag is set in the FieldsPresentFlags field of TS_WINDOW_ORDER_HEADER. Resize margins SHOULD be used to extend the window geometry (defined by the WindowOffsetX, WindowOffsetY, WindowWidth and WindowHeight fields) and are not included in the window boundaries. Changed to: WindowRightResizeMargin (4 bytes): An unsigned 32-bit integer specifying the width of the transparent hit-testable margin along the right edge of the window. Any mouse, pen or touch input within this margin SHOULD be sent to the server. This field is present only if the WINDOW_ORDER_FIELD_RESIZE_MARGIN_X flag is set in the FieldsPresentFlags field of TS_WINDOW_ORDER_HEADER. Resize margins SHOULD be used to extend the window geometry (defined by the WindowOffsetX, WindowOffsetY, WindowWidth and WindowHeight fields) and are not included in the window boundaries. WindowTopResizeMargin (4 bytes): An unsigned 32-bit integer specifying the height of the transparent hit-testable margin along the top edge of the window. Any mouse, pen or touch input within this margin SHOULD be sent to the server. This field is present only if the WINDOW_ORDER_FIELD_RESIZE_MARGIN_Y flag is set in the FieldsPresentFlags field of TS_WINDOW_ORDER_HEADER. Resize margins SHOULD be used to extend the window geometry (defined by the WindowOffsetX, WindowOffsetY, WindowWidth and WindowHeight fields) and are not included in the window boundaries. In Section 2.2.1.3.1.2.3 Cached Icon, capitalized field names cacheEntry and cacheId.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Changed from: The Cached Icon Window Information Order is generated by the server when a new or existing window sets or updates the icon in its title bar or in the Alt-Tab dialog box. If the icon information was transmitted by the server in a previous Window Information Order or Notification Icon Information Order in the same session, and the icon was cacheable (that is, the server specified a cacheEntry and cacheId for the icon), the server reports the icon cache entries to avoid sending duplicate information. Changed to: The Cached Icon Window Information Order is generated by the server when a new or existing window sets or updates the icon in its title bar or in the Alt-Tab dialog box. If the icon information was transmitted by the server in a previous Window Information Order or Notification Icon Information Order in the same session, and the icon was cacheable (that is, the server specified a CacheEntry and CacheId for the icon), the server reports the icon cache entries to avoid sending duplicate information. In Section 2.2.1.3.1.2.3 Cached Icon, revised 'TS_CACHED ICON_INFO' to 'TS_CACHED_ICON_INFO'. Changed from: CachedIcon (3 bytes): Three bytes. TS_CACHED ICON_INFO structure. Describes a cached icon on the client. Changed to: CachedIcon (3 bytes): Three bytes. TS_CACHED_ICON_INFO (section 2.2.1.2.4) structure. Describes a cached icon on the client. In Section 4.1.1.6 Non-Monitored Desktop, revised title from 'Non-monitored Desktop' Changed from: 4.1.1.6 Non-monitored Desktop Changed to: 4.1.1.6 Non-Monitored Desktop In Section 3.2.5.1.8 Processing Desktop Information Orders, revised 'non-monitored desktop' to 'Non-Monitored Desktop' to reflect section title change. Changed from: • Upon receipt of a Desktop Information Order for a non-monitored desktop, as specified in section 2.2.1.3.3.2.2, the client SHOULD discard all of the existing RAIL windows and Notify Icons. Changed to: • Upon receipt of a Desktop Information Order for a Non-Monitored Desktop packet, as specified in section 2.2.1.3.3.2.2, the client SHOULD discard all of the existing RAIL windows and Notify Icons.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

September 23, 2019 - Download

August 24, 2020 – Download

Copyright © 2020 Microsoft Corporation

[MS-RDPEUDP2]: Remote Desktop Protocol: UDP Transport Extension Version 2

This topic lists the Errata found in [MS-RDPEUDP2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

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

RSS
Atom

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 13, 2019 - Download

September 23, 2019 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Errata below are for Protocol Document Version V20.0 – 2018/09/12.

Errata Published*	Description
2019/02/19	In Section 4.2.4.1, Input TS_RFX_TILESET Message, updated the first line of an annotated dump of a TS_RFX_TILESET message containing a single encoded 64x64 tile from "00000000 c7 cc 3e 0b 00 00 01 01 c2 ca 00 00 51 50 01 40" to "00000000 c7 cc 3e 0b 00 00 01 00 c2 ca 00 00 51 50 01 40". Changed from: The following is an annotated dump of a TS_RFX_TILESET (section 2.2.2.3.4) message containing a single encoded 64x64 tile. 00000000 c7 cc 3e 0b 00 00 01 01 c2 ca 00 00 51 50 01 40 ... Changed to: The following is an annotated dump of a TS_RFX_TILESET (section 2.2.2.3.4) message containing a single encoded 64x64 tile. 00000000 c7 cc 3e 0b 00 00 01 00 c2 ca 00 00 51 50 01 40 ...
2019/02/19	In Section 3.1.8.1.6, Linearization, updated the converted value of -10 to 10 after coefficients from LL3 undergo differential encoding. Changed from: ... The coefficients from LL3 also undergo differential encoding. Except for the first coefficient, every raster-scanned LL3 coefficient is subtracted from its previous neighbor. For example, if the raster-scanned LL3 coefficients are [64, 32, 42, 54, 50, 60, 40, 70] Then, after differential encoding, they would get converted to

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	[64, -32, 10, 12, -4, -10, -20, 30] Changed to: ... The coefficients from LL3 also undergo differential encoding. Except for the first coefficient, every raster-scanned LL3 coefficient is subtracted from its previous neighbor. For example, if the raster-scanned LL3 coefficients are [64, 32, 42, 54, 50, 60, 40, 70] Then, after differential encoding, they would get converted to [64, -32, 10, 12, -4, 10, -20, 30]

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Errata below are for Protocol Document Version V38.0 – 2018/09/12.

Errata Published*	Description
2019/10/16	In Section 2.2.3.4, string Element, parentheses around the ArrayOfString element have been removed. In Section 3.4.4.3.2.1, AcquireTemplates, parentheses around the ArrayOfString element have been removed. In Section 3.4.4.3.2.2, AcquireTemplatesResponse: Changed from: ArrayOfGuideTemplate Changed to: ArrayOfGuidTemplate In Section 3.5.4.2.3.2, ArrayOfGetClientLicensorCertResponse: Changed from: name="ArrayOfGetClIentLicensorCertResponse"> <xs:sequence> Changed to: name="ArrayOfGetClientLicensorCertResponse"> <xs:sequence>

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	In Section 3.6.4.1, Synchronous Enrollment Operation, and Section 3.6.4.2, Asynchronous Enrollment Operation: Changed from: serverState Changed to: ServerState

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

September 15, 2017 - Download

Errata below are for Protocol Document Version V31.0 - 2020/09/12

Errata Published*	Description
2021/02/08	In Section 2.2.2.13.4, rpc_sec_vt_pcontext, the descriptions of the InterfaceId and TransferSyntax fields were updated: Changed from: InterfaceId: The interface identifier for the presentation context of the request PDU in which this verification trailer appears. This MUST match the chosen abstract_syntax field from the bind or alter_context PDU where the presentation context was negotiated. For information on how a presentation context is negotiated, see section 3.3.1.5.6. TransferSyntax: The transfer syntax identifier for the presentation context of the request PDU in which this verification trailer appears. This MUST match the chosen transfer_syntax from the bind or alter_context PDU where the presentation context was negotiated. For information on how a presentation context is negotiated, see section 3.3.1.5.6. Changed to: InterfaceId: The interface identifier for the presentation context of the request PDU in which this verification trailer appears. This value MUST match the chosen abstract_syntax field from the bind or alter_context PDU where the presentation context was negotiated. For information on how a presentation context is negotiated, see section 3.3.1.5.6. TransferSyntax: The transfer syntax identifier for the presentation context of the request PDU in which this verification trailer appears. This value MUST match the chosen transfer_syntax from the bind or alter_context PDU where the presentation context was negotiated. For information on how a presentation context is negotiated, see section 3.3.1.5.6.
2020/10/26	In Section 2.2.2.11 sec_trailer Structure, an update was made to clarify that the structure alignment is 16-bytes Changed from: The sec_trailer structure MUST be placed at the end of the PDU, including past stub data, when present. The sec_trailer structure MUST be 4-byte aligned with respect to the beginning

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	of the PDU. Padding octets MUST be used to align the sec_trailer structure if its natural beginning is not already 4-byte aligned. Changed to: The sec_trailer structure MUST be placed at the end of the PDU, including past stub data, when present. The sec_trailer structure MUST be 16-byte aligned with respect to the beginning of the PDU Body. Padding octets MUST be used to align the sec_trailer structure if its natural beginning is not already 16-byte aligned.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

December 1, 2017 - Download

August 24, 2020 – Download

Errata below are for Protocol Document Version V33.0 - 2020/08/26

Errata Published*	Description
2021/01/25	In Section 2.2.2.14.1, CONFIG_INFO_DATA_1, clarified use of the port data structures. Changed from: Version (4 bytes): A 32-bit unsigned integer that is the level of the PORT_DATA structure that contains the configuration information. This value MUST be 0x00000001 or 0x00000002. Changed to: Version (4 bytes): A 32-bit unsigned integer that indicates whether a PORT_DATA_1 or PORT_DATA_2 structure is provided to return the configuration information. This value MUST be 0x00000001 or 0x00000002. In Section 2.2.2.14.3, PORT_DATA_1, clarified use of the port data structure: Changed from: The PORT_DATA_1 structure specifies PORT_DATA level 1 data. Changed to: The PORT_DATA_1 structure specifies level 1 port configuration data. In Section 2.2.2.14.4, PORT_DATA_2, clarified use of the port data structure:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Changed from: The PORT_DATA_2 structure specifies PORT_DATA level 2 data. Changed to: The PORT_DATA_2 structure specifies level 2 port configuration data. In section, 3.1.4.2.27, RpcSendRecvBidiData (Opnum 97), clarified a field name: Changed from: Verify that the port monitor supports this method, and if that verification fails, return ERROR_NOT_SUPPPORTED. Changed to: Verify that the port monitor supports this method, and if that verification fails, return ERROR_NOT_SUPPORTED. In section 3.1.4.11, Monitor Module Methods, added a method to the list of port monitor modules: Changed from: XcvOpenPort XcvClosePort Changed to: XcvOpenPort XcvDataPort XcvClosePort
2021/01/11	The following sections have had field names, structure names, and section names updated: Section 2.2.1.10.3, PRINTER_INFO_2 Section 2.2.1.15.3, RPC_BranchOfficeJobDataError Section 2.2.2.4.9, _DRIVER_INFO_101 Section 2.2.2.5.2, _FORM_INFO_2 Section 2.2.3.3, Job Notification Values Section 3.1.4.8.5, RpcEnumPrintProcessorDatatypes (Opnum 51) For more details, please see the diff file.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 V23.0 – 2018/09/12.

Errata Published *	Description
2021/01/11	In Section 1 Introduction, added information about the RAS client. Changed from: … This protocol also specifies the format of the phonebook file used by RRAS server. The management application can use the phonebook file format to specify the connection configuration to be used for site-to-site connections. Changed to: … This protocol also specifies the format of the phonebook file used by RRAS server. The management application can use the phonebook file format to specify the connection configuration to be used for site-to-site connections. The client side Remote Access Service (RAS) is a point to point or point to site service that is not in the RRASM protocol. See legacy information in [MSDOCS-RRAS] and [MSDOCS-RAS-API]. RAS client uses a different phonebook file, see legacy information in [MSDOCS-RASpbk]. In Section 1.3 Overview, added information about the RAS client. Changed from: The routing and remote access service (RRAS) server management (RRASM) protocol enables remote management (configuration and monitoring) of RRAS. … … The phonebook file can be created remotely at a well-known location using any remote file management mechanism such as the Server Message Block (SMB) protocol. The RRAS implementation can read the settings and realize the configuration based on the semantics specified. The interaction between a RRASM client and a RRASM server itself is stateless and is accomplished through RPC method invocation. … Changed to:

Copyright © 2020 Microsoft Corporation

Errata Published *	Description
	The routing and remote access service (RRAS) server management (RRASM) protocol enables remote management (configuration and monitoring) of RRAS routers. … … The phonebook file can be created remotely at a well-known location using any remote file management mechanism such as the Server Message Block (SMB) protocol. The RRAS implementation can read the settings and realize the configuration based on the semantics specified. The client side Remote Access Service (RAS) is a point to point or point to site service that is not in this RRASM protocol server site to site router remote access service. See legacy information in [MSDOCS-RRAS] and [MSDOCS-ROUT-API]. Some of the functions in the RAS API are supported only on network servers and other functions are supported only on network clients, see legacy information in [MSDOCS-RA-API]. RAS client uses a different phonebook file, see legacy information in [MSDOCS-RASpbk]. The interaction between a RRASM client and a RRASM server itself is stateless and is accomplished through RPC method invocation. … In Section 1.4 Relationship to Other Protocols, added information about the RAS client. Changed from: The RRAS Management Protocol relies on RPC [MS-RPCE] as a transport. It is used to remotely manage RRAS server implementations. For more information about RRAS, see [MSDN-RAS]. . . . The registry values that the RRASM client uses for configurations are handled using the [MS-RRP] protocol. Any RRAS server implementation can use these registry settings to initialize the RRAS server configuration. Changed to: The RRAS Management Protocol relies on RPC [MS-RPCE] as a transport. It is used to remotely manage RRAS server implementations. . . . The registry values that the RRASM client uses for configurations are handled using the [MS-RRP] protocol. Any RRAS server implementation can use these registry settings to initialize the RRAS server configuration. The client side Remote Access Service (RAS) is a point to point or point to site service. It is not to be confused with this RRASM protocol that is a site to site server side router management protocol. Some of the functions in the RAS API are supported only on network servers and other functions are supported only on network clients, see [MSDOCS-RA-API]. In Section 2.2.2 File Format for Phonebook, added product note about the RAS client phone book. Changed from: The Phonebook is an 8-bit ASCII-encoded text file that contains the names and settings for the demand-dial connections. … RRAS can read the phonebook file from this location<201> for gathering the demand-dial connection settings.

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td></td><td>
<201> Section 2.2.2: The phonebook file used by Windows is router.pbk …

Changed to:

The Phonebook<201> is an 8-bit ASCII-encoded text file that contains the names and settings for the demand-dial connections. … RRAS can read the phonebook file from this location<201> for gathering the demand-dial connection settings.

<201> Section 2.2.2: The client side Remote Access Service (RAS) is not in this server side RRASM protocol. The client RAS creates a different default phonebook file called rasphone.pbk. If the caller does not specify a phonebook file, the default phonebook file is used. For more information see legacy information in[MSDOCS-RASpbk]).

<202> Section 2.2.2: The phonebook file used by Windows servers is router.pbk …

In Section 2.2.2.2.11 VpnStrategy, added MPRI_INTERFACE values and a product note about RAS client values.

Changed from:

. . . and SHOULD take one of the values in the following table.

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0</td><td>Try a series of tunnel protocols.<205></td></tr>
<tr><td>1</td><td>RRAS attempts PPTP only.</td></tr>
<tr><td>2</td><td>RRAS attempts PPTP first. If PPTP fails, L2TP is tried. If L2TP fails, demand-dial connection fails.</td></tr>
<tr><td>3</td><td>RRAS attempts L2TP only.</td></tr>
<tr><td>7</td><td>RRAS attempts IKEv2 only.<206></td></tr>
</table>

Changed to:

. . . and SHOULD take one of the values in the following table.<206>

<table>
<tr><th>Value</th><th>Name</th><th>Meaning</th></tr>
<tr><td>0</td><td>MPR_VS_Default</td><td>Try a series of tunnel protocols.<207></td></tr>
<tr><td>1</td><td>MPR_VS_PptpOnly</td><td>RRAS attempts PPTP only.</td></tr>
<tr><td>2</td><td>MPR_VS_PptpFirst</td><td>RRAS attempts PPTP first. If PPTP fails, L2TP is tried. If L2TP fails, demand-dial connection fails.</td></tr>
<tr><td>3</td><td>MPR_VS_L2tpOnly</td><td>RRAS attempts L2TP only.</td></tr>
<tr><td>4</td><td>MPR_VS_L2tpFirst</td><td>RRAS attempts L2TP first, PPTP second, and IKEv2 third.</td></tr>
</table>
</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>7</td><td>MPR_VS_Ikev2Only</td><td>RRAS attempts IKEv2 only.<208></td></tr>
<tr><td>8</td><td>MPR_VS_Ikev2First</td><td>RRAS attempts IKEv2 first, PPTP second, and L2TP third.</td></tr>
</table>
<206> Section 2.2.2.2.11: The RAS client side RASENTRY structure, dwVpnStrategy field uses a different set of VpnStrategy values. The following client values are not supported by RRASM server protocol. For more information see legacy information in [MSDOCS-RASENTRY].
<table>
<tr><th>Value</th><th>Name</th><th>Meaning</th></tr>
<tr><td>5</td><td>VS_SstpOnly</td><td>Windows Vista with SP1 and later: RAS attempts only SSTP.</td></tr>
<tr><td>6</td><td>VS_SstpFirst</td><td>Windows Vista with SP1 and later: RAS attempts SSTP first followed by IKEv2, PPTP, and then L2TP.</td></tr>
<tr><td>12</td><td>VS_PptpSstp</td><td>Windows 7 and later: RAS attempts PPTP followed only by SSTP.</td></tr>
<tr><td>13</td><td>VS_L2tpSstp</td><td>Windows 7 and later: RAS attempts L2TP followed only by SSTP.</td></tr>
<tr><td>14</td><td>VS_Ikev2Sstp</td><td>Windows 7 and later: RAS attempts IKEv2 followed only by SSTP.</td></tr>
<tr><td>15</td><td>VS_ProtocolList</td><td>Windows 10 and later: Use a Protocol List to determine the protocols to connect to.</td></tr>
</table>
</td></tr>
<tr><td>2019/10/28</td><td>
In Section 2.2.1.2.45, MIB_IPMCAST_OIF_STATS, changed dwIfNextHopIPAddr to dwNextHopAddr in the dwNextHopAddr field description.

Changed from:
...
dwNextHopAddr: Specifies the address of the next hop that corresponds to dwOutIfIndex. The dwOutIfIndex and dwIfNextHopIPAddr members uniquely identify a next hop on point-to-multipoint interfaces, where one interface connects to multiple networks. Examples of point-to-multipoint interfaces include non-broadcast multiple-access (NBMA) interfaces, and the internal interface on which all dial-up clients connect. For Ethernet and other broadcast interfaces, specify zero (0). Also specify zero (0) for point-to-point interfaces, which are identified by only dwOutIfIndex.
...

Changed to:
...
dwNextHopAddr: Specifies the address of the next hop that corresponds to dwOutIfIndex. The dwOutIfIndex and dwNextHopAddr members uniquely identify a next hop on point-to-multipoint interfaces, where one interface connects to multiple networks. Examples of point-to-multipoint interfaces include non-broadcast multiple-access (NBMA) interfaces, and the internal interface on which all dial-up clients connect. For Ethernet and other broadcast interfaces, specify zero (0). Also specify zero (0) for point-to-point interfaces, which are identified by only dwOutIfIndex.
...

In Section 2.2.1.2.130, PPP_PROJECTION_INFO_1, changed dwAuthenticatedData to dwAuthenticationData in the dwAuthenticationData field description.
</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

Errata Published *	Description
	Changed from: ... dwAuthenticationData: The same as dwAuthenticatedData in PPP_LCP_INFO. ... Changed to: ... dwAuthenticationData: The same as dwAuthenticationData in PPP_LCP_INFO (see section 2.2.1.2.71). ... In Section 2.2.1.2.176, IGMP_MIB_GROUP_INFO, changed interface types RAS_SERVER to IGMP_IF_RAS_SERVER and RAS_CLIENT to IGMP_IF_RAS_CLIENT. Changed from: The IGMP_MIB_GROUP_INFO structure is used in the IGMP_MIB_IF_GROUPS_LIST (section 2.2.1.2.176) structure. If the interface is of type RAS_SERVER then the group membership of all the RAS clients is summarized, and the GroupUpTime and GroupExpiryTime is the maximum over all member RAS clients, while the V1HostPresentTimeLeft is set to 0. If the interface is of type RAS_CLIENT, the IpAddr is the next hop IP address of the RAS client. The membership is summarized over the RAS clients unless the IGMP_ENUM_FOR_RAS_CLIENTS_ID flag is set in Flags. ... Changed to: The IGMP_MIB_GROUP_INFO structure is used in the IGMP_MIB_IF_GROUPS_LIST (section 2.2.1.2.175) structure. If the interface is of type IGMP_IF_RAS_SERVER then the group membership of all the RAS clients is summarized, and the GroupUpTime and GroupExpiryTime is the maximum over all member RAS clients, while the V1HostPresentTimeLeft is set to 0. If the interface is of type IGMP_IF_RAS_CLIENT, the IpAddr is the next hop IP address of the RAS client. The membership is summarized over the RAS clients unless the IGMP_ENUM_FOR_RAS_CLIENTS_ID flag is set in Flags. ... In Section 2.2.1.2.181, IP_NAT_MIB_QUERY, changed instances of RMIBGetEntryFirst to RMIBEntryGetFirst. Changed from: The IP_NAT_MIB_QUERY structure is used to retrieve Network Address Translator (NAT) information and is passed to the following methods: • RMIBEntryGet (section 3.1.4.30) • RMIBGetEntryFirst (section 3.1.4.31) • RMIBEntryGetNext (section 3.1.4.32) .... Oid: This is an index of the NAT MIB. It MUST be one of the following values.

Copyright © 2020 Microsoft Corporation

Errata Published *	Description

Value	Meaning
IP_NAT_INTERFACE_STATISTICS_OID 0x00000000	NAT interface statistics information is retrieved. When RMIBEntryGet, RMIBGetEntryFirst, and RMIBEntryGetNext return pMibOutEntry or pInfoStruct it MUST be typecast to IP_NAT_INTERFACE_STATISTICS (section 2.2.1.2.185).
IP_NAT_INTERFACE_MAPPING_TABLE_OID 0x00000001	NAT interface mapping table information. When RMIBEntryGet, RMIBGetEntryFirst, and RMIBEntryGetNext return pMibOutEntry or pInfoStruct it MUST be typecast to IP_NAT_ENUMERATE_SESSION_MAPPINGS (section 2.2.1.2.183).
IP_NAT_MAPPING_TABLE_OID 0x00000002	NAT mapping table information. Retrieves the session mappings of an interface. When RMIBEntryGet, RMIBGetEntryFirst, and RMIBEntryGetNext return pMibOutEntry or pInfoStruct it

Changed to:

The IP_NAT_MIB_QUERY structure is used to retrieve Network Address Translator (NAT) information and is passed to the following methods:

- RMIBEntryGet (section 3.1.4.30)
- RMIBEntryGetFirst (section 3.1.4.31)
- RMIBEntryGetNext (section 3.1.4.32)

...

Oid: This is an index of the NAT MIB. It MUST be one of the following values.

Value	Meaning
IP_NAT_INTERFACE_STATISTICS_OID 0x00000000	NAT interface statistics information is retrieved. When RMIBEntryGet, RMIBEntryGetFirst, and RMIBEntryGetNext return pMibOutEntry or pInfoStruct it MUST be typecast to IP_NAT_INTERFACE_STATISTICS (section 2.2.1.2.184).
IP_NAT_INTERFACE_MAPPING_TABLE_OID 0x00000001	NAT interface mapping table information. When RMIBEntryGet, RMIBEntryGetFirst, and RMIBEntryGetNext return pMibOutEntry or pInfoStruct it MUST be typecast to IP_NAT_ENUMERATE_SESSION_MAPPINGS (section 2.2.1.2.182).
IP_NAT_MAPPING_TABLE_OID 0x00000002	NAT mapping table information. Retrieves the session mappings of an interface. When RMIBEntryGet, RMIBEntryGetFirst, and RMIBEntryGetNext return pMibOutEntry or pInfoStruct it MUST be typecast to IP_NAT_ENUMERATE_SESSION_MAPPINGS.

In Section 2.2.1.2.260, BGP_POLICY, changed eType value from MatchMaxPrefix to MatchMaxPrefixes. And changed eAttrType values ModifyLocalPref to NewLocalPref, ModifyNextHop to NewNextHop, and ModifyMed to NewMed.

Changed from:

Copyright © 2020 Microsoft Corporation

Errata Published *	Description
	... A BGP policy: ● MUST NOT have more than one Match clause with eType in BGP_POLICY_MATCH set to MatchASNRange (0x3). ● MUST NOT have more than one Match clause with eType in BGP_POLICY_MATCH set to MatchMaxPrefix (0x5). ● MUST NOT have more than one modify Action clause with eAttrType in BGP_POLICY_MODIFY (section 2.2.1.2.259) set to ModifyLocalPref (0x3). ● MUST NOT have more than one modify Action clause with eAttrType in BGP_POLICY_MODIFY set to ModifyNextHop (0x4). ● MUST NOT have more than one modify Action clause with eAttrType in BGP_POLICY_MODIFY set to ModifyMed (0x5). ● MUST have only one Action clause with bDeny in BGP_POLICY_ACTION set to TRUE when a Match clause with eType in BGP_POLICY_MATCH is specified as MatchMaxPrefix (0x5). Changed to: ... A BGP policy: ● MUST NOT have more than one Match clause with eType in BGP_POLICY_MATCH set to MatchASNRange (0x3). ● MUST NOT have more than one Match clause with eType in BGP_POLICY_MATCH set to MatchMaxPrefixes (0x5). ● MUST NOT have more than one modify Action clause with eAttrType in BGP_POLICY_MODIFY (section 2.2.1.2.258) set to NewLocalPref (0x3). ● MUST NOT have more than one modify Action clause with eAttrType in BGP_POLICY_MODIFY set to NewNextHop (0x4). ● MUST NOT have more than one modify Action clause with eAttrType in BGP_POLICY_MODIFY set to NewMed (0x5). ● MUST have only one Action clause with bDeny in BGP_POLICY_ACTION set to TRUE when a Match clause with eType in BGP_POLICY_MATCH is specified as MatchMaxPrefixes (0x5). In Section 3.1.4.44, RMprAdminServerSetInfo (Opnum 43), changed return value ERROR_REBOOT_REQUIRED to ERROR_SUCCESS_REBOOT_REQUIRED when the RRAS server completes the processing successfully. Changed from: ... When processing this call, the RRASM server MUST do the following: ... ● If the RRAS server completes the processing successfully return either ERROR_SUCCESS or ERROR_REBOOT_REQUIRED<316> based on the impact of the configuration change as indicated by the RRAS server. Otherwise return the error status. ... Changed to: ... When processing this call, the RRASM server MUST do the following: ... ● If the RRAS server completes the processing successfully return either ERROR_SUCCESS or ERROR_SUCCESS_REBOOT_REQUIRED<316> based on the impact of the configuration change as indicated by the RRAS server. Otherwise return the error status. ...

Copyright © 2020 Microsoft Corporation

Errata Published *	Description
	In Section 3.1.4.48, RMprAdminServerSetInfoEx (Opnum 47), changed return value ERROR_REBOOT_REQUIRED to ERROR_SUCCESS_REBOOT_REQUIRED when the RRAS server completes the processing successfully. Changed from: ... When processing this call, the RRASM server MUST do the following: ... ● If the RRAS server completes the processing successfully, it MUST return either ERROR_SUCCESS, ERROR_REBOOT_REQUIRED<321>, or ERROR_RESTART_REQUIRED<322> based on the impact of the configuration change. Otherwise return the error status. ... Changed to: ... When processing this call, the RRASM server MUST do the following: ... ● If the RRAS server completes the processing successfully, it MUST return either ERROR_SUCCESS, ERROR_SUCCESS_REBOOT_REQUIRED<321>, or ERROR_RESTART_REQUIRED<322> based on the impact of the configuration change. Otherwise return the error status. ... In Section 3.4.4.5 RasRpcSubmitRequest (Opnum 12), changed instances of GetDevConfig to GetDevConfigStruct when describing client behavior for the ReqType REQTYPE_GETDEVCONFIG. Changed from: ... REQTYPE_GETDEVCONFIG Before calling the method, the client MUST set the GetDevConfig.size value to the size of the GetDevConfig.config buffer. If the returned GetDevConfig.retcode is set to ERROR_BUFFER_TOO_SMALL (0x0000025B), the buffer that was passed in was not big enough to hold the device configuration information. The client SHOULD again call the API with GetDevConfig.size set to the size of returned GetDevConfig.size. ... Changed to: ... REQTYPE_GETDEVCONFIG Before calling the method, the client MUST set the GetDevConfigStruct.size value to the size of the GetDevConfigStruct.config buffer. If the returned GetDevConfigStruct.retcode is set to ERROR_BUFFER_TOO_SMALL (0x0000025B), the buffer that was passed in was not big enough to hold the device configuration information. The client SHOULD again call the API with GetDevConfigStruct.size set to the size of returned GetDevConfigStruct.size. ...

Copyright © 2020 Microsoft Corporation

Errata Published *	Description
	In Section 7, Appendix B: Product Behavior, changed the return value ERROR_REBOOT_REQUIRED to ERROR_SUCCESS_REBOOT_REQUIRED in product behavior note <316> when the configuration change requires a reboot of the machine for the settings to be applied. Changed from: <316> Section 3.1.4.44: Windows will return the error value ERROR_REBOOT_REQUIRED when the configuration change requires a reboot of the machine for the settings to be applied. One such implementation requirement is when the number of ports configured is more than the maximum number of ports that the tunneling protocols are configured to support initially. Changed to: <316> Section 3.1.4.44: Windows will return the error value ERROR_SUCCESS_REBOOT_REQUIRED when the configuration change requires a reboot of the machine for the settings to be applied. One such implementation requirement is when the number of ports configured is more than the maximum number of ports that the tunneling protocols are configured to support initially. In this document, numerous editorial fixes have also been made, e.g., changed instances of "Ipv6" and "IPv6" to "IPV6"; changed instances of "GetDevConfig" to "GetDevConfigStruct"; updated hexadecimal syntax to USHORT 16-bit format; and also added section numbers to programming elements where applicable. Sections updated: 2.2.1.2.103 2.2.1.2.104 2.2.1.2.134 2.2.1.2.136 2.2.1.2.156 2.2.1.2.158 2.2.2.2.79 2.2.5.1.1 3.1.4.30 3.1.4.31 3.1.4.33 3.1.4.38 3.1.4.44 3.3.4.5 7 - the following product behavior notes were upated: <266> <268> <272> <290> <293> <298> <305>

Copyright © 2020 Microsoft Corporation

Errata Published *	Description
2019/10/28	In Section 2.2.1.2.37 MIB_IPMCAST_BOUNDARY, added names of dwStatus values in the table. Changed from: dwStatus: A status value that describes the current status of this entry in a mullticast forwarding entry (MFE) boundary table. Value Meaning 0x00000001 The entry has an active status. 0x00000002 The entry has a notInService status. 0x00000003 The entry has a notReady status. 0x00000004 The entry has a createAndGo status. 0x00000005 The entry has a createAndWait status. 0x00000006 The entry has a destroy status. Changed to: dwStatus: A status value that describes the current status of this entry in a multicast forwarding entry (MFE) boundary table. Value Meaning ROWSTATUS_ACTIVE 0x00000001 The entry has an active status. ROWSTATUS_NOTINSERVICE 0x00000002 The entry has a notInService status. ROWSTATUS_NOTREADY 0x00000003 The entry has a notReady status. ROWSTATUS_CREATEANDGO 0x00000004 The entry has a createAndGo status. ROWSTATUS_CREATEANDWAIT 0x00000005 The entry has a createAndWait status. ROWSTATUS_DESTROY 0x00000006 The entry has a destroy status.

Copyright © 2020 Microsoft Corporation

Errata Published *	Description
	Section 2.2.1.2.105 IPX_MIB_INDEX, added missing value 3 in the table. Changed from: TableId: Specifies the type of table. Values MUST be one of the following values. Value Meaning IPX_BASE_ENTRY 0x00000000 IPX base. See IPXMIB_BASE (section 2.2.1.2.107). IPX_INTERFACE_TABLE 0x00000001 IPX interface table. See IPX_INTERFACE (section 2.2.1.2.109). IPX_DEST_TABLE 0x00000002 IPX destination table. See IPX_ROUTE (section 2.2.1.2.110). IPX_SERV_TABLE 0x00000004 IPX service table. See IPX_SERVICE (section 2.2.1.2.121). IPX_STATIC_SERV_TABLE 0x00000005 IPX static service table. See IPX_STATIC_SERVICE_INFO (section 2.2.1.2.95). Changed to: TableId: Specifies the type of table. Values MUST be one of the following values. Value Meaning IPX_BASE_ENTRY 0x00000000 IPX base. See IPXMIB_BASE (section 2.2.1.2.106). IPX_INTERFACE_TABLE 0x00000001 IPX interface table. See IPX_INTERFACE (section 2.2.1.2.108). IPX_DEST_TABLE 0x00000002 IPX destination table. See IPX_ROUTE (section 2.2.1.2.109). IPX_STATIC_ROUTE_TABLE 0x00000003 IPX Static Route Table. See IPX_STATIC_ROUTE_INFO (section 2.2.1.2.93).

Copyright © 2020 Microsoft Corporation

Errata Published *	Description
	IPX_SERV_TABLE 0x00000004 IPX service table. See IPX_SERVICE (section 2.2.1.2.120). IPX_STATIC_SERV_TABLE 0x00000005 IPX static service table. See IPX_STATIC_SERVICE_INFO (section 2.2.1.2.94). Section 2.2.1.2.177 IGMP_MIB_GROUP_INFO, updated names of values in the introduction: RAS_SERVER to IGMP_IF_RAS_SERVER, RAS_CLIENT to IGMP_IF_RAS_CLIENT, and IGMP_ENUM_FOR_RAS_CLIENTS_ID to IGMP_ENUM_FOR_RAS_CLIENTS. Changed from: The IGMP_MIB_GROUP_INFO structure is used in the IGMP_MIB_IF_GROUPS_LIST (section 2.2.1.2.176) structure. If the interface is of type RAS_SERVER then the group membership of all the RAS clients is summarized, and the GroupUpTime and GroupExpiryTime is the maximum over all member RAS clients, while the V1HostPresentTimeLeft is set to 0. If the interface is of type RAS_CLIENT, the IpAddr is the next hop IP address of the RAS client. The membership is summarized over the RAS clients unless the IGMP_ENUM_FOR_RAS_CLIENTS_ID flag is set in Flags. Changed to: The IGMP_MIB_GROUP_INFO structure is used in the IGMP_MIB_IF_GROUPS_LIST (section 2.2.1.2.175) structure. If the interface is of type IGMP_IF_RAS_SERVER then the group membership of all the RAS clients is summarized, and the GroupUpTime and GroupExpiryTime is the maximum over all member RAS clients, while the V1HostPresentTimeLeft is set to 0. If the interface is of type IGMP_IF_RAS_CLIENT, the IpAddr is the next hop IP address of the RAS client. The membership is summarized over the RAS clients unless the IGMP_ENUM_FOR_RAS_CLIENTS_ID flag is set in Flags. Section 2.2.1.2.178 IGMP_MIB_IF_STATS, in the LastQuerierChangeTime description changed member name from igmpInterfaceQuerier to QuerierIpAddr. Changed from: LastQuerierChangeTime: The number of seconds since igmpInterfaceQuerier was last changed. Changed to: LastQuerierChangeTime: The number of seconds since QuerierIpAddr was last changed. Section 2.2.1.2.179 IGMP_MIB_GROUP_SOURCE_INFO_V3, added section. Adjusted references and reference numbers 2.2.1.2.180 to 2.2.1.2.271 throughout to compensate for section number changes. Changed from: (missing section) Changed to: The IGMP_MIB_GROUP_SOURCE_INFO_V3 structure provides information about each source IP endpoint.

Copyright © 2020 Microsoft Corporation

Errata Published *	Description

	typedef struct _IGMP_MIB_GROUP_SOURCE_INFO_V3 {
	
	DWORD Source;
	
	DWORD SourceExpiryTime;
	
	DWORD SourceUpTime;
	
	DWORD Flags;
	
	} IGMP_MIB_GROUP_SOURCE_INFO_V3, *PIGMP_MIB_GROUP_SOURCE_INFO_V3;
	
	Source: IP endpoint address of a source.
	
	SourceExpiryTime: The time, in seconds, that remains before source expires. Not valid for exclusion mode.
	
	SourceUpTime: The time, in seconds since the source was up.
	Flags: Reserved. This is unused and SHOULD be NULL, or MAY be set to 0x00000000.
	
	Section 2.2.1.2.180 IGMP_MIB_GROUP_INFO_V3, for Sources array of IGMP_MIB_GROUP_SOURCE_INFO_V3 added reference to 2.2.1.2.179.
	
	Changed from:
	
	NumSources: The number of entries of IGMP_MIB_GROUP_SOURCE_INFO_V3.
	
	Sources: The IGMP_MIB_GROUP_SOURCE_INFO_V3 structure.
	
	Changed to:
	
	NumSources: The number of entries of IGMP_MIB_GROUP_SOURCE_INFO_V3.
	Sources: The IGMP_MIB_GROUP_SOURCE_INFO_V3 structure (section 2.2.1.2.179).
	
	6 Appendix A: Full IDL, moved location of struct IGMP_MIB_GROUP_SOURCE_INFO_V3 to before struct IGMP_MIB_GROUP_INFO_V3.
	
	Changed from:
	
	typedef struct _IPRIP_PEER_STATS {
	
	DWORD PS_LastPeerRouteTag;
	
	DWORD PS_LastPeerUpdateTickCount;
	
	DWORD PS_LastPeerUpdateVersion;

Copyright © 2020 Microsoft Corporation

Errata Published *	Description

	DWORD PS_BadResponsePacketsFromPeer;
	DWORD PS_BadResponseEntriesFromPeer;
	} IPRIP_PEER_STATS, *PIPRIP_PEER_STATS;
	typedef struct _IGMP_MIB_GROUP_SOURCE_INFO_V3 {
	DWORD Source;
	DWORD SourceExpiryTime; //not valid for exclusion mode
	DWORD SourceUpTime;
	DWORD Flags;
	} IGMP_MIB_GROUP_SOURCE_INFO_V3, *PIGMP_MIB_GROUP_SOURCE_INFO_V3;
	typedef struct _IGMP_MIB_GET_INPUT_DATA {
	DWORD TypeId;
	USHORT Flags;
	USHORT Signature;
	DWORD IfIndex;
	DWORD RasClientAddr;
	DWORD GroupAddr;
	DWORD Count;
	} IGMP_MIB_GET_INPUT_DATA, *PIGMP_MIB_GET_INPUT_DATA;
	Changed to:
	typedef struct _IGMP_MIB_GROUP_IFS_LIST {
	DWORD GroupAddr;
	DWORD NumInterfaces;
	BYTE Buffer[1];

Copyright © 2020 Microsoft Corporation

Errata Published *	Description

	} IGMP_MIB_GROUP_IFS_LIST, *PIGMP_MIB_GROUP_IFS_LIST;
	typedef struct _IGMP_MIB_GROUP_SOURCE_INFO_V3 {
	DWORD Source;
	DWORD SourceExpiryTime; //not valid for exclusion mode
	DWORD SourceUpTime;
	DWORD Flags;
	} IGMP_MIB_GROUP_SOURCE_INFO_V3, *PIGMP_MIB_GROUP_SOURCE_INFO_V3;
	typedef struct _IGMP_MIB_GROUP_INFO_V3
	{
	union {
	DWORD IfIndex;
	DWORD GroupAddr;
	};
	DWORD IpAddr;
	DWORD GroupUpTime;
	DWORD GroupExpiryTime;
	DWORD LastReporter;
	DWORD V1HostPresentTimeLeft;
	DWORD Flags;
	//v3 additions
	DWORD Version; //1/2/3
	DWORD Size; //size of this struct
	DWORD FilterType;//EXCLUSION/INCLUSION

Copyright © 2020 Microsoft Corporation

Errata Published *	Description
	DWORD V2HostPresentTimeLeft; DWORD NumSources; //IGMP_MIB_GROUP_SOURCE_INFO_V3 Sources[0]; } IGMP_MIB_GROUP_INFO_V3, *PIGMP_MIB_GROUP_INFO_V3;

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-RRP]: Windows Remote Registry Protocol

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

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

RSS
Atom

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

September 12, 2018 - Download

March 4, 2020 - Download

Errata below are for Protocol Document Version V35.0 – 2020/03/04.

Errata Published*	Description
2020/04/27	In Section 3.1.5.7, BaseRegCreateKey (Opnum 6), we corrected hKEY to hKey in the explanatory text. Changed from: The server then checks to see if the key specified by the hKEY parameter is a key that can only be operated on in the 64-bit key namespace (KEYS64). See section 3.1.1.4. Changed to: The server then checks to see if the key specified by the hKey parameter is a key that can only be operated on in the 64-bit key namespace (KEYS64). See section 3.1.1.4. In Section 3.1.5.15, BaseRegOpenKey (Opnum 15), we corrected hKEY to hKey in the explanatory text. Changed from: The server then checks to see if the key specified by the hKEY parameter is a key that can only be operated on in the 64-bit key namespace (KEYS64). See section 3.1.1.4. Changed to: The server then checks to see if the key specified by the hKey parameter is a key that can only be operated on in the 64-bit key namespace (KEYS64). See section 3.1.1.4. In Section 3.1.5.22, BaseRegSetValue (Opnum 22), we corrected hKEY to hKey in the explanatory text. Changed from:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	If the key specified by hKEY has a KEYTYPE of symbolic link and lpValueName is specified to any string other than "SymbolicLinkValue", the server MUST fail the method and return ERROR_ACCESS_DENIED. ... The server MUST determine if the key path indicated by hKey refers to a path that is within the list of paths for which updates to either the 32-bit or 64-bit namespaces are copied into the 64-bit or 32-bit namespace, respectively, as specified in section 3.1.1.4. If the key indicated by hKey is within one of the paths, the server MUST set the UPDATECOPY column of the HANDLETABLE for the row indicated by hKEY to TRUE. This indicates that the value is copied between the 32-bit and 64-bit key namespaces when the handle is closed. ... The server MUST set the KEYISMODIFIED property of the key indicated by hKEY to TRUE. Changed to: If the key specified by hKey has a KEYTYPE of symbolic link and lpValueName is specified to any string other than "SymbolicLinkValue", the server MUST fail the method and return ERROR_ACCESS_DENIED. ... The server MUST determine if the key path indicated by hKey refers to a path that is within the list of paths for which updates to either the 32-bit or 64-bit namespaces are copied into the 64-bit or 32-bit namespace, respectively, as specified in section 3.1.1.4. If the key indicated by hKey is within one of the paths, the server MUST set the UPDATECOPY column of the HANDLETABLE for the row indicated by hKey to TRUE. This indicates that the value is copied between the 32-bit and 64-bit key namespaces when the handle is closed. ... The server MUST set the KEYISMODIFIED property of the key indicated by hKey to TRUE. In Section 3.1.5.31, BaseRegDeleteKeyEx (Opnum 35), we corrected hKEY to hKey in the explanatory text. Changed from: The server MUST then check to see if the key specified by the hKEY parameter is a key that can only be operated on in the 64-bit key namespace (KEYS64). See section 3.1.1.4. Changed to: The server MUST then check to see if the key specified by the hKey parameter is a key that can only be operated on in the 64-bit key namespace (KEYS64). See section 3.1.1.4. In Section 3.1.5.26, BaseRegQueryMultipleValues (Opnum 29), we corrected valListOut to val_listOut and valListIn to val_listIn in the explanatory text.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Changed from: If any one of the parameters ldwTotsize and valListOut is NULL, the server MUST return ERROR_INVALID_PARAMETER. ... For each of the RVALENT structures returned by calling parameter valListIn: if the return value is greater than zero and the buffer is NULL, the server MUST return ERROR_INVALID_PARAMETER Changed to: If any one of the parameters ldwTotsize and val_listOut is NULL, the server MUST return ERROR_INVALID_PARAMETER. ... For each of the RVALENT structures returned by calling parameter val_listIn: if the return value is greater than zero and the buffer is NULL, the server MUST return ERROR_INVALID_PARAMETER In Section 3.1.5.30, BaseRegQueryMultipleValues2 (Opnum 34), we corrected valListOut to val_listOut and valListIn to val_listIn in the explanatory text. Changed from: If any one of the parameters ldwTotsize, ldwRequiredSize, and valListOut is NULL, the server MUST return ERROR_INVALID_PARAMETER. ... For each of the RVALENT structures returned by calling the valListIn parameter: if the return value is greater than zero and the buffer is NULL, the server MUST return ERROR_INVALID_PARAMETER Changed to: If any one of the parameters ldwTotsize, ldwRequiredSize, and val_listOut is NULL, the server MUST return ERROR_INVALID_PARAMETER. ... For each of the RVALENT structures returned by calling the val_listIn parameter: if the return value is greater than zero and the buffer is NULL, the server MUST return ERROR_INVALID_PARAMETER In Sections 3.1.5.10, BaseRegEnumKey (Opnum 9), 3.1.5.11 BaseRegEnumValue (Opnum 10), 3.1.5.14 BaseRegLoadKey (Opnum 13), and 3.1.5.22 BaseRegSetValue (Opnum 22), we

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	corrected links to the top-level Section 3.1.1 to more appropriate child sections for key and value names. In Section 3.1.5.16, BaseRegQueryInfoKey (Opnum 16), we corrected lpcSubkeys to lpcSubKeys in the explanatory text. Changed from: The server MUST return a pointer to the variable that contains the number of subkeys for the specified key in the lpcSubkeys parameter. If there are no subkeys under the key indicated by hKey, the server MUST set this value to 0. Changed to: The server MUST return a pointer to the variable that contains the number of subkeys for the specified key in the lpcSubKeys parameter. If there are no subkeys under the key indicated by hKey, the server MUST set this value to 0.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

September 26, 2016 - Download

March 20, 2017 - Download

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

Errata below are for Protocol Document Version V40.0 – 2018/09/12.

Errata Published*	Description
2019/05/27	In Section 2.1, Transport, changed from: The server SHOULD use this identity to perform method-specific access checks, as specified in the message processing section of each method.<11> The server SHOULD<12> reject calls that do not use an authentication level of either RPC_C_AUTHN_LEVEL_NONE or RPC_C_AUTHN_LEVEL_PKT_PRIVACY (see [MS-RPCE] section 2.2.1.1.8). Changed to: The server SHOULD use this identity to perform method-specific access checks, as specified in the message processing section of each method.<11> RPC clients for this protocol MUST use authentication level RPC_C_AUTHN_LEVEL_NONE when invoking RPC over SMB methods. The server SHOULD<12> reject calls that do not use an authentication level of either RPC_C_AUTHN_LEVEL_NONE or RPC_C_AUTHN_LEVEL_PKT_PRIVACY (see [MS-RPCE] section 2.2.1.1.8).

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

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

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

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

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[MS-SCMR]: Service Control Manager Remote Protocol

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

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

RSS
Atom

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:

September 12, 2018 - Download

September 23, 2019 - Download

Copyright © 2020 Microsoft Corporation

[MS-SHLLINK]: Shell Link (.LNK) Binary File Format

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

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

RSS
Atom

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:

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 20, 2017 - Download

Copyright © 2020 Microsoft Corporation

[MS-SFU]: Kerberos Protocol Extensions Service for User and Constrained Delegation Protocol

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

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

RSS
Atom

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 4, 2020 - Download

November 23, 2020 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

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

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

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

RSS
Atom

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

March 4, 2020 - Download

August 24, 2020 – Download

Errata below are for Protocol Document Version V61.0 - 2020/08/26

Errata Published*	Description
2021/03/22	The following sections were updated for processing rules on unauthenticated session. Section 3.3.1.5 Global Section 3.3.1.7 Per Transport Connection Section 3.3.3 Initialization Section 3.3.5.1 Accepting an Incoming Connection Section 3.3.5.2.9 Verifying the Session Section 3.3.5.5.3 Handling GSS-API Authentication For details, please see the diff file.
2021/03/22	In Section 3.2.4.1.1 Signing the Message, the following was updated. Changed from: The client MUST sign the message under the following conditions: • If the request message being sent contains a nonzero value in the SessionId field, the session identified by the SessionId has Session.SigningRequired equal to TRUE and either the request is a TREE_CONNECT request or the tree connection identified by the TreeId field has TreeConnect.EncryptData equal to FALSE. • If Connection.Dialect is "3.1.1" and the message being sent is a TREE_CONNECT Request and the session identified by SessionId has Session.EncryptData equal to FALSE. If Session.SigningRequired is FALSE, the client MAY<92> sign the request. Changed to: The client MUST sign the message if one of the following conditions is TRUE:

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>• If Connection.Dialect is equal to "2.0.2" or "2.1", the message being sent contains a nonzero value in the SessionId field, and the session identified by the SessionId has Session.SigningRequired equal to TRUE.

• If Connection.Dialect belongs to the SMB 3.x dialect family, the message being sent contains a nonzero value in the SessionId field and one of the following conditions is TRUE:

● The session identified by SessionId has Session.EncryptData equal to FALSE.

● The tree connection identified by the TreeId field has TreeConnect.EncryptData equal to FALSE.
If Session.SigningRequired is FALSE, the client MAY<92> sign the request.</td></tr>
<tr><td>2021/03/08</td><td>In section 6, Appendix A: Product Behavior, behavior note 349 was updated for allowed FSCTLs:

Changed from:

Windows 10 v20H2 and later and Windows Server v20H2 and later allow the additional CtlCode value, as specified in [MS-FSCC].
<table>
<tr><th>FSCTL name</th><th>FSCTL function number</th></tr>
<tr><td>FSCTL_GET_RETRIEVAL_POINTERS_AND_REFCOUNT</td><td>0x903D3</td></tr>
<tr><td>FSCTL_GET_RETRIEVAL_POINTER_COUNT</td><td>0x9042B</td></tr>
</table>

Changed to:

Windows 10 v20H2 and later and Windows Server v20H2 and later allow the additional CtlCode value, as specified in [MS-FSCC].
<table>
<tr><th>FSCTL name</th><th>FSCTL function number</th></tr>
<tr><td>FSCTL_GET_RETRIEVAL_POINTER_COUNT</td><td>0x9042B</td></tr>
</table></td></tr>
<tr><td>2021/02/08</td><td>In Section 2.2.3, SMB2 NEGOTIATE Request, the description of SMB2_NEGOTIATE_SIGNING_ENABLED was updated:

Changed from:

When set, indicates that security signatures are enabled on the client. The client MUST set this bit if the SMB2_NEGOTIATE_SIGNING_REQUIRED bit is not set, and MUST NOT set this bit if the SMB2_NEGOTIATE_SIGNING_REQUIRED bit is set. The server MUST ignore this bit.

Changed to:

When set, indicates that security signatures are enabled on the client. The server MUST ignore this bit.</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	In Section 2.2.5, SMB2 SESSION_SETUP Request, the description of SMB2_NEGOTIATE_SIGNING_ENABLED was updated: Changed from: When set, indicates that security signatures are enabled on the client. The client MUST set this bit if the SMB2_NEGOTIATE_SIGNING_REQUIRED bit is not set, and MUST NOT set this bit if the SMB2_NEGOTIATE_SIGNING_REQUIRED bit is set. The server MUST ignore this bit. Changed to: When set, indicates that security signatures are enabled on the client. The server MUST ignore this bit. In Section 2.2.10, SMB2 TREE_CONNECT Response, the description of SMB2_SHAREFLAG_DFS, SMB2_SHAREFLAG_DFS_ROOT and SMB2_SHARE_CAP_DFS were updated: Changed from: SMB2_SHAREFLAG_DFS: The specified share is present in a Distributed File System (DFS) tree structure. The server SHOULD set the SMB2_SHAREFLAG_DFS bit in the ShareFlags field if the per-share property Share.IsDfs is TRUE. SMB2_SHAREFLAG_DFS_ROOT: The specified share is present in a DFS tree structure. The server SHOULD set the SMB2_SHAREFLAG_DFS_ROOT bit in the ShareFlags field if the per-share property Share.IsDfs is TRUE. SMB2_SHARE_CAP_DFS: The specified share is present in a DFS tree structure. The server MUST set the SMB2_SHARE_CAP_DFS bit in the Capabilities field if the per-share property Share.IsDfs is TRUE. Changed to: SMB2_SHAREFLAG_DFS: The specified share is present in a Distributed File System (DFS) tree structure. SMB2_SHAREFLAG_DFS_ROOT: The specified share is present in a DFS Root (as specified in [MS-DFSC]) tree structure SMB2_SHARE_CAP_DFS: The specified share is present in a DFS tree structure.
2021/01/11	In Section 3.3.5.9.7 Handling the SMB2_CREATE_DURABLE_HANDLE_RECONNECT Create Context the following bullet points were added under step 6 ● Open.IsDurable is TRUE, Open.Lease is NULL, and Open.OplockLevel is not equal to SMB2_OPLOCK_LEVEL_BATCH. ● Open.IsDurable is TRUE and Open.Lease.LeaseState does not contain SMB2_LEASE_HANDLE_CACHING.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	In Section 3.3.5.9.12 Handling the SMB2_CREATE_DURABLE_HANDLE_RECONNECT_V2 Create Context the following was updated: Changed from: There is no processing done for "Path Name Validation" or "Open Execution" as listed in section 3.3.5.9. Changed to: There is no processing done for "Path Name Validation" as listed in section 3.3.5.9. The following bullet points were added: ... ● Open.Lease is NULL and the SMB2_CREATE_REQUEST_LEASE or SMB2_CREATE_REQUEST_LEASE_V2 create context is present. ● Open.Lease is NOT NULL and the SMB2_CREATE_REQUEST_LEASE or SMB2_CREATE_REQUEST_LEASE_V2 create context is not present. ● The SMB2_CREATE_REQUEST_LEASE_V2 create context is also present in the request, the server supports directory leasing, and Open.Lease.LeaseKey does not match the LeaseKey provided in the SMB2_CREATE_REQUEST_LEASE_V2 create context. ... To ... ● Open.Lease is NULL and the SMB2_CREATE_REQUEST_LEASE or SMB2_CREATE_REQUEST_LEASE_V2 create context is present. ● Open.IsDurable is TRUE, Open.Lease is NULL, and Open.OplockLevel is not equal to SMB2_OPLOCK_LEVEL_BATCH. ● Open.Lease is NOT NULL and the SMB2_CREATE_REQUEST_LEASE or SMB2_CREATE_REQUEST_LEASE_V2 create context is not present. ● Open.IsDurable is TRUE and Open.Lease.LeaseState does not contain SMB2_LEASE_HANDLE_CACHING. ● The SMB2_CREATE_REQUEST_LEASE_V2 create context is also present in the request, the server supports directory leasing, and Open.Lease.LeaseKey does not match the LeaseKey provided in the SMB2_CREATE_REQUEST_LEASE_V2 create context. ... The following bullet point was changed from: ● The server MUST ignore the DesiredAccess, ShareAccess, and CreateOptions fields in the request. To ● If the SMB2_DHANDLE_FLAG_PERSISTENT bit in the Flags field of the SMB2_CREATE_DURABLE_HANDLE_RECONNECT_V2 create context is not set, the server MUST ignore the DesiredAccess, ShareAccess, and CreateOptions fields in the request.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
2020/11/23	In Section 2.2.26 SMB2 LOCK Request, the description of LockSequenceNumber and LockSequenceIndex have been updated. Changed from: LSN – LockSequenceNumber (4 bits): In the SMB 2.0.2 dialect, this field is unused and MUST be 0. The client MUST set this to 0, and the server MUST ignore it on receipt. In all other dialects, a 4-bit integer value. LockSequenceIndex (28 bits): In the SMB 2.0.2 dialect, this field is unused and MUST be 0. The client MUST set this to 0, and the server MUST ignore it on receipt. In all other dialects, a 28-bit integer value that MUST contain a value from 0 to 64, where 0 is reserved. Changed to: LockSequenceNumber,LockSequenceIndex (4 bytes): A 32-bit unsigned integer. In the SMB 2.0.2 dialect, this field is unused and MUST be reserved. The client MUST set this to 0, and the server MUST ignore it on receipt. In all other dialects, this field is interpreted as LockSequenceNumber and LockSequenceIndex fields. LockSequenceNumber (4 bits): The 4 least significant bits of this field containing integer value. LockSequenceIndex (28 bits): A 28-bit integer value that MUST contain a value from 0 to 64, where 0 is reserved.
2020/11/23	The following sections were updated for chained and unchained compression: Section 2.2.42 SMB2 COMPRESSION_TRANSFORM_HEADER Section 2.2.42.1 SMB2_COMPRESSION_PAYLOAD_HEADER Section 3.2.5.1.1.2 Decompressing the Message Section 3.3.5.2.1.2 Decompressing the Message In Section 3.1.4.4 Compressing the Message, all instances of "SMB2_COMPRESSION_TRANSFORM_HEADER" have been changed to "SMB2_COMPRESSION_TRANSFORM_HEADER_UNCHANED" and all instances of "SMB2_COMPRESSION_PAYLOAD_HEADER" have been changed to "SMB2_COMPRESSION_CHAINED_PAYLOAD_HEADER" In Section3.1.5.3 Decompressing the Chained Message, all instances of "SMB2_COMPRESSION_PAYLOAD_HEADER" have been changed to "SMB2_COMPRESSION_CHAINED_PAYLOAD_HEADER" and all instances of "SMB2_COMPRESSION_TRANSFORM_HEADER" have been changed to "SMB2_COMPRESSION_TRANSFORM_HEADER_CHAINED". For details, please see the diff file.
2020/11/23	In Section 2.2.2.2.2 Share Redirect Error Context Response, field descriptions have been updated. Changed from: StructureSize (4 bytes): This field MUST be set to the size of the structure. NotificationType (4 bytes): This field MUST be set to 3. ResourceNameOffset (4 bytes): The offset from the start of this structure to the ResourceName field.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	ResourceNameLength (4 bytes): The length of the share name provided in the ResourceName field, in bytes. Flags (2 bytes): This field MUST be set to zero. TargetType (2 bytes): This field MUST be set to zero. IPAddrCount (4 bytes): The number of MOVE_DST_IPADDR structures in the IPAddrMoveList field. IPAddrMoveList (variable): Array of MOVE_DST_IPADDR structures, as specified in section 2.2.2.2.2.1. ResourceName (variable): Name of the share as a counted Unicode string, as specified in [MS-DTYP] section 2.3.10. Changed to: StructureSize (4 bytes): This field MUST be set 48, indicating the size of this structure with a single MOVE_DST_IPADDR structure. This value is set regardless of the number of MOVE_DST_IPADDR structures returned and the length of ResourceName field. NotificationType (4 bytes): This field indicates the notification type and MUST be set to 3 (SHARE_MOVE_NOTIFICATION) defined in [MS-SWN] section 2.2.2.4. ResourceNameOffset (4 bytes): The offset from the start of this structure to the ResourceName field. ResourceNameLength (4 bytes): The length of the share name provided in the ResourceName field, in bytes. Reserved (2 bytes): This field MUST NOT be used and MUST be reserved. This field MUST be set to zero and MUST be ignored on receipt. TargetType (2 bytes): This field indicates the target is an IP address MUST be set to zero. IPAddrCount (4 bytes): The number of MOVE_DST_IPADDR structures in the IPAddrMoveList field. IPAddrMoveList (variable): Array of MOVE_DST_IPADDR structures, as specified in section 2.2.2.2.2.1. ResourceName (variable): A Unicode string containing the share name. In Section 2.2.2.2.2.1 MOVE_DST_IPADDR structure, the description of the values in the Type field have been updated. Changed from: Value Meaning MOVE_DST_IPADDR_V4 0x00000001 The type of destination IP address in this structure is IPv4 address. The fields after Reserved field in this structure are interpreted as IPv4Address followed by Reserved2 as described below. MOVE_DST_IPADDR_V6 0x00000002 The type of destination IP address in this structure is IPv6 address. The field after Reserved field in this structure is interpreted as IPv6Address as described below. Changed to: Value Meaning MOVE_DST_IPADDR_V4 0x00000001 The type of destination IP address in this structure is IPv4 address. MOVE_DST_IPADDR_V6

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	0x00000002 The type of destination IP address in this structure is IPv6 address.
2020/11/10	In Section 3.2.1.1 Global, added ShareList element. In Section 3.2.1.3 Per Session, added IsAnonymous and IsGuest Boolean session elements. In Section 3.2.1.10 Per Share, added Section. In Section 3.2.3 Initialization, added ShareList element setting. In Section 3.2.4.1.8 Encrypting the Message, added processing for IsAnonymous and IsGuest user sessions. In Section 3.2.5.3.1 Handling a New Authentication, added processing for IsAnonymous and IsGuest user sessions. In Section 3.2.5.5 Receiving an SMB2 TREE_CONNECT Response, added processing for the ShareList element. In Section 3.3.5.2.1.1 Decrypting the Message, added processing for IsAnonymous and IsGuest user sessions. Please see the diff pdf file for details.
2020/10/26	In Section 3.3.4.1.5 Compressing the Message, the processing rules for Connection.CompressionIds was updated. Changed from: If Connection.Dialect is 3.1.1, IsCompressionSupported is TRUE, Connection.CompressionIds is not empty, and Request.CompressReply is TRUE, the server MUST process the message as specified in section 3.1.4.4, before sending it to the client. Changed to: If Connection.Dialect is 3.1.1, IsCompressionSupported is TRUE, Connection.CompressionIds is not empty, and Request.CompressReply is TRUE, the server SHOULD<206> process the message as specified in section 3.1.4.4, before sending it to the client. <206> Section 3.3.4.1.5: Windows 10 v2004, Windows 10 v20H2, Windows Server v2004, and Windows Server v20H2 do not compress the message if Connection.CompressionIds does not include LZNT1, LZ77 and LZ77+Huffman algorithms.
2020/10/12	In section 3.3.5.4 Receiving an SMB2 NEGOTIATE Request the processing rules for CompressionAlgorithmCount and CompressionAlgorithms were updated. Changed from: • Set CompressionAlgorithmCount to 1. • Set CompressionAlgorithms to “NONE”.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Changed to: ● The server SHOULD<251> set CompressionAlgorithmCount to 1. ● The server SHOULD<252> set CompressionAlgorithms to "NONE". <251> Section 3.3.5.4: Windows 10 v2004 and Windows Server v2004 set CompressionAlgorithmCount to 0. <252> Section 3.3.5.4: Windows 10 v2004 and Windows Server v2004 set CompressionAlgorithms to empty.
2020/09/28	In Section 2.2.13 SMB2 CREATE Request, the Buffer field was changed. Changed from: Buffer (variable): A variable-length buffer that contains the Unicode file name and create context list, as defined by NameOffset, NameLength, CreateContextsOffset, and CreateContextsLength. In the request, the Buffer field MUST be at least one byte in length. The file name (after DFS normalization if needed) MUST conform to the specification of a relative pathname in [MS-FSCC] section 2.1.5. Changed to: Buffer (variable): A variable-length buffer that contains the Unicode file name and create context list, as defined by NameOffset, NameLength, CreateContextsOffset, and CreateContextsLength. In the request, the Buffer field MUST be at least one byte in length. In Section 3.2.4.3 Application Requests Opening a File, was updated with the following processing rule: The client MUST conform to the specification in [MS-FSCC] section 2.1.5 for the application-supplied path name. In Section 3.3.5.9 Receiving an SMB2 CREATE Request, was updated with the following processing rules: The server MUST fail the request with STATUS_INVALID_PARAMETER in the following cases: ● If NameLength number of bytes in the Buffer field extends beyond the CREATE request received. ● If NameLength is not a multiple of 2. ● If NameOffset is less than the Buffer field offset. Product behavior note 266 was updated. Changed from:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	<266> Section 3.3.5.9: Windows-based servers fail the CREATE request with STATUS_INVALID_PARAMETER if the file name in the Buffer field of the request begins in the form "subfolder\..\", for example "x\..\y.txt". Changed to: <266> Section 3.3.5.9: Windows-based servers accept the path names containing Dot Directory Names specified in [MS-FSCC]: section 2.1.5.1 and attempt to normalize the path name by removing the pathname components of "." and "..". Windows-based servers fail the CREATE request with STATUS_INVALID_PARAMETER if the file name in the Buffer field of the request begins in the form "subfolder\..\", for example "x\..\y.txt".
2020/09/28	In Section 3.2.5.2 Receiving an SMB2 NEGOTIATE Response, the processing rules for compression were updated. Changed from: ... ● For each algorithm in CompressionAlgorithms, if the value of algorithm is greater than 32, the client MUST return an error to the calling application. ● If there is a duplicate value in CompressionAlgorithms, the client MUST return an error to the calling application. ● If CompressionAlgorithmCount is 1 and CompressionAlgorithms contains “NONE”, the client MUST set Connection.CompressionIds to an empty list. ... Changed to: ... ● For each algorithm in CompressionAlgorithms, if the value of algorithm is greater than or equal to 32, the client MUST return an error to the calling application. ● If there is a duplicate value in CompressionAlgorithms, the client MUST return an error to the calling application. ● If CompressionAlgorithmCount is 1 and CompressionAlgorithms contains “NONE”, the client SHOULD<162> set Connection.CompressionIds to an empty list. <162> Section 3.2.5.2: Windows 10 v1903 through Windows 10 v20H2 and Windows Server v1903 through Windows Server v20H2 will disconnect the connection. ...
2020/09/28	In Section 2.2.19 SMB2 READ Request, the following was changed from: Changed from:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	MinimumCount (4 bytes): The minimum number of bytes to be read for this operation to be successful. If fewer than the minimum number of bytes are read by the server, the server MUST return an error rather than the bytes read. Changed to: MinimumCount (4 bytes): The minimum number of bytes to be read for this operation to be successful. In Section 3.2.4.6 Application Requests Reading from a File or Named Pipe, the following was changed from: Changed from: ● The MinimumCount field is set to the value that is provided by the application. If no value is provided by the application, the client MUST set this field to 0. Changed to: ● The client SHOULD<127> set MinimumCount field to the value that is provided by the application. If no value is provided by the application, the client SHOULD set this field to 0. <127> Section 3.2.4.6: Windows-based clients set MinimumCount field to 0. In Section 3.3.5.12 Receiving an SMB2 READ Request, the following was changed from: Changed from: ● DataOffset MUST be set to the offset into the response, in bytes, from the beginning of the SMB2 header where the data is located. ● The data MUST be copied into the response. ● DataLength MUST be set to the number of bytes returned. ● DataRemaining MUST be set to zero. ... ● The data MUST be sent via the processing specified in [MS-SMBD] section 3.1.4.5 RDMA Write to Peer Buffer, providing the Connection, the data, and the array of SMB_DIRECT_BUFFER_DESCRIPTOR_V1 structures passed in the request at offset ReadChannelInfoOffset and of length ReadChannelInfoLength fields. ● The DataOffset field MUST be set to the offset into the response, in bytes, from the beginning of the SMB2 header to the Buffer field. ● The data MUST NOT be copied into the response.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	• DataRemaining MUST be set to the number of bytes returned via RDMA. <317> Section 3.3.5.12: Windows reads from a file with Server Requests a Read [MS-FSA] section 2.1.5.2. Object Store parameter SMB2 parameter ByteOffset ByteOffset ByteCount ByteCount Open Open.Local Key 0 Unbuffered Set to TRUE if SMB2_READFLAG_READ_UNBUFFERED is set in the Flags field of the request, otherwise set to FALSE. Changed to: If the read fails, the server MUST fail the request using the error code received from the read operation. If the underlying object store returns fewer bytes than specified by the MinimumCount field of the request, the server MUST fail the request with STATUS_END_OF_FILE. If the read succeeds, the server MUST construct a read response using the syntax specified in section 2.2.20 with the following values. If the request Channel field contains the value SMB2_CHANNEL_NONE, then: • DataOffset MUST be set to the offset into the response, in bytes, from the beginning of the SMB2 header where the data is located. • If the number of bytes returned from the underlying object store is more than the Length field in the request, DataLength MUST be set to the Length field of the request. Otherwise, DataLength MUST be set to the number of bytes returned from the underlying object store. • The data MUST be copied into the response. • DataRemaining MUST be set to zero. ... • The DataOffset field MUST be set to the offset into the response, in bytes, from the beginning of the SMB2 header to the Buffer field. • If the number of bytes returned from the underlying object store is more than the Length field in the request, DataRemaining MUST be set to the Length field of the request. Otherwise, DataRemaining MUST be set to the number of bytes returned from the underlying object store.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	• The data MUST NOT be copied into the response. • The data MUST be sent via the processing specified in [MS-SMBD] section 3.1.4.5, providing the Connection, the data, and the array of SMB_DIRECT_BUFFER_DESCRIPTOR_V1 structures passed in the request at offset ReadChannelInfoOffset and of length ReadChannelInfoLength fields. <317> Section 3.3.5.12: Windows reads from a file with Server Requests a Read [MS-FSA] section 2.1.5.2. Object Store parameter SMB2 parameter ByteOffset Offset ByteCount Length Open Open.Local Key 0 Unbuffered Set to TRUE if SMB2_READFLAG_READ_UNBUFFERED is set in the Flags field of the request, otherwise set to FALSE.
2020/08/31	In MS-SMB2 Section 6 Appendix A: Product Behavior, note 133 has been changed. Changed from: <133> Section 3.2.4.9: In a SET_INFO request where FileInfoClass is set to FileRenameInformation, and the size of the buffer is less than 24, Windows clients pad the buffer to 24 bytes. These padding bytes are set to arbitrary values. Windows Vista SP1, Windows Server 2008, Windows 7, and Windows Server 2008 R2 clients append up to 4 additional padding bytes set to arbitrary values. Changed to: <133> Section 3.2.4.9: In a SET_INFO request where FileInfoClass is set to FileRenameInformation, Windows Vista SP1, Windows Server 2008, Windows 7, and Windows Server 2008 R2 clients append up to 4 additional padding bytes set to arbitrary values.
2020/08/31	In Section 3.3.5.9 Receiving an SMB2 CREATE Request, the following was updated Changed from: If the file name length is greater than zero and the first character is a path separator character, the server MUST fail the request with STATUS_INVALID_PARAMETER. If the file name fails to conform with the specification of a relative pathname in [MS-FSCC] section 2.1.5, the server MUST fail the request with STATUS_OBJECT_NAME_INVALID. Changed to:

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	If the file name in the Buffer field of the request fails to resolve the pathname components as specified in [MS-FSCC] section 2.1.5.1, the server SHOULD<262> fail the request with STATUS_INVALID_PARAMETER. <262> Section 3.3.5.9: Windows-based servers fail the CREATE request with STATUS_INVALID_PARAMETER if the file name in the Buffer field of the request begins in the form "subfolder\..\", for example "x\..\y.txt".

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 V12.0 – 2018/09/12.

Errata Published*	Description
2019/11/11	In Section 2.2.3.1, Buffer Descriptor V1 Structure, changed the structure name from SMB_DIRECT_BUFFER_DESCRIPTOR_1 to SMB_DIRECT_BUFFER_DESCRIPTOR_V1. Changed from: The SMB_DIRECT_BUFFER_DESCRIPTOR_1 structure represents a registered RDMA buffer and is used to Advertise the source and destination of RDMA Read and RDMA Write operations, respectively. The upper layer optionally embeds one or more of these structures in its payload when requesting RDMA direct placement of peer data via the protocol. ... Changed to: The SMB_DIRECT_BUFFER_DESCRIPTOR_V1 structure represents a registered RDMA buffer and is used to Advertise the source and destination of RDMA Read and RDMA Write operations, respectively. The upper layer optionally embeds one or more of these structures in its payload when requesting RDMA direct placement of peer data via the protocol. ...
2019/11/11	In Section 3.1.5.1, Sending Upper Layer Messages, the following was changed from: ... The new messages to be sent, if any, MUST be appended to the list of messages in the Connection.SendQueue. If there are no messages to be sent and Connection.SendImmediate is TRUE, a newly constructed Data Transfer Message MUST be added to Connection.SendQueue. • the credit processing specified in section 3.1.5.9 MUST be performed, and the CreditsGranted field of the first message in Connection.SendQueue MUST be incremented by the number of new credits returned. For each message in Connection.SendQueue: • If Connection.SendCredits is 0, stop processing messages, and break the loop. • If Connection.SendCredits is 1 and the CreditsGranted field of the message is 0, then at least one credit MUST be granted to the peer to prevent deadlock. If the processing specified in section 3.1.5.9 returns zero, stop processing Sends, and break the loop. Otherwise,

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	increment the CreditsGranted field of the current first message in Connection.SendQueue by the number of new credits returned. ● The first message MUST be removed from Connection.SendQueue. ● The value of Connection.SendCredits MUST be decremented by one. ● The value of the CreditsRequested field of the message MUST be set to Connection.SendCreditTarget. ● If Connection.KeepaliveRequested is "PENDING", the Flags field of the message MUST be set to SMB_DIRECT_RESPONSE_REQUESTED, Connection.KeepaliveRequested MUST be set to "SENT", and the Idle Connection Timer SHOULD<3> be set to an implementation-specific value. Otherwise, the Flags field of the message MUST be set to 0x0000. ● If the message to be sent was provided with an optional remote memory token to be invalidated on the receiving peer, the token SHOULD be provided in an implementation-specific manner to the RDMA provider when sending. If sending of remote invalidation is not supported by the RDMA provider, the token MAY be ignored. ● The message MUST be sent on the connection in an implementation-specific manner, and any error MUST be returned to the caller. ● If Connection.SendQueue is empty, Connection.SendImmediate MUST be set to FALSE and success MUST be returned to the caller. Changed to: ... For each message in Connection.SendQueue: ● If Connection.SendCredits is 0, stop processing. ● If CreditsGranted field of the first message in Connection.SendQueue is zero, the credit processing specified in section 3.1.5.9 MUST be performed, and the CreditsGranted field of the message MUST be set to the number of new credits returned. ● If Connection.SendCredits is 1 and the CreditsGranted field of the message is 0, stop processing. ● The first message MUST be removed from Connection.SendQueue. ● The value of Connection.SendCredits MUST be decremented by one. ● The value of the CreditsRequested field of the message MUST be set to Connection.SendCreditTarget. ● If Connection.KeepaliveRequested is "PENDING", the Flags field of the message MUST be set to SMB_DIRECT_RESPONSE_REQUESTED, Connection.KeepaliveRequested MUST be set to "SENT", and the Idle Connection Timer SHOULD<3> be set to an implementation-specific value. Otherwise, the Flags field of the message MUST be set to 0x0000. ● If the message to be sent was provided with an optional remote memory token to be invalidated on the receiving peer, the token SHOULD be provided in an implementation-specific manner to the RDMA provider when sending. If sending of remote invalidation is not supported by the RDMA provider, the token MAY be ignored. ● The message MUST be sent on the connection in an implementation-specific manner. ● Connection.SendImmediate MUST be set to FALSE. In Section 3.1.5.8, Receiving a Data Transfer Message, the following was changed from: ... If Connection.SendQueue is empty, the credit processing specified in section 3.1.5.9 MUST be performed. If the number of new credits returned is greater than zero, the receiver MUST set

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	Connection.SendImmediate to TRUE and MUST promptly send a Data Transfer message on the Connection, as specified in section 3.1.5.1. ... Changed to: ... If Connection.SendQueue is empty, the credit processing specified in section 3.1.5.9 MUST be performed. If the number of new credits returned is greater than zero, the receiver MUST promptly send a newly constructed Data Transfer message with its CreditsGranted field set to the number of new credits on the Connection, as specified in section 3.1.5.1. ...

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[MS-SSTR]: Smooth Streaming Protocol

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

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

RSS
Atom

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

March 16, 2018 - Download

Errata below are for Protocol Document Version V8.0 – 2019/03/13.

Errata Published*	Description
2020/07/06	In Section 1.5 Prerequisites/Preconditions, added reference to the amendment for HEVC. Changed from: It is also assumed that the client is integrated with a higher-layer implementation that supports any media formats that are used and can otherwise play the media that is transmitted by the server.<1> <1> Section 1.5: The Smooth Streaming Protocol is supported… Changed to: It is also assumed that the client is integrated with a higher-layer implementation that supports any media formats that are used and can otherwise play the media that is transmitted by the server.<1><2> <1> Section 1.5: For requirements to enable cloud-based Smooth Streaming of High Efficiency Video Coding (HEVC) encoded video see the amendment for HEVC [MSDOCS-SSTR-HEVC]. <2> Section 1.5: The Smooth Streaming Protocol is supported…

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 – 2018/09/12.

Errata Published*	Description
2019/02/19	In Section 7, Appendix B: Product Behavior Product Behavior, note 2 has been changed from: <2> Section 3.1.3: Windows Server 2012 sets this value to 0x00010001. Windows Server 2012 R2, Windows Server 2016, Windows Server operating system, and Windows Server 2019 set this value to 0xFFFFFFFF. Changed to: <2> Section 3.1.3: Windows Server 2012 sets this value to 0x00010001. Windows Server 2012 R2, Windows Server 2016, Windows Server operating system, and Windows Server 2019 set this value to 0x00020000.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

March 20, 2017 - Download

August 21, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

October 14, 2019 - Download

June 15, 2020 - Download

Errata below are for Protocol Document Version V30.0 – 2020/10/01

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2021/02/22</td><td>In section 2.2.7.4 COLMETADATA, the descriptions of EncryptionAlgo and AlgoName have been updated.

Changed from:

<table>
<tr><td>EncryptionAlgo</td><td>A byte that describes the encryption algorithm that is used.
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.</td></tr>
<tr><td>AlgoName</td><td>Reserved for future use.</td></tr>
</table>

Changed to:</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	<table><tr><td>EncryptionAlgo</td><td>This byte describes the encryption algorithm that is used. For a custom encryption algorithm, the EncryptionAlgo value MUST be set to 0 and the actual encryption algorithm MUST be inferred from the AlgoName. For all other values, 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. If EncryptionAlgo is set to 2, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA256. Other values are reserved for future use.</td></tr><tr><td>AlgoName</td><td>Reserved for future use. Algorithm name literal that is used for encrypting the plaintext value. This is an optional field and MUST be sent when EncryptionAlgo = 0. For all other values of EncryptionAlgo, this field MUST NOT be sent.</td></tr></table>

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 15, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

Errata below are for Protocol Document Version V39.0 – 2018/09/12.

Errata Published*	Description
2020/10/26	In Section 2.2.10.21 HTTP_TUNNEL_RESPONSE_OPTIONAL Structure, corrected the size and description of the nonce field. Changed from: nonce (20 bytes): A GUID defined in 2.2.2.1. It represents the nonce for the statement of health (SoH). Changed to: nonce (16 bytes): A GUID ([MS-DTYP] section 2.3.4.2) representing the nonce for the statement of health (SoH).
2019/10/28	In Section 3.1.1, Abstract Data Model, changed HTTP_CHANNEL_REQUEST to HTTP_CHANNEL_PACKET in the Target server names and Channel id element descriptions. Changed from: Target server names: An array of alias names for a target server. A target server alias name is a string of Unicode characters. The server name applies to the machine to which the RDG server connects.<23> ... • For HTTP transport, this is initialized when the RDG server receives an HTTP_CHANNEL_REQUEST from the RDG client. ... Channel id: An unsigned long representing the channel identifier for tracking purposes on the RDG server. The Channel id, which is then generated on the server, is stored by the RDG server and RDG client and can later be used for subsequent channel-related calls.<25>

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	... ● For HTTP transport, this is generated after the RDG server receives HTTP_CHANNEL_REQUEST …. Changed to: Target server names: An array of alias names for a target server. A target server alias name is a string of Unicode characters. The server name applies to the machine to which the RDG server connects.<23> ... ● For HTTP transport, this is initialized when the RDG server receives an HTTP_CHANNEL_PACKET (section 2.2.10.2) from the RDG client. ... Channel id: An unsigned long representing the channel identifier for tracking purposes on the RDG server. The Channel id, which is then generated on the server, is stored by the RDG server and RDG client and can later be used for subsequent channel-related calls.<25> ... ● For HTTP transport, this is generated after the RDG server receives HTTP_CHANNEL_PACKET....
2019/10/28	In Section 2.2.9.2.1.1, TSG_PACKET_HEADER, changed the field names ComponentID to ComponentId and PacketID to PacketId. Changed from: The TSG_PACKET_HEADER structure contains information about the ComponentID and PacketID fields of the TSG_PACKET structure. The value of PacketID in TSG_PACKET MUST be set to TSG_PACKET_TYPE_HEADER. ... Changed to: The TSG_PACKET_HEADER structure contains information about the ComponentId and PacketId fields of the TSG_PACKET structure. The value of PacketId in TSG_PACKET MUST be set to TSG_PACKET_TYPE_HEADER. ... In Section 3.5.1, Abstract Data Model, changed the structure name AUTHENTICATION_COOKIE_DATA to AUTHN_COOKIE_DATA in the UDPAuthCookie description. Changed from: ... UDPAuthCookie: A signed and encoded byte BLOB containing an AUTHENTICATION_COOKIE_DATA structure. ... Changed to: ... UDPAuthCookie: A signed and encoded byte BLOB containing an AUTHN_COOKIE_DATA structure. ...

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	In Section 3.7.1, Abstract Data Model, changed the structure name AUTHENTICATION_COOKIE_DATA to AUTHN_COOKIE_DATA in the UDPAuthCookie description. Changed from: UDPAuthCookie: A signed and encoded byte BLOB containing an AUTHENTICATION_COOKIE_DATA structure. ... Changed to: UDPAuthCookie: A signed and encoded byte BLOB containing an AUTHN_COOKIE_DATA structure. ... In Section 4.3.1, Normal Scenario, changed the structure name AUTHENTICATION_COOKIE_DATA to AUTHN_COOKIE_DATA and the ADM element name AUTHENTICATION_COOKIE_DATA.szServerName to AUTHN_COOKIE_DATA.szServerName. Changed from: .. 6. The RDG server decrypts the packet received with DTLS. The RDG server decodes the message and verifies the signature on the decoded message. The RDG server maps the decoded message to the AUTHENTICATION_COOKIE_DATA structure. 7. The RDG server connects to the target server specified in the ADM element AUTHENTICATION_COOKIE_DATA.szServerName. ... Changed to: ... 6. The RDG server decrypts the packet received with DTLS. The RDG server decodes the message and verifies the signature on the decoded message. The RDG server maps the decoded message to the AUTHN_COOKIE_DATA structure. 7. The RDG server connects to the target server specified in the ADM element AUTHN_COOKIE_DATA.szServerName....

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 V26.0 – 2018/09/12.

Errata Published*	Description
2019/04/15	In Section 3.10.4.1.1, RpcShadow2 (Opnum 0), the format of the pszInvitation field has been clarified. In addition, a reference to a Windows platform-specific API has been removed and substituted with a link to MS-RAI Section 2.2.2. Changed from: pszInvitation: The output data containing the invitation string for the shadow session. The data returned is an invitation string in an XML format that can be used with the Windows Desktop Sharing API IRDPSRAPIViewer::Connect method to connect to the session running in the target session (specified by TargetSessionId). The caller must allocate a buffer to hold this data and specify the size of the buffer in cchInvitation. Changed to: pszInvitation: The output data containing the invitation string for the shadow session. The data returned is a Unicode string in the XML format specified in [MS-RAI] section 2.2.2 that can be used to connect to a session running in the target session (specified by TargetSessionId). The caller must allocate a buffer to hold this data and specify the size of the buffer in cchInvitation.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-TSWP]: Terminal Services Workspace Provisioning Protocol

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

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

RSS
Atom

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:

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[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.

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[MS-VAPR]: Virtual Application Publication and Reporting (App-V) Protocol

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

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

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Errata below are for Protocol Document Version V4.0 – 2018/09/12.

Errata Published*	Description
2020/11/23	In Section 2.6.2.6.2 Parent Locator Entry, the length of the KeyLegth and ValueLength fields has been updated: Changed from KeyLength (4 bytes): Specifies the length in bytes of the entry's key. This field MUST be greater than zero. ValueLength (4 bytes): Specifies the length in bytes of an entry's value. This field MUST be greater than zero. Changed to KeyLength (2 bytes): Specifies the length in bytes of the entry's key. This field MUST be greater than zero. ValueLength (2 bytes): Specifies the length in bytes of an entry's value. This field MUST be greater than zero.
2020/11/23	In Section 2 structures, the Castagnoli polynomial has been updated. Changed from The algorithm used to detect errors after transmission or storage is called a cyclic redundancy check (CRC). Unless specified otherwise, the CRC used to validate data is CRC-32C (see [Castagnoli93]), which uses the Castagnoli polynomial, code 0x11EDC6F41. Changed to The algorithm used to detect errors after transmission or storage is called a cyclic redundancy check (CRC). Unless specified otherwise, the CRC used to validate data is CRC-32C (see [Castagnoli93]), which uses the Castagnoli polynomial, code 0x1EDC6F41.
2020/05/25	In Section 2.2.2, Headers, the following was changed from: ... Reserved (4016 bytes): MUST be set to 0 and ignored.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	The LogLength and LogOffset fields specify the byte offset in the file and the length of the log. These values MUST be multiples of 1 MB and LogOffset MUST be at least 1 MB. The log MUST NOT overlap any other structures. The space between a 4-KB structure containing header data and a 64-KB alignment boundary for the header is reserved. Changed to: ... LogLength (4 bytes): A 32-bit unsigned integer. Specifies the size, in bytes of the log. This value MUST be a multiple of 1MB. LogOffset (8 bytes): A 64-bit unsigned integer. Specifies the byte offset in the file of the log. This value MUST be a multiple of 1MB. The log MUST NOT overlap any other structures. Reserved (4016 bytes): MUST be set to 0 and ignored. The space between a 4-KB structure containing header data and a 64-KB alignment boundary for the header is reserved.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

September 29, 2020 – Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[MS-WDSOSD]: Windows Deployment Services Operation System Deployment Protocol

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

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

RSS
Atom

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:

September 12, 2018 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

June 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

March 20, 2017 - Download

June 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 V28.0 – 2018/09/12.

Errata Published*	Description
2018/11/12	In Section 3.2.4.8, NetrUseGetInfo (Opnum 9), changed from: … The server MUST fill the return structures as follows: • If the Level member is 0, the server MUST return the information about the connection by filling the USE_INFO_0_CONTAINER (section 2.2.5.25) structure in the Buffer field of the InfoStruct parameter as follows. USE_INFO_0_CONTAINER contains an array of USE_INFO_0 structures. • ui0_local set to Connection.local • ui0_remote set to Connection.Remote • If the Level member is 1, the server MUST return the information about the connection by filling the USE_INFO_1_CONTAINER (section 2.2.5.26) structure in the Buffer field of the InfoStruct parameter as follows. USE_INFO_1_CONTAINER contains an array of USE_INFO_1 structures. • ui1_local set to Connection.local • ui1_remote set to Connection.remote • ui1_password set to NULL • ui1_status set to Connection.status • ui1_asg_type set to Connection.asgtype • ui1_refcount set to Connection.refcount • ui1_usecount set to Connection.useCount • If the Level member is 2, the server MUST return the information about the connection by filling the USE_INFO_2_CONTAINER (section 2.2.5.27) structure in the Buffer field of the InfoStruct parameter as follows. USE_INFO_2_CONTAINER contains an array of USE_INFO_2 structures. • ui2_local set to Connection.local • ui2_remote set to Connection.remote • ui2_password set to NULL • ui2_status set to Connection.status • ui2_asg_type set to Connection.asgtype • ui2_refcount set to Connection.refcount • ui2_usecount set to Connection.useCount • ui2_domainname set to Connection.domain • If the Level member is 3, the server MUST return the information about the connection by filling the USE_INFO_3_CONTAINER structure in the Buffer field of the

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	InfoStruct parameter as follows. USE_INFO_3_CONTAINER contains an array of USE_INFO_3 structures. ● ui2_local set to Connection.local ● ui2_remote set to Connection.remote ● ui2_password set to NULL ● ui2_status set to Connection.status ● ui2_asg_type set to Connection.asgtype ● ui2_refcount set to Connection.refcount ● ui2_usecount set to Connection.useCount ● ui2_domainname set to Connection.domain ● ui2_flag set to 0 The server MUST invoke the event to end the client impersonation ([MS-RPCE] section 3.3.3.4.3.3). Changed to: … The server MUST fill the return structures as follows: ● If the Level member is 0, the server MUST return the information about the connection by filling the USE_INFO_0_CONTAINER (section 2.2.5.25) structure in the Buffer field of the InfoStruct parameter as follows. USE_INFO_0_CONTAINER contains an array of USE_INFO_0 structures. ● ui0_local set to Connection.local ● ui0_remote set to Connection.Remote ● If the Level member is 1, the server MUST return the information about the connection by filling the USE_INFO_1_CONTAINER (section 2.2.5.26) structure in the Buffer field of the InfoStruct parameter as follows. USE_INFO_1_CONTAINER contains an array of USE_INFO_1 structures. ● ui1_local set to Connection.local ● ui1_remote set to Connection.remote ● ui1_password set to NULL ● ui1_status set to Connection.status ● ui1_asg_type set to Connection.asgtype ● ui1_refcount set to Connection.refcount ● ui1_usecount set to Connection.usecount ● If the Level member is 2 or 3, the server MUST return the information about the connection by filling the USE_INFO_2_CONTAINER (section 2.2.5.27) structure in the Buffer field of the InfoStruct parameter as follows. USE_INFO_2_CONTAINER contains an array of USE_INFO_2 structures. ● ui2_local set to Connection.local ● ui2_remote set to Connection.remote ● ui2_password set to NULL ● ui2_status set to Connection.status ● ui2_asg_type set to Connection.asgtype ● ui2_refcount set to Connection.refcount ● ui2_usecount set to Connection.usecount ● ui2_username set to Connection.username ● ui2_domainname set to Connection.domain The server MUST invoke the event to end the client impersonation ([MS-RPCE] section 3.3.3.4.3.3).

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2018/11/12</td><td>In Section 3.2.4.13, NetrJoinDomain2 (Opnum 22), changed from:

<table>
<tr><th>Value/code</th><th>Meaning</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>NETSETUP_MACHINE_PWD_PASSED
0x00000080</td><td>Indicates that the Password parameter SHOULD<58> specify the password for the machine joining the domain. This flag is valid only for unsecured joins, which MUST be indicated by setting the NETSETUP_JOIN_UNSECURE flag. If this flag is set, the value of Password determines the value stored for the computer password during the join process.</td></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>NETSETUP_INSTALL_INVOCATION
0x00040000</td><td>Indicates that the protocol method was invoked during installation</td></tr>
</table>

Changed to:

<table>
<tr><th>Value/code</th><th>Meaning</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>NETSETUP_MACHINE_PWD_PASSED
0x00000080</td><td>Indicates that the Password parameter SHOULD<58> specify the password for the machine joining the domain. This flag is valid only for unsecured joins, which MUST be indicated by setting the NETSETUP_JOIN_UNSECURE flag, or read-only joins, which MUST be indicated by setting the NETSETUP_JOIN_READONLY flag. If this flag is set, the value of Password determines the value stored for the computer password during the join process.</td></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>NETSETUP_JOIN_READONLY
0x00000800</td><td>Specifies that the join SHOULD <121> be performed in a read-only manner against an existing account object. This option is intended to enable the server to join a domain using a read-only domain controller.</td></tr>
<tr><td>NETSETUP_INSTALL_INVOCATION
0x00040000</td><td>Indicates that the protocol method was invoked during installation</td></tr>
</table>
<121> Section 3.2.4.13: Windows NT, Windows 2000, Windows XP, Windows Server 2003, and Windows Server 2003 R2 do not implement this option.</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	In Section 3.2.4.13.3, Domain Join Specific Message Processing, changed from: The following statements define the sequence of message-processing operations: 1. If the NETSETUP_MACHINE_PWD_PASSED bit is set in Options, and the NETSETUP_JOIN_UNSECURE bit is not set in Options, the server MUST return ERROR_INVALID_PARAMETER. Otherwise, message processing continues. 2. If the NETSETUP_MACHINE_PWD_PASSED bit is set in Options, and AccountName is not NULL, the server MUST return ERROR_INVALID_PARAMETER. Otherwise, message processing continues. 3. If the NETSETUP_MACHINE_PWD_PASSED bit is set in Options, and either Password is NULL or the length of the PasswordString is zero, the server MUST return ERROR_PASSWORD_RESTRICTION. Otherwise, message processing continues. 4. If the NETSETUP_MACHINE_PWD_PASSED bit is set in Options, the value of PasswordString MUST be copied to the value of ComputerPasswordString, and PasswordString MUST be set to NULL. 5. If the server processing the message is already joined to a domain, and the NETSETUP_DOMAIN_JOIN_IF_JOINED bit is not set in Options, the server MUST return NERR_SetupAlreadyJoined. Otherwise, message processing continues. … 6. If DomainNameString contains the character "\",… The specified domain controller MUST be validated by invoking the DsrGetDcNameEx2 method ([MS-NRPC] section 3.5.4.3.1) on the DomainControllerString computer, specifying the following parameters: … • Flags = B | J | R … If the call fails, or the returned domain controller name does not match DomainControllerString, the server MUST invoke the DsrGetDcNameEx2 method ([MS-NRPC] section 3.5.4.3.1) on the DomainControllerString computer, specifying the following parameters: … • Flags = B | J | S … 29. The following LDAP attributes… Changed to: The following statements define the sequence of message-processing operations: 1. If the NETSETUP_MACHINE_PWD_PASSED bit is set in Options, and the NETSETUP_JOIN_UNSECURE bit is not set in Options, the server MUST return ERROR_INVALID_PARAMETER. Otherwise, message processing continues. 2. If the NETSETUP_MACHINE_PWD_PASSED bit is set in Options, and AccountName is not NULL, the server MUST return ERROR_INVALID_PARAMETER. Otherwise, message processing continues. 3. If the NETSETUP_MACHINE_PWD_PASSED bit is set in Options, and either Password is NULL or the length of the PasswordString is zero, the server MUST return ERROR_PASSWORD_RESTRICTION. Otherwise, message processing continues. 4. If the NETSETUP_MACHINE_PWD_PASSED bit is set in Options, the value of PasswordString MUST be copied to the value of ComputerPasswordString, and PasswordString MUST be set to NULL.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	5. If the NETSETUP_JOIN_READONLY bit is set in Options, and NETSETUP_MACHINE_PWD_PASSED bit is not set in Options, the server MUST return ERROR_INVALID_PARAMETER. Otherwise, message processing continues. 6. If the NETSETUP_JOIN_READONLY bit is set in Options, and the NETSETUP_ACCT_CREATE bit is set in Options, the server MUST return ERROR_INVALID_PARAMETER. Otherwise, message processing continues. 7. If the NETSETUP_JOIN_READONLY bit is set in Options, the server MUST perform all subsequent message processing as if NETSETUP_DEFER_SPN_SET and NETSETUP_JOIN_UNSECURE bits are set in Options. 8. If the server processing the message is already joined to a domain, and the NETSETUP_DOMAIN_JOIN_IF_JOINED bit is not set in Options, the server MUST return NERR_SetupAlreadyJoined. Otherwise, message processing continues.… 9. If DomainNameString contains the character "\",… The specified domain controller MUST be validated by invoking the DsrGetDcNameEx2 method ([MS-NRPC] section 3.5.4.3.1) on the DomainControllerString computer, specifying the following parameters: … ● Flags : if NETSETUP_JOIN_READONLY bit is set in Options, set Flags = (B | R); otherwise set Flags to (B | J | R) … If the call fails, or the returned domain controller name does not match DomainControllerString, the server MUST invoke the DsrGetDcNameEx2 method ([MS-NRPC] section 3.5.4.3.1) on the DomainControllerString computer, specifying the following parameters: … ● Flags : if NETSETUP_JOIN_READONLY bit is set in Options, set Flags = (B | S); otherwise set Flags to (B | J | S) … 32. If the NETSETUP_JOIN_READONLY bit is not set in Options, the following LDAP attributes…

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-WMIO]: Windows Management Instrumentation Encoding Version 1.0 Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V15.0 – 2018/09/12.

Errata Published*	Description
2019/06/10	In Section 3 Structure Examples, we revised the octet value of PropertyInfoRef. Changed from: A0 00 00 00 Changed to: 0A 00 00 00

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

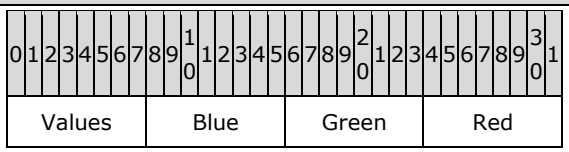
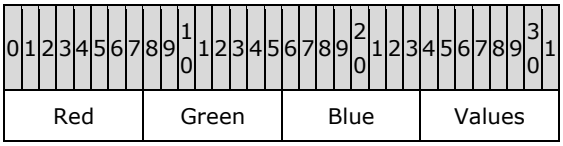
October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V15.0 – 2018/09/12

Errata Published*	Description
2021/03/08	In Section 2.2.2.11, LogColorSpace Object, updated the length of the Filename field: Changed from: Filename (variable): An optional, ASCIIcharacter string that specifies the name of a file that contains a color profile. If a file name is specified, and the ColorSpaceType field is set to LCS_CALIBRATED_RGB, the other fields of this structure SHOULD be ignored. Changed to: Filename (260 bytes): An optional, ASCII character string that specifies the name of a file that contains a color profile. If a file name is specified, and the ColorSpaceType field is set to LCS_CALIBRATED_RGB, the other fields of this structure SHOULD be ignored. In Section 2.2.2.12, LogColorSpaceW Object, updated the length of the Filename field: Changed from: Filename (variable):An optional, null-terminated UnicodeUTF16-LE character string, which specifies the name of a file that contains a color profile. If a file name is specified, and the ColorSpaceType field is set to LCS_CALIBRATED_RGB, the other fields of this structure SHOULD be ignored.Changed to: Filename (520 bytes): An optional, null-terminated UnicodeUTF16-LE character string, which specifies the name of a file that contains a color profile. If a file name is specified, and the ColorSpaceType field is set to LCS_CALIBRATED_RGB, the other fields of this structure SHOULD be ignored.
2021/02/08	In section 2.2.2.13, PaletteEntry Object, revised the order of the fields. Changed from: The PaletteEntry Object defines the color and usage of an entry in a palette.

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	 Values (1 byte): An 8-bit unsigned integer that defines how the palette entry is to be used. The Values field MUST be 0x00 or one of the values in the PaletteEntryFlag Enumeration (section 2.1.1.22) table. Blue (1 byte): An 8-bit unsigned integer that defines the blue intensity value for the palette entry. Green (1 byte): An 8-bit unsigned integer that defines the green intensity value for the palette entry. Red (1 byte): An 8-bit unsigned integer that defines the red intensity value for the palette entry. Changed to: The PaletteEntry Object defines the color and usage of an entry in a palette.  Red (1 byte): An 8-bit unsigned integer that defines the red intensity value for the palette entry. Green (1 byte): An 8-bit unsigned integer that defines the green intensity value for the palette entry. Blue (1 byte): An 8-bit unsigned integer that defines the blue intensity value for the palette entry. Values (1 byte): An 8-bit unsigned integer that defines how the palette entry is to be used. The Values field MUST be 0x00 or one of the values in the PaletteEntryFlag Enumeration (section 2.1.1.22) table.
2021/02/08	In Section 2.2.2.5, BitmapV5Header Object, revised the values used in the Intent field: Changed from: Intent (4 bytes): A 32-bit unsigned integer that defines the rendering intent for the DIB. This MUST be defined in the LogicalColorSpace Enumeration (section 2.1.1.14). Changed to: Intent (4 bytes): A 32-bit unsigned integer that defines the rendering intent for the DIB. This MUST be a value defined in the GamutMappingIntent Enumeration (section 2.1.1.11).
2021/02/08	In Section 2.2.2.17, PolyPolygon Object, revised the definition of aPoints: Changed from: aPoints (variable): An array of 16-bit unsigned integers that define the coordinates of the polygons. Changed to:

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>aPoints (variable): An array of PointS values that define the coordinates of the polygons. The length of the array is equal to the sum of all 16-bit integers in the aPointsPerPolygon array.

In Section 2.3.3.15 META_POLYGON Record, revised casing and details of NumberOfPoints:

Changed from:

<table><tr><td>RecordFunction</td><td>NumberofPoints</td></tr></table>
Changed to:
<table><tr><td>RecordFunction</td><td>NumberOfPoints</td></tr></table>
Changed from:

NumberofPoints (2 bytes): A 16-bit signed integer that defines the number of points in the array.

Changed to:

NumberOfPoints (2 bytes): A 16-bit signed integer that defines the number of points in the array. This value must be greater than or equal to 2.</td></tr>
<tr><td>2021/02/08</td><td>In Section 2.3.3.5, META_EXTTEXTOUT RECORD, added string encoding details:

Changed from:

String (variable): A variable-length string that specifies the text to be drawn. The string does not need to be null-terminated, because StringLength specifies the length of the string. If the length is odd, an extra byte is placed after it so that the following member (optional Dx) is aligned on a 16-bit boundary.

Changed to:

String (variable): A variable-length string that specifies the text to be drawn. The string does not need to be null-terminated, because StringLength specifies the length of the string. If the length is odd, an extra byte is placed after it so that the following member (optional Dx) is aligned on a 16-bit boundary. The string will be decoded based on the font object currently selected into the playback device context. If a font matching the font object’s specification is not found, the decoding is undefined. If a matching font is found that matches the charset specified in the font object, the string should be decoded with the codepages in the following table.
<table><tr><td>CharSet</td><td>CodePage ID</td></tr><tr><td>ANSI_CHARSET</td><td>1252</td></tr><tr><td>OEM_CHARSET</td><td>437</td></tr><tr><td>SHIFTJIS_CHARSET</td><td>932</td></tr><tr><td>HANGEUL_CHARSET</td><td>949</td></tr></table></td></tr>
</table>

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>JOHAB_CHARSET</td><td>1361</td></tr>
<tr><td>GB2312_CHARSET</td><td>936</td></tr>
<tr><td>CHINESEBIG5_CHARSET</td><td>950</td></tr>
<tr><td>HEBREW_CHARSET</td><td>1255</td></tr>
<tr><td>ARABIC_CHARSET</td><td>1256</td></tr>
<tr><td>GREEK_CHARSET</td><td>1253</td></tr>
<tr><td>TURKISH_CHARSET</td><td>1254</td></tr>
<tr><td>BALTIC_CHARSET</td><td>1257</td></tr>
<tr><td>EASTEUROPE_CHARSET</td><td>1250</td></tr>
<tr><td>RUSSIAN_CHARSET</td><td>1251</td></tr>
<tr><td>THAI_CHARSET</td><td>874</td></tr>
<tr><td>VIETNAMESE_CHARSET</td><td>1258</td></tr>
<tr><td>SYMBOL_CHARSET</td><td>42</td></tr>
</table>
</td></tr>
<tr><td>2021/02/08</td><td>In Section 2.3, WMF Records, added information about record processing:

Changed from:

When a WMFmetafile (2) is processed, the order in which graphics output is performed MUST be the same as the order of drawing records in the metafile (2). Thus, a given drawing command is always rendered on top of the renderings of preceding commands. The following packet definition specifies the generic structure of all WMF Records except Control Record Types (section 2.3.2).

Changed to:

When a WMFmetafile (2) is processed, the order in which graphics output is performed MUST be the same as the order of drawing records in the metafile (2). Thus, a given drawing command is always rendered on top of the renderings of preceding commands.
Implementations MUST ignore records with undocumented or unsupported record types and proceed to process the next valid record.
The following packet definition specifies the generic structure of all WMF Records except Control Record Types (section 2.3.2).</td></tr>
<tr><td>2021/02/08</td><td>In Section 2.3.2.3, META_PLACEABLE Record, clarified calculation of the value in the CheckSum field.

Changed from:

Checksum (2 bytes): A checksum for the previous 10 16-bit values in the header. This value can be used to determine whether the metafile has become corrupted.

Changed to:</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>Checksum (2 bytes): A checksum for the previous 10 16-bit values in the header. This value can be used to determine whether the metafile has become corrupted. The value is calculated by initializing the checksum to zero and then XORing it one at a time with the 10 16-bit values in the header.</td></tr>
<tr><td>2021/02/08</td><td>In Section 2.2.1.2, Font Object, changed the length and description of the Facename field:

Changed from:

<table><tr><td>Quality</td><td>PitchAndFamily</td><td>Facename (Variable)</td></tr><tr><td colspan="3">...</td></tr></table>
Changed to:

<table><tr><td>Quality</td><td>PitchAndFamily</td><td>Facename (32 bytes)</td></tr><tr><td colspan="3">...</td></tr></table>
Changed from:

Facename (variable): A null-terminated string of 8-bit Latin-1 [ISO/IEC-8859-1] ANSI characters that specifies the typeface name of the font. The length of this string MUST NOT exceed 32 8-bit characters, including the terminating null.

Changed to:

Facename (32 bytes): A null-terminated string of up to 32 8-bit Latin-1 [ISO/IEC-8859-1] ANSI characters that specifies the typeface name of the font. Any characters following the terminating null are ignored.</td></tr>
<tr><td>2021/02/08</td><td>In Section 2.3.3.5, META_EXTTEXTOUT Record, added information about when the Rectangle field is optional:

Changed from:

Rectangle (8 bytes): An optional 8-byte Rect Object (section 2.2.2.18) that defines the dimensions, in logical coordinates, of a rectangle that is used for clipping, opaquing, or both.

Changed to:

Rectangle (8 bytes): An optional 8-byte Rect Object (section 2.2.2.18). When either ETO_CLIPPED, ETO_OPAQUE, or both are specified, the rectangle defines the dimensions, in logical coordinates, used for clipping, opaquing, or both. When neither ETO_CLIPPED nor ETO_OPAQUE is specified, the coordinates in Rectangle are ignored.</td></tr>
<tr><td>2021/02/08</td><td>In Section 2.3.2.3, META_PLACEABLE Record, added a cross-reference defining the BoundingBox:

Changed from:</td></tr>
</table>

Copyright © 2020 Microsoft Corporation

Errata Published*	Description
	BoundingBox (8 bytes): The rectangle in the playback context (or simply the destination rectangle), measured in logical units, for displaying the metafile. The size of a logical unit is specified by the Inch field. Changed to: BoundingBox (8 bytes): The rectangle in the playback context (or simply the destination rectangle), measured in logical units, for displaying the metafile. The size of a logical unit is specified by the Inch field. See section 2.2.2.18 for details about the structure of the BoundingBox field.
2021/02/08	The following sections have been changed. Section 2.1.1.17, MetafileEscapes Enumeration Section 2.1.1.23, PenStyle Enumeration Section 2.2.1.2, Font Object Section 2.3.3.15, META_POLYGON Record Section 2.3.6, Escape Record Types Section 2.3.6.4, CHECKJPEGFORMAT Record Section 2.3.6.5, CHECKPNGFORMAT Record Section 2.3.6.7, CLOSECHANNEL Record Section 2.3.6.8, DOWNLOADFACE Record Section 2.3.6.9, DOWNLOADHEADER Record Section 2.3.6.10, DRAWPATTERNRECT Record Section 2.3.6.14, EPSPRINTING Record Section 2.3.6.16, GETCOLORTABLE Record Section 2.3.6.17, GETDEVICEUNITS Record Section 2.3.6.18, GETEXTENDEDTEXTMETRICS Record Section 2.3.6.19, GETFACENAME Record Section 2.3.6.20, GETPAIRKERNTABLE Record Section 2.3.6.21, GETPHYSPAGESIZE Record Section 2.3.6.22, GETPRINTINGOFFSET Record Section 2.3.6.24, GETSCALINGFACTOR Record Section 2.3.6.35, OPENCHANNEL Record Section 2.3.6.36, QUERYDIBSUPPORT Record Section 2.3.6.37, QUERYESCSUPPORT Record Section 2.3.6.38, SETCOLORTABLE Record Section 2.3.6.39, SETCOPYCOUNT Record Section 2.3.6.40, SETLINECAP Record Section 2.3.6.41, SETLINEJOIN Record Section 2.3.6.42, SETMITERLIMIT Record Please see diff file

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 20, 2017 - Download

June 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

December 1, 2017 - Download

September 12, 2018 - Download

Errata below are for Protocol Document Version V33.0 - 2018/09/12

Errata Published*	Description
2020/10/12	In Section 2.2.9.1.2.2.2 Encrypted Data, added note about padding. Changed from: Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework as specified in [RFC4121]. The initial bytes of the Message MUST be the per-message token portion, whose length MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose original length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.2.2.1. Changed to: Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework as specified in [RFC4121]. The initial bytes of the Message MUST be the per-message token portion, whose length MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose original length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.2.2.1. Note: No padding is added irrespective of the type of cipher used for encryption.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

September 23, 2019 - Download

March 4, 2020 - Download

August 24, 2020 – Download

Errata below are for Protocol Document Version V35.0 - 2020/08/26

Errata Published*	Description
2020/09/14	In Section 2.2.1 Structures, the row for Section 2.2.1.29 CInGroupSortAggregSet, was removed. Changed from: CSortAggregSet Contains a set of grouping sort keys. CInGroupSortAggregSet Contains sorting information for a group with regard to a parent group. CInGroupSortAggregSets Contains sorting information for a group with regard to one or more parent groups. Changed to: CSortAggregSet Contains a set of grouping sort keys. CInGroupSortAggregSets Contains sorting information for a group with regard to one or more parent groups. Section 2.2.1.29 CInGroupSortAggregSet has been removed from the document.
2020/09/14	A new Section 2.2.5.3 ODBC Property, was added to the document: Changed to: ODBC Property set `#define ODBCGuid { 0xC8B52232L, 0x5CF3, 0x11CE, {0xAD, 0xE5, 0x00, 0xAA, 0x00,0x44, 0x77, 0x3D } }`

Copyright © 2020 Microsoft Corporation

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Name/Prop</th><th>DataType</th><th>Description</th></tr>
<tr><td>Chapter / 0x3</td><td>VT_I4</td><td>Chapter handle</td></tr>
<tr><td>Bookmark / 0x2</td><td>VT_I4</td><td>Bookmark handle</td></tr>
</table>
In Section 3.2.4.2.4 Sending a CPMGetRowsIn Request, the first paragraph was changed.
Changed from:
When the higher layer is about to receive rows information, it will provide the protocol client with valid cursor and chapter handles and give an appropriate seek description. Typically, a higher layer is expected to do so when it has a valid cursor and/or chapter handle, and the bindings have been set with the CPMSetBindingsIn message. To access the rowset in a chapter, the higher layer is to use the chapter handle received from the server in a previous CPMGetRowsOut message.
Changed To:
When the higher layer is about to receive rows information, it will provide the protocol client with valid cursor and chapter handles and give an appropriate seek description. Typically, a higher layer is expected to do so when it has a valid cursor and/or chapter handle, and the bindings have been set with the CPMSetBindingsIn message. To access the rowset in a chapter, the higher layer is to use the chapter handle received from the server in a previous CPMGetRowsOut message as ODBC property value (Chapter).
</td></tr>
<tr><td>2020/09/14</td><td>
In Section 2.2.1.38 CRowSeekByBookmark, the first paragraph was changed:
Changed from:
The CRowSeekByBookmark structure identifies the bookmarks from which to begin retrieving rows for a CPMGetRowsIn message.
Changed to:
The CRowSeekByBookmark structure identifies the bookmarks from which to begin retrieving rows for a CPMGetRowsIn message. The client needs to previously have set up the ODBC Bookmark property per row at the column bindings, which is done by adding ODBC Bookmark property at first binding element from the CPMSetBindingIn message.
</td></tr>
</table>

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

July 18, 2016 - Download

June 1, 2017 - Download

March 4, 2020 - Download

Errata below are for Protocol Document Version V7.0 – 2020/03/04.

Errata Published*	Description
2020/07/06	Throughout this document, changed all occurrences of "computerId", "eulaFailed", and "updateRevisionId" and variations of those terms to "ComputerId", "EULAFailed", and "UpdateRevisionId".

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-WSUSOD]: Windows Server Update Services Protocols Overview

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

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

RSS
Atom

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 1, 2017 - Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

July 18, 2016 - Download

June 1, 2017 - Download

Errata below are for Protocol Document Version V13.0 – 2018/09/12

Errata Published*	Description
2020/11/23	In Section 1.7, Versioning and Capability Negotiation, the table in behavior note <2> has been updated. Changed from: Operating system version Windows Server 2016 WSUS 10.0 supported Changed to: Operating system version Windows Server 2016 WSUS 10.0 supported Windows Server 2019 WSUS 10.0 supported In Section 3.1.4.1.2.1 GetCookie, the protocolVersion field element description has been updated: Changed from: protocolVersion: This field MUST be present. It identifies the version of the protocol that the DSS supports, as specified in section 1.7. Its values can be 1.1, 1.2, 1.3, 1.6, or 1.8. Changed to: protocolVersion: This field MUST be present. It identifies the version of the protocol that the DSS supports, as specified in section 1.7. Its values can be 1.1, 1.2, 1.3, 1.6, 1.8, or 1.20.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

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

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

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

RSS
Atom

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

June 1, 2017 - Download

March 4, 2020 - Download

Errata below are for Protocol Document Version V29.0 – 2020/03/04

Errata Published*	Description
2020/12/07	In Section 2.2.2.2.6, GetExtendedUpdateInfo, clarified the default locale returned by the update service: Changed from: "locales: Optionally specifies the locales (2) for which localizable extended metadata MUST be returned. Localizable metadata are elements such as human-readable strings, which are represented differently between locales, as specified in [MS-LCID]." Changed to: "locales: Optionally specifies the locales (2) for which localizable extended metadata MUST be returned. Localizable metadata are elements such as human-readable strings, which are represented differently between locales, as specified in [MS-LCID]. The service SHOULD always return the EN locale extended metadata."
2020/11/23	Updated the text and behavior notes in several sections to provide more complete versioning information: Section 2.2.2.2.1 GetConfig (behavior notes) Section 2.2.2.2.3 RegisterComputer (behavior notes) Section 2.2.2.2.4 SyncUpdates Section 3.1.5.7 SyncUpdates Section 3.1.5.12 SyncPrinterCatalog Section 6.2 Client Web Service WSDL Please see the diff file for revision-marked changes.

*Date format: YYYY/MM/DD

Copyright © 2020 Microsoft Corporation

[MS-XCA]: Xpress Compression Algorithm

This topic lists the Errata found in [MS-XCA] since it was last published.

Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

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

RSS
Atom

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 4, 2020 - Download

August 24, 2020 – Download

Copyright © 2020 Microsoft Corporation

[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.

RSS
Atom

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

Copyright © 2020 Microsoft Corporation