

# Windows Protocols Errata

---

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



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

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

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

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

## Protocols Documents with Active Errata

[\[MC-NMF\]: .NET Message Framing Protocol](#)

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

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

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

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

[\[MS-KILE\]: Kerberos Protocol Extensions](#)

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

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

[\[MS-MDE2\]: Mobile Device Enrollment Protocol Version 2](#)

[\[MS-MDM\]: Mobile Device Management Protocol](#)

[\[MS-NCNBI\]: Network Controller Northbound Interface](#)

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

[\[MS-NRBF\]: .NET Remoting: Binary Format Data Structure](#)

[\[MS-NRPC\]: Netlogon Remote Protocol](#)

[\[MS-PAC\]: Privilege Attribute Certificate Data Structure](#)

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

[\[MS-RDPEAR\]: Remote Desktop Protocol Authentication Redirection Virtual Channel](#)

[\[MS-RDPECLIP\]: Remote Desktop Protocol Clipboard Virtual Channel Extension](#)

[\[MS-RDPEUDP2\]: Remote Desktop Protocol UDP Transport Extension Version 2](#)

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

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

[\[MS-SFU\]: Kerberos Protocol Extensions Service for User and Constrained Delegation Protocol](#)

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

[\[MS-SSTR\]: Smooth Streaming Protocol](#)

[\[MS-WCCE\]: Windows Client Certificate Enrollment Protocol](#)

[\[MS-WKST\]: Workstation Service Remote Protocol](#)

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

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

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

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

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



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

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

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



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



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

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



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

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

September 15, 2017 - [Download](#)

## [MS-ABTP]: Automatic Bluetooth Pairing Protocol

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)



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

This topic lists the Errata found in the MS-ADA2 document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

June 1, 2017 - [Download](#)

Errata Published*	Description
2023/03/06	<p>Section 2.64 Attribute ms-LAPS-Password Description: Created new section for new Active Directory schema element, the "ms-LAPS-Password" attribute, to support the new Local Administrator Password Solution (LAPS) feature.</p> <p>Section 2.65 Attribute ms-LAPS-PasswordExpirationTime Description: Created new section for new Active Directory schema element, the "ms-LAPS-PasswordExpirationTime" attribute, to support the new Local Administrator Password Solution (LAPS) feature.</p> <p>Section 2.66 Attribute ms-LAPS-EncryptedPassword Description: Created new section for new Active Directory schema element, the "ms-LAPS-EncryptedPassword" attribute, to support the new Local Administrator Password Solution (LAPS) feature.</p> <p>Section 2.67 Attribute ms-LAPS-EncryptedPasswordHistory Description: Created new section for new Active Directory schema element, the "ms-LAPS-EncryptedPasswordHistory" attribute, to support the new Local Administrator Password Solution (LAPS) feature.</p> <p>Section 2.68 Attribute ms-LAPS-EncryptedDSRMPassword Description: Created new section for new Active Directory schema element, the "ms-LAPS-EncryptedDSRMPassword" attribute, to support the new Local Administrator Password Solution (LAPS) feature.</p>

Errata Published*	Description
	<p>Section 2.69 Attribute ms-LAPS-EncryptedDSRMPasswordHistory Description: Created new section for new Active Directory schema element, the "ms-LAPS-EncryptedDSRMPasswordHistory" attribute, to support the new Local Administrator Password Solution (LAPS) feature.</p> <p>Section 2.70 Attribute ms-Mcs-AdmPwd Description: Created new section for new Active Directory schema element, the "ms-Mcs-AdmPwd" attribute, to support the new Local Administrator Password Solution (LAPS) feature.</p> <p>Section 2.71 Attribute ms-Mcs-AdmPwdExpirationTime Description: Created new section for new Active Directory schema element, the "ms-Mcs-AdmPwdExpirationTime" attribute, to support the new Local Administrator Password Solution (LAPS) feature.</p>

\*Date format: YYYY/MM/DD

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

**This topic lists the Errata found in the MS-ADA3 document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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

June 1, 2017 - [Download](#)

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

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



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

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



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

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

July 18, 2016 - [Download](#)

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

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



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

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

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

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



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

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

July 18, 2016 - [Download](#)

April 7, 2021 - [Download](#)

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

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



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

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

June 1, 2017 - [Download](#)



## [MS-ADSC]: Active Directory Schema Classes

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



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

To view a PDF 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; CIIIO; SW; 9b026da6-0d3c-465c-8bee-5199d7165cba; bf967a86-0de6-11d0-a285-00aa003049e2; PS) (OA; CIIIO; 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 the Errata found in the MS-ADTS document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

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 [V55.0 - 2022/04/29](#).

Errata Published*	Description
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:</p> <p>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:</p> <p>Information that is applicable to AD LDS on Windows Server v1903 is also applicable to AD LDS for Windows 10 v1903.</p> <p>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>



Errata Published*	Description																																																	
	<table border="1" data-bbox="402 226 1089 277"> <tr> <td>msDS-DatabaseIndicesWithSize</td> <td>Y</td> <td>String(Unicode)</td> </tr> </table> <p>(New sections)</p> <p>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 <a href="#">[MSKB-5023705]</a>, <a href="#">[MSKB-5023702]</a>, <a href="#">[MSKB-5023706]</a>, <a href="#">[MSKB-5023698]</a>, and <a href="#">[MSKB-5023696]</a>; 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-DatabaseIndicesWithSize	Y	String(Unicode)																																														
msDS-DatabaseIndicesWithSize	Y	String(Unicode)																																																
2022/01/18	<p>Section 3.1.1.3.4.6 LDAP Policies</p> <p>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> <p>Changed from:</p> <p>The table contains information for the following products. See section 3 for more information.</p> <p>....</p> <table border="1" data-bbox="402 1171 1414 1430"> <thead> <tr> <th>Policy name</th> <th>A</th> <th>D, DR2, G, J</th> <th>M</th> <th>R</th> <th>U</th> <th>X, A2, D2, G2, J2</th> </tr> </thead> <tbody> <tr> <td>MaxActiveQueries</td> <td>X*</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>InitRecvTimeout</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> </tr> <tr> <td>....</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>* Support for this policy was removed in Windows Server 2003.</td> </tr> </tbody> </table> <p>Changed to:</p> <p>The table contains information for the following products. See section 3 for more information.</p> <p>....</p> <table border="1" data-bbox="402 1640 1365 1793"> <thead> <tr> <th>Policy name</th> <th>A</th> <th>D, DR2, G, J</th> <th>M</th> <th>R</th> <th>U</th> <th>X, A2, D2, G2, J2</th> </tr> </thead> <tbody> <tr> <td>MaxActiveQueries</td> <td>X*</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>InitRecvTimeout</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> <td>X</td> </tr> </tbody> </table>	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.	Policy name	A	D, DR2, G, J	M	R	U	X, A2, D2, G2, J2	MaxActiveQueries	X*						InitRecvTimeout	X	X	X	X	X	X
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.																																												
Policy name	A	D, DR2, G, J	M	R	U	X, A2, D2, G2, J2																																												
MaxActiveQueries	X*																																																	
InitRecvTimeout	X	X	X	X	X	X																																												

Errata Published*	Description																	
	....																	
	SecurityDescriptorWarningSize**																	
	<p>* Support for this policy was removed in Windows Server 2003. ** Support for this policy only exists on Windows 11 v22H2 and later.</p>																	
	<p>Changed from:</p>																	
	<table border="1"> <thead> <tr> <th data-bbox="402 529 651 606">Policy name</th> <th data-bbox="651 529 764 606">Default value</th> <th data-bbox="764 529 1430 606">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="402 606 651 663">....</td> <td data-bbox="651 606 764 663"></td> <td data-bbox="764 606 1430 663"></td> </tr> <tr> <td data-bbox="402 663 651 835">MaxDirSyncDuration</td> <td data-bbox="651 663 764 835">60</td> <td data-bbox="764 663 1430 835">The maximum time, in seconds, that a DC will spend on a single search when using the LDAP_SERVER_DIRSYNC_OID or LDAP_SERVER_DIRSYNC_EX_OID controls. When this limit is reached, the DC returns a timeLimitExceeded / ERROR_INVALID_PARAMETER error.</td> </tr> </tbody> </table>						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.			
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.																
	<p>Changed to:</p>																	
	<table border="1"> <thead> <tr> <th data-bbox="402 936 764 1058">Policy name</th> <th data-bbox="764 936 873 1058">Default value</th> <th data-bbox="873 936 1430 1058">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="402 1058 764 1115">....</td> <td data-bbox="764 1058 873 1115"></td> <td data-bbox="873 1058 1430 1115"></td> </tr> <tr> <td data-bbox="402 1115 764 1314">MaxDirSyncDuration</td> <td data-bbox="764 1115 873 1314">60</td> <td data-bbox="873 1115 1430 1314">The maximum time, in seconds, that a DC will spend on a single search when using the LDAP_SERVER_DIRSYNC_OID or LDAP_SERVER_DIRSYNC_EX_OID controls. When this limit is reached, the DC returns a timeLimitExceeded / ERROR_INVALID_PARAMETER error.</td> </tr> <tr> <td data-bbox="402 1314 764 1478">SecurityDescriptorWarningSize</td> <td data-bbox="764 1314 873 1478">61,440</td> <td data-bbox="873 1314 1430 1478">This policy controls when warning events will be logged for originating writes to the ntSecurityDescriptor attribute that meet or exceed the configured size value.</td> </tr> </tbody> </table>						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.	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.
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.																
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 the Errata found in the MS-AIPS document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**

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



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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

## [MS-APDS]: Authentication Protocol Domain Support

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



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

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

\*Date format: YYYY/MM/DD

## [MS-AZOD]: Authorization Protocols Overview

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

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



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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

June 1, 2021 - [Download](#)



## [MS-BKRP]: BackupKey Remote Protocol

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



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

To view a PDF 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 <a href="#">diff document</a> for the details.</p> <p>In Section 3.2.4.1 Performing Client-Side Wrapping of Secrets, Product Behavior Note&lt;18&gt;</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 <a href="#">[MSFT-CVE-2022-21925]</a>. 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 the Errata found in the MS-BKUP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

No errata are available for the latest version of 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 the Errata found in the MS-CAPR document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

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

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



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

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>

Errata Published*	Description																																																																																																																																																																																																																																																																																																																																																																																																																								
	<p>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.</p> <table border="1" data-bbox="386 344 1401 707"> <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>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td> </tr> <tr> <td colspan="10">Scenario Type</td> <td colspan="6">Version and Device Type</td> <td colspan="6">Version and Flags</td> <td colspan="6">Reserved</td> </tr> <tr> <td colspan="32">Salt</td> </tr> <tr> <td colspan="32">Device Hash (16 bytes)</td> </tr> <tr> <td colspan="32">...</td> </tr> <tr> <td colspan="32">...</td> </tr> </table> <p>Scenario Type (1 byte): Set to 1</p> <p>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:</p> <p>Changed to:</p> <p>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.</p> <table border="1" data-bbox="386 1031 1401 1417"> <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>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td> </tr> <tr> <td colspan="10">Scenario_Type</td> <td colspan="6">Version_and_Device_Type</td> <td colspan="6">Version_and_Flags</td> <td colspan="6">Flags_and_Device_Status</td> </tr> <tr> <td colspan="32">Salt</td> </tr> <tr> <td colspan="32">Device_Hash (19 bytes)</td> </tr> <tr> <td colspan="32">...</td> </tr> <tr> <td colspan="32">...</td> </tr> <tr> <td colspan="16">...</td> <td colspan="16"></td> </tr> </table> <p>Scenario_Type (1 byte): Set to 1 (Bluetooth scenario).</p> <p>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:</p> <p>Changed from:</p> <p>Version and Flags (1 byte): The high 3 bits are set to 001; the lower 3 bits to 00000.</p> <p>Reserved (1 byte): Currently set to zero.</p> <p>Salt (4 bytes): Four random bytes.</p> <p>Device Hash (16 bytes): SHA256 Hash of Salt plus Device Thumbprint. Truncated to 16 bytes.</p>	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	Scenario Type										Version and Device Type						Version and Flags						Reserved						Salt																																Device Hash (16 bytes)																																...																																...																																0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	Scenario_Type										Version_and_Device_Type						Version_and_Flags						Flags_and_Device_Status						Salt																																Device_Hash (19 bytes)																																...																																...																																...																															
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31																																																																																																																																																																																																																																																																																																																																																																																										
Scenario Type										Version and Device Type						Version and Flags						Reserved																																																																																																																																																																																																																																																																																																																																																																																																			
Salt																																																																																																																																																																																																																																																																																																																																																																																																																									
Device Hash (16 bytes)																																																																																																																																																																																																																																																																																																																																																																																																																									
...																																																																																																																																																																																																																																																																																																																																																																																																																									
...																																																																																																																																																																																																																																																																																																																																																																																																																									
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31																																																																																																																																																																																																																																																																																																																																																																																										
Scenario_Type										Version_and_Device_Type						Version_and_Flags						Flags_and_Device_Status																																																																																																																																																																																																																																																																																																																																																																																																			
Salt																																																																																																																																																																																																																																																																																																																																																																																																																									
Device_Hash (19 bytes)																																																																																																																																																																																																																																																																																																																																																																																																																									
...																																																																																																																																																																																																																																																																																																																																																																																																																									
...																																																																																																																																																																																																																																																																																																																																																																																																																									
...																																																																																																																																																																																																																																																																																																																																																																																																																									

Errata Published*	Description																																		
	<p>Changed to:</p> <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="402 411 1414 514"> <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="402 747 1414 1104"> <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.&lt;5&gt;</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.&lt;6&gt;</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 the Errata found in the MS-CHAP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

## [MS-CFB]: Compound File Binary File Format

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

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



No errata are available for the latest version of 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 the Errata found in the MS-CIFS document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

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>&lt;245&gt; 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>

Errata Published*	Description
	<ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul> <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"> <li>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.</li> <li>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.</li> </ul> <p>...</p> <p>Changed from:</p> <p>&lt;297&gt; 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>

Errata Published*	Description
	<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"> <li>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.</li> <li>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.</li> </ul> <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"> <li>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.</li> <li>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.</li> </ul> <p>...</p> <p>Changed from:</p> <p>&lt;339&gt; Section 3.3.5.58.2</p>

Errata Published*	Description
	<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> <p>0xFF FCB mode (see following)</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul> <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"> <li>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.</li> <li>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</li> </ul>

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

\*Date format: YYYY/MM/DD

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

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

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



No errata are available for the latest version of 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 the Errata found in the MS-COMA document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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



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

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</p> <p>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</p> <p>CT_FLAG_DONOTPERSISTINDB</p> <p>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</p> <p>CT_FLAG_DONOTPERSISTINDB</p> <p>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</p> <p>CT_FLAG_DONOTPERSISTINDB</p>



Errata Published*	Description										
	<p>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>2022/05/10</p>	<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 <a href="#">[MSFT-CVE-2022-26931]</a> for this security update."</p> <p>Changed From:</p> <table border="1" data-bbox="407 583 1414 716"> <thead> <tr> <th data-bbox="407 583 792 636">Flag</th> <th data-bbox="792 583 1414 636">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="407 636 792 716">0x00040000 CT_FLAG_SKIP_AUTO_RENEWAL</td> <td data-bbox="792 636 1414 716">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="407 827 1414 1161"> <thead> <tr> <th data-bbox="407 827 846 879">Flag</th> <th data-bbox="846 827 1414 879">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="407 879 846 982">0x00040000 CT_FLAG_SKIP_AUTO_RENEWAL</td> <td data-bbox="846 879 1414 982">This flag indicates that the certificate should not be auto-renewed, although it has a valid template.</td> </tr> <tr> <td data-bbox="407 982 846 1161">0x00080000 CT_FLAG_NO_SECURITY_EXTENSION</td> <td data-bbox="846 982 1414 1161">This flag<sup>34</sup> 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><sup>34</sup> This flag is supported by the operating systems specified in <a href="#">[MSFT-CVE-2022-26931]</a>, 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 <sup>34</sup> 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 <sup>34</sup> 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.										
<p>2021/07/27</p>	<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="407 1440 1414 1625"> <thead> <tr> <th data-bbox="407 1440 743 1524">Flag</th> <th data-bbox="743 1440 1414 1524">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="407 1524 743 1625">0x00000010 CT_FLAG_EXPORTABLE_KEY</td> <td data-bbox="743 1524 1414 1625">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>	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										
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.										

Errata Published*	Description	
	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 [RFC7292], at a later time.

\*Date format: YYYY/MM/DD

## [MS-CSRA]: Certificate Services Remote Administration Protocol

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



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

To view a PDF 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 <a href="#">[MSFT-CVE-2022-37976]</a>.</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.&lt;18&gt;</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. &lt;18&gt; &lt;19&gt;</p> <p>&lt;19&gt; 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 <a href="#">[MSFT-CVE-2022-37976]</a>.</p>

Errata Published*	Description
	<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. 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).&lt;67&gt;</p> <p>&lt;67&gt; 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 the Errata found in the MS-CSSP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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

July 18, 2016 - [Download](#)

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&lt;22&gt; be specified by the CredSSP server operating system for the package that provided them.</p> <p>&lt;22&gt; 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&lt;22&gt; be specified by the CredSSP server operating system for the package that provided them.</p> <p>&lt;22&gt; 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	
	Value	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 the Errata found in the MS-CSVP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

August 24, 2020 - [Download](#)



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

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



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

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>&lt;pbn81&gt;: 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>&lt;pbn81&gt;: 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>&lt;pbn81&gt;: 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>&lt;pbn81&gt;: 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>

Errata Published*	Description
	<p>On Windows Vista and later and Windows Server 2008 and later, DCOM clients specify the higher of the LegacyAuthenticationLevel value ([MSDN-LegAuthLevel]) or RPC_C_AUTHN_LEVEL_PKT_INTEGRITY ([MS-RPCE] section 2.2.1.1.8) as the default authentication level value for the call.</p>
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&lt;pbn-80&gt;. Otherwise, the client MUST specify a default authentication level that is obtained in an implementation-specific manner&lt;pbn-81&gt;.</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>&lt;pbn-80&gt; 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</p>

Errata Published*	Description
	<p>KB article download installed: Windows 11 (Sun Valley) Desktop, Windows 11 (Sun Valley) Desktop Refresh, Windows 11 Desktop v22H2, Windows Server 2022 - Full/Core, Windows 10 Desktop v22H2, Windows 10 Desktop v21H2, Windows 10 Desktop v21H1, and Windows 10 Desktop v20H2.</p>
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 <code>RPC_C_AUTHN_LEVEL_PKT_INTEGRITY</code>, if it is less than that. Also specified the operating systems that support this behavior.</p> <p>Changed from:</p> <p>The client <b>MUST</b> specify the authentication level requested by the application, if one was supplied; otherwise, it <b>MUST</b> specify a default authentication level that is obtained in an implementation-specific manner.</p> <p>Changed to:</p> <p>The client <b>MUST</b> 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 <b>MAY</b> raise the authentication level&lt;pbm-80&gt;. Otherwise, the client <b>MUST</b> specify a default authentication level that is obtained in an implementation-specific manner&lt;pbm-81&gt;.</p> <p>&lt;pbm-80&gt;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 <code>RPC_C_AUTHN_LEVEL_PKT_INTEGRITY</code> (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 <code>LegacyAuthenticationLevel</code> value (for more information, see [MSDN-LegAuthLevel]) and <code>RPC_C_AUTHN_LEVEL_PKT_INTEGRITY</code> (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 <code>RPC_C_AUTHN_LEVEL_PKT_INTEGRITY</code> level on client side and the required activation authentication level needs to be at least at <code>RPC_C_AUTHN_LEVEL_PKT_INTEGRITY</code> 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>&lt;pbm-80&gt; On Windows, the authentication level requested by the application is raised to <code>RPC_C_AUTHN_LEVEL_PKT_INTEGRITY</code> ([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</p>

Errata Published*	Description
	operating system with Service Pack 2 (SP2), Windows 10 version 22H2 operating system, Windows 10 v21H2 operating system, Windows 10 v21H1 operating system, Windows 10 v20H2 operating system, Windows 10 v1809 operating system, Windows 10 v1909 operating system, Windows 10 v1607 operating system, Windows 10 v1507 operating system, and Windows 7 operating system with Service Pack 1 (SP1).
2022/10/11	<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>&lt;37&gt; 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>&lt;37&gt; 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 <a href="#">[MSFT-CVE-2022-37978]</a>, 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&lt;pbn-80&gt;. Otherwise, the client MUST specify a default authentication level that is obtained in an implementation-specific manner&lt;pbn-81&gt;.</p> <p>&lt;pbn-80&gt;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>

Errata Published*	Description
	<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.</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>&lt;pbn-80&gt; 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 the Errata found in [MS-DFSC] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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



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

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



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

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

June 1, 2017 - [Download](#)

September 15, 2017 - [Download](#)



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

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



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

To view a PDF 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_DnssrvUpdateRecord (opnum 4), added processing behavior for the static condition.</p> <p>Changed from:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.</li></ul> <p>Changed to:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• 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.&lt;279&gt;</li><li>• 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.</li></ul> <p>&lt;279&gt; 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 2.2.2.4.23) 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 2.2.2.4.23) 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 2.2.2.4.23) 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 2.2.2.4.23) 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 2.2.2.4.23) 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 the Errata found in [MS-DPWSSN] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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

July 18, 2016 - [Download](#)

June 1, 2017 - [Download](#)

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

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



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

To view a PDF 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 &lt;42&gt; 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. &lt;42&gt;"</p> <p>&lt;42&gt; 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.&lt;42&gt;"</p> <p>&lt;42&gt; 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 the Errata found in the MS-DTCO document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

December 1, 2017 - [Download](#)

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

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



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

No errata are available for the latest version of 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 the Errata found in the MS-DTYP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

June 1, 2017 - [Download](#)

September 15, 2017 - [Download](#)

December 1, 2017 - [Download](#)

September 12, 2018 - [Download](#)

April 7, 2021 - [Download](#)

April 29, 2022 - [Download](#)

Errata below are for Protocol Document Version [V38.0 - 2022/04/29](#).

Errata Published*	Description
2023/01/30	<p>In section 2.4.4.17.9, "Examples: Conditional Expression Binary Representation," changed row 1, column 1 text in Figures 4 and 5:</p> <p>Changed from: SSDL (descending in post-fix notation)</p> <p>Changed to: SDDL (descending in post-fix notation)</p>
2022/12/13	<p>In Section 2.2.57, "UNC", revised the description of creating a hostname from an IPV6 address: changed ipv6literal.net to ipv6-literal.net in the description.</p> <p>Changed from:</p> <p>An IPV6 address host-name is formed by substituting hyphens for the colons and appending ".ipv6literal.net". For example, the IPV6 address 2001:DB8:D87:FFFF:CCAA:132B:1:221B becomes 2001-DB8-D87-FFFF-CCAA-132B-1-221B.ipv6-literal.net.</p> <p>Changed to:</p>

<b>Errata Published*</b>	<b>Description</b>
	An IPV6 address host-name is formed by substituting hyphens for the colons and appending ".ipv6-literal.net". For example, the IPV6 address 2001:DB8:D87:FFFF:CCAA:132B:1:221B becomes 2001-DB8-D87-FFFF-CCAA-132B-1-221B.ipv6-literal.net.

\*Date format: YYYY/MM/DD



## [MS-DVRD]: Device Registration Discovery Protocol

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



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

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

July 18, 2016 - [Download](#)

## [MS-DVRE]: Device Registration Enrollment Protocol

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

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



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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

## [MS-DVRJ]: Device Registration Join Protocol

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



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

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

June 1, 2017 - [Download](#)

## [MS-ECS]: Enterprise Client Synchronization Protocol

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

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



No errata are available for the latest version of this Windows Protocols document. To view a PDF 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 the Errata found in the MS-EFSR document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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: 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.&lt;37&gt;</p> <p>Changed to: The following table specifies the opnum associated with each RPC method in this protocol. An EFSRPC server SHOULD support all of the methods specified in this table.&lt;37&gt;&lt;38&gt;</p> <p>&lt;38&gt; Section 3.1.4.2: After installation of one of the updates listed in [MSFT-CVE-2022-26925], a client using a null session will receive RPC_S_ACCESS_DENIED when calling any of these methods using lsarpc.</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: The DDF and DRF Protector List structure in the Version 4 EFSRPC Metadata MUST be formatted as follows.</p> <table border="1" style="margin-left: 40px;"> <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>10</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>20</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>30</td><td>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_Entry 1 (variable)</td> </tr> <tr> <td colspan="32" style="text-align: center;">...</td> </tr> <tr> <td colspan="32" 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;">Protector_List_Entry ProtectorsCount (variable)</td> </tr> </table>	0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	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	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1																																																																																																																																																																																																		
StructureSize																																																																																																																																																																																																																																	
ProtectorsCount																Protector_List_Entry 1 (variable)																																																																																																																																																																																																																	
...																																																																																																																																																																																																																																	
Protector_List_Entries (variable)																																																																																																																																																																																																																																	
...																																																																																																																																																																																																																																	
Protector_List_Entry ProtectorsCount (variable)																																																																																																																																																																																																																																	

Errata Published*	Description																																																																																																																																																																																						
	<div style="border: 1px solid black; width: fit-content; margin: 0 auto; padding: 5px; text-align: center;">...</div> <p>Changed to: The DDF and DRF Protector List structure in the Version 4 EFSRPC Metadata MUST be formatted as follows.</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <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;">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;">2</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;">3</td><td style="width: 10px; text-align: center;">0</td><td style="width: 10px; text-align: center;">1</td> </tr> <tr> <td colspan="30" style="text-align: center;">StructureSize</td> </tr> <tr> <td colspan="15" style="text-align: center;">ProtectorsCount</td> <td colspan="15" style="text-align: center;">Protector_List_Entries (variable)</td> </tr> <tr> <td colspan="30" style="text-align: center;">...</td> </tr> <tr> <td colspan="30" style="text-align: center;">...</td> </tr> <tr> <td colspan="30" style="text-align: center;">...</td> </tr> </table>	0	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	2	1	2	3	4	5	6	7	8	9	3	0	1	StructureSize																														ProtectorsCount															Protector_List_Entries (variable)															...																														...																														...																													
0	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7	8	9	2	1	2	3	4	5	6	7	8	9	3	0	1																																																																																																																																																								
StructureSize																																																																																																																																																																																							
ProtectorsCount															Protector_List_Entries (variable)																																																																																																																																																																								
...																																																																																																																																																																																							
...																																																																																																																																																																																							
...																																																																																																																																																																																							

\*Date format: YYYY/MM/DD

## [MS-EMF]: Enhanced Metafile Format

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

June 1, 2017 - [Download](#)

April 7, 2021 - [Download](#)

April 29, 2022 - [Download](#)

## [MS-EMFPLUS]: Enhanced Metafile Format Plus Extensions

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



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

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



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

No errata are available for the latest version of 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 the Errata found in the MS-ERREF document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

No errata are available for the latest version of 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 the Errata found in the MS-EVEN document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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.&lt;6&gt;</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.&lt;6&gt;.</p>

\*Date format: YYYY/MM/DD

## [MS-EVEN6]: EventLog Remoting Protocol Version 6.0

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



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

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.&lt;5&gt;</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.&lt;5&gt;</p>

\*Date format: YYYY/MM/DD

## [MS-FASP]: Firewall and Advanced Security Protocol

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



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

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.</p> <p>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).</p> <p>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.</p> <p>Changed from:</p> <pre>typedef struct _tag_FW_QUERY_CONDITIONS {     unsigned LONG dwNumEntries;     [size_is(dwNumEntries)] FW_QUERY_CONDITION* pAndedConditions; } FW_QUERY_CONDITIONS, *PFW_QUERY_CONDITIONS;</pre> <p>dwNumEntries: Specifies the number of query conditions that the structure contains.</p> <p>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:</p> <pre>typedef struct_tag_FW_QUERY_CONDITIONS {     DWORD dwNumEntries;     [size_is(dwNumEntries)]     FW_QUERY_CONDITION *AndedConditions;</pre>

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

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

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



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

No errata are available for the latest version of 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 the Errata found in the MS-FRS2 document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

April 7, 2021 - [Download](#)



## [MS-FSA]: File System Algorithms

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



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

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

March 2, 2016 - [Download](#)

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

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](#)

Errata below are for Protocol Document Version [36.0 - 2022/04/29](#).

Errata Published*	Description
2023/02/14	<p>Section 2.1.1.4 Per Link, added link usage description, includes information duplication with reference to algorithm to retrieve the latest.</p> <p>Changed from:</p> <p>The object store MUST implement the following persistent attributes:&lt;26&gt; . . .</p> <p>Changed to:</p> <p>A Link structure connects a file name to a directory containing the file. Additionally, a Link duplicates certain information about the file (timestamps, sizes, etc.), that can be used to satisfy directory query operations (see section 2.1.5.6). Note that for performance reasons an object store MAY delay updating a Link's duplicated information following modifications to a file, resulting in directory queries returning stale information. Some file modifications require an</p>

Errata Published*	Description
	<p>immediate update of the duplicated information, which will be noted in this document by invoking the algorithm described in section 2.1.4.18.</p> <p>The object store MUST implement the following persistent attributes:&lt;26&gt; . . .</p> <p>Section 2.1.5.6.3 Directory Information Queries, added directory query usage description, includes information duplication with reference to algorithm to retrieve the latest.</p> <p>Changed from:</p> <p>This section describes how the object store processes directory queries for the following FileInformationClass values: . . .</p> <p>Changed to:</p> <p>Directory queries return requested information about files contained in the directory, based on the Link structures in Open.DirectoryList. Note that for performance reasons an object store MAY delay updating a Link's duplicated information following modifications to a file, resulting in directory queries returning stale information. Some file modifications require an immediate update of the duplicated information, which will be noted in this document by invoking the algorithm described in section 2.1.4.18.</p> <p>This section describes how the object store processes directory queries for the following FileInformationClass values: . . .</p>
2022/08/09	<p>In section 2.1.5.15.11, FileRenameInformation, revised renaming processing.</p> <p>Changed from:</p> <ul style="list-style-type: none"> <li>▪ If <i>RemoveSourceLink</i> is TRUE: <ul style="list-style-type: none"> <li>▪ If <b>Open.File.FileType</b> is DirectoryFile <ul style="list-style-type: none"> <li>▪ <i>FilterMatch</i> = FILE_NOTIFY_CHANGE_DIR_NAME</li> </ul> </li> <li>▪ Else <ul style="list-style-type: none"> <li>▪ <i>FilterMatch</i> = FILE_NOTIFY_CHANGE_FILE_NAME</li> </ul> </li> </ul> </li> <li>▪ EndIf</li> <li>▪ If <i>MoveToNewDir</i> is TRUE or <i>AddTargetLink</i> is FALSE or <i>RemoveTargetLink</i> and <i>ExactCaseMatch</i> are TRUE: <i>Action</i> = FILE_ACTION_REMOVED</li> <li>▪ Else <ul style="list-style-type: none"> <li>▪ <i>Action</i> = FILE_ACTION_REMOVED_OLD_NAME</li> </ul> </li> <li>▪ EndIf</li> </ul> <p>Changed to:</p> <ul style="list-style-type: none"> <li>▪ If <i>RemoveSourceLink</i> is TRUE: <ul style="list-style-type: none"> <li>▪ If <b>Open.File.FileType</b> is DirectoryFile <ul style="list-style-type: none"> <li>▪ <i>FilterMatch</i> = FILE_NOTIFY_CHANGE_DIR_NAME</li> </ul> </li> <li>▪ Else <ul style="list-style-type: none"> <li>▪ <i>FilterMatch</i> = FILE_NOTIFY_CHANGE_FILE_NAME</li> </ul> </li> </ul> </li> <li>▪ EndIf</li> <li>▪ If <i>MoveToNewDir</i> is TRUE or <i>AddTargetLink</i> is FALSE or <i>RemoveTargetLink</i> and <i>ExactCaseMatch</i> are TRUE: <i>Action</i> = FILE_ACTION_REMOVED</li> <li>▪ Else <ul style="list-style-type: none"> <li>▪ <i>Action</i> = FILE_ACTION_RENAMED_OLD_NAME</li> </ul> </li> <li>▪ EndIf</li> </ul>
2022/07/26	<p>Added revisions to section 2.1.5.2, Server Requests an Open of a Named Pipe. Please see the <a href="#">diff file</a>.</p>

Errata Published*	Description
2022/06/01	Added new section, 2.1.5.2, Server Requests an Open of a Named Pipe. Please see the <a href="#">diff file</a> .
2022/06/01	<p>In section 2.1.5.15.11, FileRenameInformation, added information about how NTFS prevents a race condition during renaming.</p> <p>Changed from:</p> <p>If Open.File contains open files as specified in section 2.1.4.2, the operation MUST be failed with STATUS_ACCESS_DENIED.</p> <p>Changed to:</p> <p>If Open.File contains open files as specified in section 2.1.4.2, the operation MUST be failed with STATUS_ACCESS_DENIED.&lt;174&gt;</p> <p>&lt;174&gt; On Windows NTFS, NTFS checks for open files beneath the directory being renamed (performs section 2.1.4.2), it records the count of open files. If there is a lease to break, NTFS requests the break and then goes back to the start of performing 2.1.5.15.11. NTFS waits for the lease break acknowledgment and restarts the rename operation. When NTFS performs section 2.1.4.2 again, it again records how many open files there are beneath the directory and compares that to the previous count. If the current count is greater than or equal to the previous count, NTFS fails the rename and prevents a possible race condition.</p>
2022/05/27	<p>In section 2.1.5.10.34, FSCTL_SET_INTEGRITY_INFORMATION_EX, updated list of applicable updates.</p> <p>Changed from:</p> <p>&lt;127&gt; Section 2.1.5.10.34: 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 <a href="#">[MSKB-5014019]</a>, <a href="#">[MSKB-5014021]</a>, <a href="#">[MSKB-5014022]</a>, or <a href="#">[MSKB-5014023]</a>.</p> <p>Changed to:</p> <p>&lt;127&gt; Section 2.1.5.10.34: 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 <a href="#">[MSKB-5014019]</a>, <a href="#">[MSKB-5014021]</a>, <a href="#">[MSKB-5014022]</a>, <a href="#">[MSKB-5014023]</a>, <a href="#">[MSKB-5014701]</a>, <a href="#">[MSKB-5014702]</a>, or <a href="#">[MSKB-5014710]</a>.</p>
2022/05/18	<p>The following sections were changed. Please see the <a href="#">diff document</a> for the details.</p> <p>In Section 2.1.1.3, Per File, updated a product behavior about how registry entries affect the handling of LastAccessTime:</p> <p>Changed from:</p> <p>&lt;17&gt; Section 2.1.1.3: In Windows Vista and subsequent, LastAccessTime updates are disabled by default in the ReFS and NTFS file systems. It is only updated when the file is closed. This behavior is controlled by the following registry key: HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate. A nonzero value means LastAccessTime updates are disabled. A value of zero means they are enabled.</p> <p>Changed to:</p> <p>&lt;17&gt; Section 2.1.1.3: In Windows Vista and subsequent, LastAccessTime updates are disabled by default in the ReFS and NTFS file systems. It is only updated when the file is closed. This behavior is controlled by the following registry values (respectively): HKLM\System\CurrentControlSet\Control\FileSystem\RefsDisableLastAccessUpdate, and HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate. A value of 1 means LastAccessTime updates are disabled. Any other value (or undefined) means they are enabled.</p> <p>In Windows 10 v1803 operating system and subsequent, NTFS has two registry values controlling LastAccessTime updates: HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate and HKLM\System\CurrentControlSet\Control\FileSystem\NtfsLastAccessUpdatePolicyVolumeSizeThreshold. The NtfsDisableLastAccessUpdate value is now treated as a bitfield as follows:</p>

Errata Published*	Description								
	<table border="1" data-bbox="397 262 1412 1050"> <thead> <tr> <th data-bbox="397 262 738 304">Value</th> <th data-bbox="738 262 1412 304">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="397 304 738 357">0x00000001</td> <td data-bbox="738 304 1412 357">Disable LastAccessTime updates.</td> </tr> <tr> <td data-bbox="397 357 738 892">0x00000002</td> <td data-bbox="738 357 1412 892"> <p>System managed. Indicates that NTFS uses its own policy for updating LastAccessTime as follows:</p> <p>On client systems, LastAccessTime updates are enabled if any of the following conditions are true:</p> <ul style="list-style-type: none"> <li>• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is 0.</li> <li>• The size of the boot volume is &lt;= NtfsLastAccessUpdatePolicyVolumeSizeThreshold in GB.</li> <li>• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is undefined and (prior to Windows 10 v2004) the size of the boot volume is &lt;= 128GB.</li> </ul> <p>On server systems, or client systems where the above conditions do not apply, LastAccessTime updates are always disabled.</p> <p>At system startup, after evaluating the above policy, NTFS will set/clear flag 0x00000001 accordingly to reflect that LastAccessTime updates are disabled/enabled.</p> </td> </tr> <tr> <td data-bbox="397 892 738 1050">0x80000000</td> <td data-bbox="738 892 1412 1050">Flags initialized. Indicates NTFS recognizes flags other than 0x00000001. At system startup, if flag 0x80000000 is not set, the system will automatically set flag 0x80000000 and will additionally set flag 0x00000002 (becoming system managed) if flag 0x00000001 was set.</td> </tr> </tbody> </table> <p data-bbox="381 1071 1323 1123">If the value of NtfsDisableLastAccessUpdate is controlled by group policy, then only flag 0x00000001 is recognized.</p> <p data-bbox="381 1144 1388 1207">In Section 2.1.1.4, Per Link, updated a product behavior about how registry entries affect the handling of LastAccessTime:</p> <p data-bbox="381 1228 544 1260">Changed from:</p> <p data-bbox="381 1281 1412 1417">&lt;31&gt; Section 2.1.1.4: In Windows Vista and subsequent LastAccessTime updates are disabled by default in the ReFS and NTFS file systems. It is only updated when the file is closed. This behavior is controlled by the following registry key: HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate. A nonzero value means LastAccessTime updates are disabled. A value of zero means they are enabled.</p> <p data-bbox="381 1438 511 1470">Changed to:</p> <p data-bbox="381 1512 1421 1690">&lt;31&gt; Section 2.1.1.4: In Windows Vista and subsequent, LastAccessTime updates are disabled by default in the ReFS and NTFS file systems. It is updated only when the file is closed. This behavior is controlled by the following registry values (respectively): HKLM\System\CurrentControlSet\Control\FileSystem\RefsDisableLastAccessUpdate, and HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate. A value of 1 means LastAccessTime updates are disabled. Any other value (or undefined) means they are enabled.</p> <p data-bbox="381 1711 1421 1816">In Windows 10 v1803 and subsequent, NTFS has two registry values controlling LastAccessTime updates: HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate and HKLM\System\CurrentControlSet\Control\FileSystem\NtfsLastAccessUpdatePolicyVolumeSizeThreshold. The NtfsDisableLastAccessUpdate value is</p>	Value	Meaning	0x00000001	Disable LastAccessTime updates.	0x00000002	<p>System managed. Indicates that NTFS uses its own policy for updating LastAccessTime as follows:</p> <p>On client systems, LastAccessTime updates are enabled if any of the following conditions are true:</p> <ul style="list-style-type: none"> <li>• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is 0.</li> <li>• The size of the boot volume is &lt;= NtfsLastAccessUpdatePolicyVolumeSizeThreshold in GB.</li> <li>• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is undefined and (prior to Windows 10 v2004) the size of the boot volume is &lt;= 128GB.</li> </ul> <p>On server systems, or client systems where the above conditions do not apply, LastAccessTime updates are always disabled.</p> <p>At system startup, after evaluating the above policy, NTFS will set/clear flag 0x00000001 accordingly to reflect that LastAccessTime updates are disabled/enabled.</p>	0x80000000	Flags initialized. Indicates NTFS recognizes flags other than 0x00000001. At system startup, if flag 0x80000000 is not set, the system will automatically set flag 0x80000000 and will additionally set flag 0x00000002 (becoming system managed) if flag 0x00000001 was set.
Value	Meaning								
0x00000001	Disable LastAccessTime updates.								
0x00000002	<p>System managed. Indicates that NTFS uses its own policy for updating LastAccessTime as follows:</p> <p>On client systems, LastAccessTime updates are enabled if any of the following conditions are true:</p> <ul style="list-style-type: none"> <li>• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is 0.</li> <li>• The size of the boot volume is &lt;= NtfsLastAccessUpdatePolicyVolumeSizeThreshold in GB.</li> <li>• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is undefined and (prior to Windows 10 v2004) the size of the boot volume is &lt;= 128GB.</li> </ul> <p>On server systems, or client systems where the above conditions do not apply, LastAccessTime updates are always disabled.</p> <p>At system startup, after evaluating the above policy, NTFS will set/clear flag 0x00000001 accordingly to reflect that LastAccessTime updates are disabled/enabled.</p>								
0x80000000	Flags initialized. Indicates NTFS recognizes flags other than 0x00000001. At system startup, if flag 0x80000000 is not set, the system will automatically set flag 0x80000000 and will additionally set flag 0x00000002 (becoming system managed) if flag 0x00000001 was set.								

Errata Published*	Description								
	<p>now treated as a bitfield as follows:</p> <table border="1" data-bbox="399 275 1414 1094"> <thead> <tr> <th data-bbox="404 281 745 327">Value</th> <th data-bbox="745 281 1409 327">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="404 327 745 380">0x00000001</td> <td data-bbox="745 327 1409 380">Disable LastAccessTime updates.</td> </tr> <tr> <td data-bbox="404 380 745 940">0x00000002</td> <td data-bbox="745 380 1409 940"> <p>System managed. Indicates that NTFS uses its own policy for updating LastAccessTime as follows:</p> <p>On client systems, LastAccessTime updates are enabled if any of the following conditions are true:</p> <ul style="list-style-type: none"> <li>• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is 0.</li> <li>• The size of the boot volume is less than or equal to NtfsLastAccessUpdatePolicyVolumeSizeThreshold in GB.</li> <li>• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is undefined and (prior to Windows 10 v2004) the size of the boot volume is &lt;= 128GB.</li> </ul> <p>On server systems, or client systems where the above conditions do not apply, LastAccessTime updates are always disabled.</p> <p>At system startup, after evaluating the above policy, NTFS will set/clear flag 0x00000001 accordingly to reflect that LastAccessTime updates are disabled/enabled.</p> </td> </tr> <tr> <td data-bbox="404 940 745 1087">0x80000000</td> <td data-bbox="745 940 1409 1087">Flags initialized. Indicates NTFS recognizes flags other than 0x00000001. At system startup, if flag 0x80000000 is not set, the system will automatically set flag 0x80000000 and will additionally set flag 0x00000002 (becoming system managed) if flag 0x00000001 was set.</td> </tr> </tbody> </table> <p>If the value of NtfsDisableLastAccessUpdate is controlled by group policy, then only flag 0x00000001 is recognized.</p>	Value	Meaning	0x00000001	Disable LastAccessTime updates.	0x00000002	<p>System managed. Indicates that NTFS uses its own policy for updating LastAccessTime as follows:</p> <p>On client systems, LastAccessTime updates are enabled if any of the following conditions are true:</p> <ul style="list-style-type: none"> <li>• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is 0.</li> <li>• The size of the boot volume is less than or equal to NtfsLastAccessUpdatePolicyVolumeSizeThreshold in GB.</li> <li>• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is undefined and (prior to Windows 10 v2004) the size of the boot volume is &lt;= 128GB.</li> </ul> <p>On server systems, or client systems where the above conditions do not apply, LastAccessTime updates are always disabled.</p> <p>At system startup, after evaluating the above policy, NTFS will set/clear flag 0x00000001 accordingly to reflect that LastAccessTime updates are disabled/enabled.</p>	0x80000000	Flags initialized. Indicates NTFS recognizes flags other than 0x00000001. At system startup, if flag 0x80000000 is not set, the system will automatically set flag 0x80000000 and will additionally set flag 0x00000002 (becoming system managed) if flag 0x00000001 was set.
Value	Meaning								
0x00000001	Disable LastAccessTime updates.								
0x00000002	<p>System managed. Indicates that NTFS uses its own policy for updating LastAccessTime as follows:</p> <p>On client systems, LastAccessTime updates are enabled if any of the following conditions are true:</p> <ul style="list-style-type: none"> <li>• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is 0.</li> <li>• The size of the boot volume is less than or equal to NtfsLastAccessUpdatePolicyVolumeSizeThreshold in GB.</li> <li>• NtfsLastAccessUpdatePolicyVolumeSizeThreshold is undefined and (prior to Windows 10 v2004) the size of the boot volume is &lt;= 128GB.</li> </ul> <p>On server systems, or client systems where the above conditions do not apply, LastAccessTime updates are always disabled.</p> <p>At system startup, after evaluating the above policy, NTFS will set/clear flag 0x00000001 accordingly to reflect that LastAccessTime updates are disabled/enabled.</p>								
0x80000000	Flags initialized. Indicates NTFS recognizes flags other than 0x00000001. At system startup, if flag 0x80000000 is not set, the system will automatically set flag 0x80000000 and will additionally set flag 0x00000002 (becoming system managed) if flag 0x00000001 was set.								
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: The server provides:&lt;127&gt;</p> <p>&lt;127&gt; 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: The server provides:&lt;127&gt;</p> <p>&lt;127&gt; 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 <a href="#">[MSKB-5014019]</a>, <a href="#">[MSKB-5014021]</a>, <a href="#">[MSKB-5014022]</a>, or <a href="#">[MSKB-5014023]</a>.</p>								

## [MS-FSCC]: File System Control Codes

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

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.&lt;86&gt;</p> <p>&lt;86&gt; 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>&lt;97&gt; Section 2.4.7: The file system updates the values of the <b>LastAccessTime</b>, <b>LastWriteTime</b>, and <b>ChangeTime</b> 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 <b>CreationTime</b> 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="397 730 1414 1230"> <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>&lt;98&gt; Section 2.4.7: The file system updates the values of the <b>LastAccessTime</b>, <b>LastWriteTime</b>, and <b>ChangeTime</b> 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 <b>CreationTime</b> 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="397 1619 1414 1818"> <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> </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
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																								

Errata Published *	Description																	
	Cdfs	No																
	UDFS	No																
	NTFS	Windows 8.1 and later, Windows Server 2012 R2 and later and Windows Server v1709 and later																
	ReFS	Windows 10 v1507 and later, Windows Server 2016 and later, and Windows Server v1709 and later																
	<p>&lt;99&gt; Section 2.4.7: The file system updates the values of the <b>LastAccessTime</b>, <b>LastWriteTime</b>, and <b>ChangeTime</b> 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 <b>CreationTime</b> 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="365 934 901 987">File system</th> <th data-bbox="901 934 1427 987">Support value of -2</th> </tr> </thead> <tbody> <tr> <td data-bbox="365 987 901 1039">FAT</td> <td data-bbox="901 987 1427 1039">No</td> </tr> <tr> <td data-bbox="365 1039 901 1092">EXFAT</td> <td data-bbox="901 1039 1427 1092">No</td> </tr> <tr> <td data-bbox="365 1092 901 1144">FAT32</td> <td data-bbox="901 1092 1427 1144">No</td> </tr> <tr> <td data-bbox="365 1144 901 1197">Cdfs</td> <td data-bbox="901 1144 1427 1197">No</td> </tr> <tr> <td data-bbox="365 1197 901 1249">UDFS</td> <td data-bbox="901 1197 1427 1249">No</td> </tr> <tr> <td data-bbox="365 1249 901 1344">NTFS</td> <td data-bbox="901 1249 1427 1344">Windows 8.1 and later, Windows Server 2012 R2 and later and Windows Server v1709 and later</td> </tr> <tr> <td data-bbox="365 1344 901 1438">ReFS</td> <td data-bbox="901 1344 1427 1438">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>&lt;100&gt; Section 2.4.7: The file system updates the values of the <b>LastAccessTime</b>, <b>LastWriteTime</b>, and <b>ChangeTime</b> 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 <b>CreationTime</b> field, they have no effect because file creation time is never updated in response to file system calls such as read and write.</p>																	



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



Changed to:

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

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

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

Errata Published *	Description																																
	<p>is consistent across all file system types. Note that even though -1 and -2 can be used with the <b>CreationTime</b> 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="397 336 1412 787"> <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>&lt;99&gt; Section 2.4.7: The file system updates the value of the <b>LastWriteTime</b> 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 <b>CreationTime</b> 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="397 1144 1412 1596"> <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>&lt;100&gt; Section 2.4.7: The file system updates the value of the <b>ChangeTime</b> 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</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>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 <b>CreationTime</b> 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="397 388 1412 829"> <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>	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="397 945 1412 1396"> <thead> <tr> <th>Error code</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>STATUS_INVALID_PARAMETER 0xC000000D</td> <td>The input buffer length is less than the size, in bytes, of the FSCTL_SET_INTEGRITY_INFORMATION_BUFFER element; the handle is not to a file or directory; or the requested ChecksumAlgorithm field is not one of the values listed in the table for the ChecksumAlgorithm field in the FSCTL_SET_INTEGRITY_INFORMATION Request.</td> </tr> <tr> <td>STATUS_INVALID_DEVICE_REQUEST 0xC0000010</td> <td>The volume does not support integrity.</td> </tr> <tr> <td>STATUS_DISK_FULL 0xC000007F</td> <td>The disk is full.</td> </tr> </tbody> </table> <p>Changed to:</p> <table border="1" data-bbox="397 1470 1412 1795"> <thead> <tr> <th>Error code</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>STATUS_INVALID_PARAMETER 0xC000000D</td> <td>The input buffer length is less than the size, in bytes, of the FSCTL_SET_INTEGRITY_INFORMATION_BUFFER element; the handle is not to a file or directory; or the requested ChecksumAlgorithm field is not one of the values listed in the table for the ChecksumAlgorithm field in the FSCTL_SET_INTEGRITY_INFORMATION Request.</td> </tr> <tr> <td>STATUS_INVALID_DEVICE_REQUEST</td> <td>The volume does not support integrity.</td> </tr> </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	The volume does not support integrity.		
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	The volume does not support integrity.																

Errata Published *	Description													
	0xC0000010													
	STATUS_DISK_FULL 0xC000007F	The disk is full.												
	STATUS_NOT_SUPPORTED 0xC00000BB	The file has been ghosted (allocation blocks are being shared).												
	<p>In section 2.3.75, FSCTL_SET_INTEGRITY_INFORMATION_EX Request, revised note &lt;76&gt; to indicate which versions support this request:</p> <p>Changed from:</p> <p>&lt;76&gt; 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 <a href="#">[MSKB-5014019]</a>, <a href="#">[MSKB-5014021]</a>, <a href="#">[MSKB-5014022]</a>, <a href="#">[MSKB-5014023]</a>, <a href="#">[MSKB-5014701]</a>, <a href="#">[MSKB-5014702]</a>, or <a href="#">[MSKB-5014710]</a>.</p> <p>Changed to:</p> <p>&lt;76&gt; 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 <a href="#">[MSKB-5014019]</a>, <a href="#">[MSKB-5014021]</a>, <a href="#">[MSKB-5014022]</a>, <a href="#">[MSKB-5014023]</a>, <a href="#">[MSKB-5014701]</a>, <a href="#">[MSKB-5014702]</a>, or <a href="#">[MSKB-5014710]</a>.</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="397 1165 1412 1564"> <thead> <tr> <th>Error code</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>STATUS_INVALID_PARAMETER 0xC000000D</td> <td>The input buffer length is less than the size, in bytes, of the FSCTL_SET_INTEGRITY_INFORMATION_BUFFER_EX element; the handle is not to a file or directory; or Version is not equal to 1.</td> </tr> <tr> <td>STATUS_INVALID_DEVICE_REQUEST 0xC0000010</td> <td>The volume does not support integrity.</td> </tr> <tr> <td>STATUS_DISK_FULL 0xC000007F</td> <td>The disk is full.</td> </tr> </tbody> </table> <p>Changed to:</p> <table border="1" data-bbox="397 1669 1412 1816"> <thead> <tr> <th>Error code</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>STATUS_INVALID_PARAMETER 0xC000000D</td> <td>The input buffer length is less than the size, in bytes, of the FSCTL_SET_INTEGRITY_INFORMATION_BUFFER_EX</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
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													

Errata Published *	Description																	
		X 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.																
	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="402 737 1414 1100"> <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="402 1178 1414 1623"> <thead> <tr> <th>Value</th> <th>Meaning</th> </tr> </thead> <tbody> <tr> <td>FILE_ACTION_ADDED 0x00000001</td> <td>The file was renamed, and <b>FileName</b> 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 <b>FileName</b> 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 <b>FileName</b> 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 <b>FileName</b> 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 <b>FileName</b> 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 <b>FileName</b> 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>&lt;76&gt; 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
	<p>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>&lt;76&gt; 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>
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:&lt;127&gt;</p> <p>&lt;127&gt; 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:&lt;127&gt;</p> <p>&lt;127&gt; 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 the Errata found in the MS-FSRVP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**

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



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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

June 1, 2017 - [Download](#)

## [MS-FSVCA]: File Set Version Comparison Algorithms

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)



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

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



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

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

July 18, 2016 - [Download](#)

September 12, 2018 - [Download](#)

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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

September 12, 2018 - [Download](#)

## [MS-GPOL]: Group Policy: Core Protocol

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

June 1, 2017 - [Download](#)

April 7, 2021 - [Download](#)

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

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



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

No errata are available for the latest version of 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 the Errata found in the MS-GSSA document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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

June 1, 2017 - [Download](#)

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

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

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



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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

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

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



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

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

March 20, 2017 - [Download](#)



## [MS-ICPR]: ICertPassage Remote Protocol

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



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

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

July 18, 2016 - [Download](#)

## [MS-IKEE]: Internet Key Exchange Protocol Extensions

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

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



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

July 18, 2016 - [Download](#)

September 15, 2017 - [Download](#)

April 7, 2021 - [Download](#)

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

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



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

No errata are available for the latest version of 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 the Errata found in the MS-IPHTTPS document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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



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

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

June 1, 2017 - [Download](#)

## [MS-KILE]: Kerberos Protocol Extensions

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



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

To view a PDF 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
2023/03/06	<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 KILE has the same security considerations as Kerberos V5 (<a href="#">[RFC4120]</a>, <a href="#">[RFC3961]</a>, <a href="#">[RFC3962]</a>, and <a href="#">[RFC4757]</a>) and GSS-API (<a href="#">[RFC2743]</a>, <a href="#">[RFC1964]</a>, and <a href="#">[RFC4121]</a>).</p> <p>Changed to:</p> <p>5.1 Security Considerations for Implementers KILE has the same security considerations as Kerberos V5 (<a href="#">[RFC4120]</a>, <a href="#">[RFC3961]</a>, <a href="#">[RFC3962]</a>, and <a href="#">[RFC4757]</a>) and GSS-API (<a href="#">[RFC2743]</a>, <a href="#">[RFC1964]</a>, and <a href="#">[RFC4121]</a>).</p> <p>The encryption types AES128-CTC-HMAC-SHA1-96/AES256-CTC-HMAC-SHA1-96 or including AES256-CTS-HMAC-SHA1-96-SK if RC4 encryption types is selected is recommended. Setting RC4/DES only is weak and not recommended. For more information see section 2.2.7.</p>
2023/03/06	<p>Section 2.2.7 Supported Encryption Types Bit Flags: Added note to recommend strong vs. weak encryption usage.</p> <p>Changed from:</p>

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



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

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

June 1, 2017 - [Download](#)



## [MS-KPS]: Key Protection Service Protocol

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



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

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

June 1, 2017 - [Download](#)

September 15, 2017 - [Download](#)

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

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



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

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

Errata Published *	Description		
			a 1-to-1 relationship between this LCID and the user's current default locale name.
	Transient LCIDs<16>	0x3000, 0x3400, 0x3800, 0x3C00, 0x4000, 0x4400, 0x4800, 0x4C00	Some user configurations temporarily associate a locale without a permanent LCID assignment with one of these 8 transient LCIDs. This assignment is transient and it is not guaranteed; it will likely refer to the same locale for the lifetime of the process. However, this assignment will differ for other users on the machine, or other machines, and, as such, is unsuitable for use in protocols or persisted data. This assignment is a temporary 1-to-1 relationship between an LCID and a particular locale name and will round trip until that relationship changes.
	Changed to:		
LOCALE_CUSTOM_USER_DEFAULT<15>	0x0C00		When an LCID without a permanent LCID assignment is also the current user locale, the protocol will respond with LOCALE_CUSTOM_USER_DEFAULT for that locale. This assignment persists until the user changes the locale. Because the meaning changes over time, applications are discouraged from persisting this data. Though this value will likely refer to the same locale for the lifetime of the current process, that is not guaranteed. This assignment is a 1-to-1 relationship between this LCID and the user's current default locale name.
Transient LCIDs<16>	0x2000, 0x2400, 0x2800, 0x2C00, 0x3000, 0x3400, 0x3800, 0x3C00, 0x4000, 0x4400,		Some user configurations temporarily associate a locale without a permanent LCID assignment with one of these 12 transient LCIDs. This assignment is transient and it is not guaranteed; it will likely refer to the same locale for the lifetime of the process. However, this assignment will differ for other users on the

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

\*Date format: YYYY/MM/DD

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

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



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

To view a PDF 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 0x01</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 0x01	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 0x01	Version identifier																				

Errata Published*	Description															
	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 <a href="#">PDF diff document</a> for details.</p> <table border="1" data-bbox="399 1367 1414 1799"> <thead> <tr> <th data-bbox="399 1367 1187 1419">Section</th> <th data-bbox="1187 1367 1414 1419">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="399 1419 1187 1472">1.3 Overview</td> <td data-bbox="1187 1419 1414 1472">Updated</td> </tr> <tr> <td data-bbox="399 1472 1187 1524">1.6 Applicability Statement</td> <td data-bbox="1187 1472 1414 1524">Updated</td> </tr> <tr> <td data-bbox="399 1524 1187 1577">2.2 Common Data Types</td> <td data-bbox="1187 1524 1414 1577">Updated</td> </tr> <tr> <td data-bbox="399 1577 1187 1650">2.2.1.4 AEAD-AES-256-CBC-HMAC-SHA512 Constants</td> <td data-bbox="1187 1577 1414 1650">Created new section</td> </tr> <tr> <td data-bbox="399 1650 1187 1724">2.2.1.5 LSA Trust Record Flags</td> <td data-bbox="1187 1650 1414 1724">Created new section</td> </tr> <tr> <td data-bbox="399 1724 1187 1799">2.2.2.6 LSAPR_REVISION_INFO_V1</td> <td data-bbox="1187 1724 1414 1799">Created new section</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
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															

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

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

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



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

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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

September 15, 2017 - [Download](#)

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

This topic lists the Errata found in [MS-MDE2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

To view a PDF 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
2022/12/30	<p>&lt;14&gt; Section 3.1.4.1.3.1 DiscoveryRequest: Product note &lt;14&gt; 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>&lt;15&gt; Section 3.1.4.1.3.2 DiscoveryResponse</p> <p>&lt;16&gt; Section 3.3.4.1.1.2 GetPoliciesResponse</p> <p>&lt;17&gt; Section 3.3.4.1.1.2 GetPoliciesResponse</p>

Errata Published*	Description
	<p>&lt;20&gt; Section 3.4.4.1.1.1.1 RequestSecurityToken using Federated Authentication</p> <p>&lt;23&gt; Section 3.4.4.1.1.1.2 RequestSecurityToken using Certificate Authentication</p> <p>&lt;26&gt; Section 3.4.4.1.1.1.3 RequestSecurityToken using On-Premise Authentication</p> <p>Changed From:</p> <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:</p> <p>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>&lt;14&gt; 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:</p> <p>RequestVersion value 5.0 is supported only in the Windows 11, version 22H2 operating system and later.</p> <p>Changed To:</p> <p>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>&lt;15&gt; Section 3.1.4.1.3.2 DiscoveryResponse</p> <p>&lt;16&gt; Section 3.3.4.1.1.2 GetPoliciesResponse</p> <p>&lt;17&gt; Section 3.3.4.1.1.2 GetPoliciesResponse</p> <p>&lt;20&gt; Section 3.4.4.1.1.1.1 RequestSecurityToken using Federated Authentication</p> <p>&lt;23&gt; Section 3.4.4.1.1.1.2 RequestSecurityToken using Certificate Authentication</p> <p>&lt;26&gt; Section 3.4.4.1.1.1.3 RequestSecurityToken using On-Premise Authentication</p> <p>Changed From:</p> <p>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:</p> <p>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 the Errata found in [MS-MDM] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

To view a PDF 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.&lt;16&gt;</p> <p>&lt;16&gt; 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.&lt;16&gt;</p> <p>&lt;16&gt; 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>

Errata Published*	Description
	<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.&lt;9&gt; 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.&lt;9&gt; 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.&lt;10&gt;</p> <p>Appendix B:</p> <p>&lt;10&gt; 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.&lt;15&gt; To allow configuration of user settings, the MDM server must support "multi-user AVD" mode...</p> <p>&lt;15&gt; 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 the Errata found in [MS-MICE] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

December 1, 2017 - [Download](#)

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

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



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

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

June 30, 2015 - [Download](#)



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

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



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

No errata are available for the latest version of 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 the Errata found in the Windows Protocols Technical Specifications, Overview Documents, and Reference documents since they were last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**

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



No errata are available for the latest version of 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 the Errata found in the MS-NCNBI document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications. Errata are subject to the same terms as the Open Specifications documentation referenced.



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</p>

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

## [MS-NCT]: Network Cost Transfer Protocol

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



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

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

June 1, 2017 - [Download](#)

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

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



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

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

June 1, 2017 - [Download](#)

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

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



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

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

June 1, 2017 - [Download](#)

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

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



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

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

June 1, 2017 - [Download](#)

December 1, 2017 - [Download](#)



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

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



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

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



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

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

December 1, 2017 - [Download](#)

## [MS-NNS]: .NET NegotiateStream Protocol

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



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

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



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

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 style="padding-left: 40px;">BinaryMethodCall: RecordTypeEnum: BinaryMethodCall (0x21) MessageEnum: 00000014</p> <p>Changed to:</p> <p style="padding-left: 40px;">BinaryMethodCall: RecordTypeEnum: BinaryMethodCall (0x15) MessageEnum: 00000014</p>

\*Date format: YYYY/MM/DD

## [MS-NRPC]: Netlogon Remote Protocol

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

September 23, 2019 - [Download](#)

August 24, 2020 - [Download](#)

April 7, 2021 - [Download](#)

June 24, 2021 - [Download](#)

April 29, 2022 - [Download](#)

Errata below are for Protocol Document Version [V40.0 2022/04/29](#).

Errata Published*	Description
2022/11/08	<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 &lt;69&gt; 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&lt;69&gt; 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.&lt;70&gt;</p>

Errata Published*	Description
	<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.&lt;69&gt;</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.&lt;75&gt;</p> <ol style="list-style-type: none"> <li>1. The client SHOULD&lt;76&gt; bind to the RPC server using TCP/IP.</li> </ol> <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> <ol style="list-style-type: none"> <li>2. ...</li> <li>3. ...</li> <li>4. If secure bind is not used, the server MUST deny the request unless client is in the VulnerableChannelAllowList setting.&lt;77&gt;</li> </ol> <p>&lt;75&gt; 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 <a href="#">[MSFT-CVE-2020-1472]</a>.</p> <p>Changed to:</p> <p>The client and server follow this sequence of steps.&lt;74&gt;</p> <ol style="list-style-type: none"> <li>1. The client SHOULD&lt;75&gt; bind to the RPC server using TCP/IP.</li> </ol> <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> <ol style="list-style-type: none"> <li>2. ...</li> </ol>

Errata Published*	Description
	<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.&lt;76&gt;</p> <p>&lt;74&gt; 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 <a href="#">[MSFT-CVE-2020-1472]</a> and <a href="#">[MSFT-CVE-2022-38023]</a>.</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&lt;87&gt; 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&lt;87&gt; 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> <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&lt;92&gt; be initialized to TRUE.</p> <p>Changed to:</p> <p>RequireSignOrSeal MUST&lt;92&gt; 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>

Errata Published*	Description
	<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	<p>In section 1.3.1 Pass-Through Authentication: Added little endian usage statement.</p> <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.&lt;24&gt;</p> <p>&lt;24&gt; 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</p>



<b>Errata Published*</b>	<b>Description</b>
	<p>ServerSessionInfo table entry for PrimaryName) and the session key established as the encryption key.</p> <p>Changed to:</p> <p>Encrypt &lt;98&gt; 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>&lt;98&gt; 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&lt;178&gt; as specified in Calling NetrServerPasswordSet2 (section 3.4.5.2.5).</p> <p>&lt;178&gt; 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 the Errata found in [MS-NSPI] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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

June 1, 2017 - [Download](#)

## [MS-OAPX]: OAuth 2.0 Protocol Extensions

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



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

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



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

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

July 18, 2016 - [Download](#)

September 26, 2016 - [Download](#)

June 1, 2017 - [Download](#)

September 15, 2017 - [Download](#)

September 12, 2018 - [Download](#)

October 6, 2021 - [Download](#)

## [MS-OCSPA]: Microsoft OCSP Administration Protocol

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



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

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



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

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



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

No errata are available for the latest version of 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 the Errata found in [MC-OLEPS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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



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

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



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

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

November 23, 2020 - [Download](#)

April 29, 2022 - [Download](#)

Errata below are for Protocol Document Version [V23.0 – 2022/04/29](#).

Errata Published*	Description
2023/02/27	<p>Section 2.4 PAC_INFO_BUFFER, in the ulType table clarified 4 checksums for Kerberos ticket-granting service (TGS) requests or Kerberos application protocol (AP) requests.</p> <p>Changed from:</p> <p>...</p> <p>0x00000006 Server checksum (section 2.8). PAC structures MUST contain one buffer of this type. Additional logon server checksum buffers MUST be ignored.</p> <p>...</p> <p>0x00000007 KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type. Additional KDC checksum buffers MUST be ignored.</p> <p>...</p> <p>0x00000010 Ticket checksum (section 2.8). PAC structures SHOULD NOT contain more than one buffer of this type. Additional ticket checksum buffers MUST be ignored.&lt;7&gt;</p> <p>...</p> <p>0x00000013 Extended KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type. Additional KDC checksum buffers MUST be ignored.</p> <p>Changed to:</p> <p>...</p> <p>0x00000006 Server checksum (section 2.8). PAC structures MUST contain one buffer of this type for Kerberos ticket-granting service (TGS) requests or Kerberos application protocol (AP) requests, and none otherwise. Additional logon server checksum buffers MUST be ignored.</p>

Errata Published*	Description												
	<p>0x00000007 KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type for Kerberos ticket-granting service (TGS) requests or Kerberos application protocol (AP) requests, and none otherwise. Additional KDC checksum buffers MUST be ignored.</p> <p>...</p> <p>0x00000010 Ticket checksum (section 2.8). PAC structures MUST contain one buffer of this type for Kerberos ticket-granting service (TGS) requests, and none otherwise. Additional ticket checksum buffers MUST be ignored.&lt;7&gt;</p> <p>...</p> <p>0x00000013 Extended KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type for Kerberos ticket-granting service (TGS) requests, and none otherwise. Additional Extended KDC checksum buffers MUST be ignored.</p>												
2023/02/27	<p>In section 2.4 PAC_INFO_BUFFER, added to ulType: ...Types that are not understood MUST be ignored.</p> <p>Changed from:</p> <p>ulType (4 bytes): A 32-bit unsigned integer in little-endian format that describes the type of data present in the buffer contained at Offset.</p> <p>Changed to:</p> <p>ulType (4 bytes): A 32-bit unsigned integer in little-endian format that describes the type of data present in the buffer contained at Offset. Types that are not understood MUST be ignored.</p>												
2022/12/12	<p>The following sections were changed. Please see the <a href="#">diff document</a> for the details.</p> <p>In section 2.4 PAC_INFO_BUFFER: Added new required ulType 0x00000013 for Extended KDC (privilege server) checksum buffer.</p> <p>Changed from:</p> <table border="1" data-bbox="418 1207 1396 1465"> <thead> <tr> <th data-bbox="418 1207 909 1260">Value</th> <th data-bbox="909 1207 1396 1260">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="418 1260 909 1312">...</td> <td data-bbox="909 1260 1396 1312"></td> </tr> <tr> <td data-bbox="418 1312 909 1465">0x00000012</td> <td data-bbox="909 1312 1396 1465">PAC Requestor indicates that the buffer contains the SID of principal that requested the PAC (section 2.15). PAC structures MUST contain one buffer of this type.&lt;9&gt;</td> </tr> </tbody> </table> <p>Changed to:</p> <table border="1" data-bbox="418 1507 1409 1766"> <thead> <tr> <th data-bbox="418 1507 915 1560">Value</th> <th data-bbox="915 1507 1409 1560">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="418 1560 915 1612">...</td> <td data-bbox="915 1560 1409 1612"></td> </tr> <tr> <td data-bbox="418 1612 915 1766">0x00000012</td> <td data-bbox="915 1612 1409 1766">PAC Requestor indicates that the buffer contains the SID of principal that requested the PAC (section 2.15). PAC structures MUST contain one buffer of this type.&lt;9&gt;</td> </tr> </tbody> </table>	Value	Meaning	...		0x00000012	PAC Requestor indicates that the buffer contains the SID of principal that requested the PAC (section 2.15). PAC structures MUST contain one buffer of this type.<9>	Value	Meaning	...		0x00000012	PAC Requestor indicates that the buffer contains the SID of principal that requested the PAC (section 2.15). PAC structures MUST contain one buffer of this type.<9>
Value	Meaning												
...													
0x00000012	PAC Requestor indicates that the buffer contains the SID of principal that requested the PAC (section 2.15). PAC structures MUST contain one buffer of this type.<9>												
Value	Meaning												
...													
0x00000012	PAC Requestor indicates that the buffer contains the SID of principal that requested the PAC (section 2.15). PAC structures MUST contain one buffer of this type.<9>												

Errata Published*	Description		
	<table border="1" data-bbox="423 226 1409 352"> <tr> <td data-bbox="423 226 915 352">0x00000013</td> <td data-bbox="915 226 1409 352">Extended KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type. Additional KDC checksum buffers MUST be ignored.</td> </tr> </table> <p data-bbox="402 365 1349 417">In section 2.8.1 Server Signature: Added that the server signature MUST be generated AFTER the extended KDC signature.</p> <p data-bbox="402 424 565 449">Changed from:</p> <p data-bbox="402 457 1243 510">... The resulting hash value is then placed in the Signature field of the server's PAC_SIGNATURE_DATA structure.</p> <p data-bbox="402 552 537 577">Changed to:</p> <p data-bbox="402 583 1243 636">... The resulting hash value is then placed in the Signature field of the server's PAC_SIGNATURE_DATA structure.</p> <p data-bbox="402 644 1401 669">The server signature MUST be generated AFTER the extended KDC signature (section 2.3.4).</p> <p data-bbox="402 711 1357 737">Section 2.8.3 Ticket Signature: Added the extended KDC signature in the recompute list.</p> <p data-bbox="402 745 565 770">Changed from:</p> <p data-bbox="402 779 1382 831">... the KDC SHOULD verify the integrity of the existing ticket signature and then recompute the ticket signature, server signature, and KDC signature in the PAC.</p> <p data-bbox="402 840 537 865">Changed to:</p> <p data-bbox="402 873 1382 947">... the KDC SHOULD verify the integrity of the existing ticket signature and then recompute the ticket signature, server signature, KDC signature, and extended KDC signature in the PAC.</p> <p data-bbox="402 989 1044 1014">Section 2.8.4 Extended KDC Signature: Added new section.</p> <p data-bbox="402 1022 1414 1178">Describes its usage and contents. It is used to detect tampering of PACs by parties other than the KDC. Describes where to use it in tickets for various accounts. Contains the ulType 0x00000013 same as described in section 2.4 PAC_INFO_BUFFER. Contains the SignatureType and its key. It is comprised of keyed hash of the entire PAC message with all other Signature fields of all other PAC_SIGNATURE_DATA structures set to zero. It is placed in the Signature field of the extended KDC's PAC_SIGNATURE_DATA structure (section 2.8).</p>	0x00000013	Extended KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type. Additional KDC checksum buffers MUST be ignored.
0x00000013	Extended KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type. Additional KDC checksum buffers MUST be ignored.		

## [MS-PAR]: Print System Asynchronous Remote Protocol

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



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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

## [MS-PKAP]: Public Key Authentication Protocol

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



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

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



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

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

October 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&lt;22&gt; 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"><li>• SAN UPNName</li><li>• SAN DNSName</li><li>• altSecurityIdentities Issuer Name and Subject Name</li><li>• altSecurityIdentities Subject Name</li><li>• altSecurityIdentities 822 field</li></ul> <p>The following mappings are considered strong:</p> <ul style="list-style-type: none"><li>• SID (section 3.1.5.2.1.6)</li><li>• Key Trust (section 3.1.5.2.1.4)</li><li>• altSecurityIdentities Issuer and Serial Number</li><li>• altSecurityIdentities Subject Key Identifier</li><li>• altSecurityIdentities SHA1 Hash of Public Key</li></ul> <p>If a KDC maps a certificate to a user using one of the above weak mappings, it SHOULD&lt;23&gt; 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="402 260 1403 310">&lt;22&gt; Section 3.1.5.2.1.5 Certificate mapping strength is applicable to Windows Server 2008 R2 and later.</p> <p data-bbox="402 352 1403 403">&lt;23&gt; Section 3.1.5.2.1.5 Certificate mapping strength is applicable to Windows Server 2008 R2 and later.</p> <p data-bbox="402 445 829 474">Section 3.1.5.2.1.6 SID: added section.</p> <p data-bbox="402 516 1409 697">If a KDC has exhausted all other mapping types for a certificate and found a weak mapping without finding a strong mapping, it SHOULD&lt;24&gt; 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="402 739 1386 789">&lt;24&gt; 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 the Errata found in [MS-PSRDP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

## [MS-PSRP]: PowerShell Remoting Protocol

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

## [MS-RA]: Remote Assistance Protocol

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

## [MS-RAI]: Remote Assistance Initiation Protocol

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

April 7, 2021 - [Download](#)

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

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



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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

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										
2022/01/04	<p>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>Changed from:</p> <table border="1"><thead><tr><th>Value</th><th>Meaning</th></tr></thead><tbody><tr><td>0x00080001</td><td>RDP 4.0 clients</td></tr><tr><td>0x00080004</td><td>RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 clients</td></tr><tr><td>0x00080005</td><td>RDP 10.0 clients</td></tr><tr><td>0x00080006</td><td>RDP 10.1 clients</td></tr></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
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										

Errata Published*	Description																													
	0x00080007	RDP 10.2 clients																												
	0x00080008	RDP 10.3 clients																												
	0x00080009	RDP 10.4 clients																												
	0x0008000A	RDP 10.5 clients																												
	0x0008000B	RDP 10.6 clients																												
	0x0008000C	RDP 10.7 clients																												
	0x0008000D	RDP 10.8 clients																												
	0x0008000E	RDP 10.9 clients																												
	Changed to:																													
	<table border="1"> <thead> <tr> <th data-bbox="440 737 638 793">Value</th> <th data-bbox="638 737 1430 793">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="440 793 638 850">0x00080001</td> <td data-bbox="638 793 1430 850">RDP 4.0 clients</td> </tr> <tr> <td data-bbox="440 850 638 907">0x00080004</td> <td data-bbox="638 850 1430 907">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="440 907 638 963">0x00080005</td> <td data-bbox="638 907 1430 963">RDP 10.0 clients</td> </tr> <tr> <td data-bbox="440 963 638 1020">0x00080006</td> <td data-bbox="638 963 1430 1020">RDP 10.1 clients</td> </tr> <tr> <td data-bbox="440 1020 638 1077">0x00080007</td> <td data-bbox="638 1020 1430 1077">RDP 10.2 clients</td> </tr> <tr> <td data-bbox="440 1077 638 1134">0x00080008</td> <td data-bbox="638 1077 1430 1134">RDP 10.3 clients</td> </tr> <tr> <td data-bbox="440 1134 638 1190">0x00080009</td> <td data-bbox="638 1134 1430 1190">RDP 10.4 clients</td> </tr> <tr> <td data-bbox="440 1190 638 1247">0x0008000A</td> <td data-bbox="638 1190 1430 1247">RDP 10.5 clients</td> </tr> <tr> <td data-bbox="440 1247 638 1304">0x0008000B</td> <td data-bbox="638 1247 1430 1304">RDP 10.6 clients</td> </tr> <tr> <td data-bbox="440 1304 638 1360">0x0008000C</td> <td data-bbox="638 1304 1430 1360">RDP 10.7 clients</td> </tr> <tr> <td data-bbox="440 1360 638 1417">0x0008000D</td> <td data-bbox="638 1360 1430 1417">RDP 10.8 clients</td> </tr> <tr> <td data-bbox="440 1417 638 1474">0x0008000E</td> <td data-bbox="638 1417 1430 1474">RDP 10.9 clients</td> </tr> <tr> <td data-bbox="440 1474 638 1530">0x0008000F</td> <td data-bbox="638 1474 1430 1530">RDP 10.10 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	0x0008000E	RDP 10.9 clients	0x0008000F	RDP 10.10 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																													
	In section 2.2.1.4.2, Server Core Data (TS_UD_SC_CORE), added the server version number for RDP 10.10:																													
	Changed from: <table border="1"> <thead> <tr> <th data-bbox="440 1577 638 1703">Value</th> <th data-bbox="638 1577 1430 1703">Meaning</th> </tr> </thead> <tbody> <tr> <td data-bbox="440 1703 638 1759">0x00080001</td> <td data-bbox="638 1703 1430 1759">RDP 4.0 servers</td> </tr> <tr> <td data-bbox="440 1759 638 1808">0x00080004</td> <td data-bbox="638 1759 1430 1808">RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 servers</td> </tr> </tbody> </table>		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																						
Value	Meaning																													
0x00080001	RDP 4.0 servers																													
0x00080004	RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, and 8.1 servers																													



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

\*Date format: YYYY/MM/DD

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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

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

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



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

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
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> <p>Changed to:</p> <pre> 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 the Errata found in [MS-RDPECLIP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

To view a PDF 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 ..... </pre>

Errata Published*	Description
	<p>00000010 02 00 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 .....</p> <p>00000020 00 00 00 00 00 00 00 00 00 .....</p> <p>Changed to:</p> <p>The following is an annotated dump of a File Contents Request PDU (section 2.2.5.3).</p> <p>00000000 08 00 00 00 18 00 00 00 02 00 00 00 01 00 00 00 .....</p> <p>00000010 02 00 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 the Errata found in [MS-RDPECAM] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

No errata are available for the latest version of 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 the Errata found in the MS-RDPEDISP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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



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

No errata are available for the latest version of this Windows Protocols document. To view a PDF 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 the Errata found in [MS-RDPEFS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

June 1, 2017 - [Download](#)

September 15, 2017 - [Download](#)

December 1, 2017 - [Download](#)

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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

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

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



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

No errata are available for the latest version of this Windows Protocols document. To view a PDF 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](#)

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

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



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

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

June 1, 2017 - [Download](#)

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

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



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

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



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

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



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

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

July 18, 2016 - [Download](#)

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

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



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

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

March 2, 2016 - [Download](#)

April 7, 2021 - [Download](#)



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

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



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

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



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

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

July 18, 2016 - [Download](#)

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

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



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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

June 1, 2017 - [Download](#)

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

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



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

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

July 18, 2016 - [Download](#)

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

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



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

No errata are available for the latest version of 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 the Errata found in [MS-RDPEUDP2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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>



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

\*Date format: YYYY/MM/DD

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

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



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

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

July 18, 2016 - [Download](#)

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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

June 1, 2017 - [Download](#)

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

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



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

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

July 18, 2016 - [Download](#)

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

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



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

No errata are available for the latest version of this Windows Protocols document. To view a PDF 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 the Errata found in [MS-RMPR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

No errata are available for the latest version of this Windows Protocols document. To view a PDF 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 the Errata found in [MS-RMSOD] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

No errata are available for the latest version of this Windows Protocols document. To view a PDF 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 the Errata found in the Windows Protocols Technical Specifications, Overview Documents, and Reference documents since they were last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

Errata 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>	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														
...																			
MS-RDG-Device-Redirection	0	0-1	0	0	0														



Errata Published*	Description					
	Microsoft vendor-specific attribute	Request	Accept	Reject	Challenge	Accounting-Request
	. . .					
	MS-RDG-Device-Redirection	0	0-1	0	0	0
	MS-Azure-Policy-ID	0	0-1	0	0	0
	<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 the Errata found in the MS-RPCE document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**

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



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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

## [MS-RPRN]: Print System Remote Protocol

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

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



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

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

July 18, 2016 - [Download](#)

April 7, 2021 - [Download](#)

## [MS-RRP]: Windows Remote Registry Protocol

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

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



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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

June 1, 2017 - [Download](#)

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

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



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

No errata are available for the latest version of this Windows Protocols document. To view a PDF 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 the Errata found in [MS-SAMR] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

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"><li>• SamrCloseHandle: This method releases server resources associated with the RPC context handle that is passed as a parameter.</li></ul> <p>Changed to:</p> <ul style="list-style-type: none"><li>• SamrCloseHandle: This method releases server resources associated with the RPC context handle that is passed as a parameter.</li><li>• SamrValidateComputerAccountReuseAttempt: This method validates whether a client attempt to re-use a given computer account is permitted.</li></ul> <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.&lt;pbn72&gt;</p> <p>&lt;pbn72&gt;: 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 <b>2.2.1.18</b>, 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="402 457 1414 911"> <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="402 953 1414 1646"> <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"> <li>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.</li> </ul> <p>Changed to:</p> <ul style="list-style-type: none"> <li>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.</li> <li>For SamrUnicodeChangePasswordUser4 and SamrSetInformationUser2, the secret plaintext MUST be in the format specified in section 2.2.6.32.</li> </ul> <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</p> <p>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:</p> <p>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:</p> <p>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.</p> <p>The Iteration Count MUST be between 5000 and 1,000,000 inclusive.</p> <p>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 the Errata found in the MS-KPP document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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

June 1, 2017 - [Download](#)

## [MS-SCMR]: Service Control Manager Remote Protocol

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



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

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



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

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



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

No errata are available for the latest version of 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 the Errata found in the MS-SFU document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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</p>

Errata Published*	Description
	<p>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> <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"> <li>• 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".</li> </ul> <p>Changed to:</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>
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,&lt;22&gt; 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,&lt;22&gt; then the KDC MUST return KRB-ERR-BADOPTION with STATUS_ACCOUNT_RESTRICTION ([MS-ERREF] section 2.3.1).&lt;23&gt;</p> <p>&lt;23&gt; 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 the Errata found in [MS-SMB] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

No errata are available for the latest version of this Windows Protocols document. To view a PDF 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 the Errata found in [MS-SMB2] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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

March 4, 2020 - [Download](#)

August 24, 2020 - [Download](#)

April 7, 2021 - [Download](#)

June 1, 2021 - [Download](#)

October 6, 2021 - [Download](#)

April 29, 2022 - [Download](#)

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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

April 7, 2021 - [Download](#)

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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

April 29, 2022 - [Download](#)

## [MS-SQOS]: Storage Quality of Service Protocol

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



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

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

July 18, 2016 - [Download](#)

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

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



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

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"><li>1. The default maximum transmission unit (MTU) is set to 1400 bytes.</li><li>2. The maximum receive unit (MRU) exchanged for SSTP is 4091 bytes, which is 4095 – sizeof(SSTP_HEADER).</li><li>3. The default MTU can be increased using the registry values, but it is still capped at the MRU of the tunnel type.</li><li>4. The default MRU for the PPP adapter is set to 1614 bytes.</li><li>5. The default MRU can be increased by setting the following registry value: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NdisWan\Parameters\MRU</li></ol> <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 the Errata found in the [MS-SSTR] document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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.&lt;1&gt;</p> <p>&lt;1&gt; 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.&lt;1&gt;&lt;2&gt;</p> <p>&lt;1&gt; Section 1.5: For requirements to enable cloud-based Smooth Streaming of High Efficiency Video Coding (HEVC) encoded video see the amendment for HEVC <a href="#">[MSDOCS-SSTR-HEVC]</a>.</p> <p>&lt;2&gt; Section 1.5: The Smooth Streaming Protocol is supported...</p>

\*Date format: YYYY/MM/DD

## [MS-SWN]: Service Witness Protocol

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



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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

## [MS-TDS]: Tabular Data Stream Protocol

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



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

No errata are available for the latest version of this Windows Protocols document. To view a PDF 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 the Errata found in [MS-TLSP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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

July 18, 2016 - [Download](#)

September 15, 2017 - [Download](#)

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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

## [MS-TSCH]: Task Scheduler Service Remoting Protocol

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



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

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

July 18, 2016 - [Download](#)

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

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



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

No errata are available for the latest version of this Windows Protocols document. To view a PDF 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 the Errata found in [MS-TSTS] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

April 7, 2021 - [Download](#)

## [MS-TSWP]: Terminal Services Workspace Provisioning Protocol

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



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

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

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

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

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

June 1, 2017 - [Download](#)

## [MS-UCODEREF]: Windows Protocols Unicode Reference

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

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

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



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

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

June 1, 2017 - [Download](#)

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

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



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

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

June 1, 2017 - [Download](#)

April 7, 2021 - [Download](#)

April 29, 2022 - [Download](#)

## [MS-W32T]: W32Time Remote Protocol

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



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

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

June 1, 2017 - [Download](#)

# [MS-WCCE]: Windows Client Certificate Enrollment Protocol

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



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

To view a PDF 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...\nTemplateNameN\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</p>



Errata Published*	Description
	<p>certificate administrative operations, the CA MUST deny a connection to the client and return a non-zero error. &lt;7&gt;</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. &lt;7&gt; &lt;8&gt;</p> <p>&lt;8&gt; The operating systems specified in <a href="#">[MSFT-CVE-2022-37976]</a>, 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. &lt;70&gt;</p> <p>&lt;70&gt;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. &lt;82&gt;</p>

Errata Published*	Description
	<p>&lt;82&gt;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. &lt;85&gt;</p> <p>&lt;85&gt;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&lt;88&gt;</p> <p>&lt;88&gt;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</p>

Errata Published*	Description
	<p>administrative operations to ensure a connection to the CA server is not denied. Also specified the operating 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. &lt;108&gt;</p> <p>&lt;108&gt;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 the Errata found in [MS-WCFESAN] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

July 18, 2016 - [Download](#)

## [MS-WDHCE]: Wi-Fi Display Protocol Hardware Cursor Extension

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



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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

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

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



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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

June 1, 2017 - [Download](#)



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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

March 20, 2017 - [Download](#)

June 1, 2017 - [Download](#)

## [MS-WKST]: Workstation Service Remote Protocol

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



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

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.</p> <p>versionbyte = 0x01 versionbyte_len = 1 algorithmString = "AEAD-AES-256-CBC-HMAC-SHA512"</p> <p>EncryptKey and MACKey are calculated as follows:</p> <p>EncryptKey := HMAC-SHA-512(SessionKey, "Microsoft WKST encryption key" + algorithmString + Length(SessionKey)) MACKey := HMAC-SHA-512(SessionKey, "Microsoft WKST MAC key" + algorithmString + Length(SessionKey))</p> <p>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>

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

EncryptKey and MACKey are calculated as follows:  
EncryptKey := HMAC-SHA-512(SessionKey, WKST\_AES256\_ENC\_KEY\_STRING)  
MACKey := HMAC-SHA-512(SessionKey, WKST\_AES256\_MAC\_KEY\_STRING)  
Note that the SessionKey is calculated as in section 2.2.5.19.2. See [RFC4868] for details of the HMAC-SHA-512 algorithm.

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

Changed from:

Encrypt the encoded password as follows:

Salt := Randomly generated 16 bytes  
Cipher := AES-CBC( EncryptKey[0:256], IV, EncodedPasswordLength(4 bytes) + EncodedPassword)  
AuthData := HMAC-SHA-512(MACKey, Cipher+Salt+ versionbyte + versionbyte\_len)  
Note that the Salt value is used as the initialization vector (IV). The MACKey is calculated in section 2.2.5.19.3.

Changed to:

Encrypt the encoded password as follows:  
Salt := Randomly generated 16 bytes  
Encoded\_Plaintext:= EncodedPasswordlength (4 bytes) + EncodedPassword.  
Cipher := AES-CBC( EncryptKey[0:256], IV, Encoded\_Plaintext)  
AuthData := HMAC-SHA-512(MACKey, Cipher+Salt+ versionbyte + versionbyte\_len)  
Note that the Salt value is used as the initialization vector (IV). The MACKey is calculated in section 2.2.5.19.3.  
Note that EncryptKey is truncated to 32 bytes and the entire 64-byte MACKey is used.

\*Date format: YYYY/MM/DD

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

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



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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

April 7, 2021 - [Download](#)

## [MS-WPO]: Windows Protocols Overview

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

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

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



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

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

March 20, 2017 - [Download](#)

June 1, 2017 - [Download](#)



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

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



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

No errata are available for the latest version of this Windows Protocols document. To view a PDF 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 the Errata found in [MS-WSP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.**



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)

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



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

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"><li>• &lt;xs:element ref="wsse:BinarySecurityToken" /&gt;</li><li>• &lt;xs:element ref="wsse:SecurityTokenReference" /&gt;</li></ul> <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"><li>• &lt;xs:element ref="wsse:BinarySecurityToken" /&gt;</li><li>• &lt;xs:element ref="wsse:SecurityTokenReference" /&gt;</li></ul> <p>The server SHOULD&lt;2&gt; 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>&lt;2&gt; 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 the Errata found in the MS-WSUSAR document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.



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

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



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

No errata are available for the latest version of 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-WSUOSS]: Windows Update Services: Server-Server Protocol

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



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

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

July 18, 2016 - [Download](#)

June 1, 2017 - [Download](#)

April 7, 2021 - [Download](#)

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

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



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

To view a PDF 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](#)

Errata below are for Protocol Document Version [V33.0 – 2022/04/29](#).

Errata Published*	Description
2022/09/20	<p>Section 2.2.2.2.6 GetExtendedUpdateInfo</p> <p>Description: Updated product behavior note 25 to read: The GeoId property is supported on Windows 11 v22H2 and later. It has also been backported to the down-level operating systems specified in [MSKB-5005101] and [MSKB-5014668], each with its related KB article download installed.</p> <p>Changed from:</p> <p>The GeoId property is supported in the down-level operating systems specified in [MSKB-5005101], each with its related KB article download installed. It is also supported on Windows 11 v22H2 and later.</p> <p>Changed to:</p> <p>The GeoId property is supported on Windows 11 v22H2 and later. It has also been backported to the down-level operating systems specified in [MSKB-5005101] and [MSKB-5014668], each with its related KB article download installed.</p> <p>Section 3.1.1.1 Populating the Data Model</p> <p>Description: Updated product behavior note 36 to read: The GeoId property is supported on Windows 11 v22H2 and later. It has also been backported to the down-level operating systems specified in [MSKB-5005101] and [MSKB-5014668], each with its related KB article download installed.</p> <p>Changed from:</p>

<b>Errata Published*</b>	<b>Description</b>
	<p>The GeoId property is supported on the down-level operating systems specified in [MSKB-5005101], each with its related KB article download installed. It is also supported on Windows 11 v22H2 and later.</p> <p>Changed to:</p> <p>The GeoId property is supported on Windows 11 v22H2 and later. It has also been backported to the down-level operating systems specified in [MSKB-5005101] and [MSKB-5014668], each with its related KB article download installed.</p>
2022/07/26	<p>Changed from:</p> <p>The SOAP operation is defined as follows.</p> <pre data-bbox="365 609 1412 724">&lt;wsdl:operation name="GetExtendedUpdateInfo2"&gt; &lt;soap:operation soapAction="http://www.microsoft.com/SoftwareDistribution/Server/ClientWebService/GetExtendedUpdateInfo2" style="document" /&gt;</pre> <p>Changed to:</p> <pre data-bbox="365 798 1412 871">&lt;soap:operation soapAction="http://www.microsoft.com/SoftwareDistribution/Server/ClientWebService/GetExtendedUpdateInfo2" style="document" /&gt;</pre>
2022/07/12	<p>In Section 2.2.2.2.10 GetExtendedUpdateInfo2, removed additional statement '&lt;wsdl:operation name="GetExtendedUpdateInfo2"&gt;' from SOAP operation definition.</p> <p>Changed from:</p> <p>The SOAP operation is defined as follows.</p> <pre data-bbox="365 1018 1412 1134">&lt;wsdl:operation name="GetExtendedUpdateInfo2"&gt; &lt;soap:operation soapAction="http://www.microsoft.com/SoftwareDistribution/Server/ClientWebService/GetExtendedUpdateInfo2" style="document" /&gt;</pre> <p>Changed to:</p> <pre data-bbox="365 1176 1412 1249">&lt;soap:operation soapAction="http://www.microsoft.com/SoftwareDistribution/Server/ClientWebService/GetExtendedUpdateInfo2" style="document" /&gt;</pre>

\*Date format: YYYY/MM/DD



## [MS-XCA]: Xpress Compression Algorithm

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



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

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>

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

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

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



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

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

October 16, 2015 - [Download](#)

June 30, 2015 - [Download](#)