

[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.

Errata below are for Protocol Document Version [V19.0 – 2016/07/14](#).

Errata Published*	Description
2017/01/23	<p>In Section 2.2.5.5.4, SQL_VARIANT Values, the first sentence of the final paragraph is changed from:</p> <p>Note T data types cannot be NULL when inside a sql_variant.</p> <p>Changed to: Note Data types cannot be NULL when inside a sql_variant.</p> <p>In the first table in Section 2.2.6.4, LOGIN7, a product behavior note is added to the description of the OptionFlags2 parameter. The third bullet is changed from:</p> <ul style="list-style-type: none">• fODBC: Set if the client is the ODBC driver. This causes the server to set ANSI_DEFAULTS to ON, CURSOR_CLOSE_ON_COMMIT and IMPLICIT_TRANSACTIONS to OFF, TEXTSIZE to 0x7FFFFFFF (2GB) (TDS 7.2 and earlier), TEXTSIZE to infinite (introduced in TDS 7.3), and ROWCOUNT to infinite. <p>Changed to:</p> <ul style="list-style-type: none">• fODBC: Set if the client is the ODBC driver. This causes the server to set ANSI_DEFAULTS to ON, CURSOR_CLOSE_ON_COMMIT and IMPLICIT_TRANSACTIONS to OFF, TEXTSIZE to 0x7FFFFFFF (2GB) (TDS 7.2 and earlier), TEXTSIZE to infinite (introduced in TDS 7.3), and ROWCOUNT to infinite.<24> <p><24> Section 2.2.6.4: ANSI_DEFAULTS, CURSOR_CLOSE_ON_COMMIT, IMPLICIT_TRANSACTIONS, and ROWCOUNT are supported only by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014.</p> <p>In the second table in Section 2.2.6.4, LOGIN7, the FeatureId in the first row is changed from: %0x01 (SESSIONRECOVERY)</p> <p>Changed to: %0x01 (SESSIONRECOVERY) (introduced in TDS 7.4)</p> <p>Also in the second table in Section 2.2.6.4, LOGIN7, the FeatureData Description for %0x04 (COLUMNENCRYPTION) is changed. The last two paragraphs are changed from:</p>

Errata Published*	Description
	<p>COLUMNENCRYPTION_VERSION: This field describes the cryptographic protocol version that the client understands.</p> <p>Length: This field is the length of the COLUMNENCRYPTION_VERSION.</p> <p>Changed to: COLUMNENCRYPTION_VERSION: This field describes the cryptographic protocol version that the client understands. The value of COLUMNENCRYPTION_VERSION is 1.</p> <p>In Section 2.2.6.6, RPC Request, the following line of code is deleted: <pre>CekHash</pre> and replaced with the following lines: <pre>DatabaseId CekId CekVersion CekMDVersion</pre> </p> <p>The following line of code is changed from: <pre>ParamCipherInfo</pre> Changed to: <pre>[ParamCipherInfo]</pre> </p> <p>In the table in Section 2.2.6.6, RPC Request, the description of the OptionFlags parameter is changed and a product behavior note is added. The second bullet is changed from:</p> <ul style="list-style-type: none"> • fNoMetaData: 1 if the client has already cached the metadata for the result set from previous calls to the same RPC, and wants the server to avoid sending metadata by using NoMetaData (see COLMETADATA section 2.2.7.4). <p>Changed to:</p> <ul style="list-style-type: none"> • fNoMetaData: The server sends NoMetaData only if fNoMetadata is set to 1 in the request (see COLMETADATA section 2.2.7.4).<31> <p><31> Section 2.2.6.6: The option to have NoMetaData returned is not supported by SQL Server 2016.</p> <p>Also in the table in Section 2.2.6.6, RPC Request, the name of the "EmryptionAlgo" parameter is changed to "EncryptionAlgo" and the name of the "EncryptionName" parameter is changed to "EncryptionType".</p> <p>Also in the table in Section 2.2.6.6, RPC Request, the description of the NormVersion parameter is changed from:</p> <p>The normalization version to which plaintext data MUST be normalized. Version numbering starts at 0x01.</p> <p>Changed to:</p> <p>Reserved for future use. The value MUST be set to 1.</p> <p>Also in the table in Section 2.2.6.6, RPC Request, the following row is deleted:</p>

Errata Published*	Description																		
	<table border="1" data-bbox="391 275 1227 380"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>...</td> <td>...</td> </tr> <tr> <td>CekHash</td> <td>The hash of encryption key as reported by stored procedure <code>sp_describe_parameter_encryption</code>.</td> </tr> </tbody> </table> <p data-bbox="391 422 760 447">And the following rows are added:</p> <table border="1" data-bbox="391 485 1227 674"> <thead> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>...</td> <td>...</td> </tr> <tr> <td>DatabaseId</td> <td>A 4 byte integer value that represents the database ID where the column encryption key is stored.</td> </tr> <tr> <td>CekId</td> <td>An identifier for the column encryption key.</td> </tr> <tr> <td>CekVersion</td> <td>The key version of the column encryption key.</td> </tr> <tr> <td>CekMDVersion</td> <td>The metadata version for the column encryption key.</td> </tr> </tbody> </table> <p data-bbox="391 711 1349 762">Also in the table in Section 2.2.6.6, RPC Request, the description of the ParamCipherInfo parameter is changed from:</p> <p data-bbox="391 800 1385 905">Describes the parameter encryption information when that information is transparently encrypted. It defines the original TYPE_INFO of the data that is encrypted, the encryption algorithm that is used, and the normalization version, and hash of the encryption key that is used. This field MUST be sent only when fEncrypted is set to 1.</p> <p data-bbox="391 942 524 968">Changed to:</p> <p data-bbox="391 1005 1409 1157">Describes the parameter encryption information when the parameter is transparently encrypted. It defines the original TYPE_INFO of the data that is encrypted, the encryption algorithm that is used, the normalization version, the id of the database containing the column encryption key used for encryption, the id of the column encryption key, the version of the column encryption key and the version of the column encryption key metadata. These fields MUST be sent only when fEncrypted is set to 1.</p> <p data-bbox="391 1257 1328 1308">In the table in Section 2.2.7.1, ALTMETADATA, a product behavior note is added to the description of the TokenType parameter. The description is changed from:</p> <p data-bbox="391 1346 638 1371">ALTMETADATA_TOKEN</p> <p data-bbox="391 1409 524 1434">Changed to:</p> <p data-bbox="391 1472 695 1497">ALTMETADATA_TOKEN<33></p> <p data-bbox="391 1535 1349 1585"><33> Section 2.2.7.1: ALTMETADATA_TOKEN is supported only by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, and SQL Server 2008 R2.</p> <p data-bbox="391 1623 1417 1673">In the table in Section 2.2.7.2, ALTROW, a product behavior note is added to the description of the TokenType parameter. The description is changed from:</p> <p data-bbox="391 1711 573 1736">ALTROW_TOKEN</p> <p data-bbox="391 1774 524 1799">Changed to:</p> <p data-bbox="391 1837 634 1862">ALTROW_TOKEN<34></p>	Parameter	Description	CekHash	The hash of encryption key as reported by stored procedure <code>sp_describe_parameter_encryption</code> .	Parameter	Description	DatabaseId	A 4 byte integer value that represents the database ID where the column encryption key is stored.	CekId	An identifier for the column encryption key.	CekVersion	The key version of the column encryption key.	CekMDVersion	The metadata version for the column encryption key.
Parameter	Description																		
...	...																		
CekHash	The hash of encryption key as reported by stored procedure <code>sp_describe_parameter_encryption</code> .																		
Parameter	Description																		
...	...																		
DatabaseId	A 4 byte integer value that represents the database ID where the column encryption key is stored.																		
CekId	An identifier for the column encryption key.																		
CekVersion	The key version of the column encryption key.																		
CekMDVersion	The metadata version for the column encryption key.																		

Errata Published*	Description										
	<p data-bbox="375 268 1430 331"><34> Section 2.2.7.2: ALTROW_TOKEN is supported only by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, and SQL Server 2008 R2.</p> <p data-bbox="375 422 1430 453">In Section 2.2.7.4, COLMETADATA, the following line of code is changed from:</p> <pre data-bbox="440 506 1260 558">(usReserved / (FRESEVEDBIT fSparseColumnSet fEncrypted usReserved3)</pre> <p data-bbox="375 621 524 646">Changed to:</p> <pre data-bbox="440 699 1260 751">(usReserved / (FRESEVEDBIT fSparseColumnSet fEncrypted usReserved3))</pre> <p data-bbox="375 814 1276 842">Also in Section 2.2.7.4, COLMETADATA, the following line of code is changed from:</p> <pre data-bbox="727 894 927 919">CryptoMetaData</pre> <p data-bbox="375 982 524 1008">Changed to:</p> <pre data-bbox="732 1060 954 1085">[CryptoMetaData]</pre> <p data-bbox="375 1148 1321 1201">In the table in Section 2.2.7.4, COLMETADATA, added a product behavior note and the following rows are changed from:</p> <table border="1" data-bbox="391 1234 1227 1749"> <thead> <tr> <th data-bbox="391 1234 602 1276">Parameter</th> <th data-bbox="602 1234 1227 1276">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="391 1276 602 1318">...</td> <td data-bbox="602 1276 1227 1318">...</td> </tr> <tr> <td data-bbox="391 1318 602 1665">EncryptionAlgo</td> <td data-bbox="602 1318 1227 1665"> <p data-bbox="602 1329 1227 1381">A byte that describes the encryption algorithm that is used.</p> <p data-bbox="602 1392 1227 1497">If EncryptionAlgo is set to 0, a custom encryption algorithm is used and AlgoName MUST be sent. AlgoName is populated with the name of the custom encryption algorithm.</p> <p data-bbox="602 1507 1227 1560">For all EncryptionAlgo values other than 0, AlgoName MUST NOT be sent.</p> <p data-bbox="602 1591 1227 1665">If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4.</p> </td> </tr> <tr> <td data-bbox="391 1665 602 1717">AlgoName</td> <td data-bbox="602 1665 1227 1717">Algorithm name literal that is used to encrypt the plaintext value.</td> </tr> <tr> <td data-bbox="391 1717 602 1749">* * *</td> <td data-bbox="602 1717 1227 1749">* * *</td> </tr> </tbody> </table>	Parameter	Description	EncryptionAlgo	<p data-bbox="602 1329 1227 1381">A byte that describes the encryption algorithm that is used.</p> <p data-bbox="602 1392 1227 1497">If EncryptionAlgo is set to 0, a custom encryption algorithm is used and AlgoName MUST be sent. AlgoName is populated with the name of the custom encryption algorithm.</p> <p data-bbox="602 1507 1227 1560">For all EncryptionAlgo values other than 0, AlgoName MUST NOT be sent.</p> <p data-bbox="602 1591 1227 1665">If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4.</p>	AlgoName	Algorithm name literal that is used to encrypt the plaintext value.	* * *	* * *
Parameter	Description										
...	...										
EncryptionAlgo	<p data-bbox="602 1329 1227 1381">A byte that describes the encryption algorithm that is used.</p> <p data-bbox="602 1392 1227 1497">If EncryptionAlgo is set to 0, a custom encryption algorithm is used and AlgoName MUST be sent. AlgoName is populated with the name of the custom encryption algorithm.</p> <p data-bbox="602 1507 1227 1560">For all EncryptionAlgo values other than 0, AlgoName MUST NOT be sent.</p> <p data-bbox="602 1591 1227 1665">If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4.</p>										
AlgoName	Algorithm name literal that is used to encrypt the plaintext value.										
* * *	* * *										

Errata Published*	Description														
	<table border="1" data-bbox="391 275 1227 457"> <tr> <td data-bbox="391 275 597 457">NoMetaData</td> <td data-bbox="597 275 1227 457">This notifies client that no metadata will follow the COLMETADATA token. Client notifies the server that it has already cached the metadata from previous request, by setting fNoMetadata to 1 in RPC Request (section 2.2.6.6). The server SHOULD not send NoMetaData unless fNoMetadata is set to 1 in the request.</td> </tr> </table> <p data-bbox="391 495 521 520">Changed to:</p> <table border="1" data-bbox="391 558 1227 1083"> <thead> <tr> <th data-bbox="391 558 597 600">Parameter</th> <th data-bbox="597 558 1227 600">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="391 600 597 642">...</td> <td data-bbox="597 600 1227 642">...</td> </tr> <tr> <td data-bbox="391 642 597 842">EncryptionAlgo</td> <td data-bbox="597 642 1227 842">A byte that describes the encryption algorithm that is used. If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4. Other values are reserved for future use.</td> </tr> <tr> <td data-bbox="391 842 597 884">AlgoName</td> <td data-bbox="597 842 1227 884">Reserved for future use.</td> </tr> <tr> <td data-bbox="391 884 597 905">...</td> <td data-bbox="597 884 1227 905">...</td> </tr> <tr> <td data-bbox="391 905 597 1083">NoMetaData</td> <td data-bbox="597 905 1227 1083">This notifies client that no metadata will follow the COLMETADATA token. Client notifies the server that it has already cached the metadata from previous request, by setting fNoMetadata to 1 in RPC Request (section 2.2.6.6). The server sends NoMetaData only if fNoMetadata is set to 1 in the request.<36></td> </tr> </tbody> </table> <p data-bbox="391 1121 1354 1171"><36> Section 2.2.7.4: The option to have NoMetaData returned is not supported by SQL Server 2016.</p> <p data-bbox="391 1272 1133 1297">In Section 2.2.7.8, ENVCHANGE, the last paragraph is changed from:</p> <ul data-bbox="391 1335 1390 1465" style="list-style-type: none"> ▪ ENVCHANGE type 20 MAY be sent back to a client running TDS 7.4 or later whether or not the fReadOnlyIntent bit is set in the preceding LOGIN7 record. Type 20 MAY be sent to a TDS client running TDS 7.1 to 7.3 but only when the fReadOnlyIntent bit is set in the preceding LOGIN7 record. <p data-bbox="391 1503 521 1528">Changed to:</p> <ul data-bbox="391 1566 1370 1696" style="list-style-type: none"> ▪ ENVCHANGE type 20 can be sent back to a client running TDS 7.4 or later regardless of whether the fReadOnlyIntent bit is set in the preceding LOGIN7 record. If a client is running TDS 7.1 to 7.3, type 20 can be sent only if the fReadOnlyIntent bit is set in the preceding LOGIN7 record. <p data-bbox="391 1797 1390 1848">In the second table in Section 2.2.7.10, FEATUREEXTACK, the FeatureId in the second row is changed from:</p>	NoMetaData	This notifies client that no metadata will follow the COLMETADATA token. Client notifies the server that it has already cached the metadata from previous request, by setting fNoMetadata to 1 in RPC Request (section 2.2.6.6). The server SHOULD not send NoMetaData unless fNoMetadata is set to 1 in the request.	Parameter	Description	EncryptionAlgo	A byte that describes the encryption algorithm that is used. If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4. Other values are reserved for future use.	AlgoName	Reserved for future use.	NoMetaData	This notifies client that no metadata will follow the COLMETADATA token. Client notifies the server that it has already cached the metadata from previous request, by setting fNoMetadata to 1 in RPC Request (section 2.2.6.6). The server sends NoMetaData only if fNoMetadata is set to 1 in the request.<36>
NoMetaData	This notifies client that no metadata will follow the COLMETADATA token. Client notifies the server that it has already cached the metadata from previous request, by setting fNoMetadata to 1 in RPC Request (section 2.2.6.6). The server SHOULD not send NoMetaData unless fNoMetadata is set to 1 in the request.														
Parameter	Description														
...	...														
EncryptionAlgo	A byte that describes the encryption algorithm that is used. If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4. Other values are reserved for future use.														
AlgoName	Reserved for future use.														
...	...														
NoMetaData	This notifies client that no metadata will follow the COLMETADATA token. Client notifies the server that it has already cached the metadata from previous request, by setting fNoMetadata to 1 in RPC Request (section 2.2.6.6). The server sends NoMetaData only if fNoMetadata is set to 1 in the request.<36>														

Errata Published*	Description														
	<p data-bbox="389 273 625 325">%0x01 (SESSIONRECOVERY)</p> <p data-bbox="389 357 527 388">Changed to:</p> <p data-bbox="389 420 641 504">%0x01 (SESSIONRECOVERY) (introduced in TDS 7.4)</p> <p data-bbox="389 535 1396 588">Also in the second table in Section 2.2.7.10, FEATUREEXTACK, the following row with product behavior note is added:</p> <table border="1" data-bbox="389 619 1356 1176"> <thead> <tr> <th data-bbox="389 619 730 661">FeatureId</th> <th data-bbox="730 619 1356 661">FeatureExtData Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="389 661 730 703">...</td> <td data-bbox="730 661 1356 703">...</td> </tr> <tr> <td data-bbox="389 703 730 1176">%0x04 (COLUMNENCRYPTION)<46> (introduced in TDS 7.4)</td> <td data-bbox="730 703 1356 1176"> <p data-bbox="747 714 1339 829">Presence of COLUMNENCRYPTION FeatureExt indicates that the client is capable of performing cryptographic operations on data. The feature data is described as follows:</p> <table data-bbox="787 840 1339 1018"> <tr> <td data-bbox="787 840 1209 871">Length</td> <td data-bbox="1209 840 1339 871">= DWORD</td> </tr> <tr> <td data-bbox="787 871 1209 903">COLUMNENCRYPTION_VERSION</td> <td data-bbox="1209 871 1339 903">= BYTE</td> </tr> <tr> <td data-bbox="787 924 1209 955">FeatureData</td> <td data-bbox="1209 924 1339 955">= Length</td> </tr> <tr> <td data-bbox="787 976 1209 1008">COLUMNENCRYPTION_VERSION</td> <td data-bbox="1209 976 1339 1008"></td> </tr> </table> <p data-bbox="747 1060 1315 1176">COLUMNENCRYPTION_VERSION: This field describes the cryptographic protocol version that the client understands. The value of COLUMNENCRYPTION_VERSION is 1.</p> </td> </tr> </tbody> </table> <p data-bbox="389 1270 1388 1354"><46> Section 2.2.7.10: Column encryption is not supported by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014.</p> <p data-bbox="389 1449 1242 1480">In Section 2.2.7.18, RETURNVALUE, the following line of code is changed from:</p> <pre data-bbox="438 1533 1185 1564">(usReserved / (usReserved2 fEncrypted usReserved3))</pre> <p data-bbox="389 1617 527 1648">Changed to:</p> <pre data-bbox="438 1701 1193 1732">(usReserved / (usReserved2 fEncrypted usReserved3))</pre> <p data-bbox="389 1785 1315 1837">In the table in Section 2.2.7.18, RETURNVALUE, the description of the EncryptionAlgo parameter is changed from:</p>	FeatureId	FeatureExtData Description	%0x04 (COLUMNENCRYPTION)<46> (introduced in TDS 7.4)	<p data-bbox="747 714 1339 829">Presence of COLUMNENCRYPTION FeatureExt indicates that the client is capable of performing cryptographic operations on data. The feature data is described as follows:</p> <table data-bbox="787 840 1339 1018"> <tr> <td data-bbox="787 840 1209 871">Length</td> <td data-bbox="1209 840 1339 871">= DWORD</td> </tr> <tr> <td data-bbox="787 871 1209 903">COLUMNENCRYPTION_VERSION</td> <td data-bbox="1209 871 1339 903">= BYTE</td> </tr> <tr> <td data-bbox="787 924 1209 955">FeatureData</td> <td data-bbox="1209 924 1339 955">= Length</td> </tr> <tr> <td data-bbox="787 976 1209 1008">COLUMNENCRYPTION_VERSION</td> <td data-bbox="1209 976 1339 1008"></td> </tr> </table> <p data-bbox="747 1060 1315 1176">COLUMNENCRYPTION_VERSION: This field describes the cryptographic protocol version that the client understands. The value of COLUMNENCRYPTION_VERSION is 1.</p>	Length	= DWORD	COLUMNENCRYPTION_VERSION	= BYTE	FeatureData	= Length	COLUMNENCRYPTION_VERSION	
FeatureId	FeatureExtData Description														
...	...														
%0x04 (COLUMNENCRYPTION)<46> (introduced in TDS 7.4)	<p data-bbox="747 714 1339 829">Presence of COLUMNENCRYPTION FeatureExt indicates that the client is capable of performing cryptographic operations on data. The feature data is described as follows:</p> <table data-bbox="787 840 1339 1018"> <tr> <td data-bbox="787 840 1209 871">Length</td> <td data-bbox="1209 840 1339 871">= DWORD</td> </tr> <tr> <td data-bbox="787 871 1209 903">COLUMNENCRYPTION_VERSION</td> <td data-bbox="1209 871 1339 903">= BYTE</td> </tr> <tr> <td data-bbox="787 924 1209 955">FeatureData</td> <td data-bbox="1209 924 1339 955">= Length</td> </tr> <tr> <td data-bbox="787 976 1209 1008">COLUMNENCRYPTION_VERSION</td> <td data-bbox="1209 976 1339 1008"></td> </tr> </table> <p data-bbox="747 1060 1315 1176">COLUMNENCRYPTION_VERSION: This field describes the cryptographic protocol version that the client understands. The value of COLUMNENCRYPTION_VERSION is 1.</p>	Length	= DWORD	COLUMNENCRYPTION_VERSION	= BYTE	FeatureData	= Length	COLUMNENCRYPTION_VERSION							
Length	= DWORD														
COLUMNENCRYPTION_VERSION	= BYTE														
FeatureData	= Length														
COLUMNENCRYPTION_VERSION															

Errata Published*	Description
	<p>A byte that describes the encryption algorithm that is used. If EncryptionAlgo is set to 0, a custom encryption algorithm is used and AlgoName MUST be sent. AlgoName is populated with the name of the custom encryption algorithm. For all EncryptionAlgo values other than 0, AlgoName MUST NOT be sent. If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4.</p> <p>Changed to:</p> <p>A byte that describes the encryption algorithm that is used. AlgoName is populated with the name of the custom encryption algorithm. For all EncryptionAlgo values other than 0, AlgoName MUST NOT be sent. If EncryptionAlgo is set to 1, the algorithm that is used is AEAD_AES_256_CBC_HMAC_SHA512, as described in [IETF-AuthEncr] section 5.4.</p>
2016/08/29	<p>In Section 6, Appendix A: Product Behavior, product behavior notes <21>, <25>, <30>, and <31> are updated as follows.</p> <p>Note <21> is changed from: <21> Section 2.2.5.7: Column encryption is not supported by SQL Server. Changed to: <21> Section 2.2.5.7: Column encryption is not supported by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014.</p> <p>Note <25> is changed from: <25> Section 2.2.6.4: Column encryption is not supported by SQL Server. Changed to: <25> Section 2.2.6.4: Column encryption is not supported by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014.</p> <p>Note <30> is changed from: <30> Section 2.2.6.6: Column encryption is not supported by SQL Server. Changed to: <30> Section 2.2.6.6: Column encryption is not supported by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014.</p> <p>Note <31> is changed from: <31> Section 2.2.7.4: Column encryption is not supported by SQL Server. Changed to: <31> Section 2.2.7.4: Column encryption is not supported by SQL Server 7.0, SQL Server 2000, SQL Server 2005, SQL Server 2008, SQL Server 2008 R2, SQL Server 2012, and SQL Server 2014.</p>

*Date format: YYYY/MM/DD