Windows Protocols Errata

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

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

RSS
Atom

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

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

[MS-ABTP]: Automatic Bluetooth Pairing Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V3.0 – 2015/06/30.

Errata Published*	Description
2015/10/12	In Appendix A, Product Behavior, added the following Windows Server version: Windows Server 2012 R2 operating system

*Date format: YYYY/MM/DD

[MS-ADA2]: Active Directory Schema Attributes M

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

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

RSS
Atom

Errata below are for Protocol Document Version V27.0 – 2015/06/30

Errata Published*	Description
2015/07/20	In two sections, the descriptions for msDFSR-Extension and msDFSR-TombstoneExpiryInMin have been revised. In Section 2.158, Attribute msDFSR-Extension, changed from: This attribute is reserved for future use. Changed to: This attribute specifies a value used by the Distributed File System Replication Protocol to specify files that should not be compressed. In Section 2.183, Attribute msDFSR-TombstoneExpireyInMin, changed from: This attribute is reserved for future use. Changed to: This attribute specifies a value used by the Distributed File System Replication Protocol to specify a tombstone expiration in minutes for a replication group or replicated folder.

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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 ERRATA June 30 2015 Archive here.

[MS-ADSC]: Active Directory Schema Classes

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-ADTS]: Active Directory Technical Specification

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V41.0 – 2015/06/30.

Errata Published*	Description

2015/10/12	In Section 6.2.2.3.4.5, nTDSConnection Creation, clarified the pseudocode to show when failed DCs are filtered out.
	
	Changed from:
	
	`...`
	
	`CALL CreateConnection(cr, rbh, t, lbh, e.ReplInfo, sched, partialReplicaOkay)`
	`ENDFOR`
	
	`RETURN connected`
	`}`
	`...`
	`CreateConnection(IN crossRef cr, IN nTDSDSA rbh, IN interSiteTransport t, IN nTDSDSA lbh, IN REPLINFO ri, IN SCHEDULE sch, INOUT SEQUENCE<GUID> keepConnections)`
	`{`
	`LET rsiteGuid be the objectGUID of the site object ancestor of rbh`
	`LET lsiteGuid be the objectGUID of the site object ancestor of lbh`
	
	`LET rbhsAll be the result of GetAllBridgeheadDCs(rsiteGuid, cr, t, partialReplicaOkay, FALSE)`
	`LET rbhsAvail be the result of GetAllBridgeheadDCs(rsiteGuid, cr, t, partialReplicaOkay, detectFailedDCs)`
	`LET lbhsAll be the result of GetAllBridgeheadDCs(lsiteGuid, cr, t, partialReplicaOkay, FALSE)`
	`LET lbhsAvail be the result of GetAllBridgeheadDCs(lsiteGuid, cr, t, partialReplicaOkay, detectFailedDCs)`
	`...`
	
	Changed to:
	
	`...`
	
	`CALL CreateConnection(cr, rbh, t, lbh, e.ReplInfo, sched, detectFailedDCs, partialReplicaOkay, keepConnections)`
	`ENDFOR`

Errata Published*	Description

	RETURN connected
	}
	
	...
	CreateConnection(IN crossRef cr, IN nTDSDSA rbh,
	IN interSiteTransport t, IN nTDSDSA lbh, IN REPLINFO ri,
	IN SCHEDULE sch, IN bool detectFailedDCs, IN bool partialReplicaOkay,
	INOUT SEQUENCE<GUID> keepConnections)
	{
	LET rsiteGuid be the objectGUID of the site object ancestor of rbh
	LET lsiteGuid be the objectGUID of the site object ancestor of lbh
	
	LET rbhsAll be the result of GetAllBridgeheadDCs(rsiteGuid, cr,
	t, partialReplicaOkay, FALSE)
	LET lbhsAll be the result of GetAllBridgeheadDCs(lsiteGuid, cr,
	t, partialReplicaOkay, FALSE)

2015/09/28	In Section 6.2.2.4, Removing Unnecessary Connections, clarified when and how a KCC deletes a connection. Changed from: Given an nTDSConnection object cn, if the DC with the nTDSDSA object dc that is the parent object of cn and the DC with the nTDSDA object referenced by cn!fromServer are in the same site, the KCC on dc deletes cn if all of the following are true: ▪ Bit NTDSCONN_OPT_IS_GENERATED is clear in cn!options. ▪ No site settings object s exists for the local DC's site, or bit NTDSSETTINGS_OPT_IS_TOPL_CLEANUP_DISABLED is clear in s!options. ▪ Another nTDSConnection object cn2 exists such that cn and cn2 have the same parent object, cn!fromServer = cn2!fromServer, and either ▪ cn!whenCreated < cn2!whenCreated ▪ cn!whenCreated = cn2!whenCreated and cn!objectGUID < cn2!objectGUID ▪ Bit NTDSCONN_OPT_RODC_TOPOLOGY is clear in cn!options Given an nTDSConnection object cn, if the DC with the nTDSDSA object dc that is the parent object of cn and the DC with the nTDSDSA object referenced by cn!fromServer are in different sites, a KCC acting as an ISTG in dc's site deletes cn if all of the following are true: ▪ Bit NTDSCONN_OPT_IS_GENERATED is clear in cn!options. ▪ cn!fromServer references an nTDSDSA object for a DC in a site other than the local DC's site. Changed to: Given an nTDSConnection object cn, if the DC with the nTDSDSA object dc that is the parent object of cn and the DC with the nTDSDA object referenced by cn!fromServer are in the same site, the KCC on dc deletes cn if all of the following are true: ▪ Bit NTDSCONN_OPT_IS_GENERATED is set in cn!options. ▪ No site settings object s exists for the local DC's site, or bit NTDSSETTINGS_OPT_IS_TOPL_CLEANUP_DISABLED is clear in s!options. ▪ Another nTDSConnection object cn2 exists such that cn and cn2 have the same parent object, cn!fromServer = cn2!fromServer, and either ▪ cn!whenCreated < cn2!whenCreated ▪ cn!whenCreated = cn2!whenCreated and cn!objectGUID < cn2!objectGUID ▪ Bit NTDSCONN_OPT_RODC_TOPOLOGY is clear in cn!options Given an nTDSConnection object cn, if the DC with the nTDSDSA object dc that is the parent object of cn and the DC with the nTDSDSA object referenced by cn!fromServer are in different sites, a KCC acting as an ISTG in dc's site deletes cn if all of the following are true: ▪ Bit NTDSCONN_OPT_IS_GENERATED is set in cn!options. ▪ cn!fromServer references an nTDSDSA object for a DC in a site other than the local DC's site.

Errata Published*	Description

2015/08/17	In Section 6.2.2.3.4.4, Spanning Tree Computation, modified the pseudo code for BridgeheadDCFailed so that the detectFailedDCs field is not a default value but a switch for detection.
	
	Changed from:
	
	`/***** BridgeheadDCFailed *****/`
	`/* Determine whether a given DC is known to be in a failed state.`
	`* IN: objectGUID - objectGUID of the DC's nTDSDSA object.`
	`* IN: detectFailedDCs - TRUE if and only failed DC detection is`
	`* enabled.`
	`* RETURNS: TRUE if and only if the DC should be considered to be in a`
	`* failed state.`
	`*/`
	`BridgeheadDCFailed(IN GUID objectGUID, IN bool detectFailedDCs) : bool`
	`{`
	`IF bit NTDSSETTINGS_OPT_IS_TOPL_DETECT_STALE_DISABLED is set in`
	`the options attribute of the site settings object for the local`
	`DC's site`
	`RETURN FALSE`
	`ELSEIF a tuple z exists in the kCCFailedLinks or`
	`kCCFailedConnections variables such that z.UUIDDsa =`
	`objectGUID, z.FailureCount > 1, and the current time -`
	`z.TimeFirstFailure > 2 hours`
	`RETURN TRUE`
	`ELSE`
	`RETURN detectFailedDCs`
	`ENDIF`
	`}`
	
	Changed to:
	
	`/***** BridgeheadDCFailed *****/`
	`/* Determine whether a given DC is known to be in a failed state.`
	`* IN: objectGUID - objectGUID of the DC's nTDSDSA object.`
	`* IN: detectFailedDCs - TRUE if and only if failed DC detection is`
	`* enabled.`
	`* RETURNS: TRUE if and only if the DC should be considered to be in a`
	`* failed state.`
	`*/`
	`BridgeheadDCFailed(IN GUID objectGUID, IN bool detectFailedDCs) : bool`
	`{`
	`IF detectFailedDCs is FALSE`
	`RETURN FALSE`
	`ENDIF`

Errata Published*	Description

	IF bit NTDSSETTINGS_OPT_IS_TOPL_DETECT_STALE_DISABLED is set in
	the options attribute of the site settings object for the local
	DC's site
	RETURN FALSE
	ENDIF
	
	IF a tuple z exists in the kCCFailedLinks or
	kCCFailedConnections variables such that
	z.UUIDDsa = objectGUID, z.FailureCount > 1, and
	the current time - z.TimeFirstFailure > 2 hours
	RETURN TRUE
	ENDIF
	
	RETURN FALSE
	}

	In Section 6.2.2.5, Connection Translation, revised the value assignment for uuidDsa during KCC connection translation from a 'GUID based DNS name' to a 'GUID'. Changed from: If s and the local DC's nTDSDSA object are in the same site, cn!transportType has no value, or the RDN of cn!transportType is CN=IP: ▪ Bit DRS_MAIL_REP in t.replicaFlags is clear. ▪ t.uuidTransport = NULL GUID. ▪ t.uuidDsa = The GUID-based DNS name of s. Otherwise: ▪ Bit DRS_MAIL_REP in t.replicaFlags is set. ▪ If x is the object with dsname cn!transportType, t.uuidTransport = x!objectGUID. ▪ Let a be the attribute identified by x!transportAddressAttribute. If a is the dNSHostName attribute, t.uuidDsa = the GUID-based DNS name of s. Otherwise, t.uuidDsa = (s!parent)!a. Finally, the KCC calls IDL_DRSReplicaAdd to add a tuple u to n!repsFrom for each IDL_DRSGetNCChanges server "implied" by the nTDSConnection object children of the local DC's nTDSDSA object if such a u does not already exist. For each such nTDSConnection cn, a tuple u is

Errata Published*	Description
	implied if all of the following are true: … Changed to: If s and the local DC's nTDSDSA object are in the same site, cn!transportType has no value, or the RDN of cn!transportType is CN=IP: ▪ Bit DRS_MAIL_REP in t.replicaFlags is clear. ▪ t.uuidTransport = NULL GUID. ▪ t.uuidDsa = s!objectGUID. Otherwise: ▪ Bit DRS_MAIL_REP in t.replicaFlags is set. ▪ If x is the object with dsname cn!transportType, t.uuidTransport = x!objectGUID. ▪ Let a be the attribute identified by x!transportAddressAttribute. If a is the dNSHostName attribute, t.uuidDsa = s!objectGUID. Otherwise, t.uuidDsa = (s!parent)!objectGUID. Finally, the KCC calls IDL_DRSReplicaAdd to add a tuple u to n!repsFrom for each IDL_DRSGetNCChanges server "implied" by the nTDSConnection object children of the local DC's nTDSDSA object if such a u does not already exist. For each such nTDSConnection cn, a tuple u is implied if all of the following are true: …
2015/08/03	In Section 7.6.2.4, Performing an LDAP Unbind Against a Directory Server, corrected the label of the input parameter from 'TaskInputLdapMessage' to 'TaskInputRequestMessage'. Changed from: 4. Invoke the Performing an LDAP Operation Against a Directory Server (section 7.6.2.5) task with the following parameters: TaskInputConnectionInfo is set to the TaskInputConnectionInfo that was passed to this task and TaskInputLdapMessage is set to ldapRequest. Changed to: 4. Invoke the Performing an LDAP Operation Against a Directory Server (section 7.6.2.5) task with the following parameters: TaskInputConnectionInfo is set to the TaskInputConnectionInfo that was passed to this task and TaskInputRequestMessage is set to ldapRequest.
2015/08/03	In two sections related to the SPN uniqueness checking logic, updated the text to account for the

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
availability of Windows Server 2012 R2 with [MSKB-3070083].
In Section 3.1.5.1.3, Uniqueness Constraints, changed from:
▪ In AD DS, if the DC functional level is DS_BEHAVIOR_WIN2012R2 or greater, then the new attribute value must be unique within the entire forest. If the DC is not a GC, then the DC should issue an LDAP search against a GC to determine uniqueness. The following additional considerations for uniqueness checking are relevant for Windows Server 2016 Technical Preview:
  ▪ …
  ▪ Neither userPrincipalName nor servicePrincipalName uniqueness is checked if the DoNotVerifyUPNAndOrSPNUniqueness character of the dsHeuristics attribute is set to "3".
Changed to:
▪ In AD DS, if the DC functional level is DS_BEHAVIOR_WIN2012R2 or greater, then the new attribute value must be unique within the entire forest. If the DC is not a GC, then the DC should issue an LDAP search against a GC to determine uniqueness. The following additional considerations for uniqueness checking are relevant for Windows Server 2012 R2 with [MSKB-3070083] and Windows Server 2016 Technical Preview:
  ▪ …
  ▪ Neither userPrincipalName nor servicePrincipalName uniqueness is checked if the DoNotVerifyUPNAndOrSPNUniqueness character of the dsHeuristics attribute is set to "3".
  ▪ userPrincipalName and servicePrincipalName uniqueness is checked if the DoNotVerifyUPNAndOrSPNUniqueness character of the dsHeuristics attribute is set to any value other than "1", "2", or "3".
In Section 6.1.1.2.4.1.2, dSHeuristics, changed from:
<table>
<tr><th>Character number</th><th>Character name</th><th>Description</th></tr>
<tr><td>21</td><td>DoNotVerifyUPNAndOrSPNUniqueness</td><td>In AD LDS, if this character is anything other than "0", AD LDS will not check values of userPrincipalName for uniqueness. See section 3.1.1.5.2.2.In AD LDS, this heuristic applies to Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.In AD DS, if this character is "1", "2" or "3", AD DS will not check values of userPrincipalName or servicePrincipalName for uniqueness. See section 3.1.1.5.1.3.In AD DS, this heuristic applies to Windows Server 2016 Technical Preview.</td></tr>
</table>

Changed to:
<table>
<tr><th>Character number</th><th>Character name</th><th>Description</th></tr>
</table>
</td></tr>
</table>

Errata Published*	Description		
	21	DoNotVerifyUPNAndOrSPNUniqueness	In AD LDS, if this character is anything other than "0", AD LDS will not check values of userPrincipalName for uniqueness. See section 3.1.1.5.2.2.In AD LDS, this heuristic applies to Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview.In AD DS, if this character is "1", "2" or "3", AD DS will not check values of userPrincipalName or servicePrincipalName for uniqueness. See section 3.1.1.5.1.3.In AD DS, this heuristic applies to Windows Server 2012 R2 with [MSKB-3070083] and Windows Server 2016 Technical Preview.

*Date format: YYYY/MM/DD

[MS-AIPS]: Authenticated Internet Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-APDS]: Authentication Protocol Domain Support

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V29.0 – 2015/06/30.

Errata Published*	Description
2015/09/28	In two sections, corrected the programming-element name LogonInformation.Identity.ParameterControl to be LogonInformation.LogonNetwork.Identity.ParameterControl. In Section 3.1.1, Abstract Data Model, changed from: The NTLM server uses the following configuration values:<3> <3> AllowComputerLogon: A Boolean setting which indicates that the caller wants to authenticate a computer. Setting this flag results in the K bit being set in LogonInformation.Identity.ParameterControl. Changed to: The NTLM server uses the following configuration values:<3> <3> AllowComputerLogon: A Boolean setting which indicates that the caller wants to authenticate a computer. Setting this flag results in the K bit being set in LogonInformation.LogonNetwork.Identity.ParameterControl. In Section 3.1.5.2, NTLM Network Logon, changed from: For NTLM network logons, the NTLM server SHOULD call NetrLogonSamLogonEx ([MS-NRPC] section 3.5.4.5.1)<20> with the following parameters (set as specified): ▪ … ▪ Set the E and K bits of LogonInformation.Identity.ParameterControl. … If the account is a computer account, the sub-authentication package is not verified, and the K bit of LogonInformation.Identity.ParameterControl is not set, then return STATUS_NOLOGON_WORKSTATION_TRUST_ACCOUNT.<23> If the account is a domain controller computer account, the sub-authentication package is not verified, and the E bit of LogonInformation.Identity.ParameterControl is not set, then return STATUS_NOLOGON_SERVER_TRUST_ACCOUNT.<24> … <22> In Windows 2000, if AllowComputerLogon is not set, then the K bit of LogonInformation.ParameterControl is not set. In Windows NT, NTLM servers never set the K bit. Changed to: For NTLM network logons, the NTLM server SHOULD call NetrLogonSamLogonEx ([MS-NRPC] section 3.5.4.5.1)<20> with the following parameters (set as specified):

Errata Published*	Description
	• … • Set the E and K bits of LogonInformation.LogonNetwork.Identity.ParameterControl.<22>. … If the account is a computer account, the sub-authentication package is not verified, and the K bit of LogonInformation.LogonNetwork.Identity.ParameterControl is not set, then return STATUS_NOLOGON_WORKSTATION_TRUST_ACCOUNT.<23> If the account is a domain controller computer account, the sub-authentication package is not verified, and the E bit of LogonInformation.LogonNetwork.Identity.ParameterControl is not set, then return STATUS_NOLOGON_SERVER_TRUST_ACCOUNT.<24> … <22> In Windows 2000, if AllowComputerLogon is not set, then the K bit of LogonInformation.LogonNetwork.Identity.ParameterControl is not set. In Windows NT, NTLM servers never set the K bit.

*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.

RSS
Atom

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 ERRATA June 30 2015 Archive here.

[MS-BKRP]: BackupKey Remote Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V16.0 – 2015/06/30.

Errata Published YYYY/MM/DD	Description
2015/10/12	In Section 3.3.1, Abstract Data Model, the description of the password ADM was corrected. Changed from: Password: A 0-256 Unicode string (generated using Normalization Form C [UNICODE5.0.0/2007]), used in the generation of NT Response ([RFC2759] section 4), Master Session Key (section 3.1.5.1), and AuthenticatorResponse ([RFC2759] section 5). Changed to: Password: A 0-256 Unicode string (generated using Normalization Form C [UNICODE5.0.0/2007]), used in the generation of NT Response ([RFC2759] section 4), Master Session Key (section 3.1.5.1), and AuthenticatorResponse ([RFC2759] section 5). The Password could belong to a user or a machine and it is obtained in an implementation-specific mechanism.

*Date format: YYYY/MM/D

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

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

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

RSS
Atom

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 ERRATA June 30 2015 Archive here.

[MS-CSRA]: Certificate Services Remote Administration Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V29.0 – 2015/06/30.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2015/08/17</td><td>In Section 2.2.2.1.2, DNS_RPC_NODE_FLAGS, added a product behavior note to the DNS_RPC_FLAG_AGING_ON flag.
Changed from:
<table><tr><th>Constant/value</th><th>Description</th></tr><tr><td>DNS_RPC_FLAG_AGING_ON
0x00020000</td><td>This flag is set when updating a record to enable or disable aging for a record. Applicable for dwFlags in DNS_RPC_RECORD (section 2.2.2.2.5).</td></tr></table>Changed to:
<table><tr><th>Constant/value</th><th>Description</th></tr><tr><td>DNS_RPC_FLAG_AGING_ON
0x00020000</td><td>This flag is set when updating a record to enable or disable aging for a record. Applicable for dwFlags in DNS_RPC_RECORD (section 2.2.2.2.5).<8></td></tr></table><8> Section 2.2.2.1.2: On Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016 Technical Preview, this behavior is not applicable for nodes that have a record with aging disabled. It is applicable for zone root nodes.</td></tr>
</table>

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V24.0 – 2015/06/30.

Errata Published YYYY/MM/DD	Description
2015/07/06	In Section 3.2.7.11, Create Subordinate Enlistment, and Section 3.2.7.21, Export Transaction, corrected the default limit of Subordinate Enlistments. In Section 3.2.7.11, Create Subordinate Enlistment, changed from: If this computed number of Enlistment objects is greater than or equal to an implementation-specific value that indicates the maximum allowed Transaction Manager Enlistments:<29> <29> Section 3.2.7.11: The limit of Subordinate Enlistments depends on the version of Windows. The default limit on Subordinate Resource Manager Enlistments is 32, except for Windows NT 4.0 Option Pack, where the limit is 16. Changed to: If this computed number of Enlistment objects is greater than or equal to an implementation-specific value that indicates the maximum allowed Transaction Manager Enlistments:<29> <29> Section 3.2.7.11: The limit of Subordinate Enlistments depends on the type of Enlistment. The default limit on Subordinate Transaction Manager Enlistments is 64 on Windows implementations, except for Windows NT 4.0 Option Pack, where the limit is 16. The limit on Subordinate Resource Manager Enlistments for Windows implementations is 32. In Section 3.2.7.21, Export Transaction, changed from: If that number is equal to an implementation-specific value that indicates the maximum allowed Transaction Manager enlistments:<31> <31> Section 3.2.7.21: The limit of Subordinate Enlistments depends on the version of Windows. The default limit on Subordinate Resource Manager Enlistments is 32, except for Windows NT 4.0 Option Pack, where the limit is 16. Changed to: If that number is equal to an implementation-specific value that indicates the maximum allowed Transaction Manager enlistments:<31> <31> Section 3.2.7.21: The limit of Subordinate Enlistments depends on the type of Enlistment. The default limit on Subordinate Transaction Manager Enlistments is 64 on Windows implementations, except for Windows NT 4.0 Option Pack, where the limit is 16. The limit on Subordinate Resource Manager Enlistments for Windows implementations is 32.

*Date format: YYYY/MM/DD

[MS-DTYP]: Windows Data Types

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

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

RSS
Atom

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 ERRATA June 30 2015 Archive here.

[MS-DVRE]: Device Registration Enrollment Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-ECS]: Enterprise Client Synchronization Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-EMF]: Enhanced Metafile Format

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-EMFPLUS]: Enhanced Metafile Format Plus Extensions

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

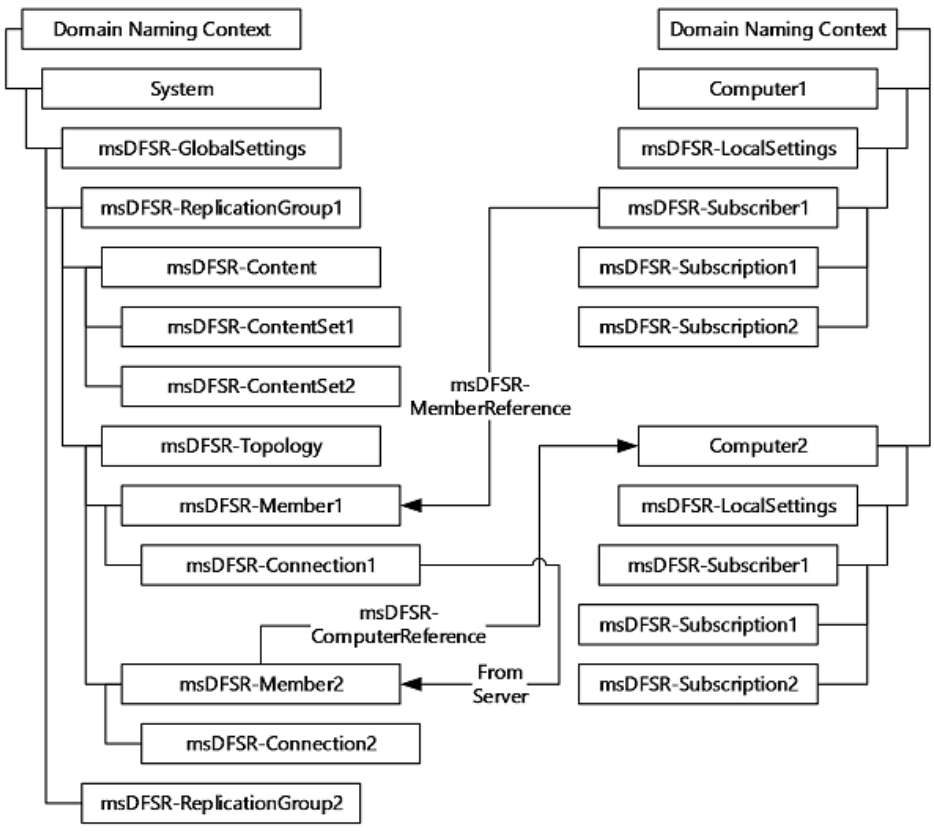
[MS-FRS2]: Distributed File System Replication Protocol

This topic lists the Errata found in the MS-FRS2 document since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

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

RSS
Atom

Errata below are for Protocol Document Version V24.0 – 2015/06/30.

Errata Published*	Description
2015/08/17	In Section 4.3.1., Example Objects in the DFS-R Object Hierarchy, the figure illustrating the object hierarchy required in Active Directory for storing configuration parameters for Windows implementations of DFS-R has been updated to correct inaccurate labels (e.g., the label "msDFSR-ReplicationGroup" should instead be "msDFSR-ReplicationGroup1"). The corrected figure is shown below: 

*Date format: YYYY/MM/DD

[MS-FSA]: File System Algorithms

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V19.0 – 2015/06/30.

Errata Published*	Description
2015/08/17	In Section 2.1.5.1.2.1, Algorithm to Check Access to an Existing File, the second bullet point in the fourth list was changed from:: For each ExistingOpen is Open.File.OpenList: Changed to: For each ExistingOpen in Open.File.OpenList:

*Date format: YYYY/MM/DD

[MS-FSCC]: File System Control Codes

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V38.0 – 2015/06/30.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2015/09/28</td><td>In Section 2.5.1, FileFsAttributeInformation, two new values have been added to the FileSystemAttributes field (additions below in bold):

FileSystemAttributes (4 bytes): A 32-bit unsigned integer that contains a bitmask of flags that specify attributes of the specified file system as a combination of the following flags. The value of this field MUST be a bitwise OR of zero or more of the following with the exception that FILE_FILE_COMPRESSION and FILE_VOLUME_IS_COMPRESSED cannot both be set. Any flag values not explicitly mentioned here can be set to any value, and MUST be ignored.

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>FILE_SUPPORTS_USN_JOURNAL
0x02000000</td><td>The file system implements a USN (2) change journal.</td></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>FILE_SUPPORTS_BLOCK_REFCOUNTING
0x08000000</td><td>The file system supports sharing logical clusters between files on the same volume. The file system reallocates on writes to shared clusters. Indicates that FSCTL_DUPLICATE_EXTENTS_TO_FILE is a supported operation.</td></tr>
<tr><td>FILE_SUPPORTS_SPARSE_VDL
0x10000000</td><td>The file system tracks whether each cluster of a file contains valid data (either from explicit file writes or automatic zeros) or invalid data (has not yet been written to or zeroed).
File systems that use Sparse VDL do not store a valid data length (section 2.4.41) and do not require that valid data be contiguous within a file.</td></tr>
</table>
</td></tr>
<tr><td>2015/08/03</td><td>In Section 2.3.7, FSCTL_DUPLICATE_EXTENTS_TO_FILE Request, corrected the name and size of the identifier of the open handle to the source file.
Changed from:
FileHandle (8 bytes): A 64-bit unsigned integer that indicates an open handle to the source file.
Changed to:</td></tr>
</table>

Errata Published*	Description
	SourceFileID (16 bytes): An SMB2_FILEID structure, as specified in [MS-SMB2] section 2.2.14.1, that is an identifier of the open to the source file. Note: The related bit table was also updated to reflect the above changes.

*Date format: YYYY/MM/DD

[MS-FSRVP]: File Server Remote VSS Protocol

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V8.0 – 2015/06/30.

Errata Published*	Description
2015/08/03	In Section 3.1.4, Message Processing Events and Sequencing Rules, clarified which security measures the server must enforce in order to verify that the caller has the required permissions to execute any method. Changed from: The server SHOULD<4> enforce security measures to verify that the caller has the required permissions to execute any method. If the server enforces security measures, and the caller does not have the required credentials, then the server MUST fail the call and return E_ACCESSDENIED. For more details on how to determine the identity of the caller for the purpose of performing an access check, see [MS-RPCE] section 3.3.3.1.3. <4> Section 3.1.4: Windows servers check whether the caller is a member of the administrators or backup operators group. Changed to: The server MUST enforce the below security measures to verify that the caller has the required permissions to execute any method.<4>. ▪ The security provider as RPC_C_AUTHN_GSS_NEGOTIATE or RPC_C_AUTHN_GSS_KERBEROS or RPC_C_AUTHN_WINNT, as specified in [MS-RPCE] section 2.2.1.1.7. ▪ The authentication level as RPC_C_AUTHN_LEVEL_PKT_INTEGRITY or RPC_C_AUTHN_LEVEL_PKT_PRIVACY, as specified in [MS-RPCE] section 2.2.1.1.8.If the caller does not have the required permissions, then the server MUST fail the call and return E_ACCESSDENIED. For more details on how to determine the identity of the caller for the purpose of performing an access check, see [MS-RPCE] section 3.3.3.1.3. <4> Section 3.1.4: Windows servers additionally check whether the caller is a member of the administrators or backup operators group.
2015/07/20	In Section 2.2.2.1, SHADOW_COPY_ATTRIBUTES, ATTR_FILE_SHARE was removed from the table of valid values. In Section 2.2.2.2, CONTEXT_VALUES, the first paragraph was changed from: The context of a shadow copy is a combination of zero or more attribute values, as defined in section 2.2.2.1. The following table lists the valid context values for the shadow copy operations. The client can additionally include the ATTR_AUTO_RECOVERY attribute in any of the following contexts. Changed to: The context of a shadow copy is a combination of zero or more attribute values, as defined in section 2.2.2.1. The following table lists the valid context values for the shadow copy operations. The client can additionally include either the ATTR_AUTO_RECOVERY or ATTR_NO_AUTO_RECOVERY attribute in any of the following contexts.

*Date format: YYYY/MM/DD

[MS-FSVCA]: File Set Version Comparison Algorithms

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-GPOL]: Group Policy: Core Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-KILE]: Kerberos Protocol Extensions

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V30.0 – 2015/06/30.

Errata Published*	Description
2015/09/28	In Section 3.1.1.5, SupportedEncryptionTypes, reverted incorrectly revised content of product behavior note to original text. Changed from: The default is 0000001C.<15> <15> Section 3.1.1.5: The default for SupportedEncryptionTypes in Windows Vista and Windows Server 2008 is 0000001F. For DCs on Windows Server 2008 R2 and subsequent versions of Windows Server operating system, according to the applicability list at the beginning of this section, the default is also 0000001F. Changed to: The default is 0000001C.<15> <15> Section 3.1.1.5: The default for SupportedEncryptionTypes in Windows Vista and Windows Server 2008 is 0000001F. The default for Windows Server 2008 R2 DCs is 0000001F.
2015/08/03	In Section 3.3.5.7, TGS Exchange, added the condition that triggers the KDC to return KRB_ERR_MUST_USE_USER2USER. The remaining user-to-user behavior is documented in RFC 4120 Section 3.7. Changed from: If the Application Server's service account AuthorizationDataNotRequired is set to TRUE, the KDC MUST NOT include a PAC in the service ticket. If the OTHER_ORGANIZATION SID ([MS-DTYP] section 2.4.2.4) is in KERB_VALIDATION_INFO.ExtraSids, the PAC MUST be used to perform an access check. … Changed to: If the Application Server's service account AuthorizationDataNotRequired is set to TRUE, the KDC MUST NOT include a PAC in the service ticket. If the Application Server's service account does not have a registered SPN, the KDC MUST return KDC_ERR_MUST_USE_USER2USER. If the OTHER_ORGANIZATION SID ([MS-DTYP] section 2.4.2.4) is in KERB_VALIDATION_INFO.ExtraSids, the PAC MUST be used to perform an access check.

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-MDE]: Mobile Device Enrollment Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V3.0 – 2015/06/30.

Errata Published*	Description
2015/07/06	In Appendix B: Product Behavior, Windows Server 2012 R2 should be removed from the applicability list, and any references to it in the product behavior notes should be ignored.

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V1.0 – 2015/06/30.

Errata Published*	Description
2015/09/14	In Section 1.3, Overview, referenced step 5 instead of step 4 in step 7 Changed from: 7. The enrollment client can send a RequestSecurityToken message (section 3.4.4.1.1.1) to the ES endpoint [MS-WSTEP] using the security token received in step 4. The ES endpoint [MS-WSTEP] responds with a RequestSecurityTokenResponseCollection message (section 3.4.4.1.1.2) containing the identity and provisioning information for the device management client [MS-MDM]. For more information about these messages, see [MS-WSTEP] sections 3.1.4.1.1.1 and 3.1.4.1.1.2. Changed to: 7. The enrollment client can send a RequestSecurityToken message (section 3.4.4.1.1.1) to the ES endpoint [MS-WSTEP] using the security token received in step 5. The ES endpoint [MS-WSTEP] responds with a RequestSecurityTokenResponseCollection message (section 3.4.4.1.1.2) containing the identity and provisioning information for the device management client [MS-MDM]. For more information about these messages, see [MS-WSTEP] sections 3.1.4.1.1.1 and 3.1.4.1.1.2.
2015/09/14	In Section 2.2.9.2, CertificateStore Configuration Service Provider, added [] brackets to UniqueID (changes in **bold**). Changed from: My/SCEP/UniqueID/CertThumbprint: Optional. Specifies the current certificate thumbprint if certificate enrollment succeeds. It is a 20-byte value of the SHA-1 certificate hash specified as a hexadecimal string value. Value type is chr. Supported operation is Get. My/SCEP/UniqueID/RespondentServerUrl: Required. Returns the URL of the SCEP server that responded to the enrollment request. Value type is string Supported operation is Get. Changed to: My/SCEP/**[UniqueID]/**CertThumbprint: Optional. Specifies the current certificate thumbprint if certificate enrollment succeeds. It is a 20-byte value of the SHA-1 certificate hash specified as a hexadecimal string value. Value type is chr. Supported operation is Get. My/SCEP/**[UniqueID]/**RespondentServerUrl: Required. Returns the URL of the SCEP server that responded to the enrollment request. Value type is string Supported operation is Get.
2015/09/04	The following missing sections were added to [MS-MDE2]:

Errata Published*	Description
	3.2 Interaction with Security Token Service (STS) 3.3 Interaction with X.509 Certificate Enrollment Policy 3.4 Interaction with WS-Trust X.509v3 Token Enrollment 3.5 Certificate Renewal View this Word document to see the information added: [MS-MDE2]_Missing_Content.
2015/07/06	In Appendix B: Product Behavior, product behavior note <1> should be ignored, and any warnings about the behavior in any given section of the document being dependent on unreleased Windows Server software should be ignored.

*Date format: YYYY/MM/DD

[MS-MDM]: Mobile Device Management Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-NRPC]: Netlogon Remote Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V25.0 – 2015/06/30.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2015/10/12</td><td>
In Sections 3.1.1, Abstract Data Model, and 3.1.5.5.2, Key Used in the Cryptobinding HMAC-SHA1-160 Operation, the length of the TunnelKey has been updated to 60 octets to match observed behavior:

TunnelKey: The PEAP Tunnel Key (TK) is a 60-octet key generated as specified in section 3.1.5.5.2.1. This variable is used while generating Cryptobinding TLVs (section 3.1.5.5) and, if using cryptobinding, the final MPPE keys (section 3.1.5.7).

Tunnel key (TK): A 60-octet key generated by phase 1 of PEAP. For details, see section 3.1.5.5.2.1. The generated Tunnel Key is stored in the variable TunnelKey.

In Section 3.1.5.7, Key Management, the derivation of the keys from the Key_Material element in [RFC5216] has been updated to the text below to eliminate references to the TunnelKey ADM element for the case where one endpoint does not accept cryptobinding TLVs.

2. When an endpoint (either a PEAP server or PEAP peer) is incapable of sending cryptobinding TLVs, and the other endpoint is configured to accept such authentications, then the keys are obtained from the first 64 octets of the Key_Material, as specified in [RFC5216]: TLS-PRF-128 (master secret, "clientEAP encryption", client.random || server.random).

<table>
<tr><th></th><th>First 32 bytes of Key_Material</th><th>Second 32 bytes of Key_Material</th></tr>
<tr><td>PEAP peer</td><td>MS-MPPE-Send-Key</td><td>MS-MPPE-Recv-Key</td></tr>
<tr><td>PEAP server</td><td>MS-MPPE-Recv-Key</td><td>MS-MPPE-Send-Key</td></tr>
</table>
</td></tr>
</table>

*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.

RSS
Atom

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 ERRATA June 30 2015 Archive here.

[MS-PSRP]: PowerShell Remoting Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-RA]: Remote Assistance Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-RAI]: Remote Assistance Initiation Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V39.0 – 2015/06/30.

Errata Published*	Description
2015/08/17	In Section 2.2.8.1.1.3.1.1.3, Mouse Event (TS_POINTER_EVENT), and Section 2.2.8.1.2.2.3, Fast-Path Mouse Event (TS_FP_POINTER_EVENT), added that the xPos and yPos fields SHOULD be ignored by the server if either the PTRFLAGS_WHEEL or PTRFLAGS_HWHEEL flag is specified in the pointerFlags field. In Section 2.2.8.1.1.3.1.1.3, Mouse Event (TS_POINTER_EVENT), changed from: xPos (2 bytes): A 16-bit, unsigned integer. The x-coordinate of the pointer relative to the top-left corner of the server's desktop. yPos (2 bytes): A 16-bit, unsigned integer. The y-coordinate of the pointer relative to the top-left corner of the server's desktop. Changed to: xPos (2 bytes): A 16-bit, unsigned integer. The x-coordinate of the pointer relative to the top-left corner of the server's desktop. This field SHOULD be ignored by the server if either the PTRFLAGS_WHEEL (0x0200) or the PTRFLAGS_HWHEEL (0x0400) flag is specified in the pointerFlags field. yPos (2 bytes): A 16-bit, unsigned integer. The y-coordinate of the pointer relative to the top-left corner of the server's desktop. This field SHOULD be ignored by the server if either the PTRFLAGS_WHEEL (0x0200) or the PTRFLAGS_HWHEEL (0x0400) flag is specified in the pointerFlags field. In Section 2.2.8.1.2.2.3,Fast-Path Mouse Event (TS_FP_POINTER_EVENT), changed from: xPos (2 bytes): A 16-bit, unsigned integer. The x-coordinate of the pointer. yPos (2 bytes): A 16-bit, unsigned integer. The y-coordinate of the pointer.

Errata Published*	Description
	Changed to: xPos (2 bytes): A 16-bit, unsigned integer. The x-coordinate of the pointer relative to the top-left corner of the server's desktop. This field SHOULD be ignored by the server if either the PTRFLAGS_WHEEL (0x0200) or the PTRFLAGS_HWHEEL (0x0400) flag is specified in the pointerFlags field. yPos (2 bytes): A 16-bit, unsigned integer. The y-coordinate of the pointer relative to the top-left corner of the server's desktop. This field SHOULD be ignored by the server if either the PTRFLAGS_WHEEL (0x0200) or the PTRFLAGS_HWHEEL (0x0400) flag is specified in the pointerFlags field.
2015/08/17	In Section 1.3.1.4.1, User-Initiated on Client, clarified options for a client-initiated disconnect. Changed from: The user can initiate a client-side disconnect by closing the RDP client application. To implement this type of disconnection the client sends the server a Shutdown Request PDU. The server response to this PDU is determined by whether the session is associated with a logged-on user account. Changed to: The user can initiate a client-side disconnect by closing the RDP client application. To implement this type of disconnection the client can initiate an immediate disconnect by sending the MCS Disconnect Provider Ultimatum PDU (with the reason code set to "user requested") and then closing the connection. Alternatively, the client can first notify the server of the intent to disconnect by sending the Shutdown Request PDU and then waiting for a response. The server response to this PDU is determined by whether the session is associated with a logged-on user account.
2015/07/20	In Section 4.1.2, Server X.224 Connection Confirm PDU, updated the example. Changed from: The following is an annotated dump of the X.224 Connection Confirm PDU (section 2.2.1.2). 00000000 03 00 00 13 0e d0 00 00 12 34 00 02 00 08 00 01 .....4..... 00000010 00 00 00 Changed to: The following is an annotated dump of the X.224 Connection Confirm PDU (section 2.2.1.2). 00000000 03 00 00 13 0e d0 00 00 12 34 00 02 00 08 00 00 .....4..... 00000010 00 00 00
2015/07/20	In Section 4, Protocol Examples, updated the examples network dump. In Section 4.1.3, Client MCS Connect Initial PDU with GCC Conference Create Request, changed from: The following is an annotated dump of the MCS Connect Initial PDU with GCC Conference Create

Errata Published*	Description
	Request (section 2.2.1.3). … 00000150 00 00 00 00 00 00 00 00 01 00 00 00 04 c0 0c 00 ..... … Changed to: The following is an annotated dump of the MCS Connect Initial PDU with GCC Conference Create Request (section 2.2.1.3). … 00000150 00 00 00 00 00 00 00 00 00 00 00 00 04 c0 0c 00 ..... … In Section 4.1.4, Server MCS Connect Response PDU with GCC Conference Create Response, changed from: The following is an annotated dump of the MCS Connect Response PDU with GCC Conference Create Response (section 2.2.1.4). … 02 01 02 -> DomainParameters::maxUserIds = 3 … Changed to: The following is an annotated dump of the MCS Connect Response PDU with GCC Conference Create Response (section 2.2.1.4). … 02 01 03 -> DomainParameters::maxUserIds = 3 …

Errata Published*	Description
	In Section 4.1.13, Client Confirm Active PDU, changed from: The following is an annotated dump of the Confirm Active PDU (section 2.2.1.13.2). … 01 00 00 00 -> TS_DRAW_GDIPLUS_CAPABILITYSET::drawGdiplusCacheLevel … Changed to: The following is an annotated dump of the Confirm Active PDU (section 2.2.1.13.2). … 00 00 00 00 -> TS_DRAW_GDIPLUS_CAPABILITYSET::drawGdiplusCacheLevel … In Section 4.4, Annotated Server-to-Client Virtual Channel PDU, changed from: The following is an annotated dump of the Virtual Channel PDU (section 2.2.6.1) that was exchanged between a Microsoft RDP 5.1 client and Microsoft RDP 5.1 server. … 00000000 03 00 00 2e 02 f0 80 68 00 01 03 ed f0 20 08 08 ....h..... .. … Changed to: The following is an annotated dump of the Virtual Channel PDU (section 2.2.6.1) that was exchanged between a Microsoft RDP 5.1 client and Microsoft RDP 5.1 server. … 00000000 03 00 00 2e 02 f0 80 68 00 01 03 ed f0 1c 08 08 ....h..... .. …

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V14.0 – 2015/06/30.

Errata Published*	Description
2015/10/12	In Section 3.2.3.2.1, DVC Create Response (DYNVC_CREATE_RSP), the failure behavior has been updated from: The client maintains this channel for the life of the connection. The client responds to the server with a DYNVC_CREATE_RSP (section 2.2.2.2) PDU indicating the channel creation status. Any positive or zero value indicates success. A negative value indicates failure. Changed to: The client responds to the server with a DYNVC_CREATE_RSP (section 2.2.2.2) PDU indicating the channel creation status. Any positive or zero value indicates success. A negative value indicates failure. On failure, the server DVC manager can reuse the failed ChannelId for another channel without first sending a DYNVC_CLOSE (section 2.2.4) PDU. Therefore, the client MUST NOT add the failed ChannelId into the list of active ChannelIds. If the channel creation was successful, the client SHOULD maintain this channel until it is closed or the connection is terminated. In Section 3.2.5.2, Closing a DVC (DYNVC_CLOSE), new content has been added to the end of the section: If the client receives a DYNVC_CLOSE (section 2.2.4) PDU for a channel which is not in the list of active ChannelIds, the client MUST ignore the PDU and SHOULD NOT respond with a DYNVC_CLOSE (section 2.2.4) PDU. In Section 3.3.3.2, DVC Initialization, further information about failure behavior and a related product behavior note has been added: On failure, the server DVC manager MAY send a DYNVC_CLOSE (section 2.2.4) PDU for the failed channel.<8> The server DVC manager SHOULD reuse a Channel ID if the channel creation failed, or if the channel has been closed. <8> Section 3.3.3.2: A DYNVC_CLOSE PDU is sent for channels which failed to be created in Windows Vista operating system, Windows Server 2008 operating system with Service Pack 2 (SP2), Windows 7 operating system, Windows Server 2008 R2 operating system, Windows 8 operating system, and Windows Server 2012 operating system.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V8.0 – 2015/06/30.

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata Published*	Description
2015/10/12	In Section 2.2.4.2.1.5, RFX_PROGRESSIVE_REGION, modified the description of the RFX_PROGRESSIVE_REGION structure. Changed from: The RFX_PROGRESSIVE_REGION structure contains the compressed data for a set of tiles from the frame. All RFX_PROGRESSIVE_REGION blocks SHOULD be present between the RFX_PROGRESSIVE_FRAME_BEGIN (section 2.2.4.2.1.2) and RFX_PROGRESSIVE_FRAME_END (section 2.2.4.2.1.3) blocks. If a block is not present between the RFX_PROGRESSIVE_FRAME_BEGIN and RFX_PROGRESSIVE_FRAME_END blocks, the decoder SHOULD ignore it. Note that RFX_PROGRESSIVE_REGION entries that are part of the same frame can share the tiles defined in the tiles field of each entry. In this scenario, tiles are not repeated in successive RFX_PROGRESSIVE_REGION entries. Across all of the RFX_PROGRESSIVE_REGION entries of a frame, the rectangles (defined in the rects field of each entry) MUST be distinct, and the region defined by these rectangles MUST be completely covered by all of the tiles defined in the RFX_PROGRESSIVE_REGION entries of the frames. Changed to: The RFX_PROGRESSIVE_REGION structure contains the compressed data for a set of tiles from the frame. All RFX_PROGRESSIVE_REGION blocks SHOULD be present between the RFX_PROGRESSIVE_FRAME_BEGIN (section 2.2.4.2.1.2) and RFX_PROGRESSIVE_FRAME_END (section 2.2.4.2.1.3) blocks. If a block is not present between the RFX_PROGRESSIVE_FRAME_BEGIN and RFX_PROGRESSIVE_FRAME_END blocks, the decoder MUST ignore it. Note that RFX_PROGRESSIVE_REGION entries that are part of the same frame can share the tiles defined in the tiles field of each entry. In this scenario, tiles are not repeated in successive RFX_PROGRESSIVE_REGION entries. Across all of the RFX_PROGRESSIVE_REGION entries of a frame, the rectangles (defined in the rects field of each entry) MUST be distinct, and the region defined by these rectangles MUST be completely covered by all of the tiles defined in the RFX_PROGRESSIVE_REGION entries of the frames. Note that in this context the frame is bracketed between the RDPGFX_START_FRAME_PDU and the RDPGFX_END_FRAME_PDU, and can span multiple RFX_PROGRESSIVE_FRAME_BEGIN and RFX_PROGRESSIVE_FRAME_END blocks.

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V19.0 – 2015/06/30.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2015/10/12</td><td>
In Section 2.2.1.1.1, Remote Programs Capability Set, added three bits:TS_RAIL_LEVEL_SHELL_INTEGRATION_SUPPORTED, TS_RAIL_LEVEL_SERVER_TO_CLIENT_IME_SYNC_SUPPORTED, and TS_RAIL_LEVEL_HIDE_MINIMIZED_APPS_SUPPORTED.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>H

TS_RAIL_LEVEL_SHELL_INTEGRATION_SUPPORTED</td><td>Set to 1 if the client/server is capable of supporting extended shell integration like tabbed windows and overlay icons for Remote Programs; set to 0 otherwise. This flag MUST be set to 0 if TS_RAIL_LEVEL_SUPPORTED is 0.</td></tr>
<tr><td>C

TS_RAIL_LEVEL_SERVER_TO_CLIENT_IME_SYNC_SUPPORTED</td><td>Set to 1 if the client/server is capable of supporting syncing IME changes originating at the server for Remote Programs; set to 0 otherwise. This flag MUST be set to 0 if TS_RAIL_LEVEL_SUPPORTED is 0.</td></tr>
<tr><td>M

TS_RAIL_LEVEL_HIDE_MINIMIZED_APPS_SUPPORTED</td><td>Set to 1 if the client/server supports hiding minimized windows of Remote Programs on the server; set to 0 otherwise. This flag MUST be set to 0 if TS_RAIL_LEVEL_SUPPORTED is 0.</td></tr>
</table>
In Section 2.2.2.1, Common Header (TS_RAIL_PDU_HEADER), the description of the TS_RAIL_ORDER_HANDSHAKE_EX value has been changed.

Changed from:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>TS_RAIL_ORDER_HANDSHAKE_EX</td><td>Indicates a bi-directional HandshakeEx PDU.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>0x0013</td><td></td></tr>
</table>
Changed to:
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>TS_RAIL_ORDER_HANDSHAKE_EX

0x0013</td><td>Indicates a HandshakeEx PDU from server to client.</td></tr>
</table>
In Section 2.2.2.2.3, HandshakeEx PDU (TS_RAIL_ORDER_HANDSHAKE_EX), the description of the HandshakeEx PDU has been changed from:
The HandshakeEx PDU is exchanged between the server and the client to establish that both endpoints are ready to begin RAIL mode. The server sends the HandshakeEx PDU and the client responds with the HandshakeEx PDU.
Changed to:
The HandshakeEx PDU is sent from the server to the client to signal that it is ready to begin Enhanced RemoteApp mode. The server sends the HandshakeEx PDU, and the client responds with the Handshake PDU.
</td></tr>
<tr><td>2015/08/17</td><td>
In Section 2.2.1.3.1.2.1, New or Existing Window, changed the FieldsPresentFlags field value WINDOW_ORDER_FIELD_WNDCLIENTDELTA to WINDOW_ORDER_FIELD_CLIENTDELTA.
Changed from:
Hdr (11 bytes): Eleven bytes. Common Window AltSec Order header, TS_WINDOW_ORDER_HEADER. The FieldsPresentFlags field of the header MUST conform to the values defined as follows.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00008000

WINDOW_ORDER_FIELD_WNDCLIENTDELTA</td><td>Indicates that the WindowClientDeltaX and WindowClientDeltaY fields are present.</td></tr>
</table>
Changed to:
Hdr (11 bytes): Eleven bytes. Common Window AltSec Order header, TS_WINDOW_ORDER_HEADER. The FieldsPresentFlags field of the header MUST conform to the values defined as follows.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x00008000

WINDOW_ORDER_FIELD_CLIENTDELTA</td><td>Indicates that the WindowClientDeltaX and WindowClientDeltaY fields are present.</td></tr>
</table>
</td></tr>
<tr><td>2015/08/17</td><td>In Section 4.7.1, TS_RAIL_ORDER_ZORDER_SYNC, changed the orderType field value from 0x0020 to 0x0014 in the network capture for TS_RAIL_PDU_HEADER.</td></tr>
</table>

Errata Published*	Description

	Changed from:
	
	The following is a network capture of the Server Z-Order Sync Information PDU (TS_RAIL_ORDER_ZORDER_SYNC, as specified in section 2.2.2.11.1).
	
	`20 00 -> TS_RAIL_PDU_HEADER::orderType = TS_RAIL_ORDER_ZORDER_SYNC (20) (2 Bytes)`
	
	`08 00 -> TS_RAIL_PDU_HEADER::orderLength = 8 (2 Bytes)`
	
	`10 05 40 00 -> WindowIdMarker (4 Bytes)`
	
	Changed to:
	
	The following is a network capture of the Server Z-Order Sync Information PDU (TS_RAIL_ORDER_ZORDER_SYNC, as specified in section 2.2.2.11.1).
	
	`14 00 -> TS_RAIL_PDU_HEADER::orderType = TS_RAIL_ORDER_ZORDER_SYNC (20) (2 Bytes)`
	
	`08 00 -> TS_RAIL_PDU_HEADER::orderLength = 8 (2 Bytes)`
	
	`10 05 40 00 -> WindowIdMarker (4 Bytes)`

2015/08/17	In Section 2.2.2.10.1, Language Profile Information PDU (TS_RAIL_ORDER_LANGUAGEIMEINFO), changed from: ProfileType (4 bytes): An unsigned 4-byte integer that identifies the profile type of the language. The value should be either TF_PROFILETYPE_INPUTPROCESSOR (0x0001) or TF_PROFILETYPE_KEYBOARDLAYOUT (0x0002). Changed to:

Errata Published*	Description
	ProfileType (4 bytes): An unsigned 4-byte integer that identifies the profile type of the language. The value SHOULD be either TF_PROFILETYPE_INPUTPROCESSOR (0x0001) or TF_PROFILETYPE_KEYBOARDLAYOUT (0x0002). In Section 2.2.2.2.3, HandshakeEx PDU (TS_RAIL_ORDER_HANDSHAKE), updated the section name from HandshakeEx PDU (TS_RAIL_ORDER_HANDSHAKE) to HandshakeEx PDU (TS_RAIL_ORDER_HANDSHAKE_**EX**)

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V33.0 – 2015/06/30.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2015/08/31</td><td>
In the following sections, the element, message, or operation name has been changed from FindServiceLocations to FindServiceLocationsForUser:

3.7.4.2 FindServiceLocationsForUser Operation
3.7.4.2.1 Messages
3.7.4.2.1.1 FindServiceLocationsForUserSoapIn
3.7.4.2.1.2 FindServiceLocationsForUserSoapOut
3.7.4.2.2.1 FindServiceLocationsForUser
6.5 Server Service WSDL

In Section 3.7.4.2, FindServiceLocationsForUser Operation, changed from:
...
<wsdl:operation name="FindServiceLocations">
<wsdl:input message="tns:FindServiceLocationsSoapIn" />
<wsdl:output message="tns:FindServiceLocationsSoapOut" />
</wsdl:operation>
...

Changed to:
...
<wsdl:operation name="FindServiceLocationsForUser">
<wsdl:input message="tns:FindServiceLocationsForUserSoapIn" />
<wsdl:output message="tns:FindServiceLocationsForUserSoapOut" />
</wsdl:operation>
…

In Section 3.7.4.2.1, Messages, changed from:
<table>
<tr><th>Message</th><th>Description</th></tr>
<tr><td>FindServiceLocationsSoapIn</td><td>Contains a ServiceType enumeration. Specifies the type of service being</td></tr>
</table>
</td></tr>
</table>

	requested.
FindServiceLocationsSoapOut	Contains the URL and ServiceType of the service that was requested.

Changed to:

Message	Description
FindServiceLocationsForUserSoapIn	Contains a ServiceType enumeration. Specifies the type of service being requested.
FindServiceLocationsForUserSoapOut	Contains the URL and ServiceType of the service that was requested.

In Section 3.7.4.2.1.1, FindServiceLocationsForUserSoapIn, changed from:

The FindServiceLocationsSoapIn message contains a ServiceType enumeration to specify the type of service being requested.

```
       <wsdl:message name="FindServiceLocationsSoapIn">
           <wsdl:part name="parameters" element="tns:FindServiceLocations"
/>
       </wsdl:message>
```

FindServiceLocations: The FindServiceLocations element, as specified in section 3.7.4.2.2.1.

Changed to:

The FindServiceLocationsForUserSoapIn message contains a ServiceType enumeration to specify the type of service being requested.

```
       <wsdl:message name="FindServiceLocationsForUserSoapIn">
           <wsdl:part name="parameters"
element="tns:FindServiceLocationsForUser" />
       </wsdl:message>
```

FindServiceLocationsForUser: The FindServiceLocationsForUser element, as specified in section 3.7.4.2.2.1.

In Section 3.7.4.2.1.2, FindServiceLocationsForUserSoapOut, changed from:

The FindServiceLocationsSoapOut message contains the URL and ServiceType of the service that was requested.

```
       <wsdl:message name="FindServiceLocationsSoapOut">
           <wsdl:part name="parameters"
element="tns:FindServiceLocationsResponse" />
       </wsdl:message>
```

FindServiceLocationsResponse: The FindServiceLocationsResponse element, as defined in section 3.7.4.2.2.2.

Changed to:

The FindServiceLocationsForUserSoapOut message contains the URL and ServiceType of the service that was requested.

```
       <wsdl:message name="FindServiceLocationsForUserSoapOut">
           <wsdl:part name="parameters"
element="tns:FindServiceLocationsForUserResponse" />
       </wsdl:message>
```

FindServiceLocationsForUserResponse: The FindServiceLocationsForUserResponse element, as defined in section 3.7.4.2.2.2.

In Section 3.7.4.2.2.1, FindServiceLocationsForUser, changed from:

...
This element MUST be populated by the client when sending a FindServiceLocations request.
...

Changed to:
...
This element MUST be populated by the client when sending a FindServiceLocationsForUser request.
...

In Section 6.5, Server Service WSDL, changed from:

...

```
<s:element name="FindServiceLocations">
              <s:complexType>
               <s:sequence>
                <s:element minOccurs="0" maxOccurs="1"
                  name="ServiceNames"
                  type="tns:ArrayOfServiceLocationRequest" />
               </s:sequence>
              </s:complexType>
             </s:element>
...
           <s:element name="FindServiceLocationsResponse">
                <s:complexType>
                  <s:sequence>
                    <s:element minOccurs="0" maxOccurs="1"
                       name="FindServiceLocationsResult"
                       type="tns:ArrayOfServiceLocationResponse" />
                  </s:sequence>
                </s:complexType>
```

```
            </s:element>
...
        <wsdl:message name="FindServiceLocationsSoapIn">
           <wsdl:part name="parameters"
             element="tns:FindServiceLocations" />
         </wsdl:message>
         <wsdl:message name="FindServiceLocationsSoapOut">
           <wsdl:part name="parameters"
             element="tns:FindServiceLocationsResponse" />
         </wsdl:message>
         <wsdl:message name="FindServiceLocationsVersionData">
           <wsdl:part name="VersionData" element="tns:VersionData" />
         </wsdl:message>
         <wsdl:message name="GetServerInfoSoapIn">
           <wsdl:part name="parameters" element="tns:GetServerInfo" />
         </wsdl:message>
         <wsdl:message name="GetServerInfoSoapOut">
           <wsdl:part name="parameters"
             element="tns:GetServerInfoResponse" />
         </wsdl:message>
         <wsdl:portType name="ServerSoap">
           <wsdl:operation name="GetLicensorCertificate">
             <wsdl:input message="tns:GetLicensorCertificateSoapIn" />
             <wsdl:output message="tns:GetLicensorCertificateSoapOut" />
           </wsdl:operation>
           <wsdl:operation name="FindServiceLocations">
             <wsdl:input message="tns:FindServiceLocationsSoapIn" />
             <wsdl:output message="tns:FindServiceLocationsSoapOut" />
           </wsdl:operation>
...
<wsdl:operation name="FindServiceLocations">
             <soap:operation soapAction=
      "http://microsoft.com/DRM/ServerService/FindServiceLocations"
                style="document" />
             <wsdl:input>
               <soap:body use="literal" />
               <soap:header message="tns:FindServiceLocationsVersionData"
                   part="VersionData" use="literal" />
             </wsdl:input>
             <wsdl:output>
               <soap:body use="literal" />
               <soap:header message="tns:FindServiceLocationsVersionData"
                   part="VersionData" use="literal" />
             </wsdl:output>
           </wsdl:operation>
...
           <wsdl:operation name="FindServiceLocations">
             <soap12:operation soapAction=
```

```
       "http://microsoft.com/DRM/ServerService/FindServiceLocations"
                style="document" />
             <wsdl:input>
               <soap12:body use="literal" />
               <soap12:header
                message="tns:FindServiceLocationsVersionData"
                part="VersionData" use="literal" />
             </wsdl:input>
             <wsdl:output>
               <soap12:body use="literal" />
               <soap12:header message="tns:FindServiceLocationsVersionData"
                   part="VersionData" use="literal" />
             </wsdl:output>
           </wsdl:operation>
```

Changed to:

```
...
<s:element name="FindServiceLocationsForUser">
              <s:complexType>
                <s:sequence>
                  <s:element minOccurs="0" maxOccurs="1"
                     name="ServiceNames"
                     type="tns:ArrayOfServiceLocationRequest" />
                </s:sequence>
              </s:complexType>
            </s:element>
...
            <s:element name="FindServiceLocationsForUserResponse">
              <s:complexType>
                <s:sequence>
                  <s:element minOccurs="0" maxOccurs="1"
                     name="FindServiceLocationsForUserResult"
                     type="tns:ArrayOfServiceLocationResponse" />
                </s:sequence>
              </s:complexType>
            </s:element>
...
         <wsdl:message name="FindServiceLocationsForUserSoapIn">
           <wsdl:part name="parameters"
             element="tns:FindServiceLocationsForUser" />
         </wsdl:message>
         <wsdl:message name="FindServiceLocationsForUserSoapOut">
           <wsdl:part name="parameters"
             element="tns:FindServiceLocationsForUserResponse" />
         </wsdl:message>
         <wsdl:message name="FindServiceLocationsForUserVersionData">
           <wsdl:part name="VersionData" element="tns:VersionData" />
```

```
          </wsdl:message>
          <wsdl:message name="GetServerInfoSoapIn">
            <wsdl:part name="parameters" element="tns:GetServerInfo" />
          </wsdl:message>
          <wsdl:message name="GetServerInfoSoapOut">
            <wsdl:part name="parameters"
              element="tns:GetServerInfoResponse" />
          </wsdl:message>
          <wsdl:portType name="ServerSoap">
            <wsdl:operation name="GetLicensorCertificate">
              <wsdl:input message="tns:GetLicensorCertificateSoapIn" />
              <wsdl:output message="tns:GetLicensorCertificateSoapOut" />
            </wsdl:operation>
            <wsdl:operation name="FindServiceLocationsForUser">
              <wsdl:input message="tns:FindServiceLocationsForUserSoapIn" />
              <wsdl:output message="tns:FindServiceLocationsForUserSoapOut"
/>
            </wsdl:operation>
...
<wsdl:operation name="FindServiceLocationsForUser">
              <soap:operation soapAction=
       "http://microsoft.com/DRM/ServerService/FindServiceLocationsForUser"
                 style="document" />
              <wsdl:input>
                <soap:body use="literal" />
                <soap:header
message="tns:FindServiceLocationsForUserVersionData"
                    part="VersionData" use="literal" />
              </wsdl:input>
              <wsdl:output>
                <soap:body use="literal" />
                <soap:header
message="tns:FindServiceLocationsForUserVersionData"
                    part="VersionData" use="literal" />
              </wsdl:output>
            </wsdl:operation>
...
       "http://microsoft.com/DRM/ServerService/FindServiceLocationsForUser"
                 style="document" />
              <wsdl:input>
                <soap12:body use="literal" />
                <soap12:header
                 message="tns:FindServiceLocationsForUserVersionData"
                 part="VersionData" use="literal" />
              </wsdl:input>
              <wsdl:output>
                <soap12:body use="literal" />
                <soap12:header
message="tns:FindServiceLocationsForUserVersionData"
```

	part="VersionData" use="literal" /> </wsdl:output> </wsdl:operation>

[MS-RMSOD]: Rights Management Services Protocols Overview

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

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

RSS
Atom

Errata below are for Protocol Document Version V7.0 – 2015/06/30.

Errata Published*	Description
2015/07/20	In various places in Section 2.5.4, Use Case Descriptions, corrected information related to the service connection points and GICURL value. Changed text is in bold. In Section 2.5.4.2, Bootstrap RMS Client - RMS Client Application, changed from: 6. To publish offline, the user has to have a separate signing certificate that is bound to the user's identity in RMS. The client first finds the service location, by deriving it from a publishing license (PL) or by discovering it from the directory service.<5> The client then sends a request to the publishing RMS server to retrieve the CLC. <5> Section 2.5.4.2: Windows RMS clients search Active Directory for the security processor certificate (SCP) unless one of the following registry keys is present: … Windows RMS servers search Active Directory for the SCP unless the GICURL value of one of the following registry keys contains the location of the certification service, http(s)://<server name>/_wmcs/certification. Changed to: 6. To publish offline, the user has to have a separate signing certificate that is bound to the user's identity in RMS. The client first finds the service location, by deriving it from a publishing license (PL) or by discovering it from the directory service.<5> The client then sends a request to the publishing RMS server to retrieve the CLC. <5> Section 2.5.4.2: Windows RMS clients search Active Directory for the service connection point (SCP) unless one of the following registry keys is present: … Windows RMS servers search Active Directory for the SCP unless the GICURL value of one of the following registry keys contains the location of the certification service, http(s)://<server name>/_wmcs/certification/certification.asmx. In Section 2.5.4.4, Find Service Locations for Client - RMS Server, changed from: Main success scenario … 5. At least one of the responses includes a valid set of security processor certificates (SCPs) for the services requested. This can be an SCP pointing to the other RMS server that responded or an SCP that is known to that server. Changed to: Main success scenario … 5. At least one of the responses includes a valid set of service connection points (SCPs) for the services requested. This can be an SCP pointing to the other RMS server that responded or an SCP that is known to that server.

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-RPRN]: Print System Remote Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V1.0 – 2015/06/30.

Errata Published*	Description
2015/08/31	In the following sections, changed all minOccurs values from "0" to "1": 3.1.4.2.3.2 RequestSslCertificateResponseBody 3.2.4.1.3.1 ConnectRequestBody 3.2.4.2.3.1 DisconnectRequestBody 3.2.4.3.3.1 GetChatIdRequestBody 3.2.4.5.3.1 SendErrorRequestBody 3.2.4.6.3.1 SendMsgRequestBody 3.4.4.1.3.1 SetSslCertificateRequestBody 3.4.4.2.3.2 RequestWmsControlCredentialsResponseBody 3.5.4.3.3.2 GetScheduledUpdateSettingsResponseBody 3.5.4.7.3.1 SetScheduledUpdateSettingsRequestBody 3.6.4.1.3.2 GetAllSessionsResponseBody 3.6.4.6.2.2 GetSystemAlertStatusResponse 3.6.4.7.2.2 GetSystemModeResponse 3.6.4.8.3.1 GetVirtualMachineIpAddressRequestBody 3.6.4.10.3.1 RegisterChatEventSinkRequestBody 3.6.4.11.3.1 RegisterCoreEventSinkRequestBody 3.6.4.21.3.2 GetNetJoinStatusResponseBody 3.6.4.22.3.2 GetVirtualMachineHostnameResponseBody

Errata Published*	Description	
	3.6.4.23.3.2	GetWmsWebLimitingResponseBody
	3.6.4.33.3.2	LoadWindowsEditionResponseBody
	3.6.4.37.3.1	ValidateAutoLogonAccountRequestBody
	3.6.4.37.3.2	ValidateAutoLogonAccountResponseBody
	3.7.4.1.3.1	CurrentActivityRequestBody
	3.7.4.4.3.1	ConfigureWebLimitingAllRequestBody
	3.7.4.5.3.1	EnableProjectToAllRequestBody
	3.7.4.9.3.1	GetSessionRunningAppsRequestBody
	3.7.4.10.3.1	GetThumbnailBitsRequestBody
	3.7.4.11.3.1	IdentifySessionRequestBody
	3.7.4.13.3.1	LockSessionRequestBody
	3.7.4.15.3.1	RunFileSessionRequestBody
	3.7.4.16.3.1	ShareDesktopRequestBody
	3.7.4.20.3.1	ViewDesktopRequestBody
	3.8.4.1.2.2	GetNextStationIdentifierResponse
	3.8.4.2.2.2	GetStationAlertStatusResponse
	3.8.4.3.3.1	GetStationAutoLogonInformationRequestBody
	3.8.4.4.2.2	GetStationDeviceInformationResponse
	3.8.4.5.3.1	GetStationFriendlyNameRequestBody
	3.8.4.6.3.1	GetStationInformationRequestBody
	3.8.4.7.3.1	GetStationServerNameRequestBody
	3.8.4.8.2.2	GetStationSplitScreenInformationResponse
	3.8.4.9.3.1	IdentifyStationRequestBody
	3.8.4.13.3.1	SetStationFriendlyNameRequestBody
	3.8.4.14.3.1	SetStationServerNameRequestBody

Errata Published*	Description

	3.9.4.1.3.1 OnManagedServerOfflineNotifyRequestBody
	
	3.9.4.2.3.1 OnManagedServerOnlineNotifyRequestBody
	
	3.10.4.1.3.1 AddUserRequestBody
	
	3.10.4.3.3.1 RemoveUserRequestBody
	
	3.10.4.4.3.1 SetUserInfoRequestBody
	
	For example, in Section 3.1.4.2.3.2, RequestSslCertificateResponseBody, changed from:
	
	`<xsd:complexType name="RequestSslCertificateResponseBody">`
	
	`<xsd:sequence>`
	
	`<xsd:element minOccurs="0" maxOccurs="1" name="pSslPort" type="xsd:unsignedInt"/>`
	
	`<xsd:element minOccurs="0" maxOccurs="1" name="pwsSslCertificateThumbprint" nillable="true" type="xsd:string"/>`
	
	`<xsd:element minOccurs="0" maxOccurs="1" name="ppSslCertificate" type="xsd:base64Binary"/>`
	
	`</xsd:sequence>`
	
	`</xsd:complexType>`
	
	Changed to (changes in **bold**):
	
	`<xsd:complexType name="RequestSslCertificateResponseBody">`
	
	`<xsd:sequence>`
	
	`<xsd:element minOccurs="`**`1`**`" maxOccurs="1" name="pSslPort" type="xsd:unsignedInt"/>`
	
	`<xsd:element minOccurs="`**`1`**`" maxOccurs="1" name="pwsSslCertificateThumbprint" nillable="true" type="xsd:string"/>`
	
	`<xsd:element minOccurs="`**`1`**`" maxOccurs="1" name="ppSslCertificate" type="xsd:base64Binary"/>`
	
	`</xsd:sequence>`
	
	`</xsd:complexType>`

2015/08/17	In Section 3.3.4.12.2.1, OnExitSplitScreen, added a description for the idStation element.

Errata Published*	Description
	Changed from: <xsd:element name="OnExitSplitScreen" nillable="true"> <xsd:complexType> <xsd:sequence> <xsd:element minOccurs="1" maxOccurs="1" name="idStation" type="xsd:unsignedInt"/> </xsd:sequence> </xsd:complexType> </xsd:element> Changed to: <xsd:element name="OnExitSplitScreen" nillable="true"> <xsd:complexType> <xsd:sequence> <xsd:element minOccurs="1" maxOccurs="1" name="idStation" type="xsd:unsignedInt"/> </xsd:sequence> </xsd:complexType> </xsd:element> idStation: Contains the ID of the MultiPoint Station. This is an unsigned integer with a range of 1 - n, where n is the number of stations currently available on the server.
2015/08/17	In Section 1.5, Prerequisites/Preconditions, updated that the client makes a web service request to the server using the HTTP protocol over TCP port 80 to the endpoint IMultiPointCertificateRequest. Changed from: 2. The client makes a web service request to the server using the HTTP protocol over TCP port 80 to the endpoint IMultiPointCredentialRequest (section 3.4) to obtain the server's X.509 certificate and the TCP port number. Changed to: 2. The client makes a web service request to the server using the HTTP protocol over TCP port 80 to the endpoint IMultiPointCertificateRequest (section 3.1) in order to obtain the server's X.509 certificate and the TCP port number.

*Date format: YYYY/MM/DD

[MS-RSVD]: Remote Shared Virtual Disk Protocol

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V5.0 – 2015/06/30.

Errata Published*	Description
2015/09/28	In Section 3.2.5.5.7.1, Receiving a Create Snapshot Request, updated the request processing steps when the server receives a Create Snapshot request. Changed from: The server MUST construct an SVHDX_META_OPERATION_REPLY structure as specified in section 2.2.4.18, with the following values: The SVHDX_TUNNEL_OPERATION_HEADER MUST be initialized as follows: ▪ The OperationCode field MUST be set to the OperationCode value of the request. ▪ The Status field MUST be set to STATUS_SUCCESS. ▪ The RequestId field MUST be set to the value received in the request. The SVHDX_META_OPERATION_REPLY structure MUST be initialized as follows: ▪ The ChangeTrackingErrorStatus field MUST be set to the value received from the virtual SCSI disk. The server MUST send the constructed SVHDX_META_OPERATION_REPLY structure to the client. Changed to: The server MUST construct an SVHDX_TUNNEL_OPERATION_HEADER structure as specified in section 2.2.4.11, with the following values: ▪ The OperationCode field MUST be set to the OperationCode value of the request. ▪ The RequestId field MUST be set to the value received in the request. ▪ The Status field MUST be set to the status returned by the virtual SCSI disk. If the SnapshotType is SvhdxSnapshotTypeCDP, the server MUST append an SVHDX_META_OPERATION_REPLY structure to the SVHDX_TUNNEL_OPERATION_HEADER in response, as specified in section 2.2.4.18, with the following values: ▪ The ChangeTrackingErrorStatus field MUST be set to one of the change-tracking status values specified in section 2.2.4.18; this value is received from the virtual SCSI disk, indicating any error in the change tracking. The server MUST send the response to the client.
2015/09/14	In Section 3.2.5.1, Receiving an Open Request, corrected the information on how the 'STATUS_VHD_SHARED' error code is used. Changed from: If the OriginatorFlags field in the request is set to SVHDX_ORIGINATOR_VHDMP, the server MUST pass the request to the underlying object store to open the file with read and write access

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>permissions. If the underlying object store fails with STATUS_SHARING_VIOLATION, the server MUST fail the request with STATUS_VHD_SHARED.

Changed to:

If the OriginatorFlags field in the request is set to SVHDX_ORIGINATOR_VHDMP, the server MUST search the OpenTable where Open.FileName matches the file name. If an Open is found, the server MUST fail the request with STATUS_VHD_SHARED. Otherwise, the server MUST pass the request to the underlying object store to open the file with read and write access permissions.</td></tr>
<tr><td>2015/08/03</td><td>In 2 sections, clarified the values for the SharedVirtualDiskSupport field and the settings when the server must set SharedVirtualDiskSupport to SharedVirtualDiskCDPSnapshotsSupported.

In Section 2.2.4.16, SVHDX_SHARED_VIRTUAL_DISK_SUPPORT_RESPONSE Structure, changed from:

SharedVirtualDiskSupport (4 bytes): This field is used to indicate the capabilities supported by the server. This field MUST contain one of the following values.

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

0x00000001</td><td>The server supports shared virtual disks.</td></tr><tr><td>SharedVirtualDiskVer2OperationsSupported

0x00000003</td><td>The server supports shared virtual disks and version 2 operations.</td></tr></table>
Changed to:

SharedVirtualDiskSupport (4 bytes): This field is used to indicate the capabilities supported by the server. This field MUST contain one of the following values.

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

0x00000001</td><td>The server supports shared virtual disks.</td></tr><tr><td>SharedVirtualDiskCDPSnapshotsSupported

0x00000007</td><td>The server supports shared virtual disks and continuous data protection (log-based) snapshots</td></tr></table>
In Section, 3.2.5.6, Receiving a Query Shared Virtual Disk Support Request, changed from:

If ServerServiceVersion is equal to RSVD Protocol version 1(0x00000001), the server MUST set SharedVirtualDiskSupport to SharedVirtualDiskSupported. Otherwise the server MUST set SharedVirtualDiskSupport to SharedVirtualDiskVer2OperationsSupported.

Changed to:

If ServerServiceVersion is equal to RSVD Protocol version 1(0x00000001), the server MUST set SharedVirtualDiskSupport to SharedVirtualDisksSupported. If ServerServiceVersion is equal to RSVD Protocol version 2(0x00000002), the server MUST set SharedVirtualDiskSupport to SharedVirtualDiskCDPSnapshotsSupported. Otherwise, the server MUST fail the request with STATUS_INVALID_PARAMETER.</td></tr>
</table>

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V28.0 – 2015/06/30.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2015/10/12</td><td>The character case of the lockOutObservationWindow attribute has been corrected from "lockoutObservationWindow" to "lockOutObservationWindow" in the following sections and locations:

Section 3.1.1.3 (Attribute Listing), in the attribute list.
Section 3.1.1.5 (Password Settings Attributes for Originating Update Constraints), in item 2.1.
Section 3.1.1.6 (Attribute Constraints for Originating Updates), in items 1 and 2.
Section 3.1.5.13.7 (SamrValidatePassword (Opnum 67)), in the third row of the table in item 2.
Section 3.1.5.14.8 (Domain Field to Attribute Name Mapping), in the sixth row of the table.</td></tr>
<tr><td>2015/09/04</td><td>In various sections, changes were made to support [MSKB-3072595], available on 2015/09/08:

In Section 3.1.1.6, Attribute Constraints for Originating Updates, changed from:
…
A client implementation MUST treat all failure codes as complete failures of the requested operation unless explicitly noted in this section. The possible status codes used for these explicit return codes are found in section 2.2.1.15.
…
19. userAccountControl MUST contain one and only one of the following bits, as defined in section 2.2.1.13; on error, return a failure code.
<table><tr><th>Bits</th></tr><tr><td>UF_NORMAL_ACCOUNT</td></tr><tr><td>UF_INTERDOMAIN_TRUST_ACCOUNT</td></tr><tr><td>UF_WORKSTATION_TRUST_ACCOUNT</td></tr><tr><td>UF_SERVER_TRUST_ACCOUNT</td></tr></table>
Changed to:
…
A client implementation MUST treat all failure codes as complete failures of the requested operation unless explicitly noted in this section. The possible status codes used for these explicit</td></tr>
</table>

Errata Published*	Description
	return codes are found in section 2.2.1.15. … 19. userAccountControl MUST contain one and only one of the following bits, as defined in section 2.2.1.13; on error, return a failure code. **Bits** UF_NORMAL_ACCOUNT UF_INTERDOMAIN_TRUST_ACCOUNT UF_WORKSTATION_TRUST_ACCOUNT UF_SERVER_TRUST_ACCOUNT 20. An existing userAccountControl attribute SHOULD NOT be modified such that the UF_WORKSTATION_TRUST_ACCOUNT bit is removed and the UF_NORMAL_ACCOUNT bit is added, or vice-versa; on error, return a failure code. This modification, however, MUST be allowed if the client is a member of the Domain Administrators group.<24a> <24a> Section 3.1.1.6: This modification is always allowed in Windows 2000 and in the following products that do NOT have [MSKB-3072595] installed: Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. In Section 3.1.5.4.4, SamrCreateUser2InDomain (Opnum 50), changed from: 13. If the client does not have the ACTRL_DS_CREATE_CHILD access right on the Container-Object objectand the AccountType parameter is USER_WORKSTATION_TRUST_ACCOUNT, then: 1. On a DC configuration: 1. If the RpcImpersonationAccessToken.Privileges[] field does not have the SE_MACHINE_ACCOUNT_NAME privilege (defined in [MS-LSAD] section 3.1.1.2.1), return a processing error. 2. Else: - 1. Let CallerSid be RpcImpersonationAccessToken.Sids[RpcImpersonationAccessToken.UserIndex]. - - 1. The number of computer objects in the domain with msDS-creatorSID equal to CallerSid MUST be less than the value of ms-DS-MachineAccountQuota on the account domain object. On error, abort and return a failure code.frommsDS-creatorSID MUST be set to CallerSid.The owner and group of the default security descriptor MUST be the Domain Admins SID for the domain in which the account is created. 2. On a nonDC configuration: ▪ The server MUST abort processing and return STATUS_ACCESS_DENIED. Changed to: 13. If the client does not have the ACTRL_DS_CREATE_CHILD access right on the Container-Object object, the client is not otherwise denied access due to an explicit DENY ACE <45a>, and the AccountType parameter is USER_WORKSTATION_TRUST_ACCOUNT, then: 1. On a DC configuration: 1. If the RpcImpersonationAccessToken.Privileges[] field does not have the SE_MACHINE_ACCOUNT_NAME privilege (defined in [MS-LSAD] section 3.1.1.2.1), return a processing error. 2. Else: - 1. Let CallerSid be RpcImpersonationAccessToken.Sids[RpcImpersonationAccessToken.UserIndex]. - 2. Let CallerPrimaryGroup be RpcImpersonationAccessToken.PrimaryGroup. - 3. If CallerPrimaryGroup is not equal to DOMAIN_GROUP_RID_COMPUTERS, then:

Errata Published*	Description
	- - 1. The number of computer objects in the domain with msDS-creatorSID equal to CallerSid MUST be less than the value of ms-DS-MachineAccountQuota on the account domain object. On error, abort and return a failure code. - 4. If CallerPrimaryGroup is equal to DOMAIN_GROUP_RID_COMPUTERS, then:<45b> - - 1. If the domain SID portion of CallerSid is different from the current domain SID, return a failure code. - - 2. The server MUST compute the sum of all computer objects in the domain created by CallerSid and transitively created by other computer objects created by CallerSid. This sum MUST be less than the value of ms-DS-MachineAccountQuota on the account domain object. On error, abort and return a failure code. - 5. If the previous constraints are met, then: - - 1. msDS-creatorSID MUST be set to CallerSid. - - 2. The owner and group of the default security descriptor MUST be the Domain Admins SID for the domain in which the account is created. 2. On a nonDC configuration: The server MUST abort processing and return STATUS_ACCESS_DENIED. <45a> Section 3.1.5.4.4: The test for an explicit DENY ACE is NOT performed in Windows 2000. This test is also NOT performed in the following products that do not have [MSKB-3072595] installed: Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. <45b> Section 3.1.5.4.4: This behavior is NOT performed in Windows 2000, and is also NOT performed in the following products that do not have [MSKB-3072595] installed: Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. In these cases, the server behaves as if CallerPrimaryGroup is NOT equal to DOMAIN_GROUP_RID_COMPUTERS.
2015/08/17	In Section 3.1.5.3, Selective Enumerate Pattern, clarified the implicit constraints for use patterns utilized to obtain deterministic results. Changed from: The client use-pattern for these methods is a call to SamrGetDisplayEnumerationIndex2, followed by a call to SamrQueryDisplayInformation3, passing in the state returned by SamrGetDisplayEnumerationIndex2. This state is used as an index to indicate the account at which SamrQueryDisplayInformation3 will start its enumeration. These methods require a domain handle from the "open" pattern of methods (section 3.1.5.1). Changed to: The client use pattern for these methods is a call to SamrGetDisplayEnumerationIndex2, followed by a call to SamrQueryDisplayInformation3, passing in the state returned by SamrGetDisplayEnumerationIndex2. This state is used as an index to indicate the account at which SamrQueryDisplayInformation3 will start its enumeration. The client can also choose to skip the call to SamrGetDisplayEnumerationIndex2 and begin the enumeration by calling SamrQueryDisplayInformation3, specifying an index of zero. With either use pattern, the client can continue the enumeration process by calling SamrQueryDisplayInformation3 repeatedly, specifying on each call the Index value of the last account returned in the previous call. These methods require a domain handle from the "open" pattern of methods (section 3.1.5.1). The server MAY<44> cache implementation-specific details about the ongoing state of the enumeration on the domain handle; clients therefore MUST follow one of the use patterns

Errata Published*	Description
	described previously in order to produce deterministic results. <44>Non-DC configurations do not cache implementation-specific enumeration states on the domain handle; DC configurations do.
2015/08/03	In Section 3.1.5.9.1, SamrGetGroupsForUser (Opnum 39), clarified the SamrGetGroupsForUser criteria for when the server determines the union of all database objects. Changed from: 3. The server MUST determine the union of all database objects with class group and groupType GROUP_TYPE_SECURITY_ACCOUNT or GROUP_TYPE_SECURITY_UNIVERSAL whose member value contains the SID of the user referenced by UserHandle.Object. Changed to: 3. The server MUST determine the union of all database objects that meet the following criteria: ▪ They are of class group. ▪ Their groupType is GROUP_TYPE_SECURITY_ACCOUNT or GROUP_TYPE_SECURITY_UNIVERSAL. ▪ Their member value contains the SID of the user referenced by UserHandle.Object. ▪ They are in the same domain as the user referenced by UserHandle.Object. The union MUST also contain the group identified by the primaryGroupId attribute of the user that is referenced by UserHandle.Object.
2015/08/03	In Section 3.1.5.3.1, SamrQueryDisplayInformation3 (Opnum 51), clarified the return value of TotalAvailable when the DisplayInformationClass is not set to the DomainDisplayUser. Changed from: 5. For each candidate object to return, the server MUST fill an element in the Buffer output parameter according to the following table. … A call with DisplayInformationClass set to DomainDisplayOemUser or DomainDisplayOemGroup MUST behave identically to a call with DisplayInformationClass set to DomainDisplayUser or DomainDisplayGroup, respectively. The only exception to this rule is that the RPC_UNICODE_STRING structures in the non-Oem cases of DisplayInformationClass MUST be translated to RPC_STRING structures using the OEM code page. Changed to: 5. For each candidate object to return, the server MUST fill an element in the Buffer output parameter according to the following table. …

Errata Published*	Description
	A call with DisplayInformationClass set to DomainDisplayOemUser or DomainDisplayOemGroup MUST behave identically to a call with DisplayInformationClass set to DomainDisplayUser or DomainDisplayGroup, respectively, with the following exceptions: ▪ The RPC_UNICODE_STRING structures in the Oem cases of DisplayInformationClass MUST be translated to RPC_STRING structures using the OEM code page. ▪ The value returned in TotalAvailable MUST be set to zero.
2015/08/03	In Section 3.1.5.12.1, SamrSetSecurityObject (DC Configuration), revised the content to indicate that the server does not ignore the request when SecurityInformation is OWNER_SECURITY_INFORMATION. Changed from: … 3. If the database object referenced by ObjectHandle.Object is not a user object and the DACL_SECURITY_INFORMATION is not set in SecurityInformation, the server MUST silently ignore the request by aborting processing and returning 0. 4. Otherwise, the server MUST determine whether the DACL of SecurityDescriptor of the input message matches one of the following DACLs. The ordering of the ACEs is not relevant. Let Self denote the SID of the user object referenced by ObjectHandle.Object. 5. If there is no match from constraint 4, the server MUST silently ignore the request by aborting processing and returning 0. Changed to: … 3. If the DACL_SECURITY_INFORMATION bit is set in SecurityInformation, the server MUST determine whether the DACL of SecurityDescriptor of the input message matches one of the following DACLs. The ordering of the ACEs is not relevant. Let Self denote the SID of the user object referenced by ObjectHandle.Object. 4 If there is no match from the preceding constraint, the server MUST silently ignore the request by aborting processing and returning 0.

*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.

RSS
Atom

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 ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V47.0 – 2015/06/30.

Errata Published*	Description
2015/09/28	In Section 3.2.4.3.5, Application Requests Creating a File Opened for Durable Operation, updated required client operations for applications requesting durability. Changed from: If the application is requesting durability, the client MUST do the following: ▪ If Connection.Dialect belongs to the SMB 3.x dialect family, the client MUST construct a create context by using the syntax specified in section 2.2.13.2.11, with the following values set: ▪ Timeout MUST be set to an implementation-specific value <115>. ▪ If TreeConnect.IsCAShare is TRUE, the client MUST set the SMB2_DHANDLE_FLAG_PERSISTENT bit in the Flags field. ▪ Reserved MUST be set to zero. ▪ CreateGuid MUST be set to a newly generated GUID. ▪ If the SMB2_DHANDLE_FLAG_PERSISTENT bit is not set in the Flags field, the client MUST perform one of the following: ▪ Request a batch oplock by setting RequestedOplockLevel in the create request to SMB2_OPLOCK_LEVEL_BATCH. ▪ Request a handle caching lease by including an SMB2_CREATE_REQUEST_LEASE or SMB2_CREATE_REQUEST_LEASE_V2 Create Context in the create request with a LeaseState that includes SMB2_LEASE_HANDLE_CACHING. ▪ Otherwise, the client MUST construct a create context using the syntax specified in section 2.2.13.2.3. The client MUST also perform one of the following: ▪ Request a batch oplock by setting RequestedOplockLevel in the create request to SMB2_OPLOCK_LEVEL_BATCH. ▪ Request a handle caching lease by including an SMB2_CREATE_REQUEST_LEASE Create Context in the create request with a LeaseState that includes SMB2_LEASE_HANDLE_CACHING. ▪ The client MUST append the newly constructed create context to any other create contexts being issued with this CREATE request. If the application is not requesting durability, the client MUST follow the normal processing, as specified in section 3.2.4.3. Changed to: If the application is requesting durability, the client MUST do the following: ▪ If Connection.Dialect belongs to the SMB 3.x dialect family, the client MUST construct a create context by using the syntax specified in section 2.2.13.2.11, with the following values set:

Errata Published*	Description
	▪ Timeout MUST be set to an implementation-specific value <115>. ▪ If TreeConnect.IsCAShare is TRUE, the client MUST set the SMB2_DHANDLE_FLAG_PERSISTENT bit in the Flags field. Otherwise, the client SHOULD perform one of the following: ▪ Request a batch oplock by setting RequestedOplockLevel in the create request to SMB2_OPLOCK_LEVEL_BATCH. ▪ Request a handle caching lease by including an SMB2_CREATE_REQUEST_LEASE or SMB2_CREATE_REQUEST_LEASE_V2 Create Context in the create request with a LeaseState that includes SMB2_LEASE_HANDLE_CACHING. ▪ Reserved MUST be set to zero. ▪ CreateGuid MUST be set to a newly generated GUID. ▪ Otherwise, the client MUST construct a create context using the syntax specified in section 2.2.13.2.3. The client SHOULD perform one of the following: ▪ Request a batch oplock by setting RequestedOplockLevel in the create request to SMB2_OPLOCK_LEVEL_BATCH. ▪ Request a handle caching lease by including an SMB2_CREATE_REQUEST_LEASE Create Context in the create request with a LeaseState that includes SMB2_LEASE_HANDLE_CACHING. ▪ The client MUST append the newly constructed create context to any other create contexts being issued with this CREATE request. If the application is not requesting durability, the client MUST follow the normal processing, as specified in section 3.2.4.3.
2015/09/28	In Section 3.3.5.9.10, Handling the SMB2_CREATE_DURABLE_HANDLE_REQUEST_V2 Create Context, the 8th paragraph has been changed. Changed from: If an Open is found and the SMB2_FLAGS_REPLAY_OPERATION bit is set in the SMB2 header, the server MUST construct an SMB2_CREATE_DURABLE_HANDLE_RESPONSE_V2 response create context. The Timeout MUST be set to Open.DurableOpenTimeout. If Open.IsPersistent is TRUE, the server MUST set the SMB2_DHANDLE_FLAG_PERSISTENT bit in the Flags field. The Buffer specified by the response MUST include the CreateContextsLength and CreateContextsOffset fields. Changed to: If an Open is found and the SMB2_FLAGS_REPLAY_OPERATION bit is set in the SMB2 header, the server MUST perform the following: ▪ The server MUST set Open.Connection to the connection that received this request. ▪ The server MUST construct an SMB2_CREATE_DURABLE_HANDLE_RESPONSE_V2 create context as follows: ▪ The Timeout field MUST be set to Open.DurableOpenTimeout. ▪ If Open.IsPersistent is TRUE, the server MUST set the SMB2_DHANDLE_FLAG_PERSISTENT bit in the Flags field. ▪ The Buffer specified by the response MUST include the CreateContextsLength and CreateContextsOffset fields.
2015/09/14	In Section 3.3.5.16, Receiving an SMB2 CANCEL Request, corrected the second paragraph. Changed from: An SMB2 CANCEL Request is the only request received by the server that is not signed and does not contain a sequence number that must be checked. Thus, the server MUST NOT process the

Errata Published*	Description
	received packet as specified in sections 3.3.5.2.3 and 3.3.5.2.4. Changed to: An SMB2 CANCEL Request does not contain a sequence number that must be checked. Thus, the server MUST NOT process the received packet as specified in section 3.3.5.2.3.
2015/08/17	In Section 3.3.5.5, Receiving an SMB2 SESSION_SETUP Request, added information about session binding from a different client Guid. Changed from: ▪ … ▪ If the SMB2_FLAGS_SIGNED bit is not set in the Flags field in the header, the server MUST fail the request with error STATUS_INVALID_PARAMETER. ▪ If Session.State is InProgress, the server MUST fail the request with STATUS_REQUEST_NOT_ACCEPTED. ▪ … Changed to: ▪ … ▪ If the SMB2_FLAGS_SIGNED bit is not set in the Flags field in the header, the server MUST fail the request with error STATUS_INVALID_PARAMETER. ▪ If Session.Connection.ClientGuid is not the same as Connection.ClientGuid, the server MAY fail the request with STATUS_USER_SESSION_DELETED. ▪ If Session.State is InProgress, the server MUST fail the request with STATUS_REQUEST_NOT_ACCEPTED. ▪ …
2015/08/03	In Section 3.3.5.9, Receiving an SMB2 CREATE Request, corrected the list of Windows product versions that check Treeconnect.MaximalAccess when deleting a file. Changed from: If the FILE_DELETE_ON_CLOSE flag is set in CreateOptions and any of the following conditions is TRUE, the server SHOULD<249> fail the request with STATUS_ACCESS_DENIED. <249> Section 3.3.5.9: Windows Vista SP1, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012 do not perform this verification. Changed to: If the FILE_DELETE_ON_CLOSE flag is set in CreateOptions and any of the following conditions is TRUE, the server SHOULD<249> fail the request with STATUS_ACCESS_DENIED. <249> Section 3.3.5.9: Windows Vista SP1, Windows Server 2008, Windows 7, and Windows Server 2008 R2 do not perform this verification.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2015/08/03</td><td>
In several sections, changed the reference that specifies the HMAC-SHA256 algorithms.

In sections:

1.6, Applicability Statement

3.1.4.1, Signing An Outgoing Message

3.1.5.1, Verifying an Incoming Message

Changed from:

[FIPS180-2] National Institute of Standards and Technology, "Secure Hash Standard", FIPS PUB 180-2, August 2002, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

Changed to:

[FIPS180-4] FIPS PUBS, "Secure Hash Standards (SHS)", March 2012, http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

In Section 2.2.3.1.1, SMB2_PREAUTH_INTEGRITY_CAPABILITIES, added this updated reference to the HashAlgorithms table.

Changed from:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x0001</td><td>SHA-512</td></tr>
</table>

Changed to:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0x0001</td><td>SHA-512 as specified in [FIPS180-4]</td></tr>
</table>
</td></tr>
<tr><td>2015/08/03</td><td>
In Section 2.2.21, SMB2 WRITE Request, corrected that SMB2_CHANNEL_RDMA_V1_INVALIDATE should reference WriteChannelInfoOffset and WriteChannelInfoLength fields.

Changed from:

Channel (4 bytes): For the SMB 2.0.2 and 2.1 dialects, this field MUST NOT be used and MUST be reserved. The client MUST set this field to 0, and the server MUST ignore it on receipt. For the SMB 3.x dialect family, this field MUST contain exactly one of the following values:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>SMB2_CHANNEL_RDMA_V1_INVALIDATE

0x00000002</td><td>This flag is not valid for the SMB 2.0.2, 2.1, and 3.0 dialects. One or more SMB_DIRECT_BUFFER_DESCRIPTOR_V1 structures as specified in [MS-SMBD] section 2.2.3.1 are present in the channel information specified by the ReadChannelInfoOffset and ReadChannelInfoLength fields. The server is requested to perform remote invalidation when responding to the request as specified in [MS-SMBD] section 3.1.4.2.</td></tr>
</table>
</td></tr>
</table>

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

Channel (4 bytes): For the SMB 2.0.2 and 2.1 dialects, this field MUST NOT be used and MUST be reserved. The client MUST set this field to 0, and the server MUST ignore it on receipt. For the SMB 3.x dialect family, this field MUST contain exactly one of the following values:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>SMB2_CHANNEL_RDMA_V1_INVALIDATE

0x00000002</td><td>This flag is not valid for the SMB 2.0.2, 2.1, and 3.0 dialects. One or more SMB_DIRECT_BUFFER_DESCRIPTOR_V1 structures as specified in [MS-SMBD] section 2.2.3.1 are present in the channel information specified by the WriteChannelInfoOffset and WriteChannelInfoLength fields. The server is requested to perform remote invalidation when responding to the request as specified in [MS-SMBD] section 3.1.4.2.</td></tr>
</table>
</td></tr>
<tr><td>2015/08/03</td><td>
In two sections, clarified that SMB2_GLOBAL_CAP_ENCRYPTION applies to SMB 3.0 and 3.0.2 dialects.

In Section 2.2.4,SMB2 NEGOTIATE Response, changed from:

Capabilities (4 bytes): The Capabilities field specifies protocol capabilities for the server. This field MUST be constructed using a combination of zero or more of the following values.

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>SMB2_GLOBAL_CAP_ENCRYPTION

0x00000040</td><td>When set, indicates that the server supports encryption. This flag is not valid for the SMB 2.0.2 and SMB 2.1 dialects.</td></tr>
</table>

Changed to:

Capabilities (4 bytes): The Capabilities field specifies protocol capabilities for the server. This field MUST be constructed using a combination of zero or more of the following values.

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>SMB2_GLOBAL_CAP_ENCRYPTION

0x00000040</td><td>When set, indicates that the server supports encryption. This flag is valid for the SMB 3.0 and 3.0.2 dialects.</td></tr>
</table>

In Section 3.2.5.2, Receiving an SMB2 NEGOTIATE Response, changed from:

If the client implements SMB 2.1 or SMB 3.x dialect family, the client MUST perform the following:

▪ The client MUST store the returned dialect in Connection.Dialect.

…

If Connection.Dialect belongs to the SMB 3.x dialect family, the client MUST perform the following:

▪ If SMB2_GLOBAL_CAP_DIRECTORY_LEASING is set in the Capabilities field of the SMB2
</td></tr>
</table>

Errata Published*	Description
	NEGOTIATE Response, the client MUST set Connection.SupportsDirectoryLeasing to TRUE. Otherwise, it MUST be set to FALSE. Changed to: If the client implements SMB 2.1 or SMB 3.x dialect family, the client MUST perform the following: ▪ The client MUST set Connection.Dialect to DialectRevision in the SMB2 NEGOTIATE Response. … If Connection.Dialect belongs to the SMB 3.x dialect family, the client MUST perform the following: ▪ If SMB2_GLOBAL_CAP_ENCRYPTION is set in the Capabilities field of the SMB2 NEGOTIATE Response and Connection.Dialect is "3.0" or "3.0.2", the client MUST set Connection.SupportsEncryption to TRUE. Otherwise, it MUST be set to FALSE.

2015/08/03	In 5 sections, corrected that Open.LockSequenceArray[] must be initialized to 0xFF, not 0.
	
	In Section 3.3.1.10, Per Open, changed from:
	
	If the server implements the SMB 2.1 or SMB 3.x dialect family and supports leasing, it MUST implement the following:
	
	▪ …
	▪ Open.ResilientOpenTimeout: A time value that indicates when a handle that has been preserved for resiliency will be closed by the system if a client has not reclaimed it.
	▪ Open.LockSequenceArray: An array of 64 entries used to maintain lock sequences for resilient Opens. Each entry value MUST be empty, or MUST be 4-bit integer modulo 16. Each entry MUST be assigned an index from the range of 1 to 64.
	
	Changed to:
	
	If the server implements the SMB 2.1 or SMB 3.x dialect family and supports leasing, it MUST implement the following:
	
	▪ …
	▪ Open.ResilientOpenTimeout: A time-out value that indicates when a handle that has been preserved for resiliency will be closed by the system if a client has not reclaimed it.
	▪ Open.LockSequenceArray: An array of 64 entries used to maintain lock sequences for resilient opens. Each entry MUST be assigned an index from the range of 1 to 64. Each entry is a structure with the following elements:
	  ▪ SequenceNumber: A 4-bit integer modulo 16.
	  ▪ Valid: A Boolean, if set to TRUE, indicates that the SequenceNumber element is valid.
	
	In Section 3.3.5.9, Receiving an SMB2 CREATE Request, changed from:

Errata Published*	Description

	If Connection.Dialect is not "2.0.2" and the server supports leasing, the server MUST initialize the following:
	
	▪ …
	▪ Open.ResilientOpenTimeout MUST be set to 0.
	  ▪ Open.LockSequenceArray: Each element of Open.LockSequenceArray MUST be initialized to empty.
	
	Changed to:
	
	If Connection.Dialect is not "2.0.2" and the server supports leasing, the server MUST initialize the following:
	
	▪ …
	▪ Open.ResilientOpenTimeout MUST be set to 0.
	▪ Each entry of Open.LockSequenceArray MUST be initialized as follows:
	  ▪ Set Valid to FALSE.
	
	In Section 3.3.5.14, Receiving an SMB2 LOCK Request, changed from:
	
	The server verifies the LockSequence by performing the following steps:
	
	▪ The server MUST use LockSequenceIndex as an index into Open.LockSequenceArray in order to locate the sequence number entry. If the index exceeds the maximum extent of the Open.LockSequenceArray, or LockSequenceIndex is 0, or if the sequence number entry is empty, the server MUST skip step 2 and continue lock/unlock processing.
	▪ The server MUST compare LockSequenceNumber to the SequenceNumber of the entry located in step 1. If the sequence numbers are equal, the server MUST complete the lock/unlock request with success. Otherwise, the server MUST reset the entry value to empty and continue lock/unlock processing.
	
	Changed to:
	
	The server verifies the LockSequence by performing the following steps:
	
	▪ The server MUST use LockSequenceIndex as an index into Open.LockSequenceArray in order to locate the sequence number entry. If the index exceeds the maximum extent of the Open.LockSequenceArray, or LockSequenceIndex is 0, or if the Open.LockSequenceArray.Valid is FALSE, the server MUST skip step 2 and continue lock/unlock processing.
	▪ The server MUST compare LockSequenceNumber to the SequenceNumber of the entry located in step 1. If the sequence numbers are equal, the server MUST complete the lock/unlock request with success. Otherwise, the server MUST reset the entry by setting Valid to FALSE

Errata Published*	Description
	and continue lock/unlock processing. In Section 3.3.5.14.1, Processing Unlocks, changed from: If the unlock operation succeeds and there are no remaining entries in the Locks array, Connection.Dialect is "2.1" or belongs to the SMB 3.x dialect family, the server supports leasing, and Open.IsResilient is TRUE, the server MUST set the lock sequence number in Open.LockSequenceArray through the following step to indicate that the unlock request with LockSequence has been successfully processed by the server: ▪ If an entry is found via the lock request process described in the numbered list in section 3.3.5.14, the server MUST save LockSequenceNumber into the corresponding entry. Changed to: If the unlock operation succeeds and there are no remaining entries in the Locks array, Connection.Dialect is "2.1" or belongs to the SMB 3.x dialect family, the server supports leasing, and Open.IsResilient is TRUE, the server MUST set the lock sequence number in Open.LockSequenceArray through the following step to indicate that the unlock request with LockSequence has been successfully processed by the server: ▪ If an entry is found via the lock request process described in the numbered list in section 3.3.5.14, the server MUST set Valid to TRUE and save LockSequenceNumber into SequenceNumber of the corresponding entry. In Section 3.3.5.14.2, Processing Locks, changed from: If the lock operation succeeds and there are no remaining entries in the Locks array, Connection.Dialect is "2.1" or belongs to the SMB 3.x dialect family, the server supports leasing, and Open.IsResilient is TRUE, the server MUST set the lock sequence number in Open.LockSequenceArray through the following step to indicate that the lock request with LockSequence has been successfully processed by the server: ▪ If an entry is found via the lock request process described in the numbered list in section 3.3.5.14, the server MUST save LockSequenceNumber into the corresponding entry. Changed to: If the lock operation succeeds and there are no remaining entries in the Locks array, Connection.Dialect is "2.1" or belongs to the SMB 3.x dialect family, the server supports leasing, and Open.IsResilient is TRUE, the server MUST set the lock sequence number in Open.LockSequenceArray through the following step to indicate that the lock request with LockSequence has been successfully processed by the server:

Errata Published*	Description
	▪ If an entry is found via the lock request process described in the numbered list in section 3.3.5.14, the server MUST set Valid to TRUE and save LockSequenceNumber into SequenceNumber of the corresponding entry

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-TCC]: Tethering Control Channel Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V3.0 – 2015/06/30.

Errata Published*	Description
2015/10/12	In Appendix A, Product Behavior, added the following Windows Server version: Windows Server 2012 R2 operating system

*Date format: YYYY/MM/DD

[MS-TDS]: Tabular Data Stream Protocol

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V18.0 – 2015/06/30.

Errata Published*	Description
2015/06/30	In section 6, Appendix A: Product Behavior, product behavior notes <11>, <13>, <17>, <22>, <27>, <31>, and <41> are updated as follows. Note <11> is changed from: <11> Section 2.2.3.1.1: Only legacy clients that support SQL Server versions that were released prior to sql_server 7.0 can use Pre-TDS7 Login. Changed to: <11> Section 2.2.3.1.1: Only legacy clients that support SQL Server versions that were released prior to SQL Server 7.0 can use Pre-TDS7 Login. Note <13> is changed from: <13> Section 2.2.3.1.1: Only clients that support sql_server 7.0 or later can use TDS7 Login. Changed to: <13> Section 2.2.3.1.1: Only clients that support SQL Server 7.0 or later can use TDS7 Login. In note <17>, the second paragraph is changed from: Version can be of value 0, 1, or 2. A value of 0 denotes collations in SQL Server 2000. A value of 1 denotes collations in SQL Server 2005. A value of 2 denotes collations in SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014. Changed to: Version can be of value 0, 1, or 2. A value of 0 denotes collations in SQL Server 2000. A value of 1 denotes collations in SQL Server 2005. A value of 2 denotes collations in SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, SQL Server 2014, and SQL Server 2016 CTP2. Note <22> is changed from: <22> Section 2.2.6.4: The version numbers used by clients are as follows.

Errata Published*	Description

SQL Server version	Version sent from client to server
SQL Server 7.0	0x00000070
SQL Server 2000	0x00000071
SQL Server 2000 SP1	0x01000071
SQL Server 2005	0x02000972
SQL Server 2008	0x03000A73
SQL Server 2008 R2	0x03000B73
SQL Server 2012 SQL Server 2014	0x04000074

Changed to:

<22> Section 2.2.6.4: The version numbers used by clients are as follows.

SQL Server version	Version sent from client to server
SQL Server 7.0	0x00000070
SQL Server 2000	0x00000071
SQL Server 2000 SP1	0x01000071
SQL Server 2005	0x02000972
SQL Server 2008	0x03000A73
SQL Server 2008 R2	0x03000B73
SQL Server 2012 SQL Server 2014 SQL Server 2016 CTP2	0x04000074

Note <27> is changed from:

<27> Section 2.2.6.5: In SQL Server 2012, and SQL Server 2014, the server always sends the value 0 for the INSTOPT option when the string specified in the client's INSTOPT option is "MSSQLServer". The reason for this is that "MSSQLServer" is the name of a default instance, and "MSSQLServer" may be provided by the client even in the absence of an explicit instance name. SQL Server 2000, SQL Server 2005, SQL Server 2008, and SQL Server 2008 R2, which support the INSTOPT field always validate the client-specified string against the server's instance name.

Changed to:

<27> Section 2.2.6.5: In SQL Server 2012, SQL Server 2014, and SQL Server 2016 CTP2, the server always sends the value 0 for the INSTOPT option when the string specified in the client's INSTOPT option is "MSSQLServer". The reason for this is that "MSSQLServer" is the name of a default instance, and "MSSQLServer" may be provided by the client even in the absence of an explicit instance name. SQL Server 2000, SQL Server 2005, SQL Server 2008, and SQL Server 2008 R2, which support the INSTOPT field always validate the client-specified string against the server's instance name.

In note <31>, the fourth paragraph is changed from:

SNAC [MSDN-SNAC] and SQLClient use the VERSION option in the Pre-Login Response message to detect whether DoneRowCount is LONG or ULONGLONG. It is ULONGLONG if VERSION in the

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
Pre-Login Response message indicates that the server is SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, or SQL Server 2014. Otherwise, DoneRowCount is LONG.

Changed to:

SNAC [MSDN-SNAC] and SQLClient use the VERSION option in the Pre-Login Response message to detect whether DoneRowCount is LONG or ULONGLONG. It is ULONGLONG if VERSION in the Pre-Login Response message indicates that the server is SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, SQL Server 2014, or SQL Server 2016 CTP2. Otherwise, DoneRowCount is LONG.

Note <41> is changed from:

<41> Section 2.2.7.13: The following table shows the values in network transfer format.

<table>
<tr><th>SQL Server</th><th>Client to server</th><th>Server to client</th></tr>
<tr><td>SQL Server 7.0</td><td>0x00000070</td><td>0x07000000</td></tr>
<tr><td>SQL Server 2000</td><td>0x00000071</td><td>0x07010000</td></tr>
<tr><td>SQL Server 2000 SP1</td><td>0x01000071</td><td>0x71000001</td></tr>
<tr><td>SQL Server 2005</td><td>0x02000972</td><td>0x72090002</td></tr>
<tr><td>SQL Server 2008*</td><td>0x03000A73</td><td>0x730A0003</td></tr>
<tr><td>SQL Server 2008 R2</td><td>0x03000B73</td><td>0x730B0003</td></tr>
<tr><td>SQL Server 2012

SQL Server 2014</td><td>0x04000074</td><td>0x74000004</td></tr>
</table>
*SQL Server 2008 TDS version 0x03000A73 does not include support for NBCROW and fSparseColumnSet.

Changed to:

<41> Section 2.2.7.13: The following table shows the values in network transfer format.

<table>
<tr><th>SQL Server</th><th>Client to server</th><th>Server to client</th></tr>
<tr><td>SQL Server 7.0</td><td>0x00000070</td><td>0x07000000</td></tr>
<tr><td>SQL Server 2000</td><td>0x00000071</td><td>0x07010000</td></tr>
<tr><td>SQL Server 2000 SP1</td><td>0x01000071</td><td>0x71000001</td></tr>
<tr><td>SQL Server 2005</td><td>0x02000972</td><td>0x72090002</td></tr>
<tr><td>SQL Server 2008*</td><td>0x03000A73</td><td>0x730A0003</td></tr>
<tr><td>SQL Server 2008 R2</td><td>0x03000B73</td><td>0x730B0003</td></tr>
<tr><td>SQL Server 2012

SQL Server 2014

SQL Server 2016 CTP2</td><td>0x04000074</td><td>0x74000004</td></tr>
</table>
</td></tr>
</table>

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V3.0 – 2015/06/30.

Errata Published*	Description
2015/10/12	In Section 3.4.4.1, CreateVirtualSmartCardWithAttestation (Opnum 6), changed from: AttestationType: A TPMVSC_ATTESTATION_TYPE value specifying the desired attestation properties of the new VSC. Changed to: attestationType: A TPMVSC_ATTESTATION_TYPE value specifying the desired attestation properties of the new VSC.

*Date format: YYYY/MM/DD

[MS-TSGU]: Terminal Services Gateway Server Protocol

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

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

RSS
Atom

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 ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V22.0 – 2015/06/30.

Errata Published*	Description
2015/08/17	In Section 2.2.1.17, UINT_PTR, clarified that the UINT_PTR is an unsigned integer. Changed from: A pointer to an unsigned integer, whose length is dependent on processor word size. Changed to: An unsigned integer, whose length is dependent on processor word size.

*Date format: YYYY/MM/DD

[MS-UCODEREF]: Windows Protocols Unicode Reference

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-WCCE]: Windows Client Certificate Enrollment Protocol

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V3.0 – 2015/06/30.

Errata Published*	Description
2015/10/12	In Appendix A, Product Behavior, added the following Windows Server versions: Windows Server 2012 operating system Windows Server 2012 R2 operating system Windows Server 2016 Technical Preview operating system

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V1.0 – 2015/06/30.

Errata Published*	Description

2015/08/17	In Section 2.1.1.5, intel_sink_model_name, updated the ABNF syntax for the intel_sink_model_name parameter.
	
	Changed from:
	
	The ABNF syntax is as follows:
	
	`intel-sink-model-name = "intel_sink_model_name:" SP model_name CRLF`
	`model-name = 1*32(VCHAR) / "none"`
	
	Changed to:
	
	The ABNF syntax is as follows:
	
	`intel-sink-model-name = "intel_sink_model_name:" SP model-name CRLF`
	`model-name = 1*32(VCHAR) / "none"`

2015/08/17	In Section 2.1.1.6, intel_sink_version, updated the definitions for hw-version and sw-version, and added new definitions for sku and build in the intel_sink_version parameter syntax.
	
	Changed from:
	
	The intel_sink_version parameter specifies the product identifier, hardware version, and software version of the Wi-Fi Display Sink.
	
	`intel-sink-version = "intel_sink_version:" SP product-id SP hw-version SP sw-version CRLF`
	`product-id = "product_ID=" 1*16(VCHAR)`
	`hw-version = "hw_version=" version_tag`
	`sw-version = "sw_version=" version_tag`
	`version-tag = major "." minor "." sku "." build`
	`major = 1*2(DIGIT)`
	`minor = 1*2(DIGIT)`
	
	Changed to:

Errata Published*	Description

	The intel_sink_version parameter specifies the product identifier, hardware version, and software version of the Wi-Fi Display Sink.
	
	`intel-sink-version = "intel_sink_version:" SP product-id SP hw-version SP sw-version CRLF`
	`product-id = "product_ID=" 1*16(VCHAR)`
	`hw-version = "hw_version=" version-tag`
	`sw-version = "sw_version=" version-tag`
	`version-tag = major "." minor "." sku "." build`
	`major = 1*2(DIGIT)`
	`minor = 1*2(DIGIT)`
	`sku = 1*2(DIGIT)`
	`build = 1*4(DIGIT)`

2015/08/17	In Section 2.4.1.1, microsoft_latency_management_capability, clarified where the microsoft_latency_management_capability parameter is being used. Changed from: The microsoft_latency_management_capability parameter specifies whether the Wi-Fi Display Sink is capable of dynamically changing the display latency of the video bit stream. When sent by the Wi-Fi Display Sink, the parameter specifies the desired latency mode. Changed to: The microsoft_latency_management_capability parameter specifies whether the Wi-Fi Display Sink is capable of dynamically changing the display latency of the video bit stream. When sent by the Wi-Fi Display Sink, the parameter specifies the desired latency mode. This parameter is included by the Wi-Fi Display Source in the M3 request to specify support for latency management, by the Wi-Fi Display Sink in the M3 response to specify support for latency management, and by the Wi-Fi Display Source in a SET_PARAMETER request to set the latency mode to a new value.

*Date format: YYYY/MM/DD

[MS-WPO]: Windows Protocols Overview

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

[MS-WMF]: Windows Metafile Format

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

Errata below are for Protocol Document Version V12.0 – 2015/06/30.

Errata Published*	Description
2015/10/12	In Section 2.1.1.3, BitCount Enumeration, clarified the meaning of the DIB Colors field for BitCount enumeration values. Changed from: **BI_BITCOUNT_4:** The image is specified with a maximum of 2^16 colors. Each pixel in the bitmap in the **BitmapBuffer** field of the DIB Object is represented by a 16-bit value. If the **Compression** field of the BitmapInfoHeader Object is BI_RGB, the **Colors** field of the DIB Object is NULL. Each WORD in the bitmap represents a single pixel. The relative intensities of red, green, and blue are represented with 5 bits for each color component. The value for blue is in the least significant 5 bits, followed by 5 bits each for green and red. The most significant bit is not used. The color table is used for optimizing colors on palette-based devices, and contains the number of entries specified by the **ColorUsed** field of the BitmapInfoHeader Object. If the **Compression** field of the BitmapInfoHeader Object is BI_BITFIELDS, the **Colors** field contains three DWORD color masks that specify the red, green, and blue components, respectively, of each pixel. Each WORD in the bitmap array represents a single pixel. When the **Compression** field is set to BI_BITFIELDS, bits set in each DWORD mask MUST be contiguous and SHOULD NOT overlap the bits of another mask. BI_RGB and BI_BITFIELDS are defined in Compression Enumeration, section 2.1.1.7. **BI_BITCOUNT_5:** The bitmap in the **BitmapBuffer** field of the DIB Object has a maximum of 2^24 colors, and the **Colors** field is NULL. Each 3-byte triplet in the bitmap represents the relative intensities of blue, green, and red, respectively, for a pixel. The **Colors** color table is used for optimizing colors used on palette-based devices, and MUST contain the number of entries specified by the **ColorUsed** field of the BitmapInfoHeader Object. **BI_BITCOUNT_6:** The bitmap in the **BitmapBuffer** field of the DIB Object has a maximum of 2^24 colors. If the **Compression** field of the BitmapInfoHeader Object is set to BI_RGB, the **Colors** field of the DIB Object is set to NULL. Each DWORD in the bitmap in the **BitmapBuffer** field represents the relative intensities of blue, green, and red, respectively, for a pixel. The high byte in each DWORD is not used. The **Colors** color table is used for optimizing colors used on palette-based devices, and MUST contain the number of entries specified by the **ColorUsed** field of the BitmapInfoHeader Object. If the **Compression** field is set to BI_BITFIELDS, the color table in the **Colors** field contains

Errata Published*	Description
	three DWORD color masks that specify the red, green, and blue components, respectively, of each pixel. Each DWORD in the bitmap represents a single pixel. . When the **Compression** field is set to BI_BITFIELDS, bits set in each DWORD mask MUST be contiguous and MUST NOT overlap the bits of another mask. All the bits in the pixel do not need to be used. BI_RGB and BI_BITFIELDS are specified in Compression Enumeration, section 2.1.1.7. Changed to: **BI_BITCOUNT_4:** The image is specified with a maximum of 2^16 colors. Each pixel in the bitmap in the **BitmapBuffer** field of the DIB Object is represented by a 16-bit value. If the **Compression** field of the BitmapInfoHeader Object is BI_RGB, the **Colors** field of the DIB Object is NULL. Each WORD in the bitmap represents a single pixel. The relative intensities of red, green, and blue are represented with 5 bits for each color component. The value for blue is in the least significant 5 bits, followed by 5 bits each for green and red. The most significant bit is not used. If the **Compression** field of the BitmapInfoHeader Object is BI_BITFIELDS, the **Colors** field contains three DWORD color masks that specify the red, green, and blue components, respectively, of each pixel. Each WORD in the bitmap array represents a single pixel. The color table is used for optimizing colors on palette-based devices, and contains the number of entries specified by the **ColorUsed** field of the BitmapInfoHeader Object. When the **Compression** field is set to BI_BITFIELDS, bits set in each DWORD mask MUST be contiguous and SHOULD NOT overlap the bits of another mask. BI_RGB and BI_BITFIELDS are defined in Compression Enumeration, section 2.1.1.7. **BI_BITCOUNT_5:** The bitmap in the **BitmapBuffer** field of the DIB Object has a maximum of 2^24 colors, and the **Colors** field is NULL. Each 3-byte triplet in the bitmap represents the relative intensities of blue, green, and red, respectively, for a pixel. **BI_BITCOUNT_6:** The bitmap in the **BitmapBuffer** field of the DIB Object has a maximum of 2^24 colors. If the **Compression** field of the BitmapInfoHeader Object is set to BI_RGB, the **Colors** field of the DIB Object is set to NULL. Each DWORD in the bitmap in the **BitmapBuffer** field represents the relative intensities of blue, green, and red, respectively, for a pixel. The high byte in each DWORD is not used. If the **Compression** field is set to BI_BITFIELDS, the color table in the **Colors** field contains three DWORD color masks that specify the red, green, and blue components, respectively, of each pixel. Each DWORD in the bitmap represents a single pixel. The color table is used for optimizing colors used on palette-based devices and contains the number of entries specified by the **ColorUsed** field of the BitmapInfoHeader Object. When the **Compression** field is set to BI_BITFIELDS, bits set in each DWORD mask MUST be contiguous and MUST NOT overlap the bits of another mask. All the bits in the pixel do not need to be used. BI_RGB and BI_BITFIELDS are specified in Compression Enumeration, section 2.1.1.7.

*Date format: YYYY/MM/D

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

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

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

RSS
Atom

To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here. Errata below are for Protocol Document Version V28.0 – 2015/06/30.

Errata Published*	Description
2015/09/14	In Appendix A: Full WSDL, compilation errors were fixed. View this PDF document to see the corrections: [MS-WSMV]_WSDL.
2015/09/14	In the description of the Message field in three sections, corrected that the original length of the field must be equal to the lengthvalue field (changes in **bold** below). In Section 2.2.9.1.2.2.2, Encrypted Data, changed from: Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework as specified in [RFC4121]. The initial bytes of the Message MUST be the Security token portion, whose length MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.2.2.1. Changed to: Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework as specified in [RFC4121]. The initial bytes of the Message MUST be the Security token portion, whose length MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose **original** length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.2.2.1. In Section 2.2.9.1.3.1.2.2, Encrypted Data, changed from: Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework as specified in [RFC4121]. The initial bytes of the Message MUST be the Security token portion, whose length MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.3.1.2.1. Changed to: Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework as specified in [RFC4121]. The initial bytes of the Message MUST be the Security token portion, whose length MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose **original** length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.3.1.2.1.

Errata Published*	Description
	In Section 2.2.9.1.3.2.2.2, Encrypted Data, changed from: Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework as specified in [RFC4121]. The initial bytes of the Message MUST be the Security token portion, whose length MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.3.2.2.1. Changed to: Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework as specified in [RFC4121]. The initial bytes of the Message MUST be the Security token portion, whose length MUST be given in the Length-Field value. The remaining bytes MUST be the encrypted data, whose **original** length MUST be equal to the lengthvalue field as defined in section 2.2.9.1.3.2.2.1.

*Date format: YYYY/MM/DD

[MS-WSP]: Windows Search Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V28.0 – 2015/06/30.

Errata Published*	Description
2015/10/12	In Section 2.1, Transport, corrected the ImpersonationLevel cited from SECURITY_IDENTIFICATION to SECURITY_IMPERSONATION. Changed from: This protocol uses the underlying server message block (SMB) named pipe protocol to retrieve the identity of the caller that made the connection as specified in [MS-SMB] section 2.2.4.9.1. The client MUST set SECURITY_IDENTIFICATION as the ImpersonationLevel in the request to open the named pipe. Changed to: This protocol uses the underlying server message block (SMB) named pipe protocol to retrieve the identity of the caller that made the connection as specified in [MS-SMB] section 2.2.4.9.1. The client MUST set SECURITY_IMPERSONATION as the ImpersonationLevel in the request to open the named pipe.
2015/10/12	In Section 2.2.1.29, CInGroupSortAggregSet, the description of SortAggregSet has been changed from: SortAggregSet (variable): A CSortAggregSet structure, specifying the sort order for the range in the parent's group. Changed to: SortAggregSet (variable): A CSortSet structure, specifying the sort order for the range in the parent's group. In Section 2.2.3.4, CPMCreateQueryIn, the description of SortAggregSet has been changed from: SortSet (variable): A CSorSet structure indicating the sort order (1) of the query. Changed to: SortSet (variable): A CInGroupSortAggregSets structure indicating the sort order (1) of the query.
2015/10/12	In Section 2.2, Message Syntax, the values of DBBMK_FIRST and DBBMK_LAST, incorrectly

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>documented as 1 and 2 have been corrected to 0xfffffffc and 0xfffffffd.

Changed from:

<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>DBBMK_FIRST
0x00000001</td><td>A bookmark handle to a bookmark that identifies the first row in the rowset.</td></tr><tr><td>DBBMK_LAST
0x00000002</td><td>A bookmark handle to a bookmark that identifies the last row in the rowset.</td></tr></table>
Changed to:

<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>DBBMK_FIRST
0xFFFFFFFC</td><td>A bookmark handle to a bookmark that identifies the first row in the rowset.</td></tr><tr><td>DBBMK_LAST
0xFFFFFFFD</td><td>A bookmark handle to a bookmark that identifies the last row in the rowset.</td></tr></table></td></tr>
<tr><td></td><td></td></tr>
</table>

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

No errata are available for the latest version of this Windows Protocols document. To view a PDF file of the errata for the previous version of this document, see the ERRATA June 30 2015 Archive here.

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V10.0 – 2015/06/30.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2015/08/31</td><td>In Section 2.3, Directory Service Schema Elements, added 6 user class attributes.

Changed from:
<table><tr><th>Class</th><th>Attibute</th></tr><tr><td>User</td><td>userCertificate</td></tr></table>
Changed to:
<table><tr><th>Class</th><th>Attibutes</th></tr><tr><td>User</td><td>cn
distinguishedName
dNSHostName
mail
objectGUID
userCertificate
userPrincipalName</td></tr></table></td></tr>
</table>

*Date format: YYYY/MM/DD