Windows Protocols Errata

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

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

RSS
Atom

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

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

The sections below list the Windows Protocols documents that contain active Errata (i.e., Errata not yet released with the documents on MSDN) and provide links to archived Errata (i.e., Errata already released with the documents on MSDN).

Protocols Documents with Active Errata

[MS-ADA2]: Active Directory Schema Attributes M

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

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

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

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

[MS-ADTS]: Active Directory Technical Specification

[MS-AIPS]: Authenticated Internet Protocol

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

[MS-CSRA]: Certificate Services Remote Administration Protocol

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

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

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

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

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

[MS-DTYP]: Windows Data Types

[MS-DVRD]: Device Registration Discovery Protocol

[MS-ECS]: Enterprise Client Synchronization Protocol

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

[MS-ERREF]: Windows Error Codes

[MS-EVEN]: EventLog Remoting Protocol

[MS-FASP]: Firewall and Advanced Security Protocol

[MS-FSA]: File System Algorithms

[MS-FSCC]: File System Control Codes

[MS-FSRVP]: File Server Remote VSS Protocol

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

[MS-ICPR]: ICertPassage Remote Protocol

[MS-IKEE]: Internet Key Exchange Protocol Extensions

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

[MS-KILE]: Kerberos Protocol Extensions

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

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

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

[MS-MDM]: Mobile Device Management Protocol

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

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

[MS-NRPC]: Netlogon Remote Protocol

[MS-OAPX]: OAuth 2.0 Protocol Extensions

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

[MS-PSRP]: PowerShell Remoting Protocol

[MS-RAI]: Remote Assistance Initiation Protocol

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

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

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

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

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

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

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

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

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

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

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

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

[MS-RPRN]: Print System Remote Protocol

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

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

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

[MS-RSVD]: Remote Shared Virtual Disk Protocol

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

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

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

[MS-SQOS]: Storage Quality of Service Protocol

[MS-SWN]: Service Witness Protocol

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

[MS-TSCH]: Task Scheduler Service Remoting Protocol

[MS-TSGU]: Terminal Services Gateway Server Protocol

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

[MS-WCCE]: Windows Client Certificate Enrollment Protocol

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

[MS-WKST]: Workstation Service Remote Protocol

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

[MS-WSUSAR]: Windows Server Update Services: Administrative API Remoting Protocol

[MS-WSUSSS]: Windows Update Services: Server-Server Protocol

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

Errata Archives

March 2, 2016 - Download

October 16, 2015 - Download

June 30, 2015 - Download

Last date updated: June 27, 2016

[MS-ABTP]: Automatic Bluetooth Pairing Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-ADA2]: Active Directory Schema Attributes M

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V28.0 – 2015/10/16.

Errata Published*	Description
2016/06/27	In Section 2.347, msDS-KeyCredentialLink-BL, updated the msDS-KeyCredentialLink-BL attribute class with the omObjectClass attribute. Changed from: attributeSyntax: 2.5.5.1 oMSyntax: 127 Changed to: attributeSyntax: 2.5.5.1 omObjectClass: 1.3.12.2.1011.28.0.714 oMSyntax: 127

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V12.0 – 2015/10/16.

Errata Published*	Description
2015/11/23	In Section 2.1, Endpoints, for more information on the semantics of the net.tcp binding, changed an informative reference ([MSDN-BINDINGS]) to a normative reference ([MS-NMFTB]). Changed from: For more information on this binding type, see [MSDN-BINDINGS], "NetTcpBinding" Changed to: For semantics of this binding type, see [MS-NMFTB].

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

Errata Published*	Description
2016/05/16	In the following sections, updated the name of query parameter ClientRequestId to client-request-id: Section 2.2.2.1 client-request-id Section 2.2.3 Common URI Parameters Section 2.2.3.3 client-request-id Section 3.2.4.1.1 GET

*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

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 V4.0 – 2015/06/30.

Errata Published*	Description
2016/06/27	In Section 3.8.5, Message Processing Events and Sequencing Rules, changed the resource name from Proxy/RelyingPartyTrusts/{Identity}/PublishingSettings to Proxy/RelyingPartyTrusts/{Identity}/PublishedSettings. Changed the name of Section 3.8.5.1, Proxy/RelyingPartyTrusts/{Identifier}/PublishingSettings, to 3.8.5.1, Proxy/RelyingPartyTrusts/{Identifier}/PublishedSettings and changed references to "PublishingSetting" throughout the section to "PublishedSettings". In Section 3.8.5.1.2, DELETE, changed references to "PublishingSetting" throughout the section to "PublishedSettings". Changed the name of Section 3.9.5.1, Proxy/RelyingPartyTrusts/{Identifier}/PublishingSettings to 3.9.5.1, Proxy/RelyingPartyTrusts/{Identifier}/PublishedingSettings.
2016/06/27	In multiple sections, added or updated descriptions about client TLS authentication. In Section 3.3.5, Message Processing Events and Sequencing Rules, changed from: In all operations where the server requires authenticating the proxy using client TLS authentication [RFC2246], the proxy MUST present the certificate on [Proxy Service State Data].TrustCertificate during client TLS authentication. Changed to: In all operations where the server requires authenticating the proxy using client TLS authentication [RFC2246], the proxy MUST present the certificate on [Client State].TrustCertificate during client TLS authentication. In Section 3.4.5, Message Processing Events and Sequencing Rules, included the following paragraph at the end of the section: For all operations in this section, the server requires authenticating the proxy using client TLS authentication [RFC2246]. The server MUST validate that the certificate that is presented by the proxy during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated, the server MUST return an HTTP error code of 401. In Section 3.4.5.1.1, GET, removed the following paragraph because the content is specified in

Errata Published*	Description
	the parent section 3.4.5, Message Processing Events and Sequencing Rules: The request MUST authenticate using client TLS authentication [RFC2246]. The server MUST validate that the certificate presented by the client during client TLS authentication [RFC2246] can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated the server MUST return a HTTP error code of 400. In Section 3.4.5.2.1, GET, removed the following paragraph because the content is specified in the parent section 3.4.5, Message Processing Events and Sequencing Rules: The request MUST authenticate using client TLS authentication [RFC2246]. The server MUST validate that the certificate presented by the client during client TLS authentication [RFC2246] can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated the server MUST return a HTTP error code of 401. In Section 3.4.5.3.1, GET, removed the following paragraph because the content is specified in the parent section 3.4.5, Message Processing Events and Sequencing Rules: The request MUST authenticate using client TLS authentication [RFC2246]. The server MUST validate that the certificate presented by the client during client TLS authentication [RFC2246] can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated the server MUST return a HTTP error code of 401. In Section 3.5.5, Message Processing Events and Sequencing Rules, changed from: In all operations where the server requires authenticating the client using client TLS authentication [RFC2246], the client MUST do client TLS authentication [RFC2246] using the certificate in [Proxy Service State Data].TrustCertificate. Changed to: For all operations in this section, the client MUST perform client TLS authentication [RFC2246] using the certificate in [Client State].TrustCertificate. In Section 3.6.5, Message Processing Events and Sequencing Rules, changed from: In all operations where the server requires authenticating the proxy using client TLS authentication [RFC2246], the server MUST validate that the certificate presented by the proxy during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated, the server MUST return a HTTP error code of 401. Changed to: For all operations in this section, the server requires authenticating the proxy using client TLS authentication [RFC2246]. The server MUST validate that the certificate that is presented by the proxy during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated, the server MUST return an HTTP error code of 401. In Section 3.7.5, Message Processing Events and Sequencing Rules, included the following paragraph at the beginning of the section: For all operations in this section, the client MUST perform client TLS authentication [RFC2246] using the certificate in [Client State].TrustCertificate.

Errata Published*	Description
	In Section 3.8.5, Message Processing Events and Sequencing Rules, changed from: In all operations where the server requires authenticating the proxy using client TLS authentication [RFC2246], the server MUST validate that the certificate presented by the proxy during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated the server MUST return a HTTP error code of 401. Changed to: For all operations in this section, the server requires authenticating the proxy using client TLS authentication [RFC2246]. The server MUST validate that the certificate that is presented by the proxy during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated, the server MUST return an HTTP error code of 401. In Section 3.9.5, Message Processing Events and Sequencing Rules, changed from: In all operations where the server requires authenticating the client using client TLS authentication [RFC2246], the client MUST use the certificate represented by [Proxy Service State Data].TrustCertificate during client TLS authentication. Changed to: In all operations where the server requires authenticating the client using client TLS authentication [RFC2246], the client MUST perform client TLS authentication [RFC2246] using the certificate in [Client State].TrustCertificate. In Section 3.10.5, Message Processing Events and Sequencing Rules, changed from: In all operations where the server requires authenticating the proxy using client TLS authentication [RFC2246], the server MUST validate that the certificate presented by the client during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated the server MUST return a HTTP error code of 401. Changed to: For all operations in this section, the server requires authenticating the proxy using client TLS authentication [RFC2246]. The server MUST validate that the certificate that is presented by the client during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated, the server MUST return an HTTP error code of 401. Section 3.12.5.1.5, Proxy Preauthentication for Active Clients, included the following paragraph at the end of the section: For this operation, the server requires authenticating the proxy using client TLS authentication [RFC2246]. The server MUST validate that the certificate that is presented by the proxy during client TLS authentication can be validated by one of the values of [Server State].ProxyTrustedCertificates. If the certificate cannot be validated, the server MUST return an HTTP error code of 401. In Section 3.13.5.2.3, Response to Active Requests, included the following paragraph about client TLS authentication: The proxy MUST perform client TLS authentication [RFC2246] using the certificate in [Client

Errata Published*	Description
	State].TrustCertificate.
2016/05/31	In several sections, revised quotation marks around values in the JSON definitions for complex types to accurately represent data types. In Section 2.2.2.4, Configuration, changed from: `{ "ServiceConfiguration" : { "ServiceHostName" : "<service-host-name>", "HttpPort" : "<http-port-number>", "HttpsPort" : "<https-port-number >", "HttpsPortForUserTlsAuth" : "<user-TLS-port-number>", "DeviceCertificateIssuers" : ["<device-certificate-issuer>", *], "ProxyTrustCertificateLifetime" : "<trust-renewal-interval>", "DiscoveredUpnSuffixes" : ["<upn-suffix>", *], "CustomUpnSuffixes" : ["<upn-suffix>", *] }, "EndpointConfiguration" : [{ "Path" : "<endpoint-uri>", "PortType" : "<port-type>", "AuthenticationSchemes" : "<credential-collection-scheme>", "ClientCertificateQueryMode" : "<tls-query-behavior>", "CertificateValidation" : "<certificate-validation>", "SupportsNtlm" : "<support-ntlm>", "ServicePath" : "<service-endpoint-uri>", "ServicePortType" : "<service-port-type>" }, *] }`  Changed to:  `{ "ServiceConfiguration" : { "ServiceHostName" : "<service-host-name>", "HttpPort" : <http-port-number>, "HttpsPort" : <https-port-number >, "HttpsPortForUserTlsAuth" : <user-TLS-port-number>, "DeviceCertificateIssuers" : ["<device-certificate-issuer>", *], "ProxyTrustCertificateLifetime" : <trust-renewal-interval>, "DiscoveredUpnSuffixes" : ["<upn-suffix>", *], "CustomUpnSuffixes" : ["<upn-suffix>", *] }, "EndpointConfiguration" : [{ "Path" : "<endpoint-uri>", "PortType" : "<port-type>", "AuthenticationSchemes" : "<credential-collection-scheme>", "ClientCertificateQueryMode" : "<tls-query-behavior>", "CertificateValidation" : "<certificate-validation>",`

Errata Published*	Description

	"SupportsNtlm" : "<support-ntlm>",
	"ServicePath" : "<service-endpoint-uri>",
	"ServicePortType" : "<service-port-type>"
	}, *
	]
	}
	
	In Section 2.2.2.5, Relying Party Trust List, changed from:
	
	[{
	"objectIdentifier" : "<object-identifier>",
	"name" : "<web-application-name>",
	"publishedThroughProxy" : "<is-web-application-published>",
	"nonClaimsAware" : "<is-a-non-claims-aware-web-application>",
	"enabled" : "<is-web-application-enabled>"
	}, +]
	
	Changed to:
	
	[{
	"objectIdentifier" : "<object-identifier>",
	"name" : "<web-application-name>",
	"publishedThroughProxy" : <is-web-application-published>,
	"nonClaimsAware" : <is-a-non-claims-aware-web-application>,
	"enabled" : <is-web-application-enabled>
	}, +]
	
	In Section 2.2.2.6, Relying Party Trust, changed from:
	
	{
	"objectIdentifier" : "<object-identifier>",
	"name" : "<web-application-name>",
	"publishedThroughProxy" : "<is-web-application-published>",
	"nonClaimsAware" : "<is-a-non-claims-aware-web-application>",
	"enabled" : "<is-web-application-enabled>",
	"identifiers" : [<web-application-identifier>, *],
	"proxyTrustedEndpoints" : [<web-application-at-proxy-endpoint-url>, *],
	"proxyEndpointMappings" :
	[{ "Key" = "<internal-url>", "Value" = "external-url" }, *]
	}
	
	…
	enabled: Boolean value specifying if the web application is enabled at the server.
	…
	
	Changed to:
	
	{
	"objectIdentifier" : "<object-identifier>",
	"name" : "<web-application-name>",
	"publishedThroughProxy" : <is-web-application-published>,
	"nonClaimsAware" : <is-a-non-claims-aware-web-application>,
	"enabled" : <is-web-application-enabled>,
	"identifiers" : [<web-application-identifier>, *],
	"proxyTrustedEndpoints" : [<web-application-at-proxy-endpoint-url>, *],

Errata Published*	Description

	"proxyEndpointMappings" :
	[{ "Key" = "<internal-url>", "Value" = "<external-url>" }, *]
	}
	
	…
	is-web-application-enabled: Boolean value specifying if the web application is enabled at the server.
	…
	
	In Section 2.2.2.9, Store Entry, changed from:
	
	{
	"key" : "<entry-key>",
	"version" : "<entry-version>",
	"value" : "<entry-value>"
	}
	
	Changed to:
	
	{
	"key" : "<entry-key>",
	"version" : <entry-version>,
	"value" : "<entry-value>"
	}
	
	In Section 2.2.2.11, Serialized Request with Certificate, changed from:
	
	{
	"Request" :
	{
	"AcceptTypes" : ["<accept-type>", *],
	"Content" : [<byte>, *],
	"ContentEncoding" : "<content-encoding>",
	"ContentLength" : "<content-length>",
	"ContentType" : "<content-type>",
	"Cookies" :
	[{
	"Name" : "<cookie-name>",
	"Value" : "<cookie-value>",
	"Path" : "<cookie-path>",
	"Domain" : "<cookie-domain>",
	"Expires" : "<cookie-expires>",
	"Version" : "<cookie-version>",
	}, *],
	"Headers" :
	[{ "Name" : "<header-name>", "Value" : "<header-value>" }, *],
	"HttpMethod" : "<http-method>",
	"RequestUri" : "<request-uri>",
	"QueryString" : [{ "Name" : "<query-param>", "Value" : "<query-value>" }, *],
	"UserAgent" : "<user-agent>",
	"UserHostAddress" : "<user-host-address>",
	"UserHostName" : "<user-host-name>",
	"UserLanguages" : ["<user-language>", *]
	},
	"SerializedClientCertificate" : "<serialized-client-certificate>",
	"CertificateUsage" : "<certificate-usage>",

Errata Published*	Description

	}
	
	Changed to:
	
	{
	"Request" :
	{
	"AcceptTypes" : ["<accept-type>", *],
	"Content" : [<byte>, *],
	"ContentEncoding" : "<content-encoding>",
	"ContentLength" : <content-length>,
	"ContentType" : "<content-type>",
	"Cookies" :
	[{
	"Name" : "<cookie-name>",
	"Value" : "<cookie-value>",
	"Path" : "<cookie-path>",
	"Domain" : "<cookie-domain>",
	"Expires" : <cookie-expires>,
	"Version" : <cookie-version>,
	}, *],
	"Headers" :
	[{ "Name" : "<header-name>", "Value" : "<header-value>" }, *],
	"HttpMethod" : "<http-method>",
	"RequestUri" : "<request-uri>",
	"QueryString" : [{ "Name" : "<query-param>", "Value" : "<query-value>" }, *],
	"UserAgent" : "<user-agent>",
	"UserHostAddress" : "<user-host-address>",
	"UserHostName" : "<user-host-name>",
	"UserLanguages" : ["<user-language>", *]
	},
	"SerializedClientCertificate" : "<serialized-client-certificate>",
	"CertificateUsage" : "<certificate-usage>",
	}
	
	In Section 2.2.2.17, Proxy Token, changed from:
	
	{
	"ver" : "<version>",
	"aud" : "<audience>",
	"iat" : "<issued-at>",
	"exp" : "<expire>",
	"iss" : "<issuer>",
	"relyingpartytrustid" : "<rp-trust-id>",
	"deviceregid" : "<device-registration-id>",
	"authinstant" : "<auth-instant>",
	"authmethod" : "<auth-method>",
	"upn" : "<upn>"
	}
	
	Changed to:
	
	{
	"ver" : "<version>",
	"aud" : "<audience>",
	"iat" : <issued-at>,
	"exp" : <expire>,

Errata Published*	Description

	"iss" : "<issuer>",
	"relyingpartytrustid" : "<rp-trust-id>",
	"deviceregid" : "<device-registration-id>",
	"authinstant" : <auth-instant>,
	"authmethod" : "<auth-method>",
	"upn" : "<upn>"
	}
	
	In Section 2.2.2.21, Error Response, changed from:
	
	{
	"id" : "<error-id>",
	"message" : "<message>",
	"type" : "<type>",
	}
	
	Changed to:
	
	{
	"id" : <error-id>,
	"message" : "<message>",
	"type" : "<type>",
	}
	
	In Section 3.1.1.3, Relying Party Trust State, changed from:
	
	{
	"RelyingPartyTrust" : "<web-application>",
	"RedirectBasedPreauth" : "<redirect-based-preauth>"
	}
	
	Changed to:
	
	{
	"RelyingPartyTrust" : "<web-application>",
	"RedirectBasedPreauth" : <redirect-based-preauth>
	}
	
	In Section 6, Appendix A: Full JSON Schema, changed from:
	…
	
	{
	"title" : "Configuration",
	"type" : "object",
	"properties" :
	{
	"ServiceConfiguration" :
	{
	"type" : "object",
	"properties" :
	{
	"ServiceHostName" : {"type" : "string"},

Errata Published*	Description

	"HttpPort" : {"type" : "integer"},
	"HttpsPort" : {"type" : "integer"},
	"HttpsPortForUserTlsAuth" : {"type" : "integer"},
	"DeviceCertificateIssuers" :
	{
	"type" : "array",
	"items" : {"type" : "string"}
	},
	"ProxyTrustCertificateLifetime" : {"type" : "integer"}
	}
	},
	"EndpointConfiguration" :
	
	…
	
	Changed to:
	…
	
	{
	"title" : "Configuration",
	"type" : "object",
	"properties" :
	{
	"ServiceConfiguration" :
	{
	"type" : "object",
	"properties" :
	{
	"ServiceHostName" : {"type" : "string"},
	"HttpPort" : {"type" : "integer"},
	"HttpsPort" : {"type" : "integer"},
	"HttpsPortForUserTlsAuth" : {"type" : "integer"},
	"DeviceCertificateIssuers" :
	{
	"type" : "array",
	"items" : {"type" : "string"}
	},
	"ProxyTrustCertificateLifetime" : {"type" : "integer"},
	"DiscoveredUpnSuffixes" :
	{
	"type" : "array",
	"items" : {"type" : "string"}
	}
	"CustomUpnSuffixes" :
	{
	"type" : "array",
	"items" : {"type" : "string"}
	}
	}
	},
	"EndpointConfiguration" :
	
	…

2016/05/16	In Section 2.2.2.15, Certificate Validation, updated the values for the Certificate Validation enumeration. Changed from: … { "None" "User"

Errata Published*	Description

	"Device"
	}
	…
	
	Changed to:
	
	…
	{
	"None"
	"Ssl"
	"IssuedByDrs"
	}
	…
	
	In Section 6, Appendix A: Full JSON Schema, updated values for the CurrentEndpointConfiguration.CertificateValidation enumeration.
	
	Changed from:
	
	…
	"CertificateValidation" :
	{
	"enum" : ["None", "User", "Device"]
	},
	…
	
	Changed to:
	
	…
	"CertificateValidation" :
	{
	"enum" : ["None", "Ssl", "IssuedByDrs"]
	},
	
	…

2016/05/02	In Section 2.2.2.11, Serialized Request with Certificate, added details to clarify the purpose of the serialized request contained by this object. Changed from: … This is a JSON object containing a serialized request plus a serialized client certificate and its usage. The format of the object is as follows: … Changed to: … This is a JSON object containing a serialized HTTP request that is intended for the target service, plus a serialized client certificate and its usage. The format of the object is as follows: …
2016/04/18	In Section 3.6.5.2.4, DELETE, revised the description to call out the correct operation and behavior.

Errata Published*	Description
	Changed from: This operation modifies the value of an existing entry in the store. The operation is transported by a HTTP PUT and can be invoked through the following URIs: … Changed to: This operation removes the value of an existing entry in the store. The operation is transported by an HTTP DELETE and can be invoked through the following URIs: …

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

Errata Published*	Description
2016/05/16	In Section 3.1.4.1.1.3, GetFsTrustInformationSoapOut, updated the namespace for the guid element/type in the VersionInformation complex type from tns to s1. Changed from: … <s:complexType name="VersionInformation"> <s:sequence> <s:element minOccurs="1" maxOccurs="1" name="SoftwareVersion" type="s:long" /> <s:element minOccurs="1" maxOccurs="1" name="Guid" type="tns:guid" /> <s:element minOccurs="1" maxOccurs="1" name="Version" type="s:long" /> </s:sequence> </s:complexType> … Changed to: … <s:complexType name="VersionInformation"> <s:sequence> <s:element minOccurs="1" maxOccurs="1" name="SoftwareVersion" type="s:long" /> <s:element minOccurs="1" maxOccurs="1" name="Guid" type="s1:guid" /> <s:element minOccurs="1" maxOccurs="1" name="Version" type="s:long" /> </s:sequence> </s:complexType> … In Section 3.1.4.3.1.3 GetClaimsSoapOut, updated the namespace for the guid type of the uuid attribute in the TrustPolicyEntryBase complex type from tns to s1. Changed from: … <s:complexType name="TrustPolicyEntryBase"> <s:attribute name="uuid" type="tns:guid" use="required" /> <s:attribute name="Disabled" type="s:boolean" use="required" /> </s:complexType> …

Errata Published*	Description
	Changed to: … <s:complexType name="TrustPolicyEntryBase"> <s:attribute name="uuid" type="s1:guid" use="required" /> <s:attribute name="Disabled" type="s:boolean" use="required" /> </s:complexType> …

*Date format: YYYY/MM/DD

[MS-ADSC]: Active Directory Schema Classes

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-ADTS]: Active Directory Technical Specification

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V42.0 – 2015/10/16.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2016/06/27</td><td>In Section 6.1.6.7.9, trustAttributes, added a reference to KB article 3155495 for Windows Server 2012 R2.

Changed from:
<table><tr><th>Name and value</th><th>Description and restrictions/special notes</th></tr><tr><td>…</td><td>…</td></tr><tr><td>TAPT (TRUST_ATTRIBUTE_PIM_TRUST) 0x00000400</td><td>Evaluated only on Windows Server 2016</td></tr></table>
Changed to:
<table><tr><th>Name and value</th><th>Description and restrictions/special notes</th></tr><tr><td>…</td><td>…</td></tr><tr><td>TAPT (TRUST_ATTRIBUTE_PIM_TRUST) 0x00000400</td><td>Evaluated on Windows Server 2012 R2 only with [MSKB-3155495] installed. Also evaluated on Windows Server 2016.</td></tr></table></td></tr>
<tr><td>2016/04/18</td><td>In several sections, removed references to [MSASRT] in favor of [MS-UCODEREF].

In Section 1.2.1, Normative References, removed the reference for [MSASRT].

In Section 6.5.1, String Comparison by Using Sort Keys, removed the reference for [MSASRT] in the first sentence.

Changed from:
To compare strings, the implementer needs to get a "sort key" for each string (see [MSASRT]). A binary comparison of the sort keys can then be used to arrange the strings in any desired order.
…</td></tr>
</table>

Errata Published*	Description
	Changed to: To compare strings, the implementer needs to get a "sort key" for each string. A binary comparison of the sort keys can then be used to arrange the strings in any desired order. …
2016/02/22	In Section 3.1.1.3.2.40, spnRegistrationResult, updated the description of the value for spnRegistrationResult for various Windows versions. Changed from: When running as AD DS, this value is 0. When running as AD LDS, if the DC was unable to register its service principal names (SPNs) ([MS-DRSR] section 2.2.2), this attribute returns the Windows error code associated with the failure. Otherwise, it returns zero. Note When running as AD DS on Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 Technical Preview, this value is 21. Changed to: When running as AD DS on Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016 Technical Preview, this value is 0. When running as AD LDS, if the DC was unable to register its service principal names (SPNs) ([MS-DRSR] section 2.2.2), this attribute returns the Windows error code associated with the failure. Otherwise, it returns zero. Note When running as AD DS on Windows Server 2003 or Windows Server 2008, this value is the Windows error code that is associated with the failure if the DC was unable to register its service principal names (SPNs), or zero upon success.
2016/02/08	In Section 3.1.1.12.1.7, DomainDescriptionElements, corrected the element names Inter**D**omainTrustAccounts and Inter**D**omainTrustAccountDescription to Inter**d**omainTrustAccounts and Inter**d**omainTrustAccountDescription.

2016/01/25	In Section 3.1.1.3.4.1.6, LDAP_SERVER_GET_STATS_OID, moved the tag values from before the type to after the type in the CHOICE encoding to align with the ASN standard.
	
	Changed from:
	
	`StatsResponseValueV4 ::= SEQUENCE OF SEQUENCE {`
	`  statisticName  OCTET STRING`
	`  CHOICE {`
	`  [0] intStatistic  INTEGER`
	`  [1] stringStatistic  OCTET STRING`
	`  }`
	`}`
	
	Changed to:
	
	`StatsResponseValueV4 ::= SEQUENCE OF SEQUENCE {`
	`  statisticName  OCTET STRING`
	`  CHOICE {`
	`  intStatistic [0]  INTEGER`
	`  stringStatistic [1]  OCTET STRING`
	`  }`
	`}`

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2016/01/25</td><td>
In two sections, updated the minimum required forest revisions and domain revisions for installed and upgraded DCs.

In Section 3.1.1.10.1, Forest Revision, changed from:

<table>
<tr><th>DC functional level</th><th>Minimum required forest revision</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>DS_BEHAVIOR_WIN2008</td><td>2.9</td></tr>
<tr><td>DS_BEHAVIOR_WIN2008R2</td><td>5.9</td></tr>
<tr><td>DS_BEHAVIOR_WIN2012</td><td>10.9</td></tr>
<tr><td>DS_BEHAVIOR_WIN2012R2</td><td>12.10</td></tr>
</table>

Changed to:
<table>
<tr><th>DC functional level</th><th>Minimum required forest revision</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>DS_BEHAVIOR_WIN2008</td><td>2.10</td></tr>
<tr><td>DS_BEHAVIOR_WIN2008R2</td><td>5.10</td></tr>
<tr><td>DS_BEHAVIOR_WIN2012</td><td>11.10</td></tr>
<tr><td>DS_BEHAVIOR_WIN2012R2</td><td>15.10</td></tr>
</table>

Note The preceding table specifies the minimum required forest revisions for the case of a freshly-installed DC. In the case of a DC that has been upgraded from an older version of Windows Server, some of the minimum required forest revisions are different, depending on the DC functional level. These differences are shown in the following table.

<table>
<tr><th>DC functional level,</th><th>Minimum required forest revision</th></tr>
<tr><td>DS_BEHAVIOR_WIN2008,</td><td>2.9</td></tr>
<tr><td>DS_BEHAVIOR_WIN2008R2,</td><td>5.9</td></tr>
<tr><td>DS_BEHAVIOR_WIN2012,</td><td>11.9</td></tr>
<tr><td>DS_BEHAVIOR_WIN2012R2,</td><td>15.9</td></tr>
</table>

In Section 3.1.1.10.3, Domain Revision, changed from:

<table>
<tr><th>DC functional level</th><th>Minimum required forest revision</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>DS_BEHAVIOR_WIN2008</td><td>3.8</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>DS_BEHAVIOR_WIN2008R2</td><td>5.8</td></tr>
<tr><td>DS_BEHAVIOR_WIN2012</td><td>8.8</td></tr>
<tr><td>DS_BEHAVIOR_WINTHRESHOLD</td><td>14.9</td></tr>
</table>
Changed to:
<table>
<tr><th>DC functional level</th><th>Minimum required forest revision</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>DS_BEHAVIOR_WIN2008</td><td>3.9</td></tr>
<tr><td>DS_BEHAVIOR_WIN2008R2</td><td>5.9</td></tr>
<tr><td>DS_BEHAVIOR_WIN2012</td><td>9.9</td></tr>
<tr><td>DS_BEHAVIOR_WINTHRESHOLD</td><td>15.9</td></tr>
</table>
Note The preceding table specifies the minimum required domain revisions for the case of a freshly-installed DC. In the case of a DC that has been upgraded from an older version of Windows Server, some of the minimum required domain revisions are different, depending on the DC functional level. These differences are shown in the following table.
<table>
<tr><th>DC functional level</th><th>Minimum required domain revision</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>DS_BEHAVIOR_WIN2008</td><td>3.8</td></tr>
<tr><td>DS_BEHAVIOR_WIN2008R2</td><td>5.8</td></tr>
<tr><td>DS_BEHAVIOR_WIN2012</td><td>9.8</td></tr>
<tr><td>DS_BEHAVIOR_WIN2012R2</td><td>10.8</td></tr>
</table>
</td></tr>
<tr><td>2016/01/25</td><td>
Added two new sections to discuss the mapping between the values in LDAP and the valid values for client/server/service principal names.
New Section 3.1.1.13.6, GetUserLogonInfoByAttribute:
<pre>
procedure GetUserLogonInfoByAttribute(
SearchKey: unicodestring,
Attribute: ATTRTYP,
ExpandedSids: ARRAY(SID),
MaxValidityTimeHint: LARGE_INTEGER) : NTSTATUS
</pre>
SearchKey: The principal whose logon information is to be retrieved.
Attribute: The attribute to use when searching for the principal.
ExpandedSids: Returns the set of expanded SIDs.
MaxValidityTimeHint: Returns a future timestamp that specifies when the returned results are no longer considered valid; a value of zero signifies that no hint is being returned.
Return Values: This procedure returns STATUS_SUCCESS ([MS-ERREF] section 2.3.1) to indicate success; otherwise, an NTSTATUS error code.
</td></tr>
</table>

Errata Published*	Description

	Note This procedure uses the pseudocode language defined in [MS-DRSR] section 3.4, and other functions defined in [MS-DRSR] section 4.1.4.2.
	Logical Processing:
	`Status: NTSTATUS;`
	`Names: set of DSName`
	`/* Look for user account */`
	`Names := LookupAttr(0, Attribute, SearchKey)`
	`if Names == null`
	`return STATUS_NO_SUCH_USER`
	`endif`
	`/* Ensure uniqueness */`
	`if number(Names) != 1`
	`return STATUS NO SUCH USER`
	`endif`
	`Status = GetUserLogonInfo(`
	`Names[0],`
	`ExpandedSids,`
	`MaxValidityTimeHint);`
	`return Status;`
	
	New Section 3.1.1.13.7, GetUserLogonInfoByUPNOrAccountName:
	
	`procedure GetUserLogonInfoByUPNOrAccountName(`
	`UPNOrName: unicodestring,`
	`ExpandedSids: ARRAY(SID),`
	`MaxValidityTimeHint: LARGE_INTEGER) : NTSTATUS`
	
	UPNOrName: The principal whose logon information is to be retrieved.
	ExpandedSids: Returns the set of expanded SIDs.
	MaxValidityTimeHint: Returns a future timestamp that specifies when the returned results are no longer considered valid; a value of zero signifies that no hint is being returned.
	Return Values: This procedure returns STATUS_SUCCESS ([MS-ERREF] section 2.3.1) to indicate success; otherwise, an NTSTATUS error code.
	Note This procedure uses functions defined in [MS-DRSR] section 4.1.4.2.
	Logical Processing:
	`Status: NTSTATUS;`
	`UserName: unicodestring`
	`/* Search on the userPrincipalName attribute first */`
	`Status := GetUserLogonInfoByAttribute(`
	`UPNOrName,`
	`userPrincipalName,`
	`ExpandedSids,`
	`MaxValidityTimeHint);`
	`if Status == STATUS SUCCESS`
	`return Status;`
	`endif`
	`/* Search on the sAMAccountName attribute next */`
	`Status := GetUserLogonInfoByAttribute(`
	`UPNOrName,`

Errata Published*	Description
	sAMAccountName, ExpandedSids, MaxValidityTimeHint); if Status == STATUS_SUCCESS return Status; endif /* Parse the input for the user name and search on that */ UserName := UserNameFromUPN(UPNOrName); if UserName != null Status := GetUserLogonInfoByAttribute(UserName, sAMAccountName, ExpandedSids, MaxValidityTimeHint); if Status == STATUS_SUCCESS return Status; endif endif return STATUS_NO_SUCH_USER;
2016/01/25	In Section 3.1.1.3.4.1.6, LDAP_SERVER_GET_STATS_OID, corrected the name of a field. Changed from: If the client does not have the SE_DEBUG_PRIVILEGE, a Windows 2000 DC MUST return the value 0 for the suboperations field of this structure. Changed to: If the client does not have the SE_DEBUG_PRIVILEGE, a Windows 2000 DC MUST return the value 0 for the searchSubOperations field of this structure.
2016/01/11	In Section 6.1.1.2.2.2.1, Subnet Object, added that the subnet name for an IPv6 subnet must be in compact format so that no two strings can refer to the same subnet and clarified that 'leading zeroes' refers to the additional zeroes used to fill out the field and that subnet strings are case-insensitive. Changed from: 1. There is only one occurrence of the character "/" in s. Let i be the index of the character "/" in s. 2. The substring s[0, i-1] does not have any leading zeros and is either a valid IPv4 address in dotted decimal notation (as specified in [RFC1166]) or a valid IPv6 address in colon-hexadecimal form or compressed form (as specified in [RFC4291]). Let b be the binary representation of the address in little-endian format. 3. …. Changed to: 1. There is only one occurrence of the character "/" in s. Let i be the index of the character "/" in s. 2. The substring s[0, i-1] is either a valid IPv4 address in dotted decimal notation (as specified in [RFC1166]) or a valid IPv6 address in colon-hexadecimal form or compressed form (as specified in [RFC4291]), and must meet the following constraints: ▪ IPv4 addresses must not have any leading zeros in any individual component of the address.

Errata Published*	Description
	▪ IPv6 addresses must be in canonical text representation format (as specified in [RFC5952] section 4), except that the addresses are treated as case insensitive. Examples: Valid IPv4 subnet names: ▪ 10.2.1.0/24 ▪ 10.20.1.0/24 Invalid IPv4 subnet names: ▪ 10.02.0.0/16 Valid IPv6 subnet names: ▪ A:A:A:A::/64 ▪ a:b::c:d:0:0/64 ▪ 0:0:e0::/48 ▪ A:b:C::/128 ▪ A:B::F:0/128 ▪ 12AB:0:0:CD30::/60 ▪ A:a:e:b:0:d:e:f/128 Invalid IPv6 subnet names: ▪ A:B:0C:D::/64 ▪ A:B:0:0:0:0:E:F/128 ▪ 12AB::CD30:0:0:0:0/60 ▪ 12AB:0:0:CD30::F:0/60 ▪ A:a:e:b::d:e:f/128 Let b be the binary representation of the address in little-endian format. … 3. …

*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

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V25.0 – 2015/10/16.

Errata Published*	Description
2016/06/27	In Section 3.10.4.1, New Connection Initiated, updated the product behavior note to include all the relevant products. Changed from: If the IsAuthenticatedFirewallConnection flag is set to TRUE in the connection state table entry corresponding to the connection, the first packet of every new connection (that is, the first packet sent by the connection initiator after creating the new entry in the connection state table) MUST be sent twice: initially with IPSec encapsulation and then again without IPSec encapsulation. These messages are known as the ESP SYN and cleartext SYN messages, respectively.<22> <22> Section 3.10.4.1: It is possible for the cleartext SYN message to be received before the ESP SYN message. If this scenario occurs, a common practice for the server is to drop both messages, after which the client must attempt to reconnect. This reconnection attempt will delay a connection by approximately three seconds. For inbound TCP connections where NAT-T is not enabled, Windows can be configured to decrypt the ESP SYN message and send it up the stack as if it were the cleartext SYN message. By taking this action, the client is not required to reconnect. Windows Server 2012 R2 with [MSKB-3023555] and all subsequent versions of Windows according to the applicability list at the beginning of this section support this behavior. Changed to: If the IsAuthenticatedFirewallConnection flag is set to TRUE in the connection state table entry corresponding to the connection, the first packet of every new connection (that is, the first packet sent by the connection initiator after creating the new entry in the connection state table) MUST be sent twice: initially with IPSec encapsulation and then again without IPSec encapsulation. These messages are known as the ESP SYN and cleartext SYN messages, respectively.<22> <22> Section 3.10.4.1: It is possible for the cleartext SYN message to be received before the ESP SYN message. If this scenario occurs, a common practice for the server is to drop both messages, after which the client must attempt to reconnect. This reconnection attempt will delay a connection by approximately three seconds. For inbound TCP connections where NAT-T is not enabled, Windows can be configured to decrypt the ESP SYN message and send it up the stack as if it were the cleartext SYN message. By taking this action, the client is not required to reconnect. Windows 8.1 and Windows Server 2012 R2 that have [MSKB-3023555], as well as Windows 10 and Windows Server 2016 support this behavior."

*Date format: YYYY/MM/DD

[MS-APDS]: Authentication Protocol Domain Support

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-AZOD]: Authorization Protocols Overview

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-BKRP]: BackupKey Remote Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V31.0 – 2015/10/16.

Errata Published*	Description
2016/03/21	In Section 2.2.3.37, SR_RESOURCE_TYPE_ELIGIBLE_DISKS_RESULT, corrected the field name DiskGuild to DiskGuid. Changed from: DiskGuild (variable): An array of GUID structures, as specified in [MS-DTYP] section 2.3.4.2, each containing the resource ID of a storage class resource. Changed to: DiskGuid (variable): An array of GUID structures, as specified in [MS-DTYP] section 2.3.4.2, each containing the resource ID of a storage class resource.
2015/10/26	In Section 2.2.3.38, SR_RESOURCE_TYPE_QUERY_ELIGIBLE_TARGET_DATADISKS, added the following fields: Reserved1 (1 byte): This field MUST be ignored. Reserved2 (1 byte): This field MUST be ignored. In Section 2.2.3.39, SR_RESOURCE_TYPE_QUERY_ELIGIBLE_SOURCE_DATADISKS, added the following fields: Reserved1 (1 byte): This field MUST be ignored. Reserved2 (1 byte): This field MUST be ignored. Reserved3 (1 byte): This field MUST be ignored.
2015/10/26	In Section 2.2.3.39, SR_RESOURCE_TYPE_QUERY_ELIGIBLE_SOURCE_DATADISKS, corrected all instances of SR_RESOURCE_TYPE_ELIGIBLE_SOURCE_DATADISKS to SR_RESOURCE_TYPE_QUERY_ELIGIBLE_SOURCE_DATADISKS.

*Date format: YYYY/MM/DD

[MS-CSRA]: Certificate Services Remote Administration Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V4.0 – 2015/10/16.

Errata Published*	Description
2016/03/07	In Section 3.1.4.1.18, ICertAdminD::BackupPrepare (Opnum 20), revised the description for pwszBackupAnnotation. Changed from: pwszBackupAnnotation: Not Used. MUST be empty string (L""). MUST be ignored on receipt. Changed to: pwszBackupAnnotation: Not Used. Can be set to any arbitrary value, and MUST be ignored on receipt.
2016/03/07	In Section 2.2.5, Common Error Codes, obsolete errors codes, 0x80004003 and 0xc800020D, were removed from the error code table. Changed from:

Return value/code	Description
0x80070057 ERROR_INVALID_PARAMETER	The parameter is incorrect.
0x80070006 ERROR_INVALID_HANDLE	The handle is invalid.
0x8000FFFF ERROR_UNEXPECTED_ERROR	An unexpected error occurred.
0x80004003 ERROR_INVALID_POINTER	An invalid pointer.
0x80071392 ERROR_OBJECT_EXISTS	An object already exists.
0x00000001 ERROR_ARITHMETIC_OVERFLOW	Arithmetic overflow.
0xc800020D	An invalid backup sequence.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>ERROR_INVALID_BACKUP_SEQUENCE</td><td></td></tr>
<tr><td>0xc800042D
ERROR_OUT_OF_MEMORY</td><td>Out of memory.</td></tr>
</table>

Changed to:
<table>
<tr><th>Return value/code</th><th>Description</th></tr>
<tr><td>0x80070057
ERROR_INVALID_PARAMETER</td><td>The parameter is incorrect.</td></tr>
<tr><td>0x80070006
ERROR_INVALID_HANDLE</td><td>The handle is invalid.</td></tr>
<tr><td>0x8000FFFF
ERROR_UNEXPECTED_ERROR</td><td>An unexpected error occurred.</td></tr>
<tr><td>0x80071392
ERROR_OBJECT_EXISTS</td><td>An object already exists.</td></tr>
<tr><td>0x00000001
ERROR_ARITHMETIC_OVERFLOW</td><td>Arithmetic overflow.</td></tr>
<tr><td>0xc800042D
ERROR_OUT_OF_MEMORY</td><td>Out of memory.</td></tr>
</table>
</td></tr>
<tr><td>2016/01/25</td><td>In various sections, revised an incorrect field length from a variable to a long - 4 bytes, corrected the description in the Officer and Enrollment Agent Access Rights section, and corrected the AccessMask description along with the field descriptions for Array of SIDs and TemplateName.

In Section 2.2.1.7.1, CERTTRANSDBCOLUMN Marshaling Format, changed from:

Column_1_obwzDisplayName_Offset (variable): The offset from the beginning of the byte array buffer that is pointed to by the pb field in the containing CERTTRANSBLOB structure to where the string that contains the display name of this column can be found. The format is a null-terminated Unicode string. The offset MUST be divisible by 4. The offset value MUST be little-endian encoded.

Changed to:
Column_obwzDisplayName_Offset (4 bytes): The offset from the beginning of the byte array buffer that is pointed to by the pb field in the containing CERTTRANSBLOB structure to where the string that contains the display name of this column can be found. The format is a null-terminated Unicode string. The offset MUST be divisible by 4. The offset value MUST be little-endian encoded.

In Section 2.2.1.8.1, CERTTRANSDBATTRIBUTE Marshaling Format, changed from:

Attribute 1 obwzValue (variable): The offset from the beginning of the byte array buffer that is pointed to by the pb field in the containing CERTTRANSBLOB structure to where the string that contains the value of this attribute (1) can be found. The format is a null-terminated UNICODE string. The offset MUST be divisible by 4. The offset MUST be little-endian encoded.

Changed to:
Attribute obwzValue 4 bytes): The offset from the beginning of the byte array buffer that is pointed to by the pb field in the containing CERTTRANSBLOB structure to where the string that</td></tr>
</table>

Errata Published*	Description
	contains the value of this attribute (1) can be found. The format is a null-terminated UNICODE string. The offset MUST be divisible by 4. The offset MUST be little-endian encoded. In Section 2.2.1.9.1, CERTTRANSDBEXTENSION Marshaling Format, changed from: Extension_1_obValue (variable): The offset from the beginning of the byte array buffer that is pointed to by the pb field in the containing CERTTRANSBLOB structure to where the value for this extension can be found. The offset MUST be divisible by 4. The offset value MUST be little-endian encoded. Changed to: Extension_obValue (4 bytes): The offset from the beginning of the byte array buffer that is pointed to by the pb field in the containing CERTTRANSBLOB structure to where the value for this extension can be found. The offset MUST be divisible by 4. The offset value MUST be little-endian encoded. In Section 2.2.1.10.1, CERTTRANSDBRESULTCOLUMN Marshaling Format, changed from: Result_Column_1_cbValue (variable): The length of the data in Result Column 1the column referenced by obValue (offset). The length value MUST be little-endian encoded. Changed to: Result_Column_cbValue (4 bytes): The length of the data in Result Column 1the column referenced by obValue (offset). The length value MUST be little-endian encoded. In Section 2.2.1.11, Officer and Enrollment Agent Access Rights, changed from: Officer rights and Enrollment Agent rights are security descriptors. Security descriptor structures (SID structures) are defined in [MS-DTYP] section 2.4.2. Officer rights and Enrollment Agent rights security descriptors have the following properties: 1. Each access control entry (ACE) in the discretionary access control list (DACL) MUST have: 1. AceType 0x9 (ACCESS_ALLOWED_CALLBACK_ACE_TYPE) 2. AccessMask 0x0001000 … Array of SIDs (variable): An array of SID structures that identify either (i) principals for whom the officer can approve requests; or (ii) principals on whose behalf the enrollment agent can obtain certificates. For an Officer rights security descriptor, case (i) applies. For an Enrollment Agent rights security descriptor, case (ii) applies. SID structures are as defined in [MS-DTYP] section 2.4.2. TemplateName (variable): A little-endian encoded Unicode string that identifies the common name (CN) of the template (as defined in [MS-CRTD]) for which the officer is authorized to approve requests. Changed to: Officer rights and Enrollment Agent rights are security descriptors. Security descriptor structures are defined in [MS-DTYP] section 2.4.6 and can contain SID structures ([MS-DTYP] section 2.4.2). Officer rights and Enrollment Agent rights security descriptors have the following properties: 1. Each access control entry (ACE) in the discretionary access control list (DACL) MUST have: 1. AceType 0x9 (ACCESS_ALLOWED_CALLBACK_ACE_TYPE for the ACCESS_ALLOWED_CALLBACK_ACE, [MS-DTYP] section 2.4.4.6) 2. AccessMask 0x00010000 …

Errata Published*	Description
	Array of SIDs (variable): An array of SID structures marshaled in packet representation ([MS-DTYP] section 2.4.2.2) that identify either (i) principals (4) for whom the officer can approve requests; or (ii) principals (4) on whose behalf the enrollment agent can obtain certificates (1). For an Officer rights security descriptor, case (i) applies. For an Enrollment Agent rights security descriptor, case (ii) applies. TemplateName (variable): A little-endian encoded Unicode and null-terminated string that identifies the common name (CN) of the template (as defined in [MS-CRTD]) for which the officer is authorized to approve requests.

2015/11/23	In various sections, updated a member of the CERTTRANSDBRESULTROW structure and the parameter datatypes of some method declarations to match the IDL and removed the ENUM_CATYPES definition from the IDL because it is not referenced in this or any other specification.
	
	In Section 2.2.3, CERTTRANSDBRESULTROW, changed from:
	DWORD RowId;
	
	Changed to:
	DWORD rowid;
	
	In Section 3.1.4.1.13, ICertAdminD::EnumView (Opnum 15), changed from:
	
	[out, ref] CERTTRANSBLOB*& pctbResultRows
	
	Changed to:
	[out, ref] CERTTRANSBLOB* pctbResultRows
	
	In Section 3.1.4.1.18, ICertAdminD::BackupPrepare (Opnum 20), changed from:
	
	[in] const WCHAR* pwszBackupAnnotation,
	
	Changed to:
	[in] WCHAR const * pwszBackupAnnotation,
	
	In Section 6, Appendix A: Full IDL, removed the following:
	
	`typedef enum _ENUM_CATYPES`
	`{`
	`ENUM_ENTERPRISE_ROOTCA = 0x00000000,`
	`ENUM_ENTERPRISE_SUBCA = 0x00000001,`
	`ENUM_STANDALONE_ROOTCA = 0x00000003,`
	`ENUM_STANDALONE_SUBCA = 0x00000004`
	`} ENUM_CATYPES;`

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V12.0 – 2015/10/16.

Errata Published*	Description
2016/06/27	In Section 2.2.1, TSRequest, the authInfo field description has been changed from: authInfo: A TSCredentials structure, as defined in section 2.2.1.2, that contains the user's credentials that are delegated to the server. The authinfo field MUST be encrypted under the encryption key that is negotiated under the SPNEGO package. Changed to: authInfo: A TSCredentials structure, as defined in section 2.2.1.2, that contains the user's credentials that are delegated to the server. The authInfo field MUST be encrypted under the encryption key that is negotiated under the SPNEGO package. The authInfo field carries the message signature and then the encrypted data.

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V18.0 – 2015/10/16.

Errata Published*	Description
2016/06/27	In Section 1.7, Versioning and Capability Negotiation, the list of supported minor versions has been changed from: 1, 2, 3, 4, 6, or 7 Changed to: 1, 2, 4, 6, or 7 The list of unused minor versions has been changed from: 5 Changed to: 3 or 5

*Date format: YYYY/MM/DD

[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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V30.0 – 2015/10/16.

Errata Published*	Description
2016/06/27	In Section 3.1.4.1, R_DnssrvOperation (Opnum 0), changed the description for the ExpireZone operation to reflect current behavior. Changed from: Force expiration of the secondary zone pointed to by pszZone on the DNS server, by invalidating the zone data locally and contacting primary to refresh. For this operation pszZone MUST point to a secondary zone only. dwTypeId, and pData MUST be ignored by the server. Changed to: Force a refresh of the secondary zone pointed to by pszZone on the DNS server, from primary zone server. For this operation pszZone MUST point to a secondary zone only. dwTypeId and pData MUST be ignored by the server.
2016/01/25	In Section 2.2.16.2.1, DNS_RPC_RRL_PARAMS, corrected the names IPv4PrefixLength and PrefixLength to dwIPv4PrefixLength and dwIPv6PrefixLength. Changed from: dwResponsesPerSecond: The maximum number of responses a DNS server can give for each successful "unique response" in one-second intervals. A DNS response is considered a unique response if the combination of the following parameters is unique: the requestor's IP address, masked according to either IPv4PrefixLength or PrefixLength; an imputed domain name that is either a wildcard (if a wildcard match occurred), the zone name (if no match occurred), or the query name; and a Boolean error indicator (response code Refused, FormErr, or ServFail). Changed to: dwResponsesPerSecond: The maximum number of responses a DNS server can give for each successful "unique response" in one-second intervals. A DNS response is considered a unique response if the combination of the following parameters is unique: the requestor's IP address, masked according to either dwIPv4PrefixLength or dwIPv6PrefixLength; an imputed domain name that is either a wildcard (if a wildcard match occurred), the zone name (if no match occurred), or the query name; and a Boolean error indicator (response code Refused, FormErr, or ServFail).

Errata Published*	Description
2016/01/25	In Section 4.18, Getting Response Rate Limiting Settings, corrected the type name from DNSSRV_TYPEID_UNICODE_RRL to DNSSRV_TYPEID_RRL. Changed from: The DNS server returns ERROR_SUCCESS if the operation is successful or a Windows error code if the operation fails. If the operation is successful, pdwTypeOut SHOULD be of type DNSSRV_TYPEID_UNICODE_RRL, and ppDataOut SHOULD point to a structure of type PDNS_RPC_RRL_PARAMS. Changed to: The DNS server returns ERROR_SUCCESS if the operation is successful or a Windows error code if the operation fails. If the operation is successful, pdwTypeOut SHOULD be of type DNSSRV_TYPEID_ RRL, and ppDataOut SHOULD point to a structure of type PDNS_RPC_RRL_PARAMS.
2016/01/25	In Section 2.2.16.2.1, DNS_RPC_RRL_PARAMS, revised the description of dwWindowSize to refer to "dwTotalResponsesInWindow" instead of "Total Responses in Window". Changed from: dwWindowSize: The duration, in seconds, where the state of "Total Responses in Window" is maintained for each "unique response". See dwResponsesPerSecond for the definition of "unique response". After this duration, the value for "Total responses in Window" is reset to 0. The default value for this parameter is 5. The parameter can be set to any positive integer (see [RRL] section 2.2.4). Changed to: dwWindowSize: The duration, in seconds, where the state of dwTotalResponsesInWindow is maintained for each "unique response". See dwResponsesPerSecond for the definition of "unique response". After this duration, the value for dwTotalResponsesInWindow is reset to 0. The default value for this parameter is 5. The parameter can be set to any positive integer (see [RRL] section 2.2.4).
2016/01/25	In Section 2.2.16.2.1, DNS_RPC_RRL_PARAMS, in the description of dwResponsesPerSecond and dwErrorsPerSecond, changed FormErr to FormError. Changed from: dwErrorsPerSecond: The maximum number of responses a DNS server can give for queries resulting in error (ServFail, FormErr, Refused) in one-second intervals. This parameter can be set to any positive integer; the default value is 5. Changed to: dwErrorsPerSecond: The maximum number of responses a DNS server can give for queries resulting in error (ServFail, FormError, Refused) in one-second intervals. This parameter can be set to any positive integer; the default value is 5.
2015/12/11	In Section 2.2.12.2.6, DNSSRV_ZONE_RRL_STATS, corrected the structure name in a product behavior note. Changed from: The DNSSRV_ZONE_RRL_STATS structure SHOULD<83> contain zone statistics about Response Rate Limiting. <83> Section 2.2.12.2.6: The DNS_RPC_ZONE_RRL_STATS structure is implemented in Windows Server 2016 Technical Preview.

Errata Published*	Description
	Changed to: The DNSSRV_ZONE_RRL_STATS structure SHOULD<83> contain zone statistics about Response Rate Limiting. <84> Section 2.2.12.2.6: The DNSSRV_ZONE_RRL_STATS structure is implemented in Windows Server 2016 Technical Preview.

*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

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V34.0 – 2015/10/16.

Errata Published*	Description
2016/01/25	In Section 4.1.27.1.4, DRS_MSG_VERIFYREPLY_V1, updated RequestAttrs to RequiredAttrs in the rpEntInf array definition. Changed from: rpEntInf: An array of ENTINF structures that contain the attributes requested in the RequestAttrs field of the input DRS_MSG_VERIFYREQ_V1 structure if the corresponding name is verified. Changed to: rpEntInf: An array of ENTINF structures that contain the attributes requested in the RequiredAttrs field of the input DRS_MSG_VERIFYREQ_V1 structure if the corresponding name is verified.

2016/01/25	In Section 4.1.10.5.12, ProcessFsmoRoleRequest, updated the use of pMsgIn in the procedure implementation to match the procedure's signature (msgIn: DRS_MSG_GETCHGREQ_V10) and the use of NC to match the pNC member of the DRS_MSG_GETCHGREQ_V10 structure.
	
	Changed from:
	
	`if(not FullReplicaExists(GetObjectNC(pMsgIn.NC)) and`
	`not pMsgIn.pPartialAttrSet = null)`
	`msgOut.ulExtendedRet := EXOP_ERR_PARAM_ERR`
	`return`
	`else if not GetFilteredAttributeSet()∩ pMsgIn.pPartialAttrSet = {} then`
	
	Changed to:
	
	`if(not FullReplicaExists(GetObjectNC(msgIn.pNC^)) and`
	`not msgIn.pPartialAttrSet = null)`
	`msgOut.ulExtendedRet := EXOP_ERR_PARAM_ERR`
	`return`
	`else if not GetFilteredAttributeSet() ∩ msgIn.pPartialAttrSet = {} then`

2015/11/09	In Section 4.1.18.2 (Server Behavior of the IDL_DRSRemoveDsServer Method), added pseudo

Errata Published*	Description

	code for method CleanupRODCStates to clean up read-only domain controllers in the IDL_DRSRemoveDsServer implementation.
	
	Changed from:
	
	`ULONG`
	`IDL_DRSRemoveDsServer(`
	`[in, ref] DRS_HANDLE hDrs,`
	`[in] DWORD dwInVersion,`
	`[in, ref, switch_is(dwInVersion)]`
	`DRS_MSG_RMSVRREQ *pmsgIn,`
	`[out, ref] DWORD *pdwOutVersion,`
	`[out, ref, switch_is(*pdwOutVersion)]`
	`DRS_MSG_RMSVRREPLY *pmsgOut);`
	
	`serverDn: unicodestring`
	`domainDn: unicodestring`
	`server: DSName`
	`ntdsdsa: DSName`
	`otherNtdsdsa: DSName`
	`spnsToRemove: set of unicodestring`
	`computerDn: unicodestring`
	`computer: DSName`
	`objectsToDelete: set of DSName`
	`rt: ULONG`
	`ValidateDRSInput(hDrs, 14)`
	
	`serverDn := pmsgIn^.V1.ServerDN`
	`domainDn := pmsgIn^.V1.DomainDN`
	
	`pdwOutVersion^ := 1`
	`pmsgOut^.V1.fLastDcInDomain = false`
	
	`/* Basic parameter validation */`
	`if dwInVersion ≠ 1 then`
	`return ERROR_INVALID_PARAMETER`
	`endif`
	
	`if serverDn = null or serverDn = "" then`
	`return ERROR_INVALID_PARAMETER`
	`endif`
	
	`/* Note that DomainDN may be null, but it cannot be empty. */`
	`if domainDn = "" then`
	`return ERROR_INVALID_PARAMETER`
	`endif`
	
	`/* Compute fLastDcInDomain if domainDn is non-null. */`
	`if domainDn ≠ null then`
	`otherNtdsdsa := select one o from subtree ConfigNC() where`
	`(o!objectCategory = nTDSDSA)`
	`and`
	`(domainDn in o!hasMasterNCs or domainDn in o!msDS-hasMasterNCs)`
	`and`
	`(o ≠ ntdsdsa)`
	`if otherNtdsdsa = null then`
	`pmsgOut^.V1.fLastDcInDomain = true`

Errata Published*	Description

	else
	pmsgOut^.V1.fLastDcInDomain = false
	endif
	endif
	
	/* If nothing to commit, processing is complete. */
	if not pmsgIn^.V1.fCommit then
	return 0
	endif
	
	ntdsdsa := DescendantObject([dn: serverDn], "CN=NTDS Settings,")
	if ntdsdsa = null then
	return ERROR_DS_CANT_FIND_DSA_OBJ
	endif
	
	/* Perform the actual DC metadata removal. */
	
	/* Locate the computer object for the DC's account. */
	server := ntdsdsa!parent
	computerDn := server!serverReference
	computer := null
	if computerDn ≠ null then
	computer := GetDSNameFromDN(computerDn)
	endif
	
	/* Remove the subtree of objects rooted at the DC's ntdsDsa object.*/
	
	if not AccessCheckObject(ntdsdsa, RIGHT_DS_DELETE_TREE) then
	return ERROR_ACCESS_DENIED
	endif
	
	rt := RemoveObj(ntdsdsa,true)
	if rt ≠ 0 then
	return rt
	endif
	
	/* If the DC's computer account exists, remove rIDSet objects and
	* remove the DRS SPNs from the computer object. */
	
	if computer ≠ null then
	foreach r in computer!rIDSetReferences
	if (not AccessCheckObject(r, RIGHT_DELETE)) and
	(not AccessCheckObject(r.parent, RIGHT_DS_DELETE_CHILD)) then
	return ERROR_ACCESS_DENIED
	endif
	
	RemoveObj(r, false)
	endfor
	
	foreach spn in computer!servicePrincipalName
	if StartsWith(spn, "ldap/") or
	StartsWith(spn, "GC/") or
	StartsWith(spn, "E3514235-4B06-11D1-AB04-00C04FC2DCD2/") then
	spnsToRemove := spnsToRemove + {spn}
	endif
	endfor

Errata Published*	Description

```
        if not AccessCheckAttr(computer, servicePrincipalName,
            RIGHT_DS_WRITE_PROPERTY) then
          return ERROR_ACCESS_DENIED
        endif

        computer!servicePrincipalName :=
          computer!servicePrincipalName - spnsToRemove
      endif

      return 0
```

Changed to:

```
      ULONG
      IDL_DRSRemoveDsServer(
          [in, ref] DRS_HANDLE hDrs,
          [in] DWORD dwInVersion,
          [in, ref, switch_is(dwInVersion)]
              DRS_MSG_RMSVRREQ *pmsgIn,
          [out, ref] DWORD *pdwOutVersion,
          [out, ref, switch_is(*pdwOutVersion)]
              DRS_MSG_RMSVRREPLY *pmsgOut);

      serverDn: unicodestring
      domainDn: unicodestring
      server: DSName
      ntdsdsa: DSName
      otherNtdsdsa: DSName
      spnsToRemove: set of unicodestring
      computerDn: unicodestring
      computer: DSName
      objectsToDelete: set of DSName
      rt: ULONG
      RODCKrbtgtAcct: DSName
      accountList: set of DSName
      ValidateDRSInput(hDrs, 14)

      serverDn := pmsgIn^.V1.ServerDN
      domainDn := pmsgIn^.V1.DomainDN

      pdwOutVersion^ := 1
      pmsgOut^.V1.fLastDcInDomain = false

      /* Basic parameter validation */
      if dwInVersion ≠ 1 then
        return ERROR_INVALID_PARAMETER
      endif

      if serverDn = null or serverDn = "" then
        return ERROR_INVALID_PARAMETER
      endif

      /* Note that DomainDN may be null, but it cannot be empty. */
      if domainDn = "" then
```

Errata Published*	Description

	return ERROR_INVALID_PARAMETER
	endif
	
	/* Compute fLastDcInDomain if domainDn is non-null. */
	if domainDn ≠ null then
	otherNtdsdsa := select one o from subtree ConfigNC() where
	(o!objectCategory = nTDSDSA)
	and
	(domainDn in o!hasMasterNCs or domainDn in o!msDS-hasMasterNCs)
	and
	(o ≠ ntdsdsa)
	if otherNtdsdsa = null then
	pmsgOut^.V1.fLastDcInDomain = true
	else
	pmsgOut^.V1.fLastDcInDomain = false
	endif
	endif
	
	/* If nothing to commit, processing is complete. */
	if not pmsgIn^.V1.fCommit then
	return 0
	endif
	
	ntdsdsa := DescendantObject([dn: serverDn], "CN=NTDS Settings,")
	if ntdsdsa = null then
	return ERROR_DS_CANT_FIND_DSA_OBJ
	endif
	
	/* Perform the actual DC metadata removal. */
	
	/* Locate the computer object for the DC's account. */
	server := ntdsdsa!parent
	computerDn := server!serverReference
	computer := null
	if computerDn ≠ null then
	computer := GetDSNameFromDN(computerDn)
	endif
	
	/* Remove the subtree of objects rooted at the DC's ntdsDsa object.*/
	
	if not AccessCheckObject(ntdsdsa, RIGHT_DS_DELETE_TREE) then
	return ERROR_ACCESS_DENIED
	endif
	
	rt := RemoveObj(ntdsdsa,true)
	if rt ≠ 0 then
	return rt
	endif
	
	/* If the DC's computer account exists, remove rIDSet objects and
	* remove the DRS SPNs from the computer object. */
	
	if computer ≠ null then
	foreach r in computer!rIDSetReferences
	if (not AccessCheckObject(r, RIGHT_DELETE)) and
	(not AccessCheckObject(r.parent, RIGHT_DS_DELETE_CHILD)) then

Errata Published*	Description

	return ERROR_ACCESS_DENIED
	endif
	
	RemoveObj(r, false)
	endfor
	
	foreach spn in computer!servicePrincipalName
	if StartsWith(spn, "ldap/") or
	StartsWith(spn, "GC/") or
	StartsWith(spn, "E3514235-4B06-11D1-AB04-00C04FC2DCD2/") or
	StartsWith(spn, "RPC/") then
	spnsToRemove := spnsToRemove + {spn}
	endif
	endfor
	/* Cleanup for read-only domain controllers */
	
	/* Clear the KrbTgtLink from computer and delete its object */
	
	/* Get the msDS-KrbTgtLink attribute from the object */
	RODCKrbtgtAcct := computer!msDS-KrbTgtLink
	
	/* Delet the attribute from the object */
	Computer!msDS-KrbTgtLink := null
	
	/* Remove the KrbTgtLink */
	RemoveObj(RODCKrbTgtLink, false)
	
	/* Delete RODC policies */
	computer!msDS-NeverRevealGroup := null
	computer!msDS-RevealOnDemandGroup := null
	computer!msDS-RevealedUsers := null
	
	/* Delete msDS-AuthenticatedToAccountList links */
	accountList := { computer!msDS-AuthenticatedToAccountList }
	
	foreach entry in accountList
	entry!msDS-AuthenticatedAtDC := entry!msDS-AuthenticatedAtDC – computer
	endfor
	
	if not AccessCheckAttr(computer, servicePrincipalName,
	RIGHT_DS_WRITE_PROPERTY) then
	return ERROR_ACCESS_DENIED
	endif
	
	computer!servicePrincipalName :=
	computer!servicePrincipalName - spnsToRemove
	endif
	
	return 0

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V4.0 – 2015/10/16.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2015/11/23</td><td>In Section 2.2.2.1, Content-Type, changed from:
Example: Content-Type: application/octetstring

Changed to:
Example: Content-Type: application/octet-stream</td></tr>
<tr><td>2015/11/23</td><td>In Section 3.4.5, Message Processing Events and Sequencing Rules, and Section 3.5.5, Message Processing Events and Sequencing Rules, corrected the name of the resource.

In Section 3.4.5, Message Processing Events and Sequencing Rules, changed from:
<table><tr><th>Resource</th><th>Description</th></tr><tr><td>Nodes(ConfigurationID={ConfigurationId})/SendStatusReport</td><td>Send the status report to the server.</td></tr></table>
Changed to:
<table><tr><th>Resource</th><th>Description</th></tr><tr><td>Node(ConfigurationID={ConfigurationId})/SendStatusReport</td><td>Send the status report to the server.</td></tr></table>
In Section 3.5.5, Message Processing Events and Sequencing Rules, changed from:
<table><tr><th>Resource</th><th>Description</th></tr><tr><td>Nodes(ConfigurationId={ConfigurationId})/Reports(JobId={JobId}))</td><td>Get the status report from the server.</td></tr></table>
Changed to:
<table><tr><th>Resource</th><th>Description</th></tr><tr><td>Node(ConfigurationId={ConfigurationId})/Reports(JobId={JobId}))</td><td>Get the status report from the server.</td></tr></table></td></tr>
</table>

*Date format: YYYY/MM/DD

[MS-DTYP]: Windows Data Types

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V30.0 – 2015/10/16.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2016/02/22</td><td>In Section 2.4.10.1, CLAIM_SECURITY_ATTRIBUTE_RELATIVE_V1, added a product behavior note to clarify how the CLAIM_SECURITY_ATTRIBUTE_NON_INHERITABLE flag is interpreted.

Changed from:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>CLAIM_SECURITY_ATTRIBUTE_NON_INHERITABLE
0x0001</td><td>This claim security attribute is not inherited across processes.</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
…

Changed to:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>CLAIM_SECURITY_ATTRIBUTE_NON_INHERITABLE
0x0001</td><td>This claim security attribute is not inherited across processes.<69></td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
<69> Section 2.4.10.1: This value is ignored by Windows when set on a security descriptor.</td></tr>
</table>

*Date format: YYYY/MM/DD

[MS-DVRD]: Device Registration Discovery Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V3.0 – 2015/10/16.

Errata Published*	Description
2016/04/04	In Section 3.1.5.1.1.3, Processing Details, clarified server processing when an unsupported header value is given for the Accept header. Changed from: … 3. If the Accept header is present in the request, the server MUST allow only the Accept header values as defined in section 2.2.2.1. If the Accept header is not present, the response format in step 4 below MUST be XML. Any other header value MUST be ignored and the server MUST continue processing. … Changed to: … 3. If the Accept header is present in the request, the server MUST allow only the Accept header values as defined in section 2.2.2.1. If the Accept header is not present, the response format in step 4 below MUST be XML. Any other header value MUST return an HTTP error code in the 400 range. The body of the message response in this case is insignificant to the protocol; clients MUST halt processing upon receiving an HTTP error. …

*Date format: YYYY/MM/DD

[MS-DVRE]: Device Registration Enrollment Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-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

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V5.0 – 2015/10/16.

Errata Published*	Description
2016/01/25	In Section 3.3.5.1.1.2, Response Body, the description of the Length field has been corrected. Changed from: Length: This indicates the size of the AdminEmail field. Changed to: Length: This indicates the size of the AdminInfo field.
2015/12/11	In Section 2.2.2.7, FILE_INFO_ENTRY, clarified the description for PrepareResult. Changed from: … PrepareResult (4 bytes): This value contains the result of the preparation process. … Changed to: … PrepareResult (4 bytes): This value contains the result of the preparation process of type HRESULT as specified in [MS-DTYP] section 2.2.18. …
2015/11/23	A new error code section has been added. **Section 2.2.2.28 Error Codes** The following HRESULT codes are defined in this document. Error Code | Value

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>ECS_E_SYNC_INVALID_PROTOCOL_FORMAT</td><td>0x80C80001</td></tr>
<tr><td>ECS_E_SYNC_SESSION_BUSY</td><td>0x80C80003</td></tr>
<tr><td>ECS_E_USER_SUSPENDED</td><td>0x80C80005</td></tr>
<tr><td>ECS_E_SYNC_INVALID_SESSION_TYPE</td><td>0x80C80012</td></tr>
<tr><td>ECS_E_SYNC_REQUIRED_HTTP_HEADER_MISSING</td><td>0x80C8001A</td></tr>
<tr><td>ECS_E_SYNC_TOO_MANY_SESSIONS</td><td>0x80C8001B</td></tr>
<tr><td>ECS_E_STREAM_NOT_NEEDED</td><td>0x80C80030</td></tr>
<tr><td>ECS_E_FILE_TOO_LARGE_FOR_UPLOAD</td><td>0x80C80039</td></tr>
<tr><td>ECS_E_DISCOVERY_NEEDED</td><td>0x80C8003B</td></tr>
<tr><td>ECS_E_SYNC_SERVER_BUSY</td><td>0x80C8003E</td></tr>
<tr><td>ECS_E_ERROR_SYNC_SHARE_BLOCKED</td><td>0x80C80303</td></tr>
</table>

In Section 3.4.5, Message Processing Events and Sequencing Rules, Section 3.4.5.1.1.3, Processing Details, and Section 3.4.5.4.1.3, Processing Details, after each error code a reference to the new Section 2.2.28, Error Codes, has been added.

In Section 3.4.5, Message Processing Events and Sequencing Rules, and Section 3.4.5.1.1.3, Processing Details, the numeric error code values have been replaced with their name from the new Section 2.2.28, Error Codes, or from MS-ERREF Section 2.1.1, HRESULT Values.
</td></tr>
<tr><td>2015/10/26</td><td>In Section 2.2.3.39, SR_RESOURCE_TYPE_QUERY_ELIGIBLE_SOURCE_DATADISKS, corrected all instances of SR_RESOURCE_TYPE_ELIGIBLE_SOURCE_DATADISKS to SR_RESOURCE_TYPE_QUERY_ELIGIBLE_SOURCE_DATADISKS.</td></tr>
</table>

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V23.0 – 2015/10/16.

Errata Published*	Description
2016/04/18	In Section 2.2.2.3, EFSRPC Metadata Version 3, corrected two field names. Changed from: … EncryptedDataOffset (4 bytes): The offset, in bytes, from the beginning of the Preamble field to the EncryptedDataOffset field. … MetaDataOffset (4 bytes): The offset, in bytes, from the beginning of the Preamble field to the EncryptedDataOffset field, formatted as a ULONGLONG (unsigned 64-bit integer as described in section [MS-DTYP] section 2.2.55). … Changed to: … EncryptedDataOffset (4 bytes): The offset, in bytes, from the beginning of the Preamble field to the EncryptedData field. … MetaDataOffset (4 bytes): The offset, in bytes, from the beginning of the Preamble field to the MetaData field, formatted as a ULONGLONG (unsigned 64-bit integer as described in section [MS-DTYP] section 2.2.55). …
2016/01/25	In Section 3.1.4.2.13, Receiving an EfsRpcDuplicateEncryptionInfoFile Message (Opnum 13), clarified how to check whether the objects are of the same type. Changed from: Return Values: The server MUST return 0 if it successfully processes the message received from the client. The server MUST return a nonzero value if processing fails. … If an encrypted object exists with the name specified in the SrcFileName and dwCreationDisposition parameters is equal to CREATE_NEW, then: … ▪ If an object already exists with the name specified in the DestFileName parameter, the server MUST check whether the object referred to by SrcFileName is of the same type; if the object is not of the same type, the server MUST return a nonzero value. In addition, if the object referred to by DestFileName is a container for other objects, and it is not already encrypted, the server MUST return a nonzero value. Otherwise, the server SHOULD overwrite the object, clear its existing attributes, create a new object in its place with the attributes specified, and duplicate the EFSRPC Metadata from the SrcFileName parameter into it.

Errata Published*	Description
	Changed to: Return Values: The server MUST return 0 if it successfully processes the message received from the client. The server MUST return a nonzero value if processing fails. … If an encrypted object exists with the name specified in the SrcFileName and dwCreationDisposition parameters is equal to CREATE_NEW, then: … ▪ If an object already exists with the name specified in the DestFileName parameter, the server MUST check whether the object referred to by SrcFileName is of the same type (either simple object or container for other objects); if the object is not of the same type, the server MUST return a nonzero value. In addition, if the object referred to by DestFileName is a container for other objects, and it is not already encrypted, the server MUST return a nonzero value. Otherwise, the server SHOULD overwrite the object, clear its existing attributes, create a new object in its place with the attributes specified, and duplicate the EFSRPC Metadata from the SrcFileName parameter into it.

* Date format: YYYY/MM/DD

[MS-EMF]: Enhanced Metafile Format

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-EMFPLUS]: Enhanced Metafile Format Plus Extensions

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-ERREF]: Windows Error Codes

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

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

RSS
Atom

Errata below are for Protocol Document Version V15.0 – 2015/10/16.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2016/01/11</td><td>In Section 2.3.1, NTSTATUS values, the below tabular entry for the returned value 0xC0000480, STATUS_SHARE_UNAVAILABLE, has been added.

<table>
<tr><th>Return value/code</th><th>Description</th></tr>
<tr><td>0xC0000480
STATUS_SHARE_UNAVAILABLE</td><td>The share is temporarily unavailable</td></tr>
</table>
</td></tr>
<tr><td>2015/11/23</td><td>In Section 2.1.1, HRESULT Values, added a new Error Code.

Changed from:
<table>
<tr><th>Returned value/code</th><th>Description</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>0x80070057
E_INVALIDARG</td><td>One or more arguments are invalid.</td></tr>
<tr><td>0x80080001
CO_E_CLASS_CREATE_FAILED</td><td>Attempt to create a class object failed.</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>

Changed to:
<table>
<tr><th>Returned value/code</th><th>Description</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>0x80070057
E_INVALIDARG</td><td>One or more arguments are invalid.</td></tr>
<tr><td>0x80070070
ERROR_DISK_FULL</td><td>There is not enough space on the disk.</td></tr>
<tr><td>0x80080001
CO_E_CLASS_CREATE_FAILED</td><td>Attempt to create a class object failed.</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description
	*Date format: YYYY/MM/DD

[MS-EVEN]: EventLog Remoting Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V19.0 – 2015/10/16.

Errata Published*	Description

2016/04/04	In Section 6, Appendix A: Full IDL, updated the full IDL regarding ElfrReportEventExW and ElfrReportEventExA.
	
	Changed from:
	
	`NTSTATUS`
	`ElfrReportEventExW(`
	`[in] IELF_HANDLE LogHandle,`
	`[in] PFILETIME TimeGenerated,`
	`[in] USHORT EventType,`
	`[in] USHORT EventCategory,`
	`[in] ULONG EventID,`
	`[in, range(0, MAX_STRINGS)] USHORT NumStrings,`
	`[in, range(0, MAX_SINGLE_EVENT)] ULONG DataSize,`
	`[in] PRPC_UNICODE_STRING ComputerName,`
	`[in, unique] PRPC_SID UserSID,`
	`[in, size_is(NumStrings), unique] PRPC_UNICODE_STRING Strings[*],`
	`[in, size_is(DataSize), unique] PBYTE Data,`
	`[in] USHORT Flags,`
	`[in, out, unique] PULONG RecordNumber`
	`);`
	
	`NTSTATUS`
	`ElfrReportEventExA(`
	`[in] IELF_HANDLE LogHandle,`
	`[in] PFILETIME TimeGenerated,`
	`[in] USHORT EventType,`
	`[in] USHORT EventCategory,`
	`[in] ULONG EventID,`
	`[in, range(0, MAX_STRINGS)] USHORT NumStrings,`
	`[in, range(0, MAX_SINGLE_EVENT)] ULONG DataSize,`
	`[in] PRPC_STRING ComputerName,`

Errata Published*	Description
	[in, unique] PRPC_SID UserSID, [in, size_is(NumStrings), unique] PRPC_STRING Strings[*], [in, size_is(DataSize), unique] PBYTE Data, [in] USHORT Flags, [in, out, unique] PULONG RecordNumber); Changed to: NTSTATUS ElfrReportEventExW([in] IELF_HANDLE LogHandle, [in] PFILETIME TimeGenerated, [in] unsigned short EventType, [in] unsigned short EventCategory, [in] unsigned long EventID, [in, range(0, 256)] unsigned short NumStrings, [in, range(0, 61440)] unsigned long DataSize, [in] PRPC_UNICODE_STRING ComputerName, [in, unique] PRPC_SID UserSID, [in, size_is(NumStrings), unique] PRPC_UNICODE_STRING Strings[*], [in, size_is(DataSize), unique] unsigned char* Data, [in] unsigned short Flags, [in, out, unique] unsigned long* RecordNumber); NTSTATUS ElfrReportEventExA([in] IELF_HANDLE LogHandle, [in] PFILETIME TimeGenerated, [in] unsigned short EventType, [in] unsigned short EventCategory, [in] unsigned long EventID, [in, range(0, 256)] unsigned short NumStrings, [in, range(0, 61440)] unsigned long DataSize, [in] PRPC_STRING ComputerName, [in, unique] PRPC_SID UserSID, [in, size_is(NumStrings), unique] PRPC_STRING Strings[*], [in, size_is(DataSize), unique] unsigned char* Data, [in] unsigned short Flags, [in, out, unique] unsigned long* RecordNumber);
2016/02/22	In Section 2.2.3, EVENTLOGRECORD, corrected the field name numStrings to NumStrings.

Errata Published*	Description
	Changed from: Strings (variable): Zero or more null-terminated strings containing information on the event. The numStrings field contains the number of items in this field. Changed to: Strings (variable): Zero or more null-terminated strings containing information on the event. The NumStrings field contains the number of items in this field.
2016/02/22	In Section 3.1.4.16, ElfrReportEventExW (Opnum 25), corrected that if the handle is valid, the method attempts to create an event with the supplied parameters and by setting the TimeGenerated, not the TimeWritten, field. Changed from: If the handle is valid, the method attempts to create an event with the supplied parameters and by setting the TimeWritten and the RecordNumber fields in the event. The TimeWritten is obtained from the system clock. The server MUST get the RecordNumber from the state maintained for the event log. The server can get the last record in the event log file, read the record number from that record, and use that record number plus 1 as the new record number. The new record number SHOULD be set to the value in the event log file header so that the total number of records in the file is stored. The server sets the RecordNumber parameter to the same value written to the event prior to returning from this method. Changed to: If the handle is valid, the method attempts to create an event with the supplied parameters and by setting the TimeGenerated and the RecordNumber fields in the event. The TimeGenerated is obtained from the system clock. The server MUST get the RecordNumber from the state maintained for the event log. The server can get the last record in the event log file, read the record number from that record, and use that record number plus 1 as the new record number. The new record number SHOULD be set to the value in the event log file header so that the total number of records in the file is stored. The server sets the RecordNumber parameter to the same value written to the event prior to returning from this method.

* Date format: YYYY/MM/DD

[MS-FASP]: Firewall and Advanced Security Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V22.1 – 2015/10/16.

Errata Published*	Description

2016/06/27	In two sections, added content for some FW_RULE_FLAGS values that indicates support by Windows Server versions to specify that they not be used for schema versions 0x0200 and 0x0201.
	
	In Section 2.2.34, 2.2.34 FW_RULE_FLAGS, included the following statement for the descriptions of 5 flags:
	For schema versions 0x0200 and 0x0201, this value is invalid and MUST NOT be used.
	
	The 5 flags are:
	FW_RULE_FLAGS_AUTH_WITH_NO_ENCAPSULATION,
	FW_RULE_FLAGS_AUTH_WITH_ENC_NEGOTIATE,
	FW_RULE_FLAGS_ROUTEABLE_ADDRS_TRAVERSE_DEFER_APP,
	FW_RULE_FLAGS_ROUTEABLE_ADDRS_TRAVERSE_DEFER_USER, and
	FW_RULE_FLAGS_AUTHENTICATE_BYPASS_OUTBOUND
	
	In Section 6, Appendix A: Full IDL, changed from:
	
	FW_RULE_FLAGS_LOOSE_SOURCE_MAPPED = 0x00010,
	// This is the new "NoEncapsulation" flag in Win7.
	FW_RULE_FLAGS_AUTH_WITH_NO_ENCAPSULATION = 0x0020,
	// These are the new flags added for SSP in Win 7.
	
	Changed to:
	FW_RULE_FLAGS_LOOSE_SOURCE_MAPPED = 0x00010,
	// This is the new "NoEncapsulation" flag in Windows 7 and Windows Server 2008 R2.
	FW_RULE_FLAGS_AUTH_WITH_NO_ENCAPSULATION = 0x0020,
	// These are the new flags added for SSP in Windows 7 and Windows Server 2008 R2.
	
	Changed from:
	FW_RULE_FLAGS_AUTHENTICATE_BYPASS_OUTBOUND = 0x0200,
	// This is the new flag in Windows 8 to allow profile crossings for clusters.
	FW_RULE_FLAGS_ALLOW_PROFILE_CROSSING = 0x0400,
	// This is the new flag in Windows 8 to allow LOM on flows.
	
	Changed to:
	FW_RULE_FLAGS_AUTHENTICATE_BYPASS_OUTBOUND = 0x0200,

Errata Published*	Description

	// This is the new flag in Windows 8 and Windows Server 2012 to allow profile crossings
	// for clusters.
	FW_RULE_FLAGS_ALLOW_PROFILE_CROSSING = 0x0400,
	// This is the new flag in Windows 8 and Windows Server 2012 to allow LOM on flows.

2016/01/25	In Section 4.2, Adding a Firewall Rule, changed the definitions of wide character string literals by assigning an L before each of them. Changed from: WCHAR* wszName = "Web server requests"; WCHAR* wszDescription = "This rule allows incoming HTTP server requests"; WCHAR* wszLocalApplication = "c:\servers\MyWebServer.exe"; WCHAR* wszLocalService = "WebServerSVC"; Changed to: WCHAR* wszName = L"Web server requests"; WCHAR* wszDescription = L"This rule allows incoming HTTP server requests"; WCHAR* wszLocalApplication = L"c:\servers\MyWebServer.exe"; WCHAR* wszLocalService = L"WebServerSVC";
2016/01/25	In two sections, corrected the descriptions of the ppAuth parameter of RRPC_FWEnumAuthenticationSets2_10 and the ppCryptoSets parameter of RRPC_FWEnumCryptoSets2_10 to describe them as output parameters rather than input parameters. In Section 3.1.4.55, RRPC_FWEnumAuthenticationSets2_10 (Opnum 54), changed from: ppAuth: This parameter represents the authentication set that the client adds to the store. The set MUST be valid, as specified in the definition of the FW_AUTH_SET2_10 data type. Changed to: ppAuth: This is an output parameter that, on success, contains a linked list of FW_AUTH_SET2_10 data types. In Section 3.1.4.58, RRPC_FWEnumCryptoSets2_10 (Opnum 57), changed from: ppCryptoSets: This parameter represents the authentication set that the client adds to the store. The set MUST be valid, as specified in the definition of the FW_AUTH_SET data type. Changed to: ppCryptoSets: This is an output parameter that, on success, contains a linked list of FW_CRYPTO_SET data types.
2015/10/26	In Section 3.1.4.5, RRPC_FWSetGlobalConfig (Opnum 4), corrected the description of the dwBufSize parameter. Changed from: **dwBufSize:** This parameter is the size of the buffer to which the *pBuffer* parameter points.

Errata Published*	Description

	Changed to:
	
	dwBufSize: This parameter is the size of the buffer to which the *lpBuffer* parameter points.
	
	In Section 3.1.4.12, RRPC_FWSetConfig (Opnum 11), corrected the descriptions of the configID and Profile parameters.
	
	Changed from:
	
	configID: This parameter specifies the specific profile configuration option the client is interested in retrieving.
	
	Profile: This parameter specifies from which specific profile this value MUST be retrieved.
	
	Changed to:
	
	configID: This parameter specifies the specific profile configuration option the client wants to modify.
	
	Profile: This parameter specifies in which specific profile this value MUST be written.
	
	In Section 4.3, Enumerating the Firewall Rules, corrected the example.
	
	Changed from:
	
	…
	
	`FW_RULE_STATUS_CLASS_OK | FW_RULE_STATUS_CLASS_PARTIALLY_IGNORED,`
	`[in] DWORD dwProfileFilter, FW_PROFILE_TYPE_CURRENT,`
	
	…
	
	Changed to:
	
	`FW RULE STATUS CLASS OK | FW RULE STATUS CLASS PARTIALLY IGNORED,`
	`[in] DWORD dwProfileFilter =FW_PROFILE_TYPE_CURRENT,`

* Date format: YYYY/MM/DD

[MS-FRS2]: Distributed File System Replication Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-FSA]: File System Algorithms

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

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

RSS
Atom

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

March 2, 2016 - Download

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V21.0 – 2016/03/02.

Errata Published*	Description
2016/06/27	In Section 2.1.5.1.2.1, Algorithm to Check Access to an Existing File, changed the pseudocode to clarify GrantedAccess.DELETE and STATUS_SHARING_VIOLATION during access check. Changed from: • If Open.SharingMode.FILE_SHARE_DELETE is FALSE and Open.GrantedAccess contains any one or more of (FILE_EXECUTE | FILE_READ_DATA | FILE_WRITE_DATA | FILE_APPEND_DATA): • For each ExistingOpen in Open.File.OpenList: • If ExistingOpen.Mode.FILE_DELETE_ON_CLOSE is TRUE and (ExistingOpen.Stream.StreamType is DirectoryStream or ExistingOpen.Stream.Name is empty), then return STATUS_SHARING_VIOLATION. • EndFor • EndIf • If Open.GrantedAccess.DELETE is TRUE and (Open.Stream.StreamType is DirectoryStream or Open.Stream.Name is empty): • For each ExistingOpen in Open.File.OpenList: • If ExistingOpen.SharingMode.FILE_SHARE_DELETE is FALSE, then return STATUS_SHARING_VIOLATION. • EndFor • EndIf • Return STATUS_SUCCESS. Changed to: • If Open.SharingMode.FILE_SHARE_DELETE is FALSE and Open.GrantedAccess contains any one or more of (FILE_EXECUTE | FILE_READ_DATA | FILE_WRITE_DATA | FILE_APPEND_DATA | DELETE): • For each ExistingOpen in Open.File.OpenList: • If ExistingOpen.GrantedAccess.DELETE is TRUE and (ExistingOpen.Stream.StreamType is DirectoryStream or ExistingOpen.Stream.Name is empty), then return

Errata Published*	Description
	STATUS_SHARING_VIOLATION. • EndFor • EndIf • If Open.GrantedAccess.DELETE is TRUE and (Open.Stream.StreamType is DirectoryStream or Open.Stream.Name is empty): • For each ExistingOpen in Open.File.OpenList: • If ExistingOpen.SharingMode.FILE_SHARE_DELETE is FALSE and ExistingOpen.GrantedAccess contains one or more of (FILE_EXECUTE | FILE_READ_DATA | FILE_WRITE_DATA | FILE_APPEND_DATA | DELETE), then return STATUS_SHARING_VIOLATION. • EndFor • EndIf • Return STATUS_SUCCESS
2016/06/27	In Section 2.1.5.1.2.2, Algorithm to Check Sharing Access to an Existing Stream or Directory, the following bullet points have been changed from: If ExistingOpen.SharingMode.FILE_SHARE_READ is FALSE and DesiredAccess contains either FILE_READ_DATA or FILE_EXECUTE If ExistingOpen.SharingMode.FILE_SHARE_WRITE is FALSE and DesiredAccess contains either FILE_WRITE_DATA or FILE_APPEND_DATA If ExistingOpen.SharingMode.FILE_SHARE_DELETE is FALSE and ExistingOpen contains DELETE Changed to: If ExistingOpen.SharingMode.FILE_SHARE_READ is FALSE and Open.GrantedAccess contains either FILE_READ_DATA or FILE_EXECUTE If ExistingOpen.SharingMode.FILE_SHARE_WRITE is FALSE and Open.GrantedAccess contains either FILE_WRITE_DATA or FILE_APPEND_DATA If ExistingOpen.SharingMode.FILE_SHARE_DELETE is FALSE and Open.GrantedAccess contains DELETE
2016/03/21	In Section 2.1.5.14.1, FileAllocationInformation, added text and a product behavior note to clarify that the FAT/FAT32/exFAT/UDFS file allocation behavior is different from NTFS. Changed from: ▪ If NewAllocationSize is less than Open.Stream.Size: ▪ The object store MUST set Open.Stream.Size to NewAllocationSize, truncating the Stream. ▪ … Changed to: ▪ If InputBuffer.AllocationSize is less than Open.Stream.Size: ▪ Set NewFileSize to min(Open.Stream.Size, NewAllocationSize<127>). ▪ If NewFileSize is less than Open.Stream.Size: ▪ The object store MUST set Open.Stream.Size to NewFileSize, truncating the stream. ▪ … <127> Section 2.1.5.14.1: The FAT, FAT32, exFAT, and UDFS file systems instead set NewFileSize to min(Open.Stream.Size, InputBuffer.AllocationSize).

Errata Published*	Description
2016/03/21	In Section 2.1.5.14.11, FileRenameInformation, added Unicode Strings for the root path name and the destination full link name. Also, clarified the behavior for renaming file path names for files at the root directory and for files at a linked destination. Changed from: This routine uses the following local variables: ▪ Unicode strings: PathName, NewLinkName, PrevFullLinkName, SourceFullLinkName ▪ … Changed to: This routine uses the following local variables: ▪ Unicode strings: PathName, RootPathName, NewLinkName, PrevFullLinkName, SourceFullLinkName, DestFullLinkName ▪ … Changed from: Pseudocode for the operation is as follows: … The operation MUST be failed with STATUS_INVALID_PARAMETER under any of the following conditions: … ▪ Split InputBuffer.FileName into PathName and NewLinkName per section 2.1.5.1. ▪ If the first character of InputBuffer.FileName is '\': … Changed to: Pseudocode for the operation is as follows: … The operation MUST be failed with STATUS_INVALID_PARAMETER under any of the following conditions: … ▪ If this operation is from a remote client, and either InputBuffer.RootDirectory is nonzero or the first character of InputBuffer.FileName is '\'. ▪ If InputBuffer.RootDirectory is nonzero and the first character of InputBuffer.FileName is '\'. ▪ If InputBuffer.RootDirectory is nonzero: ▪ The object store MUST set RootPathName to the full pathname from Open.File.Volume.RootDirectory to the file represented by InputBuffer.RootDirectory, in an implementation-specific manner. ▪ The object store MUST set DestFullLinkName to RootPathName + '\' + InputBuffer.FileName. ▪ Else: ▪ The object store MUST set DestFullLinkName to InputBuffer.FileName. ▪ EndIf ▪ Split DestFullLinkName into PathName and NewLinkName per section 2.1.5.1. ▪ If the first character of InputBuffer.FileName is '\' or InputBuffer.RootDirectory is nonzero or this operation is from a remote client: ▪ …

Errata Published*	Description

2016/03/21	In Section 2.1.5.4, Server Requests Closing an Open, corrected the processing rules for Phase1 (Delete on Close behavior).
	
	Changed from:
	
	▪ Phase 1 - Delete on Close:
	▪ If Open.Mode.FILE_DELETE_ON_CLOSE is TRUE:
	  ▪ If Open.Stream.StreamType is DirectoryStream or Open.Stream.Name is empty:
	  ▪ Open.Link.IsDeleted MUST be set to TRUE.
	  ▪ Else:
	  ▪ Open.Stream.IsDeleted MUST be set to TRUE.
	  ▪ EndIf
	▪ EndIf
	
	Changed to:
	
	▪ Phase 1 - Delete on Close:
	▪ If Open.Mode.FILE_DELETE_ON_CLOSE is TRUE:
	  ▪ If Open.Stream.Name is empty:
	  ▪ If (Open.Stream.StreamType is DataStream or Open.File.DirectoryList is empty), then Open.Link.IsDeleted MUST be set to TRUE.
	  ▪ Else:
	  ▪ Open.Stream.IsDeleted MUST be set to TRUE.
	  ▪ EndIf
	▪ EndIf

*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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V39.0 – 2015/10/16.

Errata Published *	Description
2016/03/21	In Section 2.3.40.1, FILE_REGION_INFO, and Section 2.3.79 STORAGE_OFFLOAD_TOKEN, corrected two field names – DesiredUsage and TokenId. In Section 2.3.40.1, FILE_REGION_INFO, changed from: Usage (4 bytes): A 32-bit unsigned integer that indicates the usage for the given region of the file. The valid values are defined in section 2.3.39. Changed to: DesiredUsage (4 bytes): A 32-bit unsigned integer that indicates the usage for the given region of the file. The valid values are defined in section 2.3.39. Also, corrected the field name in the bit table. In Section 2.3.79 STORAGE_OFFLOAD_TOKEN, changed from: The TokenType and TokenIdLength fields of STORAGE_OFFLOAD_TOKEN structure MUST be sent in big-endian format. The TokenID field is a stream of bytes and has no endian property. Changed to: The TokenType and TokenIdLength fields of STORAGE_OFFLOAD_TOKEN structure MUST be sent in big-endian format. The TokenId field is a stream of bytes and has no endian property.
2015/11/23	In various sections, changed the normative language. In Section 1.7, Vendor-Extensible Fields, "should" has been changed to "MUST" in the first paragraph. Changed from: File system control codes that are used to set reparse point data specify a ReparseTag field value that identifies the file system filter that understands the application-specific reparse point data format. A vendor developing an application protocol that sets reparse point data should request a unique reparse tag for that application from Microsoft by following the instructions described in

Errata Published *	Description
	[WHDC-RPTR]. For more information about reparse points, see [REPARSE]. Changed to: File system control codes that are used to set reparse point data specify a ReparseTag field value that identifies the file system filter that understands the application-specific reparse point data format. A vendor developing an application protocol that sets reparse point data MUST request a unique reparse tag for that application from Microsoft by following the instructions described in [WHDC-RPTR]. For more information about reparse points, see [REPARSE]. In Section 2.1.2.1, Reparse Tags, "should" has been changed to "SHOULD" in the third paragraph. Changed from: The following reparse tags, with the exception of IO_REPARSE_TAG_SYMLINK, are processed on the server and are not processed by a client after transmission over the wire. Clients should treat associated reparse data as opaque data.<2> Changed to: The following reparse tags, with the exception of IO_REPARSE_TAG_SYMLINK, are processed on the server and are not processed by a client after transmission over the wire. Clients SHOULD treat associated reparse data as opaque data.<2> In Section 2.1.7, FILE_NAME_INFORMATION, "should not" has been changed to "MUST NOT" in the description of FileName. Changed from: FileName (variable): A sequence of Unicode characters containing a pathname (section 2.1.5). The meaning of the pathname depends on the operation. The name string is not null-terminated. There are scenarios where one or more padding characters may be at the end of the string due to buffer alignment requirements, but their presence and their values should not be relied upon. When working with this field, use FileNameLength to determine the length of the file name rather than assuming the presence of a trailing null delimiter. Changed to: FileName (variable): A sequence of Unicode characters containing a pathname (section 2.1.5). The meaning of the pathname depends on the operation. The name string is not null-terminated. There are scenarios where one or more padding characters may be at the end of the string due to buffer alignment requirements, but their presence and their values MUST NOT be relied upon. When working with this field, use FileNameLength to determine the length of the file name rather than assuming the presence of a trailing null delimiter. In Section 2.3.19, FSCTL_GET_OBJECT_ID Request, "should" has been changed to "SHOULD" in the second paragraph. Changed from: Object identifiers are 16-byte opaque values that are used to track files and directories, and they are generated by the server. File and directory object identifiers are invisible to most applications and should never be modified by applications. Changed to: Object identifiers are 16-byte opaque values that are used to track files and directories, and they are generated by the server. File and directory object identifiers are invisible to most applications and SHOULD never be modified by applications.

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td>2015/11/23</td><td>In Section 2.4.42, FileNotifyInformation, added two missing values for the Action field.

Changed from:

Action (4 bytes): The changes that occurred on the file. This field MUST contain one of the following values.

<table>
<tr><th>Values</th><th>Meaning</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>FILE_ACTION_REMOVED_BY_DELETE
0x00000009</td><td>An object ID was removed because the file the object ID referred to was deleted.
This notification is only sent when the directory being monitored is the special directory "\$Extend\$ObjId:$O:$INDEX_ALLOCATION".<125></td></tr>
</table>
Changed to:

Action (4 bytes): The changes that occurred on the file. This field MUST contain one of the following values.

<table>
<tr><th>Values</th><th>Meaning</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>FILE_ACTION_REMOVED_BY_DELETE
0x00000009</td><td>An object ID was removed because the file the object ID referred to was deleted.
This notification is only sent when the directory being monitored is the special directory "\$Extend\$ObjId:$O:$INDEX_ALLOCATION".<125></td></tr>
<tr><td>FILE_ACTION_ID_NOT_TUNNELLED
0x0000000A</td><td>An attempt to tunnel object ID information to a file being created or renamed failed because the object ID is in use by another file on the same volume.

This notification is only sent when the directory being monitored is the special directory "\$Extend\$ObjId:$O:$INDEX_ALLOCATION".<126></td></tr>
<tr><td>FILE_ACTION_TUNNELLED_ID_COLLISION
0x0000000B</td><td>An attempt to tunnel object ID information to a file being renamed failed because the file already has an object ID.

This notification is only sent when the directory being monitored is the special directory "\$Extend\$ObjId:$O:$INDEX_ALLOCATION".<127></td></tr>
</table>
<126> Only NTFS supports this special directory.
<126> Only NTFS supports this special directory</td></tr>
</table>

<table>
<tr><th>Errata Published *</th><th>Description</th></tr>
<tr><td></td><td></td></tr>
<tr><td>2015/10/26</td><td>
In Section 2.1.2.6, Network File System (NFS) Reparse Data Buffer, the composition of the DataBuffer field in the descriptions of NFS_SPECFILE_CHR and NFS_SPECFILE_BLK has been corrected.

Changed from:

Type (8 bytes): A 64-bit unsigned integer value describing the type and format of the data stored in the DataBuffer field. The valid values for this field are:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>NFS_SPECFILE_CHR
0x0000000000524843</td><td>Indicates that the DataBuffer field has two 16–bit integers that contain the major and minor numbers for the character special device created by the Network File System client.</td></tr>
<tr><td>NFS_SPECFILE_BLK
0x00000000004b4c42</td><td>Indicates that the DataBuffer field has two 16–bit integers that contain the major and minor numbers for the block special created by the Network File System client.</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
…
DataBuffer (variable): A variable buffer that has the following formats depending upon the Type field defined earlier.

▪ NFS_SPECFILE_CHR and NFS_SPECFILE_BLK: The DataBuffer field contains two 16-bit integers that represent major and minor device numbers.

Changed to:

Type (8 bytes): A 64-bit unsigned integer value describing the type and format of the data stored in the DataBuffer field. The valid values for this field are:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>NFS_SPECFILE_CHR
0x0000000000524843</td><td>Indicates that the DataBuffer field has two 32–bit integers that contain the major and minor device numbers for the character special device created by the Network File System client.</td></tr>
<tr><td>NFS_SPECFILE_BLK
0x00000000004b4c42</td><td>Indicates that the DataBuffer field has two 32–bit integers that contain the major and</td></tr>
</table>
</td></tr>
</table>

Errata Published *	Description
	<table><tr><td></td><td>minor device numbers for the character special device created by the Network File System client.</td></tr><tr><td>…</td><td>…</td></tr></table> … **DataBuffer (variable):** A variable buffer that has the following formats depending upon the **Type** field defined earlier. ▪ NFS_SPECFILE_CHR and NFS_SPECFILE_BLK: The DataBuffer field contains two 32-bit integers that represent major and minor device numbers.

*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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V9.0 – 2015/10/16.

Errata Published*	Description
2016/06/27	In Section 3.1.4, Message Processing Events and Sequencing Rules, updated the processing rules to clarify the server access check of FSRVP (client) caller permissions. Changed from: The server MUST enforce the following 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. Changed to: The server MUST enforce the following security measures to verify that the caller has the required permissions to execute any method: • 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. The server can perform additional implementation-specific<4> checks to verify that the caller has permission.

Errata Published*	Description
	If the caller does not have the required permissions, then the server MUST fail the call and return E_ACCESSDENIED. The details on how to determine the identity of the caller for the purpose of performing an access check are specified in [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 local administrators or backup operators group.

2016/04/04	In Section 3.1.4.2, SetContext (Opnum 1), corrected the sequence of methods that must be called from the client.
	
	Changed from:
	
	▪ Otherwise, if the requestor client address is the same as ShadowCopyClientAddress, the server MUST increment the ShadowCopyClientRetryCount.
	  ▪ If ShadowCopyClientRetryCount exceeds the implementation-specific count, the server MUST set the ContextSet to FALSE, set ShadowCopyClientAddress to NULL, and fail the call with FSRVP_E_SHADOW_COPY_SET_IN_PROGRESS.
	
	Changed to:
	
	▪ Otherwise, if the requestor client address is the same as ShadowCopyClientAddress, the server MUST process as follows:
	  ▪ Remove the ShadowCopySet if a ShadowCopySet exists in the GlobalShadowCopySetTable where ShadowCopySet.Status is not equal to "Recovered".
	  ▪ Set ContextSet to FALSE.
	  ▪ Set ShadowCopyClientAddress to NULL.
	  ▪ Increment the ShadowCopyClientRetryCount.
	  ▪ If ShadowCopyClientRetryCount exceeds the implementation-specific count, the server MUST fail the call with FSRVP_E_SHADOW_COPY_SET_IN_PROGRESS.

2016/02/08	In Section 3.1.4.3, StartShadowCopySet (Opnum 2), revised the processing rules. Changed from: … If ContextSet is FALSE, the server MUST fail the call with FSRVP_E_BAD_STATE. The server MUST stop the Message Sequence Timer specified in section 3.1.2. … Changed to: … If ContextSet is FALSE, the server MUST fail the call with FSRVP_E_BAD_STATE. If there is a ShadowCopySet in the GlobalShadowCopySetTable where ShadowCopySet.Status is not equal to "Recovered", the server MUST fail the call with FSRVP_E_SHADOW_COPY_SET_IN_PROGRESS. The server MUST stop the Message Sequence Timer specified in section 3.1.2. …
2016/01/25	In two sections, provided an explanation and context for the term "indexing". In Section 1.1, Glossary, added a new term: indexing: The process of extracting text or properties from files and storing the extracted values

Errata Published*	Description
	in an index or property cache. In Section 3.1.4.10, IsPathShadowCopied (Opnum 9), the last two bullets of the first list have been changed from: ▪ If the file store does not allow defragmentation operations, set the DISABLE_DEFRAG bit of ShadowCopyCompatibility. ▪ If the file store does not allow content index operations, the server MUST set the DISABLE_CONTENTINDEX bit of ShadowCopyCompatibility. Changed to: ▪ If the shadow copy provider does not support defragmentation operations on the file store, set the DISABLE_DEFRAG bit of ShadowCopyCompatibility. ▪ If the shadow copy provider does not support indexing (see the definition in section 1.1) on the file store, the server MUST set the DISABLE_CONTENTINDEX bit of ShadowCopyCompatibility.
2016/01/25	In two sections, removed an unnecessary Windows implementation detail. In Section 3.1.1, Abstract Data Model, the following paragraph was removed: A server implementing this RPC interface maintains the following metadata for the shadow copies created on file shares. The server persists this data in an implementation-specific configuration store in order to process the methods appropriately. In Section 3.2.1, Abstract Data Model, the following paragraph was removed: A client that interacts with the FSRVP server maintains the following metadata of the shadow copies created on file shares on the remote file server. The client persists this data in an implementation-specific configuration store.
2016/01/25	In various sections, corrected the description for the SetContext method. In Section 3.1.1.1, Global ContextSet, changed from: ContextSet: A Boolean value that, when set to TRUE, indicates that the client has set a valid context for the shadow copy operations by calling the SetContext method, as specified in section 3.1.4.2. Changed to: ContextSet: A Boolean value that, when set to TRUE, indicates that the shadow copy operation is in progress and the client has set a valid context for the shadow copy operations by calling the SetContext method, as specified in section 3.1.4.2. In Section 3.1.1.1, Global ContextSet, added the following two new ADM elements: ShadowCopyClientAddress: The IP address of the client, in a string format, that has set the context for shadow copy operation. ShadowCopyClientRetryCount: A numeric value that indicates the count of SetContext retry attempts.

Errata Published*	Description
	In Section 3.1.4.2, SetContext (Opnum 1), added a new return value and updated the processing rules: | Return value/code | Description | | 0x80042316 FSRVP_E_SHADOW_COPY_SET_IN_PROGRESS | Creation of another shadow copy set is in progress. | Changed from: If the Context parameter contains an invalid value, the server MUST fail the call with FSRVP_E_UNSUPPORTED_CONTEXT. If the Context parameter is valid, the server MUST update CurrentContext to Context, set ContextSet to TRUE, start the Message Sequence Timer (as specified in section 3.1.2) with a timeout value of 180 seconds, and return ZERO to the caller. Changed to: If the Context parameter contains an invalid value, the server MUST fail the call with FSRVP_E_UNSUPPORTED_CONTEXT. The server MUST get the requestor client address corresponding to the hBinding parameter as specified in [C706] section 2.12.1. If ContextSet is TRUE, the server MUST process as follows: ▪ If the requestor client address is not the same as ShadowCopyClientAddress, the server MUST fail the call with FSRVP_E_SHADOW_COPY_SET_IN_PROGRESS. ▪ Otherwise, if the requestor client address is the same as ShadowCopyClientAddress, the server MUST increment the ShadowCopyClientRetryCount. If ShadowCopyClientRetryCount exceeds the implementation-specific count,<5> the server MUST set the ContextSet to FALSE, set ShadowCopyClientAddress to NULL, and fail the call with FSRVP_E_SHADOW_COPY_SET_IN_PROGRESS. Otherwise, if ContextSet is FALSE, set ShadowCopyClientRetryCount to 0. The server MUST set ShadowCopyClientAddress to the retrieved requestor client address. The server MUST update CurrentContext to Context, set ContextSet to TRUE, start the Message Sequence Timer (as specified in section 3.1.2) with a timeout value of 180 seconds, and return ZERO to the caller. <5> Section 3.1.4.2: Windows Server 2012 R2 and Windows Server 2016 Technical Preview FSRVP servers set this retry attempt limit to 5. Windows Server 2012 operating system doesn't perform this verification. In Section 3.1.4.7, RecoveryCompleteShadowCopySet (Opnum 6), the last paragraph was changed from: The server MUST update ShadowCopySet.Status to "Recovered", set ContextSet to FALSE, and return ZERO to the caller. Changed to: The server MUST update ShadowCopySet.Status to "Recovered", set ContextSet to FALSE, set

Errata Published*	Description
	ShadowCopyClientAddress to NULL, and return ZERO to the caller. In Section 3.1.4.8, AbortShadowCopySet (Opnum 7), the last paragraph was changed from: The server MUST delete ShadowCopySet from GlobalShadowCopySetTable and free the ShadowCopySet object. The server MUST set ContextSet to FALSE, and return ZERO to the caller. Changed to: The server MUST delete ShadowCopySet from GlobalShadowCopySetTable and free the ShadowCopySet object. The server MUST set ContextSet to FALSE, set ShadowCopyClientAddress to NULL, and return ZERO to the caller. In Section 3.1.5, Timer Events, the first paragraph has been changed from: Message Sequence Timer elapses: When the Message Sequence Timer elapses, the server MUST delete the ShadowCopySet in the GlobalShadowCopySetTable where ShadowCopySet.Status is not equal to "Recovered", ContextSet MUST be set to FALSE, and the ShadowCopySet object MUST be freed. Changed to: Message Sequence Timer elapses: When the Message Sequence Timer elapses, the server MUST delete the ShadowCopySet in the GlobalShadowCopySetTable where ShadowCopySet.Status is not equal to "Recovered", ContextSet MUST be set to FALSE, ShadowCopyClientAddress MUST be set to NULL, and the ShadowCopySet object MUST be freed.
2015/12/11	In Section 3.1.4.12, DeleteShareMapping (Opnum 11), corrected two names - ShadowCopy.ShareMappingTable changed to ShadowCopy.ShareMappingList and ShadowCopyList.ShadowCopyList changed to ShadowCopySet.ShadowCopyList. Changed from: The server MUST delete the MappedShare from ShadowCopy.ShareMappingTable and free the MappedShare object. If ShadowCopy.ShareMappingTable is now empty, the server SHOULD remove the shadow copy for the file store identified by ShadowCopy.VolumeName and MUST delete ShadowCopy from ShadowCopySet.ShadowCopyList and free the ShadowCopy object. If the ShadowCopyList.ShadowCopyList is now empty, the server MUST remove the ShadowCopySet from GlobalShadowCopySetTable and free the ShadowCopySet object. Changed to: The server MUST delete the MappedShare from ShadowCopy.ShareMappingList and free the MappedShare object. If ShadowCopy.ShareMappingList is now empty, the server SHOULD remove the shadow copy for the file store identified by ShadowCopy.VolumeName and MUST delete ShadowCopy from ShadowCopySet.ShadowCopyList and free the ShadowCopy object.

Errata Published*	Description
	If the ShadowCopySet.ShadowCopyList is now empty, the server MUST remove the ShadowCopySet from GlobalShadowCopySetTable and free the ShadowCopySet object.

*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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V21.0 – 2015/10/16.

Errata Published*	Description
2016/03/07	The registry keys described in the table in Section 2.2.1.10.4 apply to both Internet Explorer 10 and Internet Explorer 11. The section title was changed from: Internet Explorer 10 Registry Keys Changed to: Internet Explorer 10 and Internet Explorer 11 Registry Keys

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-GPOL]: Group Policy: Core Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-ICPR]: ICertPassage Remote Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V18.0 – 2015/10/16.

Errata Published*	Description
2015/11/09	In Section 2.2, Common Data Types, changed from: This protocol specification makes use of the BYTE, wchar_t, and DWORD datatypes defined in [MS-DTYP] sections 2.2.6, 2.1.6, and 2.2.9. Changed to: This protocol specification makes use of the wchar_t and DWORD datatypes defined in [MS-DTYP] sections 2.1.6 and 2.2.9. In Section 3.2.4.1.1, CertServerRequest (Opnum 0), changed from: [in] const handle_t h, Changed to: [in] handle_t h, In Section 6, Appendix A: Full IDL, removed the following lines: // basic type aliases typedef byte BYTE;

* Date format: YYYY/MM/DD

[MS-IKEE]: Internet Key Exchange Protocol Extensions

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

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

RSS
Atom

Errata below are for Protocol Document Version V23.0 – 2015/10/16.

Errata Published*	Description
2016/01/25	In the sections listed below, corrected the bit/field names 'Fragment ID', 'Fragment Number', 'Fragment Data' and 'Payload Length' to 'Fragment_ID', 'Fragment_Number', 'Fragment_Data' and 'Payload_Length': 2.2.1 NAT-T Payload Types 2.2.3.1 Fragment Payload Packet 3.3.1 Abstract Data Model 3.3.5.3 Receiving Other IKE Messages In addition, in Section 3.3.6.1 Expiration of Fragmentation Timer, added information that specifies how the Fragment payload header values are set. In Section 2.2.1, NAT-T Payload Types, changed from: Each ISAKMP message consists of a header and a variable number of payloads, each identified by a 1-octet payload type value in its Payload Type field, as specified in [RFC2408] section 3.1. Changed to: Each ISAKMP message consists of a header and a variable number of payloads, each identified by a 1-octet payload type value in its Next Payload field, as specified in [RFC2408] section 3.1. In Section 2.2.3.1, Fragment Payload Packet, changed from: … Fragment_ID (2 bytes): The Fragment ID field is 2 bytes that MUST specify the same value for every fragment that is generated from a particular IKE message. Fragment_Number (1 byte): The Fragment Number field MUST indicate the order in which the fragments are sent. ... Flags (1 byte): The flag field MUST have the following value. ... Fragment_Data (variable): The Fragment Data field MUST contain the fragment. The size of the Fragment Data field MUST be computed by subtracting the size of the Fragment Payload header (8 bytes) from the value of the Payload Length field.

Errata Published*	Description
	Changed to: ... Fragment_ID (2 bytes): This field is 2 bytes and contains the fragment ID. It MUST specify the same value for every fragment that is generated from a particular IKE message. Fragment_Number (1 byte): This field MUST indicate the order in which the fragments are sent. ... Flags (1 byte): The Flags field MUST have the following value. ... Fragment_Data (variable): This field MUST contain the fragment data. The size of the Fragment_Data field MUST be computed by subtracting the size of the Fragment payload header (8 bytes) from the value of the Payload_Length field. In Section 3.3.1, Abstract Data Model, changed from: ... ▪ A Flag that indicates if this fragment is the last one (that is, the Last Fragment bit is set in the Fragment payload). ... Changed to: ... ▪ A Flag that indicates whether this fragment is the last one (that is, the LAST_FRAGMENT bit is set in the Fragment payload). ... In Section 3.3.5.3, Receiving Other IKE Messages, changed from: ... The host MUST then check whether all Fragment payloads for this Fragment ID have been received (that is, whether Fragment payloads that have a Fragment number from 1 to n have been received, and fragment n has the Last Fragment flag set). The host MUST silently discard all Fragment payloads for this Fragment ID if any of the following error conditions occur: ▪ More than one Fragment payload has the Last Fragment flag set. ▪ A Fragment payload has been received with a Fragment number greater than the Fragment number of the fragment with the Last Fragment flag set. ... Changed to: ... The host MUST then check whether all Fragment payloads for this Fragment ID have been received (that is, whether Fragment payloads that have a Fragment number from 1 to n have

Errata Published*	Description
	been received, and fragment n has the Flags field set to LAST_FRAGMENT). The host MUST silently discard all Fragment payloads for this Fragment ID if any of the following error conditions occur: ▪ More than one Fragment payload has the Flags field set to LAST_FRAGMENT. ▪ A Fragment payload has been received with a Fragment number greater than the Fragment number of the fragment with the Flags field set to LAST_FRAGMENT. ... In Section 3.3.6.1, Expiration of Fragmentation Timer, changed from: ... ▪ For each fragment, a message MUST be constructed as follows: ▪ The ISAKMP header of the original IKE message has the Next Payload field set to the Fragment payload and the Encrypted flag cleared (as specified in [RFC2408] section 3.1). ▪ The Fragment payload header has the Fragment ID set to the current value of the Fragment ID counter, the Fragment number set to the current Fragment number, and the Last Fragment flag set to Fragment number n. ... Changed to: ... ▪ For each fragment, a message MUST be constructed as follows: ▪ The ISAKMP header of the original IKE message has the Next Payload field set to the Fragment payload and the Encrypted flag cleared (as specified in [RFC2408] section 3.1). ▪ The Fragment payload header has the following values set: ▪ The Fragment ID is set to the current value of the Fragment ID counter ADM element. ▪ The Fragment number is set to the current Fragment number, which starts at 1 and is incremented for each fragment, ▪ The Flags field is set to LAST_FRAGMENT in Fragment number n.
2016/01/25	In Section 3.12.1, Abstract Data Model, changed the flag value in the InboundPacketTimeStamp dead-peer detection ADM data element from "NLB present" to "Fast Failover". Changed from: InboundPacketTimeStamp: 1 octet, type: unsigned integer. A time stamp field present if the SA

Errata Published*	Description
	has the NLB present flag described in section 3.5.1 Changed to: InboundPacketTimeStamp: 1 octet, type: unsigned integer. A time stamp field that is present if the SA has the Fast Failover flag set as described in section 3.5.1.

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V5.0 – 2015/10/16.

Errata Published*	Description
2015/11/23	In several subsections in Section 2.2, Common Message Syntax, corrected the names of various fields. In Section 2.2.4.146, DhcpScopeObjectSpecificEnumerationParameters: Added the following description for field "RecordIds": RecordIds: Specifies the unique identifier for the data in the IPAM data store. In Section 2.2.4.188, DnsResourceRecordDataAtma: Corrected the name of the "addressType" field in the description to "_addressType" to match the code. In Section 2.2.4.196, DnsResourceRecordDataPtr: Corrected the name of the "HostName" field in the description to "Hostname" to match the code. In Section 2.2.4.278, IpamIPv4Address: Corrected the name of the "ClientId" field in the description to "ClientID" to match the code. In Section 2.2.4.297, IPBlockDataFormatter, and Section 2.2.4.309, IPRangeDataFormatter: Corrected the name of the "NetworkId" field in the description to "NetwordkId" to match the code. In Section 2.2.4.301, IPRange: Corrected the name of the "NumberofChildAddresses" field in the description to "NumberOfChildAddresses" to match the code. In Section 2.2.4.389, ServerRole: Corrected the name of the "ServerStatus" field in the description to "ServiceStatus" to match the code. In Section 2.2.5.5, BuiltInCustomField: Corrected the name of the enum field "Region" in the table to "RegionLegacy" to match the code. In Section 2.2.5.41, DnsResourceRecordType: Corrected the name of the enum field "None" in the table to "NONE" to match the code.

Errata Published*	Description
	In Section 2.2.5.66, ipam1:DnsZoneStatus: Corrected the name of the enum field "ShutDown" in the table to "Shutdown" to match the code. In Section 2.2.5.67, ipam1:IpamExceptionId: Corrected the name of the enum field "IpamWmiInvalidManagedObject" in the table to "IpamwmiInvalidManagedObject" to match the code. Corrected the name of the enum field "IpamApiUserDoesNotHavePermissionToEditIPAddreses" in the table to "IpamApiUserDoesNotHavePermissionToEditIPAddress" to match the code. In Section 2.2.5.75, IpamObjectType: Corrected the name of the enum field "IPv4Adress" in the table to "IPv4Address" to match the code. Corrected the name of the enum field "DHCPSuperscopeV4" in the table to "DHCPSuperscopev4" to match the code.

*Date format: YYYY/MM/DD

[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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V31.0 – 2015/10/16.

Errata Published*	Description
2016/06/13	In two sections, updated text to indicate that KILE key version numbers are encoded and decoded as signed 32-bit integers. In Section 3.1.1, Abstract Data Model, removed the following line: KILE key version numbers (as defined in [RFC4120] section 5.2.9) are signed 32-bit integers. In Section 3.1.5.8, Key Version Numbers, changed from: KILE key version numbers (as defined in [RFC4120] section 5.2.9) are unsigned 32-bit integers. Changed to: KILE key version numbers (as defined in [RFC4120] section 5.2.9) are encoded and decoded as signed 32-bit integers.
2016/01/25	In Section 3.3.5.5, Determining Authentication Policy Setting, the Boolean value for the inspection of the BelongsToSilo field when the accound does not belong to a Silo was revised from TRUE to FALSE. Changed from: ▪ If the account does not belong to a Silo (BelongsToSilo == TRUE (section 3.3.5.4)) and AssignedPolicy (section 3.3.1.1) is NULL, the KDC SHOULD set PolicyName to NULL and Enforced to FALSE. ▪ If the account does not belong to a Silo (BelongsToSilo == TRUE (section 3.3.5.4)) and the AssignedPolicy is not NULL, the KDC SHOULD set PolicyName to AssignedPolicy.RDN, Enforced to AssignedPolicy.msDS-AuthNPolicyEnforced, and when the account is of type: Changed to: ▪ If the account does not belong to a Silo (BelongsToSilo == FALSE (section 3.3.5.4)) and AssignedPolicy (section 3.3.1.1) is NULL, the KDC SHOULD set PolicyName to NULL and Enforced to FALSE. ▪ If the account does not belong to a Silo (BelongsToSilo == FALSE (section 3.3.5.4)) and the AssignedPolicy is not NULL, the KDC SHOULD set PolicyName to AssignedPolicy.RDN, Enforced to AssignedPolicy.msDS-AuthNPolicyEnforced, and when the account is of type:

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td></td></tr>
<tr><td>2016/01/25</td><td>
In an existing section, added the sAMAccountName attribute to the user schema class and added two new sections for Server Principal Lookup and Client Principal Lookup.

In Section 2.3, Directory Service Schema Elements, changed from:
<table>
<tr><th>Class</th><th>Attribute</th></tr>
<tr><td>trustedDomain</td><td>msDS-SupportedEncryptionTypes</td></tr>
<tr><td>user</td><td>logonHours
msDS-SupportedEncryptionTypes
servicePrincipalName
userAccountControl
userPrincipalName</td></tr>
</table>
Changed to:
<table>
<tr><th>Class</th><th>Attribute</th></tr>
<tr><td>trustedDomain</td><td>msDS-SupportedEncryptionTypes</td></tr>
<tr><td>user</td><td>logonHours
msDS-SupportedEncryptionTypes
servicePrincipalName
userAccountControl
userPrincipalName
sAMAccountName</td></tr>
</table>
Added new Section 3.3.5.1.1, Server Principal Lookup, and new Section 3.3.5.6.1, Client Principal Lookup.

3.3.5.1.1 Server Principal Lookup
This section is relevant only for KILE implementations that use Active Directory for the account database.
Note Some of the data types in the following procedures are defined in [RFC4120] section 5.2.
If the Name Type ([RFC4120] section 6.2) is NT-PRINCIPAL, NT-SRV-HST, or NT-SRV-INST, then the KDC SHOULD:

1. If the KerberosString[0] element of name-string of the PrincipalName is "krbtgt" and there are only two KerberosString elements in name-string, then call GetUserLogonInfoByAttribute ([MS-ADTS] section 3.1.1.13.6) where:
▪ SearchKey is set to KerberosString[1].
▪ Attribute is set to the sAMAccountName attribute ([MS-ADA3] section 2.222).
2. Otherwise:
1. Call GetUserLogonInfoByAttribute where:
▪ SearchKey is set to KerberosString[0] + "/" + the concatenation of the remaining KerberosString elements in order.
</td></tr>
</table>

Errata Published*	Description
	▪ *Attribute* is set to the **userPrincipalName** attribute ([MS-ADA3] section 2.349). 2. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned ([MS-ERREF] section 2.3.1) and there is only one KerberosString element in name-string, then: 1. Call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to KerberosString[0]. ▪ *Attribute* is set to **sAMAccountName**. 2. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to KerberosString[0] + "$". ▪ *Attribute* is set to **sAMAccountName**. 3. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then the KDC MUST return KDC_ERR_S_PRINCIPAL_UNKNOWN ([RFC4120] section 7.5.9). If the Name Type ([RFC4120] section 6.2) is NT-ENTERPRISE, then the KDC SHOULD: 1. Set local variable *UPNServerName* to the contents of the **sname** field of the request before the @ character. 2. If there is only one KerberosString element in name-string, then call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to KerberosString[0]. ▪ *Attribute* is set to the **servicePrincipalName** element. 3. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to *UPNServerName*. ▪ *Attribute* is set to **sAMAccountName**. 4. If ERROR_SUCCESS is returned and the account has no SPNs registered, then the KDC MUST return KDC_ERR_S_PRINCIPAL_UNKNOWN. 5. Or if STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to *UPNServerName* + "$". ▪ *Attribute* is set to **sAMAccountName**. 6. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then the KDC MUST return KDC_ERR_S_PRINCIPAL_UNKNOWN. In all cases, if the call succeeds, the Active Directory account for the requested principal was found. **3.3.5.6.1 Client Principal Lookup** This section is relevant only for KILE implementations that use Active Directory for the account database. If the Name Type ([RFC4120] Section 6.2) is NT-PRINCIPAL, then the KDC SHOULD: 1. If the **realm** field is not present in the request or is the DC's domain name, call

Errata Published*	Description
	GetUserLogonInfoByAttribute ([MS-ADTS] section 3.1.1.13.6) where: ▪ *SearchKey* is set to the **cname** field of the request. ▪ *Attribute* is set to the **sAMAccountName** attribute ([MS-ADA3] section 2.222). 2. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned ([MS-ERREF] section 2.3.1), then if **realm** is not present or is the DC's domain name, call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to **cname** + "$". ▪ *Attribute* is set to **sAMAccountName**. 3. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then call GetUserLogonInfoByUPNOrAccountName ([MS-ADTS] section 3.1.1.13.7) where *UPNOrName* is set to: ▪ If **realm** is present, cname@realm. ▪ Otherwise, cname@DC's domain name. 4. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned and: ▪ If no preauthentication data was provided, then call IDL_DRSCrackNames ([MS-DRSR] section 4.1.4) where: ▪ **pmsgIn.dwFlags** is set to GC and TR. ▪ **pmsgIn.formatOffered** is set to DS_USER_PRINCIPAL_NAME_AND_ALTSECID. ▪ **pmsgIn.cNames** is set to 1. ▪ **pmsgIn.rpNames** is set to: ▪ If **realm** is present, cname@realm. ▪ Otherwise, cname@DC's domain name. ▪ If preauthentication data was provided, then call IDL_DRSCrackNames where: ▪ **pmsgIn.dwFlags** is set to GC and TR. ▪ **pmsgIn.formatOffered** is set to DS_USER_PRINCIPAL_NAME. ▪ **pmsgIn.cNames** is set to 1. ▪ **pmsgIn.rpNames** is set to: ▪ If **realm** is present, cname@realm. ▪ Otherwise, cname@DC's domain name. 5. If DS_NAME_ERROR_NOT_FOUND is returned ([MS-DRSR] section 4.1.4.1.8), then the KDC MUST return KDC_ERR_C_PRINCIPAL_UNKNOWN ([RFC4120] section 7.5.9). If the Name Type is NT-ENTERPRISE, then the KDC SHOULD: 1. Set local variable *UPNClientName* to the contents of **cname** before the @ character. 2. Set local variable *UPNDomainName* to the contents of **cname** after the @ character. 3. Call GetUserLogonInfoByUPNOrAccountName where *UPNOrName* is set to **cname**.

Errata Published*	Description
	4. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned and *UPNDomainName* is the same as the DC's domain name, then call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to *UPNClientName*. ▪ *Attribute* is set to **sAMAccountName**. 5. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned and *UPNDomainName* is the same as the DC's domain name, then call GetUserLogonInfoByAttribute where: ▪ *SearchKey* is set to *UPNClientName* + "$". ▪ *Attribute* is set to **sAMAccountName**. 6. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned and: ▪ If no preauthentication data was provided, then call IDL_DRSCrackNames where: ▪ **pmsgIn.dwFlags** is set to GC and TR. ▪ **pmsgIn.formatOffered** is set to DS_USER_PRINCIPAL_NAME_AND_ALTSECID. ▪ **pmsgIn.cNames** is set to 1. ▪ **pmsgIn.rpNames** is set to **cname**. ▪ If preauthentication data was provided, then call IDL_DRSCrackNames where: ▪ **pmsgIn.dwFlags** is set to GC and TR. ▪ **pmsgIn.formatOffered** is set to DS_USER_PRINCIPAL_NAME. ▪ **pmsgIn.cNames** is set to 1. ▪ **pmsgIn.rpNames** is set to **cname**. 7. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned, then the KDC MUST return KDC_ERR_C_PRINCIPAL_UNKNOWN. In all cases, if the call succeeds, the Active Directory account for the requested principal was found.

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V38.0 – 2015/10/16.

Errata Published*	Description
2016/04/22	In several sections, added new information for security bulletin [MSKB-3149090]. In Section 1.2.1, Normative References, added a new reference: [MSKB-3149090] Microsoft Corporation, "MS16-047: Description of the security update for SAM and LSAD remote protocols", April 2016, https://support.microsoft.com/en-us/kb/3149090. In Section 2.1, Transport, changed from: … The responder MAY use the RPC-provided security-support-provider mechanisms as specified in [MS-RPCE] section 3.2.1.4.1.1.<4> Cryptographic operations (as specified in section 5.1) MUST utilize a session key obtained from the SMB session on the client or server. … Changed to: … The responder MAY use the RPC-provided security-support-provider mechanisms as specified in [MS-RPCE] section 3.2.1.4.1.1.<4> The server SHOULD<5> reject calls that do not use an authentication level of RPC_C_AUTHN_LEVEL_NONE, RPC_C_AUTHN_LEVEL_PKT_INTEGRITY, or RPC_C_AUTHN_LEVEL_PKT_PRIVACY ([MS-RPCE] section 2.2.1.1.8). Cryptographic operations (as specified in section 5.1) MUST utilize a session key obtained from the SMB session on the client or server. … <5> Section 2.1: Servers running Windows 2000, Windows XP, and Windows Server 2003 accept calls at any authentication level. Without [MSKB-3149090] installed, servers running Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10 v1507 operating system, or Windows 10 v1511 operating system also accept calls at any authentication level.

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V26.0 – 2015/10/16.

Errata Published*	Description
2016/04/22	In several sections, added new information for security bulletin [MSKB-3149090]. In Section 1.2.1, Normative References, added a new reference: [MSKB-3149090] Microsoft Corporation, "MS16-047: Description of the security update for SAM and LSAD remote protocols", April 2016, https://support.microsoft.com/en-us/kb/3149090. In Section 2.1, Transport, changed from: … RPC clients for this protocol MUST use RPC over SMB for the LsarOpenPolicy2, LsarOpenPolicy, LsarClose, LsarGetUserName, LsarLookupNames, LsarLookupNames2, LsarLookupNames3, LsarLookupSids, and LsarLookupSids2 methods. RPC clients MUST use RPC over TCP/IP for the LsarLookupNames4 and LsarLookupSids3 methods.<3> This protocol MUST use the UUID and version number as follows: … Changed to: … RPC clients for this protocol MUST use RPC over SMB for the LsarOpenPolicy2, LsarOpenPolicy, LsarClose, LsarGetUserName, LsarLookupNames, LsarLookupNames2, LsarLookupNames3, LsarLookupSids, and LsarLookupSids2 methods. RPC clients MUST use RPC over TCP/IP for the LsarLookupNames4 and LsarLookupSids3 methods.<3> The server SHOULD<4> reject calls that do not use an authentication level of RPC_C_AUTHN_LEVEL_NONE, RPC_C_AUTHN_LEVEL_PKT_INTEGRITY, or RPC_C_AUTHN_LEVEL_PKT_PRIVACY ([MS-RPCE] section 2.2.1.1.8). This protocol MUST use the UUID and version number as follows: … <4> Section 2.1: Servers running Windows 2000, Windows XP, and Windows Server 2003 accept calls at any authentication level. Without [MSKB-3149090] installed, servers running Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10 v1507 operating system, or Windows 10 v1511 operating system also accept calls at any authentication level.

* Date format: YYYY/MM/DD

[MS-MDE]: Mobile Device Enrollment Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V5.0 – 2015/10/16.

Errata Published*	Description
2016/04/18	In Section 3.2, Interaction with Security Token Service (STS), changed the description of the security token in wresult to remove any discussion of encoding. Changed from: The security token value is the base64-encoded string "http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd#base64binary" contained in the <wsse:BinarySecurityToken> EncodingType attribute (section 3.3.) Changed to: The security token in wresult is later passed back in <wsse:BinarySecurityToken> (section 3.3).

* 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

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V5.0 – 2015/10/16.

Errata Published*	Description
2016/02/22	In Section 2.1, Transport, modified a note to clarify where additional detail on GenericAlert can be found in [OMA-DMP1.2.1]. Changed from: ▪ The MDM server validates the signature, and time stamp using a device identity certificate. It ensures the device's client identity certificate is valid (issued by MDM at enrollment time), the time is valid (optional), and the signature is valid and trusted by the MDM server as of today. Note 5: The MDM-GenericAlert is a custom header that hosts one or more alert information provided in the http messages sent by the device to the server during an OMA DM session<5>. The generic alert is sent if the session is triggered by the device due to one or more critical or fatal alerts. Here is alert format: MDM-GenericAlert: <AlertType1><AlertType2> If present, the MDM-GenericAlert is presented in every outgoing MDM message in the same OMA DM session. For more information about generic alerts, see section 8.7 in [OMA-DMP1.2.1]. … Changed to: ▪ The MDM server validates the signature, and time stamp using a device identity certificate. It ensures the device's client identity certificate is valid (issued by MDM at enrollment time), the time is valid (optional), and the signature is valid and trusted by the MDM server as of today. Note 5: The MDM-GenericAlert is a custom HTTP header that hosts one or more OMA DM genericalert information provided in the http messages sent by the device to the server during an OMA DM session<5>. This custom HTTP header is sent if the DM session is triggered by the device due to one or more critical or fatal alerts, e.g. when value of Mark property of generic alert is fatal or critical. Here is this custom HTTP header format: MDM-GenericAlert: <AlertType1><AlertType2> Only Type property of generic alert is presented in the header. Each generic alert's Type information is delimited with <>. If present, the MDM-GenericAlert header is presented in every outgoing MDM message in the same OMA DM session. For more information about generic alerts and its format, see section 8.7 in [OMA-DMP1.2.1].

* Date format: YYYY/MM/DD

[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.

RSS
Atom

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

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

Errata Published*	Description
2016/05/16	In Section 2.2.3, wsignin1.0 Request Message, updated the name of query parameter ClientRequestID to client-request-id. Changed from: … - ClientRequestID (optional): This value is a string that is used to specify a request identifier that is used when logging events, including errors or failures that occur while processing the request.<16> <16> Section 2.2.3: The ClientRequestID parameter is not supported on Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012. … Changed to: … - client-request-id (optional): This value is a string that is used to specify a request identifier that is used when logging events, including errors or failures that occur while processing the request.<16> <16> Section 2.2.3: The client-request-id parameter is not supported on Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012. …

*Date format: YYYY/MM/DD

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V27.0 – 2015/10/16.

Errata Published*	Description

2016/06/27	In various sections, indicated that ClientChallenge is defined in section 3.3.2 and updated code snippets with ChallengeFromClient.
	
	In Section 2.2.2.4, LMv2_RESPONSE, changed from:
	
	ChallengeFromClient (8 bytes): An 8-byte array of unsigned char that contains the client's ClientChallenge, as defined in section 3.1.5.1.2.
	
	Changed to:
	ChallengeFromClient (8 bytes): An 8-byte array of unsigned char that contains the client's ClientChallenge (as defined in section 3.3.2). See section 3.1.5.1.2 for details.
	
	In Section 2.2.2.7, LMv2_RESPONSE, changed from:
	
	ChallengeFromClient (8 bytes): An 8-byte array of unsigned char that contains the client's ClientChallenge (section 3.1.5.1.2).
	
	Changed to:
	ChallengeFromClient (8 bytes): An 8-byte array of unsigned char that contains the client's ClientChallenge (as defined in section 3.3.2). See section 3.1.5.1.2 for details.
	
	In Section 3.1.5.1.2, Client Receives a CHALLENGE_MESSAGE from the Server, changed from:
	
	`ComputeResponse(CHALLENGE_MESSAGE.NegotiateFlags, ResponseKeyNT, ResponseKeyLM, CHALLENGE_MESSAGE.ServerChallenge, AUTHENTICATE_MESSAGE.ClientChallenge, Time, CHALLENGE_MESSAGE.TargetInfo)`
	
	Changed to:
	`ComputeResponse(CHALLENGE_MESSAGE.NegotiateFlags, ResponseKeyNT, ResponseKeyLM, CHALLENGE_MESSAGE.ServerChallenge,`

Errata Published*	Description

	ChallengeFromClient, Time,
	CHALLENGE_MESSAGE.TargetInfo)
	
	In Section 3.2.5.1.2, Server Receives an AUTHENTICATE_MESSAGE from the Client, changed from:
	
	-- Time - Temporary variable used to hold the 64-bit current time in
	the AUTHENTICATE_MESSAGE.ClientChallenge, in the format of a
	FILETIME as defined in [MS-DTYP] section 2.3.1.
	
	Changed to:
	
	-- Time - Temporary variable used to hold the 64-bit current time from the
	NTLMv2_CLIENT_CHALLENGE.Timestamp, in the format of a
	FILETIME as defined in [MS-DTYP] section 2.3.1.
	-- ChallengeFromClient – Temporary variable to hold the client's 8-byte
	challenge, if used.
	
	Changed from:
	
	Set ExpectedNtChallengeResponse, ExpectedLmChallengeResponse,
	SessionBaseKey to ComputeResponse(NegFlg, ResponseKeyNT,
	ResponseKeyLM, CHALLENGE MESSAGE.ServerChallenge,
	AUTHENTICATE_MESSAGE.ClientChallenge, Time, ServerName)
	Set KeyExchangeKey to KXKEY(SessionBaseKey,
	AUTHENTICATE_MESSAGE.LmChallengeResponse,
	CHALLENGE_MESSAGE.ServerChallenge)
	If (AUTHENTICATE_MESSAGE.NtChallengeResponse !=
	ExpectedNtChallengeResponse)
	If (AUTHENTICATE_MESSAGE.LmChallengeResponse !=
	ExpectedLmChallengeResponse)
	Retry using NIL for the domain name: Retrieve the ResponseKeyNT
	and ResponseKeyLM from the local user account database using
	the UserName specified in the AUTHENTICATE_MESSAGE and
	NIL for the DomainName.
	Set ExpectedNtChallengeResponse, ExpectedLmChallengeResponse,
	SessionBaseKey to ComputeResponse(NegFlg, ResponseKeyNT,
	ResponseKeyLM, CHALLENGE_MESSAGE.ServerChallenge,
	AUTHENTICATE_MESSAGE.ClientChallenge, Time, ServerName)
	
	Changed to:
	
	If AUTHENTICATE_MESSAGE.NtChallengeResponseFields.NtChallengeResponseLen > 0x0018
	Set ChallengeFromClient to NTLMv2_RESPONSE.NTLMv2_CLIENT_CHALLENGE.ChallengeFromClient
	ElseIf NTLMSSP_NEGOTIATE_EXTENDED_SESSIONSECURITY is set in NegFlg
	Set ChallengeFromClient to LM_RESPONSE.Response[0..7]
	Else
	Set ChallengeFromClient to NIL
	EndIf
	Set ExpectedNtChallengeResponse, ExpectedLmChallengeResponse,
	SessionBaseKey to ComputeResponse(NegFlg, ResponseKeyNT,

Errata Published*	Description

	ResponseKeyLM, CHALLENGE MESSAGE.ServerChallenge,
	ChallengeFromClient, Time, ServerName)
	Set KeyExchangeKey to KXKEY(SessionBaseKey,
	AUTHENTICATE_MESSAGE.LmChallengeResponse,
	CHALLENGE_MESSAGE.ServerChallenge)
	If (AUTHENTICATE_MESSAGE.NtChallengeResponse !=
	ExpectedNtChallengeResponse)
	If (AUTHENTICATE_MESSAGE.LmChallengeResponse !=
	ExpectedLmChallengeResponse)
	Retry using NIL for the domain name: Retrieve the ResponseKeyNT
	and ResponseKeyLM from the local user account database using
	the UserName specified in the AUTHENTICATE_MESSAGE and
	NIL for the DomainName.
	Set ExpectedNtChallengeResponse, ExpectedLmChallengeResponse,
	SessionBaseKey to ComputeResponse(NegFlg, ResponseKeyNT,
	ResponseKeyLM, CHALLENGE_MESSAGE.ServerChallenge,
	ChallengeFromClient, Time, ServerName)

2016/06/27	In Section 2.2.1.2, CHALLENGE_MESSAGE, added a product behavior note to describe product specific behavior for the TargetInfoFields field. Changed from: TargetInfoFields (8 bytes): A field containing TargetInfo information. The field diagram for TargetInfoFields is as follows. … If the NTLMSSP_NEGOTIATE_TARGET_INFO flag is not clear in NegotiateFlags, indicating that TargetInfo is required, the fields are set to the following values: … Changed to: TargetInfoFields (8 bytes): A field containing TargetInfo information. The field diagram for TargetInfoFields is as follows. … If the NTLMSSP_NEGOTIATE_TARGET_INFO flag is not clear in NegotiateFlags, indicating that TargetInfo is required, the fields are set to the following values:<7> <7> Section 2.2.1.2: In Windows Vista and subsequent versions of Windows according to the applicability list at the beginning of this section, the TargetInfo field is always sent. …
2016/01/25	In three sections, updated references and links. In Section 3.4.2, Message Integrity, changed from: -- MAC() - Defined in section 3.4.3. Changed to: -- MAC() - Defined in sections 3.4.4.1 and 3.4.4.2. In Section 3.4.6.1, Signature Creation for GSS_WrapEx(), changed from:

Errata Published*	Description
	Section 3.4.3 describes the algorithm used by GSS_WrapEx() to create the signature. Changed to: Section 3.4.2 describes the algorithm used by GSS_WrapEx() to create the signature. In Section 4.2.3.4, GSS_WrapEx Examples, changed from: The output message data and signature is created using SEAL() specified in section 3.4.4. Changed to: The output message data and signature is created using SEAL() specified in section 3.4.3.
2015/11/09	In various sections, corrected text that implies MaxLifetime applies to versions later than Windows XP. In Section 3.1.1.1, Variables Internal to the Protocol, changed from: MaxLifetime: An integer that indicates the maximum lifetime for challenge/response pairs <35> <35> In Windows NT 4.0 and Windows 2000, the maximum lifetime for the challenge is 30 minutes. In Windows XP and subsequent versions of Windows, according to the applicability list at the beginning of this section, the maximum lifetime is 36 hours. Changed to: MaxLifetime: An integer that indicates the maximum lifetime for challenge/response pairs <35> <35> In Windows NT 4.0 and Windows 2000, the maximum lifetime for the challenge is 30 minutes. In Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2, the maximum lifetime is 36 hours. In Section 3.2.5.1.2, Server Receives an AUTHENTICATE_MESSAGE from the Client, changed from: If NTLM v2 authentication is used and the AUTHENTICATE_MESSAGE.NtChallengeResponse.TimeStamp (section 2.2.2.7) is more than MaxLifetime (section 3.1.1.1) difference from the server time, then the server SHOULD return a failure.<64> <64> Supported by Windows NT, Windows 2000, and Windows XP. Changed to: If NTLM v2 authentication is used and the AUTHENTICATE_MESSAGE.NtChallengeResponse.TimeStamp (section 2.2.2.7) is more than MaxLifetime (section 3.1.1.1) difference from the server time, then the server SHOULD return a failure.<64> <64> Supported by Windows NT 4.0, Windows 2000, Windows XP, Windows Server 2003,

Errata Published*	Description
	Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2. In Section 3.2.5.2.2, Server Response Checking, changed from: If NTLM v2 authentication is used and the AUTHENTICATE_MESSAGE.NtChallengeResponse.TimeStamp (section 2.2.2.7) is more than MaxLifetime (section 3.1.1.1) difference from the server time, then the server SHOULD return a failure.<69> <69> Supported by Windows NT, Windows 2000 and Windows XP. Changed to: If NTLM v2 authentication is used and the AUTHENTICATE_MESSAGE.NtChallengeResponse.TimeStamp (section 2.2.2.7) is more than MaxLifetime (section 3.1.1.1) difference from the server time, then the server SHOULD return a failure.<69> <69> Supported by Windows NT 4.0, windows_2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2.

* Date format: YYYY/MM/DD

[MS-NRPC]: Netlogon Remote Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V32.0 – 2015/10/16.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2016/06/27</td><td>In Section 2.2.1.3.15, NL_OSVERSIONINFO_V1, VER_SUITE_DATACENTER, added product variants Windows Server 2008 R2 Datacenter and Enterprise for the VER_SUITE_DATACENTER and VER_SUITE_ENTERPRISE values and added the VER_SUITE_WH_SERVER value to the wSuiteMask member of NL_OSVERSIONINFO_V1.

Changed from:
wSuiteMask: A bit mask that identifies the product suites available on the system. This member can be a combination of the following values.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>VER_SUITE_DATACENTER
0x00000080</td><td>Windows 2000 Datacenter Server operating system, Windows Server 2003 Datacenter Edition operating system, or Windows Server 2008 Datacenter operating system is installed.</td></tr>
<tr><td>VER_SUITE_ENTERPRISE
0x00000002</td><td>Windows NT Server 4.0 operating system, Enterprise Edition, Windows 2000 Advanced Server operating system, Windows Server 2003 Enterprise Edition operating system, or Windows Server 2008 Enterprise operating system is installed.</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>
Changed to:
wSuiteMask: A bit mask that identifies the product suites available on the system. This member can be a combination of the following values.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>VER_SUITE_DATACENTER</td><td>Windows 2000 Datacenter Server operating system, Windows Server 2003 Datacenter</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>0x00000080</td><td>Edition operating system, Windows Server 2008 Datacenter operating system, or Windows Server 2008 R2 Datacenter operating system is installed.</td></tr>
<tr><td>VER_SUITE_ENTERPRISE
0x00000002</td><td>Windows NT Server 4.0 operating system, Enterprise Edition, Windows 2000 Advanced Server operating system, Windows Server 2003 Enterprise Edition operating system, Windows Server 2008 Enterprise operating system, or Windows Server 2008 R2 Enterprise operating system is installed.</td></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>VER_SUITE_WH_SERVER
0x00008000</td><td>Windows Home Server server software is installed.</td></tr>
</table>
</td></tr>
<tr><td>2016/04/18</td><td>In Section 3.5.4.4.9, NetrLogonGetDomainInfo (Opnum 29), added details to indicate the constraints against which the dNSHostName attribute is validated.

Changed from:
…
If WkstaBuffer.WorkstationInfo.WorkstationFlags has the 0x2 bit set, NETLOGON_DOMAIN_INFO.DnsHostNameInDs is set to the dNSHostName ([MS-ADA1] section 2.185) of the client account. If there was a change in domain naming, this value holds the previous DNS host name since the AD query is done prior to changing the value. If WkstaBuffer.WorkstationInfo.WorkstationFlags does not have the 0x2 bit set, the server adds the following SPNs to the ServicePrincipalName attribute of the clients account:
…

Changed to:
…
If WkstaBuffer.WorkstationInfo.WorkstationFlags has the 0x2 bit set, NETLOGON_DOMAIN_INFO.DnsHostNameInDs is set to the dNSHostName element ([MS-ADA1] section 2.185) of the client account. The dNSHostName element is validated against the constraints specified in [MS-ADTS] section 3.1.1.5.3.1.1.2. If there was a change in domain naming, this value holds the previous DNS host name since the AD query is done prior to changing the value. If WkstaBuffer.WorkstationInfo.WorkstationFlags does not have the 0x2 bit set, the server adds the following SPNs to the ServicePrincipalName attribute of the clients account:
…</td></tr>
<tr><td>2016/01/11</td><td>In two sections, updated a member of the NL_IN_CHAIN_SET_CLIENT_ATTRIBUTES_V1 structure to OsVersionInfo_V1, and removed parameter RestartState from NetrDatabaseSync to match the Full IDL section.

In Section 2.2.1.3.16, NL_IN_CHAIN_SET_CLIENT_ATTRIBUTES_V1, changed all 8 instances of "OsVersionInfo" to "OsVersionInfo_V1".

In Section 3.5.4.6.3, NetrDatabaseSync, changed from:

<pre>NTSTATUS NetrDatabaseSync(
  [in, string] LOGONSRV_HANDLE PrimaryName,
  [in, string] wchar_t* ComputerName,</pre></td></tr>
</table>

Errata Published*	Description
	[in] PNETLOGON_AUTHENTICATOR Authenticator, [in, out] PNETLOGON_AUTHENTICATOR ReturnAuthenticator, [in] DWORD DatabaseID, [in] SYNC_STATE RestartState, [in, out] ULONG * SyncContext, [out] PNETLOGON_DELTA_ENUM_ARRAY* DeltaArray, [in] DWORD PreferredMaximumLength); Changed to: NTSTATUS NetrDatabaseSync([in, string] LOGONSRV_HANDLE PrimaryName, [in, string] wchar_t* ComputerName, [in] PNETLOGON_AUTHENTICATOR Authenticator, [in, out] PNETLOGON_AUTHENTICATOR ReturnAuthenticator, [in] DWORD DatabaseID, [in, out] ULONG * SyncContext, [out] PNETLOGON_DELTA_ENUM_ARRAY* DeltaArray, [in] DWORD PreferredMaximumLength);

* Date format: YYYY/MM/DD

[MS-OAPX]: OAuth 2.0 Protocol Extensions

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

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

RSS
Atom

Errata below are for Protocol Document Version V4.0 – 2015/06/30.

Errata Published*	Description
2016/05/16	In the following sections, updated the name of query parameter ClientRequestId to client-request-id: 2.2.1.1 client-request-id 2.2.2 Common URI Parameters 2.2.2.1 resource 2.2.2.2 resource_params 2.2.2.3 ClientRequestId 2.2.2.6 nonce 2.2.2.8 max_age 2.2.2.9 id_token_hint 3.1.5.2.1 POST 3.2.5.1.1 GET 3.2.5.1.1.3 Processing Details 3.2.5.2.1 POST 3.2.5.2.1.3 Processing Details 4.1 Authorization Code Request 4.8 Authorization Code Request with nonce Parameter 4.9 Authorization Code Request with prompt Parameter 4.10 Authorization Code Request with max_age Parameter 4.11 Authorization Code Request with id_token_hint Parameter
2016/02/22	Added an example section showing the sequence of requests and responses involved in the use of a multi-resource refresh token. Newly added sections: **4.6 Access Token Request and Response – Use of Multi-Resource Refresh Token** Note: All of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as an aid to the reader. This example shows the sequence of requests and responses involved in the use of a multi-resource refresh token. **4.6.1 Authorization Code Request** Refer to [RFC6749] section 4.1.1 (Authorization Request).

Errata Published*	Description

```
GET /authorize?response_type=code&client_id=s6BhdRkqt3&state=xyz
 &resource= https:%2F%2Fresource_server
 &ClientRequestId=EC09AB2D-9655-453B-B555-3317011523E8


&resource params=eyJQcm9wZXJ0aWVzIjpbeyJLZXkiOiJhY3IiLCJWYWx1ZSI6IndpYW9ybXVsdG
lhdXRobiJ9XX
        0
 &redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb HTTP/1.1
Host: server.example.com
```

4.6.2 Authorization Code Response

Refer to [RFC6749] section 4.1.2 (Authorization Response).

```
HTTP/1.1 302 Found
Location: https://client.example.com/cb?code=SplxlOBeZQQYbYS6WxSbIA
&state=xyz
```

4.6.3 Access Token Request

Refer to [RFC6749] section 4.1.3 (Access Token Request).

```
POST /token HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded
grant_type=authorization_code&client_id=s6BhdRkqt3&code=SplxlOBeZQQYbYS6WxS
bIA&redirect_uri
=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb
```

4.6.4 Access Token Response

Refer to [RFC6749] section 5.1 (Successful Response).

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
  "access_token":"2YotnFZFEjr1zCsicMWpAA",
  "token_type":"bearer",
  "expires in":3600,
  "refresh token":"tGzv3JOkF0XG5Qx2TlKWIA"
}
```

Errata Published*	Description

	4.6.5 Access Token Request – Using Multi-Resource Refresh Token
	Refer to [RFC6749] section 4.1.3 (Access Token Request).
	
	`POST /token HTTP/1.1`
	`Host: server.example.com`
	`Content-Type: application/x-www-form-urlencoded`
	`grant_type=refresh_token&assertion=tGzv3JOkF0XG5Qx2TlKWIA&client_id=s6BhdRkqt3&code=SplxlOBeZ`
	`QQYbYS6WxSbIA&redirect uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb&resource=https:%2F%2Fres`
	`ource_server`
	
	4.6.6 Access Token Response for Multi-Resource Refresh Token Request
	Refer to [RFC6749] section 5.1 (Successful Response).
	
	`HTTP/1.1 200 OK`
	`Content-Type: application/json;charset=UTF-8`
	`Cache-Control: no-store`
	`Pragma: no-cache`
	`{`
	`"access token":"X0RJQk5FS1NESlNabFNE",`
	`"token_type":"bearer",`
	`"expires_in":3600,`
	`"refresh_token":"U0lETkRKNDMyMzRORVVE"`
	`}`

2016/02/22	In the following sections, corrected the updated link for the csr_type parameter value from http://schemas.microsoft.com/windows/**pki2009**/01/enrollment#PKCS10 to http://schemas.microsoft.com/windows/**pki/2009**/01/enrollment#PKCS10: 2.2.3 Common Data Structures 2.2.3.6 csr_type 3.1.5.2.1.1 Request Body 3.2.5.2.1.3 Processing Details 4.13.5 OAuth logon certificate Request
2016/02/22	In two sections, clarified how the token response is handled. In Section 4.7.4, Initial Access Token Response, changed from: ... In this example sequence of requests and responses, the AD FS server returns the message below in response to the request in section 4.7.3. ... Changed to: ... In this example sequence of requests and responses, the AD FS server returns the message below in response to the request in section 4.7.3. Note that because the AD FS server has not rejected the request or indicated a reduced scope via the scope response parameter, this response was

Errata Published*	Description
	granted with the "user_impersonation" scope originally requested in section 4.7.1. ... In Section 4.13.4, Initial Access Token Response, changed from: ... This message is returned by the AD FS server in response to the request shown in section 4.13.3. ... Changed to: ... This message is returned by the AD FS server in response to the request shown in section 4.13.3. Note that because the AD FS server has not rejected the request or indicated a reduced scope via the scope response parameter, this response was granted with the "logon_cert" scope originally requested in section 4.13.1. ...

2016/02/22	In Section 4.7.1, Authorization Code Request, corrected the request example by moving HTTP/1.1 to the user_impersonation scope in the initial authorization code request. In Section 4.13.1, Authorization Code Request, also corrected the request example, in this instance by moving HTTP/1.1 to the logon_cert scope in the initial authorization code request.
	
	In Section 4.7.1, Authorization Code Request, changed from:
	
	Below is the initial authorization code request made by the client. Note that the client requests the "user_impersonation" scope, because only an access token that was granted with this scope can be used later when making an OAuth on-behalf-of request.
	
	`GET /authorize?response_type=code&client_id=s6BhdRkqt3`
	`&resource=https%3A%2F%2Fresource_server1`
	`&redirect uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb HTTP/1.1`
	`&scope=user impersonation`
	`Host: server.example.com`
	
	Changed to:
	...
	Below is the initial authorization code request made by the client. Note that the client requests the "user_impersonation" scope, because only an access token that was granted with this scope can be used later when making an OAuth on-behalf-of request.
	
	`GET /authorize?response_type=code&client_id=s6BhdRkqt3`
	`&resource=https%3A%2F%2Fresource_server1`
	`&redirect uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb`
	`&scope=user_impersonation HTTP/1.1`
	`Host: server.example.com`

Errata Published*	Description

	In Section 4.13.1, Authorization Code Request, changed from:
	...
	The following message is the initial authorization code request made by the client. Note that the client requests the "logon_cert" scope, because only an access token that was granted with this scope can be used later when making an OAuth logon certificate request.
	
	`GET /authorize?response_type=code&client_id=s6BhdRkqt3`
	`  &resource=https%3A%2F%2Fresource server1`
	`  &redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb HTTP/1.1`
	`  &scope=logon cert`
	`Host: server.example.com`
	
	Changed to:
	...
	The following message is the initial authorization code request made by the client. Note that the client requests the "logon_cert" scope, because only an access token that was granted with this scope can be used later when making an OAuth logon certificate request.
	
	`GET /authorize?response type=code&client id=s6BhdRkqt3`
	`  &resource=https%3A%2F%2Fresource_server1`
	`  &redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb`
	`  &scope=logon_cert HTTP/1.1`
	`Host: server.example.com`

2016/02/22	In Section 3.2.5.2.1.3, Processing Details, clarified the condition when the AD FS server's ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher and the client is refreshing an access token. Changed from: ... ▪ If the AD FS server's ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher and the client is refreshing an access token ([RFC6749] section 6): ▪ If the client provides a resource parameter in the request and the provided refresh token is a multi-resource refresh token, the AD FS server issues the access token for the resource given in this request. Otherwise, the AD FS server returns an access token for the same resource as was specified when the refresh token was initially granted to the client. ... Changed to: ... ▪ If the AD FS server's ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher and the client is refreshing an access token ([RFC6749] section 6):

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>

If the client provides a resource parameter in the request and the provided refresh token is a multi-resource refresh token, the AD FS server issues the access token for the resource given in this request.
If the client provides a resource parameter in the request and the provided refresh token is not a multi-resource refresh token, the AD FS server SHOULD either issue an access token for the resource given in this request, or send an error response to the OAuth 2.0 client according to the requirements of [RFC6749] section 5.2 (Error Response).<3> If sending an error, the recommended value for the REQUIRED error parameter of the response is invalid_grant.
If the client does not provide a resource parameter in the request, the AD FS server returns an access token for the same resource as was specified when the refresh token was initially granted to the client.

<3> Windows implementations return an access token for the resource given in this request even if the provided refresh token is not a multi-resource refresh token.
...</td></tr>
<tr><td>2016/02/08</td><td>In Section 3.2.5.1.1, GET, added a domain_hint query parameter example to the URI.

Changed from:
...
The method can be invoked through the following URI:

<pre>/authorize?response_type={response_type}&client_id={client_id}&redirect_uri
={redirect_uri}&scope={scope}&state={state}&resource={resource}&resource_params
={resource_params}&ClientRequestId={ClientRequestId}&login_hint={login_hint}</pre>
...

Changed to:
...
The method can be invoked through the following URI:

<pre>/authorize?response_type={response_type}&client_id={client_id}&redirect_uri
={redirect_uri}&scope={scope}&state={state}&resource={resource}&resource_params
={resource_params}&ClientRequestId={ClientRequestId}&login_hint={login_hint}&do
main_hint={domain_hint}</pre></td></tr>
<tr><td>2016/02/08</td><td>In Section 2.2.3, Common Data Structures, clarified that the message body parameter x5c is optional.
Changed from:
<table>
<tr><th>Message body parameter</th><th>Description</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>x5c</td><td>The AD FS server includes this parameter in the successful response to an OAuth logon</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description
	<table><tr><td></td><td>certificate request. The value is a base64-encoded CMS certificate chain or CMC full PKI response (see [MS-WCCE] section 2.2.2.8). The AD FS server does not return this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher.</td></tr><tr><td>…</td><td>…</td></tr></table> Changed to: <table><tr><th>Message body parameter</th><th>Description</th></tr><tr><td>…</td><td>…</td></tr><tr><td>x5c</td><td>OPTIONAL. The AD FS server includes this parameter in the successful response to an OAuth logon certificate request. The value is a base64-encoded CMS certificate chain or CMC full PKI response (see [MS-WCCE] section 2.2.2.8). The AD FS server does not return this parameter unless its ad_fs_behavior_level is AD_FS_BEHAVIOR_LEVEL_2 or higher.</td></tr><tr><td>…</td><td>…</td></tr></table>

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V1.0 – 2015/10/16.

Errata Published*	Description
2016/02/22	In Section 3.2.5.1.2.3, Processing Details, updated alternateSecurityIdentifiers to altSecurityIdentities. Changed from: The server finds the msDS-Device object in Active Directory that has an alternateSecurityIdentifiers value matching the value of the x5c parameter of the request header. Changed to: The server finds the msDS-Device object in Active Directory that has an altSecurityIdentities value matching the value of the x5c parameter of the request header.
2016/02/22	In Section 3.2.5.1.2.1.2, User JWT Authentication, removed the redundant "use" fields. Changed from: assertion (REQUIRED): A signed JWT used to authenticate the user. The JWT fields for the JWT provided in the assertion field MUST be given the following values: iss (REQUIRED): The username of the user for which the primary refresh token is requested. iat (REQUIRED): See [OIDCCore] section 6.1. exp (REQUIRED): See [OIDCCore] section 6.1. use (REQUIRED): "ngc" aud (REQUIRED): The Issuer Identifier ([OIDCCore] section 1.2) of the server that the client is sending the request to. use (REQUIRED): "ngc" Changed to: assertion (REQUIRED): A signed JWT used to authenticate the user. The JWT fields for the JWT provided in the assertion field MUST be given the following values: iss (REQUIRED): The username of the user for which the primary refresh token is requested. iat (REQUIRED): See [OIDCCore] section 6.1. exp (REQUIRED): See [OIDCCore] section 6.1. aud (REQUIRED): The Issuer Identifier ([OIDCCore] section 1.2) of the server that the client is sending the request to.
2016/02/22	In Section 4.2, Obtain a Primary Refresh Token, and Section 4.3, Obtain an Access Token, corrected the example for grant_type. Changed from:

Errata Published*	Description
	grant_type=urn:ietf:params:oauth:grant-type:jwt-bearer Changed to: grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Ajwt-bearer

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-PSRDP]: PowerShell Remote Debugging Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-PSRP]: PowerShell Remoting Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V27.0 – 2015/10/16.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2015/11/09</td><td>In Section 2.2.1, PowerShell Remoting Protocol Message, corrected the name of the RUNSPACE_INIT_DATA value to RUNSPACEPOOL_INIT_DATA.

Changed from:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>RUNSPACE_INIT_DATA
0x0002100B</td><td>RunspacePool initialization data.
Direction: Server to client.
Target: RunspacePool.</td></tr>
</table>

Changed to:

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>RUNSPACEPOOL_INIT_DATA
0x0002100B</td><td>RunspacePool initialization data.
Direction: Server to client.
Target: RunspacePool.</td></tr>
</table>
</td></tr>
</table>

* Date format: YYYY/MM/DD

[MS-RA]: Remote Assistance Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-RAI]: Remote Assistance Initiation Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V27.0 – 2015/10/16.

Errata Published*	Description
2016/02/22	In Section 6, Appendix A: Remote Assistance Invitation File Format, added a description for the RCTICKETENCRYPTED value. Changed from: **Value** / **Meaning** UPLOADINFO — The UPLOADINFO TYPE is set to "Escalated". UPLOADDATA — The UPLOADDATA contains the following information: USERNAME: The name of the Remote Assistance novice computer. RCTICKET: The Remote Assistance Connection String. DtStart: The time when the Remote Assistance Connection String was created. This time is the number of seconds elapsed since UTC 1/1/70. DtLength: The duration for which the Remote Assistance Connection String is valid. This is expressed in minutes. If the expert computer cannot connect to the novice computer successfully within this time, Remote Assistance closes on the novice computer. PassStub: The encrypted novice computer's password string. When the Remote Assistance Connection String is sent as a file over email, to provide additional security, a password is used. L: Indicates whether the novice computer is connected via a modem. L = 1 means MODEM is used, 0 means high-speed connectivity is used.

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

<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>UPLOADINFO</td><td>The UPLOADINFO TYPE is set to "Escalated".</td></tr>
<tr><td>UPLOADDATA</td><td>The UPLOADDATA contains the following information:
USERNAME: The name of the Remote Assistance novice computer.
RCTICKET: The Remote Assistance Connection String.
RCTICKETENCRYPTED: Indicates whether the ticket identified by RCTICKET is encrypted. RCTICKETENCRYPTED = 1 means the ticket is encrypted, zero means the ticket is not encrypted.
DtStart: The time when the Remote Assistance Connection String was created. This time is the number of seconds elapsed since UTC 1/1/70.
DtLength: The duration for which the Remote Assistance Connection String is valid. This is expressed in minutes. If the expert computer cannot connect to the novice computer successfully within this time, Remote Assistance closes on the novice computer.
PassStub: The encrypted novice computer's password string. When the Remote Assistance Connection String is sent as a file over email, to provide additional security, a password is used.
L: Indicates whether the novice computer is connected via a modem. L = 1 means MODEM is used, 0 means high-speed connectivity is used.</td></tr>
</table></td></tr>
</table>

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V41.0 – 2016/03/02.

Errata Published*	Description
2016/05/02	In Section 2.2.1.3.2, Client Core Data (TS_UD_CS_CORE), in the keyboardLayout field description, clarified when the server should use the default active input locale identifier and active language identifier associated with the user account. Changed from: ... keyboardLayout (4 bytes): A 32-bit, unsigned integer. The active input locale identifier, also known as the "HKL" (for example, 0x00010409 for a "United States-Dvorak" keyboard layout and 0x00020418 for a "Romanian (Programmers)" keyboard layout). For a list of input locale identifiers, see [MSFT-DIL].<5> ... Changed to: ... keyboardLayout (4 bytes): A 32-bit, unsigned integer. The active input locale identifier, also known as the "HKL" (for example, 0x00010409 for a "United States-Dvorak" keyboard layout and 0x00020418 for a "Romanian (Programmers)" keyboard layout). For a list of input locale identifiers, see [MSFT-DIL].<5> If the keyboardLayout field is set to zero, then the server SHOULD use the default active input locale identifier and active language identifier (see the CodePage field in section 2.2.1.11.1.1) associated with the user account.<6> <6> Section 2.2.1.3.2: Microsoft RDP servers apply only the active locale identifier to a newly created session. The value is ignored when connecting to an existing session. ... In Section 2.2.1.11.1.1, Info Packet (TS_INFO_PACKET), in the CodePage field description, clarified when the active language identifier should be ignored by the server. Changed from: ... CodePage (4 bytes): A 32-bit, unsigned integer. If the flags field does not contain the INFO_UNICODE flag (0x00000010), then this field MUST contain the ANSI code page descriptor being used by the client (for a list of code pages, see [MSDN-CP]) to encode the character fields

Errata Published*	Description
	in the Info Packet and Extended Info Packet (section 2.2.1.11.1.1.1). However, if the flags field contains the INFO_UNICODE flag, then the CodePage field MUST contain the active language identifier in the low-word<13> (for a list of language identifiers, see [MSDN-MUI]); the contents of the high-word MUST be ignored by the server. ... Changed to: ... CodePage (4 bytes): A 32-bit, unsigned integer. If the flags field does not contain the INFO_UNICODE flag (0x00000010), then this field MUST contain the ANSI code page descriptor being used by the client (for a list of code pages, see [MSDN-CP]) to encode the character fields in the Info Packet and Extended Info Packet (section 2.2.1.11.1.1.1). However, if the flags field contains the INFO_UNICODE flag, then the CodePage field MUST contain the active language identifier in the low-word<14> (for a list of language identifiers, see [MSDN-MUI]); the contents of the high-word MUST be ignored by the server. The active language identifier SHOULD be ignored by the server if the keyboardLayout field of the Client Core Data structure (section 2.2.1.3.2) is set to zero.<15> <15> Section 2.2.1.11.1.1: Microsoft RDP servers only apply the active language identifier to a newly created session. The value is ignored when connecting to an existing session. ...
2016/04/18	In Section 2.2.1.11.1.1, Info Packet (TS_INFO_PACKET), added details to the description of the UserName field to clarify how it is affected by the value of the flags field. Changed from: UserName (variable): Variable-length logon user name of the user (the length in bytes is given by the cbUserName field). The maximum length allowed by RDP 4.0 servers is 44 bytes (including the mandatory null terminator), while all other versions of RDP servers allow a maximum length of 512 bytes (including the mandatory null terminator). The field MUST contain at least a null terminator character in Windows-1252 or Unicode format (depending on the presence of the INFO_UNICODE flag). … Changed to: UserName (variable): Variable-length logon user name of the user (the length in bytes is given by the cbUserName field). The maximum length allowed by RDP 4.0 servers is 44 bytes (including the mandatory null terminator), while all other versions of RDP servers allow a maximum length of 512 bytes (including the mandatory null terminator). The field MUST contain at least a null terminator character in Windows-1252 or Unicode format (depending on the presence of the INFO_UNICODE flag). The contents of the UserName field SHOULD be ignored if the INFO_PASSWORD_IS_SC_PIN (0x00040000) flag is specified in the flags field. …
2016/04/18	In several sections, updated with the RDP versions that send the Set Keyboard IME Status PDU and added more specific information about the fields that are used with a Fujitsu Oyayubi-specific IME control function. In Section 2.2.8.2.2, Server Set Keyboard IME Status PDU, changed from: The Set Keyboard IME Status PDU is sent by the server when the user's session employs at least one input method editor (IME) and is used to set the IME state. This PDU is accepted and ignored by non-IME aware clients. Changed to:

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>The Set Keyboard IME Status PDU is used to request that the client set the state of the input method editor (IME) and is sent by the server<31> when the user's session employs at least one IME. This PDU is accepted and ignored by non-IME-aware clients.
<31> Section 2.2.8.2.2: Only Microsoft RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, and 7.1 servers send the Set Keyboard IME Status PDU.

In Section 2.2.8.2.2.1, Set Keyboard IME Status PDU Data (TS_SET_KEYBOARD_IME_STATUS_PDU), changed from:

On RDP 5.0, 5.1, 5.2, 6.0, 6.1, 7.0, 7.1, 8.0, 8.1, 10.0, and 10.1 clients, the latter two fields are used as input parameters to a Fujitsu Oyayubi specific IME control function of East Asia IME clients.

Changed to:

The ImeState and ImeConvMode fields are used as input parameters to a Fujitsu Oyayubi-specific IME control function on Far East IME clients.</td></tr>
<tr><td>2016/04/04</td><td>In Section 2.2.7.1.1, General Capability Set (TS_GENERAL_CAPABILITYSET), added OSMAJORTYPE_CHROME_OS to the osMajorType field table.

Changed from:
...
osMajorType (2 bytes): A 16-bit, unsigned integer. The type of platform.

<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>OSMAJORTYPE_UNSPECIFIED
0x0000</td><td>Unspecified platform</td></tr><tr><td>OSMAJORTYPE_WINDOWS
0x0001</td><td>Windows platform</td></tr><tr><td>OSMAJORTYPE_OS2
0x0002</td><td>OS/2 platform</td></tr><tr><td>OSMAJORTYPE_MACINTOSH
0x0003</td><td>Macintosh platform</td></tr><tr><td>OSMAJORTYPE_UNIX
0x0004</td><td>UNIX platform</td></tr><tr><td>OSMAJORTYPE_IOS
0x0005</td><td>iOS platform</td></tr><tr><td>OSMAJORTYPE_OSX
0x0006</td><td>OS X platform</td></tr><tr><td>OSMAJORTYPE_ANDROID
0x0007</td><td>Android platform</td></tr></table>
...

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

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>...
osMajorType (2 bytes): A 16-bit, unsigned integer. The type of platform.

<table><tr><th>Value</th><th>Meaning</th></tr><tr><td>OSMAJORTYPE_UNSPECIFIED
0x0000</td><td>Unspecified platform</td></tr><tr><td>OSMAJORTYPE_WINDOWS
0x0001</td><td>Windows platform</td></tr><tr><td>OSMAJORTYPE_OS2
0x0002</td><td>OS/2 platform</td></tr><tr><td>OSMAJORTYPE_MACINTOSH
0x0003</td><td>Macintosh platform</td></tr><tr><td>OSMAJORTYPE_UNIX
0x0004</td><td>UNIX platform</td></tr><tr><td>OSMAJORTYPE_IOS
0x0005</td><td>iOS platform</td></tr><tr><td>OSMAJORTYPE_OSX
0x0006</td><td>OS X platform</td></tr><tr><td>OSMAJORTYPE_ANDROID
0x0007</td><td>Android platform</td></tr><tr><td>OSMAJORTYPE_CHROME_OS
0x0008</td><td>Chrome OS platform</td></tr></table>
...</td></tr>
<tr><td>2016/03/21</td><td>In various sections, corrected the names of fields and ENUMs and updated the description for one field.

In Section 2.2.1.1, Client X.224 Connection Request PDU, changed from:
rdpCorrelationInfo (36 bytes): An optional Correlation Info (section 2.2.1.1.2) structure. The length of this field is included in the X.224 Connection Request Length Indicator field. This field MUST be present if the CORRELATION_INFO_PRESENT (0x08) flag is set in the flags field of the RDP Negotiation Request structure, encapsulated within the optional rdpNegRsp field. If the CORRELATION_INFO_PRESENT (0x08) flag is not set, then this field MUST NOT be present.

Changed to:
rdpCorrelationInfo (36 bytes): An optional Correlation Info (section 2.2.1.1.2) structure. The length of this field is included in the X.224 Connection Request Length Indicator field. This field MUST be present if the CORRELATION_INFO_PRESENT (0x08) flag is set in the flags field of the RDP Negotiation Request structure, encapsulated within the optional rdpNegReq field. If the CORRELATION_INFO_PRESENT (0x08) flag is not set, then this field MUST NOT be present.

In Section 2.2.3.1.1, Deactivate All PDU Data (TS_DEACTIVATE_ALL_PDU), changed from:

shareControlHeader (6 bytes): Share Control Header (section 2.2.8.1.1.1.1) containing</td></tr>
</table>

Errata Published*	Description
	information about the packet. The type subfield of the pduType field of the Share Control Header MUST be set to **TS_PDUTYPE_DEACTIVATEALLPDU** (6). Changed to: shareControlHeader (6 bytes): Share Control Header (section 2.2.8.1.1.1.1) containing information about the packet. The type subfield of the pduType field of the Share Control Header MUST be set to **PDUTYPE_DEACTIVATEALLPDU** (6). In Section 2.2.4.1.1, Auto-Reconnect Status PDU Data (TS_AUTORECONNECT_STATUS_PDU), changed from: shareDataHeader (18 bytes): Share Data Header containing information about the packet. The type subfield of the pduType field of the Share Control Header (section 2.2.8.1.1.1.1) MUST be set to PDUTYPE_DATAPDU (7). The pduType2 field of the Share Data Header MUST be set to PDUTYPE2_ARC_STATUS_PDU (50), and the **pduSource** field MUST be set to zero. Changed to: shareDataHeader (18 bytes): Share Data Header containing information about the packet. The type subfield of the pduType field of the Share Control Header (section 2.2.8.1.1.1.1) MUST be set to PDUTYPE_DATAPDU (7). The pduType2 field of the Share Data Header MUST be set to PDUTYPE2_ARC_STATUS_PDU (50), and the **PDUSource** field MUST be set to zero. In Section 2.2.5.1.1, Set Error Info PDU Data (TS_SET_ERROR_INFO_PDU), changed from: shareDataHeader (18 bytes): Share Data Header containing information about the packet. The type subfield of the pduType field of the Share Control Header (section 2.2.8.1.1.1.1) MUST be set to PDUTYPE_DATAPDU (7). The pduType2 field of the Share Data Header MUST be set to PDUTYPE2_SET_ERROR_INFO_PDU (47), and the **pduSource** field MUST be set to zero. Changed to: shareDataHeader (18 bytes): Share Data Header containing information about the packet. The type subfield of the pduType field of the Share Control Header (section 2.2.8.1.1.1.1) MUST be set to PDUTYPE_DATAPDU (7). The pduType2 field of the Share Data Header MUST be set to PDUTYPE2_SET_ERROR_INFO_PDU (47), and the **PDUSource** field MUST be set to zero. In Section 2.2.5.2, Server Status Info PDU, changed from: shareDataHeader (18 bytes): A Share Data Header containing information about the packet. The type subfield of the pduType field of the Share Control Header (section 2.2.8.1.1.1.1) MUST be set to PDUTYPE_DATAPDU (7). The pduType2 field of the Share Data Header MUST be set to PDUTYPE2_STATUS_INFO_PDU (54), and the **pduSource** field MUST be set to zero. Changed to: shareDataHeader (18 bytes): A Share Data Header containing information about the packet. The type subfield of the pduType field of the Share Control Header (section 2.2.8.1.1.1.1) MUST be set to PDUTYPE_DATAPDU (7). The pduType2 field of the Share Data Header MUST be set to PDUTYPE2_STATUS_INFO_PDU (54), and the **PDUSource** field MUST be set to zero. In Section 2.2.9.1.1.3.1.2.2, Bitmap Data (TS_BITMAP_DATA), changed from: bitmapComprHdr (8 bytes): Optional Compressed Data Header structure (section 2.2.9.1.1.3.1.2.3) specifying the bitmap data in the bitmapDataStream. This field MUST be present if the BITMAP_COMPRESSION (0x0001) flag is present in the **Flags** field, but the NO_BITMAP_COMPRESSION_HDR (0x0400) flag is not.

Errata Published*	Description
	Changed to: bitmapComprHdr (8 bytes): Optional Compressed Data Header structure (section 2.2.9.1.1.3.1.2.3) specifying the bitmap data in the bitmapDataStream. This field MUST be present if the BITMAP_COMPRESSION (0x0001) flag is present in the **flags** field, but the NO_BITMAP_COMPRESSION_HDR (0x0400) flag is not. In Section 2.2.9.1.2.1, Fast-Path Update (TS_FP_UPDATE), changed from: updateHeader (1 byte): An 8-bit, unsigned integer. The TS_FP_UPDATE structure begins with a 1- byte, bit-packed update header field. Three pieces of information are collapsed into this byte: … Changed to: updateHeader (1 byte): An 8-bit, unsigned integer. Three pieces of information are collapsed into this byte: … In Section 2.2.12.1, Monitor Layout PDU, changed from: shareDataHeader (18 bytes): A Share Data Header containing information about the packet. The type subfield of the pduType field of the Share Control Header (section 2.2.8.1.1.1.1) MUST be set to PDUTYPE_DATAPDU (7). The pduType2 field of the Share Data Header MUST be set to PDUTYPE2_MONITOR_LAYOUT_PDU (55), and the **pduSource** field MUST be set to zero. Changed to: shareDataHeader (18 bytes): A Share Data Header containing information about the packet. The type subfield of the pduType field of the Share Control Header (section 2.2.8.1.1.1.1) MUST be set to PDUTYPE_DATAPDU (7). The pduType2 field of the Share Data Header MUST be set to PDUTYPE2_MONITOR_LAYOUT_PDU (55), and the **PDUSource** field MUST be set to zero.

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[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

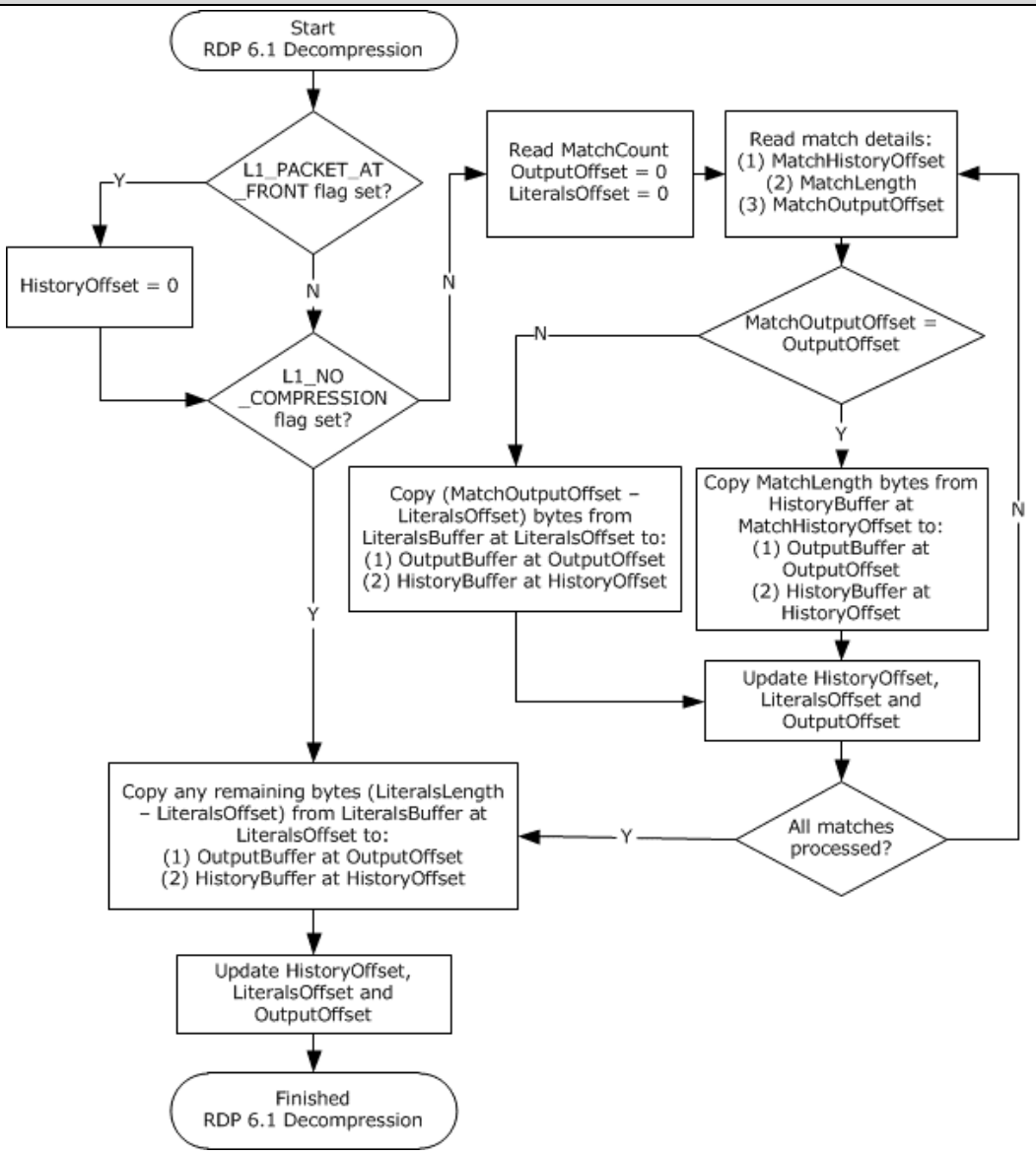
To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

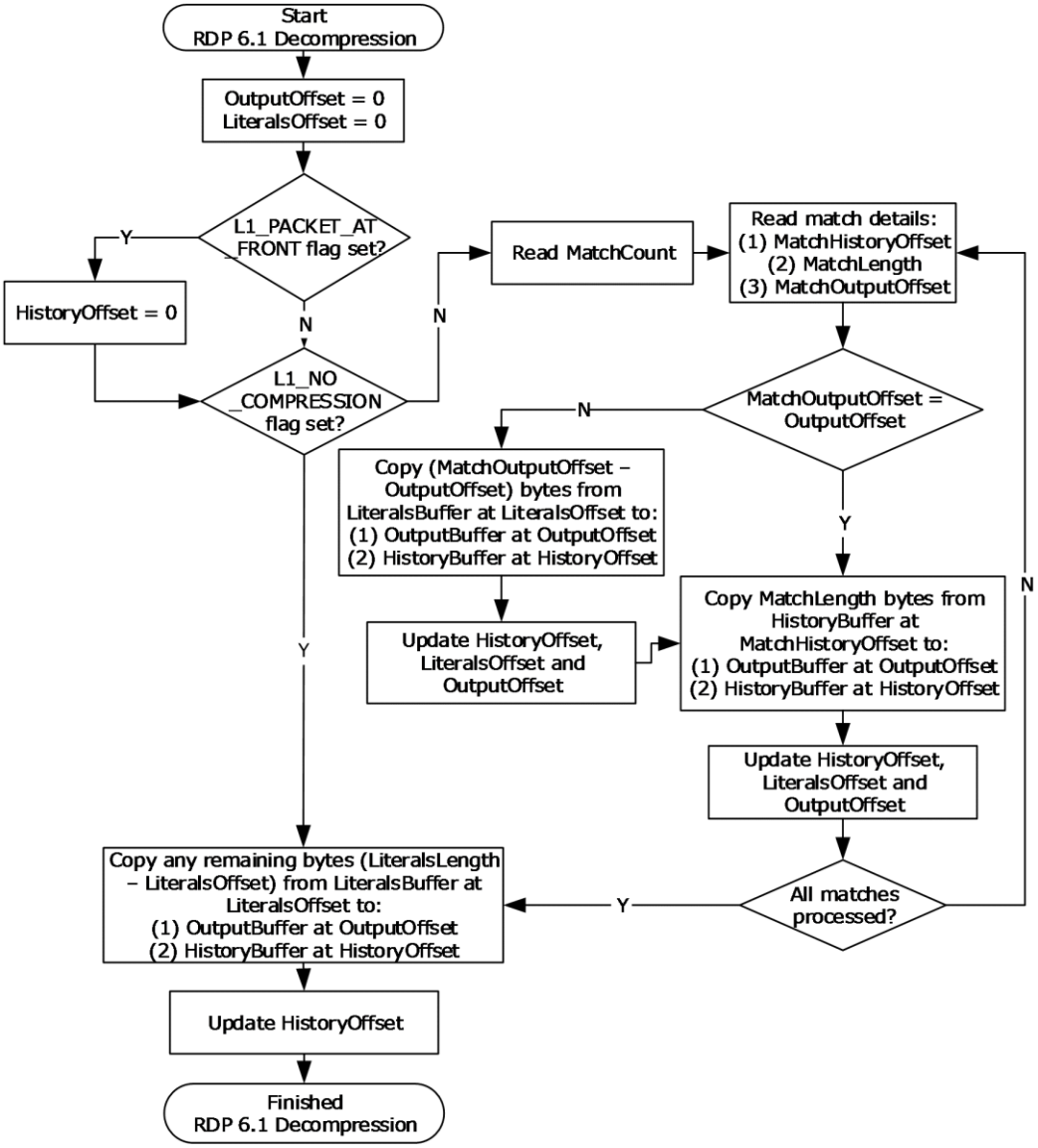
October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V41.0 – 2016/03/02.

Errata Published*	Description
2016/05/02	In Section 3.1.8.2.3, Decompressing Data, updated the figure illustrating the RDP 6.1 bulk decompression algorithm. Changed from: The following flowchart describes how the RDP6.1-BC decompression algorithm operates.

Errata Published*	Description
	 Figure 13: The RDP 6.1 bulk decompression algorithm Changed to: The following flowchart describes how the RDP6.1-BC decompression algorithm operates.

Errata Published*	Description
	 Figure 13: The RDP 6.1 bulk decompression algorithm
2016/05/02	In Section 3.3.5.1.2.1.7, Construction of Cache Bitmap (Revision 3), changed Cache Bitmap (Revision 2) to Cache Bitmap (Revision 3). Changed from: ... The Cache Bitmap (Revision 3) Order MUST NOT be sent to the client if support for bitmap caching was not specified using the Revision 2 Bitmap Cache Capability Set ([MS-RDPBCGR] section 2.2.7.1.4.2). Furthermore, if client-side support for the MemBlt (section 3.3.5.1.1.1.9) and Mem3Blt (section 3.3.5.1.1.1.10) Primary Drawing Orders (specified using the Order Capability Set specified in [MS-RDPBCGR] section 2.2.7.1.3) does not exist, the Cache Bitmap (Revision 2)

Errata Published*	Description
	Order SHOULD NOT be sent to the client. Changed to: ... The Cache Bitmap (Revision 3) Order MUST NOT be sent to the client if support for bitmap caching was not specified using the Revision 2 Bitmap Cache Capability Set ([MS-RDPBCGR] section 2.2.7.1.4.2). Furthermore, if client-side support for the MemBlt (section 3.3.5.1.1.1.9) and Mem3Blt (section 3.3.5.1.1.1.10) Primary Drawing Orders (specified using the Order Capability Set specified in [MS-RDPBCGR] section 2.2.7.1.3) does not exist, the Cache Bitmap (Revision 3) Order SHOULD NOT be sent to the client.
2016/03/21	In Section 2.2.2.2.1.3.3, Switch Surface (SWITCH_SURFACE_ORDER), added a product behavior note for the bitmapId field. Changed from: If this field has a value less than SCREEN_BITMAP_SURFACE (0xFFFF), it identifies an entry in the Offscreen Bitmap Cache which contains a bitmap surface that MUST become the new target drawing surface. Changed to: If this field has a value less than SCREEN_BITMAP_SURFACE (0xFFFF), it SHOULD<5> identify an entry in the Offscreen Bitmap Cache that contains a bitmap surface that MUST become the new target drawing surface. <5> Section 2.2.2.2.1.3.3: It is possible that the bitmapId field sent by the Windows implementation of RDP identifies a nonexistent or deleted bitmap. In this case, a substitute surface that is the same size as the virtual desktop is used as the target of the switch operation.

*Date format: YYYY/MM/DD

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V9.0 – 2015/10/16.

Errata Published*	Description
2016/04/18	In several sections, clarified how the width and height of the MPEG-4 AVC/H.264 codec bitstream should be aligned and cropped. Also clarified the chroma subframe behavior in the "A representation of a YUV444 macroblock as two YUV240p macroblocks" figure. In Section 2.2.4.4, RFX_AVC420_BITMAP_STREAM, changed from: The RFX_AVC420_BITMAP_STREAM structure encapsulates regions of a graphics frame compressed using the MPEG-4 AVC/H.264 codec in YUV420p mode (as specified in [ITU-H.264-201201]) and conforming to the byte stream format specified in [ITU-H.264-201201] Annex B. The data compressed using these techniques is transported in the bitmapData field of the RD PGFX_WIRE_TO_SURFACE_PDU_1 (section 2.2.2.1) message or encapsulated in the RFX_AVC444_BITMAP_STREAM structure (section 2.2.4.5). ... Changed to: The RFX_AVC420_BITMAP_STREAM structure encapsulates regions of a graphics frame compressed using the MPEG-4 AVC/H.264 codec in YUV420p mode (as specified in [ITU-H.264-201201]) and conforming to the byte stream format specified in [ITU-H.264-201201] Annex B. The data compressed using these techniques is transported in the bitmapData field of the RD PGFX_WIRE_TO_SURFACE_PDU_1 (section 2.2.2.1) message or encapsulated in the RFX_AVC444_BITMAP_STREAM structure (section 2.2.4.5). Note that the width and height of the MPEG-4 AVC/H.264 codec bitstream MUST be aligned to a multiple of 16 and MUST be cropped by the region mask specified in the regionRects field that is embedded in the avc420MetaData field. ... In Section 3.3.8.3.2, YUV420p Stream Combination, changed from: ... For macroblocks that are in rectangles in a received chroma subframe (refer to the regionRects field of the corresponding RFX_AVC420_METABLOCK), color conversion MUST use the Y, U, and V components from the last corresponding rectangle in a luma subframe together with the current chroma subframe.

Errata Published*	Description
	The following reverse filter must be applied to $\tilde{U}_{444}(2x,2y)$ and $\tilde{V}_{444}(2x,2y)$ prior to color conversion: $U_{444}(2x,2y) = \tilde{U}_{444}(2x,2y) * 4 - U_{444}(2x+1,2y) - U_{444}(2x,2y+1) - U_{444}(2x+1,2y+1)$ $V_{444}(2x,2y) = \tilde{V}_{444}(2x,2y) * 4 - V_{444}(2x+1,2y) - V_{444}(2x,2y+1) - V_{444}(2x+1,2y+1)$ Changed to: ... For macroblocks that are in rectangles in a received chroma subframe (refer to the regionRects field of the corresponding RFX_AVC420_METABLOCK), color conversion MUST use the Y, U, and V components from the last corresponding rectangle in a luma subframe together with the current chroma subframe. The following reverse filter must be applied to $\tilde{U}_{444}(2x,2y)$ and $\tilde{V}_{444}(2x,2y)$ prior to color conversion: $U_{444}(2x,2y) = \tilde{U}_{444}(2x,2y) * 4 - U_{444}(2x+1,2y) - U_{444}(2x,2y+1) - U_{444}(2x+1,2y+1)$ $V_{444}(2x,2y) = \tilde{V}_{444}(2x,2y) * 4 - V_{444}(2x+1,2y) - V_{444}(2x,2y+1) - V_{444}(2x+1,2y+1)$ Note that the ranges for x and y in the chroma subframe (auxiliary view) are based on 16x16 macroblock sizes, and the view in the figure captioned "A representation of a YUV444 macroblock as two YUV240p macroblocks" shows interleaving in the chroma subframe for B4 and B5 on an 8-line basis. Color conversion MUST be performed for the entire macroblock, after which the region mask in regionRects MUST be applied. The use of 2x or 2y denotes even pixels, while (2x+1) or (2y+1) denotes odd pixels.
2015/12/11	Field names were corrected in three sections. In sections 2.2.4.2.1.5.4 RFX_PROGRESSIVE_TILE_FIRST and 2.2.4.2.1.5.5 RFX_PROGRESSIVE_TILE_UPGRADE, the field name was changed from progQuantVals to quantProgVals. In section 3.3.5.17 Processing an RDPGFX_CACHE_IMPORT_REPLY_PDU message, the field name was changed from entriesToImport to importedEntriesCount.

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V5.0 – 2015/10/16.

Errata Published*	Description
2016/03/21	In Section 2.2.3.5, RDPINPUT_RESUME_INPUT_PDU, corrected the field name EVENTID_RESUME_TOUCH to EVENTID_RESUME_INPUT. Changed from: header (6 bytes): An RDPINPUT_HEADER (section 2.2.2.6) structure. The eventId field MUST be set to EVENTID_RESUME_TOUCH (0x0005). Changed to: header (6 bytes): An RDPINPUT_HEADER (section 2.2.2.6) structure. The eventId field MUST be set to EVENTID_RESUME_INPUT (0x0005).

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V10.0 – 2015/10/16.

Errata Published*	Description
2016/02/08	In Section 3.1.5.3, Processing Application, Window, and Participant IDs, corrected the name of the ID field to Appid. Changed from: When an Application-Created message is received, the client SHOULD check its application list to see if it contains a record for the value in the **ID** field. If no record exists, the client MUST create a record that contains the application ID, the name of the application, and the shared state. If a record with the ID exists in the list, the client MUST replace the information in that record with the information in the message. When an Application-Removed message is received, the client MUST remove the record with the corresponding ID from its list. If no such record exists, the client MUST silently discard the message. … Changed to: When an Application-Created message is received, the client SHOULD check its application list to see if it contains a record for the value in the **AppId** field. If no record exists, the client MUST create a record that contains the application ID, the name of the application, and the shared state. If a record with the ID exists in the list, the client MUST replace the information in that record with the information in the message. When an Application-Removed message is received, the client MUST remove the record with the corresponding ID from its list. If no such record exists, the client MUST silently discard the message. …
2016/01/11	In Section 4, Examples, the ORDER_HDR and UNICODE_STRING member names and the FILTER_ENABLED flag in the Filter-Updated PDU 2 subsection have been corrected. In Section 4.1.1, Filter-Updated PDU 1, changed from: ORDER_HDR : cbSize Changed to: ORDER_HDR : Length In Section 4.1.2, Participant-Created PDU, changed from: UNICODE_STRING : cbSize Changed to: UNICODE_STRING : cchString

Errata Published*	Description
	In Section 4.1.4, Filter-Updated PDU 2: Changed from: ORDER_HDR : cbSize Changed to: ORDER_HDR : Length Changed from: FILTERED_ENABLE Changed to: FILTER_ENABLED In Section 4.1.5, Application-Created PDU Changed from: ORDER_HDR : cbSize Changed to: ORDER_HDR : Length Changed from: UNICODE_STRING : chSize Changed to: UNICODE_STRING : cchString In Section 4.1.6, Application-Removed PDU, changed from: ORDER_HDR : cbSize Changed to: ORDER_HDR : Length In Section 4.1.7, Window-Created PDU Changed from: ORDER_HDR : cbSize Changed to: ORDER_HDR : Length Changed from: UNICODE_STRING : chSize Changed to:

Errata Published*	Description
	UNICODE_STRING : cchString In Section 4.1.8, Window-Removed PDU, changed from: ORDER_HDR : cbSize Changed to: ORDER_HDR : Length In Section 4.1.9, Request Control Level Change Response PDU, changed from: ORDER_HDR : cbSize Changed to: ORDER_HDR : Length In Section 4.1.10, Window Region Update PDU, changed from: ORDER_HDR : cbSize Changed to: ORDER_HDR : Length In Section 4.2.1, Request Control Level Change PDU, changed from: ORDER_HDR : cbSize Changed to: ORDER_HDR : Length In Section 4.2.2, Request Show Window PDU, changed from: ORDER_HDR : cbSize Changed to: ORDER_HDR : Length
2016/01/11	In Section 4, Protocol Examples, corrected the UNICODE_STRING String member name and Flags values and other issues with the Participant-Created PDU sections. In Section 4.1.2, Participant-Created PDU, Changed from: This is the PDU sent to the participant that is being added. IS_PARTICIPANT is set to 1. Changed to: This is the PDU sent to the participant that is being added. The IS_PARTICIPANT flag is set. Changed from: 57 00 49 00 4C 00 48 00 45 00 4C 00 4D 00 53 00 57 00 31 00

Errata Published*	Description
	-> OD_PARTICIPANT_CREATED: UNICODE_STRING: data "TESTUSER02" Changed to: 54 00 45 00 53 00 54 00 55 00 53 00 45 00 52 00 30 00 32 00 -> OD_PARTICIPANT_CREATED: UNICODE_STRING: String "TESTUSER02" Changed from: This network capture shows the PDU sent to notify a participant of a change to its current control level. Note that the IS_PARTICIPANT flag is set and indicates permission to view only. Changed to: This network capture shows the PDU sent to notify a participant of a change to its current control level. Note that the flag indicates permission to view only. Changed from: This network capture shows the PDU sent to notify a participant of a change to its control level. It has the IS_PARTICIPANT flag set to 0 and indicates permission to view only. OD_PARTICIPANT_CREATED 00000000 08 00 24 00 00 00 00 00 00 00 00 00 01 00 0A 00 ..$..... 00000010 54 00 45 00 53 00 54 00 55 00 53 00 45 00 52 00 T.E.S.T.U.S.E.R. 00000020 30 00 32 00 0.2. 08 00 -> OD_PARTICIPANT_CREATED: ORDER_HDR: Type = 08 (OD_PARTICIPANT_CREATED) 24 00 -> OD_PARTICIPANT_CREATED: ORDER_HDR: Length = 36 00 00 00 00 -> OD_PARTICIPANT_CREATED: ParticipantId = 0 00 00 00 00 -> OD_PARTICIPANT_CREATED: GroupId = 0 01 00 -> OD_PARTICIPANT_CREATED: Flags = 1 MAY_VIEW 0A 00 -> OD_PARTICIPANT_CREATED: UNICODE_STRING : cbSize = 10 57 00 49 00 4C 00 48 00 45 00 4C 00 4D 00 53 00 57 00 31 00 -> OD_PARTICIPANT_CREATED: UNICODE_STRING: data "TESTUSER02" Changed to: none (removed because of duplication) In Section 4.1.5, Application-Created PDU, Changed from: UNICODE_STRING : "calc" Changed to: UNICODE_STRING : String "calc" In Section 4.1.7, Window-Created PDU, Changed from: UNICODE_STRING : "Calculator" Changed to: UNICODE_STRING : String "Calculator"
2015/11/09	In Section 7, Appendix B: Product Behavior, added the following preliminary statement to the top of the section since Windows Server 2016 Technical Preview is included in the applicability list:

Errata Published*	Description
	Note: Some of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as an aid to the reader.

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

March 2, 2016 - Download

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V7.0 – 2015/10/16.

Errata Published*	Description
2015/11/09	In Section 7, Appendix B: Product Behavior, added the following preliminary statement to the top of the section since Windows Server 2016 Technical Preview is included in the applicability list: Note: Some of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as an aid to the reader.

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V16.0 – 2015/10/16.

Errata Published*	Description
2016/01/25	In Section 2.2.2.1.1, Server Message Header (SERVER_IO_HEADER), revised the description of the UnusedBits field. Changed from: UnusedBits (1 byte): An 8-bit reserved field. This value SHOULD be set to 0x00. Changed to: UnusedBits (1 byte): An 8-bit padding field. Values in this field MUST be ignored.

* 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

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

March 2, 2016 - Download

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V21.0 – 2016/03/02.

Errata Published*	Description
2016/04/04	In Section 2.2.2.10.1, Language Profile Information PDU, updated that the ProfileGUID field is set to GUID_NULL if the ProfileType field is set to TF_PROFILETYPE_KEYBOARDLAYOUT instead of TF_PROFILETYPE_INPUTPROCESSOR. Changed from: ProfileGUID (16 bytes): A globally unique identifier (section 2.2.2.10.1.1) which uniquely identifies the language profile of the client. This field MUST be set to GUID_NULL if the ProfileType field is set to TF_PROFILETYPE_INPUTPROCESSOR (0x0001). Changed to: ProfileGUID (16 bytes): A globally unique identifier (section 2.2.2.10.1.1) that uniquely identifies the language profile of the client. This field MUST be set to GUID_NULL if the ProfileType field is set to TF_PROFILETYPE_KEYBOARDLAYOUT (0x0002).
2016/04/04	In Section 2.2.2.10.1, Language Profile Information PDU (TS_RAIL_ORDER_LANGUAGEIMEINFO), updated the size of the LanguageID field from 4 bytes to 2 bytes. Changed from: LanguageID (4 bytes): An unsigned 4-byte integer. Changed to: LanguageID (2 bytes): An unsigned 2-byte integer.

* 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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V9.0 – 2015/10/16.

Errata Published*	Description
2015/11/09	In Section 7, Appendix B: Product Behavior, added the following preliminary statement to the top of the section since Windows Server 2016 Technical Preview is included in the applicability list: Note: Some of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as an aid to the reader.

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

March 2, 2016 - Download

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V12.0 – 2015/10/16.

Errata Published*	Description
2015/11/09	In Section 7, Appendix B: Product Behavior, added the following preliminary statement to the top of the section since Windows Server 2016 Technical Preview is included in the applicability list: Note: Some of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as an aid to the reader.

* Date format: YYYY/MM/DD

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V7.0 – 2015/10/16.

Errata Published*	Description
2015/11/09	In Section 7, Appendix B: Product Behavior, added the following preliminary statement to the top of the section since Windows Server 2016 Technical Preview is included in the applicability list: Note: Some of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as an aid to the reader.

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V11.0 – 2015/10/16.

Errata Published*	Description
2015/11/09	In Section 7, Appendix B: Product Behavior, added the following preliminary statement to the top of the section since Windows Server 2016 Technical Preview is included in the applicability list: Note: Some of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as an aid to the reader.

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V34.0 – 2015/10/16.

Errata Published*	Description
2016/04/18	In Section 3.5.4.1, AcquireIssuanceLicense Operation, replaced 'Section Key field' with 'session key' and clarified that it is the hash extracted from the sealedkey field of the ENABLINGBITS element that should be used for validation. Changed from: To service the request, the server MUST validate the ENABLINGBITS element of the PL. If the Section Key field of the ENABLINGBITS element of the PL is DES symmetric key, the server SHOULD return the Microsoft.DigitalRightsManagement.Cryptography.CryptoUnsupportedSymKeyException SOAP fault code. If the Hash field of the ENABLINGBITS cannot be validated, the server SHOULD return the Microsoft.DigitalRightsManagement.EnablingBitsHashDoesNotMatchException SOAP fault code. If validation succeeds, the server SHOULD regenerate the Hash field of the ENABLINGBITS element of the PL by using the ISSUEDPRINCIPALS element of the PL. ... Changed to: To service the request, the server MUST validate the ENABLINGBITS element of the PL. If the session key of the ENABLINGBITS element of the PL is DES symmetric key, the server SHOULD return the Microsoft.DigitalRightsManagement.Cryptography.CryptoUnsupportedSymKeyException SOAP fault code. If the hash that is extracted from the sealedkey field of the ENABLINGBITS cannot be validated, the server SHOULD return the Microsoft.DigitalRightsManagement.EnablingBitsHashDoesNotMatchException SOAP fault code. If validation succeeds, the server SHOULD regenerate the Hash field of the ENABLINGBITS element of the PL by using the ISSUEDPRINCIPALS element of the PL. ...
2016/01/25	In Section 4.3, SOAP on DIME Response from Activate Method Example, updated the description of the ID contents of the header of DIME Record 2. Changed from:

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Element</th><th>Contents</th><th>Explanation</th></tr>
<tr><td>ID</td><td><GUID></td><td>This record is identified as the beginning of the records that contain the binary data. This GUID is automatically generated.</td></tr>
<tr><td>…</td><td>…</td><td>…</td></tr>
</table>

Changed to:
<table>
<tr><th>Element</th><th>Contents</th><th>Explanation</th></tr>
<tr><td>ID</td><td>SecureRepository</td><td>This record is identified as the beginning of the records that contain the binary data.</td></tr>
<tr><td>…</td><td>…</td><td>…</td></tr>
</table>
</td></tr>
<tr><td>2015/11/23</td><td>In Section 4.3, SOAP on DIME Response from Activate Method Example, corrected the DIME record 3 Type length element to match the table explanation.

Changed from:
Record 3 is also broken into three parts:
▪ Fixed-Length Binary Header
<table>
<tr><th>Element</th><th>Contents</th><th>Explanation</th></tr>
<tr><td>…</td><td></td><td></td></tr>
<tr><td>Type length</td><td>0000000011000</td><td>All chunked records inherit the type of the first chunked record; thus this is zero.</td></tr>
<tr><td>…</td><td></td><td></td></tr>
</table>

Changed to:
Record 3 is also broken into three parts:
▪ Fixed-Length Binary Header
<table>
<tr><th>Element</th><th>Contents</th><th>Explanation</th></tr>
<tr><td>…</td><td></td><td></td></tr>
<tr><td>Type length</td><td>0000000000000</td><td>All chunked records inherit the type of the first chunked record; thus this is zero.</td></tr>
<tr><td>…</td><td></td><td></td></tr>
</table>
</td></tr>
</table>

* Date format: YYYY/MM/DD

[MS-RMSOD]: Rights Management Services Protocols Overview

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-RPRN]: Print System Remote Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V27.0 – 2015/10/16.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2016/01/25</td><td>In Section 1.7, Versioning and Capability Negotiation, added the Windows build number for Windows 10 and Windows Server 2016 Technical Preview.

Changed from:
▪ Capability Negotiation: Functional negotiation is supported through the use of Container levels; see section 2.2.1.2. On connection to a server, the client requests a level. If the information level is a level supported by the server, the server is required to process the request. Otherwise, the server has to return an error to the client, and the client would preferably repeat the request with a lower level.
Furthermore, to avoid unnecessary network calls, the client determines the server's capabilities by comparing the value returned by the server in the dwBuildNumber member of OSVERSIONINFO (section 2.2.3.10.1) with well-known version-specific dwBuildNumber values.<2>
<2> Section 1.7: The dwBuildNumber value for OSVERSIONINFO and OSVERSIONINFOEX (section 2.2.3.10.2) for specific versions of Windows is shown in the table that follows.

<table><tr><th>Version</th><th>dwBuildNumber value</th></tr><tr><td>Windows 8.1 and Windows Server 2012 R2</td><td>>= 9431</td></tr><tr><td>…</td><td>…</td></tr></table>
Changed to:
<table><tr><th>Version</th><th>dwBuildNumber value</th></tr><tr><td>Windows 10 and Windows Server 2016 Technical Preview</td><td>>= 10586</td></tr><tr><td>Windows 8.1 and Windows Server 2012 R2</td><td>>= 9431</td></tr><tr><td>…</td><td>…</td></tr></table></td></tr>
</table>

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V20.0 – 2015/10/16.

Errata Published*	Description

2016/02/22	In Section 2.2.1.2.210, OSPF_PROTO_FILTER_INFO, replaced dwNumFilters with dwNumProtoIds and updated the field description.
	Changed from:
	...
	`typedef struct _OSPF_PROTO_FILTER_INFO {`
	`  DWORD type;`
	`  OSPF_FILTER_ACTION ofaActionOnMatch;`
	`  DWORD dwNumFilters;`
	`  DWORD pdwProtoId[1];`
	`} OSPF_PROTO_FILTER_INFO, *POSPF_PROTO_FILTER_INFO;`
	...
	dwNumFilters: The number of protocol filters present in the pFilter field.
	...
	Changed to:
	...
	`typedef struct _OSPF_PROTO_FILTER_INFO {`
	`  DWORD type;`
	`  OSPF FILTER ACTION ofaActionOnMatch;`
	`  DWORD dwNumProtoIds;`
	`  DWORD pdwProtoId[1];`
	`} OSPF_PROTO_FILTER_INFO, *POSPF_PROTO_FILTER_INFO;`
	...
	dwNumProtoIds: The number of protocol IDs present in the pdwProtoId field.
	...
	In Section 6, Appendix A: Full IDL, replaced dwNumFilters with dwNumProtoIds in the OSPF_PROTO_FILTER_INFO structure.
	Changed from:
	...
	`typedef struct  OSPF PROTO FILTER INFO`
	`{`
	`  DWORD  type;`

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<pre>
            OSPF_FILTER_ACTION ofaActionOnMatch;
            DWORD   dwNumFilters;
            DWORD   pdwProtoId[1];
        }OSPF_PROTO_FILTER_INFO, *POSPF_PROTO_FILTER_INFO;
</pre>
...

Changed to:
...
<pre>
        typedef struct _OSPF_PROTO_FILTER_INFO
        {
            DWORD   type;
            OSPF_FILTER_ACTION ofaActionOnMatch;
            DWORD   dwNumProtoIds;
            DWORD   pdwProtoId[1];
        }OSPF_PROTO_FILTER_INFO, *POSPF_PROTO_FILTER_INFO;
</pre>
...
</td></tr>
<tr><td>2016/01/11</td><td>In the following sections, added missing hexadecimal digits to make 8-digit hexadecimal values (e.g., 0x0000000 to 0x00000000 and 0x0000002 to 0x00000002).

In Section 2.2.1.2.109, IPX_INTERFACE, in the MediaType table.
In Section 2.2.1.2.110, IPX_ROUTE, in the Protocol and Flags tables.
In Section 3.1.4.30, RMIBEntryGet (Opnum 29), in the dwVarId values table.
In Section 3.5.4.4.1, GetIcfEnabled Method (Opnum 3), in the Return Values decription.</td></tr>
<tr><td>2015/11/09</td><td>In Section 2.2.2.1, RRAS entry section name, Section 2.2.2.2, Phonebook entry settings, and Section 4.10, Sample Phonebook File for a Demand-dial Connection, replaced all instances of LF\CR with CR\LF, and replaced all instances of " line feed and carriage return" with "carriage return and line feed".</td></tr>
<tr><td>2015/11/09</td><td>In Section 2.2.1.2.270, L2TP_TUNNEL_CONFIG_PARAMS_1, removed the rows for dwConfigOptions and dwTotalCertificates in the packet diagram to be consistent with the text and added the following definition for dwEncryptionType:

dwEncryptionType (4 bytes): Specifies the encryption type to be negotiated for the L2TP tunnel based VPN connections. This SHOULD have one of the values in the following table.
<table>
<tr><th>Value</th><th>Meaning</th></tr>
<tr><td>0</td><td>RRAS will not negotiate encryption.</td></tr>
<tr><td>1</td><td>RRAS requests encryption during negotiation. Negotiation will succeed even if remote RRAS does not support encryption.</td></tr>
<tr><td>2</td><td>RRAS requires encryption to be negotiated.</td></tr>
<tr><td>3</td><td>RRAS requires maximum-strength encryption to be negotiated.</td></tr>
</table>
</td></tr>
<tr><td>2015/11/09</td><td>In Section 4.10, Sample Phonebook File for a Demand-dial Connection, corrected the value of</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>IpNameAssign from 1 to 3.

Changed from:

<table>
<tr><th>Phonebook file</th><th>Meaning</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>IpDnsAddress=0.0.0.0\CR\LF</td><td>Ignored since IpNameAssign is 1</td></tr>
<tr><td>IpDns2Address=0.0.0.0\CR\LF</td><td>Ignored since IpNameAssign is 1</td></tr>
<tr><td>IpWinsAddress=0.0.0.0\CR\LF</td><td>Ignored since IpNameAssign is 1</td></tr>
<tr><td>IpWins2Address=0.0.0.0\CR\LF</td><td>Ignored since IpNameAssign is 1</td></tr>
<tr><td>…</td><td></td></tr>
</table>

Changed to:

<table>
<tr><th>Phonebook file</th><th>Meaning</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>IpDnsAddress=0.0.0.0\CR\LF</td><td>Ignored since IpNameAssign is 3</td></tr>
<tr><td>IpDns2Address=0.0.0.0\CR\LF</td><td>Ignored since IpNameAssign is 3</td></tr>
<tr><td>IpWinsAddress=0.0.0.0\CR\LF</td><td>Ignored since IpNameAssign is 3</td></tr>
<tr><td>IpWins2Address=0.0.0.0\CR\LF</td><td>Ignored since IpNameAssign is 3</td></tr>
<tr><td>…</td><td></td></tr>
</table>
</td></tr>
</table>

* Date format: YYYY/MM/D

[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

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V2.0 – 2015/10/16.

Errata Published*	Description

2016/02/08	In Section 3.6.4.28.2.2, IsChatEnabledResponse, added a description for the pfEnabled element.
	
	Changed from:
	
	`<xsd:element name="IsChatEnabledResponse">`
	`<xsd:complexType>`
	`<xsd:sequence>`
	`<xsd:element minOccurs="1" maxOccurs="1" name="pfEnabled" type="xsd:boolean"/>`
	`</xsd:sequence>`
	`</xsd:complexType>`
	`</xsd:element>`
	
	Changed to:
	
	`<xsd:element name="IsChatEnabledResponse">`
	`<xsd:complexType>`
	`<xsd:sequence>`
	`<xsd:element minOccurs="1" maxOccurs="1" name="pfEnabled" type="xsd:boolean"/>`
	`</xsd:sequence>`
	`</xsd:complexType>`
	`</xsd:element>`
	
	pfEnabled: Contains "true" if the chat system is enabled or "false" if it is disabled.

2016/01/25	In Section 3.7.4.22.1, Messages, updated the messages names to reflect the LogOffConsoleSession operation name. Changed from:

Errata Published*	Description

Message	Description
IMultiPointSession_DisconnectSession_InputMessage	This message requests that the server log off the console session.
IMultiPointSession_DisconnectSession_OutputMessage	Response message.
IMultiPointSession_DisconnectSession_WmsFaultType_FaultMessage	This message contains the internal server failure status code if one occurs.

Changed to:

Message	Description
IMultiPointSession_LogOffConsoleSession_InputMessage	This message requests that the server log off the console session.
IMultiPointSession_LogOffConsoleSession_OutputMessage	Response message.
IMultiPointSession_LogOffConsoleSession_WmsFaultType_FaultMessage	This message contains the internal server failure status code if one occurs.

* 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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V6.0 – 2015/10/16.

Errata Published*	Description
2016/06/27	In Section 3.2.5.5.4, Receiving a Shared Virtual Disk Information Request, corrected the processing rules for initializing the SVHDX_TUNNEL_DISK_INFO_RESPONSE structure. Changed from: • DiskType MUST be set to the value received from the virtual SCSI disk. • If the server implements RSVD Protocol version 2 and Open.IsVHDSet is TRUE, DiskFormat MUST be set to VIRTUAL_STORAGE_TYPE_DEVICE_VHDSET. Otherwise, DiskFormat MUST be set to VIRTUAL_STORAGE_TYPE_DEVICE_VHDX. • BlockSize MUST be set to the number of bytes received from virtual SCSI disk. • LinkageId MUST be set to the linkage GUID received from virtual SCSI disk. • IsMounted MUST be set to TRUE if the virtual SCSI disk indicates that the disk is ready for read or write operations. Otherwise, the server MUST set this field to FALSE. • Is4kAligned MUST be set to TRUE if the virtual SCSI disk indicates that the disk sectors are aligned to 4 kilobytes. Otherwise, the server MUST set this field to FALSE. • Reserved MUST be set to zero. • FileSize MUST be set to the value received from the virtual SCSI disk. • VirtualDiskId MUST be set to the virtual disk GUID received from virtual SCSI disk. Changed to: • DiskType MUST be set to the value received from the virtual SCSI disk, as specified in section 2.2.4.6. • If the server implements RSVD Protocol version 2 and Open.IsVHDSet is TRUE, DiskFormat MUST be set to VIRTUAL_STORAGE_TYPE_DEVICE_VHDSET. Otherwise, DiskFormat MUST be set to VIRTUAL_STORAGE_TYPE_DEVICE_VHDX. • BlockSize MUST be set to an implementation-specific<14> number of bytes received from the virtual SCSI disk. • If the virtual SCSI disk is related to another virtual disk, LinkageId MUST be set to the implementation-specific GUID of the related virtual disk. Otherwise, LinkageID MAY<15> be set to zero. • IsMounted MUST be set to TRUE if the virtual SCSI disk indicates that the disk is ready for read or write operations. Otherwise, the server MUST set this field to FALSE. • Is4kAligned MUST be set to TRUE if the virtual SCSI disk indicates that the disk sectors are

Errata Published*	Description
	aligned to 4 kilobytes. Otherwise, the server MUST set this field to FALSE. • Reserved MUST be set to zero. • FileSize MUST be set to the physical size of the virtual SCSI disk on the underlying storage. • VirtualDiskId MUST be set to the virtual disk GUID received from the virtual SCSI disk. <14> Section 3.2.5.5.4: Windows sets BlockSize to zero for DiskType VHD_TYPE_FIXED. <15> Section 3.2.5.5.4: Windows sets LinkageID to the GUID of the related virtual disk. In Section 3.2.5.5.4, Receiving a Shared Virtual Disk Information Request, changed from: • If the virtual SCSI disk is related to another virtual disk, LinkageId MUST be set to the implementation-specific GUID of the related virtual disk. Otherwise, LinkageID MAY<15> be set to zero. <15> Section 3.2.5.5.4: Windows sets LinkageID to the GUID of the related virtual disk. Changed to: • If the virtual SCSI disk has a linked disk, LinkageId MUST be set to the implementation-specific unique identifier of the linked disk. Otherwise, LinkageID SHOULD be set to an implementation-specific<15> value. <15> Section 3.2.5.5.4: Windows sets LinkageID to zero.
2016/05/16	In Section 2.2.4.12, SVHDX_OPEN_DEVICE_CONTEXT Structure, and Section 2.2.4.32, SVHDX_OPEN_DEVICE_CONTEXT_V2 Structure, updated the description of the Flags field. Changed from: Flags (4 bytes): Reserved. The client SHOULD set this field to 0x00000000, and the server MUST ignore it on receipt. Changed to: Flags (4 bytes): An application-provided value for the open.
2016/05/02	In Section 2.2.4.37, SVHDX_TUNNEL_QUERY_VIRTUAL_DISK_CHANGES_REQUEST Structure, added a new field to the bit table and the subsequent field descriptions. Changed from: … SnapshotType (4 bytes): The type of snapshot. This field MUST contain one of the values defined in section 2.2.6. ByteOffset (8 bytes): The byte offset of the region in the virtual disk to query changes for. … Changed to: … SnapshotType (4 bytes): The type of snapshot. This field MUST contain one of the values defined in section 2.2.6. Reserved (4 bytes): This field ensures the 8-byte alignment of the ByteOffset field. This value MUST be set to 0 by the client and MUST be ignored by the server. ByteOffset (8 bytes): The byte offset of the region in the virtual disk to query changes for. …

Errata Published*	Description
2016/04/18	In Section 3.2.5.5.14, Receiving a Query Virtual Disk changes request, revised the Ranges field description. Changed from: … ▪ The Ranges field is filled with an array of SVHDX_VIRTUAL_DISK_CHANGED_RANGE structures, each initialized as follows: … Changed to: … ▪ The Ranges field is filled with an array of SVHDX_VIRTUAL_DISK_CHANGED_RANGE structures returned from the virtual SCSI disk in an implementation-specific manner, each initialized as follows: …
2016/04/18	In Section 3.2.5.5.7, Receiving a Start Meta-Operation Request, added missing operation types. Changed from: If the OperationType is not one of SvhdxMetaOperationTypeCreateSnapshot, SvhdxMetaOperationTypeOptimize, or SvhdxMetaOperationTypeExtractVHD, the operation is failed with the STATUS_INVALID_PARAMETER. Processing for a specific OperationType is as specified in sections 3.2.5.5.7.1, 3.2.5.5.7.2, and 3.2.5.5.7.3. Changed to: SvhdxMetaOperationTypeOptimize, SvhdxMetaOperationTypeExtractVHD, SvhdxMetaOperationTypeConvertToVHDSet, SvhdxMetaOperationTypeResize, or SvhdxMetaOperationTypeApplySnapshot, the operation is failed with the STATUS_INVALID_PARAMETER. Processing for a specific OperationType is specified in the following subsections.
2016/04/04	In Section 2.2.4.27, SVHDX_CHANGE_TRACKING_START_REQUEST Structure, the LogFileNameOffset field was added as follows: LogFileNameOffset (4 bytes): The offset, in bytes, of the LogFileName field.
2016/04/04	In Section 3.2.5.3, Receiving a Read Request, changed from: If the Open is found and Open.InitiatorId is zero, the server MUST process as follows: Changed to: If the Open is found, Open.IsVirtualSCSIDisk is true, and Open.InitiatorId is zero, the server MUST process as follows:

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>In Section 3.2.5.4, Receiving a Write Request, changed from:

If the Open is found and Open.InitiatorId is zero, the server MUST process as follows:

Changed to:

If the Open is found, Open.IsVirtualSCSIDisk is true, and Open.InitiatorId is zero, the server MUST process as follows:</td></tr>
<tr><td>2016/02/22</td><td>In Section 3.2.5.5.7.1, Receiving a Create Snapshot Request, updated the definition of stage value validation.

Changed from:
…
Each Stage2 through Stage6 field is checked with the following:
▪ If the current stage value is less than or equal to that of the prior stage, the operation is failed with STATUS_INVALID_PARAMETER_3.
▪ If the current stage value is not SvhdxSnapshotStageInvalid and the server has observed an SvhdxSnapshotStageInvalid for this request, the operation is failed with STATUS_INVALID_PARAMETER_4.
…

Changed to:
…
Each Stage2 through Stage6 is processed as follows:
▪ If the current stage value is not SvhdxSnapshotStageInvalid and is less than or equal to the previous stage value, the server MUST fail the request with STATUS_INVALID_PARAMETER_4.
▪ If the current state value is not SvhdxSnapshotStageInvalid and if the previous stage value is equal to SvhdxSnapshotStageInvalid, the server MUST fail the request with STATUS_INVALID_PARAMETER_3.
…</td></tr>
<tr><td>2016/01/25</td><td>In various sections, changes have been made to clarify the Create Context V2 structure relative to the V1 structure.

In Section 1.5, Prerequisites/Preconditions, the second bullet has been changed from:

▪ The SMB client and server support the SVHDX_OPEN_DEVICE_CONTEXT create context, as specified in section 2.2.4.12.

Changed to:

▪ The SMB client and server support accessing shared virtual disk files on a remote server.

In Section 2.2.1, Constants, two new constants have been added:

<table><tr><th>Constant name</th><th>Meaning</th></tr><tr><td>RSVD_ECP_CONTEXT_VERSION_1</td><td>Value of Version field in create context</td></tr></table></td></tr>
</table>

Errata Published*	Description
	<table><tr><td>0x00000001</td><td>specified in section 2.2.4.12</td></tr><tr><td>RSVD_ECP_CONTEXT_VERSION_2 0x00000002</td><td>Value of Version field in create context specified in section 2.2.4.32</td></tr></table> In Section 2.2.4.12, SVHDX_OPEN_DEVICE_CONTEXT Structure, the Version field has been changed from: Version (4 bytes): The version of the create context. It MUST be set to 0x0000001. Changed to: Version (4 bytes): The version of the create context. It MUST be set to RSVD_ECP_CONTEXT_VERSION_1. In Section 2.2.4.31, SVHDX_OPEN_DEVICE_CONTEXT_RESPONSE Structure, the Version field has been changed from: Version (4 bytes): The version of the create context. It MUST be set to the highest supported version of the protocol, as specified in section 1.7. Changed to: Version (4 bytes): The version of the create context. It MUST be set to RSVD_ECP_CONTEXT_VERSION_1. In Section 2.2.4.32, SVHDX_OPEN_DEVICE_CONTEXT_V2 Structure, the Version field has been changed from: Version (4 bytes): The version of the create context. It MUST be set to 0x00000002. Changed to: Version (4 bytes): The version of the create context. It MUST be set to RSVD_ECP_CONTEXT_VERSION_2. In Section 2.2.4.33, SVHDX_OPEN_DEVICE_CONTEXT_V2_RESPONSE Structure, the Version field has been changed from: Version (4 bytes): The version of the create context received. Changed to: Version (4 bytes): The version of the create context. It MUST be set to RSVD_ECP_CONTEXT_VERSION_2.
2016/01/25	In Section 3.2.1.2, Per Open, changed from: InitiatorId: A GUID that identifies the initiator of the open request.

Errata Published*	Description
	Changed to: Open.InitiatorId: A GUID that identifies the initiator of the open request.
2016/01/25	In Section 2.2.4.17, SVHDX_META_OPERATION_START_REQUEST Structure, the second paragraph of the Data field has been changed from: If the OperationType is SvhdxMetaOperationTypeCreateSnapshot, this field is provided in the format SVHDX_META_OPERATION_CREATE as specified in section 2.2.4.17.1. Changed to: If the OperationType is SvhdxMetaOperationTypeCreateSnapshot, this field is provided in the format SVHDX_META_OPERATION_CREATE_SNAPSHOT as specified in section 2.2.4.17.1.
2016/01/25	In Section 2.2.4.8, SVHDX_TUNNEL_SCSI_RESPONSE Structure, the Length field has been changed from: Length (2 bytes): Specifies the size, in bytes, of the SVHDX_TUNNEL_SCSI_RESPONSE structure. Changed to: Length (2 bytes): Specifies the size, in bytes, of the SVHDX_TUNNEL_SCSI_RESPONSE structure excluding the DataBuffer field. This field MUST be set to 36. The size of SrbStatus has been changed from 1 byte to 7 bits.
2016/01/11	In several sections, added clarification regarding Sense Information. In Section 2.2.4.4, SVHDX_TUNNEL_SRB_STATUS_RESPONSE Structure, the description of the SenseInfoExLength field has been changed from: SenseInfoExLength (1 byte): The length, in bytes, of the request sense data buffer. Changed to: SenseInfoExLength (1 byte): The length, in bytes, of the sense data in the SenseDataEx field. The SenseDataEx field has been changed from: SenseDataEx (variable): A buffer of maximum size 20 bytes that contains the sense data. Changed to: SenseDataEx (20 bytes): A buffer that contains the sense data. In Section 2.2.4.8, SVHDX_TUNNEL_SCSI_RESPONSE Structure, the description of the SenseInfoExLength field has been changed from: SenseInfoExLength (1 byte): The length, in bytes, of the request sense data buffer.

Errata Published*	Description
	Changed to: SenseInfoExLength (1 byte): The length, in bytes, of the sense data in the SenseDataEx field. The SenseDataEx field has been changed from: SenseDataEx (variable): A buffer of maximum size 20 bytes that contains the sense data. Changed to: SenseDataEx (20 bytes): A buffer that contains the sense data. In Section 3.2.5.5.5, Receiving a SCSI Command Request, the 8th bullet of the second list has been changed from: ▪ The SenseInfoExLength field is set to the length of the sense information received from the virtual SCSI disk, if any. Changed to: ▪ The SenseInfoExLength field is set to the SenseInfoExLength received in the request.

* 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.

RSS
Atom

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

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V36.0 – 2015/10/16.

Errata Published*	Description
2016/06/27	Added 2 new sections and updated several others to describe that the 16-byte encryption key that is used to encrypt the user password is the application key that is derived for the underlying SMB session. In Section 1.2.1, Normative References, added the following references: [MS-CIFS] Microsoft Corporation, "Common Internet File System (CIFS) Protocol". [MS-SMB2] Microsoft Corporation, "Server Message Block (SMB) Protocol Versions 2 and 3". In Section 1.4, Relationship to Other Protocols, updated the figures to include blocks for [MS-SMB2]. In Section 1.5, Prerequisites/Preconditions, added a reference to [MS-SMB2]. In Section 2.2.7.6, SAMPR_USER_ALL_INFORMATION, changed from: LmOwfPassword: An RPC_SHORT_BLOB structure where Length and MaximumLength MUST be 16, and the Buffer MUST be formatted with an ENCRYPTED_LM_OWF_PASSWORD structure with the cleartext value being an LM hash, and the encryption key being the 16-byte SMB [MS-SMB] session key established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]). NtOwfPassword: An RPC_SHORT_BLOB structure where Length and MaximumLength MUST be 16, and the Buffer MUST be formatted with an ENCRYPTED_NT_OWF_PASSWORD structure with the cleartext value being an NT hash, and the encryption key being the 16-byte SMB [MS-SMB] session key established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]). Changed to: LmOwfPassword: An RPC_SHORT_BLOB structure where Length and MaximumLength MUST be 16, and the Buffer MUST be formatted with an ENCRYPTED_LM_OWF_PASSWORD structure with the cleartext value being an LM hash, and the encryption key being the 16-byte SMB session key obtained as specified in either section 3.1.2.3 or section 3.2.2.3.

Errata Published*	Description
	NtOwfPassword: An RPC_SHORT_BLOB structure where Length and MaximumLength MUST be 16, and the Buffer MUST be formatted with an ENCRYPTED_NT_OWF_PASSWORD structure with the cleartext value being an NT hash, and the encryption key being the 16-byte SMB session key obtained as specified in either section 3.1.2.3 or section 3.2.2.3. In Section 2.2.7.23, SAMPR_USER_INTERNAL1_INFORMATION, changed from: EncryptedNtOwfPassword: An NT hash encrypted with the 16-byte SMB [MS-SMB] session key for the connection established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]). EncryptedLmOwfPassword: An LM hash encrypted with the 16-byte SMB [MS-SMB] session key for the connection established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]). Changed to: EncryptedNtOwfPassword: An NT hash encrypted with the 16-byte SMB session key obtained as specified in either section 3.1.2.3 or section 3.2.2.3. EncryptedLmOwfPassword: An LM hash encrypted with the 16-byte SMB session key obtained as specified in either section 3.1.2.3 or section 3.2.2.3. In Section 2.2.7.26, SAMPR_USER_INTERNAL5_INFORMATION, changed from: UserPassword: A cleartext password, encrypted according to the specification for SAMPR_ENCRYPTED_USER_PASSWORD, with the encryption key being the 16-byte SMB [MS-SMB] session key established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]). Changed to: UserPassword: A cleartext password, encrypted according to the specification for SAMPR_ENCRYPTED_USER_PASSWORD, with the encryption key being the 16-byte SMB session key obtained as specified in either section 3.1.2.3 or section 3.2.2.3. In Section 2.2.7.27, SAMPR_USER_INTERNAL5_INFORMATION_NEW, changed from: UserPassword: A password, encrypted according to the specification for SAMPR_ENCRYPTED_USER_PASSWORD_NEW, with the encryption key being the 16-byte SMB [MS-SMB] session key established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]). Changed to: UserPassword: A password, encrypted according to the specification for SAMPR_ENCRYPTED_USER_PASSWORD_NEW, with the encryption key being the 16-byte SMB session key obtained as specified in either section 3.1.2.3 or section 3.2.2.3. Added section 3.1.2.3 Acquiring an SMB Session Key 3.1.2.3 Acquiring an SMB Session Key The server MUST retrieve the SMB session key as specified in [MS-CIFS] section 3.3.4.6. In Section 3.1.5.6.4.4, UserInternal4Information, changed from:

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>3. If the USER_ALL_NTPASSWORDPRESENT or USER_ALL_LMPASSWORDPRESENT flag is present in the WhichFields field, the server MUST update the clearTextPassword attribute with the (decrypted) value of SAMPR_USER_INTERNAL4_INFORMATION.UserPassword, using the decryption key of the 16-byte SMB [MS-SMB] session key established by the underlying authentication protocol (Kerberos or NTLM).

Changed to:
3. If the USER_ALL_NTPASSWORDPRESENT or USER_ALL_LMPASSWORDPRESENT flag is present in the WhichFields field, the server MUST update the clearTextPassword attribute with the (decrypted) value of SAMPR_USER_INTERNAL4_INFORMATION.UserPassword, using, as the decryption key, the 16-byte SMB session key obtained as specified in section 3.1.2.3.

In Section 3.2.2.2, MD5 Usage, changed from:

user-session-key is a 16-byte value obtained from the 16-byte SMB [MS-SMB] session key established by the underlying authentication protocol (either Kerberos [MS-KILE] or NTLM [MS-NLMP]).

Changed to:
user-session-key is the 16-byte SMB session key obtained as specified in section 3.2.2.3.

Added section 3.2.2.3 Acquiring an SMB Session Key
3.2.2.3 Acquiring an SMB Session Key
The client MUST retrieve the SMB session key as specified in [MS-CIFS] section 3.4.4.6.</td></tr>
<tr><td>2016/05/02</td><td>In Section 3.1.5.13.7.1, SamValidateAuthentication, updated the order of the constraints.

Changed from:
<table><tr><th>Condition (fields based on ValidateAuthenticationInput)</th><th>ValidateAuthenticationOutput changes</th></tr><tr><td>If the current time is less than or equal to LockoutTime plus DomainLockoutDuration.</td><td>ValidationStatus MUST be set to SamValidateAccountLockedOut.</td></tr><tr><td>If the current time is greater than LockoutTime plus DomainLockoutDuration.</td><td>LockoutTime MUST be set to 0 (and continue processing)</td></tr><tr><td>PasswordLastSet is zero.</td><td>ValidationStatus MUST be set to SamValidatePasswordMustChange.</td></tr><tr><td>PasswordLastSet plus DomainMaximumPasswordAge is less than the current time.</td><td>ValidationStatus MUST be set to SamValidatePasswordExpired.</td></tr><tr><td>PasswordMatch is zero, and BadPasswordTime plus DomainLockoutObservationWindow is greater than or equal to the current time.</td><td>1. ValidationStatus MUST be set to SamValidatePasswordIncorrect.
2. BadPasswordCount MUST be set to ValidateAuthenticationInput.BadPasswordCount plus 1.
3. BadPasswordTime MUST be set to the current time.
4. If DomainLockoutThreshold is greater than 0 and BadPasswordCount is greater than or</td></tr></table></td></tr>
</table>

Errata Published*	Description

	equal to DomainLockoutThreshold, LockoutTime MUST be set to the current time.
PasswordMatch is zero, and BadPasswordTime plus DomainLockoutObservationWindow is less than the current time.	1. ValidationStatus MUST be set to SamValidatePasswordIncorrect. 2. BadPasswordCount MUST be set to 1. 3. BadPasswordTime MUST be set to the current time.
PasswordMatched is nonzero.	1. ValidationStatus MUST be set to SamValidateSuccess. 2. If BadPasswordCount is nonzero, BadPasswordCount MUST be set to 0.

Changed to:

Constraint	Condition (fields based on ValidateAuthenticationInput)	ValidateAuthenticationOutput changes
1	If the current time is less than or equal to LockoutTime plus DomainLockoutDuration.	ValidationStatus MUST be set to SamValidateAccountLockedOut.
2	If the current time is greater than LockoutTime plus DomainLockoutDuration.	LockoutTime MUST be set to 0 (and continue processing).
3	PasswordMatch is zero, and BadPasswordTime plus DomainLockoutObservationWindow is greater than or equal to the current time.	1. ValidationStatus MUST be set to SamValidatePasswordIncorrect. 2. BadPasswordCount MUST be set to ValidateAuthenticationInput.BadPasswordCount plus 1. 3. BadPasswordTime MUST be set to the current time. 4. If DomainLockoutThreshold is greater than 0 and BadPasswordCount is greater than or equal to DomainLockoutThreshold, LockoutTime MUST be set to the current time.
4	PasswordMatch is zero, and BadPasswordTime plus DomainLockoutObservationWindow is less than the current time.	1. ValidationStatus MUST be set to SamValidatePasswordIncorrect. 2. BadPasswordCount MUST be set to 1. 3. BadPasswordTime MUST be set to the current time.
5	PasswordLastSet is zero.[1]	ValidationStatus MUST be set to SamValidatePasswordMustChange.
6	PasswordLastSet plus DomainMaximumPasswordAge is less than the current time.[1]	ValidationStatus MUST be set to SamValidatePasswordExpired.
7	PasswordMatched is nonzero.	1. ValidationStatus MUST be set to SamValidateSuccess. 2. If BadPasswordCount is nonzero, BadPasswordCount MUST be set to 0.

Errata Published*	Description
	[1] The order in which these conditions are tested SHOULD<64> follow the order shown in the preceding table. <64> Section 3.1.5.13.7.1: Windows Server 2003 operating system, Windows Server 2003 R2, and Windows Server 2008 operating system with Service Pack 2 (SP2) test the PasswordLastSet conditions (constraints 5 and 6) immediately after testing the LockoutTime conditions (constraints 1 and 2).
2016/04/22	In several sections, added new information for security bulletin [MSKB-3149090]. In Section 1.2.1, Normative References, added a new reference: [MSKB-3149090] Microsoft Corporation, "MS16-047: Description of the security update for SAM and LSAD remote protocols", April 2016, https://support.microsoft.com/en-us/kb/3149090. In Section 2.1, Transport, changed from: … The protocol uses the underlying RPC protocol to retrieve the identity of the client that made the method call, as specified in [MS-RPCE] section 3.3.3.4.3. The server SHOULD use this identity to perform method-specific access checks, as specified in the message processing section of each method.<11> RPC clients for this protocol MUST use RPC over TCP/IP for the SamrValidatePassword method and MUST use RPC over SMB for the SamrSetDSRMPassword method. … Changed to: … The protocol uses the underlying RPC protocol to retrieve the identity of the client that made the method call, as specified in [MS-RPCE] section 3.3.3.4.3. The server SHOULD use this identity to perform method-specific access checks, as specified in the message processing section of each method.<11> The server SHOULD<12> reject calls that do not use an authentication level of either RPC_C_AUTHN_LEVEL_NONE or RPC_C_AUTHN_LEVEL_PKT_PRIVACY (see [MS-RPCE] section 2.2.1.1.8). RPC clients for this protocol MUST use RPC over TCP/IP for the SamrValidatePassword method and MUST use RPC over SMB for the SamrSetDSRMPassword method. … <12> Section 2.1: Servers running Windows 2000, Windows XP, and Windows Server 2003 accept calls at any authentication level. Without [MSKB-3149090] installed, servers running Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10 v1507 operating system, or Windows 10 v1511 operating system also accept calls at any authentication level.

* 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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V48.0 – 2015/10/16.

Errata Published*	Description
2016/06/27	In various sections, updated the content to clarify support for SMB2 or higher over NetBT (port 139). In Section 2.1, Transport, changed from: SMB2Message (variable): The body of the SMB2 packet. The length of an SMB2Message varies based on the SMB2 command represented by the message. • SMB2 dialects 2.0.2, 2.1, 3.0, and 3.0.2 support NetBIOS over TCP [RFC1001] [RFC1002]. • SMB2 dialects 3.0, 3.0.2, and 3.1.1 support operation over SMB2 RDMA Transport [MS-SMBD]. Changed to: SMB2Message (variable): The body of the SMB2 packet. The length of an SMB2Message varies based on the SMB2 command represented by the message. • SMB2 dialects 2.0.2, 2.1, 3.0, and 3.0.2 allow NetBIOS over TCP [RFC1001] [RFC1002]. • SMB2 dialects 3.0, 3.0.2, and 3.1.1 allow operation over SMB2 RDMA Transport [MS-SMBD]. In Section 3.2.4.2.1, Connecting to the Target Server, changed from: The client MUST attempt to connect to the target server over the registered transports specified in section 2.1 and [MS-SMB] section 2.1. The ServerName and the optional TransportIdentifier provided by the caller are used to establish the connection. The client SHOULD resolve the ServerName as described in [MS-WPO] section 7.1.4, and SHOULD attempt connections to one or more of the returned addresses. The client can attempt to initiate each such SMB2 connection on all configured transports that it supports, most commonly Direct TCP and the other transports described in section 2.1. The client can choose to prioritize the addresses and/or transport order and try each one sequentially, or try to connect on them all and select one using any implementation-specific heuristic<102>. The client can accept the TransportIdentifier parameter from the calling application, which specifies what transport to use, and then attempt to use the transport specified. If the connection attempt is successful, a connection object MUST be created, as specified in section 3.2.1.2, with the following default parameters: … This connection MUST be inserted into ConnectionTable, and processing MUST continue, as specified in section 3.2.4.2.2. If the connection attempt fails, the client returns the error code to the calling application.

Errata Published*	Description
	If the client implements the SMB 3.x dialect family, the client MUST look up a server entry in ServerList where Server.ServerName matches the ServerName to which the connection is established. If an entry is found, the client MUST set Connection.Server to the server entry found. Otherwise the client MUST initialize a server object and MUST set Server.ServerName to ServerName and Connection.Server to NULL. Changed to: The ServerName and the optional TransportIdentifier provided by the caller are used to establish the connection. The client SHOULD resolve the ServerName as described in [MS-WPO] section 7.1.4, and SHOULD attempt connections to one or more of the returned addresses. The client can attempt to initiate each such SMB2 connection on all configured transports that it allows<102>, most commonly Direct TCP and the other transports described in section 2.1. <102> Section 3.2.4.2.1: Windows clients initiate new transport connections to the server with Direct TCP and NetBIOS over TCP. Windows Server 2012, Windows Server 2012 R2 operating system, Windows Server 2016, and Windows 10 v1511 Enterprise operating system do not initiate a new transport connection with RDMA, but do after a multichannel exchange if a suitable interface is available. The client can choose to prioritize the addresses and/or transport order and try each one sequentially, or try to connect on them all and select one using any implementation-specific heuristic<103>. The client can accept the TransportIdentifier parameter from the calling application, which specifies what transport to use, and then attempt to use the transport specified. If the connection attempt is successful, a connection object MUST be created, as specified in section 3.2.1.2, with the following default parameters: … This connection MUST be inserted into ConnectionTable, and processing MUST continue, as specified in section 3.2.4.2.2. If the connection attempt fails, the client returns the error code to the calling application. In Section 3.2.5.2, Receiving an SMB2 NEGOTIATE Response, changed from: … If the client implements the SMB 3.x dialect family and Connection.Server is not NULL, the client MUST disconnect the connection if any of the following conditions is satisfied: … If the client implements the SMB 3.x dialect family and Connection.Server is NULL, the client MUST set the following values: • Connection.Server.ServerGUID to ServerGUID in the response Changed to: … If the client implements the SMB 3.x dialect family, the client MUST look up the server entry in ServerList where Server.ServerName matches the Connection.ServerName. If an entry is found, the client MUST set Connection.Server to the server entry found. Otherwise, the client MUST initialize a server object and MUST set Server.ServerName to Connection.ServerName and Connection.Server to NULL. The client MUST add the Server entry to ServerList. If the client implements the SMB 3.x dialect family and Connection.Server is not NULL, the client MUST disconnect the connection if any of the following conditions is satisfied: … If the client implements the SMB 3.x dialect family and Connection.Server is NULL, the client MUST set the following values: • Connection.Server to the server entry in ServerList where Server.ServerName matches the Connection.ServerName.

Errata Published*	Description
	• Connection.Server.ServerGUID to ServerGUID in the response.
2016/06/27	In Section 3.3.5.9, Receiving an SMB2 CREATE Request, corrected the processing rules. Changed from: • If Open.IsDurable is TRUE or Open.IsResilient is TRUE, Open.DurableFileId is set to a generated value that uniquely identifies this open in GlobalOpenTable. Otherwise, Open.DurableFileId is set to a generated value that uniquely identifies this Open in Session.OpenTable. Changed to: • Open.DurableFileId is set to a generated value that uniquely identifies this open in GlobalOpenTable.
2016/06/27	In Section 3.3.4.7, Object Store Indicates a Lease Break, corrected the processing rules. Changed from: If Open.Connection is NULL, Open.IsResilient is FALSE, and Open.IsPersistent is FALSE, the server SHOULD close the Open as specified in section 3.3.4.17. Otherwise, if Lease.BreakToLeaseState does not contain SMB2_LEASE_HANDLE_CACHING and Open.IsDurable is TRUE, the server MUST close the Open as specified in section 3.3.4.17. Changed to: If Open.Connection is NULL, the server MUST close the Open as specified in section 3.3.4.17 for the following cases: • Open.IsResilient is FALSE, Open.IsDurable is FALSE, and Open.IsPersistent is FALSE. • Lease.BreakToLeaseState does not contain SMB2_LEASE_HANDLE_CACHING and Open.IsDurable is TRUE.
2016/05/16	In 4 sections, updated the text to remove the implication that resiliency requires leasing. In Section 3.3.1.5, Global, changed from: If the server implements the SMB 2.1 or SMB 3.x dialect family and supports leasing, it MUST implement the following: ▪ GlobalLeaseTableList: A list of all the lease tables as described in 3.3.1.11, indexed by the ClientGuid. ▪ MaxResiliencyTimeout: The maximum resiliency time-out in milliseconds, for the TimeOut field of NETWORK_RESILIENCY_REQUEST Request, as specified in section 2.2.31.3. Changed to: If the server implements the SMB 2.1 or SMB 3.x dialect family and supports leasing, it MUST implement the following: ▪ GlobalLeaseTableList: A list of all the lease tables as described in 3.3.1.11, indexed by the ClientGuid. If the server implements the SMB 2.1 or SMB 3.x dialect family and supports resiliency, it MUST implement the following: ▪ MaxResiliencyTimeout: The maximum resiliency time-out in milliseconds, for the TimeOut

Errata Published*	Description
	field of NETWORK_RESILIENCY_REQUEST Request, as specified in section 2.2.31.3. In Section 3.3.3, Initialization, changed from: If the server implements the SMB 2.1 or 3.x dialect family and supports leasing, the server MUST initialize the following: ▪ GlobalLeaseTableList MUST be set to an empty list. ▪ MaxResiliencyTimeout SHOULD<185> be set to an implementation-specific default value. Changed to: If the server implements the SMB 2.1 or 3.x dialect family and supports leasing, the server MUST initialize the following: ▪ GlobalLeaseTableList MUST be set to an empty list. If the server implements the SMB 2.1 or SMB 3.x dialect family and supports resiliency, it MUST implement the following: ▪ MaxResiliencyTimeout SHOULD<185> be set to an implementation-specific default value. 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: 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, and Open.IsResilient or Open.IsPersistent 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: 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 nu mber in Open.LockSequenceArray through the following step to indicate that the lock request with LockSequence has been successfully processed by the server: 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, and Open.IsResilient or Open.IsPersistent 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:
2016/04/18	In Section 2.2.13, SMB2 CREATE Request, clarified the use of "can" in the description of the

Errata Published*	Description
	NameOffset field. Changed from: NameOffset (2 bytes): The offset, in bytes, from the beginning of the SMB2 header to the 8-byte aligned file name. If SMB2_FLAGS_DFS_OPERATIONS is set in the Flags field of the SMB2 header, the file name can be prefixed with Distributed File System (DFS) link information that will be removed during DFS name normalization as specified in section 3.3.5.9. Otherwise, the file name is relative to the share that is identified by the TreeId in the SMB2 header. The NameOffset field SHOULD be set to the offset of the Buffer field from the beginning of the SMB2 header. The file name (after DFS normalization if needed) MUST conform to the specification of a relative pathname in [MS-FSCC] section 2.1.5. A zero length file name indicates a request to open the root of the share. Changed to: NameOffset (2 bytes): The offset, in bytes, from the beginning of the SMB2 header to the 8-byte aligned file name. If SMB2_FLAGS_DFS_OPERATIONS is set in the Flags field of the SMB2 header, the file name includes a prefix that will be processed during DFS name normalization as specified in section 3.3.5.9. Otherwise, the file name is relative to the share that is identified by the TreeId in the SMB2 header. The NameOffset field SHOULD be set to the offset of the Buffer field from the beginning of the SMB2 header. The file name (after DFS normalization if needed) MUST conform to the specification of a relative pathname in [MS-FSCC] section 2.1.5. A zero length file name indicates a request to open the root of the share.
2016/04/18	In Section 3.3.5.9.14, Handling the SVHDX_OPEN_DEVICE_CONTEXT Create Context, corrected the processing rules by adding a new paragraph and removing a second. Changed from: This section applies only to servers that implement the SMB 3.0.2 or SMB 3.1.1 dialect. If the create request has any other created contexts, the server MUST process those create contexts before processing the SVHDX_OPEN_DEVICE_CONTEXT. If IsSharedVHDSupported is FALSE, the server MUST fail the request with STATUS_INVALID_DEVICE_REQUEST. Changed to: This section applies only to servers that implement the SMB 3.0.2 or SMB 3.1.1 dialect. If IsSharedVHDSupported is FALSE, the server MUST ignore the create context. If the create request has any other create contexts, the server MUST process those create contexts before processing the SVHDX_OPEN_DEVICE_CONTEXT.
2016/04/04	In Section 3.3.5.9.7, Handling the SMB2_CREATE_DURABLE_HANDLE_RECONNECT Create Context, updated the product behavior note in processing step 3 to clarify behavior for establishing a durable handle reconnect when looking up an existing open. Changed from: The processing changes involved for this create context are: … 3. The server MUST look up an existing open in the GlobalOpenTable by doing a lookup with the FileId.Persistent portion of the create context. If the lookup fails, the server SHOULD<275> fail the request with STATUS_OBJECT_NAME_NOT_FOUND and proceed as specified in "Failed Open Handling" in section 3.3.5.9.

Errata Published*	Description
	<275> Section 3.3.5.9.7: Windows Vista SP1, Windows Server 2008, Windows 7 and Windows Server 2008 R2 ignore undefined create contexts. … Changed to: The processing changes involved for this create context are: … 3. The server MUST look up an existing open in the GlobalOpenTable by doing a lookup with the FileId.Persistent portion of the create context. If the lookup fails, the server SHOULD<275> fail the request with STATUS_OBJECT_NAME_NOT_FOUND and proceed as specified in "Failed Open Handling" in section 3.3.5.9. <275> Section 3.3.5.9.7: If the Session was established by invalidating the previous session by specifying PreviousSessionId in the SMB2 SESSION_SETUP request, Windows 8.1 and Windows Server 2012 R2 close the durable opens established on the previous session.
2016/04/04	In Section 3.2.4.4, Re-establishing a Durable Open, corrected "Open.ShareAccess" to "Open.ShareMode". Changed from: The SMB2 CREATE Request MUST be initialized as follows: If Connection.Dialect belongs to the SMB 3.x dialect family, the client MUST set the following: … ▪ The client sets the ShareAccess field to Open.ShareAccess. Changed to: The SMB2 CREATE Request MUST be initialized as follows: If Connection.Dialect belongs to the SMB 3.x dialect family, the client MUST set the following: … ▪ The client sets the ShareAccess field to Open.ShareMode.

2016/04/04	In Section 3.3.5.9.14, Handling the SVHDX_OPEN_DEVICE_CONTEXT Create Context, clarified the processing rules for Open.IsSharedVHDX and ":SharedVirtualDisk".
	
	Changed from:
	
	If IsSharedVHDSupported is TRUE, the processing changes involved for this create context are:
	…
	▪ In the "Response Construction" phase:
	  ▪ If the RSVD server has returned a response create context, as specified in [MS-RSVD] sections 2.2.4.31 and 2.2.4.33, the server MUST include it in the buffer described by the response CreateContextLength and CreateContextOffset fields.
	
	Changed to:
	
	If IsSharedVHDSupported is TRUE and the file name in the Buffer field ends with ":SharedVirtualDisk", the processing changes involved for this create context are:
	…
	▪ In the "Response Construction" phase:
	  ▪ If the RSVD server has returned a response create context, as specified in [MS-RSVD] sections 2.2.4.31 and 2.2.4.33, the server MUST include it in the buffer described by the

Errata Published*	Description
	response CreateContextLength and CreateContextOffset fields. If IsSharedVHDSupported is TRUE and the file name in the Buffer field does not end with ":SharedVirtualDisk", the processing changes involved for this create context are: ▪ The server MUST set Open.IsSharedVHDX to FALSE. ▪ If OriginatorFlags in SVHDX_OPEN_DEVICE_CONTEXT is set to SVHDX_ORIGINATOR_VHDMP, the server MUST fail the request with STATUS_VHD_SHARED. Otherwise, the create operation MUST be ignored
2016/03/21	In Section 3.3.3, Initialization, changed "implement" and "perform" to "initialize" in keeping with the purpose of the section. Changed from: The server MUST implement the following: ▪ All the members in ServerStatistics MUST be set to zero. … If the server implements the SMB 2.1 or 3.x dialect family and supports leasing, the server MUST implement the following: ▪ GlobalLeaseTableList MUST be set to an empty list. … If the server implements the SMB 3.x dialect family, the server MUST implement the following: ▪ EncryptData MUST be set in an implementation-specific manner. … If the server implements the SMB 3.0.2 or SMB 3.1.1 dialect, the server MUST implement the following: ▪ IsSharedVHDSupported: MUST be set to FALSE. If the server implements the SMB 3.1.1 dialect, the server MUST perform the following: ▪ MaxClusterDialect MUST be set in an implementation-specific manner. … Changed to: The server MUST initialize the following: ▪ All the members in ServerStatistics MUST be set to zero. … If the server implements the SMB 2.1 or 3.x dialect family and supports leasing, the server MUST initialize the following: ▪ GlobalLeaseTableList MUST be set to an empty list. … If the server implements the SMB 3.x dialect family, the server MUST initialize the following: ▪ EncryptData MUST be set in an implementation-specific manner. … If the server implements the SMB 3.0.2 or SMB 3.1.1 dialect, the server MUST initialize the following: ▪ IsSharedVHDSupported: MUST be set to FALSE. If the server implements the SMB 3.1.1 dialect, the server MUST initialize the following: ▪ MaxClusterDialect MUST be set in an implementation-specific manner. …
2016/01/25	In Section 3.3.5.9, Receiving an SMB2 CREATE Request, the first pargraph under Open Execution has been changed from:

Errata Published*	Description
	If the FILE_DELETE_ON_CLOSE flag is set in CreateOptions and any of the following conditions is TRUE, the server SHOULD<248> fail the request with STATUS_ACCESS_DENIED. ▪ DesiredAccess does not include DELETE or GENERIC_ALL. ▪ Treeconnect.MaximalAccess does not include DELETE or GENERIC_ALL. Changed to: If the FILE_DELETE_ON_CLOSE flag is set in CreateOptions and Treeconnect.MaximalAccess does not include DELETE or GENERIC, the server SHOULD<248> fail the request with STATUS_ACCESS_DENIED.
2016/01/11	In Section 3.3.5.10, Receiving an SMB2 CLOSE Request, modified the processing rules to account for Windows behavior. The 6 and 7th paragraphs have been changed from: The server MUST locate the Request in Connection.RequestList for which Request.MessageId matches the MessageId value in the SMB2 header, set Request.Open to the Open, and close the Open as specified in section 3.3.4.17. If SMB2_CLOSE_FLAG_POSTQUERY_ATTRIB is set in the Flags field of the request, the server MUST query the attributes of the file after the close.<291> This gives the client the attributes that have been updated to take into account any cached writes or extends that may have happened. The attributes that MUST be queried are the creation time, last access time, last write time, change time, allocation size in bytes, end of file in bytes, and file attributes. <291> Section 3.3.5.10: Windows obtains attributes and end of file from the object store FileBasicInformation [MS-FSA] section 2.1.5.11.6 and [MS-FSCC] section 2.4.7. Changed to: The server MUST locate the Request in Connection.RequestList for which Request.MessageId matches the MessageId value in the SMB2 header and set Request.Open to the Open. If SMB2_CLOSE_FLAG_POSTQUERY_ATTRIB is set in the Flags field of the request, the server MUST query the creation time, last access time, last write time, change time, allocation size in bytes, end of file in bytes, and file attributes of the file from the underlying object store in an implementation-specific manner<290>. The server MUST close the Open as specified in section 3.3.4.17. <290> Section 3.3.5.10: Windows obtains FileNetworkOpenInformation from the object store as described in [MS-FSA] section 2.1.5.11.21 and [MS-FSCC] section 2.4.27. Windows servers do not return an updated ChangeTime unless Open.GrantedAccess includes FILE_WRITE_DATA, FILE_WRITE_ATTRIBUTES, FILE_WRITE_EA, or FILE_APPEND_DATA and any prior WRITE/SET_INFO operations were performed on that Open.
2016/01/11	In Section 3.2.7.1, Handling a Network Disconnect, modified a processing rule. Changed from:

Errata Published*	Description
	▪ If Connection.Dialect belongs to the SMB 3.x dialect family, and if the Session has more than one channel in Session.ChannelList, the client MUST perform the following actions: … Changed to: ▪ If Connection.Dialect belongs to the SMB 3.x dialect family, and if Connection.SupportsMultiChannel or Connection.SupportsPersistentHandles is TRUE, the client MUST perform the following actions: …
2016/01/11	In various sections, added information about the disconnect behavior of Windows clients. In Section 3.2.5.2, Receiving an SMB2 NEGOTIATE Response, a new paragraph was added: The client SHOULD<154> disconnect the connection if the size, in bytes, received in MaxTransactSize, MaxReadSize, or MaxWriteSize is less than 65536. <154> Section 3.2.5.2: Windows Vista SP1, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, and Windows Server 2012 R2 disconnect the connection if MaxTransactSize, MaxReadSize, or MaxWriteSize is less than 4096. In Section 3.3.5.3.1, SMB 2.1 or SMB 3.x Support, the 6th, 7th, and 8th bullet points of the first list were changed from: ▪ MaxTransactSize is set to the maximum buffer size<220>, in bytes, that the server will accept on this connection for QUERY_INFO, QUERY_DIRECTORY, SET_INFO, and CHANGE_NOTIFY operations. This field is applicable only for buffers sent by the client in SET_INFO requests, or returned from the server in QUERY_INFO, QUERY_DIRECTORY, and CHANGE_NOTIFY responses. Connection.MaxTransactSize MUST be set to MaxTransactSize. ▪ MaxReadSize is set to the maximum size, in bytes, of the Length in an SMB2 READ Request (2.2.19) that the server will accept on the transport that established this connection.<221> Connection.MaxReadSize MUST be set to MaxReadSize. ▪ MaxWriteSize is set to the maximum size, in bytes, of the Length in an SMB2 Write Request (2.2.21) that the server will accept on the transport that established this connection.<222> Connection.MaxWriteSize MUST be set to MaxWriteSize. Changed to: ▪ MaxTransactSize is set to the maximum buffer size, in bytes, that the server will accept on this connection for QUERY_INFO, QUERY_DIRECTORY, SET_INFO, and CHANGE_NOTIFY operations. This field is applicable only for buffers sent by the client in SET_INFO requests, or returned from the server in QUERY_INFO, QUERY_DIRECTORY, and CHANGE_NOTIFY responses. This value SHOULD<221> be greater than or equal to 65536. Connection.MaxTransactSize MUST be set to MaxTransactSize. ▪ MaxReadSize is set to the maximum size, in bytes, of the Length in an SMB2 READ Request (2.2.19) that the server will accept on the transport that established this connection. This value SHOULD<222> be greater than or equal to 65536. Connection.MaxReadSize MUST be set to MaxReadSize. ▪ MaxWriteSize is set to the maximum size, in bytes, of the Length in an SMB2 Write Request (2.2.21) that the server will accept on the transport that established this connection. This value SHOULD<223> be greater than or equal to 65536. Connection.MaxWriteSize MUST be

Errata Published*	Description
	set to MaxWriteSize. In Section 3.3.5.4, Receiving an SMB2 NEGOTIATE Request, the 6th, 7th, and 8th bullet points of the second list were changed from: ▪ MaxTransactSize is set to the maximum buffer size,<228> in bytes, that the server will accept on this connection for QUERY_INFO, QUERY_DIRECTORY, SET_INFO and CHANGE_NOTIFY operations. This field is applicable only for buffers sent by the client in SET_INFO requests, or returned from the server in QUERY_INFO, QUERY_DIRECTORY, and CHANGE_NOTIFY responses. Connection.MaxTransactSize MUST be set to MaxTransactSize. ▪ MaxReadSize is set to the maximum size,<229> in bytes, of the Length in an SMB2 READ Request (section 2.2.19) that the server will accept on the transport that established this connection. Connection.MaxReadSize MUST be set to MaxReadSize. ▪ MaxWriteSize is set to the maximum size,<230> in bytes, of the Length in an SMB2 WRITE Request (section 2.2.21) that the server will accept on the transport that established this connection. Connection.MaxWriteSize MUST be set to MaxWriteSize. Changed to: ▪ MaxTransactSize is set to the maximum buffer size, in bytes, that the server will accept on this connection for QUERY_INFO, QUERY_DIRECTORY, SET_INFO and CHANGE_NOTIFY operations. This field is applicable only for buffers sent by the client in SET_INFO requests, or returned from the server in QUERY_INFO, QUERY_DIRECTORY, and CHANGE_NOTIFY responses. This value SHOULD<229> be greater than or equal to 65536. Connection.MaxTransactSize MUST be set to MaxTransactSize. ▪ MaxReadSize is set to the maximum size, in bytes, of the Length in an SMB2 READ Request (section 2.2.19) that the server will accept on the transport that established this connection. This value SHOULD<230> be greater than or equal to 65536. Connection.MaxReadSize MUST be set to MaxReadSize. ▪ MaxWriteSize is set to the maximum size, in bytes, of the Length in an SMB2 WRITE Request (section 2.2.21) that the server will accept on the transport that established this connection. This value SHOULD<231> be greater than or equal to 65536. Connection.MaxWriteSize MUST be set to MaxWriteSize.
2015/12/11	In section 3.3.5.9 Receiving an SMB2 CREATE Request, the first paragraph under Create Context Validation has been changed. Changed from: The server SHOULD<247> fail any request having a create context not specified in section 2.2.13.2 with a STATUS_INVALID_PARAMETER error. <247> Section 3.3.5.9: Windows Vista SP1, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, and Windows Server 2012 ignore create contexts having a NameLength greater than 4 and ignore create contexts with a length of 4 that are not specified in section 2.2.13.2. Changed to: The server MUST fail create contexts having a NameLength less than 4 with a

Errata Published*	Description
	STATUS_INVALID_PARAMETER error.

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-SQOS]: Storage Quality of Service Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V2.0 – 2015/10/16.

Errata Published*	Description
2016/06/13	In Section 2.2.2.3, STORAGE_QOS_CONTROL_RESPONSE Structure, moved the MaximumBandwidth field to the end of the packet. Changed from: … MaximumBandwidth (8 bytes): The maximum bandwidth currently assigned to the logical flow, expressed in kilobytes per second. This field is not present in the SQoS dialect 1.0. BaseIoSize (4 bytes): The base I/O size used to compute the normalized size of an I/O request for the logical flow. Reserved (4 bytes): Unused field. The server MUST set this field to zero. Changed to: BaseIoSize (4 bytes): The base I/O size used to compute the normalized size of an I/O request for the logical flow. Reserved (4 bytes): Unused field. The server MUST set this field to zero. MaximumBandwidth (8 bytes): The maximum bandwidth currently assigned to the logical flow, expressed in kilobytes per second. This field is not present in the SQoS dialect 1.0.
2016/01/25	In Section 3.2.5.1, Receiving a Storage Quality of Service Control Request, corrected a Product Behavior Note for Windows Server 2016 Technical Preview. Changed from: <7> Section 3.2.5.1: Windows Server 2016 Technical Preview will fail the request with error STATUS_REVISION_MISMATCH if Request.ProtocolVersion is not equal to 0x0101. Changed to: <7> Section 3.2.5.1: Windows Server 2016 Technical Preview will fail the request with error STATUS_REVISION_MISMATCH if Request.ProtocolVersion is not equal to 0x0100 or 0x0101.
2016/01/25	In Section 3.1.3, Initialization, updated the initialization rules for LogicalFlow.MaximumIoRate and LogicalFlow.MaximumBandwidth. Changed from: The following values MUST be initialized to zero: ▪ LogicalFlow.IoCountIncrement ▪ LogicalFlow.NormalizedIoCountIncrement ▪ LogicalFlow.LatencyIncrement

Errata Published*	Description
	▪ LogicalFlow.LowerLatencyIncrement LogicalFlow.BaseIoSize MUST be initialized to 8192. The LogicalFlow.StatusRequestTimer MUST be set to never expire. Dialect MUST be set to the highest dialect that the client implements.<2> If the client supports the SQoS 1.1 dialect, the following MUST be initialized to zero: ▪ LogicalFlow.KilobyteCountIncrement Changed to: The following values MUST be initialized to zero: ▪ LogicalFlow.IoCountIncrement ▪ LogicalFlow.MaximumIoRate ▪ LogicalFlow.NormalizedIoCountIncrement ▪ LogicalFlow.LatencyIncrement ▪ LogicalFlow.LowerLatencyIncrement LogicalFlow.BaseIoSize MUST be initialized to 8192. The LogicalFlow.StatusRequestTimer MUST be set to never expire. Dialect MUST be set to the highest dialect that the client implements.<2> If the client supports the SQoS 1.1 dialect, the following MUST be initialized to zero: ▪ LogicalFlow.KilobyteCountIncrement ▪ LogicalFlow.MaximumBandwidth

*Date format: YYYY/MM/DD

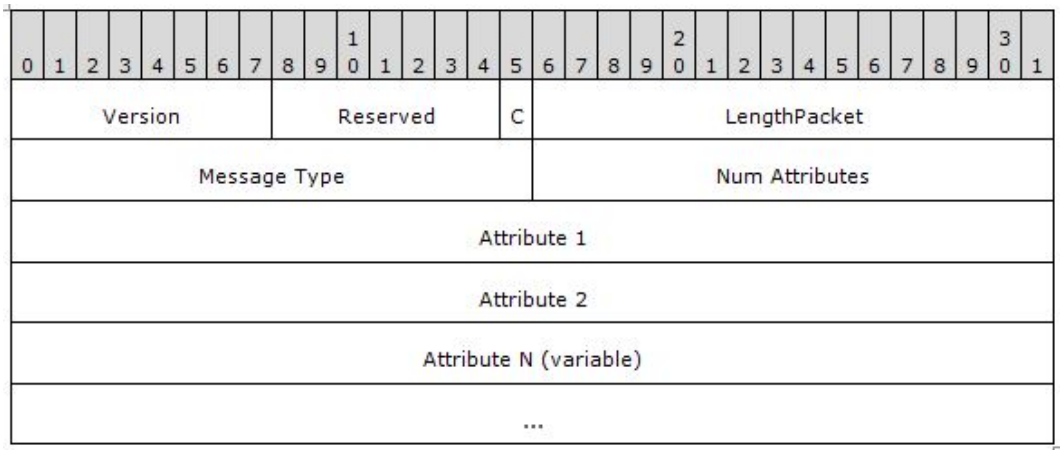
[MS-SSTP]: Secure Socket Tunneling Protocol (SSTP)

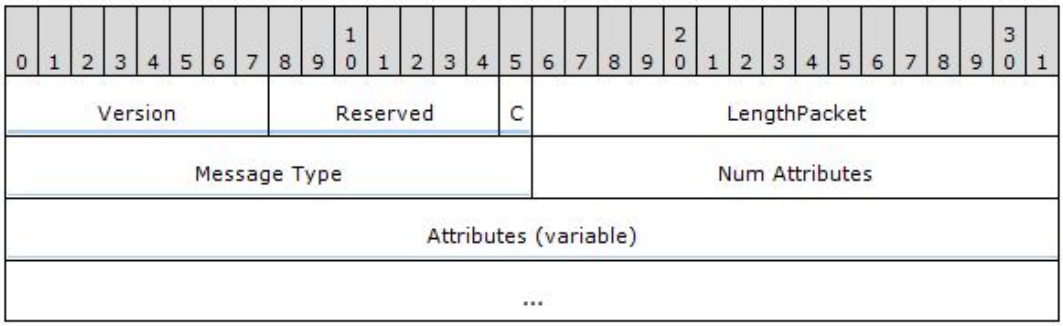
This topic lists the Errata found in [MS-SSTP] since it was last published. Since this topic is updated frequently, we recommend that you subscribe to these RSS or Atom feeds to receive update notifications.

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

RSS
Atom

Errata below are for Protocol Document Version V15.0 – 2015/10/16.

Errata Published*	Description
2015/11/23	In Section 2.2.4, SSTP Attributes, clarified the attribute-specific data. Changed from: Value (variable): A variable-length field with length equal to field Length minus 4 that contains the attribute-specific data. Changed to: Value (variable): A variable-length field with length equal to field Length minus 4 that contains the attribute-specific data. The different attribute-specific data are described in sections 2.2.5 to 2.2.8. The fields "Reserved", "Attribute ID", "LengthPacket" have been repeated in those sections for complete illustration.
2015/11/23	In Section 2.2.2, SSTP Control Packet, corrected the Attribute field lengths. Changed from:  ... Attribute 1 (4 bytes): MUST contain the first attribute. Attribute 2 (4 bytes): MUST contain the second attribute. Attribute N (variable): An ordered list of variable-sized attributes that compose an SSTP control message. Each attribute MUST follow the format as specified in section 2.2.4. Changed to:

Errata Published*	Description
	 … Attributes (variable): An ordered list of variable-sized attributes that compose an SSTP control message. Each attribute MUST follow the format as specified in section 2.2.4.
2015/11/23	In Section 2.2.8, Status Info Attribute, changed the Attribute ID field value from 0x2 to 0x02. Changed from: ... Attribute ID (1 byte): An 8-bit (1-byte) field that is used to specify the type of attribute; its value MUST be 0x2 for the Status Info attribute. ... Changed to: ... Attribute ID (1 byte): An 8-bit (1-byte) field that is used to specify the type of attribute; its value MUST be 0x02 for the Status Info attribute. ...
2015/11/23	In Section 2.2.9, Call Connect Request Message (SSTP_MSG_CALL_CONNECT_REQUEST), specified the length value in the Length field description. Changed from: ... Length (12 bits): A 12-bit unsigned integer in network byte order that MUST specify the length, in bytes, of the entire message. ... Changed to: ... Length (12 bits): A 12-bit unsigned integer in network byte order that contains the value 0x00e for the length of the entire message. ...
2015/11/23	In Section 2.2.6, Crypto Binding Request Attribute, in the Hash Protocol Bitmask field description, clarified how the bits are defined. Changed from: ... Hash Protocol Bitmask (1 byte): This 1-byte bitmask field is used (with the ServerHashProtocolSupported state variable described in section 3.3.1) to specify the hashing methods allowed by the server that the client uses to compute the Compound MAC in the Crypto

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
Binding attribute. For more information, see section 3.2.5.2. The following bits are defined.
<table>
<tr><th>Name</th><th>Value</th></tr>
<tr><td>CERT_HASH_PROTOCOL_SHA1</td><td>0x01</td></tr>
<tr><td>CERT_HASH_PROTOCOL_SHA256</td><td>0x02</td></tr>
</table>
...

Changed to:
...
Hash Protocol Bitmask (1 byte): This 1-byte bitmask field is used (with the ServerHashProtocolSupported state variable described in section 3.3.1) to specify the hashing methods allowed by the server that the client uses to compute the Compound MAC in the Crypto Binding attribute. For more information, see section 3.2.5.2. The following bits are defined.

A 1 MUST be placed in the appropriate bit position to select the supported hash protocol. The server MUST select at least one hash protocol. If the server selects both the SHA256 and the SHA1 hash protocols and the client supports both hash protocols (as indicated by the value of the ClientHashProtocolSupported state variable described in section 3.2.1), then the client MUST select the SHA256 protocol. For more information about how the client processes the Hash Protocol Bitmask when it receives a Call Connect Acknowledge message, see section 3.2.5.3.2.

0 1 2 3 4 5 6 7
0 0 0 0 0 0 B A

Where the bits are defined as:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>A</td><td>CERT_HASH_PROTOCOL_SHA1 is enabled when A=1 and is disabled when A=0.</td></tr>
<tr><td>B</td><td>CERT_HASH_PROTOCOL_SHA256 is enabled when B=1 and is disabled when B=0.</td></tr>
</table>
....
</td></tr>
<tr><td>2015/11/23</td><td>
In Section 2.2.12, Call Connect Negative Acknowledgment Message (SSTP_MSG_CALL_CONNECT_NAK), and Section 2.2.13, Call Abort Message (SSTP_MSG_CALL_ABORT), removed a value from the Status field tables.

In Section 2.2.12, Call Connect Negative Acknowledgment Message (SSTP_MSG_CALL_CONNECT_NAK), changed from:

Status (4 bytes): A 4-byte field that specifies the reason for the failure. Its value MUST be one of the following values, the description of which is specified in the Status Info attribute (section 2.2.8).
<table>
<tr><th>Name</th><th>Value</th></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>ATTRIB_STATUS_VALUE_NOT_SUPPORTED</td><td>0x00000004</td></tr>
</table>
</td></tr>
</table>

Errata Published*	Description

ATTRIB_STATUS_ATTRIB_NOT_SUPPORTED_IN_MSG	0x00000009
ATTRIB_STATUS_REQUIRED_ATTRIBUTE_MISSING	0x0000000a
…	…

Changed to:

Status (4 bytes): A 4-byte field that specifies the reason for the failure. Its value MUST be one of the following values, the description of which is specified in the Status Info attribute (section 2.2.8).

Name	Value
…	…
ATTRIB_STATUS_VALUE_NOT_SUPPORTED	0x00000004
ATTRIB_STATUS_REQUIRED_ATTRIBUTE_MISSING	0x0000000a
…	…

In Section 2.2.13, Call Abort Message (SSTP_MSG_CALL_ABORT), changed from:

Status (4 bytes): A 4-byte field that specifies the reason for the failure. Its value MUST be one of the following values, the description of which is specified in the Status Info attribute (section 2.2.8).

Name	Value
…	…
ATTRIB_STATUS_NEGOTIATION_TIMEOUT	0x00000008
ATTRIB_STATUS_ATTRIB_NOT_SUPPORTED_IN_MSG	0x00000009
ATTRIB_STATUS_REQUIRED_ATTRIBUTE_MISSING	0x0000000A

Changed to:

Status (4 bytes): A 4-byte field that specifies the reason for the failure. Its value MUST be one of the following values, the description of which is specified in the Status Info attribute (section 2.2.8).

Name	Value
…	…
ATTRIB_STATUS_NEGOTIATION_TIMEOUT	0x00000008
ATTRIB_STATUS_ATTRIB_NOT_SUPPORTED_IN_MSG	0x00000009

* Date format: YYYY/MM/DD

[MS-SWN]: Service Witness Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V8.0 – 2015/10/16.

Errata Published*	Description
2016/01/11	Two sections have been updated to clarify WitnessrRegister/WitnessrRegisterEx with invalid IpAddress and ERROR_INVALID_STATE vs ERROR_SUCCESS. In Section 3.1.4.2, WitnessrRegister (Opnum 1), the processing rules have been changed from: If the NetName parameter is not equal to ServerGlobalName, the server MUST fail the request and return the error code ERROR_INVALID_PARAMETER. The server MUST search for an Interface in InterfaceList, where Interface.IPv4Address or Interface.IPv6Address matches the IpAddress parameter based on its format. If no matching entry is found, the server MUST fail the request and return the error code ERROR_INVALID_STATE. The server MUST enumerate the shares by calling NetrShareEnum as specified in [MS-SRVS] section 3.1.4.8. In the enumerated list, if any of the shares have shi*_type set to STYPE_CLUSTER_SOFS, as specified in [MS-SRVS] section 2.2.2.4, the server MUST fail the request and return the error code ERROR_INVALID_STATE. Changed to: If NetName, IpAddress or ClientComputerName is NULL, the server MUST fail the request and return the error code ERROR_INVALID_PARAMETER. If the NetName parameter is not equal to ServerGlobalName, the server MUST fail the request and return the error code ERROR_INVALID_PARAMETER. The server MUST enumerate the shares by calling NetrShareEnum as specified in [MS-SRVS] section 3.1.4.8. In the enumerated list, if any of the shares has shi*_type set to STYPE_CLUSTER_SOFS, as specified in [MS-SRVS] section 2.2.2.4, the server MUST search for an Interface in InterfaceList, where Interface.IPv4Address or Interface.IPv6Address matches the IpAddress parameter based on its format. If no matching entry is found, the server MUST fail the request and return the error code ERROR_INVALID_STATE. In Section 3.1.4.5, WitnessrRegisterEx (Opnum 4), the processing rules have been changed from: If the NetName parameter is not equal to ServerGlobalName, the server MUST fail the request and return the error code ERROR_INVALID_PARAMETER.

Errata Published*	Description
	The server MUST search for an Interface in InterfaceList, where Interface.IPv4Address or Interface.IPv6Address matches the IpAddress parameter based on its format. If no matching entry is found, the server MUST fail the request and return the error code ERROR_INVALID_STATE. If ShareName is not NULL, the server MUST enumerate the shares by calling NetrShareEnum as specified in [MS-SRVS] section 3.1.4.8. If the enumeration fails or if no shares are returned, the server MUST return the error code ERROR_INVALID_STATE. If none of the shares in the list has shi*_type set to STYPE_CLUSTER_SOFS as specified in [MS-SRVS] section 3.1.4.8, the server MUST ignore ShareName. Otherwise, the server MUST fail the request with the error code ERROR_INVALID_STATE for the following: ▪ ShareName does not exist in the enumerated list. ▪ ShareName has shi*_type set to STYPE_CLUSTER_SOFS, as specified in [MS-SRVS] section 2.2.2.4. Changed to: If NetName, IpAddress, or ClientComputerName is NULL, the server MUST fail the request and return the error code ERROR_INVALID_PARAMETER. If the NetName parameter is not equal to ServerGlobalName, the server MUST fail the request and return the error code ERROR_INVALID_PARAMETER. If ShareName is not NULL, the server MUST enumerate the shares by calling NetrShareEnum as specified in [MS-SRVS] section 3.1.4.8. If the enumeration fails or if no shares are returned, the server MUST return the error code ERROR_INVALID_STATE. If none of the shares in the list has shi*_type set to STYPE_CLUSTER_SOFS as specified in [MS-SRVS] section 3.1.4.8, the server MUST ignore ShareName. Otherwise, the server MUST fail the request with the error code ERROR_INVALID_STATE for the following: ▪ ShareName does not exist in the enumerated list. ▪ The server MUST search for an Interface in InterfaceList, where Interface.IPv4Address or Interface.IPv6Address matches the IpAddress parameter based on its format. If no matching entry is found and ShareName has shi*_type set to STYPE_CLUSTER_SOFS, as specified in [MS-SRVS] section 2.2.2.4, the server MUST fail the request with ERROR_INVALID_STATE.

*Date format: YYYY/MM/DD

[MS-TCC]: Tethering Control Channel Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-TDS]: Tabular Data Stream Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

Errata below are for Protocol Document Version V8.0 – 2015/10/16.

Errata Published*	Description
2016/02/22	In Section 1.2.1, Normative References, and Section 2.2.1, Client and Server Hello Messages, replaced all references to [IETFDRAFT-TLSHASH-03] with [RFC7627]. In Section 1.2.1, Normative References, changed from: [IETFDRAFT-TLSHASH-03] Bhargaven, K., Delignat-Lavaud, A., Pironti, A., Paris-Rocquencourt, Inria, Langley, A., and Ray, M., "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension", draft-ietf-tls-session-hash-03, November 2014, https://tools.ietf.org/html/draft-ietf-tls-session-hash-03 Changed to: [RFC7627] Bhargaven, K., Delignat-Lavaud, A., Pironti, A., Paris-Rocquencourt, Inria, Langley, A., and Ray, M., "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension", RFC 7627, September 2015, https://tools.ietf.org/html/rfc7627 In Section 2.2.1, Client and Server Hello Messages, changed from: Cipher suites and capabilities are negotiated as specified in [IETFDRAFT-TLSHASH-03]<3>, [RFC5246], [RFC2246], [RFC4492], and [RFC3268].<4><5><6> Changed to: Cipher suites and capabilities are negotiated as specified in [RFC7627]<3>, [RFC5246], [RFC2246], [RFC4492], and [RFC3268].<4><5><6>

* 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

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-TSCH]: Task Scheduler Service Remoting Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V22.0 – 2015/10/16.

Errata Published*	Description

2015/11/23	In Section 3.2.5.4.6, SchRpcGetSecurity (Opnum 5), corrected the definition of IDL operation SchRpcGetSecurity to be consistent with the definition in Appendix A: Full IDL.
	
	Changed from:
	The SchRpcGetSecurity method MUST get the security descriptor associated with a task or folder.
	`HRESULT SchRpcGetSecurity(`
	`[in, string] const wchar_t* path,`
	`[in] SECURITY_INFORMATION securityInformation,`
	`[out, string] const wchar_t** sddl`
	`);`
	path: MUST be the full path associated with a task or folder in the format specified in section 2.3.11).
	securityInformation: MUST contain security information in the format of a SECURITY_INFORMATION structure. The SECURITY_INFORMATION structure is defined in [MS-DTYP] section 2.4.7.
	sddl: MUST be a security descriptor in SDDL. MUST be encoded as a SECURITY_INFORMATION structure ([MS-DTYP] section 2.4.7).
	
	Changed to:
	The SchRpcGetSecurity method MUST get the security descriptor associated with a task or folder.
	`HRESULT SchRpcGetSecurity(`
	`[in, string] const wchar_t* path,`
	`[in] DWORD securityInformation,`
	`[out, string] const wchar_t** sddl`
	`);`
	path: MUST be the full path associated with a task or folder in the format specified in section 2.3.11).
	securityInformation: MUST contain security information in the format of a SECURITY_INFORMATION structure. The SECURITY_INFORMATION structure is defined in [MS-DTYP] section 2.4.7.
	sddl: MUST point to a buffer that will receive security information in string format. The string format is specified in [MS-DTYP] section 2.5.1.

* 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

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V35.0 – 2015/10/16.

Errata Published*	Description
2016/01/25	In several sections, corrected descriptions of structure members as pointers to structures. In Section 2.2.9.2.1.6, TSG_PACKET_QUARENC_RESPONSE, changed from: versionCaps: A PTSG_PACKET_VERSIONCAPS structure, as specified in section 2.2.9.2.1.2. Changed to: versionCaps: A pointer to a TSG_PACKET_VERSIONCAPS structure, as specified in section 2.2.9.2.1.2. In Section 2.2.9.2.1.9.1, TSG_PACKET_TYPE_MESSAGE_UNION, changed from: consentMessage: A PTSG_PACKET_STRING_MESSAGE structure, as defined in section 2.2.9.2.1.9.1.1. This field is used if msgType field specified in section 2.2.9.2.1.9 is set to TSG_ASYNC_MESSAGE_CONSENT_MESSAGE. serviceMessage: A PTSG_PACKET_STRING_MESSAGE structure, as defined in section 2.2.9.2.1.9.1.1. This field is used if msgType field specified in section 2.2.9.2.1.9 is set to TSG_ASYNC_MESSAGE_SERVICE_MESSAGE. reauthMessage: A PTSG_PACKET_REAUTH_MESSAGE structure, as defined in section 2.2.9.2.1.9.1.2. This field is used if msgType field specified in section 2.2.9.2.1.9 is set to TSG_ASYNC_MESSAGE_REAUTH. Changed to: consentMessage: A pointer to a TSG_PACKET_STRING_MESSAGE structure, as defined in section 2.2.9.2.1.9.1.1. This field is used if msgType field specified in section 2.2.9.2.1.9 is set to TSG_ASYNC_MESSAGE_CONSENT_MESSAGE. serviceMessage: A pointer to a TSG_PACKET_STRING_MESSAGE structure, as defined in section 2.2.9.2.1.9.1.1. This field is used if msgType field specified in section 2.2.9.2.1.9 is set to TSG_ASYNC_MESSAGE_SERVICE_MESSAGE. reauthMessage: A pointer to a TSG_PACKET_REAUTH_MESSAGE structure, as defined in section 2.2.9.2.1.9.1.2. This field is used if msgType field specified in section 2.2.9.2.1.9 is set to TSG_ASYNC_MESSAGE_REAUTH.

Errata Published*	Description
	In Section 2.2.9.2.1.11.1, TSG_INITIAL_PACKET_TYPE_UNION, changed from: packetVersionCaps: A PTSG_PACKET_VERSIONCAPS structure as specified in section 2.2.9.2.1.2. packetAuth: A PTSG_PACKET_AUTH structure as specified in section 2.2.9.2.1.10. Changed to: packetVersionCaps: A pointer to a TSG_PACKET_VERSIONCAPS structure as specified in section 2.2.9.2.1.2. packetAuth: A pointer to a TSG_PACKET_AUTH structure as specified in section 2.2.9.2.1.10.

2016/01/25	In several sections, added an underline prefix to the initial structure declarations and italicized 'n' for the maximum range of the msgBuffer member of TSG_PACKET_STRING_MESSAGE to clarify that it is a meta-value determined by context as mentioned in a product behavior note.
	
	In Section 2.2.9.2.1.7, TSG_PACKET_CAPS_RESPONSE, changed from:
	
	typedef struct TSG_PACKET_CAPS_RESPONSE {
	
	Changed to:
	typedef struct _TSG_PACKET_CAPS_RESPONSE {
	
	In Section 2.2.9.2.1.8, TSG_PACKET_MSG_REQUEST, changed from:
	
	typedef struct TSG_PACKET_MSG_REQUEST {
	
	Changed to:
	typedef struct _TSG_PACKET_MSG_REQUEST {
	
	In Section 2.2.9.2.1.9.1.1, TSG_PACKET_STRING_MESSAGE, changed from:
	
	typedef struct TSG_PACKET_STRING_MESSAGE {
	
	Changed to:
	typedef struct _TSG_PACKET_STRING_MESSAGE {
	
	Changed from:
	
	n is not italicized in: [range(0,n)] unsigned long msgBytes;
	
	Changed to:
	n is italicized in: [range(0,n)] unsigned long msgBytes;
	
	In Section 2.2.9.2.1.9.1.2, TSG_PACKET_REAUTH_MESSAGE, changed from:
	
	typedef struct TSG_PACKET_REAUTH_MESSAGE {
	Changed to:
	typedef struct _TSG_PACKET_REAUTH_MESSAGE {

Errata Published*	Description
2016/01/25	In Section 3.8.3, Establishing a Connection, updated that the Authentication Cookie is generated by the RDP server, provided to the client, and then returned to the RDP server. Changed from: authCookieLen is the length of Authentication Cookie sent from the RDP server. Changed to: authCookieLen is the length of the Authentication Cookie, which was previously generated by the RDP server and provided to the client, that the client returns to the RDP server.

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V23.0 – 2015/10/16.

Errata Published*	Description
2015/11/09	In Section 7, Appendix B: Product Behavior, added the following preliminary statement to the top of the section since Windows Server 2016 Technical Preview is included in the applicability list: Note: Some of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as an aid to the reader.

* 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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-WCCE]: Windows Client Certificate Enrollment Protocol

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V39.0 – 2015/10/16.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2016/03/07</td><td>In two sections, removed unreferenced error codes from a table, added a missing code - 0x8007000D ERROR_INVALID_DATA – and revised the description of error code ERROR_INVALID_DATA.

In Section 2.2.4, Common Error Codes, changed from:

<table>
<tr><th>Return value/code</th><th>Description</th></tr>
<tr><td>0x80070002
ERROR_FILE_NOT_FOUND</td><td>The system cannot find the specified file.</td></tr>
<tr><td>0x80070003
ERROR_PATH_NOT_FOUND</td><td>The system cannot find the specified path.</td></tr>
<tr><td>0x80070006
ERROR_INVALID_HANDLE</td><td>The handle is not valid.</td></tr>
<tr><td>0x80074003
ERROR_INVALID_POINTER</td><td>The pointer is not valid.</td></tr>
<tr><td>0x80074004
CERTSRV_E_PROPERTY_EMPTY</td><td>A required property value is empty.</td></tr>
<tr><td>0x80070057
E_INVALIDARG</td><td>The parameter is incorrect.</td></tr>
<tr><td>0x80090003
NTE_BAD_KEY</td><td>The cryptographic key is not valid.</td></tr>
<tr><td>0x8009000F
ERROR_OBJECT_EXISTS</td><td>The object already exists.</td></tr>
<tr><td>0x80091004
CRYPT_E_INVALID_MSG_TYPE</td><td>The cryptographic message type is not valid.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td>0x8009200E
CRYPT_E_NO_SIGNER</td><td>The signed cryptographic message does not have a signer for the specified signer index.</td></tr>
<tr><td>0x8009310B
CRYPT_E_ASN1_BADTAG</td><td>The value for the ASN1 tag is not valid.</td></tr>
<tr><td>0x80093100
CRYPT_E_ASN1_ERROR</td><td>An ASN.1 encoding error exists.</td></tr>
</table>

Changed to:
<table>
<tr><th>Return value/code</th><th>Description</th></tr>
<tr><td>0x80070002
ERROR_FILE_NOT_FOUND</td><td>The system cannot find the specified file.</td></tr>
<tr><td>0x8007000D
ERROR_INVALID_DATA</td><td>The data is not valid.</td></tr>
<tr><td>0x80074004
CERTSRV_E_PROPERTY_EMPTY</td><td>A required property value is empty.</td></tr>
<tr><td>0x80070057
E_INVALIDARG</td><td>The parameter is incorrect.</td></tr>
<tr><td>0x80091004
CRYPT_E_INVALID_MSG_TYPE</td><td>The cryptographic message type is not valid.</td></tr>
<tr><td>0x8009200E
CRYPT_E_NO_SIGNER</td><td>The signed cryptographic message does not have a signer for the specified signer index.</td></tr>
</table>

In Section 3.2.1.4.2.1.4.2.2, Renewing a Certificate Request Using CMS and CMC Request Format, changed from:

TaggedRequest: This field contains a single PKCS #10 certificate request. If the content of this field is not exactly one PKCS #10 certificate request conforming to the rules specified in section 3.2.1.4.2.1.4.1.1, the CA MUST return 0x80007000D (ERROR_INVALID_DATA) to the client. In addition, the Attributes field in the PKCS #10 certificate request MUST include the szOID_RENEWAL_CERTIFICATE (1.3.6.1.4.1.311.13.1) attribute.

Changed to:
TaggedRequest: This field contains a single PKCS #10 certificate request. If the content of this field is not exactly one PKCS #10 certificate request conforming to the rules specified in section 3.2.1.4.2.1.4.1.1, the CA MUST return 0x8007000D (ERROR_INVALID_DATA) to the client. In addition, the Attributes field in the PKCS #10 certificate request MUST include the szOID_RENEWAL_CERTIFICATE (1.3.6.1.4.1.311.13.1) attribute.</td></tr>
<tr><td>2015/11/09</td><td>In various sections, some of the structure definitions, and parameter properties and datatypes of some method declarations have been updated to match the IDL. Also, a mention that the BYTE datatype is defined in [MS-DTYP] has been removed since it is defined in this specification.

In Section 2.2, Common Data Types, changed from:</td></tr>
</table>

Errata Published*	Description

	Data type definitions of HRESULT, BOOL, BYTE, LONG, wchar_t, and DWORD, used in the following sections, are as specified in [MS-RPCE], [MS- DTYP], and [MS-ERREF].
	
	Changed to:
	
	Data type definitions of HRESULT, BOOL, LONG, wchar_t, and DWORD, used in the following sections, are as specified in [MS-RPCE], [MS-DTYP], and [MS-ERREF].
	
	In Section 2.2.2.3, CATRANSPROP, changed from:
	
	`typedef struct {`
	
	Changed to:
	
	`typedef struct _CATRANSPROP {`
	
	In Section 2.2.2.4, CAINFO, changed from:
	
	`typedef struct {`
	`  ULONG cbSize;`
	`  LONG CAType;`
	`  ULONG cCASignatureCerts;`
	`  ULONG cCAExchangeCerts;`
	`  ULONG cExitAlgorithms;`
	`  LONG lPropIDMax;`
	`  LONG lRoleSeparationEnabled;`
	`  ULONG cKRACertUsedCount;`
	`  ULONG cKRACertCount;`
	`  ULONG fAdvancedServer;`
	`} CAINFO;`
	
	Changed to:
	
	`typedef struct _CAINFO {`
	`  DWORD cbSize;`
	`  long CAType;`
	`  DWORD cCASignatureCerts;`
	`  DWORD cCAExchangeCerts;`
	`  DWORD cExitAlgorithms;`
	`  long lPropIDMax;`
	`  long lRoleSeparationEnabled;`
	`  DWORD cKRACertUsedCount;`
	`  DWORD cKRACertCount;`
	`  DWORD fAdvancedServer;`

Errata Published*	Description
	} CAINFO; In Section 3.2.1.4.2.1, ICertRequestD::Request (Opnum 3), changed from: [in, string, unique] const wchar_t* pwszAuthority, [in, string, unique] const wchar_t* pwszAttributes, [in, ref] const CERTTRANSBLOB* pctbRequest, Changed to: [in, string, unique, range(1, 1536)] wchar_t const * pwszAuthority, [in, string, unique, range(1, 1536)] wchar_t const * pwszAttributes, [in, ref] CERTTRANSBLOB const * pctbRequest, In Section 3.2.1.4.2.2, ICertRequestD::GetCACert (Opnum 4), changed from: [in, unique, string] const wchar_t* pwszAuthority, Changed to: [in, string, unique, range(1, 1536)] wchar_t const * pwszAuthority, In Section 3.2.1.4.2.3, ICertRequestD::Ping (Opnum 5), changed from: [in, unique, string] const wchar_t* pwszAuthority Changed to: [in, string, unique, range(1, 1536)] wchar_t const * pwszAuthority In Section 3.2.1.4.3.1. ICertRequestD2::Request2 (Opnum 6), changed from:

Errata Published*	Description
	[in, string, unique] const wchar_t* pwszAuthority, [in, string, unique] const wchar_t* pwszSerialNumber, [in, string, unique] const wchar_t* pwszAttributes, [in, ref] const CERTTRANSBLOB* pctbRequest, Changed to: [in, string, unique, range(1, 1536)] wchar_t const * pwszAuthority, [in, string, unique, range(1, 64)] wchar_t const * pwszSerialNumber, [in, string, unique, range(1, 1536)] wchar_t const * pwszAttributes, [in, ref] CERTTRANSBLOB const * pctbRequest, In Section 3.2.1.4.3.2, ICertRequestD2::GetCAProperty (Opnum 7), changed from: [in, unique, string] const wchar_t* pwszAuthority, Changed to: [in, string, unique, range(1, 1536)] wchar_t const * pwszAuthority, In Section 3.2.1.4.3.3, ICertRequestD2::GetCAPropertyInfo (Opnum 8), changed from: [in, unique, string] const wchar_t* pwszAuthority, Changed to: [in, string, unique, range(1, 1536)] wchar_t const * pwszAuthority, In Section 3.2.1.4.3.4, ICertRequestD2::Ping2 (Opnum 9), changed from: [in, unique, string] const wchar_t* pwszAuthority Changed to: [in, string, unique, range(1, 1536)] wchar_t const * pwszAuthority

* Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V6.0 – 2015/10/16.

Errata Published*	Description

2016/03/21	In this document, added new content for 3 operation contracts.
	
	Added new sections:
	2.2.4.11 Client Notification Service
	2.2.4.11.1 NotificationResult
	The NotificationResult type describes the notification result in the client notification service.
	
	`<xs:complexType name="NotificationResult">`
	`<xs:sequence>`
	`<xs:element minOccurs="0" name="clientName" nillable="true" type="xs:string" />`
	`<xs:element minOccurs="0" name="result" type="xs:boolean" />`
	`</xs:sequence>`
	`</xs:complexType>`
	
	2.2.4.11.2 NotificationResults
	The NotificationResults type describes notification results in the client notification service.
	
	`<xs:complexType name="NotificationResults">`
	`<xs:sequence>`
	`<xs:list minOccurs="0" name="result" type="NotificationResult" />`
	`</xs:sequence>`
	`</xs:complexType>`
	
	…
	3.11.5.3 IClientNotificationProvider.NotifyClientByName
	The operation sends a notification message to a client by using the machine name.
	
	`<wsdl:operation name="NotifyClientByName">`
	`<wsdl:input`

Errata Published*	Description

```
    wsam:Action="http://tempuri.org/IClientNotificationProvider/NotifyClient
    ByName"
    message="tns:IClientNotificationProvider_NotifyClientByName_InputMessage
    " />
                <wsdl:output
    wsam:Action="http://tempuri.org/ClientNotificationProvider/NotifyClientB
    yNameResponse"
    message="tns:IClientNotificationProvider_NotifyClientByName_OutputMessag
    e" />
              </wsdl:operation>
```

3.11.5.3.1 Messages

3.11.5.3.1.1 IClientNotificationProvider_NotifyClientByName_InputMessage

This message is the request for the NotifyClientByName operation.

```
              <wsdl:message
    name="IClientNotificationProvider_NotifyClientByName_InputMessage">
                <wsdl:part name="parameters"
    element="tns:NotifyClientByName" />
              </wsdl:message>
```

The message MUST be sent with the following SOAP action:

http://tempuri.org/IClientNotificationProvider/NotifyClientByName

The body of the SOAP message MUST contain the NotifyClientByName element.

3.11.5.3.1.2 IClientNotificationProvider_NotifyClientByName_OutputMessage

This message is the response for the NotifyClientByName operation.

```
              <wsdl:message
    name="IClientNotificationProvider_NotifyClientByName_OutputMessage">
                <wsdl:part name="parameters"
    element="tns:NotifyClientByNameResponse" />
              </wsdl:message>
```

The message MUST be sent with the following SOAP action:

http://tempuri.org/ClientNotificationProvider/NotifyClientByNameResponse

The body of the SOAP message MUST contain the NotifyClientByNameResponse element.

3.11.5.3.2 Elements

3.11.5.3.2.1 NotifyClientByName

This element specifies input values for the NotifyClientByName operation.

```
              <xs:element name="NotifyClientByName">
                <xs:complexType>
                  <xs:sequence>
                    <xs:element minOccurs="0" name="name" nillable="true"
    type="xs:string" />
                    <xs:element minOccurs="0" name="messageId"
    type="xs:unsignedInt" />
                    <xs:element minOccurs="0" name="message" nillable="true"
    type="xs:string" />
```

Errata Published*	Description

```
                </xs:sequence>
              </xs:complexType>
            </xs:element>
```

3.11.5.3.2.2 NotifyClientByNameResponse

This element specifies output values for the NotifyClientByName operation.

```
            <xs:element name="NotifyClientByNameResponse">
              <xs:complexType>
                <xs:sequence>
                  <xs:element minOccurs="0"
name="NotifyClientByNameResult" type="xs:boolean" />
                </xs:sequence>
              </xs:complexType>
            </xs:element>
```

3.11.5.4 IClientNotificationProvider.NotifyClientById

The operation sends a notification message to a client by using the machine SID.

```
            <wsdl:operation name="NotifyClientById">
              <wsdl:input
wsam:Action="http://tempuri.org/IClientNotificationProvider/NotifyClient
ById"
message="tns:IClientNotificationProvider_NotifyClientById_InputMessage"
/>
              <wsdl:output
wsam:Action="http://tempuri.org/ClientNotificationProvider/NotifyClientB
yIdResponse"
message="tns:IClientNotificationProvider_NotifyClientById_OutputMessage"
/>
            </wsdl:operation>
```

3.11.5.4.1 Messages

3.11.5.4.1.1 IClientNotificationProvider_NotifyClientById_InputMessage

This message is the request for the NotifyClientById operation.

```
            <wsdl:message
name="IClientNotificationProvider_NotifyClientById_InputMessage">
              <wsdl:part name="parameters" element="tns:NotifyClientById"
/>
            </wsdl:message>
```

The message MUST be sent with the following SOAP action:

http://tempuri.org/IClientNotificationProvider/NotifyClientById

The body of the SOAP message MUST contain the NotifyClientById element.

3.11.5.4.1.2 IClientNotificationProvider_NotifyClientById_OutputMessage

This message is the response for the NotifyClientById operation.

```
            <wsdl:message
name="IClientNotificationProvider_NotifyClientById_OutputMessage">
              <wsdl:part name="parameters"
element="tns:NotifyClientByIdResponse" />
```

Errata Published*	Description
	</wsdl:message> The message MUST be sent with the following SOAP action: http://tempuri.org/ClientNotificationProvider/NotifyClientByIdResponse The body of the SOAP message MUST contain the NotifyClientByIdResponse element. **3.11.5.4.2 Elements** **3.11.5.4.2.1 NotifyClientById** This element specifies input values for the NotifyClientById operation. <xs:element name="NotifyClientById"> <xs:complexType> <xs:sequence> <xs:element minOccurs="0" name="id" nillable="true" type="xs:string" /> <xs:element minOccurs="0" name="messageId" type="xs:unsignedInt" /> <xs:element minOccurs="0" name="message" nillable="true" type="xs:string" /> </xs:sequence> </xs:complexType> </xs:element> **3.11.5.4.2.2 NotifyClientByIdResponse** This element specifies output values for the NotifyClientById operation. <xs:element name="NotifyClientByIdResponse"> <xs:complexType> <xs:sequence> <xs:element minOccurs="0" name="NotifyClientByIdResult" type="xs:boolean" /> </xs:sequence> </xs:complexType> </xs:element> **3.11.5.5 IClientNotificationProvider.NotifyAllClients** The operation sends notification messages to all the online clients. <wsdl:operation name="NotifyAllClients"> <wsdl:input wsam:Action="http://tempuri.org/IClientNotificationProvider/NotifyAllClients" message="tns:IClientNotificationProvider_NotifyAllClients_InputMessage" /> <wsdl:output wsam:Action="http://tempuri.org/ClientNotificationProvider/NotifyAllClientsResponse" message="tns:IClientNotificationProvider_NotifyAllClients_OutputMessage" /> </wsdl:operation>

Errata Published*	Description

	3.11.5.5.1 Messages
	3.11.5.5.1.1 IClientNotificationProvider_NotifyAllClients_InputMessage
	This message is the request for the NotifyAllClients operation.
	
	`<wsdl:message name="IClientNotificationProvider_NotifyAllClients_InputMessage"> <wsdl:part name="parameters" element="tns:NotifyAllClients" /> </wsdl:message>`
	
	The message MUST be sent with the following SOAP action:
	http://tempuri.org/IClientNotificationProvider/NotifyAllClients
	The body of the SOAP message MUST contain the NotifyAllClients element.
	
	3.11.5.5.1.2 IClientNotificationProvider_NotifyAllClients_OutputMessage
	This message is the response for the NotifyAllClients operation.
	
	`<wsdl:message name="IClientNotificationProvider_NotifyAllClients_OutputMessage"> <wsdl:part name="parameters" element="tns:NotifyAllClientsResponse" /> </wsdl:message>`
	
	The message MUST be sent with the following SOAP action:
	http://tempuri.org/ClientNotificationProvider/NotifyAllClientsResponse
	The body of the SOAP message MUST contain the NotifyAllClientsResponse element.
	
	3.11.5.5.2 Elements
	3.11.5.5.2.1 NotifyAllClients
	This element specifies input values for the NotifyAllClients operation.
	
	`<xs:element name="NotifyAllClients"> <xs:complexType> <xs:sequence> <xs:element minOccurs="0" name="messageId" type="xs:unsignedInt" /> <xs:element minOccurs="0" name="message" nillable="true" type="xs:string" /> </xs:sequence> </xs:complexType> </xs:element>`
	
	3.11.5.5.2.2 NotifyAllClientsResponse
	This element specifies output values for the NotifyAllClients operation.
	
	`<xs:element name="NotifyAllClientsResponse"> <xs:complexType> <xs:sequence> <xs:element minOccurs="0" name="NotifyAllClientsResult" type="NotificationResults" />`

Errata Published*	Description
	</xs:sequence> </xs:complexType> </xs:element>

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-WKST]: Workstation Service Remote Protocol

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

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

RSS
Atom

Errata below are for Protocol Document Version V26.0 – 2015/10/16.

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td>2016/04/18</td><td>
In three sections, corrected the name used for a return value.

In Section 3.2.4.1, NetrWkstaGetInfo (Opnum 0), changed from:

Return Values: When the message processing result meets the description in column two of the following table, this method MUST return one of the following values ([MS-ERREF] section 2.2).

<table>
<tr><th>Return value/code</th><th>Description</th></tr>
<tr><td>0x00000000
ERROR_SUCCESS</td><td>The operation completed successfully.</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>

Changed to:
Return Values: When the message processing result meets the description in column two of the following table, this method MUST return one of the following values ([MS-ERREF] section 2.2).

<table>
<tr><th>Return value/code</th><th>Description</th></tr>
<tr><td>0x00000000
NERR_Success</td><td>The operation completed successfully.</td></tr>
<tr><td>…</td><td>…</td></tr>
</table>

In Section 4.1, NetrWkstaGetInfo Example, changed from:
…
<pre>
        (type unsigned long)return_status = ERROR_SUCCESS
        NetrWkstaGetInfo (
            [in,string,unique] WKSSVC_IDENTIFY_HANDLE ServerName
                    = {unchanged},
            [in] unsigned long Level = {unchanged},
            [out, switch_is(Level)] LPWKSTA_INFO WkstaInfo
                    = {filled in as shown below}
            );
</pre>
</td></tr>
</table>

Errata Published*	Description

	Changed to:
	…
	`(type unsigned long)return_status = NERR_Success`
	`NetrWkstaGetInfo (`
	`[in,string,unique] WKSSVC_IDENTIFY_HANDLE ServerName`
	`= {unchanged},`
	`[in] unsigned long Level = {unchanged},`
	`[out, switch_is(Level)] LPWKSTA_INFO WkstaInfo`
	`= {filled in as shown below}`
	`);`
	
	In Section 4.2, NetrWkstaUserEnum Example, changed from:
	…
	On receiving this method, the server executes the method locally to continue enumeration based on a ResumeHandle value of 0x00000120, and returns ERROR_SUCCESS. The server returns the names of the next three logged-on users in the UserInfo parameter. It also sets the value of TotalEntries to 0x00000005. The value of ResumeHandle is irrelevant.
	
	Changed to:
	…
	On receiving this method, the server executes the method locally to continue enumeration based on a ResumeHandle value of 0x00000120, and returns NERR_Success. The server returns the names of the next three logged-on users in the UserInfo parameter. It also sets the value of TotalEntries to 0x00000005. The value of ResumeHandle is irrelevant.

*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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

[MS-WMF]: Windows Metafile Format

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-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 versions of this document, see the following ERRATA Archives:

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V29.0 – 2015/10/16.

Errata Published*	Description
2016/06/27	In Sections 2.2.9.1.1.1, HTTP Headers, 2.2.9.1.2.1, HTTP Headers, 2.2.9.1.3.1.1, HTTP Headers, and 2.2.9.1.3.2.1, HTTP Headers, updated that the protocolvalue token contains the authentication mechanism that is used to establish the security encryption context. For example, in Section 2.2.9.1.1.1, HTTP Headers, changed from: protocolvalue: Contains the authentication mechanism that is used to establish the security token. It MUST be set to "application/HTTP-SPNEGO-session-encrypted", which indicates the security context that is obtained from authentication by using SPNEGO over HTTP, as specified in [RFC4559] section 6, and is used to encrypt the message. Changed to: protocolvalue: Contains the authentication mechanism that is used to establish the encryption context. It MUST be set to "application/HTTP-SPNEGO-session-encrypted", which indicates the security context that is obtained from authentication by using SPNEGO over HTTP, as specified in [RFC4559] section 6, and is used to encrypt the message. In Section 2.9.1.2.2.2, Encrypted Data, updated that the Length-Field token specifies the length of the per-message token portion of the Message field. Changed from: Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of the encryption header portion of the Message field. Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework specific to the authentication protocol selected by SPNEGO. SPNEGO can select Kerberos or NTLM as the underlying authentication protocol. For Kerberos, the framework is as specified in [RFC4121]. For NTLM, the encryption details are as described in [MS-NLMP]. The initial bytes of the Message vary based on the chosen authentication protocol: • For Kerberos, it MUST be the per-message token as specified in [RFC4121].

Errata Published*	Description
	• For NTLM, it MUST be its Message Signature. The length of the initial bytes of the Message 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 2.2.9.1.1.2.1. Changed to: Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of the encryption header portion of the Message field (see the discussion of the Message encryption header that follows). Message: The encrypted message. This is an octet stream of the encrypted SOAP message, which is encrypted and integrity-protected by using the framework specific to the authentication protocol selected by SPNEGO. SPNEGO can select Kerberos or NTLM as the underlying authentication protocol. For Kerberos, the framework is as specified in [RFC4121]. For NTLM, the encryption details are as described in [MS-NLMP]. The encryption header of the Message token varies based on the chosen authentication protocol: For Kerberos, it MUST be the per-message token as specified in [RFC4121]. • For NTLM, it MUST be its Message Signature. The length of the encryption header of Message 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 2.2.9.1.1.2.1. In Section 2.2.9.1.1.2.2, Encrypted Data, clarified that the Message token encryption header varies based on the chosen authentication protocol. Changed from: Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of the security token portion of the Message field. 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. Changed to: Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of the per-message token, as specified in [RFC4121], portion of the Message field. 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 per-message 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

Errata Published*	Description
2016/02/22	In several subsections, clarified the use of TLS encryption. In Section 2.2.9.1.3, CredSSPEncryptedMessage, updated that CredSSPEncryptedMessage message can be encrypted by the Transport Layer Security (TLS) security context established as part of the CredSSP protocol. Changed from: This message is used when CredSSP, as specified in [MS-CSSP], is used for setting up a security context between the client and server. The client and server can encrypt the message by using the GSS-API security context.<41> Changed to: This message is used when CredSSP, as specified in [MS-CSSP], is used for setting up a security context between the client and server. The client and server can encrypt the message by using the Transport Layer Security (TLS) security context established as part of the CredSSP protocol.<41> In Section 2.2.9.1.3.1.2.2, Encrypted Data, updated that EncryptedData message is an octet stream of TLS encrypted SOAP message. Changed from: ... Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of the security token portion of the Message field. 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. Changed to: ... Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of any trailer portion of the Message field. Message: The encrypted message. This is an octet stream of TLS encrypted SOAP message. In Section 2.2.9.1.3.2.2.2, Encrypted Data, updated that EncryptedData message is an octet stream of TLS encrypted SOAP message. Changed from: ... Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of the security token portion of the Message field. 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. Changed to:

Errata Published*	Description
	... Length-Field: The Length-Field MUST follow immediately after the previous token. It MUST be a 32-bit unsigned integer that specifies the length of any trailer portion of the Message field. Message: The encrypted message. This is an octet stream of TLS encrypted SOAP message.

*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

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

October 16, 2015 - Download

June 30, 2015 - Download

[MS-WSUSAR]: Windows Server Update Services: Administrative API Remoting Protocol

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

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

RSS
Atom

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

Errata Published*	Description
2016/04/18	The changes summarized below are relevant for Windows Server 2012 and Windows Server 2012 R2 with [MSKB-3148812] and Windows Server 2016 Technical Preview. View this Word document to see the information added: MS-WSUSAR_diff_0315_0407_forErrata. In Section 2.2.4.10, ConfigurationTableRow, added the MaxUpdatesPerRequestInGetUpdateDecryptionData field. In Section 3.1.4.77.3.4, ServerSyncUrlData, and Section 3.1.4.85.3.7, ExportFileData, added the DecryptionKey field. In Section 3.1.4.85.3.1, ArrayOfExportFileData, updated that the ExportFileData contains the name, digest, decryption key, and URL path for the updates. In Section 6, Appendix A: Full WSDL, added the MaxUpdatesPerRequestInGetUpdateDecryptionData and DecryptionKey fields.
2016/02/22	In Section 3.1.4.46.3.1, ExecuteSetSigningCertificateRequestBody, changed the field name PFXFileConent to PFXFileContent. Changed from: passwordBytes: This field MUST be present, if the PFXFileConent field is present and the private key of the certificate is password protected. It contains a base64 encoded representation of an array of bytes that comprise the password to protect the private key of the certificate. Changed to: passwordBytes: This field MUST be present, if the PFXFileContent field is present and the private key of the certificate is password protected. It contains a base64 encoded representation of an array of bytes that comprise the password to protect the private key of the certificate.
2016/01/25	In several subsections under sections under Section 3.1.4, Message Processing Events and Sequencing Rules, updated the pseudocode to correct the minOccurs value. To download a Word document with the changes, see [MS-WSUSAR]_01_25_DIFF.
2016/01/25	There is no definition for "SetAutomaticUpdateApprovalRule1" in Section 6, Appendix A: Full WSDL, so Section 3.1.4.64 SetAutomaticUpdateApprovalRule1 has been removed.

*Date format: YYYY/MM/DD

[MS-WSUSSS]: Windows Update Services: Server-Server Protocol

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

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

RSS
Atom

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

Errata Published*	Description
2016/04/18	The changes summarized below are relevant for Windows Server 2012 and Windows Server 2012 R2 with [MSKB-3148812] and Windows Server 2016 Technical Preview. View this Word document to see the information added: MS-WSUSSS_diff_0317_0408_forErrata. In the following sections, added the GetUpdateDecryptionData method: 3.1.4.18 GetUpdateDecryptionData 3.1.4.18.1 Messages 3.1.4.18.1.1 GetUpdateDecryptionDataSoapIn 3.1.4.18.1.2 GetUpdateDecryptionDataSoapOut 3.1.4.18.2 Elements 3.1.4.18.2.1 GetUpdateDecryptionData 3.1.4.18.2.2 GetUpdateDecryptionDataResponse 3.1.4.18.3 Complex Types 3.1.4.18.3.1 ServerDecryptionData 3.1.4.18.3.2 ArrayOfServerSyncUpdateFileDecryption 3.1.4.18.3.3 ServerSyncUpdateFileDecryption 3.1.4.18.3.4 ArrayOfServerSyncFileDecryption 3.1.4.18.3.5 ServerSyncFileDecryption In the following sections, added the MaxUpdatesPerRequestInGetUpdateDecryptionData configuration element: 3.1.4.4 GetConfigData 3.1.4.4.3.1 ServerSyncConfigData In Section 6.1, Server Sync Web Service, added the GetUpdateDecryptionData method and the MaxUpdatesPerRequestInGetUpdateDecryptionData configuration element.
2016/01/25	In Section 3.1.4.7, GetDriverIdList, and Section 3.1.4.8, GetDriverSetData, specified that the method is invoked only when an upstream server (USS) syncs with Microsoft Update and replaced all references to "DSS" with "Microsoft Update". In Section 3.1.4.7, GetDriverIdList, changed from: Note: All of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as an aid to the reader. A DSS SHOULD<32> call the GetDriverIdList method to get driver revisions and driver sets for

Errata Published*	Description

	new driver updates. The DSS provides filters to be used to prune the list of revisions.
	
	`<wsdl:operation name="GetRevisionIdList">`
	`<wsdl:input message="tns:GetDriverIdListSoapIn" />`
	`<wsdl:output message="tns:GetDriverIdListSoapOut" />`
	`</wsdl:operation>`
	`The SOAP operation is defined as follows.`
	`<wsdl:operation name="GetDriverIdList">`
	`<soap:operation`
	`soapAction="http://www.microsoft.com/SoftwareDistribution/GetDriverIdList"`
	`style="document" />`
	`</wsdl:operation>`
	
	Request validation:
	The USS validates inputs as specified in the following table. If any of the inputs are not valid, the USS MUST return a SOAP fault message to the DSS with the ErrorCode set, as shown in the table.
	…
	Data processing:
	The USS MUST compose a GetDriverIdListResponse message as follows:
	1. The method checks that the number of computer Ids and device hardware Ids is not greater than the maximum configuration value that is returned to the caller in the GetConfigData method.
	2. If the caller specifies more Ids, FaultException is returned.
	3. The method looks at computer hardware Ids and PNP hardware Ids specified by the DSS and sends the corresponding driver set identities and the referenced driver identities back.
	4. If categories are specified and no values t are valid, the method returns an empty result (no exception).
	5. When only some categories are invalid, the invalid categories are ignored and the method continues to return driver sets/drivers matching ComputerIds and PnpHardwareIds with the correct operating system and category prerequisites.
	6. If ComputerIds contains a computer Id that the system is unaware of, that computer Id is ignored.
	7. Set the Anchor field in the response to mark the time this operation completed.
	Response:
	If no errors occur during processing, the USS MUST return the success response to the DSS.
	If an error occurs during processing, the USS MUST return a SOAP fault. The SOAP fault SHOULD contain an <ErrorCode> element, as described in section 2.2.9. If the SOAP fault contains an <ErrorCode> element, its value MUST be one of the following.
	If the DSS receives a SOAP fault containing an <ErrorCode> element, it MUST react to the fault, with one of the following errors defined in section 2.2.9.3.
	▪ InvalidParameters
	▪ InternalServerError
	▪ InvalidCookie
	▪ IncompatibleProtocolVersion
	If the DSS receives a fault that does not contain an <ErrorCode> element, it MUST stop the protocol.
	
	Changed to:
	Note: All of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as an aid to the reader.
	The GetDriverIdList method SHOULD<32> get driver revisions and driver sets for new driver updates. This method is invoked only when an upstream server (USS) syncs with Microsoft

Errata Published*	Description

	Update.
	
	`<wsdl:operation name="GetRevisionIdList">`
	`<wsdl:input message="tns:GetDriverIdListSoapIn" />`
	`<wsdl:output message="tns:GetDriverIdListSoapOut" />`
	`</wsdl:operation>`
	The SOAP operation is defined as follows.
	`<wsdl:operation name="GetDriverIdList">`
	`<soap:operation soapAction="http://www.microsoft.com/SoftwareDistribution/GetDriverIdList" style="document" />`
	`</wsdl:operation>`
	
	Request validation:
	The USS validates inputs as specified in the following table. If any of the inputs are not valid, the USS MUST return a SOAP fault message to Microsoft Update with the ErrorCode set, as shown in the table.
	…
	Data processing:
	The USS MUST compose a GetDriverIdListResponse message as follows:
	1. The method checks that the number of computer Ids and device hardware Ids is not greater than the maximum configuration value that is returned to the caller in the GetConfigData method.
	2. If the caller specifies more Ids, FaultException is returned.
	3. The method looks at computer hardware Ids and PNP hardware Ids specified by Microsoft Update and sends the corresponding driver set identities and the referenced driver identities back.
	4. If categories are specified and no values t are valid, the method returns an empty result (no exception).
	5. When only some categories are invalid, the invalid categories are ignored and the method continues to return driver sets/drivers matching ComputerIds and PnpHardwareIds with the correct operating system and category prerequisites.
	6. If ComputerIds contains a computer Id that the system is unaware of, that computer Id is ignored.
	7. Set the Anchor field in the response to mark the time this operation completed.
	Response:
	If no errors occur during processing, the USS MUST return the success response.
	If an error occurs during processing, the USS MUST return a SOAP fault. The SOAP fault SHOULD contain an <ErrorCode> element, as described in section 2.2.9. If the SOAP fault contains an <ErrorCode> element, its value MUST be one of the following.
	If Microsoft Update receives a SOAP fault containing an <ErrorCode> element, it MUST react to the fault, with one of the following errors defined in section 2.2.9.3.
	▪ InvalidParameters
	▪ InternalServerError
	▪ InvalidCookie
	▪ IncompatibleProtocolVersion
	If a fault that does not contain an <ErrorCode> element is received, the protocol MUST be stopped.
	
	In Section 3.1.4.8, GetDriverSetData, changed from:
	
	Note: All of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
an aid to the reader.
A DSS SHOULD<35> call the GetDriverSetData method to get a list of driver set identities and their corresponding driver targeting XMLs. The DSS provides a list of driver set identities as input.

<pre>
<wsdl:operation name="GetDriverSetData">
<wsdl:input message="tns:GetDriverSetDataSoapIn" />
<wsdl:output message="tns:GetDriverSetDataSoapOut" />
</wsdl:operation>
The SOAP operation is defined as follows.
    <wsdl:operation name="GetDriverSetData">
        <soap:operation
soapAction="http://www.microsoft.com/SoftwareDistribution/GetDriverSetData"
style="document" />
</wsdl:operation>
</pre>

Request validation:
The USS validates inputs as specified in the following table. If any of the inputs are not valid, the USS MUST return a SOAP fault message to the DSS with the <ErrorCode> set, as shown in the table.
…
Response:
If no errors occur during processing, the USS MUST return the success response to the DSS.
If an error occurs during processing, the USS MUST return a SOAP fault. The SOAP fault SHOULD contain an <ErrorCode> element, as described in section 2.2.9. If the SOAP fault contains an <ErrorCode> element, its value MUST be one of the following.
If the DSS receives a SOAP fault containing an <ErrorCode> element, it MUST react to the fault, as described in the following table. If the DSS receives a fault that does not contain an <ErrorCode> element, it MUST stop the protocol.
<table>
<tr><th>ErrorCode</th><th>Description</th></tr>
<tr><td>InvalidParameters</td><td>Parameters passed to a web method are not valid. The "message" part of the exception will contain the parameter name. The DSS MUST stop the protocol.</td></tr>
<tr><td>InternalServerError</td><td>An internal error occurred on the server. The DSS MUST stop the protocol.</td></tr>
<tr><td>InvalidCookie</td><td>The cookie has a syntax, formatting, or other error. The DSS MUST restart the protocol from the beginning.</td></tr>
<tr><td>IncompatibleProtocolVersion</td><td>The version of the protocol used by DSS is incompatible with the version used by USS. The DSS MUST stop the protocol.</td></tr>
<tr><td>TooManyIds</td><td>When the # of driver set ids specified is greater than defined by the MaxNumberOfDriverSetsPerRequest configuration value</td></tr>
</table>

Changed to:
Note: All of the information in this section is subject to change because it applies to a preliminary product version, and thus may differ from the final version of the software when released. All behavior notes that pertain to the preliminary product version contain specific references to it as
</td></tr>
</table>

<table>
<tr><th>Errata Published*</th><th>Description</th></tr>
<tr><td></td><td>
an aid to the reader.
The GetDriverSetData method SHOULD<35> get a list of driver set identities and their corresponding driver targeting XMLs. This method is only invoked when an upstream server (USS) syncs with Microsoft Update, which provides a list of driver set identities as input.

<pre>
<wsdl:operation name="GetDriverSetData">
<wsdl:input message="tns:GetDriverSetDataSoapIn" />
<wsdl:output message="tns:GetDriverSetDataSoapOut" />
</wsdl:operation>
The SOAP operation is defined as follows.
    <wsdl:operation name="GetDriverSetData">
        <soap:operation
soapAction="http://www.microsoft.com/SoftwareDistribution/GetDriverSetData"
style="document" />
</wsdl:operation>
</pre>

Request validation:
The USS validates inputs as specified in the following table. If any of the inputs are not valid, the USS MUST return a SOAP fault message with the <ErrorCode> set, as shown in the table.
…
Response:
If no errors occur during processing, the USS MUST return the success response.
If an error occurs during processing, the USS MUST return a SOAP fault. The SOAP fault SHOULD contain an <ErrorCode> element, as described in section 2.2.9. If the SOAP fault contains an <ErrorCode> element, its value MUST be one of the following.
If Microsoft Update receives a SOAP fault containing an <ErrorCode> element, it MUST react to the fault, as described in the following table. If it receives a fault that does not contain an <ErrorCode> element, it MUST stop the protocol.
<table>
<tr><th>ErrorCode</th><th>Description</th></tr>
<tr><td>InvalidParameters</td><td>Parameters passed to a web method are not valid. The "message" part of the exception will contain the parameter name. The protocol MUST be stopped.</td></tr>
<tr><td>InternalServerError</td><td>An internal error occurred on the server. The protocol MUST be stopped.</td></tr>
<tr><td>InvalidCookie</td><td>The cookie has a syntax, formatting, or other error. The protocol is restarted from the beginning.</td></tr>
<tr><td>IncompatibleProtocolVersion</td><td>The version of the protocol used by Microsoft Update is incompatible with the version used by USS. The protocol MUST be stopped.</td></tr>
<tr><td>TooManyIds</td><td>When the # of driver set ids specified is greater than defined by the MaxNumberOfDriverSetsPerRequest configuration value</td></tr>
</table>

Also replaced all references to "DSS" with "Microsoft Update" in the following sections:
Section 3.1.4.7.2.1 GetDriverIdList
Section 3.1.4.7.3.1 DriverSetAndRevisionIdList
Section 3.1.4.7.3.4 ServerSyncDriverFilter
</td></tr>
</table>

Errata Published*	Description
2016/01/25	In Section 6.1, Server Sync Web Service, updated the ServerSyncConfigData definition to be consistent with Section 3.1.4.4.3.1. Changed from: `<s:complexType name="ServerSyncConfigData"> <s:sequence> <s:element minOccurs="1" maxOccurs="1" name="CatalogOnlySync" type="s:boolean" /> <s:element minOccurs="1" maxOccurs="1" name="LazySync" type="s:boolean" /> <s:element minOccurs="1" maxOccurs="1" name="ServerHostsPsfFiles" type="s:boolean" /> <s:element minOccurs="1" maxOccurs="1" name="MaxNumberOfUpdatesPerRequest" type="s:int" /> <s:element minOccurs="0" maxOccurs="1" name="NewConfigAnchor" type="s:string" /> <s:element minOccurs="0" maxOccurs="1" name="ProtocolVersion" type="s:string" /> <s:element minOccurs="0" maxOccurs="1" name="LanguageUpdateList" type="tns:ArrayOfServerSyncLanguageData" /> </s:sequence> </s:complexType>`  Changed to:  `<s:complexType name="ServerSyncConfigData"> <s:sequence> <s:element minOccurs="1" maxOccurs="1" name="CatalogOnlySync" type="s:boolean" /> <s:element minOccurs="1" maxOccurs="1" name="LazySync" type="s:boolean" /> <s:element minOccurs="1" maxOccurs="1" name="ServerHostsPsfFiles" type="s:boolean" /> <s:element minOccurs="1" maxOccurs="1" name="MaxNumberOfUpdatesPerRequest" type="s:int" /> <s:element minOccurs="1" maxOccurs="1" name="MaxNumberOfDriverSetsPerRequest" type="s:int" /> <s:element minOccurs="1" maxOccurs="1" name="MaxNumberOfComputerIdsInRequest" type="s:int" /> <s:element minOccurs="0" maxOccurs="1" name="MaxNumberOfPnpHardwareIdsInRequest" type="s:int" /> <s:element minOccurs="0" maxOccurs="1" name="NewConfigAnchor" type="s:string" /> <s:element minOccurs="0" maxOccurs="1" name="ProtocolVersion" type="s:string" /> <s:element minOccurs="0" maxOccurs="1" name="LanguageUpdateList" type="tns:ArrayOfServerSyncLanguageData" /> </s:sequence>`
2015/11/23	In Section 4, Protocol Examples, added field 'ParentGroupID' to the element 'ServerSyncTargetGroup'. Changed from:

Errata Published*	Description
	<ServerSyncTargetGroup> <TargetGroupID>a0a08746-4dbe-4a37-9adf- 9e7652c0b421</TargetGroupID> <Name>All Computers</Name> <IsBuiltin>true</IsBuiltin> </ServerSyncTargetGroup> <ServerSyncTargetGroup> <TargetGroupID>b73ca6ed-5727-47f3-84de- 015e03f6a88a</TargetGroupID> <Name>Unassigned Computers</Name> <IsBuiltin>true</IsBuiltin> </ServerSyncTargetGroup> Changed to: <ServerSyncTargetGroup> <TargetGroupID>a0a08746-4dbe-4a37-9adf- 9e7652c0b421</TargetGroupID> <ParentGroupId>00000000-0000-0000-0000- 000000000000</ParentGroupId> <Name>All Computers</Name> <IsBuiltin>true</IsBuiltin> </ServerSyncTargetGroup> <ServerSyncTargetGroup> <TargetGroupID>b73ca6ed-5727-47f3-84de- 015e03f6a88a</TargetGroupID> <Name>Unassigned Computers</Name> <IsBuiltin>true</IsBuiltin> </ServerSyncTargetGroup>
2015/10/26	In Section 4, Protocol Examples, corrected the pseudocode. Changed from: … <soap:Body> <GetAuthorizationCookiexmlns="http://www.microsoft.com/SoftwareDistribution/Server/DssAuthWebService"> … Changed to: … <soap:Body> <GetAuthorizationCookie xmlns="http://www.microsoft.com/SoftwareDistribution/Server/DssAuthWebService"> …

*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

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

October 16, 2015 - Download

June 30, 2015 - Download

Errata below are for Protocol Document Version V24.0 – 2015/10/16.

Errata Published*	Description
2016/04/18	The changes summarized below are relevant for Windows Server 2012 and Windows Server 2012 R2 with [MSKB-3148812] and Windows Server 2016 Technical Preview. View this Word document to see the information added: MS-WUSP_diff_0316_0407_forErrata. In Section 2.2.2.2.10, GetExtendedUpdateInfo2, added the GetExtendedUpdateInfo2 method.
2016/01/11	In Section 2.2.2.4, Faults, added a missing description for tag <Method> in the faults 'detail' element. Changed from: <ErrorCode>errorCode</ErrorCode> <Message>message</Message> <ID>id</ID> … Changed to: <ErrorCode>errorCode</ErrorCode> <Message>message</Message> <ID>id</ID> <Method>method</Method> … **method:** A string indicating the web service method in which the fault occurred. This MAY be omitted.
2016/01/11	In Section 2.2.2.2.9, SyncPrinterCatalog, changed "SyncUpdatesResult" to "SyncPrinterCatalogResult". Changed from: **SyncUpdatesResult:** Upon successful completion of this operation, this element MUST be returned. The client SHOULD interpret this result, as specified in section 3.1.5.7. The format is the same as the one defined in the Response section of 2.2.2.2.4.

Errata Published*	Description
	Changed to: **SyncPrinterCatalogResult:** Upon successful completion of this operation, this element MUST be returned. The client SHOULD interpret this result, as specified in section 3.1.5.7. The format is the same as the one defined in the Response section of 2.2.2.2.4.

2016/01/11	In Section 2.2.2.2.1, GetConfig, updated minOccurs values in ConfigurationProperty to match the IDL in Section 6.2, Client Web Service WSDL.
	Changed from:
	ConfigurationProperty: Its format is as follows.
	
	`<s:complexType name="ConfigurationProperty">`
	`  <s:sequence>`
	`  <s:element minOccurs="1" maxOccurs="1" name="Name"`
	`  type="s:string" />`
	`  <s:element minOccurs="1" maxOccurs="1" name="Value"`
	`  type="s:string" />`
	`  </s:sequence>`
	`</s:complexType>`
	
	Changed to:
	ConfigurationProperty: Its format is as follows.
	
	`<s:complexType name="ConfigurationProperty">`
	`  <s:sequence>`
	`  <s:element minOccurs="0" maxOccurs="1" name="Name"`
	`  type="s:string" />`
	`  <s:element minOccurs="0" maxOccurs="1" name="Value"`
	`  type="s:string" />`
	`  </s:sequence>`
	`</s:complexType>`
	
	In Section 2.2.2.2.3, RegisterComputer, updated minOccurs values in computerInfo to match the IDL in Section 6.2, Client Web Service WSDL.
	
	Changed from:
	…
	
	`  <s:element minOccurs="0" maxOccurs="1" name="SuiteMask"`
	`  type="s:short" />`
	`  <s:element minOccurs="0" maxOccurs="1" name="OldProductType"`
	`  type="s:unsignedByte" />`
	`  <s:element minOccurs="0" maxOccurs="1" name="NewProductType"`
	`  type="s:int" />`
	`  <s:element minOccurs="0" maxOccurs="1" name="SystemMetrics"`
	`  type="s:int" />`
	`  <s:element minOccurs="0" maxOccurs="1" name="ClientVersionMajorNumber"`
	`  type="s:short" />`
	`  <s:element minOccurs="0" maxOccurs="1" name="ClientVersionMinorNumber"`
	`  type="s:short" />`
	`  <s:element minOccurs="0" maxOccurs="1" name="ClientVersionBuildNumber"`
	`  type="s:short" />`
	`  <s:element minOccurs="0" maxOccurs="1" name="ClientVersionQfeNumber"`
	` type="s:short" />

Errata Published*	Description
	… Changed to: <s:element minOccurs="1" maxOccurs="1" name="SuiteMask" type="s:short" /> <s:element minOccurs="1" maxOccurs="1" name="OldProductType" type="s:unsignedByte" /> <s:element minOccurs="1" maxOccurs="1" name="NewProductType" type="s:int" /> <s:element minOccurs="1" maxOccurs="1" name="SystemMetrics" type="s:int" /> <s:element minOccurs="1" maxOccurs="1" name="ClientVersionMajorNumber" type="s:short" /> <s:element minOccurs="1" maxOccurs="1" name="ClientVersionMinorNumber" type="s:short" /> <s:element minOccurs="1" maxOccurs="1" name="ClientVersionBuildNumber" type="s:short" /> <s:element minOccurs="1" maxOccurs="1" name="ClientVersionQfeNumber" type="s:short" /> …
2015/12/11	In Section 4 Protocol Examples, the protocol version was changed to 1.8 as defined in section 2.2.2.2. Changed from: 1.0 Changed to: 1.8

*Date format: YYYY/MM/DD

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

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

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

RSS
Atom

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

October 16, 2015 - Download

June 30, 2015 - Download