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 MSDN) and provide links to archived Errata (i.e., Errata already released with the documents on MSDN).

Protocols Documents with Active Errata

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

[MS-ADTS]: Active Directory Technical Specification

[MS-CFB]: Compound File Binary File Format

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

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

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

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

[MS-DTYP]: Windows Data Types

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

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

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

[MS-NCNBI]: Network Controller Northbound Interface Specification

[MS-OAPX]: OAuth 2.0 Protocol Extensions

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

[MS-OIDCE]: OpenID Connect 1.0 Protocol Extensions

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

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

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

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

[MS-SCMR]: Service Control Manager Remote Protocol

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

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

[MS-SSTR]: Smooth Streaming Protocol

[MS-TSGU]: Terminal Services Gateway 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

December 1, 2017 - Download

Last date updated: March 13, 2018

[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

[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

[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

[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

[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

[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

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

July 18, 2016 - Download

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

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

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

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

[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

Errata below are for Protocol Document Version V6.0 – 2017/12/01.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2018/03/05</td><td>In Section 2.2.2.4, Configuration, AD_FS_BEHAVIOR_LEVEL_3 has been mapped to the appropriate value for farm-behavior-version-number.

Changed from:
<table><tr><th>ad_fs_behavior_level</th><th>farm-behavior-version-number</th></tr><tr><td>AD_FS_BEHAVIOR_LEVEL_1</td><td>"6.3"</td></tr><tr><td>AD_FS_BEHAVIOR_LEVEL_2</td><td>"10.0"</td></tr></table>
Changed to:
<table><tr><th>ad_fs_behavior_level</th><th>farm-behavior-version-number</th></tr><tr><td>AD_FS_BEHAVIOR_LEVEL_1</td><td>"6.3"</td></tr><tr><td>AD_FS_BEHAVIOR_LEVEL_2
AD_FS_BEHAVIOR_LEVEL_3</td><td>"10.0"</td></tr></table></td></tr>
</table>

*Date format: YYYY/MM/DD

[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

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

July 18, 2016 - Download

[MS-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

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-ADTS]: Active Directory Technical Specification

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

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

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

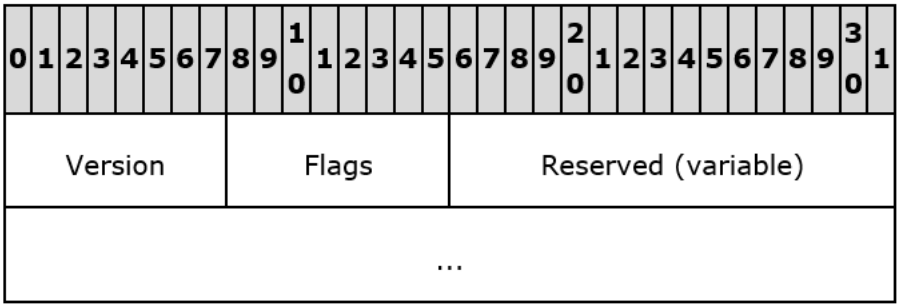
Errata below are for Protocol Document Version V47.0 – 2017/12/01.

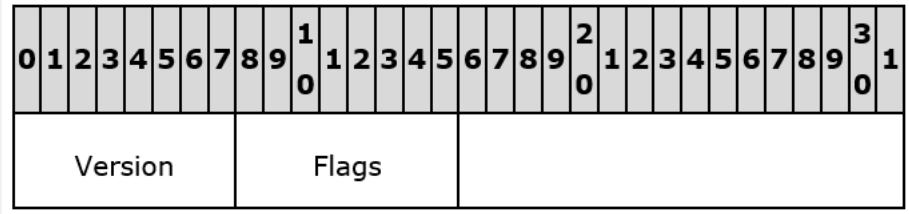
<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2018/03/13</td><td>In Sections 6.1.4.3, msDS-Behavior-Version: Domain NC Functional Level, and 6.1.4.4, msDS-Behavior-Version: Forest Functional Level, certain product names have been removed from the support lists for behavior levels DS_BEHAVIOR_WIN2000 through DS_BEHAVIOR_WIN2003.

Changed from:
<table>
<tr><th>Identifier</th><th>Domain controller operating systems that are allowed in the <domain or forest></th><th>Value</th></tr>
<tr><td>DS_BEHAVIOR_WIN2000</td><td>Windows 2000 Server
Windows Server 2003
Windows Server 2003 R2
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012</td><td>0</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description
	<table><tr><td></td><td>R2 Windows Server 2016 Windows Server operating system</td><td></td></tr><tr><td>DS_BEHAVIOR_WIN2003_WITH_MIXED_DOMAINS</td><td>Windows Server 2003 Windows Server 2003 R2 Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server operating system</td><td>1</td></tr><tr><td>DS_BEHAVIOR_WIN2003</td><td>Windows Server 2003 Windows Server 2003 R2 Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server operating system</td><td>2</td></tr></table> Changed to:

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Identifier</th><th>Domain controller operating systems that are allowed in the <domain or forest></th><th>Value</th></tr>
<tr><td>DS_BEHAVIOR_WIN2000</td><td>Windows 2000 Server
Windows Server 2003
Windows Server 2003 R2
Windows Server 2008</td><td>0</td></tr>
<tr><td>DS_BEHAVIOR_WIN2003_WITH_MIXED_DOMAINS</td><td>Windows Server 2003
Windows Server 2003 R2
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016</td><td>1</td></tr>
<tr><td>DS_BEHAVIOR_WIN2003</td><td>Windows Server 2003
Windows Server 2003 R2
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Windows Server 2012 R2
Windows Server 2016</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>2018/03/13</td><td>In Section 2.2.20.6 (formerly section 2.2.20.5), KEYCREDENTIALLINK_ENTRY Identifiers, the KeyUsage entry of the KEYCREDENTIALLINK_BLOB structure has been identified as required.</td></tr>
</table>

Errata Published*	Description
	Changed from: All keys MUST contain KeyID and KeyMaterial. Keys SHOULD contain KeyHash, KeyUsage, KeyApproximateLastLogonTimeStamp and KeyCreationTime. Changed to: All keys MUST contain KeyID, KeyMaterial, and KeyUsage entries. Keys SHOULD contain KeyHash, KeyApproximateLastLogonTimeStamp and KeyCreationTime entries.
2018/03/13	In Section 3, Details, the service pack number for Windows Server 2003 operating system has been corrected. Changed from: Windows Server 2003 operating system with Service Pack 3 (SP3) Changed to: Windows Server 2003 operating system with Service Pack 2 (SP2) In Section 3.1.1.3.3, rootDSE Modify Operations, the service pack number for Windows Server 2003 operating system has been corrected. Changed from: F --> Windows Server 2003 with SP3 Changed to: F --> Windows Server 2003 with SP2
2018/02/12	In Section 2.2.20.4, CUSTOM_KEY_INFORMATION, the Reserved field has been removed. Changed from:  Version (1 byte): ... ... Reserved (variable): Reserved for future use. Changed to:

Errata Published*	Description
	 Version (1 byte): ... ...
2018/01/16	In Section 1.2.2, Informative References, two new references have been added: [MSDN-CAR] Microsoft Corporation, "Control Access Rights", https://msdn.microsoft.com/en-us/library/ms680945(v=vs.85).aspx [MSDOCS-SchUpd] Microsoft Corporation, "Schema Updates", https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/schema-updates In Section 6.1.1.2.7.1, controlAccessRight objects, informative information about the displayName attribute has been added. Changed from: validAccesses: This is implementation-specific information for the administrative application. Changed to: validAccesses: This is implementation-specific information for the administrative application. displayName: This is implementation-specific information for human consumption. Some of the values that are used by the Windows implementation can be found at [MSDN-CAR] and [MSDOCS-SchUpd].
2018/01/16	In Section 3.1.1.2.6, ATTRTYP, a reference to the definition of ATTRTYP has been added. Changed from: Any OID-valued quantity stored on an object is stored as an ATTRTYP, a 32-bit unsigned integer. Changed to: Any OID-valued quantity stored on an object is stored as an ATTRTYP ([MS-DRSR] section 5.14), a 32-bit unsigned integer.

*Date format: YYYY/MM/DD

[MS-AIPS]: Authenticated Internet Protocol

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

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

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

[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

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-BKRP]: BackupKey Remote Protocol

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

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

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

[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

[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

[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

[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

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
2017/12/11	In Section 2.6.3, Other Directory Entries, information about stream allocation has been clarified. Changed from: To determine the file location of actual stream data from a stream directory entry, it is necessary to determine whether the stream exists in the FAT or the mini FAT. Streams whose size is less than the Mini Sector Cutoff value (typically 4,096 bytes) for the file exist in the mini stream. The Starting Sector Location is used as an index into the mini FAT (which starts at mini FAT Starting Location) to track the chain of sectors through the mini stream. Streams whose size is greater than the Mini Sector Cutoff value for the file exist as standard streams. Their Starting Sector Location value is used as an index into the standard FAT, which describes the chain of full sectors containing their data. Changed to: To determine the file location of actual stream data from a stream directory entry, it is necessary to determine whether the stream exists as normal sectors allocated in the FAT or as mini sectors (from the mini stream) allocated in the mini FAT. Streams whose size is less than the Mini Stream Cutoff Size value (typically 4,096 bytes) for the file exist in the mini stream. The Starting Sector Location is used as an index into the mini FAT (which starts at mini FAT Starting Location) to track the chain of sectors through the mini stream. Streams whose size is greater than or equal to the Mini Stream Cutoff Size value for the file exist as standard streams. Their Starting Sector Location value is used as an index into the standard FAT, which describes the chain of full sectors containing their data. In Section 2.9, Compound File Size Limits, a reference was added for details about directory-entry size and directory-sector composition. Changed from: The maximum number of directory entries (storage objects and stream objects) is MAXREGSID (0xFFFFFFFA), roughly 4 billion. This corresponds to a maximum directory sector chain length of slightly less than 512 GB for a 4,096-byte sector compound file. Changed to: The maximum number of directory entries (storage objects and stream objects) is MAXREGSID (0xFFFFFFFA), roughly 4 billion. This corresponds to a maximum directory

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>sector chain length of slightly less than 512 GB for a 4,096-byte sector compound file. (See section 2.6.1 for details about directory-entry size and directory-sector composition.)</td></tr>
<tr><td>2017/12/11</td><td>In Section 2.6.1, Compound File Directory Entry, various field descriptions have been clarified and corrected.

Changed from:
Child ID (4 bytes): This field contains the stream ID of a child object. If there is no child object, the field MUST be set to NOSTREAM (0xFFFFFFFF).
…
CLSID (16 bytes): This field contains an object class GUID, if this entry is a storage or root storage. If no object class GUID is set on this object, the field MUST be set to all zeroes. In a stream object, this field MUST be set to all zeroes. If not NULL, the object class GUID can be used as a parameter to start applications.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00000000000000000000000000000000</td><td>If no object class GUID is set on this object.</td></tr>
</table>
State Bits (4 bytes): This field contains the user-defined flags if this entry is a storage object or root storage object. If no state bits are set on the object, this field MUST be set to all zeroes.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00000000</td><td>If no state bits are set on the object.</td></tr>
</table>
Creation Time (8 bytes): This field contains the creation time for a storage object. The Windows FILETIME structure is used to represent this field in UTC. If no creation time is set on the object, this field MUST be all zeroes. For a root storage object, this field MUST be all zeroes, and the creation time is retrieved or set on the compound file itself.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x0000000000000000</td><td>If no creation time is set on the object or for a root storage object.</td></tr>
</table>
Modified Time (8 bytes): This field contains the modification time for a storage object. The Windows FILETIME structure is used to represent this field in UTC. If no modified time is set on the object, this field MUST be all zeroes. For a root storage object, this field MUST be all zeroes, and the modified time is retrieved or set on the compound file itself.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x0000000000000000</td><td>If no modified time is set on the object or the object is a root storage object.</td></tr>
</table>
Starting Sector Location (4 bytes): This field contains the first sector location if this is a stream object. For a root storage object, this field MUST contain the first sector of the mini stream, if the mini stream exists.

Stream Size (8 bytes): This 64-bit integer field contains the size of the user-defined data, if this is a stream object. For a root storage object, this field contains the size of</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
the mini stream.
…

Changed to:
Child ID (4 bytes): This field contains the stream ID of a child object. If there is no child object, including all entries for stream objects, the field MUST be set to NOSTREAM (0xFFFFFFFF).
…

CLSID (16 bytes): This field contains an object class GUID, if this entry is for a storage object or root storage object. For a stream object, this field MUST be set to all zeroes. A value containing all zeroes in a storage or root storage directory entry is valid, and indicates that no object class is associated with the storage. If an implementation of the file format enables applications to create storage objects without explicitly setting an object class GUID, it MUST write all zeroes by default. If this value is not all zeroes, the object class GUID can be used as a parameter to start applications.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00000000000000000000000000000000</td><td>No object class is associated with the storage.</td></tr>
</table>
State Bits (4 bytes): This field contains the user-defined flags if this entry is for a storage object or root storage object. For a stream object, this field SHOULD be set to all zeroes because many implementations provide no way for applications to retrieve state bits from a stream object. If an implementation of the file format enables applications to create storage objects without explicitly setting state bits, it MUST write all zeroes by default.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00000000</td><td>Default value when no state bits are explicitly set on the object.</td></tr>
</table>
Creation Time (8 bytes): This field contains the creation time for a storage object, or all zeroes to indicate that the creation time of the storage object was not recorded. The Windows FILETIME structure is used to represent this field in UTC. For a stream object, this field MUST be all zeroes. For a root storage object, this field MUST be all zeroes, and the creation time is retrieved or set on the compound file itself.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x0000000000000000</td><td>No creation time was recorded for the object.</td></tr>
</table>
Modified Time (8 bytes): This field contains the modification time for a storage object, or all zeroes to indicate that the modified time of the storage object was not recorded. The Windows FILETIME structure is used to represent this field in UTC. For a stream object, this field MUST be all zeroes. For a root storage object, this field MAY<2> be set to all zeroes, and the modified time is retrieved or set on the compound file itself.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x0000000000000000</td><td>No modified time was recorded for the object.</td></tr>
</table>
<2> Section 2.6.1: When Windows sets the modified time of a root storage, it sets the modified time of the file in the file system (as described in section 2.6.2) and also sets
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
the modified time in the root storage directory entry. When Windows retrieves the modified time of a root storage, it gets the modified time of the file in the filesystem but ignores the modified time in the root storage directory entry.

Starting Sector Location (4 bytes): This field contains the first sector location if this is a stream object. For a root storage object, this field MUST contain the first sector of the mini stream, if the mini stream exists. For a storage object, this field MUST be set to all zeroes.

Stream Size (8 bytes): This 64-bit integer field contains the size of the user-defined data, if this is a stream object. For a root storage object, this field contains the size of the mini stream. For a storage object, this field MUST be set to all zeroes.

In Section 2.6.2, Root Directory Entry, processing rules for Modified Time were updated.

Changed from:
The Creation Time and modified time fields in the root storage directory entry MUST be all zeroes.

Changed to:
The Creation Time field in the root storage directory entry MUST be all zeroes. The Modified Time field in the root storage directory entry MAY be all zeroes.

In Section 2.6.3, Other Directory Entries, composition of objects was clarified and corrected.

Changed from:
Storage objects MAY have CLSID, creation time, modified time, and Child Stream ID values. Stream objects MUST set these values to zero.
Stream objects MAY have valid Starting Sector Location and Stream Size values, whereas these fields are set to zero for storage objects (except as noted for the root directory entry).

Changed to:
The CLSID, state bits, creation time, modified time, and Child ID values are meaningful in directory entries for storage objects but not for Stream objects.
The Starting Sector Location and Stream Size values are meaningful in directory entries for stream objects but not for storage objects.

In Section 3.3.1, Stream ID 0: Root Directory Entry, the names for State Bits and Modified Time were corrected, and the correct value for Modified Time was included.

Changed from:
<table>
<tr><th>Byte offset</th><th>Field name</th><th>Field value</th></tr>
<tr><td>0x0400</td><td>Directory Entry Name</td><td>"Root Entry" (section 2.6.2)</td></tr>
<tr><td>…</td><td>…</td><td>…</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description

0x0460	State Flags	0x00000000
0x0464	Creation Time	0x0000000000000000
0x046C	Modification Time	0x0000000000000000
…	…	…

Changed to:

Byte offset	Field name	Field value
0x0400	Directory Entry Name	"Root Entry" (section 2.6.2)
…	…	…
0x0460	State Bits	0x00000000
0x0464	Creation Time	0x0000000000000000
0x046C	Modified Time	0x01BAB44B13921E80 (11/16/1995 5:43:45 PM)
…	…	…

In Section 3.3.2, Stream ID 1: Storage 1, the names for State Bits and Modified Time were corrected, and the correct values for Creation Time and Modified Time were included.

Changed from:

Byte offset	Field name	Field value
0x0480	Directory Entry Name	"Storage 1"
…	…	…
0x04E0	State Flags	0x00000000
0x04E4	Creation Time	0x0000000000000000
0x04EC	Modification Time	0x0000000000000000
…	…	…

Changed to:

Byte offset	Field name	Field value
0x0480	Directory Entry Name	"Storage 1"
…	…	…
0x04E0	State Bits	0x00000000
0x04E4	Creation Time	0x01BAB44B12F98800 (11/16/1995 5:43:44 PM)

Errata Published*	Description

0x04EC	Modified Time	0x01BAB44B13921E80 (11/16/1995 5:43:45 PM)
…	…	…

In Section 3.3.3, Stream ID 2: Stream 1 and Section 3.3.4, Stream ID 3: Unused, Free, the names for State Bits and Modified Time were corrected.

Changed from:

Byte offset	Field name	Field value
0x0500	Directory Entry Name	"Stream 1"
…	…	…
0x0560	State Flags	0x00000000
0x0564	Creation Time	0x0000000000000000
0x056C	Modification Time	0x0000000000000000
…	…	…

Changed to:

Byte offset	Field name	Field value
0x0500	Directory Entry Name	"Stream 1"
…	...	…
0x0560	State Bits	0x00000000
0x0564	Creation Time	0x0000000000000000
0x056C	Modified Time	0x0000000000000000
…	…	…

*Date format: YYYY/MM/DD

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

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

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

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

Errata below are for Protocol Document Version V28.0 – 2017/12/01.

Errata Published*	Description
2017/12/18	In Section 2.2.4.64.1, Request, the description of FILE_OVERWRITE and FILE_OVERWRITE_IF have been changed from: FILE_OVERWRITE: If the file already exists, it SHOULD be opened and truncated. If the file does not already exist, the operation MUST fail. The client MUST open the file with at least GENERIC_WRITE access for the command to succeed. FILE_OVERWRITE_IF: If the file already exists, it SHOULD be opened and truncated. If the file does not already exist, it SHOULD be created. The client MUST open the file with at least GENERIC_WRITE access. Changed to: FILE_OVERWRITE: If the file already exists, it SHOULD be opened and truncated. If the file does not already exist, the operation MUST fail. FILE_OVERWRITE_IF: If the file already exists, it SHOULD be opened and truncated. If the file does not already exist, it SHOULD be created.

*Date format: YYYY/MM/DD

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

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

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

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 V34.0 – 2017/12/01.

Errata Published*	Description
2018/01/16	In Section 2.2.3.47, CBFLT_PATH_IDS, the language for the description of the PathId field has been revised to more clearly indicate what the field contains. Changed from: ... PathId (variable): An array of Count identifiers each containing 32-bit path identifier. Changed to: ... PathId (variable): An array, of size Count, containing 32-bit path identifiers.

*Date format: YYYY/MM/DD

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

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

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

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

[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

[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

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 V15.0 – 2017/12/01.

Errata Published*	Description

2018/03/13	In Section 1.7, Versioning and Capability Negotiation, the sentence stating that only version 2.0 of the protocol is available has been removed.
	
	Changed from:
	…
	• Protocol versions: The CredSSP Protocol supports versioning (the version field of the TSRequest structure, section 2.2.1); however, version 2.0 is currently the only available version.
	
	Changed to:
	…
	• Protocol versions: The CredSSP Protocol supports versioning (the version field of the TSRequest structure, section 2.2.1).
	
	In Section 2.2.1, TSRequest, the section has been modified to specify that in version 5 and higher of the protocol, the pubKeyAuth field stores a computed hash of the public key, and to add the clientNonce field for version 5 to provide sufficient entropy during hash computation.
	
	Changed from:
	
	The TSRequest structure is the top-most structure used by the CredSSP client and CredSSP server. It contains the SPNEGO tokens or MAY contain Kerberos (1)/NTLM messages that are passed between the client and server, and either the public key authentication messages that are used to bind to the TLS session or the client credentials that are delegated to the server. The TSRequest message is always sent over the TLS-encrypted channel between the client and server in a CredSSP Protocol exchange (see step 1 in section 3.1.5).
	
	`TSRequest ::= SEQUENCE {`
	`  version  [0] INTEGER,`
	`  negoTokens [1] NegoData  OPTIONAL,`
	`  authInfo  [2] OCTET STRING OPTIONAL,`
	`  pubKeyAuth [3] OCTET STRING OPTIONAL,`
	`  errorCode  [4] INTEGER OPTIONAL`

Errata Published*	Description

	}
	
	version: This field specifies the supported version of the CredSSP Protocol. Valid values for this field are 2 and 3. If the version received is greater than the implementation understands, treat the peer as one that is compatible with the version of the CredSSP Protocol that the implementation understands.
	negoTokens: A NegoData structure, as defined in section 2.2.1.1, that contains the SPNEGO tokens or Kerberos (1)/NTLM messages that are passed between the client and server.
	authInfo: A TSCredentials structure, as defined in section 2.2.1.2, that contains the user's credentials that are delegated to the server. The authInfo field MUST be encrypted under the encryption key that is negotiated under the SPNEGO package. The authInfo field carries the message signature and then the encrypted data.
	pubKeyAuth: This field is used to assure that the public key that is used by the server during the TLS handshake belongs to the target server and not to a man-in-the-middle. This TLS session-binding is specified in section 3.1.5. After the client completes the SPNEGO phase of the CredSSP Protocol, it uses GSS_WrapEx() for the negotiated protocol to encrypt the server's public key. The pubKeyAuth field carries the message signature and then the encrypted public key to the server. In response, the server uses the pubKeyAuth field to transmit to the client a modified version of the public key (as specified in section 3.1.5) that is encrypted under the encryption key that is negotiated under SPNEGO.
	errorCode: If the negotiated protocol version is 3 and the SPNEGO exchange fails on the server, this field SHOULD be used to send the NTSTATUS failure code ([MS-ERREF] section 2.3) to the client so that it will know what failed and be able to display a descriptive error to the user.
	
	Changed to:
	The TSRequest structure is the top-most structure used by the CredSSP client and CredSSP server. It contains the SPNEGO tokens and MAY contain Kerberos (1)/NTLM messages that are passed between the client and server, and either the public key authentication messages that are used to bind to the TLS session or the client credentials that are delegated to the server. The TSRequest message is always sent over the TLS-encrypted channel between the client and server in a CredSSP Protocol exchange (see step 1 in section 3.1.5).
	
	`TSRequest ::= SEQUENCE {`
	`version [0] INTEGER,`
	`negoTokens [1] NegoData OPTIONAL,`
	`authInfo [2] OCTET STRING OPTIONAL,`
	`pubKeyAuth [3] OCTET STRING OPTIONAL,`
	`errorCode [4] INTEGER OPTIONAL,`
	`clientNonce [5] OCTET STRING OPTIONAL`
	`}`
	
	version: This field specifies the supported version of the CredSSP Protocol. Valid values for this field are 2, 3, 4, 5, and 6. If the version received is greater than the implementation understands, treat the peer as one that is compatible with the version of the CredSSP Protocol that the implementation understands.
	negoTokens: A NegoData structure, as defined in section 2.2.1.1, that contains the SPNEGO tokens or Kerberos (1)/NTLM messages that are passed between the client and server.
	authInfo: A TSCredentials structure, as defined in section 2.2.1.2, that contains the user's credentials that are delegated to the server. The authInfo field MUST be encrypted under the encryption key that is negotiated under the SPNEGO package. The authInfo field carries the message signature and then the encrypted data.
	pubKeyAuth: This field is used to assure that the public key that is used by the server during the TLS handshake belongs to the target server and not to a man-in-the-

Errata Published*	Description
	middle. This TLS session-binding is specified in section 3.1.5. After the client completes the SPNEGO phase of the CredSSP Protocol, it uses GSS_WrapEx() for the negotiated protocol to encrypt the server's public key. With version 4 or lower, the pubKeyAuth field carries the message signature and then the encrypted public key to the server. In response, the server uses the pubKeyAuth field to transmit to the client a modified version of the public key (as specified in section 3.1.5) that is encrypted under the encryption key that is negotiated under SPNEGO. In version 5 or higher, this field stores a computed hash of the public key. errorCode: If the negotiated protocol version is 3, 4, or 6, and the SPNEGO exchange fails on the server, this field SHOULD be used to send the NTSTATUS failure code ([MS-ERREF] section 2.3) to the client so that it knows what failed and be able to display a descriptive error to the user. clientNonce: A 32-byte array of cryptographically random bytes used to provide sufficient entropy during hash computation. This value is only used in version 5 or higher of this protocol. In Section 3.1.5, Processing Events, the processing rules for steps 3 through 5 have been changed to accommodate changes in versions 5 and 6 of the protocol. Changed from: … 2. Over the encrypted TLS channel, the SPNEGO, Kerberos (1), or NTLM handshake between the client and server completes authentication and establishes an encryption key that is used by the SPNEGO confidentiality services… … Note If the SPNEGO handshake fails on the server side and the client sent a version of 3 or greater, the server SHOULD send a TSRequest structure back to the client for which the errorCode field is populated with an unsuccessful NTSTATUS code ([MS-ERREF] section 2.3). The NTSTATUS code indicates the reason for the failure to the client. If the client receives a TSRequest message with the errorCode present, it must immediately fail with the provided status code and cease all further processing. The client encrypts the public key it received from the server (contained in the X.509 certificate) in the TLS handshake from step 1, by using the confidentiality support of the authentication protocol. The public key that is encrypted is the ASN.1-encoded SubjectPublicKey sub-field of SubjectPublicKeyInfo from the X.509 certificate, as specified in [RFC3280] section 4.1. The encrypted key is encapsulated in the pubKeyAuth field of the TSRequest structure and is sent over the TLS channel to the server. Note During this phase of the protocol, the OPTIONAL authInfo field is omitted from the TSRequest structure; the client MUST send its last SPNEGO token or Kerberos (1)/NTLM message to the server in the negoTokens field (see step 2) along with the encrypted public key in the pubKeyAuth field. After the server receives the public key in step 3, it first verifies that it has the same public key that it used as part of the TLS handshake in step 1. The server then adds 1 to the first byte representing the public key (the ASN.1 structure corresponding to the SubjectPublicKey field, as described in step 3) and encrypts the binary result by using the authentication protocol's encryption services. Due to the addition of 1 to the binary data, and encryption of the data as a binary structure, the resulting value might not be valid ASN.1-encoded values. The encrypted binary data is encapsulated in the pubKeyAuth field of the TSRequest structure and is sent over the encrypted TLS channel to the client.The addition of 1 to the first byte of the public key is performed so that the client-generated pubKeyAuth message cannot be replayed back to the client by an attacker. Note During this phase of the protocol, the OPTIONAL authInfo and negoTokens fields are omitted from the TSRequest structure. 3. After the client successfully verifies server authenticity by performing a binary comparison of the data from step 4 to that of the data representing the public key from

Errata Published*	Description
	the server's X.509 certificate (as specified in [RFC3280], section 4.1), it encrypts the user's credentials (either password or smart card PIN) by using the authentication protocol's encryption services. The resulting value is encapsulated in the authInfo field of the TSRequest structure and sent over the encrypted TLS channel to the server. The TSCredentials structure within the authInfo field of the TSRequest structure MUST NOT contain more than one of the following structures: TSPasswordCreds, TSSmartCardCreds, or TSRemoteGuardCreds structures. Note During this phase of the protocol, the option pubKeyAuth and negoTokens fields are omitted from the TSRequest structure. Note If the credentials were of type TSRemoteGuardCreds, the TLS channel continues to be used for redirected authentication requests, as specified in [MS-RDPEAR]. Changed to: … 2. Over the encrypted TLS channel, the SPNEGO, Kerberos (1), or NTLM handshake between the client and server completes authentication and establishes an encryption key that is used by the SPNEGO confidentiality services… … Note If the SPNEGO handshake fails on the server side and the client sent a version of 3 or greater, the server SHOULD send a TSRequest structure back to the client for which the errorCode field is populated with an unsuccessful NTSTATUS code ([MS-ERREF] section 2.3). The NTSTATUS code indicates the reason for the failure to the client. If the client receives a TSRequest message with the errorCode present, it must immediately fail with the provided status code and cease all further processing. 3. This step is version-dependent as follows: Version 5 or 6 The client SHOULD generate a cryptographically random 32-byte value and set the nonce field of the TSRequest structure to this value. It then computes a SHA256 hash of the ASN.1 encoded SubjectPublicKey concatenated with the bytes of the well-known string “CredSSP Client-To-Server Binding Hash” and the generated nonce. The hash is then encrypted using the confidentiality support of the authentication protocol. The process is defined as: Set ClientServerHashMagic to "CredSSP Client-To-Server Binding Hash" Set ClientServerHash to SHA256(UNICODE(ClientServerHashMagic), Nonce, SubjectPublicKey) Set TSRequest.pubKeyAuth to Encrypt(ClientServerHash) Note The hash MUST include the null terminator (\0) of the string. Version 2, 3, 4: The client encrypts the public key it received from the server (contained in the X.509 certificate) in the TLS handshake from step 1, by using the confidentiality support of the authentication protocol. The public key that is encrypted is the ASN.1-encoded SubjectPublicKey sub-field of SubjectPublicKeyInfo from the X.509 certificate, as specified in [RFC3280] section 4.1. All Versions: The encrypted key is encapsulated in the pubKeyAuth field of the TSRequest structure and is sent over the TLS channel to the server. Note During this phase of the protocol, the OPTIONAL authInfo field is omitted from the TSRequest structure; the client MUST send its last SPNEGO token or Kerberos (1)/NTLM message to the server in the negoTokens field (see step 2) along with the encrypted public key in the pubKeyAuth field. 4. This step is version-dependent as follows: Version 5 and 6

Errata Published*	Description
	After the server receives the TSRequest structure from step 3, it verifies the hash by computing the hash using the Nonce field from the request and the ASN.1-encoded public key used as part of the TLS handshake in step 1. If the hash matches, the server generates its own SHA256 hash of the SubjectPublicKey concatenated with the bytes of the well-known string "CredSSP Server-To-Client Binding Hash" and the provided nonce, and encrypts the binary result using the authentication protocol's encryption services. The process is defined as: Set ServerClientHashMagic to "CredSSP Server-To-Client Binding Hash" Set ServerClientHash to SHA256(UNICODE(ServerClientHashMagic), Nonce, SubjectPublicKey) Set TSRequest.pubKeyAuth to Encrypt(ServerClientHash) Note The hash MUST include the null terminator (\0) of the string. Version 2, 3, and 4 After the server receives the public key in step 3, it first verifies that it has the same public key that it used as part of the TLS handshake in step 1. The server then adds 1 to the first byte representing the public key (the ASN.1 structure corresponding to the SubjectPublicKey field, as described in step 3) and encrypts the binary result by using the authentication protocol's encryption services. Due to the addition of 1 to the binary data, and encryption of the data as a binary structure, the resulting value might not be valid ASN.1-encoded values. The addition of 1 to the first byte of the public key is performed so that the client-generated pubKeyAuth message cannot be replayed back to the client by an attacker. All versions: The encrypted binary data is encapsulated in the pubKeyAuth field of the TSRequest structure and is sent over the encrypted TLS channel to the client. Note The server SHOULD set the errorCode to STATUS_NOT_SUPPORTED if the server does not support the requested version. Note During this phase of the protocol, the OPTIONAL authInfo and negoTokens fields are omitted from the TSRequest structure. 5. The client validates the server authenticity by generating and comparing the server hash if using version 5, or higher. Otherwise, it performs a binary comparison of the data from step 4 to that of the data representing the public key from the server's X.509 certificate (as specified in [RFC3280], section 4.1). Once it successfully validates the server authenticity, it encrypts the user's credentials (either password or smart card PIN) by using the authentication protocol's encryption services. The resulting value is encapsulated in the authInfo field of the TSRequest structure and sent over the encrypted TLS channel to the server. The TSCredentials structure within the authInfo field of the TSRequest structure MUST NOT contain more than one of the following structures: TSPasswordCreds, TSSmartCardCreds, or TSRemoteGuardCreds structures. Note During this phase of the protocol, the OPTIONAL pubKeyAuth and negoTokens fields are omitted from the TSRequest structure. Note If the credentials were of type TSRemoteGuardCreds, the TLS channel continues to be used for redirected authentication requests, as specified in [MS-RDPEAR]. In Section 4, Protocol Examples, Figure 1 (CredSSP negotiation sequence using SPNEGO) has been updated. Changed from:

Errata Published*	Description

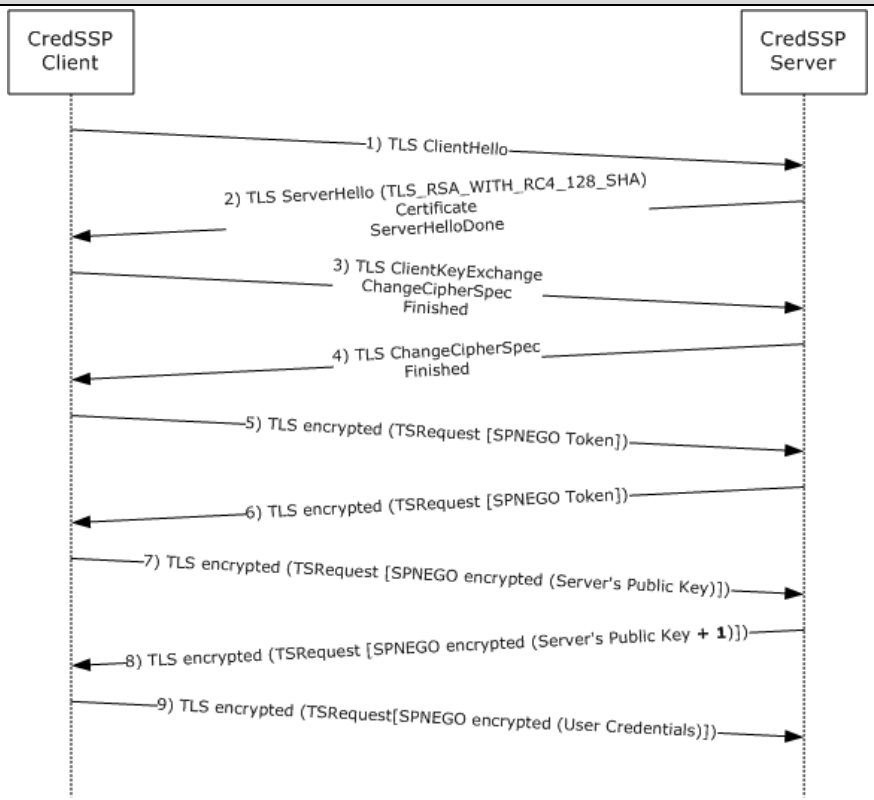
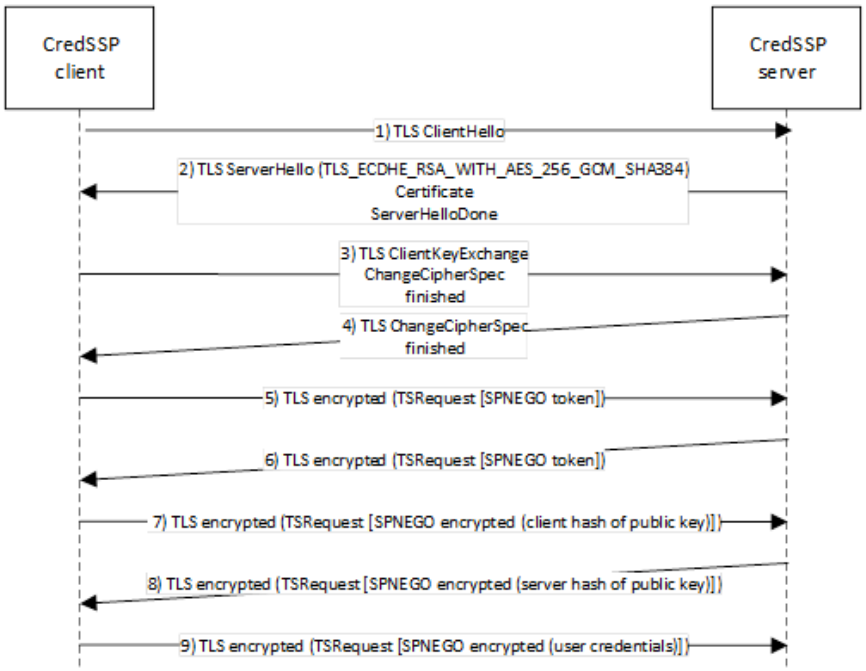


Figure 1: CredSSP negotiation sequence using SPNEGO

Changed to:



Errata Published*	Description
	Figure 1: CredSSP negotiation sequence using SPNEGO

*Date format: YYYY/MM/DD

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

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

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

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

[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

[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

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

[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

[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

[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

[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

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 15, 2017 - Download

December 1, 2017 - Download

[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

[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

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

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

Errata Published*	Description
2018/01/16	In the sections listed below, unnecessary blank spaces have been removed from the syntax and/or section numbers linked corrected. For example, in Section 3.9.5.1.1, PUT, "DSC- RegisterDscAgentRequest-URI-End" has been changed to" DSC-RegisterDscAgentRequest-URI-End" and in Section 3.12.5.1.1.3, Processing Details, the linked section number has been changed from 3.11.5.1.1.1 to 3.12.5.1.1.1. 3.5.5.1.1, GET 3.7.5.1.1, GET 3.9.5.1.1, PUT 3.10.5.1.1, POST 3.11.5.1.1, GET 3.12, CertificateRotation Details 3.12.5.1.1, POST 3.12.5.1.1.3, Processing Details

*Date format: YYYY/MM/DD

[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

Errata below are for Protocol Document Version V34.0 – 2017/12/01.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2018/01/29</td><td>In Section 2.3.2, EVENT_HEADER, two new entries - EVENT_HEADER_FLAG_DECODE_GUID and EVENT_HEADER_FLAG_PROCESSOR_INDEX - have been added to the Flags field.

Changed from:

Flags: Flags that provide information about the event such as the type of session it was logged to and whether the event contains extended data. This member can contain one or more of the following flags.

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>EVENT_HEADER_FLAG_64_BIT_HEADER</td><td>Indicates that the provider was running on a 64-bit computer.</td></tr>
<tr><td>EVENT_HEADER_FLAG_CLASSIC_HEADER</td><td>Indicates that provider used a trace event function to log the event.</td></tr>
</table>

Changed to:

Flags: Flags that provide information about the event such as the type of session it was logged to and whether the event contains extended data. This member can contain one or more of the following flags.

<table>
<tr><th>Value</th><th>Meaning</th></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>…</td><td>…</td></tr>
<tr><td>EVENT_HEADER_FLAG_64_BIT_HEADER</td><td>Indicates that the provider was running on a 64-bit computer.</td></tr>
<tr><td>EVENT_HEADER_FLAG_DECODE_GUID</td><td>Indicates that the ProviderId member of the event record is a decode GUID rather than a control GUID.<2></td></tr>
<tr><td>EVENT_HEADER_FLAG_CLASSIC_HEADER</td><td>Indicates that provider used a trace event function to log the event.</td></tr>
<tr><td>EVENT_HEADER_FLAG_PROCESSOR_INDEX</td><td>If this flag is set, the identifier for the CPU that logged the event MUST be accessed using the ProcessorIndex member of the BufferContext member of the event record.
If this flag is not set, the identifier for the CPU that logged the event MUST be read from the ProcessorNumber member of the BufferContext member of the event record.<3></td></tr>
</table>
<2> Section 2.3.2: Not supported in Windows versions earlier than the Windows 10 v1709 operating system client or the Windows Server v1709 operating system server releases. The control GUID will usually be found in the ExtendedData array. Typically, the presence of this flag indicates that the event is associated with an automatically-generated manifest, such as one generated by the Windows software trace preprocessor.
<3> Section 2.3.2: Not supported in Windows versions earlier than the Windows 8 client or Windows Server 2012 server releases.
</td></tr>
<tr><td>2017/12/18</td><td>
In Section 2.4.7, SECURITY_INFORMATION, an entry for the PROCESS_TRUST_LABEL_SECURITY_INFORMATION value has been added:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>PROCESS_TRUST_LABEL_SECURITY_INFORMATION
0x00000080</td><td>Reserved.</td></tr>
</table>
</td></tr>
</table>

*Date format: YYYY/MM/DD

[MS-DVRD]: Device Registration Discovery Protocol

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

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

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

[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

[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

[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

[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

[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

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

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-ERREF]: Windows Error Codes

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

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

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

[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

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

July 18, 2016 - Download

[MS-FASP]: Firewall and Advanced Security Protocol

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

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

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

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-FSA]: File System Algorithms

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

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

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

[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

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 15, 2017 - Download

December 1, 2017 - Download

[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

[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

[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

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 V25.0 – 2017/12/01.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2018/01/16</td><td>In Section, 2.2.1.22, Targeting, Windows Server operating system has been added to the table of OS version attributes.

Changed from:

<table>
<tr><th>Criterion</th><th>Attribute</th><th>Attribute description</th></tr>
<tr><td>…</td><td>…</td><td>…</td></tr>
<tr><td>FilterOs</td><td></td><td>Note From the perspective of interoperability, the same enumeration values for class and version are required for the correct filtering operation to occur for the classes and versions defined in their respective enumerations. An implementation is not constrained from including additional enumeration values for class or version to provide support for additional platforms.</td></tr>
<tr><td></td><td>class</td><td>(optional) SHOULD<16> be NE, 9X, or NT.</td></tr>
<tr><td></td><td>version</td><td>(optional) The value SHOULD<17> correspond to the operating system version.</td></tr>
</table>
<17> Section 2.2.1.22: The enumerated values and corresponding Windows releases are as follows:
<table>
<tr><th>Version attribute</th><th>Windows release</th><th>Version attribute</th><th>Windows release</th></tr>
</table>
</td></tr>
</table>

Errata Published*	Description

NE	Any	2K8	Windows Server 2008
95	Windows 95	WIN7	Windows 7
98	Windows 98	2K8R2	Windows Server 2008 R2
ME	Windows Millennium Edition	WIN8	Windows 8
NT	Windows NT operating system	WIN8S	Windows Server 2012
2K	Windows 2000 operating system	WINBLUE	Windows 8.1
XP	Windows XP	WINBLUESRV	Windows Server 2012 R2
2K3	Windows Server 2003	WINTHRESHOLD	Windows 10
2K3R2	Windows Server 2003 R2	WINTHRESHOLDSRV	Windows Server 2016
VISTA	Windows Vista		

Changed to:

Criterion	Attribute	Attribute description
…	…	…
FilterOs		Note From the perspective of interoperability, the same enumeration values for class and version are required for the correct filtering operation to occur for the classes and versions defined in their respective enumerations. An implementation is not constrained from including additional enumeration values for class or version to provide support for additional platforms.
	class	(optional) SHOULD<16> be NE, 9X, or NT.
	version	(optional) The value SHOULD<17> correspond to the operating system version.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<17> Section 2.2.1.22: The enumerated values and corresponding Windows releases are as follows:
<table>
<tr><th>Version attribute</th><th>Windows release</th><th>Version attribute</th><th>Windows release</th></tr>
<tr><td>NE</td><td>Any</td><td>2K8</td><td>Windows Server 2008</td></tr>
<tr><td>95</td><td>Windows 95</td><td>WIN7</td><td>Windows 7</td></tr>
<tr><td>98</td><td>Windows 98</td><td>2K8R2</td><td>Windows Server 2008 R2</td></tr>
<tr><td>ME</td><td>Windows Millennium Edition</td><td>WIN8</td><td>Windows 8</td></tr>
<tr><td>NT</td><td>Windows NT operating system</td><td>WIN8S</td><td>Windows Server 2012</td></tr>
<tr><td>2K</td><td>Windows 2000 operating system</td><td>WINBLUE</td><td>Windows 8.1</td></tr>
<tr><td>XP</td><td>Windows XP</td><td>WINBLUESRV</td><td>Windows Server 2012 R2</td></tr>
<tr><td>2K3</td><td>Windows Server 2003</td><td>WINTHRESHOLD</td><td>Windows 10</td></tr>
<tr><td>2K3R2</td><td>Windows Server 2003 R2</td><td>WINTHRESHOLDSRV</td><td>Windows Server 2016, Windows Server operating system</td></tr>
<tr><td>VISTA</td><td>Windows Vista</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td></td><td></td></tr>
</table>

*Date format: YYYY/MM/DD

[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

[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

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

[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

[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

[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

[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

[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

[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

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

[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

[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

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

[MS-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

[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

[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

[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

Errata below are for Protocol Document Version V41.0 – 2017/12/01.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2018/01/29</td><td>In Section 3.1.4.4.3, LsarQueryInformationPolicy2 (Opnum 46), we have corrected the name of an abstract data model field.

Changed from:

<table>
<tr><th>Value of InformationClass parameter</th><th>Information returned to caller from abstract data model</th></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td>PolicyDnsDomainInformationInt</td><td>DNS Domain Information</td></tr>
<tr><td>PolicyLocalAccountDomainInformation</td><td>AccountDomainInformation</td></tr>
</table>

Changed to:

<table>
<tr><th>Value of InformationClass parameter</th><th>Information returned to caller from abstract data model</th></tr>
<tr><td>...</td><td>...</td></tr>
<tr><td>PolicyDnsDomainInformationInt</td><td>DNS Domain Information</td></tr>
<tr><td>PolicyLocalAccountDomainInformation</td><td>Account Domain Information</td></tr>
</table>
</td></tr>
</table>

*Date format: YYYY/MM/DD

[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

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

June 1, 2017 - Download

September 15, 2017 - Download

[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

[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

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 15, 2017 - Download

December 1, 2017 - Download

[MS-MDM]: Mobile Device Management Protocol

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

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

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

[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

[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

[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

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 – 2017/12/01.

Errata Published*	Description
2018/03/05	In Section 1.2.1, Normative References, a new reference has been added: "[MSKB-4088889] Microsoft Corporation, "March 20, 2018-KB4088889", https://support.microsoft.com/en-us/help/4088889" In Section 2.2.3, wsignin1.0 Request Message, information has been added about the support for the mfa_max_age parameter that was added through KB 4088889. Changed from: mfa_max_age (optional): This value is a string ... . The AD FS server ignores this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_3 or higher ([MS-OAPX] section 3.2.1.1). The IP/STS SHOULD have a setting that configures it ... Changed to: mfa_max_age (optional): This value is a string ... . The AD FS server ignores this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_3 or higher ([MS-OAPX] section 3.2.1.1).<21> The IP/STS SHOULD have a setting that configures it ... <21> Section 2.2.3: Even though AD_FS_BEHAVIOR_LEVEL_3 is supported on Windows Server 2016, the mfa_max_age parameter is supported on Windows Server 2016 only if [MSKB-4088889] is installed.

*Date format: YYYY/MM/DD

[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

Errata below are for Protocol Document Version V4.0 – 2017/09/15.

Errata Published*	Description
2018/02/26	In multiple sections in this document, many resource and parameter names have been updated to correct capitalizations and remove spaces. For example, in Section 2.2.3 Common URI Parameters, parameter operation-id has been changed to OperationId. For details on the changes, see this Diff document.

*Date format: YYYY/MM/DD

[MS-NCT]: Network Cost Transfer Protocol

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

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

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

[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

[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

[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

[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

[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

[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

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

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

[MS-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

[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

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 V8.0 – 2017/12/01.

Errata Published*	Description
2018/03/05	In Section 1.2.1, Normative References, a new reference has been added: "[MSKB-4088889] Microsoft Corporation, "March 20, 2018-KB4088889", https://support.microsoft.com/en-us/help/4088889" In Section 2.2.2, Common URI Parameters, information has been added about the support for the mfa_max_age parameter that was added through KB 4088889.. Changed from: mfa_max_age: OPTIONAL. This query parameter is used... The AD FS server ignores this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_3 or higher. Changed to: mfa_max_age: OPTIONAL. This query parameter is used... The AD FS server ignores this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_3 or higher.<5> <5> Section 2.2.2: Even though AD_FS_BEHAVIOR_LEVEL_3 is supported on Windows Server 2016, the mfa_max_age parameter is supported on Windows Server 2016 only if [MSKB-4088889] is installed. In Section 2.2.2.11, mfa_max_age, a reference has been added for additional support information about the mfa_max_age parameter. Changed from: The AD FS server ignores this parameter unless its ad_fs_behavior_level is

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>AD_FS_BEHAVIOR_LEVEL_3 or higher.

Changed to:
The AD FS server ignores this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_3 or higher. See section 2.2.2 for additional support information.

In Section 7, Appendix B Product Behavior, product behavior note <6> (for section 3.2.1.1): AD_FS_BEHAVIOR_LEVEL_3 has been added to the list of behavior levels that are supported by Windows Server 2016.

Changed from:
<table><tr><td>Windows Server 2016</td><td>AD_FS_BEHAVIOR_LEVEL_1,
AD_FS_BEHAVIOR_LEVEL_2</td></tr></table>
Changed to:
<table><tr><td>Windows Server 2016</td><td>AD_FS_BEHAVIOR_LEVEL_1,
AD_FS_BEHAVIOR_LEVEL_2,
AD_FS_BEHAVIOR_LEVEL_3</td></tr></table></td></tr>
</table>

*Date format: YYYY/MM/DD

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

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

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

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 26, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

Errata below are for Protocol Document Version V6.0 – 2017/12/01.

Errata Published*	Description
2018/03/05	In Section 1.2.1, Normative References, a new reference has been added: "[MSKB-4088889] Microsoft Corporation, "March 20, 2018-KB4088889", https://support.microsoft.com/en-us/help/4088889" In Section 2.2.2.1, krctx, information has been added about the support for the krctx parameter and the "winhello_cert_kr" value that was added through KB 4088889. Changed from: The AD FS server ignores this parameter unless its AD FS behavior level is AD_FS_BEHAVIOR_LEVEL_3 or higher ([MS-OAPX] section 3.2.1.1) and the AD FS server is capable of processing the parameter, as indicated by the value "winhello_cert_kr" being included in the capabilities field of the OpenID Provider Metadata ([MS-OIDCE] section 2.2.3.2). Changed to: The AD FS server ignores this parameter unless its AD FS behavior level is AD_FS_BEHAVIOR_LEVEL_3 or higher ([MS-OAPX] section 3.2.1.1) and the AD FS server is capable of processing the parameter, as indicated by the value "winhello_cert_kr" being included in the capabilities field of the OpenID Provider Metadata ([MS-OIDCE] section 2.2.3.2).<1> <1> Section 2.2.2.1: Even though AD_FS_BEHAVIOR_LEVEL_3 is supported on Windows Server 2016, the krctx parameter and the "winhello_cert_kr" value are supported on Windows Server 2016 only if [MSKB-4088889] is installed. In Section 3.1.5.1.4.3, Processing Details, a reference has been added for additional support information about the krctx parameter and the "winhello_cert_kr" value. Changed from: The "winhello_cert_kr" value is supported on the AD FS server only if its AD FS behavior level is AD_FS_BEHAVIOR_LEVEL_3 or higher. See section 2.2.2.1 for

Errata Published*	Description
	additional support information.The "winhello_cert_kr" value is supported on the AD FS server only if its AD FS behavior level is AD_FS_BEHAVIOR_LEVEL_3 or higher. Changed to: The "winhello_cert_kr" value is supported on the AD FS server only if its AD FS behavior level is AD_FS_BEHAVIOR_LEVEL_3 or higher. See section 2.2.2.1 for additional support information.The "winhello_cert_kr" value is supported on the AD FS server only if its AD FS behavior level is AD_FS_BEHAVIOR_LEVEL_3 or higher. See section 2.2.2.1 for additional support information.

*Date format: YYYY/MM/DD

[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

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

Errata below are for Protocol Document Version V5.0 – 2017/12/01.

Errata Published*	Description
2018/03/05	In Section 1.2.1, Normative References, a new reference has been added: "[MSKB-4088889] Microsoft Corporation, "March 20, 2018-KB4088889", https://support.microsoft.com/en-us/help/4088889" In Section 3.2.5.3.1.3, Processing Details, information has been added about the support for the krctx parameter and the "winhello_cert_kr" value that was added through KB 4088889. Changed from: "winhello_cert_kr" (AD FS behavior level is AD_FS_BEHAVIOR_LEVEL_3 or higher). The server can include "winhello_cert_kr" in the capabilities field if it supports the krctx parameter as part of the OAuth token request ([MS-OAPXBC] section 2.2.2). Changed to: "winhello_cert_kr" (AD FS behavior level is AD_FS_BEHAVIOR_LEVEL_3 or higher). The server can include "winhello_cert_kr" in the capabilities field if it supports the krctx parameter as part of the OAuth token request ([MS-OAPXBC] section 2.2.2).<11> <11> Section 3.2.5.3.1.3: Even though AD_FS_BEHAVIOR_LEVEL_3 is supported on Windows Server 2016 ([MS-OAPX] section 3.2.1.1), the krctx parameter and the "winhello_cert_kr" value are supported on Windows Server 2016 only if [MSKB-4088889] is installed.
2018/01/16	In this document, information has been added about support for the Front-Channel Logout protocol in Windows Server v1709. In Section 1.2.1, Normative References, a reference for [MSKB-4058258] has been added: [MSKB-4058258] Microsoft Corporation, "January 23, 2018 - KB4058258", https://support.microsoft.com/help/4058258 In Section 6, Appendix A: Product Behavior, a citation to [MSKB-4058258] has been added to several product behavior notes as shown below.

Errata Published*	Description
	Behavior note <1> (for section 1.5), changed from: <1> Section 1.5: Only Windows Server 2016 with [MSKB-4019472] installed but without [MSKB-4038801] installed and Windows Server v1709 operating system implement the REQUIRED parts for RP-Initiated Logout as defined in [OIDCSession] section 5. Changed to: <1> Section 1.5: Only Windows Server 2016 with [MSKB-4019472] installed but without [MSKB-4038801] installed and Windows Server v1709 operating system without [MSKB-4058258] installed implement the REQUIRED parts for RP-Initiated Logout as defined in [OIDCSession] section 5. Behavior note <3> (for section 2.2.3.2), changed from: <3> Section 2.2.3.2: In Windows Server 2016 with [MSKB-4019472] installed but without [MSKB-4038801] installed and in Windows Server v1709, the AD FS server can be configured in an implementation-specific way to either return or not return the end_session_endpoint metadata. Changed to: <3> Section 2.2.3.2: In Windows Server 2016 with [MSKB-4019472] installed but without [MSKB-4038801] installed and in Windows Server v1709 without [MSKB-4058258] installed, the AD FS server can be configured in an implementation-specific way to either return or not return the end_session_endpoint metadata. Behavior note <4> (for section 2.2.3.2), changed from: <4> Section 2.2.3.2: Windows Server 2016 without [MSKB-4038801] installed and Windows Server v1709 do not support [OIDCFrontChanLO]. Changed to: <4> Section 2.2.3.2: Windows Server 2016 without [MSKB-4038801] installed and Windows Server v1709 without [MSKB-4058258] installed do not support [OIDCFrontChanLO]. Behavior note <7> (for section 3.1.5.4), changed from: <7> Section 3.1.5.4: Logout support in Windows Server 2016 without [MSKB-4038801] installed and in Windows Server v1709 is limited to OpenID Connect Session Management ([OIDCSession], specifically, section 5). Changed to: <7> Section 3.1.5.4: Logout support in Windows Server 2016 without [MSKB-4038801] installed and in Windows Server v1709 without [MSKB-4058258] installed is limited to OpenID Connect Session Management ([OIDCSession], specifically, section 5). Behavior note <11> (for section 3.2.5.4), changed from: <11> Section 3.2.5.4: The following support information applies to the Logout endpoint:

Errata Published*	Description
	... - The Logout endpoint is implemented as OpenID Connect Session Management ([OIDCSession], specifically, section 5) in Windows Server v1709. - The Logout endpoint is implemented as OpenID Connect Front-Channel Logout ([OIDCFrontChanLO]) in Windows Server 2016 with [MSKB-4038801] installed. Changed to: <11> Section 3.2.5.4: The following support information applies to the Logout endpoint: ... - The Logout endpoint is implemented as OpenID Connect Session Management ([OIDCSession], specifically, section 5) in Windows Server v1709 without [MSKB-4058258] installed. - The Logout endpoint is implemented as OpenID Connect Front-Channel Logout ([OIDCFrontChanLO]) in Windows Server 2016 with [MSKB-4038801] installed and Windows Server v1709 with [MSKB-4058258] installed.

*Date format: YYYY/MM/DD

[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

[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

[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

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

[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

[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

[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

[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

[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

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

[MS-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

Errata below are for Protocol Document Version V1.1 – 2017/06/01.

Errata Published*	Description
2018/03/13	In Section 1, Introduction, the applicable server context for this protocol has been clarified. Changed from: This document describes an extension to the RDP dynamic virtual channel protocol. Changed to: This document describes an extension to the RDP dynamic virtual channel protocol that is used exclusively in the context of Windows Multipoint Server scenarios.

*Date format: YYYY/MM/DD

[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

Errata below are for Protocol Document Version V47.0 – 2017/12/01.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2018/01/16</td><td>In Section 2.2.5.1.1, Set Error Info PDU Data (TS_SET_ERROR_INFO_PDU), the errorInfo field table with code has been updated to add a value when no error has occurred.

Changed from:
Protocol-independent codes:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>ERRINFO_RPC_INITIATED_DISCONNECT
0x00000001</td><td>The disconnection was initiated by an administrative tool on the server in another session.</td></tr>
<tr><td>ERRINFO_RPC_INITIATED_LOGOFF
0x00000002</td><td>The disconnection was due to a forced logoff initiated by an administrative tool on the server in another session.</td></tr>
<tr><td>ERRINFO_IDLE_TIMEOUT
0x00000003</td><td>The idle session limit timer on the server has elapsed.</td></tr>
<tr><td>ERRINFO_LOGON_TIMEOUT
0x00000004</td><td>The active session limit timer on the server has elapsed.</td></tr>
<tr><td>ERRINFO_DISCONNECTED_BY_OTHERCONNECTION
0x00000005</td><td>Another user connected to the server, forcing the disconnection of the</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description

	current connection.
ERRINFO_OUT_OF_MEMORY 0x00000006	The server ran out of available memory resources.
ERRINFO_SERVER_DENIED_CONNECTION 0x00000007	The server denied the connection.
ERRINFO_SERVER_INSUFFICIENT_PRIVILEGES 0x00000009	The user cannot connect to the server due to insufficient access privileges.
ERRINFO_SERVER_FRESH_CREDENTIALS_REQUIRED 0x0000000A	The server does not accept saved user credentials and requires that the user enter their credentials for each connection.
ERRINFO_RPC_INITIATED_DISCONNECT_BYUSER 0x0000000B	The disconnection was initiated by an administrative tool on the server running in the user's session.
ERRINFO_LOGOFF_BY_USER 0x0000000C	The disconnection was initiated by the user logging off his or her session on the server.

Changed to:

Protocol-independent codes:

Value	Meaning
ERRINFO_NONE 0x00000000	No error has occurred. This code SHOULD be ignored.
ERRINFO_RPC_INITIATED_DISCONNECT 0x00000001	The disconnection was initiated by an administrative tool on the server in another session.
ERRINFO_RPC_INITIATED_LOGOFF 0x00000002	The disconnection was due to a forced logoff initiated by an administrative tool on the server in another session.
ERRINFO_IDLE_TIMEOUT 0x00000003	The idle session limit timer on the server has elapsed.
ERRINFO_LOGON_TIMEOUT 0x00000004	The active session limit timer on the server has elapsed.
ERRINFO_DISCONNECTED_BY_OTHERCONNECTION	Another user connected to

Errata Published*	Description	
	0x00000005	the server, forcing the disconnection of the current connection.
	ERRINFO_OUT_OF_MEMORY 0x00000006	The server ran out of available memory resources.
	ERRINFO_SERVER_DENIED_CONNECTION 0x00000007	The server denied the connection.
	ERRINFO_SERVER_INSUFFICIENT_PRIVILEGES 0x00000009	The user cannot connect to the server due to insufficient access privileges.
	ERRINFO_SERVER_FRESH_CREDENTIALS_REQUIRED 0x0000000A	The server does not accept saved user credentials and requires that the user enter their credentials for each connection.
	ERRINFO_RPC_INITIATED_DISCONNECT_BYUSER 0x0000000B	The disconnection was initiated by an administrative tool on the server running in the user's session.
	ERRINFO_LOGOFF_BY_USER 0x0000000C	The disconnection was initiated by the user logging off his or her session on the server.

*Date format: YYYY/MM/DD

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

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

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

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

[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

[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

[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

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

Errata below are for Protocol Document Version V18.0 – 2017/12/01.

Errata Published*	Description
2018/01/16	In Section 2.2.1.2, DVC Capabilities Response PDU (DYNVC_CAPS_RSP), changed from: Sp (2 bits): Unused. MUST be set to 0x00. Changed to: Sp (2 bits): Unused. SHOULD be set to 0x00<7>. <7>Windows implementations do not initialize the Sp field. As a result, its value is random. In Section 2.2.3.4, DVC Data Compressed PDU (DYNVC_DATA_COMPRESSED), a Product Behavior Note (PBN) has been added to describe the initial value of the Sp field. Changed from: Sp (2 bits): Unused. SHOULD be initialized to 0x00. Changed to: Sp (2 bits): Unused. SHOULD be initialized to 0x00.<9> <9>Windows implementations do not initialize the Sp field. As a result, its value is random. In Section 2.2.1.1.1, Version 1 (DYNVC_CAPS_VERSION1), the Product Behavior Note (PBN) has been revised to clarify the description of the initial value of the Sp field. Changed from:

Errata Published*	Description
	Sp (2 bits): Unused. SHOULD be initialized to 0x00.<2> <2>Windows implementations initialize Sp to 0x02. Changed to: Sp (2 bits): Unused. SHOULD be initialized to 0x00.<2> <2>Windows implementations do not initialize the Sp field. As a result, its value is random. In Section 2.2.1.1.2, Version 2 (DYNVC_CAPS_VERSION2), the Product Behavior Note (PBN) has been revised to clarify the description of the initial value of the Sp field. Changed from: Sp (2 bits): Unused. SHOULD be set to 0x00.<4> <4>Windows implementations initialize Sp to 0x02. Changed to: Sp (2 bits): Unused. SHOULD be set to 0x00.<4> <4>Windows implementations do not initialize the Sp field. As a result, its value is random. In Section 2.2.1.1.3, Version 3 (DYNVC_CAPS_VERSION3), the Product Behavior Note (PBN) has been revised to clarify the description of the initial value of the Sp field. Changed from: Sp (2 bits): Unused. SHOULD be set to 0x00.<6> <6>Windows implementations initialize Sp to 0x02. Changed to: Sp (2 bits): Unused. SHOULD be set to 0x00.<6> <6>Windows implementations do not initialize the Sp field. As a result, its value is random.

*Date format: YYYY/MM/DD

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

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

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

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

[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

[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

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

March 20, 2017 - Download

September 15, 2017 - Download

[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

[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

[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

[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

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

March 2, 2016 - Download

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

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

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

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

[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

[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

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

[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

[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

[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

[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

[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

[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

[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

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

[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

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

[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

[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

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

[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

[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

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

December 1, 2017 - Download

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

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

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

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

[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

[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

[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.

RSS
Atom

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

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

Errata below are for Protocol Document Version V39.0 – 2017/12/01.

Errata Published*	Description
2018/02/12	In Section 1.1, Glossary, the default setting for UAS Compatibility has been updated. Changed from: UAS Compatibility: A configuration mode that affects protocol behavior constraints specified in this document. "UAS" is the acronym for "User Account Security (Database)" and refers to products no longer supported, such as Microsoft NT LAN Manager. The default setting in Windows is "off". Changed to: UAS Compatibility: A configuration mode that affects protocol behavior constraints specified in this document. "UAS" is the acronym for "User Account Security (Database)" and refers to products no longer supported, such as Microsoft NT LAN Manager. The default setting in Windows is "on". In Section 3.1.1.6, Attribute Constraints for Originating Updates, the value for minPwdLength has been updated. Changed from: … 6. minPwdLength MUST be less than or equal to 256 unless uASCompat is nonzero, in which case minPwdLength MUST be less than or equal to 20; on error, return a failure code. Changed to: … 6. minPwdLength MUST be less than or equal to 256 unless uASCompat is nonzero, in

Errata Published*	Description
	which case minPwdLength MUST be less than or equal to 14; on error, return a failure code.

*Date format: YYYY/MM/DD

[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

[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

Errata below are for Protocol Document Version V27.1 – 2017/09/15.

Errata Published*	Description
2018/01/29	A new section - Section 3.1.4.49, RCreateWowService (Opnum 60) - to document one method, RCreateWowService (Opnum 60), has been added and corresponding updates have been made to the IDL. For details on these changes, see the Diff file here.

*Date format: YYYY/MM/DD

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

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

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

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

[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

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

Errata below are for Protocol Document Version V47.0 – 2017/12/01.

Errata Published*	Description
2017/12/18	In Section 3.3.5.10.1, Receiving any Information Level, changed from: If the server receives client request with a pass-through Information Level (section 2.2.2.3.5) and the server supports the CAP_INFOLEVEL_PASSTHRU capability in Server.Capabilities, then the server MUST decrement the Information Level value by SMB_INFO_PASSTHROUGH by treating the value as little-endian, and pass that value to the underlying object store. If the Information Level includes any request data, then the data MUST also be passed to the underlying object store.<129> If the server does not support pass-through Information Levels, then it MUST fail this request with STATUS_INVALID_PARAMETER. The returned status and response data, if any, are sent to the client in a Trans2 subcommand response message that corresponds to the same subcommand that initiated the request. Changed to: If the server receives client request with a pass-through Information Level (section 2.2.2.3.5) and the CAP_INFOLEVEL_PASSTHRU bit is set in Server.Capabilities, then the server MUST decrement the Information Level value by SMB_INFO_PASSTHROUGH by treating the value as little-endian, and pass that value to the underlying object store. If the Information Level includes any request data, then the data MUST also be passed to the underlying object store.<129> If the server does not support pass-through Information Levels, then it MUST fail this request with STATUS_INVALID_PARAMETER. The returned status and response data, if any, are sent to the client in a Trans2 subcommand response message that corresponds to the same subcommand that initiated the request.<130> <130> Section 3.3.5.10.1: If CAP_INFOLEVEL_PASSTHRU capability is set in Server.Capabilities, and client requested "FileAllInformation" pass-through Information

Errata Published*	Description
	Level, Windows-based servers respond with the structure specified in [MS-CIFS] section 2.2.8.3.10. In Section 2.2.2.3.5, Pass-through Information Level Codes, changed from: This document provides an extension of a new Information Level code value range called pass-through Information Levels, which can be used to set or query information on the server. These Information Levels allow SMB clients to directly query Information Levels native to the underlying object store.<18> <18> Section 2.2.2.3.5: pass-through Information Levels on Windows-based servers map directly to native Windows NT operating system Information Classes, as specified in [MS-FSCC] sections 2.4 and 2.5. Windows- based servers do not support setting the following NT Information Levels via the pass-through Information Level mechanism. Changed to: This document provides an extension of a new Information Level code value range called pass-through Information Levels, which can be used to set or query information on the server. These Information Levels allow SMB clients to directly query Information Levels native to the underlying object store.<18> <18> Section 2.2.2.3.5: On Windows-based servers, pass-through Information level "FileAllInformation" is mapped to SMB_QUERY_FILE_ALL_INFO, as specified in [MS-CIFS] section 2.2.8.3.10. All other pass-through Information Levels map directly to native Windows NT operating system Information Classes, as specified in [MS-FSCC] sections 2.4 and 2.5. Windows- based servers do not support setting the following NT Information Levels via the pass-through Information Level mechanism.

*Date format: YYYY/MM/DD

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

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

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

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 26, 2016 - Download

March 20, 2017 - Download

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

Errata below are for Protocol Document Version V54.0 – 2017/12/01.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2018/02/26</td><td>In Section 2.2.9.2, SMB2 TREE_CONNECT_CONTEXT Request Values, the valid values for ContextType have been changed from:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>SMB2_RESERVED_TREE_CONNECT_CONTEXT_ID
0x00000000</td><td>This value is reserved.</td></tr>
<tr><td>SMB2_REMOTED_IDENTITY_TREE_CONNECT_CONTEXT_ID
0x00000001</td><td>The Data field contains remoted identity tree connect context data as specified in section 2.2.9.2.1.</td></tr>
</table>

Changed to:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>SMB2_RESERVED_TREE_CONNECT_CONTEXT_ID
0x0000</td><td>This value is reserved.</td></tr>
<tr><td>SMB2_REMOTED_IDENTITY_TREE_CONNECT_CONTEXT_ID
0x0001</td><td>The Data field contains remoted identity tree connect</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description
	context data as specified in section 2.2.9.2.1.
2018/02/26	In Section 3.3.5.2.9, Verifying the Session, the following has been changed from: If Connection.Dialect belongs to the SMB 3.x dialect family, and Session.EncryptData is TRUE, the server MUST locate the Request in Connection.RequestList for which Request.MessageId matches the MessageId value in the SMB2 header of the request. If Request.IsEncrypted is FALSE, the server MUST fail the request with STATUS_ACCESS_DENIED. Changed to: If Connection.Dialect belongs to the SMB 3.x dialect family, and Session.EncryptData is TRUE, the server MUST do the following: If the server supports the 3.1.1 dialect, locate the Request in Connection.RequestList for which Request.MessageId matches the MessageId value in the SMB2 header of the request. Otherwise, if the server supports 3.0 or 3.0.2 dialect, and RejectUnencryptedAccess is TRUE, locate the Request in Connection.RequestList for which Request.MessageId matches the MessageId value in the SMB2 header of the request. If Request.IsEncrypted is FALSE, the server MUST fail the request with STATUS_ACCESS_DENIED. In Section 3.3.5.2.11, Verifying the Tree Connect, the following has been changed from: The server MUST look up the TreeConnect in Session.TreeConnectTable by using the TreeId in the SMB2 header of the request. If no tree connect is found, the request MUST be failed with STATUS_NETWORK_NAME_DELETED. If Connection.Dialect belongs to the SMB 3.x dialect family, the server MUST fail the request with STATUS_ACCESS_DENIED in the following cases: TreeConnect.Share.EncryptData is TRUE, Connection.ServerCapabilities includes SMB2_GLOBAL_CAP_ENCRYPTION, and Request.IsEncrypted is FALSE. EncryptData or TreeConnect.Share.EncryptData or Request.IsEncrypted is TRUE, RejectUnencryptedAccess is TRUE, and Connection.ServerCapabilities does not include SMB2_GLOBAL_CAP_ENCRYPTION. Changed to: The server MUST look up the TreeConnect in Session.TreeConnectTable by using the TreeId in the SMB2 header of the request. If no tree connect is found, the request MUST be failed with STATUS_NETWORK_NAME_DELETED. If Connection.Dialect belongs to the SMB 3.x dialect family, the server MUST fail the request with STATUS_ACCESS_DENIED in the following cases:

Errata Published*	Description
	If the server supports the 3.1.1 dialect, TreeConnect.Share.EncryptData is TRUE, Connection.ServerCapabilities includes SMB2_GLOBAL_CAP_ENCRYPTION, and Request.IsEncrypted is FALSE. Otherwise, if the server supports 3.0 or 3.0.2 dialect, EncryptData or TreeConnect.Share.EncryptData is TRUE, Connection.ServerCapabilities includes SMB2_GLOBAL_CAP_ENCRYPTION, RejectUnencryptedAccess is TRUE, and Request.IsEncrypted is FALSE. EncryptData or TreeConnect.Share.EncryptData or Request.IsEncrypted is TRUE, RejectUnencryptedAccess is TRUE, and Connection.ServerCapabilities does not include SMB2_GLOBAL_CAP_ENCRYPTION.
2018/02/26	In Section 3.3.1.12, Per Lease, the following has been added: ● Lease.Held: A Boolean, when set to TRUE, indicates that at least one Open is associated with this lease. In Section 3.3.4.7, Object Store Indicates a Lease Break, the following has been changed from: If a lease entry is found, the server MUST check the state of Open.Connection for all Opens in Lease.LeaseOpens. If Open.Session.Connection.Dialect belongs to the SMB 3.x dialect family and Open.Connection is NULL, the server MUST select an alternate connection in Open.Session.ChannelList and update Open.Connection. ... ● Otherwise, the server MUST set Open.Lease.Breaking to FALSE and MUST complete the lease break call from the underlying object store with "NONE" as the new lease state. Changed to: If a Lease entry is found, the server MUST check the state of Open.Connection for all Opens in Lease.LeaseOpens. If Open.Session.Connection.Dialect belongs to the SMB 3.x dialect family and Open.Connection is NULL, the server MUST select an alternate connection in Open.Session.ChannelList and update Open.Connection. ... ● Otherwise, the server MUST set Open.Lease.Breaking to FALSE and MUST complete the lease break call from the underlying object store with "NONE" as the new lease state. In Section 3.3.4.17, Server Application Requests Closing an Open, the following has been changed from: ● The server MUST then remove the Open from Lease.LeaseOpens. ● If Lease.LeaseOpens is now empty: ● If Lease.Breaking is TRUE, the server MUST complete the lease break to the underlying object store with NONE as the new lease state. <203> ● The server MUST remove the Lease from the LeaseTable.LeaseList and free the Lease. Changed to:

Errata Published*	Description
	• The server MUST then remove the Open from Open.Lease.LeaseOpens. If this Open is the last open in Open.Lease.LeaseOpens, the server MUST set Open.Lease.Held to FALSE. • If Open.Lease.Held is FALSE: • If Open.Lease.Breaking is TRUE, the server MUST complete the lease break to the underlying object store with NONE as the new lease state. <203> • The server MUST remove the Open.Lease from the LeaseTable.LeaseList and free the Open.Lease. In Section 3.3.5.9.8, Handling the SMB2_CREATE_REQUEST_LEASE Create Context, the following has been changed from: The server MUST set Open.OplockState to Held, set Open.Lease to a reference to lease, set Open.OplockLevel to SMB2_OPLOCK_LEVEL_LEASE, and add open to Lease.LeaseOpens. The remainder of open response construction continues as described in "Response Construction". Changed to: The server MUST set Open.OplockState to Held, set Open.Lease to a reference to Lease, set Open.OplockLevel to SMB2_OPLOCK_LEVEL_LEASE, and add Open to Lease.LeaseOpens. If this Open is the first open in Lease.LeaseOpens, the server MUST set Lease.Held to TRUE. The remainder of open response construction continues as described in "Response Construction". In Section 3.3.5.9.11, Handling the SMB2_CREATE_REQUEST_LEASE_V2 Create Context, the following has been changed from: The server MUST set Open.OplockState to Held, set Open.Lease to a reference to lease, set Open.OplockLevel to SMB2_OPLOCK_LEVEL_LEASE, and add open to Lease.LeaseOpens. The remainder of open response construction continues as described in the "Response Construction" phase. Changed to: The server MUST set Open.OplockState to Held, set Open.Lease to a reference to Lease, set Open.OplockLevel to SMB2_OPLOCK_LEVEL_LEASE, and add Open to Lease.LeaseOpens. If this Open is the first open in Lease.LeaseOpens, the server MUST set Lease.Held to TRUE. The remainder of open response construction continues as described in the "Response Construction" phase.
2018/02/12	In Section 2.2.1, SMB2 Packet Header, the following has been changed from: If the SMB2_FLAGS_ASYNC_COMMAND bit is set in Flags, the header takes the form SMB2 Packet Header – ASYNC (section 2.2.1.1). This header format is used for responses to requests processed asynchronously by the server, as specified in sections 3.3.4.2, 3.3.4.3, 3.3.4.4, and 3.2.5.1.5. This header format MAY be used for any request, and the SMB2 CANCEL Request MUST use this format for canceling requests that have received an interim response, as specified in sections 3.2.4.24 and 3.3.5.16. If the SMB2_FLAGS_ASYNC_COMMAND bit is not set in Flags, the header takes the form SMB2 Packet Header – SYNC (section 2.2.1.2). This format can be used for all requests and responses.

Errata Published*	Description
	Changed to: If the SMB2_FLAGS_ASYNC_COMMAND bit is set in Flags, the header takes the form SMB2 Packet Header – ASYNC (section 2.2.1.1). This header format is used for responses to requests processed asynchronously by the server, as specified in sections 3.3.4.2, 3.3.4.3, 3.3.4.4, and 3.2.5.1.5. The SMB2 CANCEL Request MUST use this format for canceling requests that have received an interim response, as specified in sections 3.2.4.24 and 3.3.5.16. If the SMB2_FLAGS_ASYNC_COMMAND bit is not set in Flags, the header takes the form SMB2 Packet Header – SYNC (section 2.2.1.2).
2018/02/12	In Section 3.2.4.6, Application Requests Reading from a File or Named Pipe, the following has been changed from: • The returned list of SMB_DIRECT_BUFFER_DESCRIPTOR_1 structures MUST be appended to the SMB2 header. • The ReadChannelInfoOffset MUST be set to the offset of the appended list from the beginning of the SMB2 header. • The ReadChannelInfoLength MUST be set to the length of the appended list. Changed to: • The returned list of SMB_DIRECT_BUFFER_DESCRIPTOR_V1 structures MUST be added to the Buffer field of the request. • The ReadChannelInfoOffset MUST be set to the offset of the added list from the beginning of the SMB2 header. • The ReadChannelInfoLength MUST be set to the length of the added list. Otherwise, the following fields of the request MUST be initialized as follows: • The Channel field MUST be set to 0. • The first byte of the Buffer field MUST be set to 0. • The ReadChannelInfoOffset field MUST be set to 0. • The ReadChannelInfoLength field MUST be set to 0. In Section 3.2.4.7, Application Requests Writing to a File or Named Pipe, the following has been changed from: • The returned list of SMB_DIRECT_BUFFER_DESCRIPTOR_1 structures MUST be appended to the SMB2 header. • The WriteChannelInfoOffset MUST be set to the offset of the appended list from the beginning of the SMB2 header. • The WriteChannelInfoLength MUST be set to the length of the appended list. Changed to: • The returned list of SMB_DIRECT_BUFFER_DESCRIPTOR_V1 structures MUST be added to the Buffer field of the request. • The WriteChannelInfoOffset MUST be set to the offset of the added list from the beginning of the SMB2 header. • The WriteChannelInfoLength MUST be set to the length of the added list.
2018/01/16	In Section 2.2.41, SMB2 TRANSFORM_HEADER, the first paragraph has been changed from:

Errata Published*	Description
	The SMB2 Transform Header is used by the client or server when sending encrypted messages. The SMB2 TRANSFORM_HEADER is only valid for the SMB 3.x dialect family. Changed to: The SMB2 TRANSFORM_HEADER is used by the client or server when sending encrypted messages. The SMB2 TRANSFORM_HEADER is only valid for the SMB 3.x dialect family. In Section 3.2.5.1.1, Decrypting the Message, the fourth bullet point has been changed from: ● The client MUST decrypt the message using Session.DecryptionKey. If Connection.Dialect is "3.1.1", the algorithm specified by Connection.CipherId is used. Otherwise, the AES-128-CCM algorithm is used. The client passes in the TRANSFORM_HEADER, excluding the Signature and ProtocolId fields, and the encrypted SMB2 message as the Optional Authenticated Data input for the algorithm. If decryption succeeds, the client MUST compare the signature in the transform header with the signature returned by the decryption algorithm. If signature verification succeeds, the client MUST then continue processing the decrypted packet, as specified in subsequent sections. If signature verification fails, the client MUST fail the application request with an implementation-specific error. Changed to: ● The client MUST decrypt the message using Session.DecryptionKey. If Connection.Dialect is "3.1.1", the algorithm specified by Connection.CipherId is used. Otherwise, the AES-128-CCM algorithm is used. The client passes in the Nonce, OriginalMessageSize, Flags/EncryptionAlgorithm and SessionId fields of the SMB2 TRANSFORM_HEADER and the encrypted SMB2 message as the Optional Authenticated Data input for the algorithm. If decryption succeeds, the client MUST compare the signature in the SMB2 TRANSFORM_HEADER with the signature returned by the decryption algorithm. If signature verification succeeds, the client MUST then continue processing the decrypted packet, as specified in subsequent sections. If signature verification fails, the client MUST fail the application request with an implementation-specific error. In Section 3.3.5.2.1, Decrypting the Message, the second bullet point has been changed from: ● If OriginalMessageSize value received in the TRANSFORM _HEADER is greater than the implementation-specific limit<210> or if it is less than the size of the SMB2 Header, the server MUST disconnect the connection as specified in section 3.3.7.1. Changed to: ● If OriginalMessageSize value received in the SMB2 TRANSFORM _HEADER is greater than the implementation-specific limit<210> or if it is less than the size of the SMB2 Header, the server MUST disconnect the connection as specified in section 3.3.7.1. The fifth bullet point has been changed from: ● The server MUST decrypt the message using Session.DecryptionKey. If Connection.Dialect is less than "3.1.1", then AES-128-CCM MUST be used, as specified

Errata Published*	Description
	in [RFC4309]. Otherwise, the algorithm specified by the Connection.CipherId MUST be used. The server passes in the TRANSFORM_HEADER, excluding the Signature and ProtocolId fields, as the Optional Authenticated Data input for the algorithm. If decryption succeeds, the server MUST compare the signature in the transform header with the signature returned by the decryption algorithm. If the signature verification fails, the server MUST disconnect the connection as specified in section 3.3.7.1. If the signature verification succeeds, the server MUST continue processing the decrypted packet, as specified in subsequent sections. Changed to: • The server MUST decrypt the message using Session.DecryptionKey. If Connection.Dialect is less than "3.1.1", then AES-128-CCM MUST be used, as specified in [RFC4309]. Otherwise, the algorithm specified by the Connection.CipherId MUST be used. The server passes in the Nonce, OriginalMessageSize, Flags/EncryptionAlgorithm and SessionId fields of the SMB2 TRANSFORM_HEADER as the Optional Authenticated Data input for the algorithm. If decryption succeeds, the server MUST compare the signature in the SMB2 TRANSFORM_HEADER with the signature returned by the decryption algorithm. If the signature verification fails, the server MUST disconnect the connection as specified in section 3.3.7.1. If the signature verification succeeds, the server MUST continue processing the decrypted packet, as specified in subsequent sections.
2018/01/16	In Section 2.2.2.2, ErrorData format, changed from: The ErrorData MUST be formatted based on the error code being returned. If the error code in the header of the response is set to STATUS_STOPPED_ON_SYMLINK, this field MUST contain a Symbolic Link Error Response as specified in section 2.2.2.2.1. If the error code in the header of the response is set to STATUS_BAD_NETWORK_NAME, and the ErrorId in the SMB2 Error Context response is set to SMB2_ERROR_ID_SHARE_REDIRECT, this field MUST contain a Share Redirect Error Response as specified in section 2.2.2.2.2. If the error code in the header of the response is STATUS_BUFFER_TOO_SMALL, this field MUST be set to a 4-byte value indicating the minimum required buffer length. Changed to: The ErrorData MUST be formatted based on the error code being returned in the Status field of the SMB2 Packet header for the SMB2 Error Response (section 2.2.2). If the Status field of the header of the response is set to STATUS_STOPPED_ON_SYMLINK, this field MUST contain a Symbolic Link Error Response as specified in section 2.2.2.2.1. If the Status field of the header of the response is set to STATUS_BAD_NETWORK_NAME, and the ErrorId in the SMB2 Error Context response is set to SMB2_ERROR_ID_SHARE_REDIRECT, this field MUST contain a Share Redirect Error Response as specified in section 2.2.2.2.2. If the Status field of the header of the response is set to STATUS_BUFFER_TOO_SMALL, this field MUST be set to a 4-byte value indicating the minimum required buffer length.
2018/01/16	In Section 2.2.9.2.1.4, LUID_ATTR_DATA, the size of the Luid field has been changed from 4 to 8 bytes and the description changed from: Luid (4 bytes): LUID is a locally unique identifier, as specified in [MS-DTYP] section 2.3.7.

Errata Published*	Description
	Changed to: Luid (8 bytes): Locally unique identifier, as specified in [MS-DTYP] section 2.3.7.
2018/01/16	In Section 3.3.1.12, Per Lease, the description of Lease.Breaking has been changed from: ● Lease.Breaking: A Boolean that indicates if a lease break is in progress. Changed to: ● Lease.Breaking: A Boolean, if set to TRUE, indicating a lease break requiring acknowledgement is in progress. In Section 3.3.4.7, Object Store Indicates a Lease Break, the following was changed from: If Lease.LeaseOpens is not empty, the server MUST do the following: ● If Open.Connection is NULL, Open.IsPersistent is TRUE, and Open.DurableOpenTimeout is not earlier than the current time, the server MUST set Open.Lease.Breaking to FALSE, complete the lease break call from the underlying object store with "NONE" as the new lease state, and take no further action. ● If Open.Connection is NULL, the server MUST set Open.Lease.Breaking to TRUE, and take no further action. ● Otherwise, construct a Lease Break Notification (section 2.2.23.2) message to send to the client. The server MUST set the Command in the SMB2 header to SMB2 OPLOCK_BREAK, and the MessageId to 0xFFFFFFFFFFFFFFFF. The server MUST set the SessionId and TreeId in the SMB2 header to 0. If Lease.LeaseState is SMB2_LEASE_READ_CACHING, the server MUST set the Flags field of the message to zero and MUST set Open.OplockState to None for all opens in Lease.LeaseOpens. The server MUST set Lease.Breaking to FALSE, and the LeaseKey field MUST be set to Lease.LeaseKey. Otherwise the server MUST set the Flags field of the message to SMB2_NOTIFY_BREAK_LEASE_FLAG_ACK_REQUIRED, indicating to the client that lease acknowledgment is required. The LeaseKey field MUST be set to Lease.LeaseKey. The server MUST set Open.OplockState to Breaking for all Opens in Lease.LeaseOpens. The server MUST set the CurrentLeaseState field of the message to Lease.LeaseState, set Lease.Breaking to TRUE, set Lease.BreakToLeaseState to the new lease state indicated by the object store, and set Lease.LeaseBreakTimeout to the current time plus an implementation-specific default value in milliseconds.<200> If the server implements the SMB 3.x dialect family and Lease.Version is 2, the server MUST set NewEpoch to Lease.Epoch + 1. Otherwise, NewEpoch MUST be set to zero. The SMB2 Lease Break Notification is sent to the client using the connection specified in Open.Connection of the first Open in Lease.LeaseOpens. The message SHOULD NOT be signed. The server MUST start the oplock break acknowledgment timer as specified in 3.3.2.1. If there was an error in attempting to transmit the message to the client, the server MUST retry the send using the connection specified in Open.Connection of the next Open in Lease.LeaseOpens. If the server fails to send transmit the message on any Open.Connection associated with this lease, the server MUST complete the lease break call from the underlying object store with "NONE" as the new lease state. Changed to:

Errata Published*	Description
	If Lease.LeaseOpens is not empty, the server MUST construct a Lease Break Notification (section 2.2.23.2) message to send to the client. The server MUST set the Command field in the SMB2 header to SMB2 OPLOCK_BREAK, and the MessageId field to 0xFFFFFFFFFFFFFFFF. The server MUST set the SessionId and TreeId fields in the SMB2 header to 0. If Lease.LeaseState is SMB2_LEASE_READ_CACHING, the server MUST set the Flags field of the message to zero and MUST set Open.OplockState to "None" for all opens in Lease.LeaseOpens. The server MUST set Lease.Breaking to FALSE, and the LeaseKey field MUST be set to Lease.LeaseKey. Otherwise, the server MUST set the Flags field of the message to SMB2_NOTIFY_BREAK_LEASE_FLAG_ACK_REQUIRED, indicating to the client that lease acknowledgment is required. The LeaseKey field MUST be set to Lease.LeaseKey. The server MUST set Open.OplockState to "Breaking" for all Opens in Lease.LeaseOpens. The server MUST set the CurrentLeaseState field of the message to Lease.LeaseState, set Lease.Breaking to TRUE, set Lease.BreakToLeaseState to the new lease state indicated by the object store, and set Lease.LeaseBreakTimeout to the current time plus an implementation-specific<200> default value in milliseconds. If the server implements the SMB 3.x dialect family and Lease.Version is 2, the server MUST set NewEpoch to Lease.Epoch + 1. Otherwise, NewEpoch MUST be set to zero. The SMB2 Lease Break Notification is sent to the client using the connection specified in Open.Connection of the first Open in Lease.LeaseOpens. The message SHOULD NOT be signed. If the server fails to send the message to the client, the server MUST retry the send using the connection specified in Open.Connection of the next Open in Lease.LeaseOpens. If the server succeeds in sending the message on any Open.Connection associated with this Lease, the server MUST start the oplock break acknowledgment timer as specified in section 3.3.2.1. Otherwise, the server MUST perform the following steps: • If Open.IsPersistent is TRUE, and Lease.LeaseState is not SMB2_LEASE_READ_CACHING, and Open.DurableOpenTimeout is not earlier than the current time, the server MUST take no further action. • Otherwise, the server MUST set Open.Lease.Breaking to FALSE and MUST complete the lease break call from the underlying object store with "NONE" as the new lease state.

*Date format: YYYY/MM/DD

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

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

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

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

[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

[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

[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

[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

Errata below are for Protocol Document Version V8.0 – 2017/09/15.

Errata Published*	Description
2018/03/13	In Section 6, Appendix A: Product Behavior, Windows Server 2016 and Windows Server have been removed from the applicability list, and a new behavior note added to Section 1.5, Prerequisites/Preconditions. Changed from: 1.5 Prerequisites/Preconditions This protocol assumes HTTP [RFC2616] connectivity from the client to the server. 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. 6 Appendix A: Product Behavior The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include updates to those products. • Windows Server 2008 operating system • Windows Server 2008 R2 operating system • Windows Server 2012 operating system • Windows Server 2012 R2 operating system • Windows Server 2016 operating system • Windows Server operating system Changed to: 1.5 Prerequisites/Preconditions This protocol assumes HTTP [RFC2616] connectivity from the client to the server. 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>

Errata Published*	Description
	<1> Section 1.5: The Smooth Streaming Protocol is supported in the following IIS Media Services Windows implementations: IIS Media Services Version Applicable Windows Server Releases IIS Media Services 3.0 Windows Server 2008, Windows Server 2008 R2 IIS Media Services 4.0 Windows Server 2008, Windows Server 2008 R2 IIS Media Services 4.1 Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 6 Appendix A: Product Behavior The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include updates to those products. • Windows Server 2008 operating system • Windows Server 2008 R2 operating system • Windows Server 2012 operating system • Windows Server 2012 R2 operating system

2018/03/13	In Section 2.2.4.7, TrunBox, definitions to the DataOffset and DataOffsetPresent fields have been added.
	
	Changed from:
	SampleCount (4 bytes): The number of samples in the fragment.
	FirstSampleFlagsPresent (1 bit): Indicates that the default flags for the first sample are replaced if this field takes the value %b1.
	...
	
	TrunBoxSampleFlags (4 bytes): The sample flags of each sample. This field MUST be present if and only if the SampleFlagsPresent field takes the value %b1. If this field is not present, its implicit value is the value of the DefaultSampleFlags field. If the FirstSampleFlags field is present and this field is omitted, this field's implicit value for the first sample in the fragment MUST be the value of the FirstSampleFlags field.
	
	SampleCompositionTimeOffset (4 bytes): The Sample Composition Time offset of each sample, as defined in [ISO/IEC-14496-12]. This field MUST be present if and only if the SampleCompositionTimeOffsetPresent field takes the value %b1.
	
	`TrunBox = TrunBoxLength TrunBoxType [TrunBoxLongLength] TrunBoxFields TrunBoxChildren`
	`TrunBoxType = %d116 %d114 %d117 %d110`
	`TrunBoxLength = BoxLength`
	`TrunBoxLongLength = LongBoxLength`
	`TrunBoxFields = TrunBoxVersion`
	`TrunBoxFlags`
	`SampleCount`
	`[ FirstSampleFlags ]`
	`*( TrunBoxPerSampleFields )`
	`; TrunBoxPerSampleFields MUST be repeated exactly SampleCount times`

Errata Published*	Description
	TrunBoxFlags = 12*12 RESERVED BIT SampleCompositionTimeOffsetPresent SampleFlagsPresent SampleSizePresent SampleDurationPresent RESERVED_BIT RESERVED_BIT RESERVED_BIT RESERVED_BIT RESERVED_BIT FirstSampleFlagsPresent RESERVED_BIT RESERVED_BIT SampleCompositionTimeOffsetPresent = BIT Changed to: SampleCount (4 bytes): The number of samples in the fragment. DataOffset (4 bytes): This field MUST be set. It specifies the offset from the beginning of the MoofBox field (section 2.2.4.1). If only one TrunBox is specified, then the DataOffset field MUST be the sum of the lengths of the MoofBox and all the fields in the MdatBox field (section 2.2.4.8). FirstSampleFlagsPresent (1 bit): Indicates that the default flags for the first sample are replaced if this field takes the value %b1. ... TrunBoxSampleFlags (4 bytes): The sample flags of each sample. This field MUST be present if and only if the SampleFlagsPresent field takes the value %b1. If this field is not present, its implicit value is the value of the DefaultSampleFlags field. If the FirstSampleFlags field is present and this field is omitted, this field's implicit value for the first sample in the fragment MUST be the value of the FirstSampleFlags field. DataOffsetPresent (1 bit): Specifies whether the DataOffset field is present. This field MUST be set. SampleCompositionTimeOffset (4 bytes): The Sample Composition Time offset of each sample, as defined in [ISO/IEC-14496-12]. This field MUST be present if and only if the SampleCompositionTimeOffsetPresent field takes the value %b1. TrunBox = TrunBoxLength TrunBoxType [TrunBoxLongLength] TrunBoxFields TrunBoxChildren TrunBoxType = %d116 %d114 %d117 %d110 TrunBoxLength = BoxLength TrunBoxLongLength = LongBoxLength TrunBoxFields = TrunBoxVersion TrunBoxFlags SampleCount DataOffset [FirstSampleFlags] *(TrunBoxPerSampleFields) ; TrunBoxPerSampleFields MUST be repeated exactly SampleCount times TrunBoxFlags = 12*12 RESERVED_BIT SampleCompositionTimeOffsetPresent

Errata Published*	Description
	SampleFlagsPresent SampleSizePresent SampleDurationPresent RESERVED_BIT RESERVED_BIT RESERVED_BIT RESERVED_BIT RESERVED_BIT FirstSampleFlagsPresent RESERVED_BIT RESERVED_BIT DataOffsetPresent SampleCompositionTimeOffsetPresent = BIT
2018/01/29	In Section 2.2.2.5, TrackElement, we updated the CodecPrivateData field ABNF representation with the PPSField. Also, updated that PPSField contains the Picture Parameter Set (PPS). Changed from: ▪ The FourCC field equals "H264": The CodecPrivateData field contains a hexadecimal-coded string representation of the following byte sequence, specified in ABNF [RFC5234]: ▪ %x00 %x00 %x00 %x01 SPSField %x00 %x00 %x00 %x01 SPSField ▪ SPSField contains the Sequence Parameter Set (SPS). ▪ PPSField contains the Slice Parameter Set (PPS). Changed to: ▪ The FourCC field equals "H264": The CodecPrivateData field contains a hexadecimal-coded string representation of the following byte sequence, specified in ABNF [RFC5234]: ▪ %x00 %x00 %x00 %x01 SPSField %x00 %x00 %x00 %x01 PPSField ▪ SPSField contains the Sequence Parameter Set (SPS). ▪ PPSField contains the Picture Parameter Set (PPS)

*Date format: YYYY/MM/DD

[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

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

July 18, 2016 - Download

[MS-TCC]: Tethering Control Channel Protocol

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

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

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

[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

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

August 21, 2017 - Download

December 1, 2017 - Download

[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

[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

[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

[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

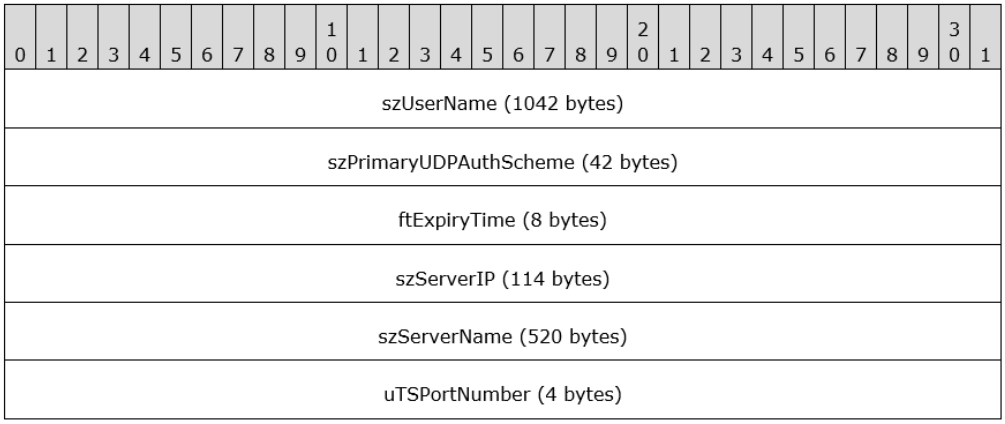
December 1, 2017 - Download

Errata below are for Protocol Document Version V39.0 – 2017/12/01.

Errata Published*	Description

2018/01/16	In Section 2.2.11.8 AUTHN_COOKIE_DATA Structure, a packet diagram has been added and field descriptions have been updated.
	
	Changed from:
	The AUTHN_COOKIE_DATA structure is used to authenticate a UDP connection.
	
	`typedef struct {`
	`  WCHAR* szUserName;`
	`  WCHAR* szPrimaryUDPAuthScheme;`
	`  FILETIME ftExpiryTime;`
	`  WCHAR* szServerIP;`
	`  WCHAR* szServerName;`
	`} AUTHN_COOKIE_DATA;`
	
	szUserName: Name of the user for which the side channel is required to be created.
	szPrimaryUDPAuthScheme: The primary authentication method to be used for authenticating a side channel. By default, all the side channels are authenticated with the UDPCookieAuthentication method. The RDG client and RDG server can also implement other strong authentication methods. For a side channel to be established, an RDG client SHOULD pass both the UDPCookieAuthentication method and the method mentioned in szPrimaryUDPAuthScheme.
	ftExpiryTime: The time at which the cookie expires.
	szServerIP: The IP address of the target server.
	szServerName: The name of the target server.
	
	Changed to:
	The AUTHN_COOKIE_DATA structure is used to authenticate a UDP connection.

Errata Published*	Description



szUserName (1042 bytes): Name of the user for which the side channel is required to be created in Unicode characters.

szPrimaryUDPAuthScheme (42 bytes): The name of the primary authentication method to be used for authenticating a side channel in Unicode characters. By default, all the side channels are authenticated with the UDPCookieAuthentication method. The RDG client and RDG server can also implement other strong authentication methods. For a side channel to be established, an RDG client SHOULD pass both the UDPCookieAuthentication method and the method mentioned in szPrimaryUDPAuthScheme.

ftExpiryTime (8 bytes): The time (FILETIME) at which the cookie expires. For information on the FILETIME structure, see [MS-DTYP] section 2.3.3.

szServerIP (114 bytes): The IP address of the target server in Unicode characters.

szServerName (520 bytes): The name of the target server in Unicode characters.

uTSPortNumber (4 bytes): The port number where RDG is listening for incoming UDP connections.

In Section 2.2.11.10 CONNECT_PKT_FRAGMENT Structure, a packet diagram has been added.

Changed from:

The RDG client MUST use the PKT_TYPE_CONNECT_REQ_FRAGMENT packet type to send connection requests to the RDP server. It MUST do so by splitting a CONNECT_PKT request into one or more fragments of type CONNECT_PKT_FRAGMENT.<22>

Multi-byte values in this structure are transmitted in little-endian byte order.

```
typedef struct _CONNECT_PKT_FRAGMENT
{
    UDP_PACKET_HEADER hdr;
    USHORT usFragmentID;
    USHORT usNoOfFragments;
    USHORT cbFragmentLength;
    BYTE fragment[0];
} CONNECT_PKT_FRAGMENT, *PCONNECT_PKT_FRAGMENT;
```

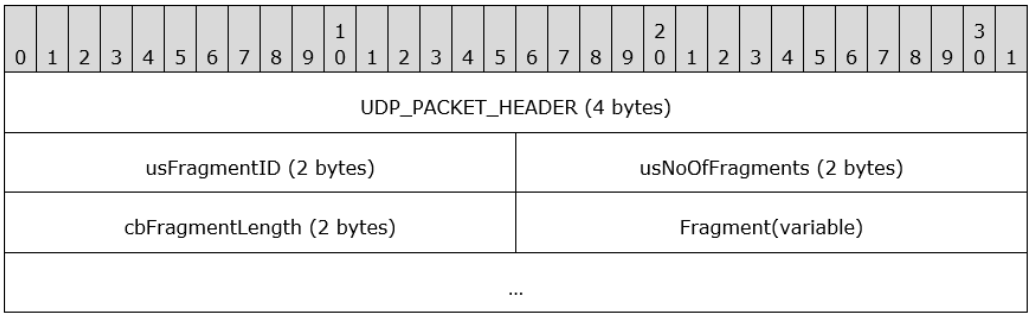
hdr (4 bytes): A UDP_PACKET_HEADER structure (section 2.2.11.7).

usFragmentID (2 bytes): Identifies the fragment number. The first fragment starts with 0.

usNoOfFragments (2 bytes): Total number of fragments.

cbFragmentLength (2 bytes): Length of this fragment.

Errata Published*	Description

	fragment (variable): An array of bytes representing a portion of the CONNECT_PKT request.
	
	Changed to:
	The RDG client MUST use the PKT_TYPE_CONNECT_REQ_FRAGMENT packet type to send connection requests to the RDP server. It MUST do so by splitting a CONNECT_PKT request into one or more fragments of type CONNECT_PKT_FRAGMENT.<22>
	
	 
	
	Multi-byte values in this structure are transmitted in little-endian byte order.
	
	`typedef struct _CONNECT_PKT_FRAGMENT`
	`{`
	`UDP_PACKET_HEADER hdr;`
	`USHORT usFragmentID;`
	`USHORT usNoOfFragments;`
	`USHORT cbFragmentLength;`
	`BYTE fragment[0];`
	`} CONNECT_PKT_FRAGMENT, *PCONNECT_PKT_FRAGMENT;`
	
	hdr (4 bytes): A UDP_PACKET_HEADER structure (section 2.2.11.7).
	usFragmentID (2 bytes): Identifies the fragment number. The first fragment starts with 0.
	usNoOfFragments (2 bytes): Total number of fragments.
	cbFragmentLength (2 bytes): Length of this fragment.
	fragment (variable): An array of bytes representing a portion of the CONNECT_PKT request.

*Date format: YYYY/MM/DD

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

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

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

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

[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

[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

[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

[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

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

[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

[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

[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

[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

[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

[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

[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

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

July 18, 2016 - Download

[MS-WPO]: Windows Protocols Overview

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

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

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

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

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

[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

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

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

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

[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

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

[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

[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

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

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

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

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

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

[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