Microsoft

Remote Desktop Protocol IO Lab
March 20-22, 2023

RDP IO Lab

Microsoft

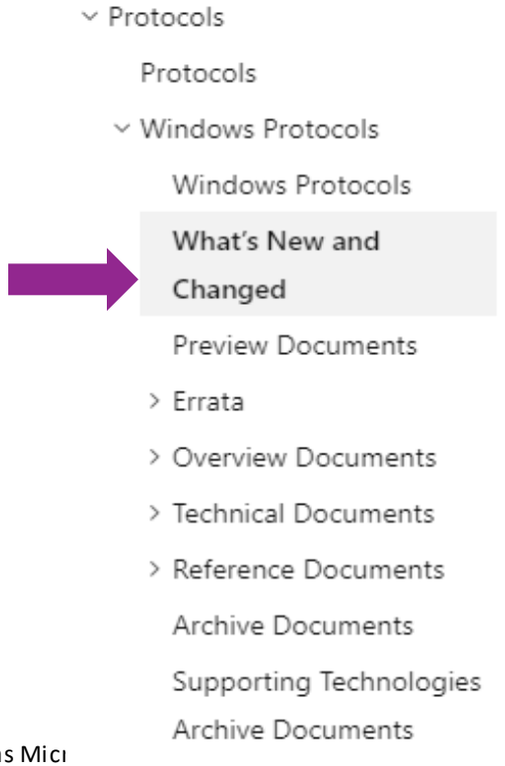
What's New in the RDP Protocols Documentation

Ron Starr
Senior Content Program Manager

Finding Changes

What's New and Changed

- High level overview of
  - New documents
  - Updated document
  - Bug fixes



Content Updates

The following documents were updated in April 2022 for service release updates and/or to fix content issues.

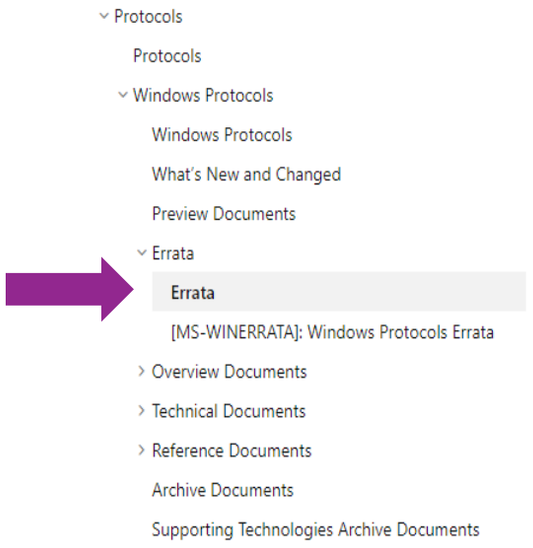
Specification	Content Updates
[MS-BKRP]: BackupKey Remote Protocol	List of Changes
[MS-CMRP]: Failover Cluster: Management API (ClusAPI) Protocol	List of Changes
[MS-DTYP]: Windows Data Types	List of Changes

The following technical documents were updated in April 2022 for Windows 11, version 22H2 operating system.

Specification	Description	Release Date
[MS-ADTS]: Active Directory Technical Specification	Specifies the core functionality of Active Directory. Active Directory extends and provides variations of the Lightweight Directory Access Protocol (LDAP). This document has been updated as follows: • Provided the ability to use LDAP limits to configure the maximum number of objects returned by the msds-TokenGroup* family constructed attributes. • Enabled information about root and child domains in trusting Active Directory forests to be queried and stored in existing msdsForestTrustInfo AD attribute; this information is then used for namespace filtering during NTLM pass-through authentications.	April 2022

Errata

- Contains the latest bug fixes
- Published every two weeks



Errata below are for Protocol Document Version V65.0 – 2021/10/06.

Errata Published*	Description
2022/04/19	In Section 2.2.25.1, Oplock Break Response, updated the text to correct the behavior to reflect the processing rule in section 3. Changed from: **OplockLevel (1 byte):** The server will set this field to the granted **OplockLevel** value. This MUST be the same as the level that is specified by the client in its oplock break acknowledgment packet. This field MUST contain one of the following values. Changed to: **OplockLevel (1 byte):** The server will set this field to the granted **OplockLevel** value. This field MUST contain one of the following values.

Landing Pages

This page and associated content may be updated frequently. We recommend you subscribe to the RSS feed to receive update notifications.

Published Version

Date	Protocol Revision	Revision Class	Downloads
9/3/2022	57.0	Major	PDF | DOCX | Diff

Click here to download a zip file of all PDF files for Windows Protocols.

Previous Versions

Date	Protocol Revision	Revision Class	Downloads
4/29/2022	56.0	Major	PDF | DOCX | Diff
6/25/2021	55.0	Major	PDF | DOCX | Errata | Diff
4/7/2021	54.0	Major	PDF | DOCX | Diff
8/26/2020	53.0	Major	PDF | DOCX | Errata | Diff

Diffs

Section headings

2.2.3.1.2 (Updated Section) SMB2_ENCRYPTION_CAPABILITIES

2.2.3.1.5 (Added Section) SMB2_TRANSPORT_CAPABILITIES

~~**2.2.2 (Removed Section) Multicast DNS Advertisement**~~

Content

- **Session.EncryptionKey**: ~~A~~For AES-128-CCM and AES-128-GCM encryption algorithms, this is a 128-bit key used for encrypting the messages ~~sent by the server~~. For AES-256-CCM and AES-256-GCM encryption algorithms, this is a 256-bit key used for encrypting the messages.
- **Session.DecryptionKey**: ~~A~~For AES-128-CCM and AES-128-GCM encryption algorithms, this is a 128-bit key used for decrypting the messages ~~received from~~. For AES-256-CCM and AES-256-GCM encryption algorithms, this is a 256-bit key used for decrypting the ~~client~~messages.

Change Tracking

- Bug fixes
- New features

Section	Description	Revision class
3.2.4.4 Re-establishing a Durable Open	11369 : Updated setting Epoch field in the case of re-establishing a durable open with SMB2_CREATE_REQUEST_LEASE_V2 create context.	Major
3.2.5.14.12 Handling a Validate Negotiate Info Response	11257 : Updated processing of validate negotiate info response when neither signed nor encrypted.	Major
3.3.5.2.1.1 Decrypting the Message	11286 : Updated processing of decrypting the message for both non-anonymous user is not authenitcated and authenticated cases.	Major
3.3.5.4 Receiving an SMB2 NEGOTIATE Request	11300 : Updated the SKU to reflect the behavior to 21H1 well.	Major
3.3.5.9 Receiving an SMB2 CREATE Request	11304 : Updated initialization of Open.ChannelSequence.	Major
3.3.5.15 Receiving an SMB2 IOCTL Request	11264 : Added the correct allowed FSCTL to right OS Version.	Minor

Change Notifications

- RSS
- ATOM

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

Article • 02/14/2023 • 2 minutes to read • 1 contributor

Feedback

This topic lists the Errata found in [MS-RDPEUDP2] since it was last published. Since this topic is updated frequ... we recommend that you 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 13, 2019 - Download

September 23, 2019 - Download

June 24, 2021 - Download

MS-RDPBCGR

MS-RDPBCGR

AAD Authentication

Section	Title	Notes
2.2.18	RDS AAD Auth PDUs	Five new sections on authenticating with AAD
4.11 ff.	RDS AAD and CloudAP	This and four subsections contain an example of using the cloud authentication provider package to help with RDS AAD Auth implementation
5.4.5.4	RDS AAD Auth Security	Brief descriptions of AAD auth (check this)
5.4.5.5	RDS AAD Auth Connection Sequence	Brief description of connection sequence (check this)

Channel Join

Section	Title	Notes
2.2.1.3.2	Client Core Data	New value for earlyCapabilityFlags - RNS_UD_CS_SUPPORT_SKIP_CHANNELJOIN - indicates client supports skipping MCS channel join request PDU & MCS channel join confirm PDU
2.2.1.4.2	Server Core Data	New value for earlyCapabilityFlags - RNS_UD_CS_SUPPORT_SKIP_CHANNELJOIN - indicates client supports skipping MCS channel join request PDU & MCS channel join confirm PDU
3.2.5.3.8	Sending MCS Channel Join Request PDU(s)	If client and server both set RNS_UD_CS_SUPPORT_SKIP_CHANNELJOIN, should skip channel join requests and channel join confirm
3.3.5.3.8	Processing MCS Channel Join Request PDU(s)	If server receives a channel join request pdu for channel already joined, should ignore request and not send channel join confirm
3.3.5.3.8	Processing MCS Channel Join Request PDU(s)	If client and server both set RNS_UD_CS_SUPPORT_SKIP_CHANNELJOIN, should skip channel join requests and channel join confirm, same as 3.2.5.3.8 -- but add more. Does more than just this.

MS-RDPBCGR

New Version Value

Section	Title	Notes
2.2.1.3.2	Client Core Data	New version value - 0x00080010 - for RDP 10.11 clients
2.2.1.4.2	Server Core Data	New version value - 0x00080010 - for RDP 10.11 clients

Security

Section	Title	Notes
5.4	Enhanced RDP Security	Added TLS 3.0 and RDS AAD Auth to list of external security protocols used for enhanced RDP security.
2.2.1.1.1	RDP Negotiation Request	New value added for "requestedProtocols" - PROTOCOL_RDSAAD for RDS AAD security
2.2.1.2.1	RDP Negotiation Response	New value added for "requestedProtocols" - PROTOCOL_RDSAAD for RDS AAD security
5.4.5	External Security Protocols Used by RDP	Added TLS 3.0 and RDS AAD Auth to list of external security protocols used for enhanced RDP security.

Servicing Updates

Section	Title	Notes
1.2.2	Informative References	References to KBs (KB5017380,KB5017381,KB5017383)

MS-RDPEAI

MS-RDPEAI

Format Change PDU

Section	Title	Notes
2.2.2.1	Version PDU (MSG_SNDIN_VERSION)	Version can be either 1 or 2. Affects use of the Format Change PDU
3.3.5.3.1	Sending a Format Change PDU	Details about how version value affects format change PDU. If version >=2, server should send format change if need diff AACcodec due to network

MS-RDPEGFX

MS-RDPEGFX

Capability Set 107

Section	Title	Notes
1.5.1	Client Implementation Requirements	Added implementations using capability set 107 to the list that must support RDPGFX_MAP_SURFACE_TO_SCALED_OUTPUT_PDU and RDPGFX_MAP_SURFACE_TO_SCALED_WINDOW_PDU
2.2.1.6	RDPGFX_CAPSET	Added RDPGFX_CAPVERSION_107 to the list of values for version in RDPGFX_CAPSET.
2.2.3.10	RDPGFX_CAPSET_VERSION107	Added new capability set for version 10.7 of the RDP graphics capability set

MS-RDPECLIP

MS-RDPECLIP

Examples

Section	Title	Notes
4.4.3.1	Requesting the Size of a File	Corrected example
4.4.3.2	Requesting the Contents of a File	Corrected example

MS-RDPEWA – New Document

MS-RDPEWA

Description

The Remote Desktop Protocol (RDP): WebAuthn Virtual Channel Protocol provides a way for a user to do WebAuthn operations over the RDP protocol. It enables a server to send a WebAuthn request to a client. The client can then use this request to talk to authenticators (platform or cross-platform) and reply with the response.

Messages

Uses two, request and response, perform different functions depending on content. Are CBOR encoded maps (see [IETF-8949]).

Protocols

Uses the [W3C-WebAuthPKC2] and [FIDO-CTAP] protocols.

Questions?

Questionnaire - https://forms.office.com/r/ThqKgz3aja

Microsoft