

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.



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.

January 2024 Update: Protocols documents will be updated in their Open Specifications Library locations, rather than being published as errata. The following documents with active errata will be republished and their active errata will be archived over the coming months.

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](#)

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

[\[MS-EFSR\]: 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](#)

[\[MS-PKCA\]: 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](#)

[\[MS-RDPEGFX\]: Remote Desktop Protocol: Graphics Pipeline 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](#)
June 28, 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.

No errata are available for the latest version of 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.

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.



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	<p>In Section 2.2.6, Preamble Message, the field descriptions have been modified as follows and have been moved to follow the packet diagram.</p> <p>Changed from:</p> <p>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</p> <p>Changed to:</p> <p>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</p>

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

To view a PDF 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	<p>In Section 2.243, Class samDomain, changed from:</p> <p>(OA; CIOI; RPWP; 3f78c3e5-f79a-46bd-a0b8-9d18116ddc79;; PS) S: (AU; SA; WDWOWP;;; WD) (AU; SA; CR;;; BA) (AU; SA; CR;;; DU)</p> <p>Changed to:</p> <p>(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)</p>

*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.

To view a PDF 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	<p>Section: 6.1.6.7.15 trustType</p> <p>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.</p> <p>Changed from: TTDCE (TRUST_TYPE_DCE, 0x00000004): Historical reference; this value is not used in Windows.</p> <p>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.</p> <p>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.</p>
2023/04/10	<p>Section: 6.1.6.7.15 trustType</p>

Errata Published*	Description																																													
	<p>Description: Added new trustType definition TTAAD (TRUST_TYPE_AAD, 0x00000005) for trusted domain Azure Active Directory applications.</p> <p>Changed from: TTDCE (TRUST_TYPE_DCE, 0x00000004): Historical reference; this value is not used in Windows.</p> <p>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.</p> <p>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.</p>																																													
2023/02/27	<p>Section 1 Introduction</p> <p>Description: Mapped the applicability of Windows 10 v21H2 operating system to Windows Server 2022 for the new rootDSE attributes.</p> <p>Changed from: Information that is applicable to AD LDS on Windows Server v1903 is also applicable to AD LDS for Windows 10 v1903.</p> <p>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.</p> <p>Section 3.1.1.3.2 rootDSE Attributes</p> <p>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].</p> <p>(Product applicability list)</p> <p>Changed from:</p> <ul style="list-style-type: none"> • N2 --> Windows Server v1903 AD DS <p>Changed to:</p> <ul style="list-style-type: none"> • N2 --> Windows Server v1903 AD LDS • P2 --> Windows Server 2022 AD DS • Q2 --> Windows Server 2022 AD LDS <p>(Attribute table)</p> <p>Changed from:</p> <table border="1" data-bbox="386 1608 1419 1659"> <tr> <td>msDS-SupportedRootDSEModifications</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td>X</td> </tr> </table> <p>Changed to:</p> <table border="1" data-bbox="386 1734 1419 1785"> <tr> <td>msDS-SupportedRootDSEModifications</td> <td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>X</td><td>X</td> </tr> </table>	msDS-SupportedRootDSEModifications																				X	X	msDS-SupportedRootDSEModifications																					X	X
msDS-SupportedRootDSEModifications																				X	X																									
msDS-SupportedRootDSEModifications																					X	X																								

Errata Published*	Description																													
	msDS-DiskUsage ****													X	X															
	msDS-DatabaseIndices ****													X	X															
	msDS-DatabaseIndicesWithSize ****													X	X															
	<p>**** 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.</p> <p>(Attribute Operational? LDAP Syntax table) Changed from:</p> <table border="1" data-bbox="386 667 1073 716"> <tr> <td>msDS-SupportedRootDSEModifications</td> <td>Y</td> <td>String(Unicode)</td> </tr> </table> <p>Changed to:</p> <table border="1" data-bbox="386 827 1073 1031"> <tr> <td>msDS-SupportedRootDSEModifications</td> <td>Y</td> <td>String(Unicode)</td> </tr> <tr> <td>msDS-DiskUsage</td> <td>Y</td> <td>String(Unicode)</td> </tr> <tr> <td>msDS-DatabaseIndices</td> <td>Y</td> <td>String(Unicode)</td> </tr> <tr> <td>msDS-DatabaseIndicesWithSize</td> <td>Y</td> <td>String(Unicode)</td> </tr> </table> <p>(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.</p> <p>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.</p> <p>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.</p> <p>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.</p>															msDS-SupportedRootDSEModifications	Y	String(Unicode)	msDS-SupportedRootDSEModifications	Y	String(Unicode)	msDS-DiskUsage	Y	String(Unicode)	msDS-DatabaseIndices	Y	String(Unicode)	msDS-DatabaseIndicesWithSize	Y	String(Unicode)
msDS-SupportedRootDSEModifications	Y	String(Unicode)																												
msDS-SupportedRootDSEModifications	Y	String(Unicode)																												
msDS-DiskUsage	Y	String(Unicode)																												
msDS-DatabaseIndices	Y	String(Unicode)																												
msDS-DatabaseIndicesWithSize	Y	String(Unicode)																												
2022/01/18	<p>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.</p>																													

Errata Published*	Description
-------------------	-------------

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

Policy name	A	D, DR2, G, J	M	R	U	X, A2, D2, G2, J2
MaxActiveQueries	X*					
InitRecvTimeout	X	X	X	X	X	X
....						* Support for this policy was removed in Windows Server 2003.

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

Policy name	A	D, DR2, G, J	M	R	U	X, A2, D2, G2, J2
MaxActiveQueries	X*					
InitRecvTimeout	X	X	X	X	X	X
....						
SecurityDescriptorWarningSize**						

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

Changed from:

Policy name	Default value	Description
....		
MaxDirSyncDuration	60	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.

Changed to:

Policy name	Default value	Description
....		

Errata Published*	Description		
		
	MaxDirSyncDuration	60	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.
	SecurityDescriptorWarningSize	61,440	This policy controls when warning events will be logged for originating writes to the ntSecurityDescriptor attribute that meet or exceed the configured size value.

*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.

No errata are available for the latest version of 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.

To view a PDF 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	<p>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.</p> <p>Changed from:</p> <ul style="list-style-type: none">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. <p>Changed to:</p> <ul style="list-style-type: none">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.

No errata are available for the latest version of 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.

To view a PDF 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	<p>The following sections were changed. Please see the diff document for the details.</p> <p>In Section 3.2.4.1 Performing Client-Side Wrapping of Secrets, Product Behavior Note<18></p> <p>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.</p> <p>Changed from:</p> <p>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.</p> <p>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.</p> <p>Changed to:</p> <p>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.</p> <p>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.</p>

[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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

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	<p>In Section 2.2.2.1.1, "Common Header," changed "inner buffer" to "Payload field" in the descriptions of deserialization.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>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.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>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.</p>
2022/11/29	<p>In section 2.2.2.2.3, "Bluetooth Advertising Beacon," added flag values and provided additional details about packet field structure and length.</p> <p>Changed from:</p> <p>Beacon Data (24 bytes): The beacon data section is further broken down. Note that the Scenario</p>

Errata Published*	Description
-------------------	-------------

and Subtype Specific Data section requirements will differ based on the Scenario and Subtype.

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Scenario Type										Version and Device Type										Version and Flags						Reserved					
Salt																															
Device Hash (16 bytes)																															
...																															
...																															

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 lower 6 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.

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Scenario_Type								Version_and_Device_Type								Version_and_Flags						Flags_and_Device_Status									
Salt																															
Device_Hash (19 bytes)																															
...																															
...																															
...																															

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.

Changed to:

Errata Published*	Description																																		
	<p>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.</p> <p>Flags_and_Device_Status (1 byte): The field has the following structure:</p> <table border="1" data-bbox="391 342 1401 447"> <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> <p>A (2 bits): Unused.</p> <p>B - Bluetooth_Address_As_Device_ID (1 bit): When set, indicates that the Bluetooth address can be used as the device ID.</p> <p>C (1 bit): Unused.</p> <p>D - ExtendedDeviceStatus (4 bits):</p> <p>One of the values in the following table. Values may be ORed.</p> <table border="1" data-bbox="391 678 1430 1035"> <thead> <tr> <th>Meaning</th> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>Salt (4 bytes): Four random bytes.</p> <p>Device_Hash (19 bytes): SHA256 Hash of Salt plus Device Thumbprint.</p>	0	1	2	3	4	5	6	7	A		B		C		D		Meaning	Value	Description	None	0x00	None.	RemoteSessionsHosted	0x01	Hosted by remote session.	RemoteSessionsNotHosted	0x02	Indicates the device does not have session hosting status available.<5>	NearShareAuthPolicySameUser	0x04	Indicates the device supports NearShare if the user is the same for the other device.	NearShareAuthPolicyPermissive	0x08	Indicates the device supports NearShare.<6>
0	1	2	3	4	5	6	7																												
A		B		C		D																													
Meaning	Value	Description																																	
None	0x00	None.																																	
RemoteSessionsHosted	0x01	Hosted by remote session.																																	
RemoteSessionsNotHosted	0x02	Indicates the device does not have session hosting status available.<5>																																	
NearShareAuthPolicySameUser	0x04	Indicates the device supports NearShare if the user is the same for the other device.																																	
NearShareAuthPolicyPermissive	0x08	Indicates the device supports NearShare.<6>																																	

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

To view a PDF 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	<p>In Section 6 Appendix A: Product Behavior, the following behavior notes have been updated:</p> <p>Changed from:</p> <p><245> Section 3.3.5.5</p> <p>...</p> <p>AccessMode.SharingMode ShareAccess</p> <p>0 Compatibility mode (see below)</p> <p>1 0x0L (don't share, exclusive use)</p> <p>2 FILE_SHARE_READ</p> <p>3 FILE_SHARE_WRITE</p> <p>4 FILE_SHARE_READ FILE_SHARE_WRITE</p> <p>0xFF FCB mode (see below)</p> <ul style="list-style-type: none">• For Compatibility mode, special filename suffixes (after the '.' in the filename) are mapped

Errata Published*	Description
	<p>to SharingMode 4. The special filename suffix set is: "EXE", "DLL", "SYM", "COM". All other file names are mapped to SharingMode 3.</p> <ul style="list-style-type: none"> • 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. <p>...</p> <p>Changed to:</p> <p>...</p> <p>AccessMode.SharingMode ShareAccess</p> <p>0 Compatibility mode (see below)</p> <p>1 0x0L (don't share, exclusive use)</p> <p>2 FILE_SHARE_READ</p> <p>3 FILE_SHARE_WRITE</p> <p>4 FILE_SHARE_READ FILE_SHARE_WRITE</p> <ul style="list-style-type: none"> • 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. <p>...</p> <p>Changed from:</p> <p><297> Section 3.3.5.35</p> <p>...</p> <p>AccessMode.SharingMode ShareAccess</p> <p>0 Compatibility mode (see below)</p> <p>1 0x0L (don't share, exclusive use)</p> <p>2 FILE_SHARE_READ</p>

Errata Published*	Description
	<p>3 FILE_SHARE_WRITE</p> <p>4 FILE_SHARE_READ FILE_SHARE_WRITE</p> <p>0xFF FCB mode (see below)</p> <ul style="list-style-type: none"> 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. <p>...</p> <p>Changed to:</p> <p>...</p> <p>AccessMode.SharingMode ShareAccess</p> <p>0 Compatibility mode (see below)</p> <p>1 0x0L (don't share, exclusive use)</p> <p>2 FILE_SHARE_READ</p> <p>3 FILE_SHARE_WRITE</p> <p>4 FILE_SHARE_READ FILE_SHARE_WRITE</p> <ul style="list-style-type: none"> 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. <p>...</p> <p>Changed from:</p> <p><339> Section 3.3.5.58.2</p> <p>...</p>

Errata Published*	Description
	<p>AccessMode.SharingMode ShareAccess</p> <p>0 Compatibility mode (see following)</p> <p>1 0x0L (don't share, exclusive use)</p> <p>2 FILE_SHARE_READ</p> <p>3 FILE_SHARE_WRITE</p> <p>4 FILE_SHARE_READ FILE_SHARE_WRITE</p> <p>0xFF FCB mode (see following)</p> <ul style="list-style-type: none"> 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. <p>...</p> <p>Changed To:</p> <p>...</p> <p>AccessMode.SharingMode ShareAccess</p> <p>0 Compatibility mode (see following)</p> <p>1 0x0L (don't share, exclusive use)</p> <p>2 FILE_SHARE_READ</p> <p>3 FILE_SHARE_WRITE</p> <p>4 FILE_SHARE_READ FILE_SHARE_WRITE</p> <ul style="list-style-type: none"> 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.

Errata Published*	Description
	...

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

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	<p>In Section 2.4 flags Attribute:</p> <p>Description: "Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000."</p> <p>Changed from:</p> <p>"0x00000400</p> <p>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."</p> <p>Changed to:</p> <p>"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."</p>
2022/06/14	<p>In Section 2.4 flags Attribute:</p> <p>Description: "Updated the value of the CT_FLAG_DONOTPERSISTINDB flag from 0x00000400 to 0x00001000."</p> <p>Changed from:</p> <p>"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."</p> <p>Changed to:</p> <p>"0x00001000 CT_FLAG_DONOTPERSISTINDB</p>

Errata Published*	Description										
	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."										
2022/05/10	<p>Section 2.26 msPKI-Enrollment-Flag Attribute</p> <p>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."</p> <p>Changed From:</p> <table border="1" data-bbox="391 579 1429 716"> <thead> <tr> <th>Flag</th> <th>Meaning</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>Changed To:</p> <table border="1" data-bbox="391 827 1429 1115"> <thead> <tr> <th>Flag</th> <th>Meaning</th> </tr> </thead> <tbody> <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 flag³⁴ 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> </tbody> </table> <p>³⁴ This flag is supported by the operating systems specified in [MSFT-CVE-2022-26931], each with its related KB article download installed.</p>	Flag	Meaning	0x00040000 CT_FLAG_SKIP_AUTO_RENEWAL	This flag indicates that the certificate should not be auto-renewed, although it has a valid template.	Flag	Meaning	0x00040000 CT_FLAG_SKIP_AUTO_RENEWAL	This flag indicates that the certificate should not be auto-renewed, although it has a valid template.	0x00080000 CT_FLAG_NO_SECURITY_EXTENSION	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.
Flag	Meaning										
0x00040000 CT_FLAG_SKIP_AUTO_RENEWAL	This flag indicates that the certificate should not be auto-renewed, although it has a valid template.										
Flag	Meaning										
0x00040000 CT_FLAG_SKIP_AUTO_RENEWAL	This flag indicates that the certificate should not be auto-renewed, although it has a valid template.										
0x00080000 CT_FLAG_NO_SECURITY_EXTENSION	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.										
2021/07/27	<p>In Section 2.27 msPKI-Private-Key-Flag Attribute, replaced normative reference [PKCS12] with [RFC7292].</p> <p>Changed from:</p> <table border="1" data-bbox="391 1394 1429 1583"> <thead> <tr> <th>Flag</th> <th>Meaning</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>Changed to:</p> <table border="1" data-bbox="391 1692 1429 1776"> <thead> <tr> <th>Flag</th> <th>Meaning</th> </tr> </thead> <tbody> </tbody> </table>	Flag	Meaning	0x00000010 CT_FLAG_EXPORTABLE_KEY	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.	Flag	Meaning				
Flag	Meaning										
0x00000010 CT_FLAG_EXPORTABLE_KEY	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.										
Flag	Meaning										

Errata Published*	Description	
	0x00000010 CT_FLAG_EXPORTABLE_KEY	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.

*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.



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	<p>Section 3.1.4.1 Processing Rules for ICertAdminD</p> <p>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].</p> <p>Changed from:</p> <p>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></p> <p>Changed to:</p> <p>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></p> <p><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.</p> <p>Section 3.1.4.2 Processing Rules for ICertAdminD2</p> <p>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].</p> <p>Changed from:</p>

Errata Published*	Description
	<p>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).</p> <p>Changed to:</p> <p>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></p> <p><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.</p>

[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.

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	<p>In Section 2.2.1.2.3.1 TSRemoteGuardPackageCred, changed credBuffer: Windows CredSSP usage of Kerberos User to User tickets.</p> <p>Changed from:</p> <p>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.</p> <p><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. . .</p> <p>Changed to:</p> <p>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.</p> <p><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. . .</p>
2021/08/10	<p>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.</p> <p>Changed from:</p> <pre>typedef struct _NTLM_REMOTE_SUPPLEMENTAL_CREDENTIAL {</pre>

Errata Published*	Description	
	L	Indicates that the LM OWF member is present and valid.
	N	Indicates that the NT OWF member is present and valid.
	C	Indicates that the reserved credential key is present and valid ([MS-RDPEAR] section 2.2.1.3.5).

*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.

No errata are available for the latest version of 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.



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	<p>Section 3.2.4.1.1.2 Issuing the Activation Request</p> <p>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.</p> <p>Changed from:</p> <p><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.</p> <p>Changed to:</p> <p><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.</p> <p>Changed from:</p> <p><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.</p> <p>Changed to:</p> <p><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.</p> <p>On Windows Vista and later and Windows Server 2008 and later, DCOM clients specify the higher of the LegacyAuthenticationLevel value ([MSDN-LegAuthLevel]) or</p>

Errata Published*	Description
	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	<p>Section 3.2.4.1.1.2 Issuing the Activation Request</p> <p>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.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>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>.</p> <p>Updated product behavior note 80:</p> <p>Changed from:</p> <p>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.</p> <p>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.</p> <p>Changed to:</p> <p><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 11 Desktop v22H2, Windows Server 2022 - Full/Core, Windows 10 Desktop</p>

Errata Published*	Description
	v22H2, Windows 10 Desktop v21H2, Windows 10 Desktop v21H1, and Windows 10 Desktop v20H2.
2022/10/24	<p>Section 3.2.4.1.1.2 Issuing the Activation Request</p> <p>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.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>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>.</p> <p><pbn-80>Updated; see below.</p> <p>Updated product behavior note 80:</p> <p>Changed from:</p> <p>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.</p> <p>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.</p> <p>Changed to:</p> <p><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 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</p>

Errata Published*	Description
	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	<p>In Section 2.2.22.2.8.1 customREMOTE_REPLY_SCM_INFO</p> <p>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.</p> <p>Changed from:</p> <p><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.</p> <p>Changed to:</p> <p><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.</p>
2022/10/04	<p>Section 3.2.4.1.1.2 Issuing the Activation Request</p> <p>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.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>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>.</p> <p><pbn-80>Updated; see below.</p> <p>Updated product behavior note 80:</p> <p>Changed from:</p> <p>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.</p> <p>On Windows XP SP2, Windows Server 2003 with SP1, Windows Vista and later, and Windows</p>

Errata Published*	Description
	<p>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.</p> <p>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.</p> <p>Changed to:</p> <p><pbm-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.</p>

[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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.



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	<p>In Section 3.1.4.5 R_DnsrvUpdateRecord (opnum 4), added processing behavior for the static condition.</p> <p>Changed from:</p> <ul style="list-style-type: none">• 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. <p>Changed to:</p> <ul style="list-style-type: none">• 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. <p><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.</p>
2021/08/10	<p>In Section 3.1.1.1.1 DNS Server Integer Properties, in DsTombstoneInterval added seconds to 100-nanosecond conversion.</p> <p>Changed from:</p>

Errata Published*	Description
	<p>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. . . .</p> <p>Changed to:</p> <p>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). . . .</p> <p>In Section 3.1.4.5 R_DnssrvUpdateRecord (Opnum 4), changed EntombedTime from seconds to 100-nanosecond intervals and removed redundant instructions.</p> <p>Changed from:</p> <p>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 in 2.3.2.2. 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.</p> <p>Changed to:</p> <p>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).</p>

*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.

No errata are available for the latest version of 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.

To view a PDF 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	<p>In Section 5.39 DRS_EXTENSIONS_INT:</p> <p>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.</p> <p>Changed From:</p> <p>"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>"</p> <p><42> This field contains the process ID of the client.</p> <p>Changed To:</p> <p>"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>"</p> <p><42> This field contains the process ID of the client or server, depending on which is current.</p>

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

To view a PDF 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](#)

Errata below are for Protocol Document Version [V39.0 - 2023/04/04](#).

Errata Published*	Description										
2023/08/16	<p>Section 2.4.2.4 Well-known SID Structures: Added Remote VM SID value with format for machine identity.</p> <p>Changed from:</p> <table border="1"><thead><tr><th>Constant/value</th><th>Description</th></tr></thead><tbody><tr><td>...</td><td></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 S-1-5-84-0-0-0-0-0</td><td>Identifies a user-mode driver process.</td></tr><tr><td>...</td><td></td></tr></tbody></table>	Constant/value	Description	...		NT VIRTUAL MACHINE\Virtual Machines S-1-5-83-0	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).	USER_MODE_DRIVERS S-1-5-84-0-0-0-0-0	Identifies a user-mode driver process.	...	
Constant/value	Description										
...											
NT VIRTUAL MACHINE\Virtual Machines S-1-5-83-0	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).										
USER_MODE_DRIVERS S-1-5-84-0-0-0-0-0	Identifies a user-mode driver process.										
...											

Errata Published*	Description													
	<table border="1"> <thead> <tr> <th data-bbox="391 228 907 275">Constant/value</th> <th data-bbox="907 228 1437 275">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="391 275 907 327">...</td> <td data-bbox="907 275 1437 327"></td> </tr> <tr> <td data-bbox="391 327 907 531">NT VIRTUAL MACHINE\Virtual Machines S-1-5-83-0</td> <td data-bbox="907 327 1437 531">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 data-bbox="391 531 907 913">NT VIRTUAL MACHINE\Remote Virtual Machine S-1-5-83-1-dd-dd-dd-dd</td> <td data-bbox="907 531 1437 913">The VM SID is only used for local access, while remote access uses the machine identity. S-1: Security ID revision level 1 5: The identifier-authority SECURITY_NT_AUTHORITY 83: First subauthority SECURITY_VIRTUALSERVER_ID_BASE_RID 1: Second subauthority SECURITY_VIRTUAL_MACHINE_RID dd: The last 4 values is the container ID There are a total of 6 subauthorities.</td> </tr> <tr> <td data-bbox="391 913 907 999">USER_MODE_DRIVERS S-1-5-84-0-0-0-0-0</td> <td data-bbox="907 913 1437 999">Identifies a user-mode driver process.</td> </tr> <tr> <td data-bbox="391 999 907 1052">...</td> <td data-bbox="907 999 1437 1052"></td> </tr> </tbody> </table>		Constant/value	Description	...		NT VIRTUAL MACHINE\Virtual Machines S-1-5-83-0	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).	NT VIRTUAL MACHINE\Remote Virtual Machine S-1-5-83-1-dd-dd-dd-dd	The VM SID is only used for local access, while remote access uses the machine identity. S-1: Security ID revision level 1 5: The identifier-authority SECURITY_NT_AUTHORITY 83: First subauthority SECURITY_VIRTUALSERVER_ID_BASE_RID 1: Second subauthority SECURITY_VIRTUAL_MACHINE_RID dd: The last 4 values is the container ID There are a total of 6 subauthorities.	USER_MODE_DRIVERS S-1-5-84-0-0-0-0-0	Identifies a user-mode driver process.	...	
Constant/value	Description													
...														
NT VIRTUAL MACHINE\Virtual Machines S-1-5-83-0	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).													
NT VIRTUAL MACHINE\Remote Virtual Machine S-1-5-83-1-dd-dd-dd-dd	The VM SID is only used for local access, while remote access uses the machine identity. S-1: Security ID revision level 1 5: The identifier-authority SECURITY_NT_AUTHORITY 83: First subauthority SECURITY_VIRTUALSERVER_ID_BASE_RID 1: Second subauthority SECURITY_VIRTUAL_MACHINE_RID dd: The last 4 values is the container ID There are a total of 6 subauthorities.													
USER_MODE_DRIVERS S-1-5-84-0-0-0-0-0	Identifies a user-mode driver process.													
...														
2023/06/27	<p data-bbox="367 1062 1437 1121">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:</p> <table border="1" data-bbox="391 1121 1437 1297"> <tbody> <tr> <td data-bbox="391 1121 907 1207">NT_SERVICE S-1-5-80</td> <td data-bbox="907 1121 1437 1207">An NT Service account prefix.</td> </tr> <tr> <td data-bbox="391 1207 907 1297">USER_MODE_DRIVERS S-1-5-84-0-0-0-0-0</td> <td data-bbox="907 1207 1437 1297">Identifies a user-mode driver process.</td> </tr> </tbody> </table> <p data-bbox="367 1339 505 1367">Changed to:</p> <table border="1" data-bbox="391 1367 1437 1751"> <tbody> <tr> <td data-bbox="391 1367 907 1453">NT_SERVICE S-1-5-80</td> <td data-bbox="907 1367 1437 1453">An NT Service account prefix.</td> </tr> <tr> <td data-bbox="391 1453 907 1665">NT VIRTUAL MACHINE\Virtual Machines S-1-5-83-0</td> <td data-bbox="907 1453 1437 1665">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 data-bbox="391 1665 907 1751">USER_MODE_DRIVERS S-1-5-84-0-0-0-0-0</td> <td data-bbox="907 1665 1437 1751">Identifies a user-mode driver process.</td> </tr> </tbody> </table>		NT_SERVICE S-1-5-80	An NT Service account prefix.	USER_MODE_DRIVERS S-1-5-84-0-0-0-0-0	Identifies a user-mode driver process.	NT_SERVICE S-1-5-80	An NT Service account prefix.	NT VIRTUAL MACHINE\Virtual Machines S-1-5-83-0	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).	USER_MODE_DRIVERS S-1-5-84-0-0-0-0-0	Identifies a user-mode driver process.		
NT_SERVICE S-1-5-80	An NT Service account prefix.													
USER_MODE_DRIVERS S-1-5-84-0-0-0-0-0	Identifies a user-mode driver process.													
NT_SERVICE S-1-5-80	An NT Service account prefix.													
NT VIRTUAL MACHINE\Virtual Machines S-1-5-83-0	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).													
USER_MODE_DRIVERS S-1-5-84-0-0-0-0-0	Identifies a user-mode driver process.													
2023/05/16	In section 2.5.1.1, "Syntax," revised grammar to properly treat ! as a unary operator.													

Errata Published*	Description
	<p>Changed from:</p> <ul style="list-style-type: none"> ; 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 <pre>cond-expr = expr expr = super-term [wspace] *(" " [wspace] super-term) super-term = factor [wspace] *("&&" [wspace] factor) factor = ["!"] [wspace] "(" [wspace] factor [wspace] ")" factor = term</pre> <p>Changed to:</p> <ul style="list-style-type: none"> ; 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 <pre>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</pre>

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.



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	<p>In section 3.1.4.2, EFSRPC Interface, added a product behavior note describing change after applying [MSFTE-CVE-2022-26925]:</p> <p>Changed from:</p> <p>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></p> <p>Changed to:</p> <p>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></p> <p><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 Isarpc.</p>																																																																																																																																																																																	
2022/07/26	<p>In section 2.2.2.2.1, Protector List Structure, removed two fields from structure diagram:</p> <p>Changed from:</p> <p>The DDF and DRF Protector List structure in the Version 4 EFSRPC Metadata MUST be formatted as follows.</p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 10%;">0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td> <td style="width: 10%;">1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td> <td style="width: 10%;">2</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td> <td style="width: 10%;">3</td><td>0</td><td>1</td> </tr> <tr> <td colspan="24">StructureSize</td> </tr> <tr> <td colspan="12">ProtectorsCount</td> <td colspan="12">Protector_List_Entry 1 (variable)</td> </tr> <tr> <td colspan="24">...</td> </tr> <tr> <td colspan="24">Protector_List_Entries (variable)</td> </tr> <tr> <td colspan="24">...</td> </tr> <tr> <td colspan="24">Protector_List_Entry ProtectorsCount (variable)</td> </tr> </table>	0	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	0	2	1	2	3	4	5	6	7	8	9	3	0	1	StructureSize																								ProtectorsCount												Protector_List_Entry 1 (variable)												...																								Protector_List_Entries (variable)																								...																								Protector_List_Entry ProtectorsCount (variable)																							
0	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	0	2	1	2	3	4	5	6	7	8	9	3	0	1																																																																																																																																																		
StructureSize																																																																																																																																																																																		
ProtectorsCount												Protector_List_Entry 1 (variable)																																																																																																																																																																						
...																																																																																																																																																																																		
Protector_List_Entries (variable)																																																																																																																																																																																		
...																																																																																																																																																																																		
Protector_List_Entry ProtectorsCount (variable)																																																																																																																																																																																		

Errata Published*	Description																																																																																																																																																																																																
	<div data-bbox="402 226 1112 281" style="border: 1px solid black; text-align: center; padding: 2px;">...</div> <p data-bbox="402 323 532 348">Changed to:</p> <p data-bbox="402 359 1430 411">The DDF and DRF Protector List structure in the Version 4 EFSRPC Metadata MUST be formatted as follows.</p> <table border="1" data-bbox="402 417 1104 844"> <tr> <td style="width: 10px; text-align: center;">0</td><td style="width: 10px; text-align: center;">1</td><td style="width: 10px; text-align: center;">2</td><td style="width: 10px; text-align: center;">3</td><td style="width: 10px; text-align: center;">4</td><td style="width: 10px; text-align: center;">5</td><td style="width: 10px; text-align: center;">6</td><td style="width: 10px; text-align: center;">7</td><td style="width: 10px; text-align: center;">8</td><td style="width: 10px; text-align: center;">9</td> <td style="width: 10px; text-align: center;">0</td><td style="width: 10px; text-align: center;">1</td><td style="width: 10px; text-align: center;">2</td><td style="width: 10px; text-align: center;">3</td><td style="width: 10px; text-align: center;">4</td><td style="width: 10px; text-align: center;">5</td><td style="width: 10px; text-align: center;">6</td><td style="width: 10px; text-align: center;">7</td><td style="width: 10px; text-align: center;">8</td><td style="width: 10px; text-align: center;">9</td> <td style="width: 10px; text-align: center;">0</td><td style="width: 10px; text-align: center;">1</td><td style="width: 10px; text-align: center;">2</td><td style="width: 10px; text-align: center;">3</td><td style="width: 10px; text-align: center;">4</td><td style="width: 10px; text-align: center;">5</td><td style="width: 10px; text-align: center;">6</td><td style="width: 10px; text-align: center;">7</td><td style="width: 10px; text-align: center;">8</td><td style="width: 10px; text-align: center;">9</td> <td style="width: 10px; text-align: center;">0</td><td style="width: 10px; text-align: center;">1</td> </tr> <tr> <td colspan="32" style="text-align: center;">StructureSize</td> </tr> <tr> <td colspan="16" style="text-align: center;">ProtectorsCount</td> <td colspan="16" style="text-align: center;">Protector_List_Entries (variable)</td> </tr> <tr> <td colspan="32" style="text-align: center;">...</td> </tr> <tr> <td colspan="32" style="text-align: center;">...</td> </tr> <tr> <td colspan="32" style="text-align: center;">...</td> </tr> </table>	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	StructureSize																																ProtectorsCount																Protector_List_Entries (variable)																																														
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1																																																																																																																																																																		
StructureSize																																																																																																																																																																																																	
ProtectorsCount																Protector_List_Entries (variable)																																																																																																																																																																																	
...																																																																																																																																																																																																	
...																																																																																																																																																																																																	
...																																																																																																																																																																																																	

*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.

No errata are available for the latest version of 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.

To view a PDF 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	<p>In Section 2.3.4.15, EmfPlusFillClosedCurve Record, amended descriptions of fill operations.</p> <p>Changed from:</p> <p>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....</p> <p>Changed to:</p> <p>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....</p>

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

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

*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.



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

*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.

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	<p>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.</p> <p>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.</p> <p>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.</p>
2022/09/20	<p>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.</p> <p>Changed to: typedef struct _tag_FW_QUERY_CONDITIONS { DWORD dwNumEntries; [size_is(dwNumEntries)] FW_QUERY_CONDITION *AndedConditions; } FW_QUERY_CONDITIONS, *PFW_QUERY_CONDITIONS;</p>

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

[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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.



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

Errata Published*	Description																										
2023/01/30	<p>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.</p> <p>Changed from:</p> <p><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.</p> <table border="1" data-bbox="386 678 1429 1178"> <thead> <tr> <th>File system</th> <th>Support value of -2</th> </tr> </thead> <tbody> <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> </tbody> </table> <p><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.</p> <table border="1" data-bbox="386 1539 1429 1789"> <thead> <tr> <th>File system</th> <th>Support value of -2</th> </tr> </thead> <tbody> <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> </tbody> </table>	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 operating system and later	ReFS	Windows 10 v1507 operating system and later, Windows Server 2016 and later, and Windows Server v1709 and later	File system	Support value of -2	FAT	No	EXFAT	No	FAT32	No	Cdfs	No
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 operating system and later																										
ReFS	Windows 10 v1507 operating system and later, Windows Server 2016 and later, and Windows Server v1709 and later																										
File system	Support value of -2																										
FAT	No																										
EXFAT	No																										
FAT32	No																										
Cdfs	No																										

Errata Published*	Description																	
	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																
	<p><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.</p>																	
	<table border="1"> <thead> <tr> <th data-bbox="386 846 906 888">File system</th> <th data-bbox="906 846 1429 888">Support value of -2</th> </tr> </thead> <tbody> <tr> <td data-bbox="386 888 906 940">FAT</td> <td data-bbox="906 888 1429 940">No</td> </tr> <tr> <td data-bbox="386 940 906 993">EXFAT</td> <td data-bbox="906 940 1429 993">No</td> </tr> <tr> <td data-bbox="386 993 906 1045">FAT32</td> <td data-bbox="906 993 1429 1045">No</td> </tr> <tr> <td data-bbox="386 1045 906 1098">Cdfs</td> <td data-bbox="906 1045 1429 1098">No</td> </tr> <tr> <td data-bbox="386 1098 906 1150">UDFS</td> <td data-bbox="906 1098 1429 1150">No</td> </tr> <tr> <td data-bbox="386 1150 906 1245">NTFS</td> <td data-bbox="906 1150 1429 1245">Windows 8.1 and later, Windows Server 2012 R2 and later and Windows Server v1709 and later</td> </tr> <tr> <td data-bbox="386 1245 906 1339">ReFS</td> <td data-bbox="906 1245 1429 1339">Windows 10 v1507 and later, Windows Server 2016 and later, and Windows Server v1709 and later</td> </tr> </tbody> </table>		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
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																	
	<p><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.</p>																	
	<table border="1"> <thead> <tr> <th data-bbox="386 1707 906 1749">File system</th> <th data-bbox="906 1707 1429 1749">Support value of -2</th> </tr> </thead> <tbody> <tr> <td data-bbox="386 1749 906 1799">FAT</td> <td data-bbox="906 1749 1429 1799">No</td> </tr> </tbody> </table>		File system	Support value of -2	FAT	No												
File system	Support value of -2																	
FAT	No																	

Errata Published*	Description																	
	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																
	<p data-bbox="370 667 418 688">☐</p> <p data-bbox="370 695 505 716">Changed to:</p> <p data-bbox="370 722 1429 1031"><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.</p> <table border="1" data-bbox="386 1041 1425 1486"> <thead> <tr> <th data-bbox="386 1041 906 1094">File system</th> <th data-bbox="906 1041 1425 1094">Support value of -2</th> </tr> </thead> <tbody> <tr> <td data-bbox="386 1094 906 1140">FAT</td> <td data-bbox="906 1094 1425 1140">No</td> </tr> <tr> <td data-bbox="386 1140 906 1186">EXFAT</td> <td data-bbox="906 1140 1425 1186">No</td> </tr> <tr> <td data-bbox="386 1186 906 1232">FAT32</td> <td data-bbox="906 1186 1425 1232">No</td> </tr> <tr> <td data-bbox="386 1232 906 1278">Cdfs</td> <td data-bbox="906 1232 1425 1278">No</td> </tr> <tr> <td data-bbox="386 1278 906 1325">UDFS</td> <td data-bbox="906 1278 1425 1325">No</td> </tr> <tr> <td data-bbox="386 1325 906 1409">NTFS</td> <td data-bbox="906 1325 1425 1409">Windows 8.1 and later, and Windows Server 2012 R2 and later</td> </tr> <tr> <td data-bbox="386 1409 906 1486">ReFS</td> <td data-bbox="906 1409 1425 1486">Windows 10 v1507 operating system and later, and Windows Server 2016 and later</td> </tr> </tbody> </table> <p data-bbox="370 1535 1429 1814"><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 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</p>		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
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																	

Errata Published*	Description																																
	<p>response to file system calls such as read and write.</p> <table border="1" data-bbox="386 258 1425 709"> <thead> <tr> <th>File system</th> <th>Support value of -2</th> </tr> </thead> <tbody> <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> </tbody> </table> <p><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.</p> <table border="1" data-bbox="386 1066 1425 1518"> <thead> <tr> <th>File system</th> <th>Support value of -2</th> </tr> </thead> <tbody> <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> </tbody> </table> <p><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 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</p>	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 and later, and Windows Server 2016 and later	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 and later, and Windows Server 2016 and later
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 and later, and Windows Server 2016 and later																																
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 and later, and Windows Server 2016 and later																																

Errata Published*	Description																
	<p>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.</p> <table border="1" data-bbox="386 285 1429 730"> <thead> <tr> <th data-bbox="386 285 906 331">File system</th> <th data-bbox="906 285 1429 331">Support value of -2</th> </tr> </thead> <tbody> <tr> <td data-bbox="386 331 906 384">FAT</td> <td data-bbox="906 331 1429 384">No</td> </tr> <tr> <td data-bbox="386 384 906 436">EXFAT</td> <td data-bbox="906 384 1429 436">No</td> </tr> <tr> <td data-bbox="386 436 906 489">FAT32</td> <td data-bbox="906 436 1429 489">No</td> </tr> <tr> <td data-bbox="386 489 906 541">Cdfs</td> <td data-bbox="906 489 1429 541">No</td> </tr> <tr> <td data-bbox="386 541 906 594">UDFS</td> <td data-bbox="906 541 1429 594">No</td> </tr> <tr> <td data-bbox="386 594 906 657">NTFS</td> <td data-bbox="906 594 1429 657">Windows 8.1 and later, and Windows Server 2012 R2 and later</td> </tr> <tr> <td data-bbox="386 657 906 730">ReFS</td> <td data-bbox="906 657 1429 730">Windows 10 v1507 and later, and Windows Server 2016 and later</td> </tr> </tbody> </table>	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 and later, and Windows Server 2016 and later
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 and later, and Windows Server 2016 and later																
2023/01/10	<p>In section 2.3.74, FSCTL_SET_INTEGRITY_INFORMATION Reply, added STATUS_NOT_SUPPORTED to the error codes list: Changed from:</p> <table border="1" data-bbox="386 846 1429 1297"> <thead> <tr> <th data-bbox="386 846 816 898">Error code</th> <th data-bbox="816 846 1429 898">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="386 898 816 1129">STATUS_INVALID_PARAMETER 0xC000000D</td> <td data-bbox="816 898 1429 1129">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 data-bbox="386 1129 816 1213">STATUS_INVALID_DEVICE_REQUEST 0xC0000010</td> <td data-bbox="816 1129 1429 1213">The volume does not support integrity.</td> </tr> <tr> <td data-bbox="386 1213 816 1297">STATUS_DISK_FULL 0xC000007F</td> <td data-bbox="816 1213 1429 1297">The disk is full.</td> </tr> </tbody> </table> <p>Changed to:</p> <table border="1" data-bbox="386 1371 1429 1822"> <thead> <tr> <th data-bbox="386 1371 816 1423">Error code</th> <th data-bbox="816 1371 1429 1423">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="386 1423 816 1654">STATUS_INVALID_PARAMETER 0xC000000D</td> <td data-bbox="816 1423 1429 1654">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 data-bbox="386 1654 816 1738">STATUS_INVALID_DEVICE_REQUEST 0xC0000010</td> <td data-bbox="816 1654 1429 1738">The volume does not support integrity.</td> </tr> <tr> <td data-bbox="386 1738 816 1822">STATUS_DISK_FULL 0xC000007F</td> <td data-bbox="816 1738 1429 1822">The disk is full.</td> </tr> </tbody> </table>	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 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.	STATUS_INVALID_DEVICE_REQUEST 0xC0000010	The volume does not support integrity.	STATUS_DISK_FULL 0xC000007F	The disk is full.	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 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.	STATUS_INVALID_DEVICE_REQUEST 0xC0000010	The volume does not support integrity.	STATUS_DISK_FULL 0xC000007F	The disk is full.
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 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.																
STATUS_INVALID_DEVICE_REQUEST 0xC0000010	The volume does not support integrity.																
STATUS_DISK_FULL 0xC000007F	The disk is full.																
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 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.																
STATUS_INVALID_DEVICE_REQUEST 0xC0000010	The volume does not support integrity.																
STATUS_DISK_FULL 0xC000007F	The disk is full.																

Errata Published*	Description																	
	<table border="1"> <tr> <td data-bbox="362 226 816 310">STATUS_NOT_SUPPORTED 0xC00000BB</td> <td data-bbox="816 226 1429 310">The file has been ghosted (allocation blocks are being shared).</td> </tr> </table>	STATUS_NOT_SUPPORTED 0xC00000BB	The file has been ghosted (allocation blocks are being shared).	<p>In section 2.3.75, FSCTL_SET_INTEGRITY_INFORMATION_EX Request, revised note <76> to indicate which versions support this request:</p> <p>Changed from:</p> <p><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].</p> <p>Changed to:</p> <p><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].</p> <p>In section 2.3.76, FSCTL_SET_INTEGRITY_INFORMATION_EX Reply, added STATUS_NOT_SUPPORTED to the error codes list:</p> <p>Changed from:</p> <table border="1" data-bbox="386 1014 1429 1388"> <thead> <tr> <th data-bbox="386 1014 816 1066">Error code</th> <th data-bbox="816 1014 1429 1066">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="386 1066 816 1220">STATUS_INVALID_PARAMETER 0xC000000D</td> <td data-bbox="816 1066 1429 1220">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.</td> </tr> <tr> <td data-bbox="386 1220 816 1304">STATUS_INVALID_DEVICE_REQUEST 0xC0000010</td> <td data-bbox="816 1220 1429 1304">The volume does not support integrity.</td> </tr> <tr> <td data-bbox="386 1304 816 1388">STATUS_DISK_FULL 0xC000007F</td> <td data-bbox="816 1304 1429 1388">The disk is full.</td> </tr> </tbody> </table> <p>Changed to:</p> <table border="1" data-bbox="386 1497 1429 1776"> <thead> <tr> <th data-bbox="386 1497 816 1549">Error code</th> <th data-bbox="816 1497 1429 1549">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="386 1549 816 1703">STATUS_INVALID_PARAMETER 0xC000000D</td> <td data-bbox="816 1549 1429 1703">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.</td> </tr> <tr> <td data-bbox="386 1703 816 1776">STATUS_INVALID_DEVICE_REQUEST 0xC0000010</td> <td data-bbox="816 1703 1429 1776">The volume does not support integrity.</td> </tr> </tbody> </table>	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.	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_NOT_SUPPORTED 0xC00000BB	The file has been ghosted (allocation blocks are being shared).																	
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.																	
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.																	

Errata Published*	Description																	
	STATUS_DISK_FULL 0xC000007F	The disk is full.																
	STATUS_NOT_SUPPORTED 0xC00000BB	The file has been ghosted (allocation blocks are being shared).																
2022/08/09	<p>In section 2.7.1, FILE_NOTIFY_INFORMATION, revised descriptions of the values in the Action field.</p> <p>Changed from:</p> <table border="1" data-bbox="386 531 1429 894"> <thead> <tr> <th>Value</th> <th>Meaning</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>Changed to:</p> <table border="1" data-bbox="386 972 1429 1417"> <thead> <tr> <th>Value</th> <th>Meaning</th> </tr> </thead> <tbody> <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> </tbody> </table>		Value	Meaning	FILE_ACTION_ADDED 0x00000001	The file was added to the directory.	FILE_ACTION_REMOVED 0x00000002	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.	FILE_ACTION_MODIFIED 0x00000003	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.	Value	Meaning	FILE_ACTION_ADDED 0x00000001	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.	FILE_ACTION_REMOVED 0x00000002	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.	FILE_ACTION_MODIFIED 0x00000003	The file was modified. This can be a change to the data or attributes of the file.
Value	Meaning																	
FILE_ACTION_ADDED 0x00000001	The file was added to the directory.																	
FILE_ACTION_REMOVED 0x00000002	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.																	
FILE_ACTION_MODIFIED 0x00000003	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.																	
Value	Meaning																	
FILE_ACTION_ADDED 0x00000001	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.																	
FILE_ACTION_REMOVED 0x00000002	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.																	
FILE_ACTION_MODIFIED 0x00000003	The file was modified. This can be a change to the data or attributes of the file.																	
2022/05/27	<p>In section 2.3.75, FSCTL_SET_INTEGRITY_INFORMATION_EX Request, updated list of applicable updates.</p> <p>Changed from:</p> <p><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], or [MSKB-5014023].</p> <p>Changed to:</p> <p><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</p>																	

Errata Published*	Description
	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	<p>In Section 2.1.5.9.34, FSCTL_SET_INTEGRITY_INFORMATION_EX, updated processing rules for system versions.</p> <p>Changed from:</p> <p>The server provides:<127></p> <p><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).</p> <p>Changed to:</p> <p>The server provides:<127></p> <p><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].</p>

[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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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-GKDI]: Group Key Distribution Protocol

This topic lists Errata found in [MS-GKDI] 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.

Errata below are for Protocol Document Version [V8.0 - 2021/06/25](#).

Errata Published*	Description																																																																																																																																																																
2023/08/16	<p>Section 2.2.4 Group Key Envelope</p> <p>Description: In the Group Key Envelope structure, updated the 'IsPublicKey' field by renaming it to 'dwFlags' and specifying bit settings that enable this structure to transport a public key or to be used for encrypting new data.</p> <p>Changed from:</p> <table border="1" data-bbox="383 751 1260 905"> <tr> <th colspan="4">Version</th> </tr> <tr> <td>0x4B</td> <td>0x44</td> <td>0x53</td> <td>0x4B</td> </tr> <tr> <td colspan="4">IsPublicKey</td> </tr> </table> <p>Changed to:</p> <table border="1" data-bbox="383 982 1260 1136"> <tr> <th colspan="2">Version</th> </tr> <tr> <td>0x53</td> <td></td> </tr> <tr> <td colspan="2">dwFlags</td> </tr> </table> <p>Changed from:</p> <p>"IsPublicKey (4 bytes): A 32-bit unsigned integer. This field MUST be set to 1 when this structure is being used to transport a public key, and otherwise set to 0. This field is encoded using little-endian format."</p> <p>Changed to:</p> <p>"dwFlags (4 bytes): A 32-bit unsigned integer. Bit 31 (LSB) MUST be set to 1 when this structure is being used to transport a public key, and otherwise set to 0. Bit 30, when set to 1, indicates that this key can be used for encrypting new data. This field is encoded using little-endian format."</p>	Version				0x4B	0x44	0x53	0x4B	IsPublicKey				Version		0x53		dwFlags																																																																																																																																															
Version																																																																																																																																																																	
0x4B	0x44	0x53	0x4B																																																																																																																																																														
IsPublicKey																																																																																																																																																																	
Version																																																																																																																																																																	
0x53																																																																																																																																																																	
dwFlags																																																																																																																																																																	
2023/08/16	<p>Section 2.2.4 Group Key Envelope: Changed isPublicKey to dwFlags and updated requirements for usage of bit 31 to indicate public key transportation and bit 30 to indicate the use of encryption.</p> <table border="1" data-bbox="367 1457 1429 1745"> <tr> <td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td> </tr> <tr> <td colspan="32">Version</td> </tr> <tr> <td colspan="8">0x4B</td> <td colspan="8">0x44</td> <td colspan="8">0x53</td> <td colspan="8">0x4B</td> </tr> <tr> <td colspan="32">isPublicKey</td> </tr> <tr> <td colspan="32">... etc...</td> </tr> </table> <p>...</p> <p>isPublicKey (4 bytes): A 32-bit unsigned integer. This field MUST be set to 1 when this structure is</p>	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	Version																																0x4B								0x44								0x53								0x4B								isPublicKey																																... etc...																															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1																																																																																																																																		
Version																																																																																																																																																																	
0x4B								0x44								0x53								0x4B																																																																																																																																									
isPublicKey																																																																																																																																																																	
... etc...																																																																																																																																																																	

Errata Published*	Description																																																																																																																																																																
	<p>being used to transport a public key, and otherwise set to 0. This field is encoded using little-endian format.</p> <p>...</p> <p>cbL1Key (4 bytes): A 32-bit unsigned integer. This field MUST be the length, in bytes, of the L1 key field. This field is encoded using little-endian format. This field MUST be set to zero if the isPublicKey field is set to 1, or if the L1 index field is set to zero and the value in the L2 index field is not equal to 31.</p> <p>...</p> <p>L2 key (variable, optional): The L2 seed key ADM element or the group public key ADM element with group key identifier (L0 index, L1 index, L2 index) in binary form. If the value in the cbL2Key field is zero, this field is absent. If this field is present and the isPublicKey field is set to 1, then the length, in bytes, of this field MUST be equal to the value of the Public Key Length field. If this field is present and the isPublicKey field is set to 0, the length of this field MUST be equal to 64 bytes.</p> <p>Changed to:</p> <table border="1" data-bbox="367 632 1433 921"> <tr> <td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td> </tr> <tr> <td colspan="32" style="text-align: center;">Version</td> </tr> <tr> <td colspan="8" style="text-align: center;">0x4B</td> <td colspan="8" style="text-align: center;">0x44</td> <td colspan="8" style="text-align: center;">0x53</td> <td colspan="8" style="text-align: center;">0x4B</td> </tr> <tr> <td colspan="32" style="text-align: center;">dwFlags</td> </tr> <tr> <td colspan="32" style="text-align: center;">... etc...</td> </tr> </table> <p>...</p> <p>dwFlags (4 bytes): A 32-bit unsigned integer. Bit 31 (LSB) MUST be set to 1 when this structure is being used to transport a public key, otherwise set to 0. Bit 30 MUST be set to 1 when the key being transported by this structure might be used for encryption and decryption, otherwise it should only be used for decryption. This field is encoded using little-endian format.</p> <p>...</p> <p>cbL1Key (4 bytes): A 32-bit unsigned integer. This field MUST be the length, in bytes, of the L1 key field. This field is encoded using little-endian format. This field MUST be set to zero if bit 31 of the dwFlags field is set to 1, or if the L1 index field is set to zero and the value in the L2 index field is not equal to 31.</p> <p>...</p> <p>L2 key (variable, optional): The L2 seed key ADM element or the group public key ADM element with group key identifier (L0 index, L1 index, L2 index) in binary form. If the value in the cbL2Key field is zero, this field is absent. If this field is present and bit 31 of the dwFlags field is set to 1, then the length, in bytes, of this field MUST be equal to the value of the Public Key Length field. If this field is present and bit 31 of the dwFlags field is set to 0, the length of this field MUST be equal to 64 bytes.</p> <p>Section 3.2.4.1 Client Side Processing: Changed isPublicKey to bit 31 of the dwFlags field.</p> <p>Changed from:</p> <p>If the client successfully retrieves a key from the server, it will have received a group key in the format specified in section 2.2.4. The client MUST parse this format as follows:</p> <ol style="list-style-type: none"> 1. If the isPublicKey field of the returned Group Key Envelope is set to 1, the value in the L2 key field is a public key with group key identifier (L0 field, L1 field, L2 field). 2. If the isPublicKey field of the returned Group Key Envelope is set to 0 and the L2 Key field is present, the value in the L2 key field is an L2 seed key with group key identifier (L0 field, L1 field, L2 field). 3. If the isPublicKey field of the returned Group Key Envelope is set to 0 and the L1 Key field is present, then: <p>Changed to:</p>	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	Version																																0x4B								0x44								0x53								0x4B								dwFlags																																... etc...																															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1																																																																																																																																		
Version																																																																																																																																																																	
0x4B								0x44								0x53								0x4B																																																																																																																																									
dwFlags																																																																																																																																																																	
... etc...																																																																																																																																																																	

Errata Published*	Description
	<p>If the client successfully retrieves a key from the server, it will have received a group key in the format specified in section 2.2.4. The client MUST parse this format as follows:</p> <ol style="list-style-type: none"> 1. If bit 31 of the dwFlags field of the returned Group Key Envelope is set to 1, the value in the L2 key field is a public key with group key identifier (L0 field, L1 field, L2 field). 2. If bit 31 of the dwFlags field of the returned Group Key Envelope is set to 0 and the L2 Key field is present, the value in the L2 key field is an L2 seed key with group key identifier (L0 field, L1 field, L2 field). 3. If bit 31 of the dwFlags field of the returned Group Key Envelope is set to 0 and the L1 Key field is present, then:

*Date format: YYYY/MM/DD

[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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

To view a PDF 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	<p>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.</p> <p>Changed from:</p> <p>KILE MUST<23> support the Advanced Encryption Standard (AES) encryption types:</p> <ul style="list-style-type: none">• AES256-CTS-HMAC-SHA1-96 [18] (RFC3962 section 7)• AES128-CTS-HMAC-SHA1-96 [17] (RFC3962 section 7) <p>and SHOULD<24> support the following encryption types, which are listed in order of relative strength:</p> <ul style="list-style-type: none">• RC4-HMAC [23] RFC4757• DES-CBC-MD5 [3] RFC3961• DES-CBC-CRC [1] RFC3961 <p>Kerberos V5 encryption type assigned numbers are specified in RFC3961 section 8, RFC4757 section 5, and RFC3962 section 7.<25></p> <p><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.</p> <p>RC4-HMAC is supported in Windows.</p> <p>Only Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 support DES by default.</p>

Errata Published*	Description
	<p>Changed to:</p> <p>KILE MUST<23> support the Advanced Encryption Standard (AES) encryption types:</p> <ul style="list-style-type: none"> • AES256-CTS-HMAC-SHA1-96 [18] ([RFC3962] section 7) • AES128-CTS-HMAC-SHA1-96 [17] ([RFC3962] section 7) <p>and SHOULD<24> support the following encryption types, which are listed in order of relative strength:</p> <ul style="list-style-type: none"> • RC4-HMAC [23] [RFC4757] • DES-CBC-MD5 [3] [RFC3961] • DES-CBC-CRC [1] [RFC3961] <p>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></p> <p><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.</p> <p>Only Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 support DES by default.</p> <p>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.</p> <p><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.</p>
2023/03/06	<p>Section 5.1 Security Considerations for Implementers: Added statement to recommend strong vs. weak encryption usage.</p> <p>Changed from:</p> <p>5.1 Security Considerations for Implementers</p> <p>KILE has the same security considerations as Kerberos V5 ([RFC4120], [RFC3961], [RFC3962], and [RFC4757]) and GSS-API ([RFC2743], [RFC1964], and [RFC4121]).</p> <p>Changed to:</p> <p>5.1 Security Considerations for Implementers</p> <p>KILE has the same security considerations as Kerberos V5 ([RFC4120], [RFC3961], [RFC3962], and [RFC4757]) and GSS-API ([RFC2743], [RFC1964], and [RFC4121]).</p> <p>The encryption types AES128-CTS-HMAC-SHA1-96/AES256-CTS-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.</p>
2023/03/06	<p>Section 2.2.7 Supported Encryption Types Bit Flags: Added note to recommend strong vs. weak encryption usage.</p>

Errata Published*	Description
	<p>Changed from:</p> <p>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.</p> <p>All other bits MUST be set to zero when sent and MUST be ignored when they are received.</p> <p>Changed to:</p> <p>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.</p> <p>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.</p> <p>All other bits MUST be set to zero when sent and MUST be ignored when they are received.</p>

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

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](#).

Errata Published *	Description						
2022/05/02	<p>In Section 2.2, LCID Structure, added the following language IDs to the table:</p> <p>0x2000 Unassigned LCID locale temporarily assigned to LCID 0x3000. See section 2.2.1.</p> <p>0x2400 Unassigned LCID locale temporarily assigned to LCID 0x3000. See section 2.2.1.</p> <p>0x2800 Unassigned LCID locale temporarily assigned to LCID 0x3000. See section 2.2.1.</p> <p>0x2C00 Unassigned LCID locale temporarily assigned to LCID 0x3000. See section 2.2.1.</p> <p>In Section 2.2.1, Locale Names without LCIDs, updated the table:</p> <p>Changed from:</p> <table border="1"><thead><tr><th>Name</th><th>Value</th><th>Conditions</th></tr></thead><tbody><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 a 1-to-</td></tr></tbody></table>	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-
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-					

Errata Published *	Description		
			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, 0x4800, 0x4C00	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 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	

Errata Published *	Description		
			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.

To view a PDF 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](#).

Errata Published*	Description																				
2022/09/20	<p>In Section 2.2.1.4, AEAD-AES-256-CBC-HMAC-SHA512 Constants</p> <p>Description: Updated AEAD-AES-256-CBC-HMAC-SHA512 constants to ensure that the value details allow an implementation to be successfully created.</p> <p>Changed from:</p> <table border="1"><thead><tr><th>Constant Name</th><th>Value</th></tr></thead><tbody><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></tbody></table> <p>Changed to:</p> <table border="1"><thead><tr><th>Constant Name</th><th>Meaning</th></tr></thead><tbody><tr><td>Versionbyte</td><td>Version identifier</td></tr></tbody></table>	Constant Name	Value	versionbyte	0x01	versionbyte_length	1	SAM_AES_256_ALG	"AEAD-AES-256-CBC-HMAC-SHA512"	SAM_AES256_ENC_KEY_STRING	"Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"	SAM_AES256_MAC_KEY_STRING	"Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"	SAM_AES256_ENC_KEY_STRING_LENGTH	sizeof(SAM_AES256_ENC_KEY_STRING)	SAM_AES256_MAC_KEY_STRING_LENGTH	sizeof(SAM_AES256_MAC_KEY_STRING)	Constant Name	Meaning	Versionbyte	Version identifier
Constant Name	Value																				
versionbyte	0x01																				
versionbyte_length	1																				
SAM_AES_256_ALG	"AEAD-AES-256-CBC-HMAC-SHA512"																				
SAM_AES256_ENC_KEY_STRING	"Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"																				
SAM_AES256_MAC_KEY_STRING	"Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"																				
SAM_AES256_ENC_KEY_STRING_LENGTH	sizeof(SAM_AES256_ENC_KEY_STRING)																				
SAM_AES256_MAC_KEY_STRING_LENGTH	sizeof(SAM_AES256_MAC_KEY_STRING)																				
Constant Name	Meaning																				
Versionbyte	Version identifier																				

Errata Published*	Description															
	0x01															
	versionbyte_length 1	Version identifier length														
	SAM_AES_256_ALG "AEAD-AES-256-CBC-HMAC-SHA512"	A NULL terminated ANSI string														
	SAM_AES256_ENC_KEY_STRING "Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"	A NULL terminated ANSI string														
	SAM_AES256_MAC_KEY_STRING "Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"	A NULL terminated ANSI string														
	SAM_AES256_ENC_KEY_STRING_LENGTH sizeof(SAM_AES256_ENC_KEY_STRING) (61)	The length of SAM_AES256_ENC_KEY_STRING, including the null terminator.														
	SAM_AES256_MAC_KEY_STRING_LENGTH sizeof(SAM_AES256_MAC_KEY_STRING) (54)	The length of SAM_AES256_MAC_KEY_STRING, including the null terminator														
	<p>In Section 5.1.5 AES Cipher Usage Description: Clarified the usage of enc_key and mac_key when encrypting the data.</p> <p>Changed from: "... Let AuthData ::= HMAC-SHA-512(mac_key, versionbyte + IV + Cipher + versionbyte_length)"</p> <p>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."</p>															
2022/01/11	<p>The following sections in the table below are updated or new. Please see the PDF diff document for details.</p> <table border="1" data-bbox="383 1409 1430 1810"> <thead> <tr> <th data-bbox="383 1409 1187 1461">Section</th> <th data-bbox="1187 1409 1430 1461">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="383 1461 1187 1514">1.3 Overview</td> <td data-bbox="1187 1461 1430 1514">Updated</td> </tr> <tr> <td data-bbox="383 1514 1187 1566">1.6 Applicability Statement</td> <td data-bbox="1187 1514 1430 1566">Updated</td> </tr> <tr> <td data-bbox="383 1566 1187 1619">2.2 Common Data Types</td> <td data-bbox="1187 1566 1430 1619">Updated</td> </tr> <tr> <td data-bbox="383 1619 1187 1692">2.2.1.4 AEAD-AES-256-CBC-HMAC-SHA512 Constants</td> <td data-bbox="1187 1619 1430 1692">Created new section</td> </tr> <tr> <td data-bbox="383 1692 1187 1766">2.2.1.5 LSA Trust Record Flags</td> <td data-bbox="1187 1692 1430 1766">Created new section</td> </tr> <tr> <td data-bbox="383 1766 1187 1810">2.2.2.6 LSAPR_REVISION_INFO_V1</td> <td data-bbox="1187 1766 1430 1810">Created new</td> </tr> </tbody> </table>		Section	Description	1.3 Overview	Updated	1.6 Applicability Statement	Updated	2.2 Common Data Types	Updated	2.2.1.4 AEAD-AES-256-CBC-HMAC-SHA512 Constants	Created new section	2.2.1.5 LSA Trust Record Flags	Created new section	2.2.2.6 LSAPR_REVISION_INFO_V1	Created new
Section	Description															
1.3 Overview	Updated															
1.6 Applicability Statement	Updated															
2.2 Common Data Types	Updated															
2.2.1.4 AEAD-AES-256-CBC-HMAC-SHA512 Constants	Created new section															
2.2.1.5 LSA Trust Record Flags	Created new section															
2.2.2.6 LSAPR_REVISION_INFO_V1	Created new															

Errata Published*	Description	
		section
	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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

To view a PDF 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](#).

Errata Published *	Description												
2023/06/12	<p>In Section 2.2.10 Faults: added CustomServerError message to the detail element table with product behavior note for applicability.</p> <p>Changed from:</p> <table border="1"><thead><tr><th>Subcode</th><th>Error</th><th>Description</th><th>HRESULT</th></tr></thead><tbody><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 calling admin. User</td><td>80180014</td></tr></tbody></table>	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	80180014
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	80180014										

Errata Published *	Description			
			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 data. The server may not be configured correctly.	80180019

Errata Published *	Description			
	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	
UserLicense	MENROLL_E_USERLICENSE	License of user is in bad state and blocking the enrollment. The user needs to call the admin.	80180018	

Errata Published *	Description			
	InvalidEnrollmentData	MENROLL_E_ENROLLMENTDATAINVALID	The server rejected the enrollment data. The server may not be configured correctly.	80180019
	CustomServerError	MENROLL_E_CUSTOMSERVERERROR	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>	80180032
	<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.			
2022/12/30	<p><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.</p> <p>Changed From:</p> <p>RequestVersion value 5.0 is supported only in the Windows 11 (version 1) 2022 10C patch and later.</p> <p>Changed To:</p> <p>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.</p> <p>In the following sections' product notes for EnrollmentVersion v5.0 added supported in Windows 10 v2004 (v20H1) 2023 1C patch and later.</p> <p><15> Section 3.1.4.1.3.2 DiscoveryResponse</p> <p><16> Section 3.3.4.1.1.2 GetPoliciesResponse</p> <p><17> Section 3.3.4.1.1.2 GetPoliciesResponse</p> <p><20> Section 3.4.4.1.1.1.1 RequestSecurityToken using Federated Authentication</p> <p><23> Section 3.4.4.1.1.1.2 RequestSecurityToken using Certificate Authentication</p> <p><26> Section 3.4.4.1.1.1.3 RequestSecurityToken using On-Premise Authentication</p> <p>Changed From:</p>			

Errata Published *	Description
	<p>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.</p> <p>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.</p>
2022/10/03	<p><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.</p> <p>Changed From: RequestVersion value 5.0 is supported only in the Windows 11, version 22H2 operating system and later.</p> <p>Changed To: RequestVersion value 5.0 is supported only in Windows 11 (version 1), 2022 10C patch and later.</p> <p>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.</p> <p><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 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</p> <p>Changed From: EnrollmentVersion value 5.0 is supported only in Windows 11 v22H2 and later, see section 3.1.4.1.3.2.</p> <p>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.</p>

[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.

To view a PDF 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	<p>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.</p> <p>Changed from:</p> <p>Windows Azure Virtual Desktop (AVD) supports multiple users that can log on simultaneously.<16></p> <p><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).</p> <p>Changed to:</p> <p>Windows Azure Virtual Desktop (AVD) supports multiple users that can log on simultaneously.<16></p> <p><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.</p>
2022/06/14	<p>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.</p> <p>Changed from:</p> <p>...</p> <p>Note 8: If the server has set EntDMID in the DMClient configuration service provider, the client</p>

Errata Published*	Description
	<p>adds client-request-id to the header and sets it to the value of EntDMID.<9> See [MSDOCS-DMClient-CSP] for more information.</p> <p>Changed to:</p> <p>. . .</p> <p>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.</p> <p>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.</p> <p>DeviceToken: CI6MTQxmCF5xgu6yYcmV9ng6vhQfaJYw...</p> <p>See [MSDOCS-DMClient-CSP] for more information.<10></p> <p>Appendix B:</p> <p><10> Section 2.1: Not available in Windows 10 v19H2 and earlier.</p>
2022/05/02	<p>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.</p> <p>Changed from:</p> <p>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...</p> <p>Changed to:</p> <p>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...</p> <p><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).</p>

[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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.



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	<p>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.</p> <p>Section 3.1.5.5.4 inboundNatRules, updated product note 8 Support for the enableTcpReset property backport to Windows Server 2019 with HCI.</p> <p>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.</p> <p>Section 3.1.5.5.4 inboundNatRules, updated product note 8 Support for the enableTcpReset property backport to Windows Server 2019 with HCI.</p> <p>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.</p> <p>Section 3.1.5.5.6 outboundNatRules, added property idleTimeoutInMinutes with version v4.2. Updated product note backport to Windows Server 2019 with HCI.</p> <p>Section 3.1.5.11 networkInterfaces, Updated QosSettings , enableHardwareLimits support from version v4 to version v3.1.</p> <p>Section 3.1.5.26 virtualSwitchManager, added enableHardwareLimits version support statement with v3.1.</p> <p>Section 6.5.6.1 PUT schema Section 6.5.6.2 GET schema Section 6.5.6.3 GET ALL schema Section 6.5.7.1 PUT schema Section 6.5.7.2 GET schema</p>

Errata Published*	Description
	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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.



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	<p>In section 2.2.1.2 CHALLENGE_MESSAGE: Added statement that the server MUST return the NTLMSSP_NEGOTIATE_SIGN if set by the client.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>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.</p>

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.

No errata are available for the latest version of 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.

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	<p>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.</p> <p>Changed from:</p> <p>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).</p> <p>Changed to:</p> <p>PayloadSize (4 bytes): The unsigned size, in bytes, of the Payload field. The maximum value for this field is 0x0000FC30 (64,560).</p>

*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.

Errata below are for Protocol Document Version [V12.0 - 2019/03/13](#).

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

*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.

To view a PDF 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
2023/07/18	<p>Please see the diff document for details of the changes.</p> <p>Section 2.2.1.3.14 NETLOGON_CAPABILITIES: Added case (2) RequestedFlags.</p> <p>Changed from:</p> <p>The NETLOGON_CAPABILITIES union SHOULD<33> carry the supported Netlogon capabilities.</p> <pre>typedef [switch_type(DWORD)] union _NETLOGON_CAPABILITIES { [case(1)] ULONG ServerCapabilities; } NETLOGON_CAPABILITIES, *PNETLOGON_CAPABILITIES;</pre> <p>ServerCapabilities: A 32-bit set of bit flags that identify the server's capabilities (section 3.5.4.4.10).</p> <p><33> Section 2.2.1.3.14: The NETLOGON_CAPABILITIES union is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.</p>

Errata Published*	Description
	<p>Changed to:</p> <p>The NETLOGON_CAPABILITIES union SHOULD<33> carry the supported Netlogon capabilities.</p> <pre>typedef [switch_type(DWORD)] union _NETLOGON_CAPABILITIES { [case(1)] ULONG ServerCapabilities; [case(2)] ULONG RequestedFlags; } NETLOGON_CAPABILITIES, *PNETLOGON_CAPABILITIES;</pre> <p>ServerCapabilities: A 32-bit set of bit flags that identify the server's capabilities (section 3.5.4.4.10).</p> <p>RequestedFlags: A 32-bit set of bit flags that identify the client capabilities that server received during negotiation (section 3.5.4.4.10).</p> <p><33> Section 2.2.1.3.14: The NETLOGON_CAPABILITIES union is not supported in Windows NT, Windows 2000, Windows XP, and Windows Server 2003.</p> <p>Section 3 Protocol Details: Added common error processing rule F expected response STATUS_INVALID_LEVEL for unsupported RPC tags seen for any Netlogon RPC requests.</p> <p>Section 3.1.1 Abstract Data Model: Added RequestedFlags to the abstract variables of the session key operations.</p> <p>Changed from:</p> <p>NegotiateFlags: A 32-bit set of bit flags that identify the negotiated capabilities between the client and the server.</p> <p>ServerStoredCredential: A NETLOGON_CREDENTIAL structure containing the credential that is created by the server and received by the client and that is used during computation and verification of the Netlogon authenticator.</p> <p>Changed to:</p> <p>NegotiateFlags: A 32-bit set of bit flags that identify the negotiated capabilities between the client and the server.</p> <p>RequestedFlags: A 32-bit set of bit flags that identify the client capabilities sent by client to server in negotiation request.</p> <p>ServerStoredCredential: A NETLOGON_CREDENTIAL structure containing the credential that is created by the server and received by the client and that is used during computation and verification of the Netlogon authenticator.</p> <p>Section 3.1.4.1 Session-Key Negotiation: Updated Client-Server processing to include Negotiated flags and Requested flags.</p> <p>Changed from:</p> <ol style="list-style-type: none"> 11. The client calls the NetrLogonGetCapabilities method (section 3.4.5.2.10). 12. The server SHOULD return the negotiated flags for the current exchange. 13. The client SHOULD compare the received ServerCapabilities (section 3.5.4.4.10) with the negotiated NegotiateFlags (section 3.5.4.4.2), and if there is a difference, the session

Errata Published*	Description
	<p>key negotiation is aborted.</p> <p>14. The client sets the ServerSessionInfo.LastAuthenticationTry (indexed by server name) to the current time. This prevents authentication retries from occurring for 45 seconds unless a new transport notification is received.</p> <p><71> Section 3.1.4.1: Returning the negotiated flags for the current exchange is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.</p> <p><72> Section 3.1.4.1: Comparing the received ServerCapabilities with the negotiated NegotiateFlags is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.</p> <p>Changed to:</p> <p>11. The client calls the NetrLogonGetCapabilities method to get Negotiated flags by setting QueryLevel to 1 (section 3.4.5.2.10).</p> <p>12. The server SHOULD<73> return the negotiated flags for the current exchange.</p> <p>13. The client SHOULD<74> compare the received ServerCapabilities (section 3.5.4.4.10) with the negotiated NegotiateFlags (section 3.5.4.4.2), and if there is a difference, the session key negotiation is aborted.</p> <p>14. The client calls the NetrLogonGetCapabilities method to get Requested flags by setting QueryLevel to 2 (section 3.4.5.2.10).</p> <p>15. The server SHOULD<75> return the client capabilities received during a negotiation request from client.</p> <p>16. The client SHOULD<76> compare the received Requested flags(section 3.5.4.4.10) with the flags it has actually sent during negotiation (section 3.5.4.4.2), and if there is a difference, the session key negotiation is aborted.</p> <p>17. The client sets the ServerSessionInfo.LastAuthenticationTry (indexed by server name) to the current time. This prevents authentication retries from occurring for 45 seconds unless a new transport notification is received.</p> <p><72> Section 3.1.4.1: Returning the negotiated flags or received client flags for the current exchange is not supported in Windows NT, Windows 2000, Windows XP, and Windows Server 2003.</p> <p><73> Section 3.1.4.1: Comparing the received ServerCapabilitiesCapabilities with the negotiated NegotiateFlags or RequestedFlags is not supported in Windows NT, Windows 2000, Windows XP, and Windows Server 2003.</p> <p><74> Section 3.1.4.1: Returning the negotiated flags or received client flags for the current exchange is not supported in Windows NT, Windows 2000, Windows XP, and Windows Server 2003.</p> <p><75> Section 3.1.4.1: Comparing the received Capabilities with the negotiated NegotiateFlags or RequestedFlags is not supported in Windows NT, Windows 2000, Windows XP, and Windows Server 2003.</p> <p>Section 3.4.1 Abstract Data Model: Updated Client-Server processing to include NegotiateFlags and RequestedFlags.</p> <p>Changed from:</p> <ul style="list-style-type: none"> • ConnectionStatus: See section 3.1.1 for ClientStoredCredential details. • LastAuthenticationTry: A FILETIME ([MS-DTYP] section 2.3.3) indicating the time when the last authentication attempt was made. The time stamp is used to determine if at least 45 seconds have passed since the last authentication attempt. <p>Changed to:</p>

Errata Published*	Description
	<ul style="list-style-type: none"> • ConnectionStatus: See section 3.1.1 for ClientStoredCredential details. • LastAuthenticationTry: A FILETIME ([MS-DTYP] section 2.3.3) indicating the time when the last authentication attempt was made. The time stamp is used to determine if at least 45 seconds have passed since the last authentication attempt. • RequestedFlags: See section 3.1.1 for RequestedFlags details <p>Section 3.4.5.2.10 Calling NetrLogonGetCapabilities: Updated processing for the comparison of received Capabilities with negotiated flags.</p> <p>Changed from:</p> <p>After the method returns, the client MUST verify the ReturnAuthenticator (section 3.1.4.5) and compare the received Capabilities with the negotiated flags of the current secure channel. If the negotiated flags do not match, then the client SHOULD<106> re-establish the secure channel with the DC.</p> <p>Upon receiving STATUS_NOT_IMPLEMENTED, the client MUST treat this as successful confirmation that the DC does not support AES [FIPS197].<107></p> <p><101> Section 3.4.5.2.10: NetrLogonGetCapabilities is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008 clients.</p> <p><102> Section 3.4.5.2.10: Re-establishing the secure channel with the DC is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.</p> <p>Changed to:</p> <p>After the method returns, the client MUST verify the ReturnAuthenticator (section 3.1.4.5) and compares the received Capabilities with the negotiated flags of the current secure channel. If the negotiated flags and the requested flags do not match, then the client SHOULD<106> re-establish the secure channel with the DC.</p> <p>On successful comparison of received Capabilities with negotiated flags, client also compares the capabilities sent in the negotiate request with the flags received by the server. If the negotiated flags and requested flags do not match, then the client SHOULD<107> re-establish the secure channel with the DC.</p> <p>Upon receiving STATUS_NOT_IMPLEMENTED, the client MUST treat this as successful confirmation that the DC does not support AES [FIPS197].<107></p> <p><105> Section 3.4.5.2.10: NetrLogonGetCapabilities is not supported by Windows NT, Windows 2000, Windows XP, and Windows Server 2003.</p> <p><106> Section 3.4.5.2.10: Re-establishing the secure channel with the DC is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.</p> <p><107> Section 3.4.5.2.10: Re-establishing the secure channel with the DC is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008.</p> <p>Section 3.5.4 Message Processing Events and Sequencing Rules: Added requested flags to NetrLogonGetCapabilities description.</p> <p>Changed from: NetrLogonGetCapabilities</p>

Errata Published*	Description
	<p>The NetrLogonGetCapabilities method returns server capabilities. Opnum: 21</p> <p>Changed to: NetrLogonGetCapabilities The NetrLogonGetCapabilities method returns server capabilities or requested flags based on input QueryLevel parameter. Opnum: 21</p> <p>Section 3.5.4.4.10 NetrLogonGetCapabilities (Opnum 21): Changed ServerCapabilities to Capabilities to include client capabilities received. Added to QueryLevel case 2 (Hex) to return client capabilities. Updated validation steps.</p> <p>Changed from: The NetrLogonGetCapabilities method is used by clients to confirm the server capabilities after a secure channel has been established.<190> ... QueryLevel: Specifies the level of information to return from the domain controller being queried. A value of 0x00000001 causes return of a NETLOGON_CAPABILITIES structure that contains server capabilities. ServerCapabilities: A pointer to a 32-bit set of bit flags that identify the server's capabilities.<191></p> <p><190> Section 3.5.4.4.10: The NetrLogonGetCapabilities method is not supported in Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. ... <194> Section 3.5.4.4.10: The ServerCapabilities parameter is not supported by Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008. These operating systems supported a dummy buffer type: ... <195> Section 3.5.4.4.10: Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008 do no processing for this call, and always return 0xC0000002 (STATUS_NOT_IMPLEMENTED).</p> <p>Changed to: The NetrLogonGetCapabilities method is used by clients to confirm the server capabilities after a secure channel has been established.<194> ... QueryLevel: Specifies the level of information to return from the domain controller being queried. A value of 0x00000001 causes return of a NETLOGON_CAPABILITIES structure that contains server capabilities. A value of 0x00000002 causes the return of a NETLOGON_CAPABILITIES structure that contains client capabilities received by server when a negotiation request is made from the client. Capabilities: A pointer to a 32-bit set of bit flags that identify the server's capabilities or client's capabilities received by server during negotiation.<195></p> <p><194> Section 3.5.4.4.10: The NetrLogonGetCapabilities method is not supported in</p>

Errata Published*	Description
	<p>Windows NT, Windows 2000, Windows XP, and Windows Server 2003.</p> <p>...</p> <p><195> Section 3.5.4.4.10: The ServerCapabilities parameter is not supported by Windows NT, Windows 2000, Windows XP, and Windows Server 2003. These operating systems supported a dummy buffer type:</p> <p>[out, switch_is(QueryLevel)] PNETLOGON_DUMMY1 Buffer</p> <p>Buffer: A pointer to a byte buffer.</p> <p><196> Section 3.5.4.4.10: Windows NT, Windows 2000, Windows XP, and Windows Server 2003 do no processing for this call, and always return 0xC0000002 (STATUS_NOT_IMPLEMENTED).</p> <p>Section 6 Appendix A: Full IDL: Added to NETLOGON_CAPABILITIES case (2) RequestedFlags and changed NetrLogonGetCapabilities (opnum 21) ServerCapabilities to Capabilities.</p> <p>Changed from:</p> <pre>typedef [switch_type(DWORD)] union _NETLOGON_CAPABILITIES { [case(1)] ULONG ServerCapabilities; } NETLOGON_CAPABILITIES, *PNETLOGON_CAPABILITIES;</pre> <p>NTSTATUS</p> <pre>NetrLogonGetCapabilities([in, string] LOGONSRV_HANDLE ServerName, [in, string, unique] wchar_t* ComputerName, [in] PNETLOGON_AUTHENTICATOR Authenticator, [in, out] PNETLOGON_AUTHENTICATOR ReturnAuthenticator, [in] DWORD QueryLevel, [out, switch_is(QueryLevel)] PNETLOGON_CAPABILITIES ServerCapabilities</pre> <p>Changed to:</p> <pre>typedef [switch_type(DWORD)] union _NETLOGON_CAPABILITIES { [case(1)] ULONG ServerCapabilities; [case(2)] ULONG RequestedFlags; } NETLOGON_CAPABILITIES, *PNETLOGON_CAPABILITIES;</pre> <p>NTSTATUS</p> <pre>NetrLogonGetCapabilities([in, string] LOGONSRV_HANDLE ServerName, [in, string, unique] wchar_t* ComputerName,</pre>

Errata Published*	Description
	<p>[in] PNETLOGON_AUTHENTICATOR Authenticator, [in, out] PNETLOGON_AUTHENTICATOR ReturnAuthenticator, [in] DWORD QueryLevel, [out, switch_is(QueryLevel)] PNETLOGON_CAPABILITIES Capabilities</p>
2022/11/08	<p>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.</p> <p>Changed from:</p> <p>TrustPasswordVersion: ...</p> <p>SealSecureChannel: ...</p> <p>StrongKeySupport: ...</p> <p>The Netlogon client and server variables are as follows:</p> <p>LocatedDCsCache: ...</p> <p>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.</p> <p>Implementations SHOULD<69> persistently store and retrieve the SealSecureChannel variable.</p> <p>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></p> <p>Changed to:</p> <p>TrustPasswordVersion: ...</p> <p>StrongKeySupport: ...</p> <p>The Netlogon client and server variables are as follows:</p> <p>LocatedDCsCache: ...</p> <p>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.</p> <p>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></p> <p>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.</p> <p>Changed from:</p> <p>The client and server follow this sequence of steps.<75></p> <p>1. The client SHOULD<76> bind to the RPC server using TCP/IP.</p>

Errata Published*	Description
	<p>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.</p> <p>2. ...</p> <p>3. ...</p> <p>4. If secure bind is not used, the server MUST deny the request unless client is in the VulnerableChannelAllowList setting.<77></p> <p><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].</p> <p>Changed to:</p> <p>The client and server follow this sequence of steps.<74></p> <p>1. The client SHOULD<75> bind to the RPC server using TCP/IP.</p> <p>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.</p> <p>2. ...</p> <p>3. ...</p> <p>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></p> <p><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].</p> <p>In section 3.4.1 Abstract Data Model: RequireSignOrSeal: Added that this setting MUST be TRUE.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>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.</p>

Errata Published*	Description
	<p>In section 3.4.3 Initialization: Changed RequireSignOrSeal from SHOULD to MUST be initialized to TRUE.</p> <p>Changed from:</p> <p>RequireSignOrSeal SHOULD<92> be initialized to TRUE.</p> <p>Changed to:</p> <p>RequireSignOrSeal MUST<92> be initialized to TRUE.</p> <p>In section 3.5.1 Abstract Data Model: SignSecureChannel: Added This setting is deprecated, as SealSecureChannel MUST be TRUE.</p> <p>Changed from:</p> <p>SignSecureChannel: A Boolean variable that determines whether a domain member attempts to negotiate signing for all secure channel traffic that it initiates.</p> <p>Changed to:</p> <p>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.</p> <p>In Section 3.5.3 Initialization: RejectMD5Clients, SealSecureChannel, and SignSecureChannel set to TRUE.</p> <p>Changed from:</p> <p>RejectMD5Clients SHOULD be initialized in an implementation-specific way and set to FALSE.</p> <p>SealSecureChannel SHOULD be TRUE.</p> <p>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).</p> <p>Changed to:</p> <p>RejectMD5Clients SHOULD be initialized in an implementation-specific way and set to TRUE.</p> <p>SealSecureChannel MUST be TRUE.</p> <p>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.</p>
2022/09/20	In section 1.3.1 Pass-Through Authentication: Added little endian usage statement.

Errata Published*	Description
	<p>Changed from:</p> <p>... 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.</p> <p>Changed to:</p> <p>... 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.</p> <p>In section 2.2.1.3.7 NL_TRUST_PASSWORD: Added product note about little endian usage for big endian users.</p> <p>Changed from:</p> <p>. . . The NL_TRUST_PASSWORD structure is encrypted using the negotiated encryption algorithm before it is sent over the wire.</p> <p>Changed to:</p> <p>. . . The NL_TRUST_PASSWORD structure is encrypted using the negotiated encryption algorithm before it is sent over the wire.<24></p> <p><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.</p> <p>In section 3.4.5.2.5 Calling NetrServerPasswordSet2: Added product note about little endian usage for big endian users.</p> <p>Changed from:</p> <p>Encrypt 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.</p> <p>Changed to:</p> <p>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.</p> <p><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.</p> <p>In section 3.5.4.4.5 NetrServerPasswordSet2 (Opnum 30): Added product note about little endian usage for big endian users.</p> <p>Changed from:</p> <p>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).</p> <p>Changed to:</p> <p>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).</p> <p><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.</p>

[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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.



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](#)

September 26, 2016 - [Download](#)

June 1, 2017 - [Download](#)

September 15, 2017 - [Download](#)

September 12, 2018 - [Download](#)

October 6, 2021 - [Download](#)

Errata Published*	Description
2023/08/11	<p>See the diff doc for details of the changes.</p> <p>Section 3.2.5.2.1.1.2 x-ms-DeviceCredential HTTP header format Added JWT field values <code>x_client_platform</code>, <code>win_ver</code>, and <code>windows_api_version</code> to inform the AAD/server.</p> <p>Changed from: The <code>x-ms-RefreshTokenCredential</code> HTTP header is a signed JWT, as defined in section 2.2.1.1.1. The JWT fields MUST be given the following values: <code>iat</code> (OPTIONAL): See [OIDCCore] section 2. <code>refresh_token</code> (REQUIRED): A primary refresh token that was previously received from the server. See section 3.1.5.1.2. <code>request_nonce</code> (REQUIRED): A nonce previously obtained from the server by making the request described in section 3.1.5.1.1.</p> <p>Changed to: The <code>x-ms-RefreshTokenCredential</code> HTTP header is a signed JWT, as defined in section 2.2.1.1.1. The JWT fields MUST be given the following values: <code>iat</code> (OPTIONAL): See [OIDCCore] section 2. <code>refresh_token</code> (REQUIRED): A primary refresh token that was previously received from the server. See section 3.1.5.1.2. <code>request_nonce</code> (REQUIRED): A nonce previously obtained from the server by making the request. See section 3.1.5.1.1. <code>x_client_platform</code> (OPTIONAL): The value is used to inform the AAD/server the platform on which this header is created.<7> <code>win_ver</code> (OPTIONAL): This claim has the operating system version information.<8> <code>windows_api_version</code> (OPTIONAL): The version value is "2.0.1". This information is used to indicate to the server that the client has the ability to handle nonce challenges. <7> Section 3.2.5.2.1.1.1: The default value is "windows" for the Windows platform. <8> Section 3.2.5.2.1.1.1: The <code>win_ver</code> value is the Windows version information.</p> <p>Section 3.2.5.2.1.1.1 x-ms-RefreshTokenCredential HTTP header format Added JWT field values <code>x_client_platform</code>, <code>win_ver</code>, and <code>windows_api_version</code> to inform</p>

Errata Published*	Description
	<p>the AAD/server.</p> <p>Changed from: The x-ms-DeviceCredential HTTP header, as defined in section 2.2.1.2, is a signed JWT. The JWT fields MUST be given the following values:<9> grant_type (OPTIONAL): Set to "device_auth" if present. iss (OPTIONAL): Set to "aad:brokerplugin" if present. request_nonce (REQUIRED): A nonce previously obtained from the server by making the request. See section 3.1.5.1.1. <9> Section 3.2.5.2.1.1.2: The Windows implementation of the client role supplies the values specified for grant_type and iss, but the Windows implementation of the server role ignores them.</p> <p>Changed to: The x-ms-DeviceCredential HTTP header, as defined in section 2.2.1.2, is a signed JWT. The JWT fields MUST be given the following values:<9> grant_type (OPTIONAL): Set to "device_auth" if present. iss (OPTIONAL): Set to "aad:brokerplugin" if present. request_nonce (REQUIRED): A nonce previously obtained from the server by making the request. See section 3.1.5.1.1. x_client_platform (OPTIONAL): The value is used to inform AAD/server the platform on which this header is created.<10> win_ver (OPTIONAL): This claim has the operating system version information.<11> windows_api_version (OPTIONAL): The version value is "2.0.1". This information is used to indicate to the server that the client has the ability to handle nonce challenges. <9> Section 3.2.5.2.1.1.2: The Windows implementation of the client role supplies the values specified for grant_type and iss, but the Windows implementation of the server role ignores them. <10> Section 3.2.5.2.1.1.2: The default value is "windows" for the Windows platform. <11> Section 3.2.5.2.1.1.2: The win_ver value is the Windows version information.</p>
2023/07/11	<p>See the diff doc for details of the changes.</p> <p>Section 3.1.5.1.2.3 Processing Details</p> <p>Description: Clarified how the client uses a previously received Nonce from the server: if user JWT authentication (section 3.2.5.1.2.1.2) is in use, the same Nonce is populated as a request_nonce field in the JWT assertion before signing.</p> <p>Added note identifying the operating systems that support this feature, as specified in [MSFT-CVE-2023-35348].</p> <p>Changed from: The client uses the Nonce abstract data model (ADM) element value (section 3.1.1) that it received from the server in a previous nonce request (section 3.1.5.1.1) to populate the request_nonce field of the request.</p> <p>Changed to: The client uses the Nonce abstract data model (ADM) element value (section 3.1.1) that it received from the server in a previous nonce request (section 3.1.5.1.1) to populate the request_nonce field of the request. If using user JSON Web Token (JWT) authentication, as described in section 3.2.5.1.2.1.2, the same Nonce should be populated as a request_nonce field in the JWT assertion before signing it.</p> <p>Note: This feature is supported by the operating systems specified in [MSFT-CVE-2023-35348], each with its related KB article download installed.</p> <p>Section 3.2.5.1.2.1.2 User JWT Authentication</p> <p>Description: Added 'request_nonce' as a required field in the 'assertion' field (the signed JWT used to authenticate the user), as required by the client.</p>

Errata Published*	Description
	<p>Added note identifying the operating systems that support this feature, as specified in [MSFT-CVE-2023-35348].</p> <p>Changed from: aud (REQUIRED): The Issuer Identifier ([OIDCCore] section 1.2) of the server that the client is sending the request to.</p> <p>The signature header fields of the assertion field MUST be given the following values:</p> <p>Changed to: aud (REQUIRED): The Issuer Identifier ([OIDCCore] section 1.2) of the server that the client is sending the request to.</p> <p>request_nonce (REQUIRED): This is the same value as request_nonce as contained in the request body (section 3.2.5.1.2.1).</p> <p>Note: The request_nonce value is supported in the assertion field by the operating systems specified in [MSFT-CVE-2023-35348], each with its related KB article download installed.</p> <p>The signature header fields of the assertion field MUST be given the following values:</p> <p>Section 3.2.5.1.2.3 Processing Details</p> <p>Description: Clarified the user JWT authentication processing steps taken by the server when the authenticated device kid is a mismatch with the assertion JWT kid. The server then verifies whether the request_nonce field in the assertion matches the request_nonce in the request body, with the server returning an "invalid grant" error upon mismatch.</p> <p>Added note identifying the operating systems that support this feature, as specified in [MSFT-CVE-2023-35348].</p> <p>Changed from: 2. It finds the public key for the signature by finding the value of the msDS-KeyCredentialLink attribute on the user object for which the SHA-256 hash ([FIPS180-2] section 6.2.2) of the attribute value matches the kid field of the assertion JWT.</p> <p>Changed to: 2. It finds the public key for the signature by finding the value of the msDS-KeyCredentialLink attribute on the user object for which the SHA-256 hash ([FIPS180-2] section 6.2.2) of the attribute value matches the kid field of the assertion JWT.</p> <p>If the kid of the authenticated device does not match the kid of the assertion JWT, the server SHOULD verify that the assertion contains the request_nonce field and that it also matches the request_nonce present in the request body (section 3.2.5.1.2.1). Otherwise, the server MUST return the "invalid_grant" error using the format described in [RFC6749] section 5.</p> <p>Note: This behavior is supported by the operating systems specified in [MSFT-CVE-2023-35348], each with its related KB article download installed.</p>

*Date format: YYYY/MM/DD

[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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.



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:

November 23, 2020 - [Download](#)

April 29, 2022 - [Download](#)

June 28, 2023 - [Download](#)

[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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

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	<p>Section 3.1.5.2.1.5 Mapping Strength: added section.</p> <p>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:</p> <ul style="list-style-type: none">• SAN UPNName• SAN DNSName• altSecurityIdentities Issuer Name and Subject Name• altSecurityIdentities Subject Name• altSecurityIdentities 822 field <p>The following mappings are considered strong:</p> <ul style="list-style-type: none">• 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 <p>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.</p>

Errata Published*	Description
	<p data-bbox="386 226 1412 279"><22> Section 3.1.5.2.1.5 Certificate mapping strength is applicable to Windows Server 2008 R2 and later.</p> <p data-bbox="386 321 1412 373"><23> Section 3.1.5.2.1.5 Certificate mapping strength is applicable to Windows Server 2008 R2 and later.</p> <p data-bbox="386 415 812 447">Section 3.1.5.2.1.6 SID: added section.</p> <p data-bbox="386 489 1412 667">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.</p> <p data-bbox="386 709 1412 762"><24> Section 3.1.5.2.1.6 Certificate SID mapping is applicable to Windows Server 2008 R2 and later.</p>

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

To view a PDF 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](#).

Errata Published*	Description						
2023/08/16	<p>Please see the diff document.</p> <p>Section 2.2.1.3.1 User Data Header (TS_UD_HEADER): Added data block type CS_UNUSED1.</p> <p>Changed from:</p> <table border="1"><thead><tr><th>Value</th><th>Meaning</th></tr></thead><tbody><tr><td>...</td><td></td></tr><tr><td>CS_MULTITRANSPORT 0xC00A</td><td>The data block that follows contains Client Multitransport Channel Data (section 2.2.1.3.8).</td></tr></tbody></table>	Value	Meaning	...		CS_MULTITRANSPORT 0xC00A	The data block that follows contains Client Multitransport Channel Data (section 2.2.1.3.8).
Value	Meaning						
...							
CS_MULTITRANSPORT 0xC00A	The data block that follows contains Client Multitransport Channel Data (section 2.2.1.3.8).						

Errata Published*	Description																								
	<table border="1" data-bbox="427 226 1429 359"> <tr> <td data-bbox="427 226 930 306">SC_CORE 0x0C01</td> <td data-bbox="930 226 1429 306">The data block that follows contains Server Core Data (section 2.2.1.4.2).</td> </tr> <tr> <td data-bbox="427 306 930 359">...</td> <td data-bbox="930 306 1429 359"></td> </tr> </table> <p data-bbox="410 405 540 426">Changed to:</p> <table border="1" data-bbox="427 436 1429 856"> <thead> <tr> <th data-bbox="427 436 930 489">Value</th> <th data-bbox="930 436 1429 489">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="427 489 930 541">...</td> <td data-bbox="930 489 1429 541"></td> </tr> <tr> <td data-bbox="427 541 930 642">CS_MULTITRANSPORT 0xC00A</td> <td data-bbox="930 541 1429 642">The data block that follows contains Client Multitransport Channel Data (section 2.2.1.3.8).</td> </tr> <tr> <td data-bbox="427 642 930 722">CS_UNUSED1 0xC00C</td> <td data-bbox="930 642 1429 722">The data block that follows contains Client Unused1 Data (section 2.2.1.3.9).</td> </tr> <tr> <td data-bbox="427 722 930 802">SC_CORE 0x0C01</td> <td data-bbox="930 722 1429 802">The data block that follows contains Server Core Data (section 2.2.1.4.2).</td> </tr> <tr> <td data-bbox="427 802 930 856">...</td> <td data-bbox="930 802 1429 856"></td> </tr> </tbody> </table> <p data-bbox="410 905 1255 926">Section 2.2.1.3.9 Client Unused1 Data (TS_UD_CS_UNUSED1): Added section.</p> <p data-bbox="410 974 1398 1020">Added TS_UD_CS_UNUSED1 packet that has a GCC user data block header (4 bytes) with a pad2Octets (2 bytes) for padding. Please see the diff document.</p>	SC_CORE 0x0C01	The data block that follows contains Server Core Data (section 2.2.1.4.2).	...		Value	Meaning	...		CS_MULTITRANSPORT 0xC00A	The data block that follows contains Client Multitransport Channel Data (section 2.2.1.3.8).	CS_UNUSED1 0xC00C	The data block that follows contains Client Unused1 Data (section 2.2.1.3.9).	SC_CORE 0x0C01	The data block that follows contains Server Core Data (section 2.2.1.4.2).	...									
SC_CORE 0x0C01	The data block that follows contains Server Core Data (section 2.2.1.4.2).																								
...																									
Value	Meaning																								
...																									
CS_MULTITRANSPORT 0xC00A	The data block that follows contains Client Multitransport Channel Data (section 2.2.1.3.8).																								
CS_UNUSED1 0xC00C	The data block that follows contains Client Unused1 Data (section 2.2.1.3.9).																								
SC_CORE 0x0C01	The data block that follows contains Server Core Data (section 2.2.1.4.2).																								
...																									
2022/01/04	<p data-bbox="410 1045 1429 1092">In section 2.2.1.3.2, Client Core Data (TS_UD_CS_CORE), added the client version number for RDP 10.10:</p> <p data-bbox="410 1140 573 1161">Changed from:</p> <table border="1" data-bbox="427 1203 1239 1814"> <thead> <tr> <th data-bbox="427 1203 589 1255">Value</th> <th data-bbox="589 1203 1239 1255">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="427 1255 589 1308">0x00080001</td> <td data-bbox="589 1255 1239 1308">RDP 4.0 clients</td> </tr> <tr> <td data-bbox="427 1308 589 1360">0x00080004</td> <td data-bbox="589 1308 1239 1360">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 data-bbox="427 1360 589 1413">0x00080005</td> <td data-bbox="589 1360 1239 1413">RDP 10.0 clients</td> </tr> <tr> <td data-bbox="427 1413 589 1465">0x00080006</td> <td data-bbox="589 1413 1239 1465">RDP 10.1 clients</td> </tr> <tr> <td data-bbox="427 1465 589 1518">0x00080007</td> <td data-bbox="589 1465 1239 1518">RDP 10.2 clients</td> </tr> <tr> <td data-bbox="427 1518 589 1570">0x00080008</td> <td data-bbox="589 1518 1239 1570">RDP 10.3 clients</td> </tr> <tr> <td data-bbox="427 1570 589 1623">0x00080009</td> <td data-bbox="589 1570 1239 1623">RDP 10.4 clients</td> </tr> <tr> <td data-bbox="427 1623 589 1675">0x0008000A</td> <td data-bbox="589 1623 1239 1675">RDP 10.5 clients</td> </tr> <tr> <td data-bbox="427 1675 589 1728">0x0008000B</td> <td data-bbox="589 1675 1239 1728">RDP 10.6 clients</td> </tr> <tr> <td data-bbox="427 1728 589 1780">0x0008000C</td> <td data-bbox="589 1728 1239 1780">RDP 10.7 clients</td> </tr> <tr> <td data-bbox="427 1780 589 1814">0x0008000D</td> <td data-bbox="589 1780 1239 1814">RDP 10.8 clients</td> </tr> </tbody> </table>	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
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																								

Errata Published*	Description																																																		
	<table border="1" data-bbox="427 226 1239 275"> <tr> <td data-bbox="427 226 592 275">0x0008000E</td> <td data-bbox="592 226 1239 275">RDP 10.9 clients</td> </tr> </table> <p data-bbox="407 317 542 344">Changed to:</p> <table border="1" data-bbox="427 386 1239 1094"> <thead> <tr> <th data-bbox="427 386 592 434">Value</th> <th data-bbox="592 386 1239 434">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="427 434 592 483">0x00080001</td> <td data-bbox="592 434 1239 483">RDP 4.0 clients</td> </tr> <tr> <td data-bbox="427 483 592 531">0x00080004</td> <td data-bbox="592 483 1239 531">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 data-bbox="427 531 592 579">0x00080005</td> <td data-bbox="592 531 1239 579">RDP 10.0 clients</td> </tr> <tr> <td data-bbox="427 579 592 627">0x00080006</td> <td data-bbox="592 579 1239 627">RDP 10.1 clients</td> </tr> <tr> <td data-bbox="427 627 592 676">0x00080007</td> <td data-bbox="592 627 1239 676">RDP 10.2 clients</td> </tr> <tr> <td data-bbox="427 676 592 724">0x00080008</td> <td data-bbox="592 676 1239 724">RDP 10.3 clients</td> </tr> <tr> <td data-bbox="427 724 592 772">0x00080009</td> <td data-bbox="592 724 1239 772">RDP 10.4 clients</td> </tr> <tr> <td data-bbox="427 772 592 821">0x0008000A</td> <td data-bbox="592 772 1239 821">RDP 10.5 clients</td> </tr> <tr> <td data-bbox="427 821 592 869">0x0008000B</td> <td data-bbox="592 821 1239 869">RDP 10.6 clients</td> </tr> <tr> <td data-bbox="427 869 592 917">0x0008000C</td> <td data-bbox="592 869 1239 917">RDP 10.7 clients</td> </tr> <tr> <td data-bbox="427 917 592 966">0x0008000D</td> <td data-bbox="592 917 1239 966">RDP 10.8 clients</td> </tr> <tr> <td data-bbox="427 966 592 1014">0x0008000E</td> <td data-bbox="592 966 1239 1014">RDP 10.9 clients</td> </tr> <tr> <td data-bbox="427 1014 592 1062">0x0008000F</td> <td data-bbox="592 1014 1239 1062">RDP 10.10 clients</td> </tr> </tbody> </table> <p data-bbox="407 1136 1409 1188">In section 2.2.1.4.2, Server Core Data (TS_UD_SC_CORE), added the server version number for RDP 10.10:</p> <p data-bbox="407 1230 570 1257">Changed from:</p> <table border="1" data-bbox="427 1299 1239 1797"> <thead> <tr> <th data-bbox="427 1299 592 1348">Value</th> <th data-bbox="592 1299 1239 1348">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="427 1348 592 1396">0x00080001</td> <td data-bbox="592 1348 1239 1396">RDP 4.0 servers</td> </tr> <tr> <td data-bbox="427 1396 592 1444">0x00080004</td> <td data-bbox="592 1396 1239 1444">RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 servers</td> </tr> <tr> <td data-bbox="427 1444 592 1493">0x00080005</td> <td data-bbox="592 1444 1239 1493">RDP 10.0 servers</td> </tr> <tr> <td data-bbox="427 1493 592 1541">0x00080006</td> <td data-bbox="592 1493 1239 1541">RDP 10.1 servers</td> </tr> <tr> <td data-bbox="427 1541 592 1589">0x00080007</td> <td data-bbox="592 1541 1239 1589">RDP 10.2 servers</td> </tr> <tr> <td data-bbox="427 1589 592 1638">0x00080008</td> <td data-bbox="592 1589 1239 1638">RDP 10.3 servers</td> </tr> <tr> <td data-bbox="427 1638 592 1686">0x00080009</td> <td data-bbox="592 1638 1239 1686">RDP 10.4 servers</td> </tr> <tr> <td data-bbox="427 1686 592 1734">0x0008000A</td> <td data-bbox="592 1686 1239 1734">RDP 10.5 servers</td> </tr> <tr> <td data-bbox="427 1734 592 1782">0x0008000B</td> <td data-bbox="592 1734 1239 1782">RDP 10.6 servers</td> </tr> </tbody> </table>	0x0008000E	RDP 10.9 clients	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	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
0x0008000E	RDP 10.9 clients																																																		
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																																																		
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																																																		

Errata Published*	Description	
	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.

No errata are available for the latest version of 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.



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](#).

Errata Published*	Description												
2023/05/16	<p>Section 2.2.1.2.1 KERB_ASN1_DATA: Updated PDU numeric values. Added product note for RS1 values.</p> <p>Changed from:</p> <p>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.</p> <table border="1"> <thead> <tr> <th>Value</th> <th>Meaning</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>Changed to:</p> <p>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></p> <table border="1"> <thead> <tr> <th>Value</th> <th>Meaning</th> </tr> </thead> <tbody> <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> </tbody> </table> <p><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.</p>	Value	Meaning	62	The encrypted data contains a KRB_AS_REP message.	63	The encrypted data contains a KRB_TGS_REP message.	Value	Meaning	70	The encrypted data contains a KRB_AS_REP message.	71	The encrypted data contains a KRB_TGS_REP message.
Value	Meaning												
62	The encrypted data contains a KRB_AS_REP message.												
63	The encrypted data contains a KRB_TGS_REP message.												
Value	Meaning												
70	The encrypted data contains a KRB_AS_REP message.												
71	The encrypted data contains a KRB_TGS_REP message.												
2021/09/07	<p>In Section 2.2 Message Syntax, changed data types in TSRemoteGuardInnerPacket.</p> <p>Changed from:</p> <pre> TSRemoteGuardInnerPacket ::= SEQUENCE { version [0] TSRemoteGuardVersion DEFAULT tsremoteguardv1, packageName [1] OCTETSTRINGNOCOPY, buffer [2] OCTETSTRINGNOCOPY, extension [3] ANYNOCOPY OPTIONAL, -- future extension point ... </pre>												

Errata Published*	Description
	<pre> } 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 ... } </pre>

*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.

To view a PDF 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	<p>In Section 4.4.3.1, Requesting the Size of a File, revised example:</p> <p>Changed from:</p> <p>The following is an annotated dump of a File Contents Request PDU (section 2.2.5.3).</p> <pre>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 </pre> <p>Changed to:</p> <p>The following is an annotated dump of a File Contents Request PDU (section 2.2.5.3).</p> <pre>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 </pre> <p>In Section 4.4.3.2, Requesting the Contents of a File, revised example:</p> <p>Changed from:</p> <p>The following is an annotated dump of a File Contents Request PDU (section 2.2.5.3).</p> <pre>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 08 00 00 00 </pre>

Errata Published*	Description
	<p>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 01 00</p>

*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.

No errata are available for the latest version of 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.  [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:

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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

To view a PDF 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.



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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

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

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

Errata Published*	Description
	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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

Errata below are for Protocol Document Version [V5.0 - 2021/06/25](#).

Errata Published*	Description																														
2022/02/08	<p>In section 2.2.1.11 MS-Azure-Policy-ID, added new section</p> <p>Changed from:</p> <p>Changed to:</p> <p>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:</p> <p>Vendor-Type: An 8-bit unsigned integer that MUST be set to 0x41.</p> <p>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.</p> <p>Attribute-Specific Value: An octet string containing the Policy ID configured on the Azure Point to Site VPN Server.</p> <p>In section 3.1.5.2 Microsoft VSA Support of RADIUS Messages, added MS-Azure-Policy-ID VSA to table.</p> <p>Changed from:</p> <table border="1"> <thead> <tr> <th>Microsoft vendor-specific attribute</th> <th>Request</th> <th>Accept</th> <th>Reject</th> <th>Challenge</th> <th>Accounting-Request</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>Changed to:</p> <table border="1"> <thead> <tr> <th>Microsoft vendor-specific attribute</th> <th>Request</th> <th>Accept</th> <th>Reject</th> <th>Challenge</th> <th>Accounting-Request</th> </tr> </thead> <tbody> <tr> <td>Microsoft vendor-specific attribute</td> <td>Request</td> <td>Accept</td> <td>Reject</td> <td>Challenge</td> <td>Accounting-Request</td> </tr> </tbody> </table>	Microsoft vendor-specific attribute	Request	Accept	Reject	Challenge	Accounting-Request	...						MS-RDG-Device-Redirection	0	0-1	0	0	0	Microsoft vendor-specific attribute	Request	Accept	Reject	Challenge	Accounting-Request	Microsoft vendor-specific attribute	Request	Accept	Reject	Challenge	Accounting-Request
Microsoft vendor-specific attribute	Request	Accept	Reject	Challenge	Accounting-Request																										
...																															
MS-RDG-Device-Redirection	0	0-1	0	0	0																										
Microsoft vendor-specific attribute	Request	Accept	Reject	Challenge	Accounting-Request																										
Microsoft vendor-specific attribute	Request	Accept	Reject	Challenge	Accounting-Request																										

Errata Published*	Description					
	...					
	MS-RDG-Device-Redirection	0	0-1	0	0	0
	MS-Azure-Policy-ID	0	0-1	0	0	0
<p>In section 3.3.5.2.3 MS-Azure-Policy-ID, added new section</p> <p>Changed from:</p> <p>Changed to:</p> <p>This attribute is consumed only by the Microsoft Azure Point to Site VPN Server.</p> <p>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.</p> <p>A NAS that is not a Microsoft Azure Point to Site VPN Server ignores this attribute.</p> <p>For more details about this attribute, see section 2.2.1.11.</p>						

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

To view a PDF 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	<p>In Section 1.3.2 Method-Based Perspective</p> <p>Description: Added description of new method 'SamrValidateComputerAccountReuseAttempt' to Miscellaneous category, which confirms whether client attempts to re-use a particular computer account are allowed.</p> <p>Changed from:</p> <ul style="list-style-type: none">• SamrCloseHandle: This method releases server resources associated with the RPC context handle that is passed as a parameter. <p>Changed to:</p> <ul style="list-style-type: none">• 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. <p>In section 2.2.7.15 SAMPR_REVISION_INFO_V1</p> <p>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.</p>

Errata Published*	Description
	<p>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).</p> <p>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).</p> <p>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.</p> <p>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.</p> <p>In Section 3.1.5 Message Processing Events and Sequencing Rules Description: Added new method to Opnum list: 'SamrValidateComputerAccountReuseAttempt' (Opnum 74)</p> <p>Changed from: SamrUnicodeChangePasswordUser4 Changes a user account password. Opnum 73</p> <p>Changed to: SamrUnicodeChangePasswordUser4 Changes a user account password. Opnum 73 SamrValidateComputerAccountReuseAttempt Validates whether clients can re-use a computer account. Opnum 74</p> <p>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></p> <p><pbn72>: ComputerAccountReuseAllowList and supporting method SamrValidateComputerAccountReuseAttempt are supported on the operating systems specified in [MSKB-5020276], each with its related KB article download installed.</p> <p>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</p>

Errata Published*	Description																																
);																																
2022/09/20	<p>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.</p> <p>Changed from:</p> <table border="1" data-bbox="386 457 1404 913"> <thead> <tr> <th>Constant Name</th> <th>Value</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>Changed to:</p> <table border="1" data-bbox="386 955 1421 1648"> <thead> <tr> <th>Constant/value</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </table> <p>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.</p> <p>Changed from:</p>	Constant Name	Value	versionbyte	0x01	versionbyte_length	1	SAM_AES_256_ALG	"AEAD-AES-256-CBC-HMAC-SHA512"	SAM_AES256_ENC_KEY_STRING	"Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"	SAM_AES256_MAC_KEY_STRING	"Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"	SAM_AES256_ENC_KEY_STRING_LENGTH	sizeof(SAM_AES256_ENC_KEY_STRING)	SAM_AES256_MAC_KEY_STRING_LENGTH	sizeof(SAM_AES256_MAC_KEY_STRING)	Constant/value	Description	Versionbyte 0x01	Version identifier.	versionbyte_length 1	Version identifier length.	SAM_AES_256_ALG "AEAD-AES-256-CBC-HMAC-SHA512"	A NULL terminated ANSI string.	SAM_AES256_ENC_KEY_STRING "Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"	A NULL terminated ANSI string.	SAM_AES256_MAC_KEY_STRING "Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"	A NULL terminated ANSI string.	SAM_AES256_ENC_KEY_STRING_LENGTH sizeof(SAM_AES256_ENC_KEY_STRING) (61)	The length of SAM_AES256_ENC_KEY_STRING, including the null terminator.	SAM_AES256_MAC_KEY_STRING_LENGTH sizeof(SAM_AES256_MAC_KEY_STRING) (54)	The length of SAM_AES256_MAC_KEY_STRING, including the null terminator
Constant Name	Value																																
versionbyte	0x01																																
versionbyte_length	1																																
SAM_AES_256_ALG	"AEAD-AES-256-CBC-HMAC-SHA512"																																
SAM_AES256_ENC_KEY_STRING	"Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"																																
SAM_AES256_MAC_KEY_STRING	"Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"																																
SAM_AES256_ENC_KEY_STRING_LENGTH	sizeof(SAM_AES256_ENC_KEY_STRING)																																
SAM_AES256_MAC_KEY_STRING_LENGTH	sizeof(SAM_AES256_MAC_KEY_STRING)																																
Constant/value	Description																																
Versionbyte 0x01	Version identifier.																																
versionbyte_length 1	Version identifier length.																																
SAM_AES_256_ALG "AEAD-AES-256-CBC-HMAC-SHA512"	A NULL terminated ANSI string.																																
SAM_AES256_ENC_KEY_STRING "Microsoft SAM encryption key AEAD-AES-256-CBC-HMAC-SHA512 16"	A NULL terminated ANSI string.																																
SAM_AES256_MAC_KEY_STRING "Microsoft SAM MAC key AEAD-AES-256-CBC-HMAC-SHA512 16"	A NULL terminated ANSI string.																																
SAM_AES256_ENC_KEY_STRING_LENGTH sizeof(SAM_AES256_ENC_KEY_STRING) (61)	The length of SAM_AES256_ENC_KEY_STRING, including the null terminator.																																
SAM_AES256_MAC_KEY_STRING_LENGTH sizeof(SAM_AES256_MAC_KEY_STRING) (54)	The length of SAM_AES256_MAC_KEY_STRING, including the null terminator																																

Errata Published*	Description
	<ul style="list-style-type: none"> • 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. <p>Changed to:</p> <ul style="list-style-type: none"> • 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. <p>Changed from:</p> <p>Let AuthData ::= HMAC-SHA-512(mac_key, versionbyte + IV + Cipher + versionbyte_length)</p> <p>Changed to:</p> <p>Let AuthData ::= HMAC-SHA-512(mac_key, versionbyte + IV + Cipher + versionbyte_length)</p> <p>Note that enc_key is truncated to 32-bytes and the entire 64-byte mac_key is used.</p> <p>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.</p> <p>Changed from:</p> <p>The client MUST derive the CEK in the following manner: CEK ::= (PBKDF2(NT HASH of "OldPassword", Salt, Iteration Count, 512))</p> <p>Changed to:</p> <p>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))</p>

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.



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	<p>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.</p> <p>Changed from:</p> <p>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.</p> <p>crealm: A KerberosString that represents the realm in which the user account is located. This value is not case-sensitive.</p> <p>Changed to:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Changed from:</p> <p>... 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.</p>

Errata Published*	Description
	<p>Changed to:</p> <p>... 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.</p> <p>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.</p> <p>Changed from:</p> <ul style="list-style-type: none"> • 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". <p>Changed to:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>Changed from:</p> <p>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).</p> <p>Changed to:</p> <p>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></p> <p><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].</p>

*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.

No errata are available for the latest version of 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.

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](#).

Errata Published*	Description								
2023/05/22	<p>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.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>If the SecurityMode field in the Negotiate Response has the SMB2_NEGOTIATE_SIGNING_REQUIRED bit set, the client MUST set Connection.RequireSigning to TRUE.</p>								
2023/04/11	<p>In section 2.2.14, "SMB2 CREATE Response," added a condition for using the SMB2_CREATE_FLAG_REPARSEPOINT in the Flags field:</p> <p>Changed from:</p> <table border="1"><thead><tr><th>Value</th><th>Meaning</th></tr></thead><tbody><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></tbody></table> <p>Changed to:</p> <table border="1"><thead><tr><th>Value</th><th>Meaning</th></tr></thead><tbody><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></tbody></table>	Value	Meaning	SMB2_CREATE_FLAG_REPARSEPOINT 0x01	When set, indicates the last portion of the file path is a reparse point.	Value	Meaning	SMB2_CREATE_FLAG_REPARSEPOINT 0x01	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
Value	Meaning								
SMB2_CREATE_FLAG_REPARSEPOINT 0x01	When set, indicates the last portion of the file path is a reparse point.								
Value	Meaning								
SMB2_CREATE_FLAG_REPARSEPOINT 0x01	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								

Errata Published*	Description	
		<p>opened is a reparse point, and the create request Create Options do not contain FILE_OPEN_REPARSE_POINT.</p>
	<p>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:</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>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.</p>	

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

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	<p>In section 3.1.5.2 SSTP Packet Processing: Added MTU and MRU rules and settings that enable packets larger than 1586 bytes.</p> <p>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.</p> <p>Changed to: Common packet processing functionality is as follows:</p> <ol style="list-style-type: none">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 <code>4095 – sizeof(SSTP_HEADER)</code>.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: <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NdisWan\Parameters\MRU</code> <p>By default, packets of any size can be sent or received through the tunnel, as Windows stack will IP fragment the packets.</p> <p>To enable large SSTP payloads, both MTU (on the sender) and MRU (on the receiver) need to be set to larger values.</p> <p>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.</p>

*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.

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	<p>In Section 1.5 Prerequisites/Preconditions, added reference to the amendment for HEVC.</p> <p>Changed from:</p> <p>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></p> <p><1> Section 1.5: The Smooth Streaming Protocol is supported...</p> <p>Changed to:</p> <p>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></p> <p><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].</p> <p><2> Section 1.5: The Smooth Streaming Protocol is supported...</p>

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.  [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:

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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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-VSOD]: Virtual Storage Protocols Overview

This topic lists Errata found in [MS-VSOD] 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.

Errata below are for Protocol Document Version [V5.0 - 2021/10/26](#).

Errata Published*	Description
2023/08/16	<p>Section 3.1.1 Connecting and Opening a Virtual Disk: Added product note on step 6 to explain SIDs included in ACEs on VHDX files.</p> <p>Changed from:</p> <p>Main success scenario</p> <ol style="list-style-type: none">1. Trigger: Based on interactions with the user, the application requests that the virtual disk be opened.2. The application requests that the file client make a connection to and open the virtual disk.3. The file client first establishes the connection with the file server, as described in [MS-SMB2] section 3.2.4.2.4. The file server authenticates the user through the mechanisms described in [MS-AUTHSOD].5. If the connection is successful, the file client opens the virtual disk on the file server, as described in [MS-SMB2] section 3.2.4.3.6. The file server processes the open request, as described in [MS-SMB2] section 3.3.5.9.7. The file client returns a handle for the virtual disk to the application, as described in [MS-SMB2] section 3.2.5.7.3. <p>Changed to:</p> <p>Main success scenario</p> <ol style="list-style-type: none">1. Trigger: Based on interactions with the user, the application requests that the virtual disk be opened.2. The application requests that the file client make a connection to and open the virtual disk.3. The file client first establishes the connection with the file server, as described in [MS-SMB2] section 3.2.4.2.4. The file server authenticates the user through the mechanisms described in [MS-AUTHSOD].5. If the connection is successful, the file client opens the virtual disk on the file server, as described in [MS-SMB2] section 3.2.4.3.6. The file server processes the open request, as described in [MS-SMB2] section 3.3.5.9.<1>7. The file client returns a handle for the virtual disk to the application, as described in [MS-SMB2] section 3.2.5.7.3. <p><1>Section 3.1.1: VM SIDs in the format S-1-5-83-1-dd-dd-dd-dd are included in ACEs on VHDX files to grant access to a specific virtual machine. See NT VIRTUAL MACHINE\Remote Virtual Machine in [MS-DTYP] section 2.4.2.4.</p>

*Date format: YYYY/MM/DD

[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.

No errata are available for the latest version of 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.



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	<p>Section 3.2.2.6.3.1.1 PropID=0x0000001D (CR_PROP_TEMPLATES) "Configured Certificate Templates"</p> <p>Description: Updated string definition ("TemplateName1\nTemplateOID1\nTemplateName2\nTemplateOID2\...") to include a null termination character, to ensure consistent results with calls to the GetCATemplates function.</p> <p>Changed from: "TemplateName1\nTemplateOID1\nTemplateName2\nTemplateOID2\... " where</p> <p>Changed to: "TemplateName1\nTemplateOID1\nTemplateName2\nTemplateOID2...\nTemplateName\nTemplateOIDN\n\0" where</p> <p>Note: The format and definition of the string cited in section 3.2.1.4.3.2.29 below is correct as is.</p>
2022/12/16	<p>Section 2.1 Transport</p> <p>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.</p> <p>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 certificate administrative operations, the CA MUST deny a connection to the client and return a non-</p>

Errata Published *	Description
	<p>zero error. <7></p> <p>Changed to:</p> <p>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></p> <p><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.</p> <p>Section 3.2.1.4.2.1 ICertRequestD::Request (Opnum 3)</p> <p>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.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>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></p> <p><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.</p> <p>Section 3.2.1.4.2.2 ICertRequestD::GetCACert (Opnum 4)</p> <p>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.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>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></p>

Errata Published *	Description
	<p><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.</p> <p>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.</p> <p>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</p> <p>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></p> <p><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.</p> <p>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.</p> <p>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.</p> <p>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></p> <p><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.</p> <p>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 administrative operations to ensure a connection to the CA server is not denied. Also specified the operating</p>

Errata Published *	Description
	<p>systems that support this behavior.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>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></p> <p><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.</p>

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

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	<p>In Section 2.2.5.19, JOINPR_ENCRYPTED_USER_PASSWORD_AES, corrected typo:</p> <p>Changed from:</p> <p>AuthDate: 64 bytes, the HMAC.</p> <p>Changed to:</p> <p>AuthData: 64 bytes, the HMAC.</p> <p>In Section 2.2.5.19.3, Encrypt Key and MAC Key, clarified the calculation of the keys:</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>The following variables and values are used in calculating the EncryptKey and MACKEY values:</p> <table border="1" data-bbox="397 1759 1430 1808"> <thead> <tr> <th data-bbox="397 1759 971 1808">Constant/value</th> <th data-bbox="971 1759 1430 1808">Description</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Constant/value	Description		
Constant/value	Description				

Errata Published*	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.
	<p>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.</p> <p>In Section 2.2.5.19.4, Encrypt Encoded Password, clarified the encryption process:</p> <p>Changed from:</p> <p>Encrypt the encoded password as follows:</p> <p>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.</p> <p>Changed to:</p> <p>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.</p>	

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

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	<p>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.</p> <p>Changed from:</p> <p>"The WSTEP extends wst: RequestedSecurityTokenType with two additional elements.</p> <ul style="list-style-type: none">• <code><xs:element ref="wsse:BinarySecurityToken" /></code>• <code><xs:element ref="wsse:SecurityTokenReference" /></code> <p>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."</p> <p>Changed to:</p> <p>"MS-WSTEP extends the wst: RequestedSecurityTokenType with two additional elements as follows.</p> <ul style="list-style-type: none">• <code><xs:element ref="wsse:BinarySecurityToken" /></code>• <code><xs:element ref="wsse:SecurityTokenReference" /></code> <p>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].</p> <p>wsse:BinarySecurityToken: The wsse:BinarySecurityToken element contains the issued certificatein either a full CMC response or as a stand alone x509v3 certificate[RFC5280].</p> <p><2> Section 3.1.4.1.3.2: Microsoft Windows always includes the requested end entity certificate in the RequestedSecurityToken."</p>

*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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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.

No errata are available for the latest version of 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](#)

Errata below are for Protocol Document Version [V14.0 - 2021/04/07](#).

Errata Published*	Description										
2023/08/16	<p>Section 2.2.5 Simple Types</p> <p>Description: Added Readonly string type 'NeutralLanguage' to the Simple Type table to designate when a common update is language-neutral, as indicated by the fixed string value "all". For use with UUP On Prem-generated updates.</p> <p>Changed from: The following table describes the XML schema simple type defined by this specification. XML schema simple type definitions that are specific to a particular operation are described with the operation.</p> <table border="1"><thead><tr><th>Simple type</th><th>Description</th></tr></thead><tbody><tr><td>GUID</td><td>A globally unique identifier (GUID) of an object or entity within the protocol. For example, each update has a unique ID that is a GUID.</td></tr></tbody></table> <p>Changed to: The following table describes the XML schema simple types defined by this specification. XML schema simple type definitions that are specific to a particular operation are described with the operation.</p> <table border="1"><thead><tr><th>Simple type</th><th>Description</th></tr></thead><tbody><tr><td>GUID</td><td>A globally unique identifier (GUID) of an object or entity within the protocol. For example, each update has a unique ID that is a GUID.</td></tr><tr><td>NeutralLanguage</td><td>A static Readonly string that designates a language-neutral common update value equal to "all", for use with UUP On Prem-generated updates.</td></tr></tbody></table> <p>Section 2.2.5.2 All Description: Created new section describing the use of the "all" value to identify language</p>	Simple type	Description	GUID	A globally unique identifier (GUID) of an object or entity within the protocol. For example, each update has a unique ID that is a GUID.	Simple type	Description	GUID	A globally unique identifier (GUID) of an object or entity within the protocol. For example, each update has a unique ID that is a GUID.	NeutralLanguage	A static Readonly string that designates a language-neutral common update value equal to "all", for use with UUP On Prem-generated updates.
Simple type	Description										
GUID	A globally unique identifier (GUID) of an object or entity within the protocol. For example, each update has a unique ID that is a GUID.										
Simple type	Description										
GUID	A globally unique identifier (GUID) of an object or entity within the protocol. For example, each update has a unique ID that is a GUID.										
NeutralLanguage	A static Readonly string that designates a language-neutral common update value equal to "all", for use with UUP On Prem-generated updates.										

Errata Published*	Description
	<p>neutral updates in UUP On-Prem applications.</p> <p>Changed from: ""</p> <p>Changed to: "Exists in SusXML for language neutral packages used by the Windows update client to identify language neutral updates with the "all" value, by using the NeutralLanguage type (as defined in section 2.2.5 Simple Types) for UUP on-Prem only applications, as shown in the example that follows.</p> <pre data-bbox="516 485 1130 625"> <upd:LocalizedPropertiesCollection> <upd:LocalizedProperties> <upd:Language>NeutralLanguage</upd:Language> <upd:Title>SQL 2005 English ia64</upd:Title> </upd:LocalizedProperties> </upd:LocalizedPropertiesCollection> </pre> <p>For more information, see "Sample 2: Metadata and Deployments Synchronization" in section 4 of this document."</p>

[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.

No errata are available for the latest version of 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.



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	<p>In section 2.1.4.3, deleted a sentence asserting that match length checks are performed.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>Note that match distances cannot be larger than 65,535, and match lengths cannot be longer than 65,538.</p> <p>In section 2.2.4, "Processing," clarified the description of processing for decompression.</p> <p>Changed from:</p> <p>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.</p> <p>Changed to:</p> <p>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.</p> <p>In section 2.2.4, Processing, added terminating conditions to the decompression pseudocode.</p>

Errata Published*	Description
	<p>Changed from:</p> <p>Loop until a decompression terminating condition</p> <p>Build the decoding table</p> <p>CurrentPosition = 256 // start at the end of the Huffman table</p> <p>NextBits = Read16Bits(InputBuffer + CurrentPosition)</p> <p>CurrentPosition += 2</p> <p>Changed to:</p> <p>Loop until a decompression terminating condition</p> <p>If remaining input buffer does not have enough space for a Huffman table</p> <p>If we're at the end of the output buffer</p> <p>Decompression is complete, return success</p> <p>The compressed data is not valid, return error</p> <p>Build the decoding table</p> <p>CurrentPosition = 256 // start at the end of the Huffman table</p> <p>NextBits = Read16Bits(InputBuffer + CurrentPosition)</p> <p>CurrentPosition += 2</p>

[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.

No errata are available for the latest version of 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](#)