Windows Protocols Errata

This topic lists Errata found in the Windows Protocols Technical Specifications, Overview Documents, and Reference documents since they were last published. Since these topics are updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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 following sections list the Windows Protocols technical documents that contain active errata that is not yet released with the documents in the Open Specifications Library. Links to previously published archived errata are available on this page, on the following pages, and on the main landing page of each document, as applicable.

Protocols Documents with Active Errata

[MC-NMF]: .NET Message Framing Protocol

[MS-ADSC]: Active Directory Schema Classes

[MS-ADTS]: Active Directory Technical Specification

[MS-APDS]: Authentication Protocol Domain Support

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

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

[MS-CRTD]: Certificate Templates Structure

[MS-CSRA]: Certificate Services Remote Administration Protocol

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

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

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

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

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

[MS-EMFPLUS]: Enhanced Metafile Format Plus Extensions

[MS-EVEN]: EventLog Remoting Protocol

[MS-EVEN6]: EventLog Remoting Protocol Version 6.0

[MS-FSCC]: File System Control Codes

[MS-KILE]: Kerberos Protocol Extensions

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

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

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

[MS-MDM]: Mobile Device Management Protocol

[MS-NCNBI]: Network Controller Northbound Interface

[MS-NNS]: .NET NegotiateStream Protocol

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

[MS-NRPC]: Netlogon Remote Protocol

[MS-PAC]: Privilege Attribute Certificate Data Structure

[MS-PKCA]: Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol

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

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

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

[MS-RNAS]: Vendor-Specific RADIUS Attributes for Network Policy and Access Server (NPAS) Data Structure

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

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

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

[MS-SSTR]: Smooth Streaming Protocol

[MS-WCCE]: Windows Client Certificate Enrollment Protocol

[MS-WKST]: Workstation Service Remote Protocol

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

[MS-XCA]: Xpress Compression Algorithm

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

March 16, 2018 - Download

September 12, 2018 - Download

March 13, 2019 - Download

June 24, 2019 – Download

September 23, 2019 - Download

October 14, 2019 - Download

March 4, 2020 - Download

June 15, 2020 - Download

August 24, 2020 – Download

September 29, 2020 – Download

November 23, 2020 - Download

April 7, 2021 - Download

June 1, 2021 - Download

June 24, 2021 - Download

October 6, 2021 - Download

May 2, 2022 - Download

December 1, 2022 - Download

February 7, 2023 - Download

February 27, 2023 - Download

April 4, 2023 - Download

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

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

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

RSS

No errata are available for the latest version of 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-NBFX]: .NET Binary Format XML Data Structure

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

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

RSS

No errata are available for the latest version of this Windows Protocols document.

December 1, 2019 – Download

[MC-NMF]: .NET Message Framing Protocol

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

RSS

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

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

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

*Date format: YYYY/MM/DD

[MC-PRCR]: Peer Channel Custom Resolver Protocol

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-ABTP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-ADA2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

May 22, 2023 - Download

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

This topic lists Errata found in [MS-ADA3] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-ADDM] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-ADFSPIP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

June 30, 2015 - Download

July 18, 2016 - Download

September 15, 2017 - Download

September 12, 2018 - Download

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-ADSC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V23.0 – 2018/03/16.

Errata Published*	Description

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

*Date format: YYYY/MM/DD

[MS-ADTS]: Active Directory Technical Specification

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

March 20, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

March 13, 2019 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V56.0 – 2023/01/20.

Errata Published*	Description
2023/04/24	Section: **6.1.6.7.15 trustType** **Description**: Specified additional supported operating systems in [MSKB-5026362] & [MSKB-5026370]; for recently added trustType definition TTAAD (TRUST_TYPE_AAD, 0x00000005), for trusted domain: Azure Active Directory. Changed from: TTDCE (TRUST_TYPE_DCE, 0x00000004): Historical reference; this value is not used in Windows. Changed to: TTDCE (TRUST_TYPE_DCE, 0x00000004): Historical reference; this value is not used in Windows. TTAAD (TRUST_TYPE_AAD, 0x00000005): The trusted domain is in Azure Active Directory. **Note**: This trustType is supported by the operating systems specified in [MSKB-5025305], [MSKB-5025298], [MSKB-5025297], [MSKB-5026362], and [MSKB-5026370], each with its related MSKB article download installed.

Errata Published*	Description
2023/04/10	Section: **6.1.6.7.15 trustType** **Description**: Added new trustType definition TTAAD (TRUST_TYPE_AAD, 0x00000005) for trusted domain Azure Active Directory applications. Changed from: TTDCE (TRUST_TYPE_DCE, 0x00000004): Historical reference; this value is not used in Windows. Changed to: TTDCE (TRUST_TYPE_DCE, 0x00000004): Historical reference; this value is not used in Windows. TTAAD (TRUST_TYPE_AAD, 0x00000005): The trusted domain is in Azure Active Directory. **Note**: This trustType is supported by the operating systems specified in [MSKB-5025305], [MSKB-5025298], and [MSKB-5025297]; each with its related MSKB article download installed.
2023/02/27	Section 1 Introduction Description: Mapped the applicability of Windows 10 v21H2 operating system to Windows Server 2022 for the new rootDSE attributes. Changed from: Information that is applicable to AD LDS on Windows Server v1903 is also applicable to AD LDS for Windows 10 v1903. Changed to: Information that is applicable to AD LDS on Windows Server v1903 is also applicable to AD LDS for Windows 10 v1903. Information that is applicable to AD LDS on Windows 2022 Server is also applicable to AD LDS for Windows 10 v21H1 client and Windows 10 v21H2 client. Section 3.1.1.3.2 rootDSE Attributes Description: Added operating system applicability for Windows Server 2022 AD DS and Windows Server AD LDS to the product applicability list; added 3 new rootDSE attributes to the 'Attribute' table and to the 'Attribute | Operational? | LDAP Syntax' table to assist in user database optimizations. Added note to indicate the supporting operating systems specified in [MSKB-5023705], [MSKB-5023702], [MSKB-5023706], [MSKB-5023698], and [MSKB-5023696]. (Product applicability list) Changed from: • N2 --> Windows Server v1903 AD DS Changed to: • N2 --> Windows Server v1903 AD LDS • P2 --> Windows Server 2022 AD DS • Q2 --> Windows Server 2022 AD LDS (Attribute table) Changed from:

msDS-SupportedRootDSEModifications													X	X

Changed to:

msDS-SupportedRootDSEModifications													X	X
msDS-DiskUsage ****													X	X
msDS-DatabaseIndices ****													X	X
msDS-DatabaseIndicesWithSize ****													X	X

**** The rootDSE attributes msDS-DiskUsage, msDS-DatabaseIndices, and msDS-DatabaseIndicesWithSize are supported by the operating systems specified in [MSKB-5023705], [MSKB-5023702], [MSKB-5023706], [MSKB-5023698], and [MSKB-5023696]; each with its related KB article download installed.

(Attribute | Operational? | LDAP Syntax table)

Changed from:

msDS-SupportedRootDSEModifications	Y	String(Unicode)

Changed to:

msDS-SupportedRootDSEModifications	Y	String(Unicode)
msDS-DiskUsage	Y	String(Unicode)
msDS-DatabaseIndices	Y	String(Unicode)
msDS-DatabaseIndicesWithSize	Y	String(Unicode)

(New sections)

Section 3.1.1.3.2.57 msDS-DiskUsage

Description: Created new section to describe the disk usage and database table indices data carried by this rootDSE attribute; includes error handling and return value formatting of the instance. Added note to specify the operating systems that support the new rootDSE attributes.

Note The rootDSE attributes msDS-DiskUsage, msDS-DatabaseIndices, and msDS-DatabaseIndicesWithSize are supported by the operating systems specified in [MSKB-5023705], [MSKB-5023702], [MSKB-5023706], [MSKB-5023698], and [MSKB-5023696]; each with its related KB article download installed.

Section 3.1.1.3.2.58 msDS-DatabaseIndices

Description: Created new section to describe the database table indices data carried by this rootDSE attribute; includes error handling and return value format of the instance.

Section 3.1.1.3.2.59 msDS-DatabaseIndicesWithSize

Description: Created new section to describe the database table indices and size data carried by this rootDSE attribute; includes error handling, and return format of the instance.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/01/18</td><td>
Section 3.1.1.3.4.6 LDAP Policies
Description: Added a new LDAP policy for SecurityDescriptorWarningSize to control when warning events will be logged for originating writes to the ntSecurityDescriptor attribute that meet or exceed a configured size value.

Changed from:
The table contains information for the following products. See section 3 for more information.
....

<table>
<tr><th>Policy name</th><th>A</th><th>D, DR2, G, J</th><th>M</th><th>R</th><th>U</th><th>X, A2, D2, G2, J2</th></tr>
<tr><td>MaxActiveQueries</td><td>X*</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>InitRecvTimeout</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>….</td><td></td><td></td><td></td><td></td><td></td><td>* Support for this policy was removed in Windows Server 2003.</td></tr>
</table>

Changed to:
The table contains information for the following products. See section 3 for more information.
….

<table>
<tr><th>Policy name</th><th>A</th><th>D, DR2, G, J</th><th>M</th><th>R</th><th>U</th><th>X, A2, D2, G2, J2</th></tr>
<tr><td>MaxActiveQueries</td><td>X*</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>InitRecvTimeout</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td><td>X</td></tr>
<tr><td>….</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>SecurityDescriptorWarningSize**</td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

* Support for this policy was removed in Windows Server 2003. ** Support for this policy only exists on Windows 11 v22H2 and later.

Changed from:

<table>
<tr><th>Policy name</th><th>Default value</th><th>Description</th></tr>
<tr><td>….</td><td></td><td></td></tr>
<tr><td>MaxDirSyncDuration</td><td>60</td><td>The maximum time, in seconds, that a DC will spend on a single search when using the LDAP_SERVER_DIRSYNC_OID or LDAP_SERVER_DIRSYNC_EX_OID controls. When this limit is reached, the DC returns a timeLimitExceeded / ERROR_INVALID_PARAMETER error.</td></tr>
</table>
</td></tr>
</table>

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

<table>
<tr><th>Policy name</th><th>Default value</th><th>Description</th></tr>
<tr><td>….</td><td></td><td></td></tr>
<tr><td>MaxDirSyncDuration</td><td>60</td><td>The maximum time, in seconds, that a DC will spend on a single search when using the LDAP_SERVER_DIRSYNC_OID or LDAP_SERVER_DIRSYNC_EX_OID controls. When this limit is reached, the DC returns a timeLimitExceeded / ERROR_INVALID_PARAMETER error.</td></tr>
<tr><td>SecurityDescriptorWarningSize</td><td>61,440</td><td>This policy controls when warning events will be logged for originating writes to the ntSecurityDescriptor attribute that meet or exceed the configured size value.</td></tr>
</table>
</td></tr>
</table>

*Date format: YYYY/MM/DD

[MS-AIPS]: Authenticated Internet Protocol

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-APDS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V35.0 – 2021/06/25.

Errata Published*	Description
2022/03/14	Section 2.2.2 Kerberos PAC Validation Message Syntax, updated product note number 2, point 3, that Windows Server 2003 with SP1 and later do not validate the PAC but use Kerberos PAC validation. Changed from: • Windows Server 2003 operating system with Service Pack 1 (SP1) does not validate the PAC when the application server is under the local system context, the network service context, the local service context, or has SeTcbPrivilege privilege. Otherwise, Windows Server 2003 with SP1 and future service packs use Kerberos PAC validation. Changed to: • Windows Server 2003 operating system with Service Pack 1 (SP1) and later Windows operating systems do not validate the PAC when the application server is under the local system context, the network service context, the local service context, or has SeTcbPrivilege privilege. Otherwise, Windows Server 2003 with SP1 and future service packs, and later Windows operating systems use Kerberos PAC validation.

*Date format: YYYY/MM/DD

[MS-AZOD]: Authorization Protocols Overview

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

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

RSS

No errata are available for the latest version of 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, 2021 - Download

[MS-BKRP]: BackupKey Remote Protocol

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V24.0 - 2021/06/25.

Errata Published*	Description
2022/01/11	The following sections were changed. Please see the diff document for the details. In Section 3.2.4.1 Performing Client-Side Wrapping of Secrets, Product Behavior Note<18> Description: Revised to disable the data protection API master key backup fallback by default, as the use of the RC4 algorithm to back up the data protection API master key is no longer available by default. Changed from: Windows XP operating system and later and Windows Server 2003 operating system and later fall back to server-side wrapping using BACKUPKEY_BACKUP_GUID when they fail to retrieve the server's public key using BACKUPKEY_RETRIEVE_BACKUP_KEY_GUID. In addition, as noted earlier, Windows clients always retry failing operations once. The resulting process is as follows: The client first tries the BACKUPKEY_RETRIEVE_BACKUP_KEY_GUID operation and, if it fails, performs DC rediscovery and retries the same operation. If the retry fails, the client tries a BACKUPKEY_BACKUP_GUID operation. If this fails, the client performs DC rediscovery again and retries the BACKUPKEY_BACKUP_GUID operation. If this also fails, an error is returned to the caller. Changed to: The process of falling back to server-side wrapping using the BACKUPKEY_BACKUP_GUID when retrieval of the server's public key fails using the BACKUPKEY_RETRIEVE_BACKUP_KEY_GUID is no longer available by default for the operating systems specified in [MSFT-CVE-2022-21925]. However, the fall back can be enabled by adding a registry key designed for this purpose. In addition, as noted earlier, Windows clients always retry failing operations once. The resulting process is as follows: The client first tries the BACKUPKEY_RETRIEVE_BACKUP_KEY_GUID operation, and if it fails, the client performs DC rediscovery and retries the same operation. If the retry fails, the client tries a BACKUPKEY_BACKUP_GUID operation. If this fails, the client performs DC rediscovery again and retries the BACKUPKEY_BACKUP_GUID operation. If this also fails, an error is returned to the caller.

[MS-BKUP]: Microsoft NT Backup File Structure

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

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

RSS

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

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-CDP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

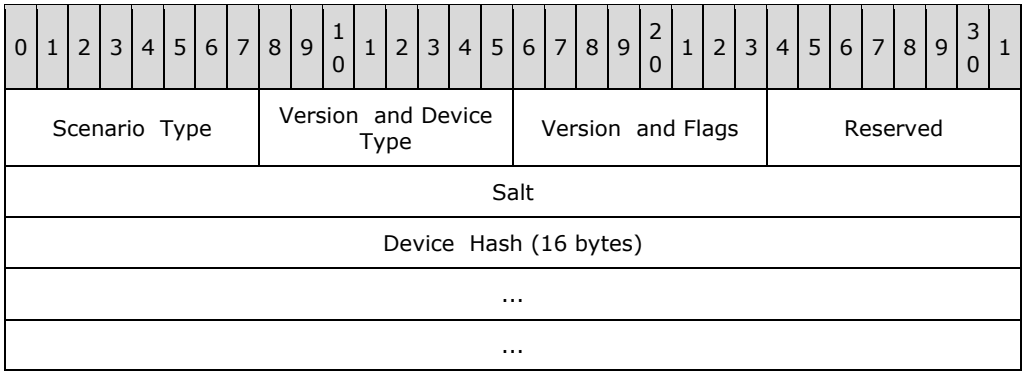
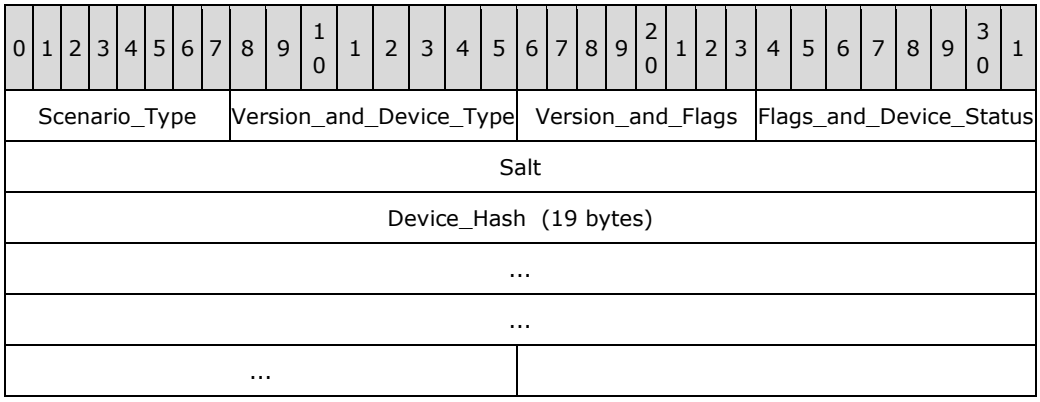
To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

June 1, 2017 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V7.0 – 2022/10/03.

Errata Published*	Description
2023/01/30	In Section 2.2.2.1.1, "Common Header," changed "inner buffer" to "Payload field" in the descriptions of deserialization. Changed from: Message deserialization is split into two phases. The first phase consists of parsing the header, validating authenticity, deduping, and decryption. The inner buffer is sent to the owner to manage the second part of the deserialization. Changed to: Message deserialization is split into two phases. The first phase consists of parsing the header, validating authenticity, deduping, and decryption. The Payload field is sent to the owner to manage the second part of the deserialization. Changed from: Message deserialization will therefore be split into two phases. With the first phase consisting of the parsing header, validating authenticity, deduping, and decryption. The inner buffer will be passed up to the owner to manage the second part of the deserialization. Changed to: Message deserialization will therefore be split into two phases. With the first phase consisting of the parsing header, validating authenticity, deduping, and decryption. The Payload field will be passed up to the owner to manage the second part of the deserialization.
2022/11/29	In section 2.2.2.2.3, "Bluetooth Advertising Beacon," added flag values and provided additional details about packet field structure and length. Changed from:

Errata Published*	Description
	Beacon Data (24 bytes): The beacon data section is further broken down. Note that the Scenario and Subtype Specific Data section requirements will differ based on the Scenario and Subtype.  Scenario Type (1 byte): Set to 1 Version and Device Type (1 byte): The high two bits are set to 00 for the version number; the lower6 bits are set to Device Type values as in section 2.2.2.2.2: Changed to: Beacon Data (24 bytes): The beacon data section is further broken down. Note that the Scenario and Subtype Specific Data section requirements will differ based on the Scenario and Subtype.  Scenario_Type (1 byte): Set to 1 (Bluetooth scenario). Version_and_Device_Type (1 byte): The high three bits are set to 001 for the version number; the lower 5 bits are set to Device Type values as in section 2.2.2.2.2: Changed from: Version and Flags (1 byte): The high 3 bits are set to 001; the lower 3 bits to 00000. Reserved (1 byte): Currently set to zero. Salt (4 bytes): Four random bytes. Device Hash (16 bytes): SHA256 Hash of Salt plus Device Thumbprint. Truncated to 16 bytes.

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

Version_and_Flags (1 byte): The high 3 bits are set to 001; the lower 5 bits are set to 00000 or 00001. Setting the lower 5 bits to 00001 indicates that the NearBy share setting is everyone rather than only my devices.
Flags_and_Device_Status (1 byte): The field has the following structure:
<table>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr>
<tr><td colspan="2">A</td><td colspan="2">B</td><td colspan="2">C</td><td colspan="2">D</td></tr>
</table>
A (2 bits): Unused.
B - Bluetooth_Address_As_Device_ID (1 bit): When set, indicates that the Bluetooth address can be used as the device ID.
C (1 bit): Unused.
D - ExtendedDeviceStatus (4 bits):
One of the values in the following table. Values may be ORed.
<table>
<tr><th>Meaning</th><th>Value</th><th>Description</th></tr>
<tr><td>None</td><td>0x00</td><td>None.</td></tr>
<tr><td>RemoteSessionsHosted</td><td>0x01</td><td>Hosted by remote session.</td></tr>
<tr><td>RemoteSessionsNotHosted</td><td>0x02</td><td>Indicates the device does not have session hosting status available.<5></td></tr>
<tr><td>NearShareAuthPolicySameUser</td><td>0x04</td><td>Indicates the device supports NearShare if the user is the same for the other device.</td></tr>
<tr><td>NearShareAuthPolicyPermissive</td><td>0x08</td><td>Indicates the device supports NearShare.<6></td></tr>
</table>
Salt (4 bytes): Four random bytes.
Device_Hash (19 bytes): SHA256 Hash of Salt plus Device Thumbprint.
</td></tr>
</table>

*Date format: YYYY/MM/DD

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-CFB] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

June 1, 2017 - Download

March 16, 2018 - Download

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

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

March 4, 2020 - Download

September 29, 2020 – Download

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

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

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

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

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

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

*Date format: YYYY/MM/DD

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

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

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

RSS

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

July 18, 2016 - Download

June 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 29, 2022 - Download

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

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

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

RSS

No errata are available for the latest version of 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-CRTD]: Certificate Templates Structure

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

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

RSS

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

April 7, 2021 - Download

Errata below are for Protocol Document Version V26.0 – 2021/06/25.

Errata Published*	Description
2022/06/28	In Section 2.4 flags Attribute: Description: "Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000." Changed from: "0x00000400 CT_FLAG_DONOTPERSISTINDB This flag indicates that the record of a certificate (1) request for a certificate (1) that is issued need not be persisted by the CA." Changed to: "0x00001000 CT_FLAG_DONOTPERSISTINDB This flag indicates that the record of a certificate (1) request for a certificate (1) that is issued need not be persisted by the CA.
2022/06/14	In Section 2.4 flags Attribute: Description: "Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000." Changed from: "0x00000400 CT_FLAG_DONOTPERSISTINDB This flag indicates that the record of a certificate (1) request for a certificate (1) that is issued need not be persisted by the CA." Changed to: "0x00001000 CT_FLAG_DONOTPERSISTINDB

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>This flag indicates that the record of a certificate (1) request for a certificate (1) that is issued need not be persisted by the CA."</td></tr>
<tr><td>2022/05/10</td><td>Section 2.26 msPKI-Enrollment-Flag Attribute

Description: "Added the CT_FLAG_NO_SECURITY_EXTENSION (0x00080000) enrollment flag that instructs the CA to not include security extension szOID_NTDS_CA_SECURITY_EXT (OID:1.3.6.1.4.1.311.25.2) in the issued certificate. Also added operating system applicability [MSFT-CVE-2022-26931] for this security update."

Changed From:

<table>
<tr><th>Flag</th><th>Meaning</th></tr>
<tr><td>0x00040000
CT_FLAG_SKIP_AUTO_RENEWAL</td><td>This flag indicates that the certificate should not be auto-renewed, although it has a valid template.</td></tr>
</table>

Changed To:

<table>
<tr><th>Flag</th><th>Meaning</th></tr>
<tr><td>0x00040000
CT_FLAG_SKIP_AUTO_RENEWAL</td><td>This flag indicates that the certificate should not be auto-renewed, although it has a valid template.</td></tr>
<tr><td>0x00080000
CT_FLAG_NO_SECURITY_EXTENSION</td><td>This flag[34] instructs the CA to not include the security extension szOID_NTDS_CA_SECURITY_EXT (OID:1.3.6.1.4.1.311.25.2), as specified in [MS-WCCE] sections 2.2.2.7.7.4 and 3.2.2.6.2.1.4.5.9, in the issued certificate.</td></tr>
</table>

[34] This flag is supported by the operating systems specified in [MSFT-CVE-2022-26931], each with its related KB article download installed.</td></tr>
<tr><td>2021/07/27</td><td>In Section 2.27 msPKI-Private-Key-Flag Attribute, replaced normative reference [PKCS12] with [RFC7292].

Changed from:

<table>
<tr><th>Flag</th><th>Meaning</th></tr>
<tr><td>0x00000010
CT_FLAG_EXPORTABLE_KEY</td><td>This flag instructs the client to allow other applications to copy the private key to a .pfx file, as specified in [PKCS12], at a later time.</td></tr>
</table>

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

Errata Published*	Description
	<table><tr><th>Flag</th><th>Meaning</th></tr><tr><td>0x00000010 CT_FLAG_EXPORTABLE_KEY</td><td>This flag instructs the client to allow other applications to copy the private key to a .pfx file, as specified in [RFC7292], at a later time.</td></tr></table>

*Date format: YYYY/MM/DD

[MS-CSRA]: Certificate Services Remote Administration Protocol

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

RSS

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

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

September 12, 2018 - Download

September 29, 2020 – Download

Errata below are for Protocol Document Version 41.0 – 2022/06/25.

Errata Published*	Description
2022/12/16	Section 3.1.4.1 Processing Rules for ICertAdminD Description: Specified client requirements to connect with RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, in order to mitigate the Active Directory Certificate Services elevation of privilege vulnerability, as described in [MSFT-CVE-2022-37976]. Changed from: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTADMIN and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning an error.<18> Changed to: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTADMIN (section 3.1.4.2.14) and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning an error. <18> <19> <19> The operating systems specified in [MSFT-CVE-2022-37976], each with their related KB article download installed, and the Active Directory Certificate Services elevation of privilege vulnerability mitigation described therein, requires that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTADMIN (section 3.1.4.2.14) setting. Section 3.1.4.2 Processing Rules for ICertAdminD2 Description: Specified client requirements to connect with RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, in order to mitigate the Active Directory Certificate Services elevation of privilege vulnerability, as described in [MSFT-CVE-2022-37976].

Errata Published*	Description
	Changed from: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTADMIN and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning an error. In Windows, the error is E_ACCESSDENIED (0x80070005). Changed to: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTADMIN (section 3.1.4.2.14) and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning the error E_ACCESSDENIED (0x80070005).<67> <67> The operating systems specified in [MSFT-CVE-2022-37976], each with their related KB article download installed, and the Active Directory Certificate Services elevation of privilege vulnerability mitigation described therein, requires that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTADMIN (section 3.1.4.2.14) setting.

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

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

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

RSS

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

July 18, 2016 - Download

June 1, 2017 - Download

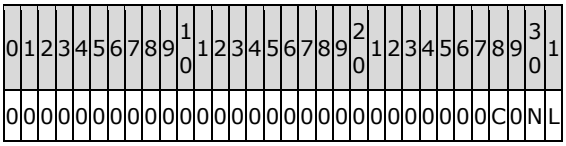
March 16, 2018 - Download

September 12, 2018 - Download

September 29, 2020 – Download

Errata below are for Protocol Document Version V20.0 – 2021/06/25.

Errata Published*	Description
2021/09/07	In Section 2.2.1.2.3.1 TSRemoteGuardPackageCred, changed credBuffer: Windows CredSSP usage of Kerberos User to User tickets. Changed from: credBuffer: An ASN.1 OCTET STRING byte buffer that contains the credentials in a format that SHOULD<22> be specified by the CredSSP server operating system for the package that provided them. <22> Section 2.2.1.2.3.1: . . .Windows CredSSP clients will use Kerberos User to User tickets ([RFC4120], section 2.9.2) as the ServiceTicket, but the server does not enforce this. . . Changed to: credBuffer: An ASN.1 OCTET STRING byte buffer that contains the credentials in a format that SHOULD<22> be specified by the CredSSP server operating system for the package that provided them. <22> Section 2.2.1.2.3.1: . . .Windows CredSSP clients do not use Kerberos User to User tickets ([RFC4120], section 2.9.2) as the ServiceTicket, but can if necessary; the server does not enforce this. . .
2021/08/10	In Section 2.2.1.2.3.1 TSRemoteGuardPackageCred, adjusted supplemental credential code arrangement and added C bit flag for the Credential Key being present. Changed from: typedef struct _NTLM_REMOTE_SUPPLEMENTAL_CREDENTIAL {

Errata Published*	Description
	ULONG Version; ULONG Flags; MSV1_0_CREDENTIAL_KEY_TYPE reserved; MSV1_0_CREDENTIAL_KEY reserved; ULONG reservedsize; [size_is(reservedSize)] UCHAR* reserved; } NTLM_REMOTE_SUPPLEMENTAL_CREDENTIAL; Version: A 32-bit unsigned integer that defines the credential version. This field is 0xFFFF0002. Flags: A 32-bit unsigned integer containing flags that define the credential options. At least one of the following values is required.  Where the bits are defined as follows: Value: L — Description: Indicates that the LM OWF member is present and valid. Value: N — Description: Indicates that the NT OWF member is present and valid. Changed to: typedef struct _NTLM_REMOTE_SUPPLEMENTAL_CREDENTIAL { ULONG Version; ULONG Flags; MSV1_0_CREDENTIAL_KEY reserved; MSV1_0_CREDENTIAL_KEY_TYPE reserved; ULONG reservedsize; [size_is(reservedSize)] UCHAR* reserved; } NTLM_REMOTE_SUPPLEMENTAL_CREDENTIAL; Version: A 32-bit unsigned integer that defines the credential version. This field is 0xFFFF0002. Flags: A 32-bit unsigned integer containing flags that define the credential options. At least one of the following values is required.  Where the bits are defined as follows:

Errata Published*	Description
	<table><tr><th>Value</th><th>Description</th></tr><tr><td>L</td><td>Indicates that the LM OWF member is present and valid.</td></tr><tr><td>N</td><td>Indicates that the NT OWF member is present and valid.</td></tr><tr><td>C</td><td>Indicates that the reserved credential key is present and valid ([MS-RDPEAR] section 2.2.1.3.5).</td></tr></table>

*Date format: YYYY/MM/DD

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

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

August 24, 2020 – Download

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

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

RSS

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

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

July 18, 2016 - Download

June 24, 2021 - Download

Errata below are for Protocol Document Version 23.0 - 2021/06/25.

Errata Published*	Description
2022/12/13	Section 3.2.4.1.1.2Issuing the Activation Request Description: Updated instances of 'RPC_C_AUTHN_LEVEL_PKT_INTEGRITY' authentication level constant value in product behavior note 81 to use RPC_C_AUTHN_LEVEL_CONNECT authentication level for specified operating systems. Changed from: <pbn81>: On Windows NT, Windows 2000, Windows XP, Windows XP SP1, and Windows Server 2003, DCOM clients specify RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. Changed to: <pbn81>: On Windows NT, Windows 2000, Windows XP, Windows XP SP1, and Windows Server 2003, DCOM clients specify RPC_C_AUTHN_LEVEL_CONNECT ([MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. Changed from: <pbn81>: On Windows XP SP2, Windows Server 2003 with SP1, Windows Vista and later, and Windows Server 2008 and later, DCOM clients specify the higher of the LegacyAuthenticationLevel value (for more information, [MSDN-LegAuthLevel]) and RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. Changed to: <pbn81>: On Windows XP SP2 and Windows Server 2003 with SP1, DCOM clients specify the higher of the LegacyAuthenticationLevel value ([MSDN-LegAuthLevel]) or RPC_C_AUTHN_LEVEL_CONNECT ([MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call.

Errata Published*	Description
	On Windows Vista and later and Windows Server 2008 and later, DCOM clients specify the higher of the LegacyAuthenticationLevel value ([MSDN-LegAuthLevel]) or RPC_C_AUTHN_LEVEL_PKT_INTEGRITY ([MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call.
2022/11/07	Section 3.2.4.1.1.2 Issuing the Activation Request Description: Updated to indicate that on Windows, the client can raise the authentication level requested by the application to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY, if it is less than that. Specified that the Windows 11 v22H2 operating system supports this behavior. Changed from: The client MUST specify the authentication level requested by the application, if one was supplied; otherwise, it MUST specify a default authentication level that is obtained in an implementation-specific manner. Changed to: The client MUST specify the authentication level at least as high as what is requested by the application; that is, if one is requested. However, note that the client MAY raise the authentication level<pbn-80>. Otherwise, the client MUST specify a default authentication level that is obtained in an implementation-specific manner<pbn-81>. Updated product behavior note 80: Changed from: On Windows NT, Windows 2000, Windows XP, Windows XP SP1, and Windows Server 2003, DCOM clients specify RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. On Windows XP SP2, Windows Server 2003 with SP1, Windows Vista and later, and Windows Server 2008 and later, DCOM clients specify the higher of the LegacyAuthenticationLevel value (for more information, see [MSDN-LegAuthLevel]) and RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. The default activation authentication level is raised to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level on client side and the required activation authentication level needs to be at least at RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level for authenticated activation on the server side, as applicable to the Windows 7 operating system with Service Pack 1 (SP1), Windows Server 2008 R2 Service Pack 1 (SP1), Windows 8.1, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 10, Windows Server 2022, Windows Server v1803 operating system, Windows Server v1809 operating system, Windows 10 v1607 operating system, Windows Server v1903 operating system, Windows Server 2019 Datacenter: Azure Edition (Turbine), Windows Server v1909 operating system, Windows Server v2004 operating system, Windows 10 v1803 operating system, Windows Server v20H2 Core operating system, Windows 10 v1809 operating system, Windows Server 2022 core, Windows 10 v1903 operating system, Windows 10 v1909 operating system, Windows 10 v2004 operating system, Windows 10 v20H2 operating system, Windows 10 v21H1 operating system, and Windows 11, to which this change has been backported. Changed to: <pbn-80> On Windows, the authentication level requested by the application is raised to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY ([MS-RPCE] section 2.2.1.1.8), if it is less than that. This behavior is supported in the specified operating systems that follow, each with its related

Errata Published*	Description
	KB article download installed: Windows 11 (Sun Valley) Desktop, Windows 11 (Sun Valley) Desktop Refresh, Windows 11 Desktop v22H2, Windows Server 2022 - Full/Core, Windows 10 Desktop v22H2, Windows 10 Desktop v21H2, Windows 10 Desktop v21H1, and Windows 10 Desktop v20H2.
2022/10/24	Section 3.2.4.1.1.2 Issuing the Activation Request Description: Updated to indicate that on Windows, the client can raise the authentication level requested by the application to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY, if it is less than that. Also specified the operating systems that support this behavior. Changed from: The client MUST specify the authentication level requested by the application, if one was supplied; otherwise, it MUST specify a default authentication level that is obtained in an implementation-specific manner. Changed to: The client MUST specify the authentication level at least as high as what is requested by the application; that is, if one is requested. However, note that the client MAY raise the authentication level<pbn-80>. Otherwise, the client MUST specify a default authentication level that is obtained in an implementation-specific manner<pbn-81>. <pbn-80>Updated; see below. Updated product behavior note 80: Changed from: On Windows NT, Windows 2000, Windows XP, Windows XP SP1, and Windows Server 2003, DCOM clients specify RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. On Windows XP SP2, Windows Server 2003 with SP1, Windows Vista and later, and Windows Server 2008 and later, DCOM clients specify the higher of the LegacyAuthenticationLevel value (for more information, see [MSDN-LegAuthLevel]) and RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. The default activation authentication level is raised to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level on client side and the required activation authentication level needs to be at least at RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level for authenticated activation on the server side, as applicable to the Windows 7 operating system with Service Pack 1 (SP1), Windows Server 2008 R2 Service Pack 1 (SP1), Windows 8.1, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 10, Windows Server 2022, Windows Server v1803 operating system, Windows Server v1809 operating system, Windows 10 v1607 operating system, Windows Server v1903 operating system, Windows Server 2019 Datacenter: Azure Edition (Turbine), Windows Server v1909 operating system, Windows Server v2004 operating system, Windows 10 v1803 operating system, Windows Server v20H2 Core operating system, Windows 10 v1809 operating system, Windows Server 2022 core, Windows 10 v1903 operating system, Windows 10 v1909 operating system, Windows 10 v2004 operating system, Windows 10 v20H2 operating system, Windows 10 v21H1 operating system, and Windows 11, to which this change has been backported. Changed to: <pbn-80> On Windows, the authentication level requested by the application is raised to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY ([MS-RPCE] section 2.2.1.1.8), if it is less than that. This behavior is supported in the specified operating systems that follow, each with its related KB article download installed: Windows 11, Windows 11 Refresh, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server v1809 operating system, Windows Server 2012 R2, Windows Server 2012 operating system, Windows Server 2008

Errata Published*	Description
	operating system with Service Pack 2 (SP2), Windows 10 version 22H2 operating system, Windows 10 v21H2 operating system, Windows 10 v21H1 operating system, Windows 10 v20H2 operating system, Windows 10 v1809 operating system, Windows 10 v1909 operating system, Windows 10 v1607 operating system, Windows 10 v1507 operating system, and Windows 7 operating system with Service Pack 1 (SP1).
2022/10/11	In Section 2.2.22.2.8.1 customREMOTE_REPLY_SCM_INFO Description: Updated product behavior note 37 in section 2.2.22.2.8.1 to ensure that RPC_C_AUTHN_LEVEL_PKT_INTEGRITY authentication level will be the minimum auth level following evaluation of the authentication level of DCOM client calls. Also specified the operating systems that support this behavior. Changed from: <37> Section 2.2.22.2.8.1: On Windows, DCOM servers return an RPC authentication level that denotes the minimum authentication level at which the object exporter can be called. On Windows, DCOM clients make calls to object exporters at an authentication level that is at least as high as the authnHint returned from the object server. Changed to: <37> Section 2.2.22.2.8.1: On Windows, DCOM servers return an RPC authentication level that denotes the minimum authentication level at which the object exporter can be called. On Windows, DCOM clients make calls to object exporters at an authentication level that is at least as high as the authnHint value returned from the object server, or the RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level, whichever is greater. Including the RPC_C_AUTHN_LEVEL_PKT_INTEGRITY authentication level in this evaluation is supported by the operating systems specified in [MSFT-CVE-2022-37978], each with its related KB article download installed.
2022/10/04	Section 3.2.4.1.1.2 Issuing the Activation Request Description: Updated to indicate that on Windows, the client can raise the authentication level requested by the application to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY, if it is less than that. Also specified the operating systems that support this behavior. Changed from: The client MUST specify the authentication level requested by the application, if one was supplied; otherwise, it MUST specify a default authentication level that is obtained in an implementation-specific manner. Changed to: The client MUST specify the authentication level at least as high as what is requested by the application; that is, if one is requested. However, note that the client MAY raise the authentication level<pbn-80>. Otherwise, the client MUST specify a default authentication level that is obtained in an implementation-specific manner<pbn-81>. <pbn-80>Updated; see below. Updated product behavior note 80: Changed from: On Windows NT, Windows 2000, Windows XP, Windows XP SP1, and Windows Server 2003, DCOM clients specify RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call.

Errata Published*	Description
	On Windows XP SP2, Windows Server 2003 with SP1, Windows Vista and later, and Windows Server 2008 and later, DCOM clients specify the higher of the LegacyAuthenticationLevel value (for more information, see [MSDN-LegAuthLevel]) and RPC_C_AUTHN_LEVEL_PKT_INTEGRITY (see [MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call. The default activation authentication level is raised to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level on client side and the required activation authentication level needs to be at least at RPC_C_AUTHN_LEVEL_PKT_INTEGRITY level for authenticated activation on the server side, as applicable to the Windows 7 operating system with Service Pack 1 (SP1), Windows Server 2008 R2 Service Pack 1 (SP1), Windows 8.1, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows 10, Windows Server 2022, Windows Server v1803 operating system, Windows Server v1809 operating system, Windows 10 v1607 operating system, Windows Server v1903 operating system, Windows Server 2019 Datacenter: Azure Edition (Turbine), Windows Server v1909 operating system, Windows Server v2004 operating system, Windows 10 v1803 operating system, Windows Server v20H2 Core operating system, Windows 10 v1809 operating system, Windows Server 2022 core, Windows 10 v1903 operating system, Windows 10 v1909 operating system, Windows 10 v2004 operating system, Windows 10 v20H2 operating system, Windows 10 v21H1 operating system, and Windows 11, to which this change has been backported. Changed to: <pbn-80> On Windows, the authentication level requested by the application is raised to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY ([MS-RPCE] section 2.2.1.1.8), if it is less than that. This behavior is supported in the specified operating systems that follow, each with its related KB article download installed: Windows 11 (Sun Valley) Desktop, Windows 11 (Sun Valley) Desktop Refresh, Windows Server 2022 - Full/Core, Windows 10 Desktop v22H2, Windows 10 Desktop v21H2, Windows 10 Desktop v21H1, and Windows 10 Desktop v20H2.

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

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

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

RSS

No errata are available for the latest version of 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 12, 2018 - Download

April 7, 2021 - Download

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

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

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

RSS

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

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-DNSP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

RSS

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 12, 2018 - Download

August 24, 2020 – Download

Errata below are for Protocol Document Version V37.0 – 2021/04/07.

Errata Published*	Description
2021/08/17	In Section 3.1.4.5 R_DnssrvUpdateRecord (opnum 4), added processing behavior for the static condition. Changed from: • If the pAddRecord is for an explicitly defined resource record type DNS_TYPE_CNAME (section 2.2.2.1.1), then delete any existing DNS_TYPE_CNAME record for the node specified in pszNodeName, before adding the record. • If pszZone is not NULL, search the DNS Zone Table for a zone with a name matching the value of pszZone. If a matching zone cannot be found return a failure. Changed to: • If the pAddRecord is for an explicitly defined resource record type DNS_TYPE_CNAME (section 2.2.2.1.1), then delete any existing DNS_TYPE_CNAME record for the node specified in pszNodeName, before adding the record. • If pAddRecord is for adding a new record to a dnsNode that has or had a static resource record (with TimeStamp at 0), then the new record is added as a static record.<279> • If pszZone is not NULL, search the DNS Zone Table for a zone with a name matching the value of pszZone. If a matching zone cannot be found return a failure. <279> Section 3.1.4.5: New records added as static in dnsNodes that contain or contained a static record is supported in Windows Server 2008 and later.
2021/08/10	In Section 3.1.1.1.1 DNS Server Integer Properties, in DsTombstoneInterval added seconds to 100-nanosecond conversion. Changed from:

Errata Published*	Description
	DsTombstoneInterval: . . . Every day at 2:00 AM local time the DNS server MUST conduct a search of all zones stored in the directory server for nodes which have the dnsTombstoned attribute set to TRUE and an EntombedTime (section 2.2.2.2.4.23) value greater than DsTombstoneInterval seconds in the past. . . . Changed to: DsTombstoneInterval: . . . Every day at 2:00 AM local time the DNS server MUST conduct a search of all zones stored in the directory server for nodes which have the dnsTombstoned attribute set to TRUE and an EntombedTime (section 2.2.2.2.4.23) value greater than DsTombstoneInterval seconds in the past (convert seconds to 100-nanosecond intervals for comparison). . . . In Section 3.1.4.5 R_DnssrvUpdateRecord (Opnum 4), changed EntombedTime from seconds to 100-nanosecond intervals and removed redundant instructions. Changed from: If pszZoneName points to a primary zone, attempt to perform addition/deletion/update of the record. If the operation is successful, increment the zone serial number using serial number arithmetic [RFC1982]. If the last record at the node is being deleted and the zone is stored in the directory server, the DNS server MUST set the node's dnsTombstoned attribute to TRUE and the node's dnsRecord (section 2.3.2.2) attribute to contain a DNS_RPC_RECORD_TS record (section 2.2.2.2.4.23) with an EntombedTime value equal to the current time expressed as the number seconds since 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC). If the zone is directory server-integrated and the update causes new or modified records to be committed to the directory, the new zone serial number MUST also be written to the Serial field of the dnsRecord attribute, as specified in2.3.2.2. If this operation deletes the last record from the node and the zone is directory server-integrated, the DNS server MUST set the node's DNS Node Tombstone State (section 3.1.1) to TRUE by setting the value of the dnsTombstoned attribute to TRUE and writing a DNS_RPC_RECORD_TS (section 2.2.2.2.4.23) in the dnsRecord attribute. Changed to: If pszZoneName points to a primary zone, attempt to perform addition/deletion/update of the record. If the operation is successful, increment the zone serial number using serial number arithmetic [RFC1982]. If the zone is directory server-integrated and the update causes new or modified records to be committed to the directory, the new zone serial number MUST also be written to the Serial field of the dnsRecord attribute (section 2.3.2.2). If the last record at the node is being deleted and the zone is stored in the directory server or is directory server-integrated, the DNS server MUST set the node's dnsTombstoned attribute to TRUE and the node's dnsRecord attribute to contain a DNS_RPC_RECORD_TS record (section 2.2.2.2.4.23) with an EntombedTime value equal to the current time expressed as the number of 100-nanosecond intervals since 12:00 A.M. January 1, 1601 Coordinated Universal Time (UTC).

*Date format: YYYY/MM/DD

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-DRSR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

April 7, 2021 - Download

Errata below are for Protocol Document Version V42.0 – 2021/06/25.

Errata Published*	Description
2022/06/01	In Section 5.39 DRS_EXTENSIONS_INT: Modified the description of the Pid field in the DRS_EXTENSIONS_INT structure to clarify how the field is set, which is to the current client or server process. Also revised behavior note <42> to clarify that the Pid field is set to the current client or server process. Changed From: "Pid (4 bytes): A 32-bit, signed integer value that specifies the process identifier of the client. This is for informational and debugging purposes only. The assignment of this field is implementation specific. <42>" <42> This field contains the process ID of the client. Changed To: "Pid (4 bytes): A 32-bit, signed integer value that specifies a process identifier. The client sets the Pid field to the current client process. The server sets the Pid to the current server process. This is for informational and debugging purposes only. The assignment of this field is implementation-specific.<42>" <42> This field contains the process ID of the client or server, depending on which is current.

*Date format: YYYY/MM/DD

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-DSCPM] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

July 18, 2016 - Download

December 1, 2017 - Download

September 12, 2018 - Download

[MS-DTYP]: Windows Data Types

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

April 7, 2021 - Download

April 29, 2022 - Download

April 4, 2023 - Download

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2023/06/27</td><td>In section 2.4.2.4, "Well-Known SID Structures," added a value (S-1-5-83-0) related to Hyper-V to the table:
<table>
<tr><td>NT_SERVICE
S-1-5-80</td><td>An NT Service account prefix.</td></tr>
<tr><td>USER_MODE_DRIVERS
S-1-5-84-0-0-0-0-0</td><td>Identifies a user-mode driver process.</td></tr>
</table>
Changed to:
<table>
<tr><td>NT_SERVICE
S-1-5-80</td><td>An NT Service account prefix.</td></tr>
<tr><td>NT VIRTUAL MACHINE\Virtual Machines
S-1-5-83-0</td><td>A built-in group. The group is created when the Hyper-V role is installed. Membership in the group is maintained by the Hyper-V Management Service (VMMS). Requires the Create Symbolic Links right (SeCreateSymbolicLinkPrivilege) and the Log on as a Service right (SeServiceLogonRight).</td></tr>
<tr><td>USER_MODE_DRIVERS</td><td>Identifies a user-mode driver process.</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description
	S-1-5-84-0-0-0-0-0
2023/05/16	In section 2.5.1.1, "Syntax," revised grammar to properly treat ! as a unary operator. Changed from: ; multiple rules for cond-expr to represent different precedence of || and && ; super-term and factor are intermediate rules and used only in this part of the grammar cond-expr = expr expr = super-term [wspace] *("||" [wspace] super-term) super-term = factor [wspace] *("&&" [wspace] factor) factor = ["!"] [wspace] "(" [wspace] factor [wspace] ")" factor = term Changed to: ; multiple rules for cond-expr to represent different precedence of || and && ; super-term and factor are intermediate rules and used only in this part of the grammar cond-expr = expr expr = super-term [wspace] *("||" [wspace] super-term) super-term = factor [wspace] *("&&" [wspace] factor) factor = term factor /= "(" [wspace] expr [wspace] ")" factor /= "!" [wspace] factor

*Date format: YYYY/MM/DD

[MS-DVRD]: Device Registration Discovery Protocol

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-DVRE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-DVRJ] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-ECS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

August 24, 2020 – Download

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

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

RSS

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

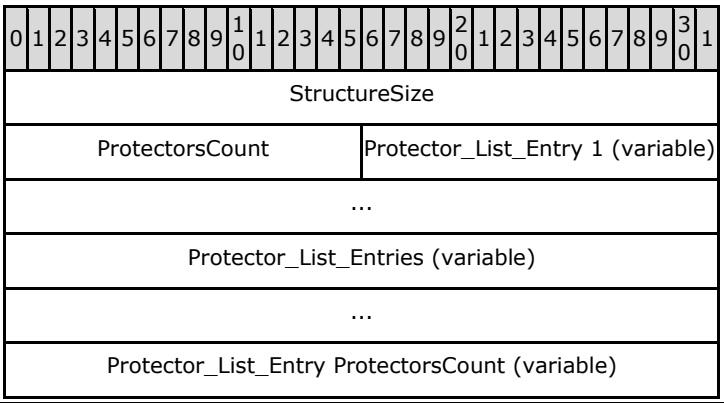
To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

July 18, 2016 - Download

October 6, 2021 - Download

April 29, 2022 - Download

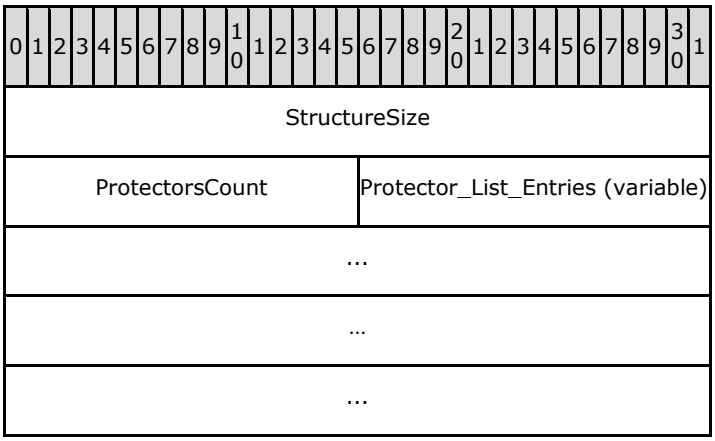
Errata below are for Protocol Document Version V30.0 – 2022/04/29.

Errata Published*	Description
2022/07/26	In section 3.1.4.2, EFSRPC Interface, added a product behavior note describing change after applying [MSFTE-CVE-2022-26925]: Changed from: The following table specifies the opnum associated with each RPC method in this protocol. An EFSRPC server SHOULD support all of the methods specified in this table.<37> Changed to: The following table specifies the opnum associated with each RPC method in this protocol. An EFSRPC server SHOULD support all of the methods specified in this table.<37><38> <38> Section 3.1.4.2: After installation of one of the updates listed in [MSFT-CVE-2022-26925], a client using a null session will receive RPC_S_ACCESS_DENIED when calling any of these methods using lsarpc.
2022/07/26	In section 2.2.2.2.1, Protector List Structure, removed two fields from structure diagram: Changed from: The DDF and DRF Protector List structure in the Version 4 EFSRPC Metadata MUST be formatted as follows. 

Errata Published*	Description
	...

Changed to:

The DDF and DRF Protector List structure in the Version 4 EFSRPC Metadata MUST be formatted as follows.



*Date format: YYYY/MM/DD

[MS-EMF]: Enhanced Metafile Format

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

April 29, 2022 - Download

[MS-EMFPLUS]: Enhanced Metafile Format Plus Extensions

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

March 4, 2020 - Download

April 7, 2021 - Download

Errata below are for Protocol Document Version V19.0 – 2021/06/25.

Errata Published*	Description
2021/10/12	In Section 2.3.4.15, EmfPlusFillClosedCurve Record, amended descriptions of fill operations. Changed from: A "winding" fill operation fills areas according to the "even-odd parity" rule... An "alternate" fill operation fills areas according to the "non-zero" rule.... Changed to: An "alternate" fill operation fills areas according to the "even-odd parity" rule... A "winding" fill operation fills areas according to the "non-zero" rule....

*Date format: YYYY/MM/DD

[MS-EMFSPOOL]: Enhanced Metafile Spool Format

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

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

RSS

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

April 7, 2021 - Download

[MS-ERREF]: Windows Error Codes

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

[MS-EVEN]: EventLog Remoting Protocol

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

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

RSS

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

July 18, 2016 - Download

April 7, 2021 - Download

June 24, 2021 - Download

Errata below are for Protocol Document Version V24.0 – 2021/06/25.

Errata Published*	Description
2021/07/27	In Section 2.1.2, Client: Changed from: The client MUST specify packet-level authentication (0x4) or higher, as specified in [MS-RPCE] section 2.2.1.1.8.<6> Changed to: The client MUST specify packet-level integrity authentication (0x5) or higher, as specified in [MS-RPCE] section 2.2.1.1.8.<6>.

*Date format: YYYY/MM/DD

[MS-EVEN6]: EventLog Remoting Protocol Version 6.0

This topic lists Errata found in [MS-EVEN6] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

RSS

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:

September 12, 2018 - Download

June 24, 2021 - Download

Errata below are for Protocol Document Version V24.0 – 2021/06/25.

Errata Published*	Description
2021/07/27	In Section 2.1.2, Client: Changed from: The client MUST specify packet-level authentication (0x4) or higher, as specified in [MS-RPCE] section 2.2.1.1.8.<5> Changed to: The client MUST specify packet-level integrity authentication (0x5) or higher, as specified in [MS-RPCE] section 2.2.1.1.8.<5>

*Date format: YYYY/MM/DD

[MS-FASP]: Firewall and Advanced Security Protocol

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

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

RSS

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

July 18, 2016 - Download

March 13, 2019 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version v31.0 – 2022/04/29.

Errata Published*	Description
2022/09/20	Section 3.1.4 Message Processing Events and Sequencing Description: Removed duplicate instances of 'unsigned' designator in subsections 3.1.4.59, 3.1.4.60, 3.1.4.62, 3.1.4.67, 3.1.4.68, 3.1.4.69, and 3.1.4.70. Section 3.1.6 Other Local Events Description: Added abstract interface definitions from subsections 3.1.6.1, 3.1.6.2, 3.1.6.3, 3.1.6.4, 3.1.6.5, 3.1.6.6, 3.1.6.7, and 3.1.6.8 to Section 6 Full IDL. Section 6 Full IDL Added policy store handle to the Full IDL. Added abstract interfaces to the Full IDL (definitions from sections 3.1.6.1, 3.1.6.2, 3.1.6.3, 3.1.6.4, 3.1.6.5, 3.1.6.6, 3.1.6.7, and 3.1.6.8). Replaced 'typedef struct _tag_FW_QUERY_CONDITIONS' in IDL with actual code instance.
2022/09/20	In Section 2.2.92: FW_QUERY_CONDITIONS Description: Updated definition of FW_QUERY_CONDITIONS struct. Changed from: typedef struct _tag_FW_QUERY_CONDITIONS {; unsigned LONG dwNumEntries; [size_is(dwNumEntries)] FW_QUERY_CONDITION* pAndedConditions; } FW_QUERY_CONDITIONS, *PFW_QUERY CONDITIONS; dwNumEntries: Specifies the number of query conditions that the structure contains. pAndedConditions: A pointer to an array of FW_QUERY_CONDITIONS elements, which are all logically AND'd together. The number of elements is given by dwNumEntries. Changed to: typedef struct_tag_FW_QUERY_CONDITIONS { DWORD dwNumEntries; [size_is(dwNumEntries)] FW_QUERY_CONDITION *AndedConditions;

Errata Published*	Description
	} FW_QUERY_CONDITIONS, *PFW_QUERY_CONDITIONS; dwNumEntries: Specifies the number of query conditions that the structure contains. AndedConditions: A pointer to an array of FW_QUERY_CONDITIONS elements, which are to be logically AND'd together by the server. Section 6 Appendix A Full IDL Changed from: Identical to the above. Changed to: Identical to the above.

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

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

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

RSS

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

September 12, 2018 - Download

[MS-FRS2]: Distributed File System Replication Protocol

This topic lists Errata found in [MS-FRS2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

[MS-FSA]: File System Algorithms

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

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

RSS

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

March 2, 2016 - Download

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

June 24, 2019 – Download

March 4, 2020 - Download

August 24, 2020 – Download

June 1, 2021 - Download

October 6, 2021 - Download

April 4, 2023 - Download

[MS-FSCC]: File System Control Codes

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

RSS

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

December 1, 2017 - Download

September 12, 2018 - Download

September 23, 2019 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

Errata below are for Protocol Document Version V52.0 – 2022/04/29.

Errata Published *	Description
2023/02/14	In MS-FSCC, added a new section documenting the FSCTL_VIRTUAL_STORAGE_QUERY_PROPERTY: Changed to: 2.3.91 FSCTL_VIRTUAL_STORAGE_QUERY_PROPERTY Request This request contains a message with the same structure as the IOCTL_STORAGE_QUERY_PROPERTY request (section 2.8.1) with the following values: PropertyId (4 bytes): 0x00000004 QueryType (4 bytes): 0x00000000 Remote servers SHOULD ignore this request.<86> <86> Section 2.3.91: All Windows Server versions return STATUS_NOT_IMPLEMENTED.

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td>2023/01/30</td><td>In section 2.4.7, revised behavior notes 97 through 100 to indicate the responses to a -2 value for certain attributes on different file systems.

Changed from:
<97> Section 2.4.7: The file system updates the values of the LastAccessTime, LastWriteTime, and ChangeTime members as appropriate after an I/O operation is performed on a file. However, a driver or application can request that the file system not update one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -1. A driver or application can subsequently request that the file system resume updating one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -2. The caller can set one, all, or any other combination of these three members to -1 and/or -2. Only the members that are set to -1 will be unaffected by I/O operations on the file handle; the other members will be updated as appropriate. This behavior is consistent across all file system types. Note that even though -1 and -2 can be used with the CreationTime field, they have no effect because file creation time is never updated in response to file system calls such as read and write.
<table>
<tr><th>File system</th><th>Support value of -2</th></tr>
<tr><td>FAT</td><td>No</td></tr>
<tr><td>EXFAT</td><td>No</td></tr>
<tr><td>FAT32</td><td>No</td></tr>
<tr><td>Cdfs</td><td>No</td></tr>
<tr><td>UDFS</td><td>No</td></tr>
<tr><td>NTFS</td><td>Windows 8.1 and later, Windows Server 2012 R2 and later, and Windows Server v1709 operating system and later</td></tr>
<tr><td>ReFS</td><td>Windows 10 v1507 operating system and later, Windows Server 2016 and later, and Windows Server v1709 and later</td></tr>
</table>
<98> Section 2.4.7: The file system updates the values of the LastAccessTime, LastWriteTime, and ChangeTime members as appropriate after an I/O operation is performed on a file. However, a driver or application can request that the file system not update one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -1. A driver or application can subsequently request that the file system resume updating one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -2. The caller can set one, all, or any other combination of these three members to -1 and/or -2. Only the members that are set to -1 will be unaffected by I/O operations on the file handle; the other members will be updated as appropriate. This behavior is consistent across all file system types. Note that even though -1 and -2 can be used with the CreationTime field, they have no effect because file creation time is never updated in response to file system calls such as read and write.
<table>
<tr><th>File system</th><th>Support value of -2</th></tr>
<tr><td>FAT</td><td>No</td></tr>
<tr><td>EXFAT</td><td>No</td></tr>
<tr><td>FAT32</td><td>No</td></tr>
</table></td></tr>
</table>

Errata Published *	Description

Cdfs	No
UDFS	No
NTFS	Windows 8.1 and later, Windows Server 2012 R2 and later and Windows Server v1709 and later
ReFS	Windows 10 v1507 and later, Windows Server 2016 and later, and Windows Server v1709 and later

<99> Section 2.4.7: The file system updates the values of the **LastAccessTime**, **LastWriteTime**, and **ChangeTime** members as appropriate after an I/O operation is performed on a file. However, a driver or application can request that the file system not update one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -1. A driver or application can subsequently request that the file system resume updating one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -2. The caller can set one, all, or any other combination of these three members to -1 and/or -2. Only the members that are set to -1 will be unaffected by I/O operations on the file handle; the other members will be updated as appropriate. This behavior is consistent across all file system types. Note that even though -1 and -2 can be used with the **CreationTime** field, they have no effect because file creation time is never updated in response to file system calls such as read and write.

File system	Support value of -2
FAT	No
EXFAT	No
FAT32	No
Cdfs	No
UDFS	No
NTFS	Windows 8.1 and later, Windows Server 2012 R2 and later and Windows Server v1709 and later
ReFS	Windows 10 v1507 and later, Windows Server 2016 and later, and Windows Server v1709 and later

<100> Section 2.4.7: The file system updates the values of the **LastAccessTime**, **LastWriteTime**, and **ChangeTime** members as appropriate after an I/O operation is performed on a file. However, a driver or application can request that the file system not update one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -1. A driver or application can subsequently request that the file system resume updating one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -2. The caller can set one, all, or any other combination of these three members to -1 and/or -2. Only the members that are set to -1 will be unaffected by I/O operations on the file handle; the other members will be updated as appropriate. This behavior is consistent across all file system types. Note that even though -1 and -2 can be used with the **CreationTime** field, they have no effect because file creation time is never updated in response to file system calls such as read and write.

File system	Support value of -2
FAT	No
EXFAT	No
FAT32	No
Cdfs	No
UDFS	No
NTFS	Windows 8.1 and later, Windows Server 2012 R2 and later and Windows Server v1709 and later
ReFS	Windows 10 v1507 and later, Windows Server 2016 and later, and Windows Server v1709 and later

Changed to:

<97> Section 2.4.7: The file system updates the values of the **LastAccessTime**, **LastWriteTime**, and **ChangeTime** members as appropriate after an I/O operation is performed on a file. However, a driver or application can request that the file system not update one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -1. A driver or application can subsequently request that the file system resume updating one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -2. The caller can set one, all, or any other combination of these three members to -1 and/or -2. Only the members that are set to -1 will be unaffected by I/O operations on the file handle; the other members will be updated as appropriate. This behavior is consistent across all file system types. Note that even though -1 and -2 can be used with the **CreationTime** field, they have no effect because file creation time is never updated in response to file system calls such as read and write.

File system	Support value of -2
FAT	No
EXFAT	No
FAT32	No
Cdfs	No
UDFS	No
NTFS	Windows 8.1 and later, and Windows Server 2012 R2 and later
ReFS	Windows 10 v1507 operating system and later, and Windows Server 2016 and later

<98> Section 2.4.7: The file system updates the value of the **LastAccessTime** member as appropriate after an I/O operation is performed on a file. However, a driver or application can request that the file system not update one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -1. A driver or application can subsequently request that the file system resume updating one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -2. The caller can set one, all, or any other combination of these three members to -1 and/or -2. Only the members that are set to -1 will be unaffected by I/O operations on the file handle; the other members will be updated as appropriate. This behavior

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td></td><td>is consistent across all file system types. Note that even though -1 and -2 can be used with the CreationTime field, they have no effect because file creation time is never updated in response to file system calls such as read and write.
<table>
<tr><th>File system</th><th>Support value of -2</th></tr>
<tr><td>FAT</td><td>No</td></tr>
<tr><td>EXFAT</td><td>No</td></tr>
<tr><td>FAT32</td><td>No</td></tr>
<tr><td>Cdfs</td><td>No</td></tr>
<tr><td>UDFS</td><td>No</td></tr>
<tr><td>NTFS</td><td>Windows 8.1 and later, and Windows Server 2012 R2 and later</td></tr>
<tr><td>ReFS</td><td>Windows 10 v1507 and later, and Windows Server 2016 and later</td></tr>
</table>
<99> Section 2.4.7: The file system updates the value of the LastWriteTime member as appropriate after an I/O operation is performed on a file. However, a driver or application can request that the file system not update one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -1. A driver or application can subsequently request that the file system resume updating one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -2. The caller can set one, all, or any other combination of these three members to -1 and/or -2. Only the members that are set to -1 will be unaffected by I/O operations on the file handle; the other members will be updated as appropriate. This behavior is consistent across all file system types. Note that even though -1 and -2 can be used with the CreationTime field, they have no effect because file creation time is never updated in response to file system calls such as read and write.
<table>
<tr><th>File system</th><th>Support value of -2</th></tr>
<tr><td>FAT</td><td>No</td></tr>
<tr><td>EXFAT</td><td>No</td></tr>
<tr><td>FAT32</td><td>No</td></tr>
<tr><td>Cdfs</td><td>No</td></tr>
<tr><td>UDFS</td><td>No</td></tr>
<tr><td>NTFS</td><td>Windows 8.1 and later, and Windows Server 2012 R2 and later</td></tr>
<tr><td>ReFS</td><td>Windows 10 v1507 and later, and Windows Server 2016 and later</td></tr>
</table>
<100> Section 2.4.7: The file system updates the value of the ChangeTime member as appropriate after an I/O operation is performed on a file. However, a driver or application can request that the file system not update one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -1. A driver or application can subsequently request that the file system resume updating one or more of these members for I/O operations that are performed on the caller's file handle by setting the appropriate members to -2. The caller can set one, all, or any other combination of these three </td></tr>
</table>

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td></td><td>members to -1 and/or -2. Only the members that are set to -1 will be unaffected by I/O operations on the file handle; the other members will be updated as appropriate. This behavior is consistent across all file system types. Note that even though -1 and -2 can be used with the CreationTime field, they have no effect because file creation time is never updated in response to file system calls such as read and write.
<table>
<tr><th>File system</th><th>Support value of -2</th></tr>
<tr><td>FAT</td><td>No</td></tr>
<tr><td>EXFAT</td><td>No</td></tr>
<tr><td>FAT32</td><td>No</td></tr>
<tr><td>Cdfs</td><td>No</td></tr>
<tr><td>UDFS</td><td>No</td></tr>
<tr><td>NTFS</td><td>Windows 8.1 and later, and Windows Server 2012 R2 and later</td></tr>
<tr><td>ReFS</td><td>Windows 10 v1507 and later, and Windows Server 2016 and later</td></tr>
</table></td></tr>
<tr><td>2023/01/10</td><td>In section 2.3.74, FSCTL_SET_INTEGRITY_INFORMATION Reply, added STATUS_NOT_SUPPORTED to the error codes list:
Changed from:
<table>
<tr><th>Error code</th><th>Meaning</th></tr>
<tr><td>STATUS_INVALID_PARAMETER
0xC000000D</td><td>The input buffer length is less than the size, in bytes, of the FSCTL_SET_INTEGRITY_INFORMATION_BUFFER element; the handle is not to a file or directory; or the requested ChecksumAlgorithm field is not one of the values listed in the table for the ChecksumAlgorithm field in the FSCTL_SET_INTEGRITY_INFORMATION Request.</td></tr>
<tr><td>STATUS_INVALID_DEVICE_REQUEST
0xC0000010</td><td>The volume does not support integrity.</td></tr>
<tr><td>STATUS_DISK_FULL
0xC000007F</td><td>The disk is full.</td></tr>
</table>
Changed to:
<table>
<tr><th>Error code</th><th>Meaning</th></tr>
<tr><td>STATUS_INVALID_PARAMETER
0xC000000D</td><td>The input buffer length is less than the size, in bytes, of the FSCTL_SET_INTEGRITY_INFORMATION_BUFFER element; the handle is not to a file or directory; or the requested ChecksumAlgorithm field is not one of the values listed in the table for the ChecksumAlgorithm field in the FSCTL_SET_INTEGRITY_INFORMATION Request.</td></tr>
<tr><td>STATUS_INVALID_DEVICE_REQUEST</td><td>The volume does not support integrity.</td></tr>
</table></td></tr>
</table>

Errata Published *	Description

0xC0000010	
STATUS_DISK_FULL 0xC000007F	The disk is full.
STATUS_NOT_SUPPORTED 0xC00000BB	The file has been ghosted (allocation blocks are being shared).

In section 2.3.75, FSCTL_SET_INTEGRITY_INFORMATION_EX Request, revised note <76> to indicate which versions support this request:

Changed from:

<76> Section 2.3.75: The FSCTL_SET_INTEGRITY_INFORMATION_EX Request message is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or higher). FSCTL_SET_INTEGRITY_INFORMATION_EX is processed as described on systems updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], [MSKB-5014023], [MSKB-5014701], [MSKB-5014702], or [MSKB-5014710].

Changed to:

<76> Section 2.3.75: The FSCTL_SET_INTEGRITY_INFORMATION_EX Request message is supported only by Windows Server 2022 and higher, and Windows 11, version 22H2 operating system and higher. FSCTL_SET_INTEGRITY_INFORMATION_EX is processed as described on systems updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], [MSKB-5014023], [MSKB-5014701], [MSKB-5014702], or [MSKB-5014710].

In section 2.3.76, FSCTL_SET_INTEGRITY_INFORMATION_EX Reply, added STATUS_NOT_SUPPORTED to the error codes list:

Changed from:

Error code	Meaning
STATUS_INVALID_PARAMETER 0xC000000D	The input buffer length is less than the size, in bytes, of the FSCTL_SET_INTEGRITY_INFORMATION_BUFFER_EX element; the handle is not to a file or directory; or Version is not equal to 1.
STATUS_INVALID_DEVICE_REQUEST 0xC0000010	The volume does not support integrity.
STATUS_DISK_FULL 0xC000007F	The disk is full.

Changed to:

Error code	Meaning
STATUS_INVALID_PARAMETER 0xC000000D	The input buffer length is less than the size, in bytes, of the FSCTL_SET_INTEGRITY_INFORMATION_BUFFER_E

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>X element; the handle is not to a file or directory; or Version is not equal to 1.</td></tr>
<tr><td>STATUS_INVALID_DEVICE_REQUEST
0xC0000010</td><td>The volume does not support integrity.</td></tr>
<tr><td>STATUS_DISK_FULL
0xC000007F</td><td>The disk is full.</td></tr>
<tr><td>STATUS_NOT_SUPPORTED
0xC00000BB</td><td>The file has been ghosted (allocation blocks are being shared).</td></tr>
</table>
</td></tr>
<tr><td>2022/08/09</td><td>
In section 2.7.1, FILE_NOTIFY_INFORMATION, revised descriptions of the values in the Action field.

Changed from:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>FILE_ACTION_ADDED
0x00000001</td><td>The file was added to the directory.</td></tr>
<tr><td>FILE_ACTION_REMOVED
0x00000002</td><td>The file was removed from the directory. When a file is renamed to a different directory the client will receive this notification along with FILE_ACTION_MODIFIED.</td></tr>
<tr><td>FILE_ACTION_MODIFIED
0x00000003</td><td>The file was modified. This can be a change to the data or attributes of the file. When a file is renamed to a different directory the client will receive this notification along with FILE_ACTION_REMOVED.</td></tr>
</table>
Changed to:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>FILE_ACTION_ADDED
0x00000001</td><td>The file was renamed, and FileName contains the new name. This notification is only sent when the rename operation changes the directory the file resides in. The client will also receive a FILE_ACTION_REMOVED notification. This notification will not be received if the file is renamed within a directory.</td></tr>
<tr><td>FILE_ACTION_REMOVED
0x00000002</td><td>The file was renamed, and FileName contains the old name. This notification is only sent when the rename operation changes the directory the file resides in. The client will also receive a FILE_ACTION_ADDED notification. This notification will not be received if the file is renamed within a directory.</td></tr>
<tr><td>FILE_ACTION_MODIFIED
0x00000003</td><td>The file was modified. This can be a change to the data or attributes of the file.</td></tr>
</table>
</td></tr>
<tr><td>2022/05/27</td><td>
In section 2.3.75, FSCTL_SET_INTEGRITY_INFORMATION_EX Request, updated list of applicable updates.

Changed from:
<76> Section 2.3.75: The FSCTL_SET_INTEGRITY_INFORMATION_EX Request message is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or
</td></tr>
</table>

Errata Published *	Description
	higher). FSCTL_SET_INTEGRITY_INFORMATION_EX is processed as described on systems updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], or [MSKB-5014023]. Changed to: <76> Section 2.3.75: The FSCTL_SET_INTEGRITY_INFORMATION_EX Request message is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or higher). FSCTL_SET_INTEGRITY_INFORMATION_EX is processed as described on systems updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], [MSKB-5014023], [MSKB-5014701], [MSKB-5014702], or [MSKB-5014710].
2022/05/02	In Section 2.1.5.9.34, FSCTL_SET_INTEGRITY_INFORMATION_EX, updated processing rules for system versions. Changed from: The server provides:<127> <127> Section 2.1.5.9.34: The FSCTL_SET_INTEGRITY_INFORMATION_EX operation is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or higher). Changed to: The server provides:<127> <127> Section 2.1.5.9.34: The FSCTL_SET_INTEGRITY_INFORMATION_EX operation is supported only by the ReFS file system v3.2 or higher (Windows 10 v1507 operating system or higher). FSCTL_SET_INTEGRITY_INFORMATION_EX is handled following the process in this section on systems updated with [MSKB-5014019], [MSKB-5014021], [MSKB-5014022], or [MSKB-5014023].

[MS-FSRVP]: File Server Remote VSS Protocol

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-FSVCA] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-GPPREF] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

July 18, 2016 - Download

September 12, 2018 - Download

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

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

September 12, 2018 - Download

[MS-GPOL]: Group Policy: Core Protocol

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

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

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

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

RSS

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

April 7, 2021 - Download

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

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

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

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

June 1, 2017 - Download

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

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

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

RSS

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

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

June 24, 2019 – Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-HVRS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-ICPR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-IKEE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

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

This topic lists Errata found in [MS-IPAMM2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

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

July 18, 2016 - Download

June 1, 2017 - Download

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

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

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

RSS

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

September 12, 2018 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-KILE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

April 29, 2022 - Download

December 1, 2022 - Download

Errata below are for Protocol Document Version V40.0 – 2022/12/01.

Errata Published*	Description
2023/04/11	In Section 3.1.5.2 Encryption Types: Added that all other encryption types, that are not listed, SHOULD be rejected. In the product notes 24 and new 25, added CVE references with product applicability. Changed from: KILE MUST<23> support the Advanced Encryption Standard (AES) encryption types: • AES256-CTS-HMAC-SHA1-96 [18] ([RFC3962] section 7) • AES128-CTS-HMAC-SHA1-96 [17] ([RFC3962] section 7) and SHOULD<24> support the following encryption types, which are listed in order of relative strength: • RC4-HMAC [23] [RFC4757] • DES-CBC-MD5 [3] [RFC3961] • DES-CBC-CRC [1] [RFC3961] Kerberos V5 encryption type assigned numbers are specified in [RFC3961] section 8, [RFC4757] section 5, and [RFC3962] section 7.<25> <24> Section 3.1.5.2: In Windows 2000 and Windows Server 2003, KDCs select the encryption type based on the preference order in the client request. Otherwise, KDCs select the encryption type used for pre-authentication or, when pre-authentication is not used, the encryption type is based on the preference order in the client request. RC4-HMAC is supported in Windows. Only Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 support DES by default.

Errata Published*	Description
	Changed to: KILE MUST<23> support the Advanced Encryption Standard (AES) encryption types: • AES256-CTS-HMAC-SHA1-96 [18] ([RFC3962] section 7) • AES128-CTS-HMAC-SHA1-96 [17] ([RFC3962] section 7) and SHOULD<24> support the following encryption types, which are listed in order of relative strength: • RC4-HMAC [23] [RFC4757] • DES-CBC-MD5 [3] [RFC3961] • DES-CBC-CRC [1] [RFC3961] All other Encryption Types SHOULD<25> be rejected. Kerberos V5 encryption type assigned numbers are specified in [RFC3961] section 8, [RFC4757] section 5, and [RFC3962] section 7.<26> <24> Section 3.1.5.2: In Windows 2000 and Windows Server 2003, KDCs select the encryption type based on the preference order in the client request. Otherwise, KDCs select the encryption type used for pre-authentication or, when pre-authentication is not used, the encryption type is based on the preference order in the client request. Only Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 support DES by default. RC4-HMAC is supported in Windows. For more information on RC4 and encryption type updates see Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability security update November 2022 [MSFT-CVE-2022-37966] and Windows Kerberos Elevation of Privilege Vulnerability security update November 2022 [MSFT-CVE-2022-37967]. These updates apply to Windows Server 2008 SP2 and later. <25> Section 3.1.5.2: For more information see Windows Kerberos Elevation of Privilege Vulnerability security updates September 2022 [MSFT-CVE-2022-33647] and [MSFT-CVE-2022-33679]. These updates apply to Windows Server 2008 SP2 and later.
2023/03/06	Section 5.1 Security Considerations for Implementers: Added statement to recommend strong vs. weak encryption usage. Changed from: 5.1 Security Considerations for Implementers KILE has the same security considerations as Kerberos V5 ([RFC4120], [RFC3961], [RFC3962], and [RFC4757]) and GSS-API ([RFC2743], [RFC1964], and [RFC4121]). Changed to: 5.1 Security Considerations for Implementers KILE has the same security considerations as Kerberos V5 ([RFC4120], [RFC3961], [RFC3962], and [RFC4757]) and GSS-API ([RFC2743], [RFC1964], and [RFC4121]). The encryption types AES128-CTC-HMAC-SHA1-96/AES256-CTC-HMAC-SHA1-96 or including AES256-CTS-HMAC-SHA1-96-SK if RC4 encryption types is selected is recommended. Setting RC4/DES only is weak and not recommended. For more information see section 2.2.7.
2023/03/06	Section 2.2.7 Supported Encryption Types Bit Flags: Added note to recommend strong vs. weak encryption usage.

Errata Published*	Description
	Changed from: AES256-CTS-HMAC-SHA1-96-SK: Enforce AES session keys when legacy ciphers are in use. When the bit is set, this indicates to the KDC that all cases where RC4 session keys can be used will be superseded with AES keys. All other bits MUST be set to zero when sent and MUST be ignored when they are received. Changed to: AES256-CTS-HMAC-SHA1-96-SK: Enforce AES session keys when legacy ciphers are in use. When the bit is set, this indicates to the KDC that all cases where RC4 session keys can be used will be superseded with AES keys. Note: The encryption types AES128-CTC-HMAC-SHA1-96/AES256-CTC-HMAC-SHA1-96 or including AES256-CTS-HMAC-SHA1-96-SK if RC4 encryption types is selected is recommended. Setting RC4/DES only is weak and not recommended. All other bits MUST be set to zero when sent and MUST be ignored when they are received.

*Date format: YYYY/MM/DD

[MS-KPP]: Key Provisioning Protocol

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-KPP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-LCID] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

March 13, 2019 - Download

June 24, 2021 - Download

Errata below are for Protocol Document Version V15.0 – 2021/06/25.

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td>2022/05/02</td><td>
In Section 2.2, LCID Structure, added the following language IDs to the table:

0x2000 Unassigned LCID locale temporarily assigned to LCID 0x3000. See section 2.2.1.

0x2400 Unassigned LCID locale temporarily assigned to LCID 0x3000. See section 2.2.1.

0x2800 Unassigned LCID locale temporarily assigned to LCID 0x3000. See section 2.2.1.
0x2C00 Unassigned LCID locale temporarily assigned to LCID 0x3000. See section 2.2.1.

In Section 2.2.1, Locale Names without LCIDs, updated the table:

Changed from:

<table>
<tr><th>Name</th><th>Value</th><th>Conditions</th></tr>
<tr><td>LOCALE_CUSTOM_USER_DEFAULT<15></td><td>0x0C00</td><td>When an LCID without a permanent LCID assignment is also the current user locale, the protocol will respond with LOCALE_CUSTOM_USER_DEFAULT for that locale. This assignment persists until the user changes the locale. Because the meaning changes over time, applications are discouraged from persisting this data. Though this value will likely refer to the same locale for the lifetime of the current process, that is not guaranteed. This assignment is</td></tr>
</table>
</td></tr>
</table>

Errata Published *	Description

		a 1-to-1 relationship between this LCID and the user's current default locale name.
Transient LCIDs<16>	0x3000, 0x3400, 0x3800, 0x3C00, 0x4000, 0x4400, 0x4800, 0x4C00	Some user configurations temporarily associate a locale without a permanent LCID assignment with one of these 8 transient LCIDs. This assignment is transient and it is not guaranteed; it will likely refer to the same locale for the lifetime of the process. However, this assignment will differ for other users on the machine, or other machines, and, as such, is unsuitable for use in protocols or persisted data. This assignment is a temporary 1-to-1 relationship between an LCID and a particular locale name and will round trip until that relationship changes.

Changed to:

Name	Value	Conditions
LOCALE_CUSTOM_USER_DEFAULT<15>	0x0C00	When an LCID without a permanent LCID assignment is also the current user locale, the protocol will respond with LOCALE_CUSTOM_USER_DEFAULT for that locale. This assignment persists until the user changes the locale. Because the meaning changes over time, applications are discouraged from persisting this data. Though this value will likely refer to the same locale for the lifetime of the current process, that is not guaranteed. This assignment is a 1-to-1 relationship between this LCID and the user's current default locale name.
Transient LCIDs<16>	0x2000, 0x2400, 0x2800, 0x2C00,0x3000, 0x3400, 0x3800, 0x3C00, 0x4000, 0x4400,	Some user configurations temporarily associate a locale without a permanent LCID assignment with one of these 12 transient LCIDs. This assignment is transient and it is not guaranteed; it will likely refer to the same locale for the lifetime of the process. However, this assignment will differ for other users on the

Errata Published *	Description		
		0x4800, 0x4C00	machine, or other machines, and, as such, is unsuitable for use in protocols or persisted data. This assignment is a temporary 1-to-1 relationship between an LCID and a particular locale name and will round trip until that relationship changes.

*Date format: YYYY/MM/DD

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

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

March 16, 2018 - Download

April 7, 2021 - Download

Errata below are for Protocol Document Version 45.0 2021/06/25.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/09/20</td><td>In Section 2.2.1.4, AEAD-AES-256-CBC-HMAC-SHA512 Constants
Description: Updated AEAD-AES-256-CBC-HMAC-SHA512 constants to ensure that the value details allow an implementation to be successfully created.

Changed from:
<table>
<tr><th>Constant Name</th><th>Value</th></tr>
<tr><td>versionbyte</td><td>0x01</td></tr>
<tr><td>versionbyte_length</td><td>1</td></tr>
<tr><td>SAM_AES_256_ALG</td><td>"AEAD-AES-256-CBC-HMAC-SHA512"</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING</td><td>"Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING</td><td>"Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING_LENGTH</td><td>sizeof(SAM_AES256_ENC_KEY_STRING)</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING_LENGTH</td><td>sizeof(SAM_AES256_MAC_KEY_STRING)</td></tr>
</table>
Changed to:
<table>
<tr><th>Constant Name</th><th>Meaning</th></tr>
<tr><td>Versionbyte
0x01</td><td>Version identifier</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>versionbyte_length
1</td><td>Version identifier length</td></tr>
<tr><td>SAM_AES_256_ALG
"AEAD-AES-256-CBC-HMAC-SHA512"</td><td>A NULL terminated ANSI string</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING
"Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"</td><td>A NULL terminated ANSI string</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING
"Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"</td><td>A NULL terminated ANSI string</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING_LENGTH
sizeof(SAM_AES256_ENC_KEY_STRING)
(61)</td><td>The length of SAM_AES256_ENC_KEY_STRING, including the null terminator.</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING_LENGTH
sizeof(SAM_AES256_MAC_KEY_STRING)
(54)</td><td>The length of SAM_AES256_MAC_KEY_STRING, including the null terminator</td></tr>
</table>

In Section 5.1.5 AES Cipher Usage
Description: Clarified the usage of enc_key and mac_key when encrypting the data.

Changed from:
"...
Let AuthData ::= HMAC-SHA-512(mac_key, versionbyte + IV + Cipher + versionbyte_length)"

Changed to:
"...
Let AuthData ::= HMAC-SHA-512(mac_key, versionbyte + IV + Cipher + versionbyte_length)
Note that enc_key is truncated to 32-bytes and the entire 64-byte mac_key is used."</td></tr>
<tr><td>2022/01/11</td><td>The following sections in the table below are updated or new.
Please see the PDF diff document for details.
<table>
<tr><th>Section</th><th>Description</th></tr>
<tr><td>1.3 Overview</td><td>Updated</td></tr>
<tr><td>1.6 Applicability Statement</td><td>Updated</td></tr>
<tr><td>2.2 Common Data Types</td><td>Updated</td></tr>
<tr><td>2.2.1.4 AEAD-AES-256-CBC-HMAC-SHA512 Constants</td><td>Created new section</td></tr>
<tr><td>2.2.1.5 LSA Trust Record Flags</td><td>Created new section</td></tr>
<tr><td>2.2.2.6 LSAPR_REVISION_INFO_V1</td><td>Created new section</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description	
	2.2.2.7 LSAPR_REVISION_INFO	Created new section
	2.2.7.2 TRUSTED_INFORMATION_CLASS	Updated
	2.2.7.3 LSAPR_TRUSTED_DOMAIN_INFO	Updated
	2.2.7.21 LSA_FOREST_TRUST_RECORD	Updated
	2.2.7.22 LSA_FOREST_TRUST_RECORD_TYPE	Updated
	2.2.7.30 LSAPR_TRUSTED_DOMAIN_FULL_INFORMATION_INTERNAL_AES	Created new section
	2.2.7.31 LSA_FOREST_TRUST_SCANNER_INFO	Created new section
	2.2.7.32 LSA_FOREST_TRUST_RECORD2	Created new section
	2.2.7.33 LSA_FOREST_TRUST_INFORMATION2	Created new section
	3.1.1.5 Trusted Domain Object Data Model	Updated
	3.1.4 Message Processing Events and Sequencing Rules	Updated
	3.1.4.4.9 LsarOpenPolicy3 (Opnum 130)	Created new section
	3.1.4.7.15 LsarQueryForestTrustInformation (Opnum 73)	Updated
	3.1.4.7.16 LsarSetForestTrustInformation (Opnum 74)	Updated
	3.1.4.7.17 LsarCreateTrustedDomainEx3 (Opnum 129)	Created new section
	3.1.4.7.18 LsarQueryForestTrustInformation2 (Opnum 132)	Created new section
	3.1.4.7.19 LsarSetForestTrustInformation2 (Opnum 133)	Created new section
	5.1.5 AES Cipher Usage	Created new section
	5.2 Index of Security Parameters	Updated
	6 Appendix A: Full IDL	Updated

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

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

[MS-MDE]: Mobile Device Enrollment Protocol

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-MDE2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

September 15, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

June 1, 2021 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version 12.0 - 2022/04/29.

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td>2023/06/12</td><td>In Section 2.2.10 Faults: added CustomServerError message to the detail element table with product behavior note for applicability.
Changed from:
<table>
<tr><th>Subcode</th><th>Error</th><th>Description</th><th>HRESULT</th></tr>
<tr><td>DeviceCapReached</td><td>MENROLL_E_DEVICECAPREACHED</td><td>User already enrolled in too many devices. Delete or unenroll old ones to fix this error. The user can fix it without admin help.</td><td>80180013</td></tr>
<tr><td>DeviceNotSupported</td><td>MENROLL_E_DEVICENOTSUPPORTED</td><td>Specific platform or version is not supported. There is no point retrying or</td><td>80180014</td></tr>
</table></td></tr>
</table>

Errata Published *	Description

		calling admin. User could upgrade device.	
NotSupported	MENROLL_E_NOTSUPPORTED	Mobile device management generally not supported (would save an admin call).	80180015
NotEligibleToRenew	MENROLL_E_NOTELIGIBLETORENEW	Device is trying to renew but server rejects the request. Client might show notification for this if Robo fails. Check time on device. The user can fix it by re-enrolling.	80180016
InMaintenance	MENROLL_E_INMAINTENANCE	Account is in maintenance ; retry later. The user can retry later, but they may need to contact the admin because they would not know when the problem was solved.	80180017
UserLicense	MENROLL_E_USERLICENSE	License of user is in bad state and blocking the enrollment. The user needs to call the admin.	80180018
InvalidEnrollmentData	MENROLL_E_ENROLLMENTDATAINVALID	The server rejected the enrollment	80180019

Errata Published *	Description

		data. The server may not be configured correctly.	

Changed to:

Subcode	Error	Description	HRESULT
DeviceCapReached	MENROLL_E_DEVICECAPREACHED	User already enrolled in too many devices. Delete or unenroll old ones to fix this error. The user can fix it without admin help.	80180013
DeviceNotSupported	MENROLL_E_DEVICENOTSUPPORTED	Specific platform or version is not supported. There is no point retrying or calling admin. User could upgrade device.	80180014
NotSupported	MENROLL_E_NOTSUPPORTED	Mobile device management generally not supported (would save an admin call).	80180015
NotEligibleToRenew	MENROLL_E_NOTELIGIBLETORENEW	Device is trying to renew but server rejects the request. Client might show notification for this if Robo fails. Check time on device. The user can fix it by re-enrolling.	80180016
InMaintenance	MENROLL_E_INMAINTENANCE	Account is in maintenance; retry later. The user can retry later, but they may need to contact the admin because they would not know when the problem was solved.	80180017

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>UserLicense</td><td>MENROLL_E_USERLICENSE</td><td>License of user is in bad state and blocking the enrollment. The user needs to call the admin.</td><td>80180018</td></tr>
<tr><td>InvalidEnrollmentData</td><td>MENROLL_E_ENROLLMENTDATAINVALID</td><td>The server rejected the enrollment data. The server may not be configured correctly.</td><td>80180019</td></tr>
<tr><td>CustomServerError</td><td>MENROLL_E_CUSTOMSERVERERROR</td><td>The server responded with a custom error string, see DeviceManagement-Enterprise-Diagnostics for details. In this case, s:reason/s:text would show as the server message.<14></td><td>80180032</td></tr>
</table>
<14> Section 2.2.10: The CustomServerError is applicable to Windows 10 v20H2 operating system and later and to Windows 11 operating system version 1 and later.
</td></tr>
<tr><td>2022/12/30</td><td>
<14> Section 3.1.4.1.3.1 DiscoveryRequest: Product note <14> for RequestVersion v5.0 added supported in Windows 10 v2004 (v20H1) 2023 1C patch and later.

Changed From:

RequestVersion value 5.0 is supported only in the Windows 11 (version 1) 2022 10C patch and later.

Changed To:

RequestVersion value 5.0 is supported in Windows 11 (version 1) 2022 10C patch and later and supported in Windows 10 v2004 (v20H1) 2023 1C patch and later.

In the following sections' product notes for EnrollmentVersion v5.0 added supported in Windows 10 v2004 (v20H1) 2023 1C patch and later.

<15> Section 3.1.4.1.3.2 DiscoveryResponse

<16> Section 3.3.4.1.1.2 GetPoliciesResponse

<17> Section 3.3.4.1.1.2 GetPoliciesResponse

<20> Section 3.4.4.1.1.1.1 RequestSecurityToken using Federated Authentication
</td></tr>
</table>

Errata Published *	Description
	<23> Section 3.4.4.1.1.1.2 RequestSecurityToken using Certificate Authentication <26> Section 3.4.4.1.1.1.3 RequestSecurityToken using On-Premise Authentication Changed From: The EnrollmentVersion value 5.0 is supported only in the Windows 11 (version 1), 2022 10C patch and later, see section 3.1.4.1.3.2. Changed To: The EnrollmentVersion value 5.0 is supported in Windows 11 (version 1), 2022 10C patch and later and supported in Windows 10 v2004 (v20H1) 2023 1C patch and later. See section 3.1.4.1.3.2.
2022/10/03	<14> Section 3.1.4.1.3.1 DiscoveryRequest, updated product note with RequestVersion v5.0 support from Windows 11 (version 2) to Windows 11 (version 1) 2022 10C patch and later. Changed From: RequestVersion value 5.0 is supported only in the Windows 11, version 22H2 operating system and later. Changed To: RequestVersion value 5.0 is supported only in Windows 11 (version 1), 2022 10C patch and later. In the following sections updated the product notes with EnrollmentVersion v5.0 support from Windows 11 (version 2) to Windows 11 (version 1) 2022 10C patch and later. <15> Section 3.1.4.1.3.2 DiscoveryResponse <16> Section 3.3.4.1.1.2 GetPoliciesResponse <17> Section 3.3.4.1.1.2 GetPoliciesResponse <20> Section 3.4.4.1.1.1.1 RequestSecurityToken using Federated Authentication <23> Section 3.4.4.1.1.1.2 RequestSecurityToken using Certificate Authentication <26> Section 3.4.4.1.1.1.3 RequestSecurityToken using On-Premise Authentication Changed From: EnrollmentVersion value 5.0 is supported only in Windows 11 v22H2 and later, see section 3.1.4.1.3.2. Changed To: EnrollmentVersion value 5.0 is supported only in Windows 11 (version 1), 2022 10C patch and later, see section 3.1.4.1.3.2.

[MS-MDM]: Mobile Device Management Protocol

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

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

RSS

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

April 7, 2021 - Download

Errata below are for Protocol Document Version 14.0 - 2022/04/29

Errata Published*	Description
2023/03/06	In section 3.2.5.1 Windows Azure Virtual Desktop for Multi-users' User Setting Configuration, updated product note that support for user sessions multi-session Edition only in Windows Virtual Desktop was backported to Windows 10. Changed from: Windows Azure Virtual Desktop (AVD) supports multiple users that can log on simultaneously.<16> <16> Section 3.2.5.1: Servicing May 2022, support for user sessions on Windows 11, version 22H2 operating system (version 2) multi-session Edition only in Windows Virtual Desktop was backported to Windows 11 (version 1). Changed to: Windows Azure Virtual Desktop (AVD) supports multiple users that can log on simultaneously.<16> <16> Section 3.2.5.1: Servicing May 2022, support for user sessions on Windows 11, version 22H2 operating system (version 2) multi-session Edition only in Windows Virtual Desktop was backported to Windows 11 (version 1). Servicing March 2023, the previous servicing update was backported to Windows 10 v2004 (v20H1) and later.
2022/06/14	In section 2.1 Transport: Added Note 9 to indicate client behavior when the ForceAadToken in the DMClient configuration service provider is set by the server. Changed from: . . .

Errata Published*	Description
	Note 8: If the server has set EntDMID in the DMClient configuration service provider, the client adds client-request-id to the header and sets it to the value of EntDMID.<9> See [MSDOCS-DMClient-CSP] for more information. Changed to: . . . Note 8: If the server has set EntDMID in the DMClient configuration service provider, the client adds client-request-id to the header and sets it to the value of EntDMID.<9> See [MSDOCS-DMClient-CSP] for more information. Note 9: If the server has set ForceAadToken in the DMClient configuration service provider, and the device is joined to an Azure Active Domain (AAD), the client adds a custom header that contains the AAD token. The header is in the following format. DeviceToken: CI6MTQxmCF5xgu6yYcmV9ng6vhQfaJYw… See [MSDOCS-DMClient-CSP] for more information.<10> Appendix B: <10> Section 2.1: Not available in Windows 10 v19H2 and earlier.
2022/05/02	3.2.5.1 Windows Azure Virtual Desktop for Multi-users' User Setting Configuration, added a product note that the added support for user sessions multi-session Edition only in WVD was backported. Changed from: Windows Azure Virtual Desktop (AVD) supports multiple users that can log on simultaneously. To allow configuration of user settings, the MDM server must support "multi-user AVD" mode… Changed to: Windows Azure Virtual Desktop (AVD) supports multiple users that can log on simultaneously.<15> To allow configuration of user settings, the MDM server must support "multi-user AVD" mode… <15> Section 3.2.5.1: Servicing May 2022, support for user sessions on Windows 11, version 22H2 operating system (version 2) multi-session Edition only in Windows Virtual Desktop was backported to Windows 11 (version 1).

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

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

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

RSS

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

September 12, 2018 - Download

[MS-MSSOD]: Media Streaming Server Protocols Overview

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-MWBE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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 Errata found in [MS-MWBF] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

July 18, 2016 - Download

June 1, 2017 - Download

September 12, 2018 - Download

[MS-NBTE]: NetBIOS over TCP (NetBT) Extensions

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

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

RSS

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

April 29, 2022 – Download

[MS-NCNBI]: Network Controller Northbound Interface Specification

This topic lists Errata found in [MS-NCNBI] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.
Errata are subject to the same terms as the Open Specifications documentation referenced.

RSS

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

March 16, 2018 - Download

September 12, 2018 - Download

April 7, 2021 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V9.0 – 2022/04/29.

Errata Published*	Description
2023/01/30	Section 1.7 Versioning and Capability Negotiation, added version v4.2. Updated product note 2 version table with V4.2, idleTimeoutInMinutes, and Windows Server 2022 Patch February 2023. Section 3.1.5.5.4 inboundNatRules, updated product note 8 Support for the enableTcpReset property backport to Windows Server 2019 with HCI. Section 3.1.5.5.5 loadBalancingRules, updated product note 9 Support for the enableTcpReset property backport to Windows Server 2019 HCI and later and Windows Server 2022 and later. Section 3.1.5.5.4 inboundNatRules, updated product note 8 Support for the enableTcpReset property backport to Windows Server 2019 with HCI. Section 3.1.5.5.5 loadBalancingRules, updated product note 9 Support for the enableTcpReset property backport to Windows Server 2019 HCI and later and Windows Server 2022 and later. Section 3.1.5.5.6 outboundNatRules, added property idleTimeoutInMinutes with version v4.2. Updated product note backport to Windows Server 2019 with HCI. Section 3.1.5.11 networkInterfaces, Updated QosSettings , enableHardwareLimits support from version v4 to version v3.1. Section 3.1.5.26 virtualSwitchManager, added enableHardwareLimits version support statement with v3.1. Section 6.5.6.1 PUT schema Section 6.5.6.2 GET schema Section 6.5.6.3 GET ALL schema

Errata Published*	Description
	Section 6.5.7.1 PUT schema Section 6.5.7.2 GET schema Section 6.5.7.3 GET ALL schema Added enableTcpReset property. Section 6.5.8.1 PUT schema Section 6.5.8.2 GET schema Section 6.5.8.3 GET ALL schema Added enableTcpReset and idleTimeoutInMinutes properties.

[MS-NCT]: Network Cost Transfer Protocol

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-NFPB] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-NFPS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-NKPU] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-NLMP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

RSS

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

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

September 23, 2019 - Download

September 29, 2020 – Download

Errata below are for Protocol Document Version V35.0 – 2022/04/29.

Errata Published*	Description
2022/07/26	In section 2.2.1.2 CHALLENGE_MESSAGE: Added statement that the server MUST return the NTLMSSP_NEGOTIATE_SIGN if set by the client. Changed from: NegotiateFlags (4 bytes): A NEGOTIATE structure that contains a set of flags, as defined by section 2.2.2.5. The server sets flags to indicate options it supports or, if there has been a NEGOTIATE_MESSAGE (section 2.2.1.1), the choices it has made from the options offered by the client. Changed to: NegotiateFlags (4 bytes): A NEGOTIATE structure that contains a set of flags, as defined by section 2.2.2.5. The server sets flags to indicate options it supports or, if there has been a NEGOTIATE_MESSAGE (section 2.2.1.1), the choices it has made from the options offered by the client. If the client has set the NTLMSSP_NEGOTIATE_SIGN in the NEGOTIATE_MESSAGE the Server MUST return it.

Date format: YYYY/MM/DD

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-NNS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

June 1, 2017 - Download

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

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

*Date format: YYYY/MM/DD

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

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

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

RSS

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

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

*Date format: YYYY/MM/DD

[MS-NRPC]: Netlogon Remote Protocol

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

September 23, 2019 - Download

August 24, 2020 – Download

April 7, 2021 - Download

June 24, 2021 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V40.0 2022/04/29.

Errata Published*	Description
2022/11/08	In section 3.1.1 Abstract Data Model: SealSecureChannel removed duplicate and adjusted to the encryption setting MUST be TRUE. Removed statement with note <69> about storing and retrieving the SealSecureChannel variable. Changed from: TrustPasswordVersion: ... SealSecureChannel: ... StrongKeySupport: ... The Netlogon client and server variables are as follows: LocatedDCsCache: ... SealSecureChannel: A Boolean setting that indicates whether the RPC message has to be encrypted or just integrity-protected ([C706] section 13.2.5). When TRUE, the message will be encrypted; otherwise, it will be integrity-protected. Implementations SHOULD<69> persistently store and retrieve the SealSecureChannel variable. VulnerableChannelAllowList: A setting expressed in Security Descriptor Definition Language (SDDL) ([MS-DTYP] section 2.5.1) of Netlogon client allowed to not use secure bindings, see section 3.1.4.6.<70>

Errata Published*	Description
	Changed to: TrustPasswordVersion: ... StrongKeySupport: ... The Netlogon client and server variables are as follows: LocatedDCsCache: ... SealSecureChannel: A Boolean setting that indicates whether the RPC message has to be encrypted or just integrity-protected ([C706] section 13.2.5). This setting MUST be TRUE. VulnerableChannelAllowList: A setting expressed in Security Descriptor Definition Language (SDDL) ([MS-DTYP] section 2.5.1) of Netlogon client allowed to not use secure bindings, see section 3.1.4.6.<69> In section 3.1.4.6 Calling Methods Requiring Session-Key Establishment: Step 1: Replaced if…TRUE... with: Clients MUST request the Privacy authentication level. Step 4: Added RPC Integrity to the MUST deny request list. Updated product note. Changed from: The client and server follow this sequence of steps.<75> 1. The client SHOULD<76> bind to the RPC server using TCP/IP. The client and server MUST utilize a secure bind. If a secure bind is used, the client instructs the RPC runtime to use the Netlogon SSP ([MS-RPCE] section 2.2.1.1.7) for privacy/integrity of the RPC messages. If the SealSecureChannel setting is TRUE, the client requests the Privacy authentication level from the RPC runtime. If the SealSecureChannel setting is FALSE, then the authentication level requested is Integrity. 2. … 3. … 4. If secure bind is not used, the server MUST deny the request unless client is in the VulnerableChannelAllowList setting.<77> <75> Section 3.1.4.6: Windows XP and later clients will request secure RPC. Windows Server 2008 R2 operating system and later will enforce that clients are using RPC Integrity and Confidentiality to secure the connection. For more information, see [MSFT-CVE-2020-1472]. Changed to: The client and server follow this sequence of steps.<74> 1. The client SHOULD<75> bind to the RPC server using TCP/IP. The client and server MUST utilize a secure bind. If a secure bind is used, the client instructs the RPC runtime to use the Netlogon SSP ([MS-RPCE] section 2.2.1.1.7) for privacy/integrity of the RPC messages. Clients MUST request the Privacy authentication level. 2. …

Errata Published*	Description
	3. … 4. If secure bind is not used or the client is using RPC Integrity instead of RPC Privacy, the server MUST deny the request unless client is in the VulnerableChannelAllowList setting.<76> <74> Section 3.1.4.6: Windows XP and later clients will request secure RPC. Windows Server 2008 and later will enforce that clients are using RPC Confidentiality to secure the connection. For more information, see [MSFT-CVE-2020-1472] and [MSFT-CVE-2022-38023]. In section 3.4.1 Abstract Data Model: RequireSignOrSeal: Added that this setting MUST be TRUE. Changed from: RequireSignOrSeal: Indicates whether the client SHOULD<87> continue session-key negotiation when the server did not specify support for Secure RPC as described in the negotiable option Y of section 3.1.4.2. Changed to: RequireSignOrSeal: Indicates whether the client SHOULD<87> continue session-key negotiation when the server did not specify support for Secure RPC as described in the negotiable option Y of section 3.1.4.2. This setting MUST be TRUE. In section 3.4.3 Initialization: Changed RequireSignOrSeal from SHOULD to MUST be initialized to TRUE. Changed from: RequireSignOrSeal SHOULD<92> be initialized to TRUE. Changed to: RequireSignOrSeal MUST<92> be initialized to TRUE. In section 3.5.1 Abstract Data Model: SignSecureChannel: Added This setting is deprecated, as SealSecureChannel MUST be TRUE. Changed from: SignSecureChannel: A Boolean variable that determines whether a domain member attempts to negotiate signing for all secure channel traffic that it initiates. Changed to: SignSecureChannel: A Boolean variable that determines whether a domain member attempts to negotiate signing for all secure channel traffic that it initiates. This setting is deprecated, as SealSecureChannel MUST be TRUE.

Errata Published*	Description
	In Section 3.5.3 Initialization: RejectMD5Clients, SealSecureChannel, and SignSecureChannel set to TRUE. Changed from: RejectMD5Clients SHOULD be initialized in an implementation-specific way and set to FALSE. SealSecureChannel SHOULD be TRUE. SignSecureChannel SHOULD be initialized in an implementation-specific way and set to TRUE. Any changes made to the SignSecureChannel registry keys are reflected in the ADM elements when a PolicyChange event is received (section 3.1.6). Changed to: RejectMD5Clients SHOULD be initialized in an implementation-specific way and set to TRUE. SealSecureChannel MUST be TRUE. SignSecureChannel SHOULD be initialized in an implementation-specific way and set to TRUE. Any changes made to the SignSecureChannel registry keys are reflected in the ADM elements when a PolicyChange event is received (section 3.1.6). This setting is deprecated, as SealSecureChannel MUST be true.
2022/09/20	In section 1.3.1 Pass-Through Authentication: Added little endian usage statement. Changed from: … The secure channel is achieved by encrypting the communication traffic with a session key computed using a secret key (called a server's machine account password) shared by the server and the DC. Changed to: … The secure channel is achieved by encrypting the communication traffic with a session key computed using a secret key (called a server's machine account password) shared by the server and the DC. Unless otherwise specified, MS-NRPC uses little endian for byte ordering before encryption. In section 2.2.1.3.7 NL_TRUST_PASSWORD: Added product note about little endian usage for big endian users. Changed from: . . . The NL_TRUST_PASSWORD structure is encrypted using the negotiated encryption algorithm before it is sent over the wire. Changed to: . . . The NL_TRUST_PASSWORD structure is encrypted using the negotiated encryption algorithm before it is sent over the wire.<24> <24> Section 2.2.1.3.7: Windows domain controller expects little-endian byte ordering for the encryption input. If your processor is in big endian, then both the wide-character buffer and length fields in the NL_TRUST_PASSWORD structure MUST be converted to little endian before encryption. After encryption, byte swapping to reverse the order will be needed. In section 3.4.5.2.5 Calling NetrServerPasswordSet2: Added product note about little endian usage for big endian users. Changed from: Encrypt the ClearNewPassword parameter using the negotiated encryption algorithm (determined by bits C, O, or W, respectively, in the NegotiateFlags member of the

Errata Published*	Description
	ServerSessionInfo table entry for PrimaryName) and the session key established as the encryption key. Changed to: Encrypt <98> the ClearNewPassword parameter using the negotiated encryption algorithm (determined by bits C, O, or W, respectively, in the NegotiateFlags member of the ServerSessionInfo table entry for PrimaryName) and the session key established as the encryption key. <98> Section 3.4.5.2.5: Windows domain controller expects little-endian byte ordering for the encryption input. If your processor is in big endian, then both the wide-character buffer and length fields in the NL_TRUST_PASSWORD structure MUST be converted to little endian before encryption. After encryption, byte swapping to reverse the order will be needed. In section 3.5.4.4.5 NetrServerPasswordSet2 (Opnum 30): Added product note about little endian usage for big endian users. Changed from: ClearNewPassword: A pointer to an NL_TRUST_PASSWORD structure, as specified in section 2.2.1.3.7, that contains the new password encrypted as specified in Calling NetrServerPasswordSet2 (section 3.4.5.2.5). Changed to: ClearNewPassword: A pointer to an NL_TRUST_PASSWORD structure, as specified in section 2.2.1.3.7, that contains the new password encrypted<178> as specified in Calling NetrServerPasswordSet2 (section 3.4.5.2.5). <178> Section 3.5.4.4.5: Windows domain controller expects little-endian byte ordering for the encryption input. If your processor is in big endian, then both the wide-character buffer and length fields in the NL_TRUST_PASSWORD structure MUST be converted to little endian before encryption. After encryption, byte swapping to reverse the order will be needed.

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-OAPX] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

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

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

RSS

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

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

July 18, 2016 - Download

September 26, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

October 6, 2021 - Download

[MS-OCSPA]: Microsoft OCSP Administration Protocol

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

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

RSS

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

April 7, 2021 - Download

[MS-OIDCE]: OpenID Connect 1.0 Protocol Extensions

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

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

RSS

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

June 1, 2017 - Download

December 1, 2017 - Download

March 16, 2018 - Download

October 6, 2021 - Download

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

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

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

RSS

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

December 1, 2017 - Download

September 12, 2018 - Download

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

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

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

RSS

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

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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-PAC]: Privilege Attribute Certificate Data Structure

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

RSS

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:

November 23, 2020 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V23.0 – 2022/04/29.

Errata Published*	Description
2023/04/10	Section 2.4 PAC_INFO_BUFFER Updated product applicability to only Windows Server for the ticket checksum (0x10) security update. Added CVE references and product applicability for the Extended KDC checksum (0x13) security update. Changed from: 0x00000010 Ticket checksum (section 2.8). PAC structures MUST contain one buffer of this type for Kerberos ticket-granting service (TGS) requests, and none otherwise. Additional ticket checksum buffers MUST be ignored.<7> 0x00000013 Extended KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type for Kerberos ticket-granting service (TGS) requests, and none otherwise. Additional Extended KDC checksum buffers MUST be ignored. <7> Section 2.4: For more information about the ticket signature, see Kerberos Security Feature Bypass Vulnerability security update November 2020 [MSFT-CVE-2020-17049]. This update applies to Windows 8 and later and to Windows Server 2012 and later. Changed to: 0x00000010 (16) Ticket checksum (section 2.8). PAC structures MUST contain one buffer of this type for Kerberos ticket-granting service (TGS) requests, and none otherwise. Additional ticket checksum buffers MUST be ignored.<7> 0x00000013 (19) Extended KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type for Kerberos ticket-granting service (TGS) requests, and none otherwise. Additional Extended KDC checksum buffers MUST be ignored.<10> <7> Section 2.4: For more information about the ticket signature, see Kerberos Security Feature Bypass Vulnerability security update November 2020 [MSFT-CVE-2020-17049]. This update applies to Windows Server 2008 SP2 and later. <10> Section 2.4: For more information about the Extended KDC checksum usage see section 2.8.4. See also Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability security update, November 2022 [MSFT-CVE-2022-37966] and Windows Kerberos Elevation

Errata Published*	Description
	of Privilege Vulnerability security update November 2022 [MSFT-CVE-2022-37967]. These updates apply to Windows Server 2008 SP2 and later. Section 2.8.3 Ticket Signature Updated product applicability to only Windows Server for the ticket signature security update. Changed from: The ticket signature<19> is generated by the issuing KDC and depends on the cryptographic algorithms available to the KDC. <19> Section 2.8.3: For more information about the ticket signature, see Kerberos Security Feature Bypass Vulnerability security update November 2020 [MSFT-CVE-2020-17049]. This update applies to Windows 8 and later and to Windows Server 2012 and later. Changed to: The ticket signature<19> is generated by the issuing KDC and depends on the cryptographic algorithms available to the KDC. <20> Section 2.8.3: For more information about the ticket signature, see Kerberos Security Feature Bypass Vulnerability security update November 2020 [MSFT-CVE-2020-17049]. This update applies to Windows Server 2008 SP2 and later. Section 2.8.4 Extended KDC Signature Added CVE references and product applicability for the Extended KDC Signature security update. Changed from: The extended KDC signature is generated by the issuing KDC and depends on the cryptographic algorithms available to the KDC. Changed to: The extended KDC signature<21> is generated by the issuing KDC and depends on the cryptographic algorithms available to the KDC. <21> Section 2.8.4: For more information about the Extended KDC Signature, see Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability security update November 2022 [MSFT-CVE-2022-37966] and Windows Kerberos Elevation of Privilege Vulnerability security update November 2022 [MSFT-CVE-2022-37967]. These updates apply to Windows Server 2008 SP2 and later.
2023/02/27	Section 2.4 PAC_INFO_BUFFER, in the ulType table clarified 4 checksums for Kerberos ticket-granting service (TGS) requests or Kerberos application protocol (AP) requests. Changed from: . . . 0x00000006 Server checksum (section 2.8). PAC structures MUST contain one buffer of this type. Additional logon server checksum buffers MUST be ignored.

Errata Published*	Description
	. . . 0x00000007 KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type. Additional KDC checksum buffers MUST be ignored. . . . 0x00000010 Ticket checksum (section 2.8). PAC structures SHOULD NOT contain more than one buffer of this type. Additional ticket checksum buffers MUST be ignored.<7> . . . 0x00000013 Extended KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type. Additional KDC checksum buffers MUST be ignored. Changed to: . . . 0x00000006 Server checksum (section 2.8). PAC structures MUST contain one buffer of this type for Kerberos ticket-granting service (TGS) requests or Kerberos application protocol (AP) requests, and none otherwise. Additional logon server checksum buffers MUST be ignored. 0x00000007 KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type for Kerberos ticket-granting service (TGS) requests or Kerberos application protocol (AP) requests, and none otherwise. Additional KDC checksum buffers MUST be ignored. . . . 0x00000010 Ticket checksum (section 2.8). PAC structures MUST contain one buffer of this type for Kerberos ticket-granting service (TGS) requests, and none otherwise. Additional ticket checksum buffers MUST be ignored.<7> . . . 0x00000013 Extended KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type for Kerberos ticket-granting service (TGS) requests, and none otherwise. Additional Extended KDC checksum buffers MUST be ignored.
2023/02/27	In section 2.4 PAC_INFO_BUFFER, added to ulType: …Types that are not understood MUST be ignored. Changed from: ulType (4 bytes): A 32-bit unsigned integer in little-endian format that describes the type of data present in the buffer contained at Offset. Changed to: ulType (4 bytes): A 32-bit unsigned integer in little-endian format that describes the type of data present in the buffer contained at Offset. Types that are not understood MUST be ignored.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/12/12</td><td>
The following sections were changed. Please see the diff document for the details.
In section 2.4 PAC_INFO_BUFFER: Added new required ulType 0x00000013 for Extended KDC (privilege server) checksum buffer.
Changed from:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>. . .</td><td></td></tr>
<tr><td>0x00000012</td><td>PAC Requestor indicates that the buffer contains the SID of principal that requested the PAC (section 2.15). PAC structures MUST contain one buffer of this type.<9></td></tr>
</table>
Changed to:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>. . .</td><td></td></tr>
<tr><td>0x00000012</td><td>PAC Requestor indicates that the buffer contains the SID of principal that requested the PAC (section 2.15). PAC structures MUST contain one buffer of this type.<9></td></tr>
<tr><td>0x00000013</td><td>Extended KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type. Additional KDC checksum buffers MUST be ignored.</td></tr>
</table>
In section 2.8.1 Server Signature: Added that the server signature MUST be generated AFTER the extended KDC signature.
Changed from:
… The resulting hash value is then placed in the Signature field of the server's PAC_SIGNATURE_DATA structure.

Changed to:
… The resulting hash value is then placed in the Signature field of the server's PAC_SIGNATURE_DATA structure.
The server signature MUST be generated AFTER the extended KDC signature (section 2.3.4).

Section 2.8.3 Ticket Signature: Added the extended KDC signature in the recompute list.
Changed from:
… the KDC SHOULD verify the integrity of the existing ticket signature and then recompute the ticket signature, server signature, and KDC signature in the PAC.
Changed to:
… the KDC SHOULD verify the integrity of the existing ticket signature and then recompute the ticket signature, server signature, KDC signature, and extended KDC signature in the PAC.

Section 2.8.4 Extended KDC Signature: Added new section.
Describes its usage and contents. It is used to detect tampering of PACs by parties other than the KDC. Describes where to use it in tickets for various accounts. Contains the ulType 0x00000013 same as described in section 2.4 PAC_INFO_BUFFER. Contains the SignatureType and its key. It is comprised of keyed hash of the entire PAC message with all
</td></tr>
</table>

Errata Published*	Description
	other Signature fields of all other PAC_SIGNATURE_DATA structures set to zero. It is placed in the Signature field of the extended KDC's PAC_SIGNATURE_DATA structure (section 2.8).

[MS-PAR]: Print System Asynchronous Remote Protocol

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-PKAP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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-PKCA]: Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol

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

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

RSS

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

October 6, 2021 - Download

Errata below are for Protocol Document Version V15.0 – 2021/10/06.

Errata Published*	Description
2022/05/10	Section 3.1.5.2.1.5 Mapping Strength: added section. The KDC SHOULD<22> map a certificate to a user using one of the following mappings. These methods of mapping a certificate to a user are classified as strong or weak based on whether they depend on a name as a secure identifier. The following mappings are considered weak: • SAN UPNName • SAN DNSName • altSecurityIdentities Issuer Name and Subject Name • altSecurityIdentities Subject Name • altSecurityIdentities 822 field The following mappings are considered strong: • SID (section 3.1.5.2.1.6) • Key Trust (section 3.1.5.2.1.4) • altSecurityIdentities Issuer and Serial Number • altSecurityIdentities Subject Key Identifier • altSecurityIdentities SHA1 Hash of Public Key If a KDC maps a certificate to a user using one of the above weak mappings, it SHOULD<23> continue to search for more mappings until it encounters a strong mapping. If it does not find such a mapping, it MAY fail the authentication request with KDC_ERR_CERTIFICATE_MISMATCH.

Errata Published*	Description
	<22> Section 3.1.5.2.1.5 Certificate mapping strength is applicable to Windows Server 2008 R2 and later. <23> Section 3.1.5.2.1.5 Certificate mapping strength is applicable to Windows Server 2008 R2 and later. Section 3.1.5.2.1.6 SID: added section. If a KDC has exhausted all other mapping types for a certificate and found a weak mapping without finding a strong mapping, it SHOULD<24> check if the certificate contains a security identifier (SID). If it does and the SID matches the user the certificate weakly mapped to, the certificate is to be considered strongly mapped. If the SID does not match, the authentication MUST fail with KDC_ERR_CERTIFICATE_MISMATCH. If the certificate does not contain a SID, the KDC MAY fail the authentication request as no strong mapping is available. For more details on the objectSID in an issued certificate see [MS-WCCE] and section 2.2.2.7.7.4. <24> Section 3.1.5.2.1.6 Certificate SID mapping is applicable to Windows Server 2008 R2 and later.

*Date format: YYYY/MM/DD

[MS-PSRDP]: PowerShell Remote Debugging Protocol

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-PSRP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RA] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RAI] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

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

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

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

RSS

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

September 12, 2018 - Download

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

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

March 20, 2017 - Download

June 1, 2017 - Download

December 1, 2017 - Download

March 16, 2018 - Download

September 12, 2018 - Download

March 13, 2019 - Download

September 23, 2019 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

Errata below are for Protocol Document Version V55.0 – 2021/06/25.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/01/04</td><td>In section 2.2.1.3.2, Client Core Data (TS_UD_CS_CORE), added the client version number for RDP 10.10:

Changed from:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00080001</td><td>RDP 4.0 clients</td></tr>
<tr><td>0x00080004</td><td>RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 clients</td></tr>
<tr><td>0x00080005</td><td>RDP 10.0 clients</td></tr>
<tr><td>0x00080006</td><td>RDP 10.1 clients</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description

0x00080007	RDP 10.2 clients
0x00080008	RDP 10.3 clients
0x00080009	RDP 10.4 clients
0x0008000A	RDP 10.5 clients
0x0008000B	RDP 10.6 clients
0x0008000C	RDP 10.7 clients
0x0008000D	RDP 10.8 clients
0x0008000E	RDP 10.9 clients

Changed to:

Value	Meaning
0x00080001	RDP 4.0 clients
0x00080004	RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 clients
0x00080005	RDP 10.0 clients
0x00080006	RDP 10.1 clients
0x00080007	RDP 10.2 clients
0x00080008	RDP 10.3 clients
0x00080009	RDP 10.4 clients
0x0008000A	RDP 10.5 clients
0x0008000B	RDP 10.6 clients
0x0008000C	RDP 10.7 clients
0x0008000D	RDP 10.8 clients
0x0008000E	RDP 10.9 clients
0x0008000F	RDP 10.10 clients

In section 2.2.1.4.2, Server Core Data (TS_UD_SC_CORE), added the server version number for RDP 10.10:

Changed from:

Value	Meaning
0x00080001	RDP 4.0 servers
0x00080004	RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 servers

Errata Published*	Description
	0x00080005 | RDP 10.0 servers 0x00080006 | RDP 10.1 servers 0x00080007 | RDP 10.2 servers 0x00080008 | RDP 10.3 servers 0x00080009 | RDP 10.4 servers 0x0008000A | RDP 10.5 servers 0x0008000B | RDP 10.6 servers 0x0008000C | RDP 10.7 servers 0x0008000D | RDP 10.8 servers 0x0008000E | RDP 10.9 servers Changed to: Value | Meaning 0x00080001 | RDP 4.0 servers 0x00080004 | RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 servers 0x00080005 | RDP 10.0 servers 0x00080006 | RDP 10.1 servers 0x00080007 | RDP 10.2 servers 0x00080008 | RDP 10.3 servers 0x00080009 | RDP 10.4 servers 0x0008000A | RDP 10.5 servers 0x0008000B | RDP 10.6 servers 0x0008000C | RDP 10.7 servers 0x0008000D | RDP 10.8 servers 0x0008000E | RDP 10.9 servers 0x0008000F | RDP 10.10 servers

*Date format: YYYY/MM/DD

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RDPEAR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

RSS

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:

September 15, 2017 - Download

September 29, 2020 – Download

Errata below are for Protocol Document Version V7.0 – 2021/06/25.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2023/05/16</td><td>Section 2.2.1.2.1 KERB_ASN1_DATA: Updated PDU numeric values. Added product note for RS1 values.
Changed from:
Pdu: A ULONG ([MS-DTYP] section 2.2.51) that contains the protocol data unit (PDU) that is used to decode the data. MUST be one of the values in the following table.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>62</td><td>The encrypted data contains a KRB_AS_REP message.</td></tr>
<tr><td>63</td><td>The encrypted data contains a KRB_TGS_REP message.</td></tr>
</table>
Changed to:
Pdu: A ULONG ([MS-DTYP] section 2.2.51) that contains the protocol data unit (PDU) that is used to decode the data. MUST be one of the values in the following table.<1>
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>70</td><td>The encrypted data contains a KRB_AS_REP message.</td></tr>
<tr><td>71</td><td>The encrypted data contains a KRB_TGS_REP message.</td></tr>
</table>
<1> Section 2.2.1.2.1: Only in Windows 10 v1607 operating system and Windows Server 2016 the values are 69 for KRB_AS_REP and 70 for KRB_TGS_REP messages.</td></tr>
<tr><td>2021/09/07</td><td>In Section 2.2 Message Syntax, changed data types in TSRemoteGuardInnerPacket.

Changed from:

<pre>
TSRemoteGuardInnerPacket ::= SEQUENCE {
        version   [0] TSRemoteGuardVersion DEFAULT tsremoteguardv1,
        packageName   [1] OCTETSTRINGNOCOPY,
        buffer   [2] OCTETSTRINGNOCOPY,
        extension   [3] ANYNOCOPY OPTIONAL,   -- future extension
point
        ...
</pre></td></tr>
</table>

Errata Published*	Description

	}
	
	Changed to:
	
	TSRemoteGuardInnerPacket ::= SEQUENCE {
	version [0] TSRemoteGuardVersion DEFAULT tsremoteguardv1,
	packageName [1] OCTET STRING,
	buffer [2] OCTET STRING,
	extension [3] ANY OPTIONAL, -- X.680 open type for future extension point
	...
	}

*Date format: YYYY/MM/DD

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

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

September 12, 2018 - Download

Errata below are for Protocol Document Version V15.0 – 2021/06/25.

Errata Published*	Description
2022/09/03	In Section 4.4.3.1, Requesting the Size of a File, revised example: Changed from: The following is an annotated dump of a File Contents Request PDU (section 2.2.5.3). 00000000 08 00 00 00 18 00 00 00 02 00 00 00 01 00 00 00 .... 00000010 01 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 .... 00000020 00 00 00 00 00 00 00 00 .... Changed to: The following is an annotated dump of a File Contents Request PDU (section 2.2.5.3). 00000000 08 00 00 00 18 00 00 00 02 00 00 00 01 00 00 00 .... 00000010 01 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 .... In Section 4.4.3.2, Requesting the Contents of a File, revised example: Changed from: The following is an annotated dump of a File Contents Request PDU (section 2.2.5.3). 00000000 08 00 00 00 18 00 00 00 02 00 00 00 01 00 00 00 ....

Errata Published*	Description
	00000010 02 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 ..... 00000020 00 00 00 00 00 00 00 00 .... Changed to: The following is an annotated dump of a File Contents Request PDU (section 2.2.5.3). 00000000 08 00 00 00 18 00 00 00 02 00 00 00 01 00 00 00 ..... 00000010 02 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 .....

*Date format: YYYY/MM/DD

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

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

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

RSS

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

April 7, 2021 - Download

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

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

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

RSS

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

April 7, 2021 - Download

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

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RDPEGDI] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RDPEGFX] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

March 20, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

August 24, 2020 – Download

April 7, 2021 - Download

April 29, 2022 - Download

Errata Published*	Description
2023/06/27	In MS-RDPEGFX, updated formulas and labels in sections 2.2.4.5, 2.2.4.6, 3.3.8.3.2, and 3.3.8.3.3. See the diff doc for details of the changes.

*Date format: YYYY/MM/DD

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RDPEI] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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-RDPELE]: Remote Desktop Protocol: Licensing Extension

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

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

RSS

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

September 12, 2018 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

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

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

RSS

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

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

July 18, 2016 - Download

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

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RDPERP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

September 12, 2018 - Download

September 23, 2019 - Download

March 4, 2020 - Download

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RDPESP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RDPEUDP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

March 2, 2016 - Download

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

September 23, 2019 - Download

August 24, 2020 – Download

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

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

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

RSS

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

March 13, 2019 - Download

September 23, 2019 - Download

June 24, 2021 - Download

Errata below are for Protocol Document Version V5.0 – 2021/06/25.

Errata Published*	Description
2021/08/17	In Section 3.1.5.2, DelayAckInfo Payload, changed case of a field name: Changed from: maxDelayedAcks Changed to: MaxDelayedAcks In Section 3.1.5.7, Acknowledgement Vector Payload, revised a field name: Changed from: AckVecSize Changed to: codedAckVecSize
2021/08/17	In Section 2.2.1.2.2, OverheadSize Payload, revised the value of OVERHEADSIZE. Changed from: OVERHEADSIZE (0x10) Changed to: OVERHEADSIZE (0x040)

Errata Published*	Description
	In Section 2.2.1.2.3, DelayAckInfo Payload, revised the value of DELAYACKINFO. Changed from: DELAYACKINFO (0x20) Changed to: DELAYACKINFO (0x100) In Section 2.2.1.2.4, AckOfAcks Payload, revised the value of AOA. Changed from: AOA (0x08) Changed to: AOA (0x010) In Section 2.2.1.2.5, DataHeader Payload, revised the value of DATA. Changed from: DATA (0x02) Changed to: DATA (0x004) In Section 2.2.1.2.6, Acknowledgement Vector Payload, revised the value of ACKVEC. Changed from: ACKVEC (0x04) Changed to: ACKVEC (0x008) In Section 2.2.1.2.7, DataBody Payload, revised the value of DATA. Changed from: DATA (0x02)

Errata Published*	Description
	Changed to: DATA (0x004)

*Date format: YYYY/MM/DD

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RDPEVOR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RDPEXPS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RDPRFX] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

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

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

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

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

April 7, 2021 - Download

[MS-RMSOD]: Rights Management Services Protocols Overview

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

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

RSS

No errata are available for the latest version of 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-RNAS]: Vendor-Specific RADIUS Attributes for Network Policy and Access Server (NPAS) Data Structure

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

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

RSS

Errata below are for Protocol Document Version V5.0 – 2021/06/25.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2022/02/08</td><td>In section 2.2.1.11 MS-Azure-Policy-ID, added new section

Changed from:

Changed to:

The MS-Azure-Policy-ID is a VSA, as specified in section 2.2.1. It is used by the Radius Server to send an identifier which is used by Azure Point to Site VPN Server to match an authenticated RADIUS user Policy configured on the Azure side. This Policy is used to select IP/ Routing configuration (assigned IP address) for the user. The fields of MS-Azure-Policy-ID MUST be set as follows:

Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x41.

Vendor-Length: An 8-bit unsigned integer that MUST be set to the length of the octet string in the Attribute-Specific Value plus 2.

Attribute-Specific Value: An octet string containing the Policy ID configured on the Azure Point to Site VPN Server.

In section 3.1.5.2 Microsoft VSA Support of RADIUS Messages, added MS-Azure-Policy-ID VSA to table.

Changed from:

<table>
<tr><th>Microsoft vendor-specific attribute</th><th>Request</th><th>Accept</th><th>Reject</th><th>Challenge</th><th>Accounting-Request</th></tr>
<tr><td>. . .</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>MS-RDG-Device-Redirection</td><td>0</td><td>0-1</td><td>0</td><td>0</td><td>0</td></tr>
</table>

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

Errata Published*	Description

Microsoft vendor-specific attribute	Request	Accept	Reject	Challenge	Accounting-Request
. . .					
MS-RDG-Device-Redirection	0	0-1	0	0	0
MS-Azure-Policy-ID	0	0-1	0	0	0

In section 3.3.5.2.3 MS-Azure-Policy-ID, added new section

Changed from:

Changed to:

This attribute is consumed only by the Microsoft Azure Point to Site VPN Server.

When a Microsoft Azure Point to Site VPN Server receives this attribute in an Access-Accept message, it applies the IP/ Routing configuration set against Policy-id received for that user.

A NAS that is not a Microsoft Azure Point to Site VPN Server ignores this attribute.
For more details about this attribute, see section 2.2.1.11.

*Date format: YYYY/MM/DD

[MS-RPCE]: Remote Procedure Call Protocol Extensions

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RPRN] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

August 24, 2020 – Download

April 7, 2021 - Download

October 6, 2021 - Download

April 29, 2022 - Download

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

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

[MS-RRP]: Windows Remote Registry Protocol

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

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

RSS

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

September 12, 2018 - Download

March 4, 2020 - Download

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-RSVD] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

April 29, 2022 - Download

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

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

June 1, 2017 - Download

September 15, 2017 - Download

September 12, 2018 - Download

April 7, 2021 - Download

October 6, 2021 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V45.0- 2022/04/29.

Errata Published*	Description
2023/02/27	In Section 1.3.2 Method-Based Perspective Description: Added description of new method 'SamrValidateComputerAccountReuseAttempt' to Miscellaneous category, which confirms whether client attempts to re-use a particular computer account are allowed. Changed from: • SamrCloseHandle: This method releases server resources associated with the RPC context handle that is passed as a parameter. Changed to: • SamrCloseHandle: This method releases server resources associated with the RPC context handle that is passed as a parameter. • SamrValidateComputerAccountReuseAttempt: This method validates whether a client attempt to re-use a given computer account is permitted. In section 2.2.7.15 SAMPR_REVISION_INFO_V1 Description: Updated SupportedFeatures parameter of the SAMPR_REVISION_INFO_V1 structure by adding hex value (0x00000020) to represent that the server validates client reuse of computer accounts through client calls to the SamrValidateComputerAccountReuseAttempt method.

Errata Published*	Description
	Changed from: 0x00000010 On receipt by the client, this value, when set, indicates that the client should use AES Encryption with the SAMPR_ENCRYPTED_PASSWORD_AES structure to encrypt password buffers when sent over the wire. See AES Cipher Usage (section 3.2.2.4) and SAMPR_ENCRYPTED_PASSWORD_AES (section 2.2.6.32). Changed to: 0x00000010 On receipt by the client, this value, when set, indicates that the client should use AES Encryption with the SAMPR_ENCRYPTED_PASSWORD_AES structure to encrypt password buffers when sent over the wire. See AES Cipher Usage (section 3.2.2.4) and SAMPR_ENCRYPTED_PASSWORD_AES (section 2.2.6.32). 0x00000020 On receipt of this value by the client, when set, indicates that the server supports the validation of computer account re-use through client calls to the SamrValidateComputerAccountReuseAttempt method. In Section 3.1.1.12 ComputerAccountReuseAllowList Description: Created new section to define ADM element 'ComputerAccountReuseAllowList' that is used to hold trusted computer account owners. In Section 3.1.5 Message Processing Events and Sequencing Rules Description: Added new method to Opnum list: 'SamrValidateComputerAccountReuseAttempt' (Opnum 74) Changed from: SamrUnicodeChangePasswordUser4 Changes a user account password. Opnum 73 Changed to: SamrUnicodeChangePasswordUser4 Changes a user account password. Opnum 73 SamrValidateComputerAccountReuseAttempt Validates whether clients can re-use a computer account. Opnum 74 In Section 3.1.5.13.8 SamrValidateComputerAccountReuseAttempt (Opnum 74) Description: Created new method 'SamrValidateComputerAccountReuseAttempt' (Opnum 74) that validates whether client attempts to reuse computer accounts are permitted.<pbn72> <pbn72>: ComputerAccountReuseAllowList and supporting method SamrValidateComputerAccountReuseAttempt are supported on the operating systems specified in [MSKB-5020276], each with its related KB article download installed. In Section 6 Appendix A: Full IDL Description: Added IDL for new method SamrValidateComputerAccountReuseAttempt Opnum 74. // opnum 74 NTSTATUS SamrValidateComputerAccountReuseAttempt([in] SAMPR_HANDLE ServerHandle, [in] PRPC_SID ComputerSid, [out] BOOL* Result

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>);</td></tr>
<tr><td>2022/09/20</td><td>In Section 2.2.1.18, AEAD-AES-256-CBC-HMAC-SHA512 Constants
Description: Updated AEAD-AES-256-CBC-HMAC-SHA512 constants to ensure that the value details allow an implementation to be successfully created.

Changed from:
<table>
<tr><th>Constant Name</th><th>Value</th></tr>
<tr><td>versionbyte</td><td>0x01</td></tr>
<tr><td>versionbyte_length</td><td>1</td></tr>
<tr><td>SAM_AES_256_ALG</td><td>"AEAD-AES-256-CBC-HMAC-SHA512"</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING</td><td>"Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING</td><td>"Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING_LENGTH</td><td>sizeof(SAM_AES256_ENC_KEY_STRING)</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING_LENGTH</td><td>sizeof(SAM_AES256_MAC_KEY_STRING)</td></tr>
</table>
Changed to:
<table>
<tr><th>Constant/value</th><th>Description</th></tr>
<tr><td>Versionbyte
0x01</td><td>Version identifier.</td></tr>
<tr><td>versionbyte_length
1</td><td>Version identifier length.</td></tr>
<tr><td>SAM_AES_256_ALG
“AEAD-AES-256-CBC-HMAC-SHA512”</td><td>A NULL terminated ANSI string.</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING
"Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"</td><td>A NULL terminated ANSI string.</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING
"Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"</td><td>A NULL terminated ANSI string.</td></tr>
<tr><td>SAM_AES256_ENC_KEY_STRING_LENGTH
sizeof(SAM_AES256_ENC_KEY_STRING)
(61)</td><td>The length of SAM_AES256_ENC_KEY_STRING, including the null terminator.</td></tr>
<tr><td>SAM_AES256_MAC_KEY_STRING_LENGTH
sizeof(SAM_AES256_MAC_KEY_STRING)
(54)</td><td>The length of SAM_AES256_MAC_KEY_STRING, including the null terminator</td></tr>
</table>
In Section 3.2.2.4, AES Cipher Usage
Description: Specified the format of secret plaintext for SamrUnicodeChangePasswordUser4 and SamrSetInformationUser2 when creating the content encryption key (CEK); and clarified the usage of enc_key and mac_key when encrypting the data.
Changed from:</td></tr>
</table>

Errata Published*	Description
	• For the SamrUnicodeChangePasswordUser4 method (section 3.1.5.10.4), the shared secret is the plaintext old password and the CEK is generated as specified in section 3.2.2.5. Changed to: • For the SamrUnicodeChangePasswordUser4 method (section 3.1.5.10.4), the shared secret is the plaintext old password and the CEK is generated as specified in section 3.2.2.5. • For SamrUnicodeChangePasswordUser4 and SamrSetInformationUser2, the secret plaintext MUST be in the format specified in section 2.2.6.32. Changed from: Let AuthData ::= HMAC-SHA-512(mac_key, versionbyte + IV + Cipher + versionbyte_length) Changed to: Let AuthData ::= HMAC-SHA-512(mac_key, versionbyte + IV + Cipher + versionbyte_length) Note that enc_key is truncated to 32-bytes and the entire 64-byte mac_key is used. In Section 3.2.2.5 Deriving an Encryption Key from a Plaintext Password Description: Clarified how a 16-byte encryption key MUST be derived. Changed from: The client MUST derive the CEK in the following manner: CEK :: = (PBKDF2(NT HASH of "OldPassword", Salt, Iteration Count, 512)) Changed to: The client MUST derive the CEK in the following manner: A 16-byte encryption key is derived using the PBKDF2 algorithm with HMAC SHA-512, the NT-hash of the users existing password, a random 16-byte Salt, and an Iteration Count. The Iteration Count MUST be between 5000 and 1,000,000 inclusive. CEK :: = (PBKDF2(NT HASH of "OldPassword", Salt, Iteration Count, 16))

*Date format: YYYY/MM/DD

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-SCMR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

September 12, 2018 - Download

September 23, 2019 - Download

April 29, 2022 – Download

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

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

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

RSS

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

September 12, 2018 - Download

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

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

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

RSS

No errata are available for the latest version of 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-SFU]: Kerberos Protocol Extensions Service for User and Constrained Delegation Protocol

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

RSS

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

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

March 4, 2020 - Download

November 23, 2020 - Download

Errata below are for Protocol Document Version V21.0 – 2021/06/25.

Errata Published*	Description
2022/12/13	In section 2.2.2 PA_S4U_X509_USER: Added that the cname is case sensitive and it MUST not be canonicalized and that the crealm will not be canonicalized by the KDC. Changed from: cname: The PrincipalName type discussed in detail in [RFC4120] section 5.2.2. It consists of a name type and name string. The default value for the name type is NT-UNKNOWN as specified in [RFC4120] section 6.2. The name string is a sequence of strings encoded as KerberosString, as specified in [RFC4120] section 5.2.1, that (together with the crealm) represents a user principal. crealm: A KerberosString that represents the realm in which the user account is located. This value is not case-sensitive. Changed to: cname: The PrincipalName type discussed in detail in [RFC4120] section 5.2.2. It consists of a name type and name string. The default value for the name type is NT-UNKNOWN as specified in [RFC4120] section 6.2. The name string is a sequence of strings encoded as KerberosString, as specified in [RFC4120] section 5.2.1, that (together with the crealm) represents a user principal. The name string is case sensitive and must not be canonicalized by the KDC. crealm: A KerberosString that represents the realm in which the user account is located. This value is not case-sensitive; however, it will not be canonicalized by the KDC. In section 3.1.5.1.1.2 Sending the S4USelf KRB_TGT_REQ: Added that string canonicalization will not occur for either userName or userRealm fields. Changed from: … The userName is a structure consisting of a name type and a sequence of a name string … The userRealm is the realm of the user account. If the user realm name is unknown, Service 1

Errata Published*	Description
	SHOULD use its own realm name. The auth-package field MUST be set to the string, "Kerberos". The auth-package field is not case-sensitive. Changed to: … The userName is a structure consisting of a name type and a sequence of a name string … The userRealm is the realm of the user account. If the user realm name is unknown, Service 1 SHOULD use its own realm name. The auth-package field MUST be set to the string, "Kerberos". The auth-package field is not case-sensitive. String canonicalization will not occur for either userName or userRealm fields. In section 3.2.5.1 KDC Receives S4U2self KRB_TGS_REQ: Added that the Name field in the PAC_CLIENT_INFO structure MUST have matching case for both the client name and the client realm fields. Changed from: • If the KDC supports the Privilege Attribute Certificate Data Structure [MS-PAC], a referral TGT is received and a PAC is provided, the Name field in the PAC_CLIENT_INFO structure MUST have the form of "client name@client realm". Changed to: • If the KDC supports the Privilege Attribute Certificate Data Structure [MS-PAC], a referral TGT is received and a PAC is provided, the Name field in the PAC_CLIENT_INFO structure MUST have the form of "client name@client realm" with matching case for both fields.
2021/09/21	In Section 3.2.5.2.3 Using ServicesAllowedToReceiveForwardedTicketsFrom, removed the UserAccountControl check and added a behavior note to document the addition of the NonForwardableDelegation flag with references to the Kerberos Security Feature Bypass Vulnerability. Changed from: If the service ticket in the additional-tickets field is not set to forwardable,<22> and the USER_NOT_DELEGATED bit is set in the UserAccountControl field in the KERB_VALIDATION_INFO structure ([MS-PAC] section 2.5), then the KDC MUST return KRB-ERR-BADOPTION with STATUS_ACCOUNT_RESTRICTION ([MS-ERREF] section 2.3.1). Changed to: If the service ticket in the additional-tickets field is not set to forwardable,<22> then the KDC MUST return KRB-ERR-BADOPTION with STATUS_ACCOUNT_RESTRICTION ([MS-ERREF] section 2.3.1).<23> <23> Section 3.2.5.2.3: The Kerberos Security Feature Bypass Vulnerability March 12,2021 [MSFT-CVE-2020-16996] update adds support for the NonForwardableDelegation registry value to (0) enable Enforcement of protection on Active Directory domain controller servers. Active Directory domain controllers will be in Enforcement mode unless the enforcement mode registry key is set to (1) disabled. This update applies to Windows Server 2012 and later. For additional information that includes Windows Server 2008 SP2 operating system and Windows Server 2008 R2 SP1 operating system see [MSFT-RBCD-ProtectedUserChanges].

*Date format: YYYY/MM/DD

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

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

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

RSS

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

October 16, 2015 - Download

June 30, 2015 - Download

June 1, 2017 - Download

December 1, 2017 - Download

September 12, 2018 - Download

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

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

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

RSS

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

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

June 1, 2021 - Download

October 6, 2021 - Download

April 29, 2022 – Download

Errata below are for Protocol Document Version V67.0 – 2023/02/27.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2023/05/22</td><td>In section 3.2.5.2, "Receiving an SMB2 Negotiate Response," revised the processing rule for the SecurityMode field to indicate that it is part of the Negotiate Response rather than the SMB2 header.
Changed from:
If the SecurityMode field in the SMB2 header of the response has the SMB2_NEGOTIATE_SIGNING_REQUIRED bit set, the client MUST set Connection.RequireSigning to TRUE.
Changed to:
If the SecurityMode field in the Negotiate Response has the SMB2_NEGOTIATE_SIGNING_REQUIRED bit set, the client MUST set Connection.RequireSigning to TRUE.</td></tr>
<tr><td>2023/04/11</td><td>In section 2.2.14, "SMB2 CREATE Response," added a condition for using the SMB2_CREATE_FLAG_REPARSEPOINT in the Flags field:

Changed from:
<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>SMB2_CREATE_FLAG_REPARSEPOINT
0x01</td><td>When set, indicates the last portion of the file path is a reparse point.</td></tr></table>
Changed to:
<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>SMB2_CREATE_FLAG_REPARSEPOINT
0x01</td><td>When set, indicates the last portion of the file path is a reparse point. This MUST be used when the last component of a file</td></tr></table></td></tr>
</table>

Errata Published*	Description
	<table><tr><td></td><td>opened is a reparse point, and the create request Create Options do not contain FILE_OPEN_REPARSE_POINT.</td></tr></table> In section 3.3.5.9, "Receiving an SMB2 CREATE Request," added a condition for creating a reparse point when Open.Local is a reparse point but there is no FILE_OPEN_REPARSE_POINT value in the Create Options: Changed from: If **Connection.Dialect** belongs to the SMB 3.x dialect family and **Open.LocalOpen** is a **reparse point**, set the SMB2_CREATE_FLAG_REPARSEPOINT bit in the **Flags** field. Changed to: If **Connection.Dialect** belongs to the SMB 3.x dialect family and **Open.LocalOpen** is a **reparse point**, and the create request Create Options do not contain FILE_OPEN_REPARSE_POINT, set the SMB2_CREATE_FLAG_REPARSEPOINT bit in the **Flags** field.

*Date format: YYYY/MM/DD

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

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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

April 29, 2022 – Download

[MS-SQOS]: Storage Quality of Service Protocol

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-SSTP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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 24, 2021 - Download

Errata below are for Protocol Document Version V20.0 – 2021/06/25.

Errata Published*	Description
2022/10/24	In section 3.1.5.2 SSTP Packet Processing: Added MTU and MUR rules and settings that enable packets larger than 1586 bytes. Changed from: SSTP packet processing for common messages is covered separately for the client state machine and server state machine, in sections 3.2.5.3 and 3.3.5.2. Changed to: Common packet processing functionality is as follows: 1. The default maximum transmission unit (MTU) is set to 1400 bytes. 2. The maximum receive unit (MRU) exchanged for SSTP is 4091 bytes, which is 4095 – sizeof(SSTP_HEADER). 3. The default MTU can be increased using the registry values, but it is still capped at the MRU of the tunnel type. 4. The default MRU for the PPP adapter is set to 1614 bytes. 5. The default MRU can be increased by setting the following registry value: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NdisWan\Parameters\MRU By default, packets of any size can be sent or received through the tunnel, as Windows stack will IP fragment the packets. To enable large SSTP payloads, both MTU (on the sender) and MRU (on the receiver) need to be set to larger values. SSTP packet processing for common messages is covered separately for the client state machine and server state machine, in sections 3.2.5.3 and 3.3.5.2.

*Date format: YYYY/MM/DD

[MS-SSTR]: Smooth Streaming Protocol

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

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

RSS

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

March 16, 2018 - Download

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

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

*Date format: YYYY/MM/DD

[MS-SWN]: Service Witness Protocol

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

[MS-TCC]: Tethering Control Channel Protocol

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-TDS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

September 12, 2018 - Download

October 14, 2019 - Download

June 15, 2020 - Download

June 1, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-TPMVSC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-TSCH] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-TSGU] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

September 12, 2018 - Download

April 7, 2021 - Download

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

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

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

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

April 7, 2021 - Download

[MS-TSWP]: Terminal Services Workspace Provisioning Protocol

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

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

RSS

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

September 12, 2018 - Download

[MS-UAMG]: Update Agent Management Protocol

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-UCODEREF] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-VAPR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

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

June 1, 2017 - Download

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

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

April 29, 2022 – Download

[MS-W32T]: W32Time Remote Protocol

This topic lists Errata found in [MS-W32T] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-WCCE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

RSS

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

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

October 16, 2015 - Download

June 30, 2015 - Download

July 18, 2016 - Download

September 29, 2020 – Download

October 6, 2021 - Download

October 3, 2022 - Download

Errata below are for Protocol Document Version V47.0 – 2021/10/06.

Errata Published*	Description
2023/02/14	Section 3.2.2.6.3.1.1 PropID=0x0000001D (CR_PROP_TEMPLATES) "Configured Certificate Templates" Description: Updated string definition ("TemplateName1\nTemplateOID1\nTemplateName2\nTemplateOID2\...) to include a null termination character, to ensure consistent results with calls to the GetCATemplates function. Changed from: "TemplateName1\nTemplateOID1\nTemplateName2\nTemplateOID2\... " where Changed to: "TemplateName1\nTemplateOID1\nTemplateName2\nTemplateOID2...\nTemplateNameN\nTemplateOIDN\n\0" where Note: The format and definition of the string cited in section 3.2.1.4.3.2.29 below is correct as is.
2022/12/16	Section 2.1 Transport Description: Added product behavior note to specify the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level value that clients MUST use for certificate-request and certificate administrative operations to ensure that a connection to the CA server is not denied. Changed from: If a CA server has IF_ENFORCEENCRYPTICERTADMIN set (section 3.2.1.1.4) and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY (0x06) authentication level is not specified by the client for

Errata Published*	Description
	certificate administrative operations, the CA MUST deny a connection to the client and return a non-zero error.<7> Changed to: If a CA server has IF_ENFORCEENCRYPTICERTADMIN set (section 3.2.1.1.4) and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY (0x06) authentication level is not specified by the client for certificate administrative operations, the CA MUST deny a connection to the client and return a non-zero error. <7> <8> <8> The operating systems specified in [MSFT-CVE-2022-37976], each with their related KB article download installed, require that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTADMIN or IF_ENFORCEENCRYPTICERTREQUEST setting. Section 3.2.1.4.2.1 ICertRequestD::Request (Opnum 3) Description: Added product behavior note to specify the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level value that clients MUST use for certificate-request and certificate administrative operations to ensure that a connection to the CA server is not denied. Changed from: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error. Changed to: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level ([MS-RPCE] section 2.2.1.1.8), is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error. <70> <70>The operating systems specified in [MSFT-CVE-2022-37976], each with their related KB article download installed, require that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTREQUEST (section 3.2.1.1.4) setting. Section 3.2.1.4.2.2 ICertRequestD::GetCACert (Opnum 4) Description: Added product behavior note to specify the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level value that clients MUST use for certificate-request and certificate administrative operations to ensure a connection to the CA server is not denied. Changed from: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error. Changed to: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level ([MS-RPCE] section 2.2.1.1.8) is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error. <82>

Errata Published*	Description
	<82>The operating systems specified in MSFT-CVE-2022-37976, each with their related KB article download installed, require that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTREQUEST (section 3.2.1.1.4) setting. Section 3.2.1.4.2.3 ICertRequestD::Ping (Opnum 5) Description: Added product behavior note to specify the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level value that clients MUST use for certificate-request and certificate administrative operations to ensure that a connection to the CA server is not denied. Changed from: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error Changed to: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level ([MS-RPCE] section 2.2.1.1.8) is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error. <85> <85>The operating systems specified in [MSFT-CVE-2022-37976], each with their related KB article download installed, require that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTREQUEST (section 3.2.1.1.4) setting. Section 3.2.1.4.3.2 ICertRequestD2::GetCAProperty (Opnum 7) Description: Added product behavior note to specify the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level value that clients MUST use for certificate-request and certificate administrative operations to ensure a connection to the CA server is not denied. Changed from: If Config_CA_Interface_Flags contain the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a non-zero error. Changed to: If Config_CA_Interface_Flags contain the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level ([MS-RPCE] section 2.2.1.1.8) is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a non-zero error<88> <88>The operating systems specified in [MSFT-CVE-2022-37976], each with their related KB article download installed, require that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTREQUEST (section 3.2.1.1.4) setting. Section 3.2.1.4.3.3 ICertRequestD2::GetCAPropertyInfo (Opnum 8) Description: Added product behavior note to specify the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level value that clients MUST use for certificate-request and certificate

Errata Published*	Description
	administrative operations to ensure a connection to the CA server is not denied. Also specified the operating systems that support this behavior. Changed from: If Config_CA_Interface_Flags contains the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level, as defined in [MS-RPCE] section 2.2.1.1.8, is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error. Changed to: If Config_CA_Interface_Flags contain the value IF_ENFORCEENCRYPTICERTREQUEST and the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level ([MS-RPCE] section 2.2.1.1.8) is not specified on the RPC connection from the client, the CA MUST refuse to establish a connection with the client by returning a nonzero error. <108> <108>The operating systems specified in [MSFT-CVE-2022-37976], each with their related KB article download installed, require that clients MUST connect with the RPC_C_AUTHN_LEVEL_PKT_PRIVACY authentication level or the connection to the CA server will be denied, regardless of the IF_ENFORCEENCRYPTICERTREQUEST (section 3.2.1.1.4) setting.

*Date format: YYYY/MM/DD

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

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

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

RSS

No errata are available for the latest version of 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-WDHCE]: Wi-Fi Display Protocol Hardware Cursor Extension

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

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

RSS

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

April 29, 2022 – Download

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

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

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

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS

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

September 12, 2018 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-WFDPE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-WKST] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

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

July 18, 2016 - Download

April 7, 2021 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V31.0 – 2022/04/29.

Errata Published*	Description
2022/09/03	In Section 2.2.5.19, JOINPR_ENCRYPTED_USER_PASSWORD_AES, corrected typo: Changed from: AuthDate: 64 bytes, the HMAC. Changed to: AuthData: 64 bytes, the HMAC. In Section 2.2.5.19.3, Encrypt Key and MAC Key, clarified the calculation of the keys: Changed from: The following variables and values are used in calculating the EncryptKey and HMACKey values. versionbyte = 0x01 versionbyte_len = 1 algorithmString = "AEAD-AES-256-CBC-HMAC-SHA512" EncryptKey and MACKey are calculated as follows: EncryptKey := HMAC-SHA-512(SessionKey, "Microsoft WKST encryption key" + algorithmString +Length(SessionKey)) MACKey := HMAC-SHA-512(SessionKey, "Microsoft WKST MAC key" + algorithmString +Length(SessionKey)) Note that the SessionKey is calculated as in section 2.2.5.19.2. See [RFC4868] for details of the HMAC-SHA-512 algorithm. Changed to: The following variables and values are used in calculating the EncryptKey and MACKEY values:

Constant/value	Description
versionbyte 0x01	Version identifier.
versionbyte_len 1	Version identifier length.
WKST_AES_256_ALG "AEAD-AES-256-CBC-HMAC-SHA512"	A NULL terminated ANSI string.
WKST_AES256_ENC_KEY_STRING "Microsoft WKST encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"	A NULL terminated ANSI string.
WKST_AES256_MAC_KEY_STRING "Microsoft WKST MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"	A NULL terminated ANSI string.
WKST_AES256_ENC_KEY_STRING_LENGTH sizeof(WKST_AES256_ENC_KEY_STRING) (62)	The length of WKST_AES256_ENC_KEY_STRING, including the null terminator.
WKST_AES256_MAC_KEY_STRING_LENGTH sizeof(WKST_AES256_MAC_KEY_STRING) (55)	The length of WKST_AES256_MAC_KEY_STRING, including the null terminator.

EncryptKey and MACKey are calculated as follows:

EncryptKey := HMAC-SHA-512(SessionKey, WKST_AES256_ENC_KEY_STRING)

MACKey := HMAC-SHA-512(SessionKey, WKST_AES256_MAC_KEY_STRING)

Note that the SessionKey is calculated as in section 2.2.5.19.2. See [RFC4868] for details of the HMAC-SHA-512 algorithm.

In Section 2.2.5.19.4, Encrypt Encoded Password, clarified the encreyption process:

Changed from:

Encrypt the encoded password as follows:

Salt := Randomly generated 16 bytes

Cipher := AES-CBC(EncryptKey[0:256], IV, EncodedPasswordLength(4 bytes) + EncodedPassword)

AuthData := HMAC-SHA-512(MACKey, Cipher+Salt+ versionbyte + versionbyte_len)

Note that the Salt value is used as the initialization vector (IV). The MACKey is calculated in section 2.2.5.19.3.

Changed to:

Encrypt the encoded password as follows:

Salt := Randomly generated 16 bytes

Encoded_Plaintext:= EncodedPasswordlength (4 bytes) + EncodedPassword.

Cipher := AES-CBC(EncryptKey[0:256], IV, Encoded_Plaintext)

AuthData := HMAC-SHA-512(MACKey, Cipher+Salt+ versionbyte + versionbyte_len)

Note that the Salt value is used as the initialization vector (IV). The MACKey is calculated in section 2.2.5.19.3.

Note that EncryptKey is truncated to 32 bytes and the entire 64-byte MACKey is used.

*Date format: YYYY/MM/DD

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

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

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

RSS

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

April 7, 2021 - Download

[MS-WMF]: Windows Metafile Format

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

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

[MS-WPO]: Windows Protocols Overview

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-WSDS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-WSMV] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

September 12, 2018 - Download

April 7, 2021 - Download

[MS-WSP]: Windows Search Protocol

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

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

RSS

No errata are available for the latest version of 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 23, 2019 - Download

March 4, 2020 - Download

August 24, 2020 – Download

April 7, 2021 - Download

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

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

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

RSS

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 V14.0 – 2021/06/25.

Errata Published*	Description
2021/09/21	In Section 3.1.4.1.3.2 wst:RequestedSecurityTokenType, updated to clarify the RequestSecurityTokenResponseCollection and RequestedSecurityToken element responses, the certificate locations, and the BinarySecurityToken format and value type. Changed from: "The WSTEP extends wst: RequestedSecurityTokenType with two additional elements. • <xs:element ref="wsse:BinarySecurityToken" /> • <xs:element ref="wsse:SecurityTokenReference" /> wsse:BinarySecurityToken: The wsse:BinarySecurityToken element contains the issued certificate. The issued certificate follows the encoding and data structure defined in [MS-WCCE] section 2.2.2.8." Changed to: "MS-WSTEP extends the wst: RequestedSecurityTokenType with two additional elements as follows. • <xs:element ref="wsse:BinarySecurityToken" /> • <xs:element ref="wsse:SecurityTokenReference" /> The server SHOULD<2> include the end entity certificate in the RequestedSecurityTokenresponse. The ValueType of the BinarySecurityToken element for this RequestedSecurityToken response MUST be X509v3 [RFC5280]. The server MUST also include a CMC full PKI response in the RequestSecurityTokenResponseCollection, as specified in sections 4.2 and 4.3 of [WSTrust1.3]. wsse:BinarySecurityToken: The wsse:BinarySecurityToken element contains the issued certificatein either a full CMC response or as a stand alone x509v3 certificate[RFC5280]. <2> Section 3.1.4.1.3.2: Microsoft Windows always includes the requested end entity certificate in the RequestedSecurityToken."

*Date format: YYYY/MM/DD

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

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

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

RSS

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

July 18, 2016 - Download

June 1, 2017 - Download

March 4, 2020 - Download

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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 Errata found in [MS-WSUSSS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to this RSS feed to receive update notifications.

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

RSS

No errata are available for the latest version of 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

April 7, 2021 - Download

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

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

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

RSS

No errata are available for the latest version of 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

March 4, 2020 - Download

April 7, 2021 - Download

October 6, 2021 - Download

April 29, 2022 - Download

[MS-XCA]: Xpress Compression Algorithm

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

RSS

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

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

March 4, 2020 - Download

August 24, 2020 – Download

Errata Published*	Description
2023/01/30	In section 2.1.4.3, deleted a sentence asserting that match length checks are performed. Changed from: Note that match distances cannot be larger than 65,535, and match lengths cannot be longer than 65,538. The LZ77 phase is implemented to ensure that match lengths and distances do not exceed these values. Changed to: Note that match distances cannot be larger than 65,535, and match lengths cannot be longer than 65,538. In section 2.2.4, "Processing," clarified the description of processing for decompression. Changed from: During the beginning of processing each block for decompression, an implementation MUST check for EOF. An implementation can do this by comparing the block size against the required space for a Huffman table — if this condition is met and all output has been written, then processing stops and success is returned. Alternately, an implementation can explicitly examine the input buffer using the Huffman table from the previous block. Changed to: During the beginning of processing each block for decompression, an implementation MUST check that the block has sufficient space for a Huffman table — if the block has enough space, then processing continues. If there is not enough space for a Huffman table and all output has been written, then processing stops and success is returned, otherwise an error indicating invalid data is returned. In section 2.2.4, Processing, added terminating conditions to the decompression pseudocode.

Errata Published*	Description

	Changed from:
	
	Loop until a decompression terminating condition
	  Build the decoding table
	  CurrentPosition = 256 // start at the end of the Huffman table
	  NextBits = Read16Bits(InputBuffer + CurrentPosition)
	  CurrentPosition += 2
	
	Changed to:
	Loop until a decompression terminating condition
	  If remaining input buffer does not have enough space for a Huffman table
	  If we're at the end of the output buffer
	  Decompression is complete, return success
	  The compressed data is not valid, return error
	  Build the decoding table
	  CurrentPosition = 256 // start at the end of the Huffman table
	  NextBits = Read16Bits(InputBuffer + CurrentPosition)
	  CurrentPosition += 2

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

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

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

RSS

No errata are available for the latest version of 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