COVIANT Software

ADMINISTRATOR GUIDE
DIPLOMAT MANAGED FILE TRANSFER
SQL AUDIT DATABASE
VERSION 9.2

V9.2

SQL AUDIT DATABASE

License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE.

Diplomat products may NOT be downloaded or otherwise exported or re-exported to any parties in Cuba, Iran, Libya, North Korea, Sudan, or Syria. You agree not to directly or indirectly export or re-export (including by transmission) these Diplomat products to any parties in the above countries without first obtaining any required export license or governmental approval.

By downloading or using Diplomat products, you are agreeing to the foregoing and you are representing and warranting that you are not located in and are not a national or resident of Cuba, Iran, Libya, North Korea, Sudan, or Syria.

DIPLOMAT PRODUCTS CONTAIN ENCRYPTION TECHNOLOGY THAT IS CONTROLLED FOR EXPORT BY THE U.S. BUREAU OF INDUSTRY AND SECURITY UNDER THE EXPORT ADMINISTRATION REGULATIONS. IN ADDITION TO OTHER RESTRICTIONS DESCRIBED IN THIS DOCUMENT AND THE DIPLOMAT LICENSE AGREEMENT, YOU MAY NOT USE DIPLOMAT PRODUCTS, OR EXPORT DIPLOMAT PRODUCTS TO ANY PARTY WHERE YOU KNOW, OR HAVE GOOD REASON TO BELIEVE, THAT DIPLOMAT PRODUCTS MAY BE USED IN CONNECTION WITH THE PROLIFERATION OF NUCLEAR, CHEMICAL OR BIOLOGICAL WEAPONS OR MISSILES.

Diplomat products are classified under ECCN 5D992B.1 with CCATS # G049200 as of June 14, 2006 which authorizes these products for export and re-export under Section 742.15 (B) (2) of the Export Administration Regulations (*Review Requirement for Mass Market Encryption Commodities and Software Exceeding 64 Bits*).

Contacting Coviant Software LLC
Installation and configuration support is provided under warranty for 45 days from initial purchase, as well as under annual maintenance agreements. Email and phone support is available from 9 a.m. ET to 5 p.m. ET weekdays. If you require assistance, contact Coviant Software support as follows:

Voice: 210.985.0985 x2

Web: www.coviantsoftware.com

E-mail: support@coviantsoftware.com

Table of Contents

1 SQL Audit Overview

Diplomat MFT Enterprise Edition allows the capture of audit data in a SQL database. SQL audit is recommended for enterprises with a high volume of jobs, stringent audit requirements, and/or the need for custom report generation.

Performance Optimization	Diplomat MFT Enterprise Edition is recommended for customers that anticipate the need to track the results of over 1000 jobs per week – or 50,000 file transfer jobs per year. Implementations of Diplomat MFT Standard Edition that use the standard audit capabilities may experience slower performance when handling high transaction volumes.
Stringent Audit Requirements	Diplomat MFT Enterprise Edition allows the user to treat the audit trail creation as a critical part of each job. If T*reat as Critical* is selected, all jobs are suspended if an audit problem is encountered.
Custom Report Generation	The SQL audit database created by Diplomat MFT Enterprise Edition can be accessed directly to generate custom reports. Diplomat MFT Standard Edition allows only standard report generation from the Reports menu.

Diplomat MFT Enterprise Edition also provides a feature for archiving audit records on a daily basis to optimize runtime and reporting performance – plus an Archive Now feature to archive records immediately. This feature is not intended to replace regular database maintenance for performance optimization.

2 Set-up

2.1 Database Set-up

Diplomat MFT supports a SQL database as part of the audit function. The SQL audit database has three tables to capture job, file, and user activity data and three tables in which to archive job, file, and user activity data plus a table that stores the DB version.

- **Jobs and Files Tables**
  Each time a Diplomat MFT job runs new records are written to the Jobs and Files tables in the SQL audit database.

- **User Activity Tables**
  Each time a user creates, updates, or deletes records in the Diplomat MFT transaction database and associated configuration files a new record is written to the User Activity table in the SQL audit database.

  NOTE: The user activity tables are NOT supported with Diplomat's built-in audit database. They are only supported as SQL tables.

- **Archive Jobs, Files, and User Activity Tables**
  If desired, Diplomat MFT can move records automatically from the Jobs, Files, and User Activity tables in the SQL audit database to the archive tables. The archive tables are identical in format to the Jobs, Files, and User Activity tables.

- **Diplomat MFT Database Version Table**
  This table stores the Diplomat MFT audit database version number. The version number is used by Diplomat MFT to ensure compatibility between the database and the Diplomat Managed File Transfer Service and Client.

2.1.1 SQL Databases Supported

Diplomat MFT supports MySQL, SQL Server and other ANSI SQL-92 compliant databases.

MySQL
MySQL is an open source database. Version 5.1 and higher of the MySQL database server.

SQL Server
Select *SQL Server* or *SQL Server ODBC*, if you are using a Microsoft SQL Server database.

Custom JDBC
Select *Custom JDBC* to use an ANSI SQL-92 compliant database with a JDBC driver, including Oracle Database, and PostgreSQL.

2.1.2 SQL Table Creation

Diplomat MFT can create the SQL audit database tables the first time the database is accessed or the tables in the SQL database may be created independently. If you choose to create the tables on your own, the DDL for creating the tables is shown in a later section of this guide. Also, a file named DiplomatAuditDB.ddl containing the DDL is provided as part of the Diplomat MFT Service installation. If Diplomat MFT Service is installed in the default directory, DiplomatAuditDB.ddl is located at C:\Program Files\Coviant Software\Diplomat-j\SQLaudit for Windows systems and /opt/coviant/diplomat-j/SQLaudit for Linux installations.

2.1.3 Database Access and Permissions

Diplomat MFT allows, but does not require, a username and password for access to the MySQL, MS SQLServer, and Other ODBC audit databases. If a username and password are used, the account associated with the username must, unless *Skip Table Creation* is selected, have permission to create tables and write records to existing tables.

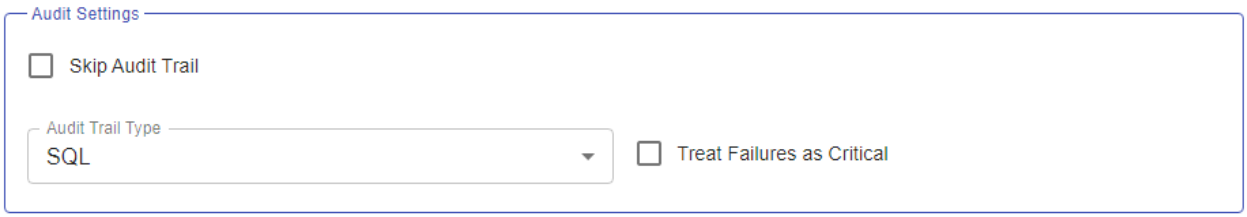
2.2 Settings

SQL audit and archival settings are entered on the Audit Trail Settings screen, which is accessed from the top menu bar of the Diplomat MFT Client by selecting Settings > Audit. An overview of the SQL audit and archival settings are provided below, as the Diplomat MFT user may need assistance from the SQL database administrator to properly enter these settings.

The Audit Trail Settings screen captures all information needed to set up and manage audit trail data, including the ability to automatically transfer SQL records to archive tables in the SQL audit database on a regular basis or immediately, if needed.

Audit trail data includes all data related to each file transfer job executed by Diplomat MFT that attempts to transfer files. Audit trail data is used to generate the Audit Detail Reports and the Audit Summary Reports available from the Reports menu item on the top menu bar. If a SQL database is used, user activity data is collected and a User Activity Report is also available.

2.2.1 Audit Settings



Audit settings determine whether or not Diplomat MFT captures audit data, what type of database is used, and what action to take if an error occurs during an attempt to write an audit record.

Skip Audit Trail
Check *Skip Audit Trail*, if you do not want audit records to be written. If you do not select *Skip Audit Trail*, an audit trail record is written for every job that is not automatically rescheduled due to File(s) Not Found (i.e., with a status of 'Success', 'Failure', or 'Warning', 'Error', or 'Critical Error').

NOTE: If *Fail if File Not Found* is checked on a transaction, then the job is a 'Failure' when the file is not found and an audit trail record is written. When *Fail if File Not Found* is NOT checked on a transaction, jobs that do not find files are simply rescheduled and no record is written to the audit trail.

Audit Trail Type
Diplomat MFT allows either a customizable SQL database or a built-in XML Diplomat MFT audit database. You can generate reports using the Reports menu item on the top menu bar for either type of audit database. If you want to create custom reports using a software product other than Diplomat, you must select 'SQL' and set up a SQL database to which Diplomat MFT can write audit records.

NOTE: If you select 'Built-in' as the *Audit Trail Type*, all fields on the remaining audit trail settings panels are disabled.

Treat Failures as Critical
Select *Treat Failure as Critical* to **SUSPEND ALL JOBS** when an audit trail problem occurs. Only select *Treat Failure as Critical* if an audit record is required for every file transfer job.

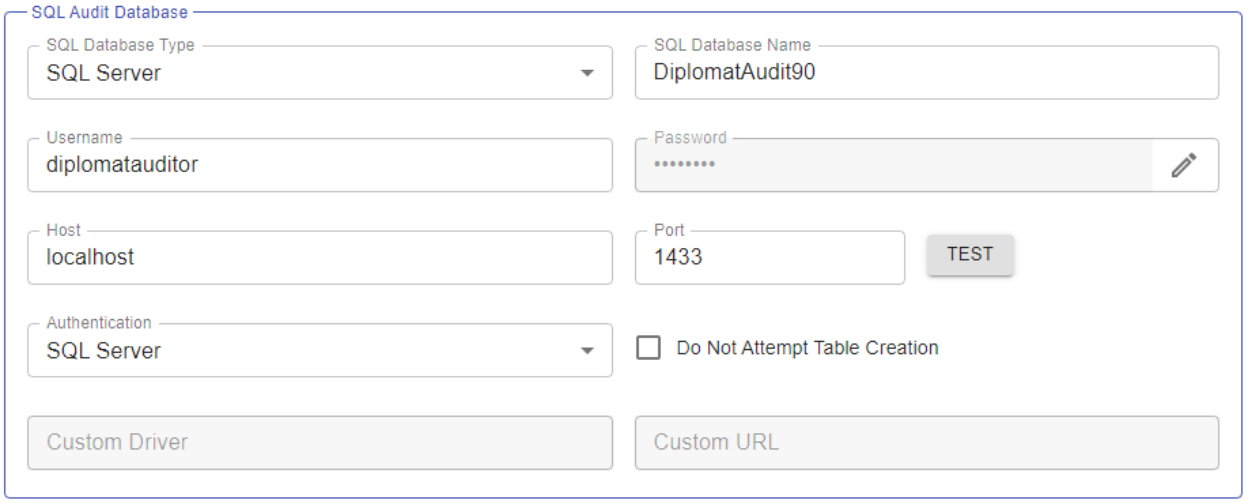
If *Treat Failure as Critical* is selected and an audit trail error occurs, job processing is suspended, which is indicated by pink status indicator '■' that is displayed next to the transactions folder in the navigation tree. In addition, an orange status indicator '■' is displayed next to all transaction objects in the tree. And, the audit trail error is treated as a critical error by email, paging, and logging.

Test jobs can be executed using '*Run Now*' to determine if an audit problem has been resolved. Once the problem has been resolved, release suspended transactions by selecting Jobs > Release > Release Critical Audit Suspend or right-click on the on the Transaction folder in the navigation tree and select **Release Critical Audit Suspend**.

If you have indicated that you want an audit trail, but it is not critical to your business (i.e., *Skip Audit Trail* is NOT checked and *Treat Failure as Critical* is NOT checked), and a job fails to write an audit record, then job processing continues. The audit trail error is treated as a critical error by email, paging, and logging.

NOTE: Email generated due to an audit trail failure is ONLY sent to IT Support. Business users do NOT receive any notification of an audit failure. If *Treat Failures as Critical* is selected, the failure email sent to IT Support includes the full contents of the records that would have been written to the audit database for the transaction in an XML format. If you have a stringent audit requirement, the data from this email can be entered manually into your SQL audit database or saved as an XML file.

2.2.2 SQL Audit DB



Contains all fields for setting up and using a SQL database for audit records. Each SQL audit database has three tables to capture job, file, and user activity data and three tables in which to archive job, file, and user activity data for improved performance, if desired.

NOTE: If you select 'Built-in' for *Audit Trail Type*, all fields on this panel are disabled.

NOTE: Changing SQL Audit DB settings while jobs are executing is potentially unsafe (e.g., audit records can be written without having their email and paging statuses set correctly). When prompted, you must select "Suspend" to suspend all jobs before updating the settings. If Diplomat MFT is unsuccessful in saving the new settings, all transactions will remain suspended. In addition, an orange status indicator '■' is displayed next to the transactions folder and all transaction objects in the navigation tree.

When setting up your SQL database, you must decide whether Diplomat MFT will be allowed to truncate data being written to character fields that are shorter than the string to be written. If Diplomat MFT does truncate data, a warning message and the complete string are written to the log file.

NOTE: This setting is NOT a Diplomat MFT setting but must be made in the SQL database set-up.

SQL DB Type
Type of SQL database. Select Custom JDBC to use an ANSI SQL-92 compliant database with a JDBC driver.

NOTE: Linux systems do not support SQL Server or other ODBC databases. Only MySQL is supported for Linux implementations.

SQL DB Name
Name of SQL database used to capture audit records.

If you choose MySQL as your *SQL DB Type*, enter the name of the schema as it appears under Catalogs in the MySQL Administrator. If you choose SQL Server as your SQL DB Type, enter the name of the database as it appears under Databases in SQL Server Administrator

Username
If required, enter the username needed to access the SQL audit database.

NOTE: *Username* and *Password* fields are disabled when Windows Authentication is selected. The login account specified in the Diplomat MFT Service is used for Windows authentication. For detailed instructions on how to update the Diplomat MFT Service, see https://knowledgebase.coviantsoftware.com/knowledge-base/setting-windows-login-for-diplomat-mft-service/.

Password
If required, enter the password needed to access the SQL audit database.

NOTE: *Username* and *Password* fields are disabled when Windows Authentication is selected. The login account specified in the Diplomat MFT Service is used for Windows authentication. For detailed instructions on how to update the Diplomat MFT Service, see https://knowledgebase.coviantsoftware.com/knowledge-base/setting-windows-login-for-diplomat-mft-service/.

Host
Host name or IP address of the system where the SQL database is located.

NOTE: A login account on the Diplomat MFT Service must be specified when accessing SQL Server on a remote system. For detailed instructions on how to update the Diplomat MFT Service, see https://knowledgebase.coviantsoftware.com/knowledge-base/setting-windows-login-for-diplomat-mft-service/.

Port
Specifies the port number used to access the SQL database. Default is 3306 for MySQL and 1433 for SQL Server.

NOTE: *Port* is not required for ODBC data sources.

Test Button
After entering the host and port information, press Test to test the connection to the SQL database.

NOTE: The test button only tests that the specified port is open on the host systems. It does NOT test the username and password for login to the database.

Authentication
When accessing a SQL Server database directly, select SQL Server or Windows authentication. If Windows authentication is selected, no *Username* or *Password* is required. Windows authentication uses the logon identity of the Diplomat MFT Service.

Do Not Attempt Table Creation
Each SQL audit database has three tables to capture job, file, and user activity data and three tables in which to archive job, file, and user activity data plus a table that stores the DB version. Select *Do Not Attempt Table Creation*, if you have already set up the seven tables required by Diplomat MFT in the SQL audit database. If you do NOT check *Do Not Attempt Table Creation* and if the tables do not already exist, Diplomat MFT attempts to create the seven required tables when the Audit Trail Settings are saved.

NOTE: If you do NOT check *Do Not Attempt Table Creation*, the account associated with the username and password specified above MUST have permission to create tables in the SQL database. If the account does not have the proper privileges, Diplomat MFT will NOT be able to create tables.

Custom Driver
Obtain a JDBC jar file from your SQL database vendor. Copy this jar file to C:\Program Files\Coviant Software\Diplomat-j\tomcatWebserver\webapps\diplomat\WEB-INF\lib\, opt/coviant/diplomat-j/Coviant Software/Diplomat-j/tomcatWebserver/webapps/diplomat/WEB-INF/lib or the corresponding directory for your installation.

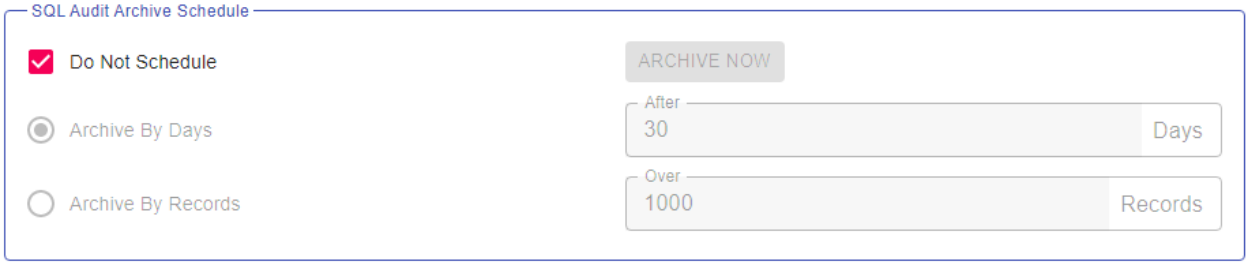
Enter the JDBC driver class name in the JDBC jar (e.g., com.microsoft.sqlserver.jdbc.SQLServerDriver) in the *Custom Driver* field. Refer to the documentation from your SQL database vendor for more information.

Custom URL
Connection URL associated with the specified *Custom Driver.* The **optional** parameters <HOST>, <PORT>, and <DBNAME> can be used in place of the host name, port number and SQL database name. At run-time, these parameters are replaced with the values in the *Host*, *Port*, and *SQL DB Name* fields.

At run-time, database authentication uses data from the *Username* and *Password* fields.

NOTE: Microsoft SQLServer also allows Windows authentication, which uses the logon identity associated with the Diplomat MFT Service. **If you are using a Microsoft SQLServer database, selection of *SQL Server* in the *SQL DB Type* field is recommended.**

2.2.3 SQL Audit Archive Schedule



Allows you to set-up automatic archival of audit records or to archive records immediately. Records are archived into the job, file, and user activity archive tables in the SQL audit database. Archiving of records is only available for SQL audit databases.

NOTE: Archiving records is only available for SQL audit databases. If you selected 'Built-in' for *Audit Trail Type*, all fields on this panel are disabled.

NOTE: Archiving SQL records may improve run-time job performance. However, performance may be adversely affected when generating reports that include archived records.

NOTE: When records are transferred to the archive tables in the SQL audit database, they are deleted from the active tables in the SQL audit database.

Do Not Schedule

Check *Do Not Schedule*, if do not want older audit records to be archived into separate SQL tables. If this field is not checked, then records are selected once a day based on the settings for *Archive by Date* or *Archive by Records* and written to the archive tables in the SQL audit database. Status of these daily jobs is shown in the *Archive Status* panel below.

Archive Now Button

Archiving normally occurs when the Diplomat MFT Service is started and once a day thereafter. Press **Archive Now** to immediately execute a job to transfer SQL records to the archive tables in the SQL audit database, using the current settings on the *Audit Archive Schedule* panel. A pop-up dialog box displays the status of the archive process.

Archive by Days or Archive by Records

Audit records can be archived based on the number of days or records. If *Archive by Days* is selected, records older than the specified number of days are moved to the archive tables in the SQL audit database. If *Archive by Records* is selected, records in excess of the number of records specified are moved to the archive tables in the SQL audit database.

NOTE: All records for a day are moved as a block to the archive tables in the SQL audit database, even when *Archive by Records* is selected. Thus, the active and the archive audit databases never contain a partial day of records. And, since all records for a day are archived as a block, records for the current day are never archived using automatic archival or Archive Now.

3 Field Formats

All fields are stored in the database as string (VARCHAR) fields of various lengths (see the DDL Section). Diplomat MFT enters null values in all fields allowing null values when the field is not applicable.

The 'Format' column in the foregoing tables describes how each field should be interpreted. Those interpreted as 'Text' do not require any special interpretation. Other fields should be interpreted as follows:

Format	**Interpretation**
Boolean	True or false corresponding to the database text, which is 'true' or 'false'
DateTime	Database text is formatted as 'yyyyMMddhhmmssSSS' where: yyyy = the year; e.g. '2004' MM = the month as a decimal number in the range 1 (Jan) to 12 (Dec) dd = the day of the month, in the range 1 to 31 hh = hour, in the range 0 to 23 mm = minute, in the range 0 to 59 ss = second, in the range 0 to 59 SSS = millisecond, in the range 0 to 999
Hex	Database text is formatted as a 16-digit hexadecimal number
Integer	Database text is formatted as a signed decimal integer in the range -2^{31} to $2^{31}-1$
Long	Database text is formatted as a signed decimal integer in the range -2^{63} to $2^{63}-1$

4 DDL

The DDL for creating the required database tables is given below:

```
USE [DiplomatAudit]
GO
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
/****** Object:  Table [dbo].[DB_VERSION] ******/
CREATE TABLE [dbo].[DB_VERSION](
	[DBID] [int] NULL,
	[VERSION] [varchar](32) NULL
) ON [PRIMARY]
GO

INSERT INTO DB_VERSION (DBID, VERSION) VALUES (1, '9.2');
GO

/****** Object:  Table [dbo].[FILE_DEST_AUDIT] ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[FILE_DEST_AUDIT](
	[RECORD_ID] [varchar](255) NOT NULL,
	[JOB_AUDIT_ID] [varchar](128) NOT NULL,
	[JOB_DEST_AUDIT_ID] [varchar](128) NOT NULL,
	[FILE_SOURCE_RECORD_ID] [varchar](255) NOT NULL,
	[DEST_FILENAME] [varchar](255) NULL,
	[DEST_WRITE_ATTEMPTED] [tinyint] NOT NULL,
	[DEST_WRITTEN] [tinyint] NULL,
	[DEST_OVERWRITE] [tinyint] NULL,
	[DEST_FILE_SIZE] [bigint] NULL,
	[DEST_FILE_STATUS] [varchar](32) NOT NULL,
	[DEST_FILE_STATUS_REASON] [varchar](255) NOT NULL,
	[AS2_MDN] [varchar](8000) NULL,
PRIMARY KEY CLUSTERED
(
	[RECORD_ID] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF) ON [PRIMARY]
) ON [PRIMARY]
GO
/****** Object:  Table [dbo].[FILE_DEST_AUDIT_ARCHIVE] ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[FILE_DEST_AUDIT_ARCHIVE](
	[RECORD_ID] [varchar](255) NOT NULL,
	[JOB_DEST_AUDIT_ID] [varchar](128) NOT NULL,
	[FILE_SOURCE_RECORD_ID] [varchar](255) NOT NULL,
	[DEST_FILENAME] [varchar](255) NOT NULL,
	[DEST_WRITE_ATTEMPTED] [tinyint] NOT NULL,
	[DEST_WRITTEN] [tinyint] NULL,
	[DEST_OVERWRITE] [tinyint] NULL,
	[DEST_FILE_SIZE] [bigint] NULL,
	[DEST_FILE_STATUS] [varchar](32) NOT NULL,
	[DEST_FILE_STATUS_REASON] [varchar](255) NOT NULL,
	[AS2_MDN] [varchar](8000) NULL,
PRIMARY KEY CLUSTERED
(
	[RECORD_ID] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF) ON [PRIMARY]
) ON [PRIMARY]
GO
```

```
/****** Object:  Table [dbo].[FILE_SRC_AUDIT] ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[FILE_SRC_AUDIT](
	[RECORD_ID] [varchar](255) NOT NULL,
	[JOB_AUDIT_ID] [varchar](128) NOT NULL,
	[SOURCE_FILENAME] [varchar](255) NOT NULL,
	[SOURCE_XFERRED] [tinyint] NOT NULL,
	[SOURCE_FILE_SIZE] [bigint] NOT NULL,
	[SOURCE_ASCII_ARMORED] [tinyint] NULL,
	[SOURCE_SIGNED] [tinyint] NULL,
	[SOURCE_ENCRYPTED] [tinyint] NULL,
	[SOURCE_DELETED] [tinyint] NOT NULL,
	[SOURCE_MOVED] [tinyint] NOT NULL,
	[SOURCE_ATTEMPT_UNARMOR] [tinyint] NULL,
	[SOURCE_UNARMORED] [tinyint] NULL,
	[SOURCE_ATTEMPT_DECRYPT] [tinyint] NULL,
	[SOURCE_DECRYPTED] [tinyint] NULL,
	[SOURCE_ATTEMPT_VERIFY] [tinyint] NULL,
	[SOURCE_VERIFIED] [tinyint] NULL,
	[DECRYPT_KEYID] [varchar](16) NULL,
	[VERIFY_KEYID] [varchar](16) NULL,
	[SOURCE_SENDER_ADDRESS] [varchar](64) NULL,
	[SOURCE_SENDER_SUBJECT] [varchar](64) NULL,
	[DEST_COMPRESSED] [tinyint] NULL,
	[DEST_ATTEMPT_ARMOR] [tinyint] NULL,
	[DEST_ASCII_ARMORED] [tinyint] NULL,
	[DEST_ATTEMPT_SIGN] [tinyint] NULL,
	[DEST_SIGNED] [tinyint] NULL,
	[DEST_ATTEMPT_ENCRYPT] [tinyint] NULL,
	[DEST_ENCRYPTED] [tinyint] NULL,
	[SIGNATURE_TIME] [varchar](17) NULL,
	[ENCRYPT_KEYID] [varchar](16) NULL,
	[AEK_ENCRYPT_KEYID] [varchar](255) NULL,
	[SIGNATURE_KEYID] [varchar](16) NULL,
	[FILE_STATUS] [varchar](32) NOT NULL,
	[FILE_STATUS_REASON] [varchar](255) NOT NULL,
	[SOURCE_ARCHIVE_FILENAME] [varchar](255) NULL,
	[PRIMARY_SRC_ARCHIVE_FILENAME] [varchar](255) NULL,
	[DEST_ARCHIVE_FILENAME] [varchar](255) NULL,
	[PRIMARY_DEST_ARCHIVE_FILENAME] [varchar](255) NULL,
PRIMARY KEY CLUSTERED
(
	[RECORD_ID] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF) ON [PRIMARY]
) ON [PRIMARY]
GO
/****** Object:  Table [dbo].[FILE_SRC_AUDIT_ARCHIVE] ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[FILE_SRC_AUDIT_ARCHIVE](
	[RECORD_ID] [varchar](255) NOT NULL,
	[JOB_AUDIT_ID] [varchar](128) NOT NULL,
	[SOURCE_FILENAME] [varchar](255) NOT NULL,
	[SOURCE_XFERRED] [tinyint] NOT NULL,
	[SOURCE_FILE_SIZE] [bigint] NOT NULL,
	[SOURCE_ASCII_ARMORED] [tinyint] NULL,
	[SOURCE_SIGNED] [tinyint] NULL,
	[SOURCE_ENCRYPTED] [tinyint] NULL,
	[SOURCE_DELETED] [tinyint] NOT NULL,
	[SOURCE_MOVED] [tinyint] NOT NULL,
	[SOURCE_ATTEMPT_UNARMOR] [tinyint] NULL,
	[SOURCE_UNARMORED] [tinyint] NULL,
	[SOURCE_ATTEMPT_DECRYPT] [tinyint] NULL,
	[SOURCE_DECRYPTED] [tinyint] NULL,
	[SOURCE_ATTEMPT_VERIFY] [tinyint] NULL,
```

```
	[SOURCE_VERIFIED] [tinyint] NULL,
	[DECRYPT_KEYID] [varchar](16) NULL,
	[VERIFY_KEYID] [varchar](16) NULL,
	[SOURCE_SENDER_ADDRESS] [varchar](64) NULL,
	[SOURCE_SENDER_SUBJECT] [varchar](64) NULL,
	[DEST_COMPRESSED] [tinyint] NULL,
	[DEST_ATTEMPT_ARMOR] [tinyint] NULL,
	[DEST_ASCII_ARMORED] [tinyint] NULL,
	[DEST_ATTEMPT_SIGN] [tinyint] NULL,
	[DEST_SIGNED] [tinyint] NULL,
	[DEST_ATTEMPT_ENCRYPT] [tinyint] NULL,
	[DEST_ENCRYPTED] [tinyint] NULL,
	[SIGNATURE_TIME] [varchar](17) NULL,
	[ENCRYPT_KEYID] [varchar](16) NULL,
	[AEK_ENCRYPT_KEYID] [varchar](255) NULL,
	[SIGNATURE_KEYID] [varchar](16) NULL,
	[FILE_STATUS] [varchar](32) NOT NULL,
	[FILE_STATUS_REASON] [varchar](255) NOT NULL,
	[SOURCE_ARCHIVE_FILENAME] [varchar](255) NULL,
	[PRIMARY_SRC_ARCHIVE_FILENAME] [varchar](255) NULL,
	[DEST_ARCHIVE_FILENAME] [varchar](255) NULL,
	[PRIMARY_DEST_ARCHIVE_FILENAME] [varchar](255) NULL,
PRIMARY KEY CLUSTERED
(
	[RECORD_ID] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF) ON [PRIMARY]
) ON [PRIMARY]
GO
/****** Object:  Table [dbo].[JOB_DEST_AUDIT] ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[JOB_DEST_AUDIT](
	[JOB_AUDIT_ID] [varchar](128) NOT NULL,
	[JOB_DEST_AUDIT_ID] [varchar](128) NOT NULL,
	[DEST_PARTNER_NAME] [varchar](128) NOT NULL,
	[DEST_PARTNER_TYPE] [varchar](32) NULL,
	[DEST_PARTNER_SAVED] [tinyint] NOT NULL,
	[DEST_TRANSPORT_METHOD] [varchar](32) NOT NULL,
	[DEST_SERVER_ADDRESS] [varchar](64) NULL,
	[DEST_SERVER_PORT] [varchar](16) NULL,
	[DEST_SERVER_ACCOUNT] [varchar](64) NULL,
	[DEST_SERVER_DIRECTORY] [varchar](255) NULL,
	[DEST_SERVER_TYPE] [varchar](32) NULL,
	[DEST_SERVER_PASSIVE] [tinyint] NULL,
	[DEST_FILE_LOCATION] [varchar](255) NULL,
	[DEST_RECIPIENT_ADDRESS] [varchar](255) NULL,
	[DEST_RECIPIENT_SUBJECT] [varchar](64) NULL,
	[DEST_FTP_MODE] [varchar](32) NULL,
	[AS2_RECEIVER_ID] [varchar](255) NULL,
	[AS2_SENDER_ID] [varchar](255) NULL,
PRIMARY KEY CLUSTERED
(
	[JOB_DEST_AUDIT_ID] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF) ON [PRIMARY]
) ON [PRIMARY]
GO
/****** Object:  Table [dbo].[JOB_DEST_AUDIT_ARCHIVE] ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[JOB_DEST_AUDIT_ARCHIVE](
	[JOB_AUDIT_ID] [varchar](128) NOT NULL,
	[JOB_DEST_AUDIT_ID] [varchar](128) NOT NULL,
	[DEST_PARTNER_NAME] [varchar](128) NOT NULL,
	[DEST_PARTNER_TYPE] [varchar](32) NULL,
	[DEST_PARTNER_SAVED] [tinyint] NOT NULL,
```

```
        [DEST_TRANSPORT_METHOD] [varchar](32) NOT NULL,
        [DEST_SERVER_ADDRESS] [varchar](64) NULL,
        [DEST_SERVER_PORT] [varchar](16) NULL,
        [DEST_SERVER_ACCOUNT] [varchar](64) NULL,
        [DEST_SERVER_DIRECTORY] [varchar](255) NULL,
        [DEST_SERVER_TYPE] [varchar](32) NULL,
        [DEST_SERVER_PASSIVE] [tinyint] NULL,
        [DEST_FILE_LOCATION] [varchar](255) NULL,
        [DEST_RECIPIENT_ADDRESS] [varchar](255) NULL,
        [DEST_RECIPIENT_SUBJECT] [varchar](64) NULL,
        [DEST_FTP_MODE] [varchar](32) NULL,
        [AS2_RECEIVER_ID] [varchar](255) NULL,
        [AS2_SENDER_ID] [varchar](255) NULL,
PRIMARY KEY CLUSTERED
(
        [JOB_DEST_AUDIT_ID] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF) ON [PRIMARY]
) ON [PRIMARY]
GO
/****** Object:  Table [dbo].[JOB_SRC_AUDIT] ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[JOB_SRC_AUDIT](
        [JOB_AUDIT_ID] [varchar](128) NOT NULL,
        [VERSION] [varchar](32) NOT NULL,
        [BUILD_NUMBER] [varchar](8) NOT NULL,
        [OS_VERSION] [varchar](64) NOT NULL,
        [DESCRIPTION] [varchar](255) NULL,
        [TRANSACTION_ID] [varchar](128) NOT NULL,
        [TRANSACTION_TYPE] [varchar](32) NOT NULL,
        [STATUS] [varchar](32) NOT NULL,
        [STATUS_REASON] [varchar](255) NOT NULL,
        [OVERWRITE] [varchar](5) NOT NULL,
        [DELETE_SOURCE] [tinyint] NOT NULL,
        [MOVE_SOURCE] [tinyint] NOT NULL,
        [MOVE_SOURCE_SUCCESSDEST] [varchar](255) NULL,
        [MOVE_SOURCE_ERRORDEST] [varchar](255) NULL,
        [TRANSFER_ORDER] [varchar](20) NULL,
        [LOG_LOCATION] [varchar](255) NOT NULL,
        [LOG_FILENAME] [varchar](64) NOT NULL,
        [ARCHIVE] [tinyint] NOT NULL,
        [ARCHIVE_FILE_TYPE] [varchar](32) NULL,
        [ARCHIVE_LOCATION] [varchar](255) NULL,
        [ARCHIVE_ZIP] [tinyint] NULL,
        [ARCHIVE_ZIP_FILENAME] [varchar](255) NULL,
        [PRIMARY_ARCHIVE] [tinyint] NOT NULL,
        [PRIMARY_ARCHIVE_FILE_TYPE] [varchar](32) NULL,
        [PRIMARY_ARCHIVE_LOCATION] [varchar](255) NULL,
        [PRIMARY_ARCHIVE_ZIP] [tinyint] NULL,
        [PRIMARY_ARCHIVE_ZIP_FILENAME] [varchar](255) NULL,
        [START_TIME] [varchar](17) NOT NULL,
        [END_TIME] [varchar](17) NOT NULL,
        [SOURCE_PARTNER_ID] [varchar](128) NOT NULL,
        [SOURCE_PARTNER_TYPE] [varchar](32) NULL,
        [SOURCE_PARTNER_SAVED] [tinyint] NOT NULL,
        [SOURCE_TRANSPORT_METHOD] [varchar](32) NOT NULL,
        [SOURCE_SERVER_ADDRESS] [varchar](64) NULL,
        [SOURCE_SERVER_PORT] [varchar](16) NULL,
        [SOURCE_SERVER_ACCOUNT] [varchar](64) NULL,
        [SOURCE_SERVER_DIRECTORY] [varchar](255) NULL,
        [SOURCE_SERVER_TYPE] [varchar](32) NULL,
        [SOURCE_SERVER_PASSIVE] [tinyint] NULL,
        [SOURCE_FILE_LOCATION] [varchar](255) NULL,
        [ENCRYPT_DECRYPT] [tinyint] NOT NULL,
        [SIGN_AUTHENTICATE] [tinyint] NOT NULL,
        [ASCII_ARMORING] [tinyint] NOT NULL,
        [CANONICAL_TEXT] [tinyint] NULL,
        [COMPRESSION] [tinyint] NULL,
```

```
        [SOURCE_FTP_MODE] [varchar](32) NULL,
        [RUN_NOW] [tinyint] NOT NULL,
        [API] [tinyint] NOT NULL,
        [FILE_MONITOR] [tinyint] NOT NULL,
        [THIRD_PARTY] [tinyint] NOT NULL,
        [LINKED] [tinyint] NOT NULL,
        [SCRIPT_ARGUMENT1] [varchar](64) NULL,
        [SCRIPT_ARGUMENT2] [varchar](64) NULL,
        [SCRIPT_ARGUMENT3] [varchar](64) NULL,
        [SCRIPT_ARGUMENT4] [varchar](64) NULL,
        [SCRIPT_ARGUMENT5] [varchar](64) NULL,
        [POLLING_FREQUENCY] [varchar](32) NULL,
        [POLLING_INTERVAL] [varchar](16) NULL,
        [NUMBER_RETRIES] [tinyint] NULL,
        [TOTAL_ATTEMPTS] [tinyint] NULL,
        [BUSINESS_EMAIL] [tinyint] NOT NULL,
        [BUSINESS_EMAIL_ADDRESSES] [varchar](255) NULL,
        [IT_EMAIL] [tinyint] NOT NULL,
        [IT_EMAIL_ADDRESSES] [varchar](255) NULL,
        [PAGING_TYPE] [varchar](32) NOT NULL,
        [PAGING_LEVEL] [varchar](32) NULL,
        [PAGING_PIN] [varchar](32) NULL,
        [PAGING_ATTEMPTED] [tinyint] NULL,
        [PAGING_SUCCESSFUL] [tinyint] NULL,
        [PAGING_EMAIL_ADDRESS] [varchar](128) NULL,
        [PRIMARY_PAGING_LOCATION] [varchar](255) NULL,
        [SECONDARY_PAGING_LOCATION] [varchar](255) NULL,
        [PAGING_FILENAME] [varchar](64) NULL,
        [PRE_COMMAND] [varchar](255) NULL,
        [PRE_COMMAND_ATTEMPTED] [tinyint] NULL,
        [PRE_COMMAND_RTRN_CODE] [varchar](16) NULL,
        [PRE_COMMAND_FAILURE_OVERRIDE] [tinyint] NULL,
        [POST_COMMAND] [varchar](255) NULL,
        [POST_COMMAND_ATTEMPTED] [tinyint] NULL,
        [POST_COMMAND_RTRN_CODE] [varchar](16) NULL,
        [POST_COMMAND_FAILURE_OVERRIDE] [tinyint] NULL,
        [PRE_ZIP] [varchar](255) NULL,
        [POST_ZIP] [varchar](255) NULL,
        [LINK_STATUS] [varchar](128) NULL,
        [MACHINE] [varchar](64) NULL,
PRIMARY KEY CLUSTERED
(
        [JOB_AUDIT_ID] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF) ON [PRIMARY]
) ON [PRIMARY]
GO
/****** Object:  Table [dbo].[JOB_SRC_AUDIT_ARCHIVE] ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[JOB_SRC_AUDIT_ARCHIVE](
        [JOB_AUDIT_ID] [varchar](128) NOT NULL,
        [VERSION] [varchar](32) NOT NULL,
        [BUILD_NUMBER] [varchar](8) NOT NULL,
        [OS_VERSION] [varchar](64) NOT NULL,
        [DESCRIPTION] [varchar](255) NULL,
        [TRANSACTION_ID] [varchar](128) NOT NULL,
        [TRANSACTION_TYPE] [varchar](32) NOT NULL,
        [STATUS] [varchar](32) NOT NULL,
        [STATUS_REASON] [varchar](255) NOT NULL,
        [OVERWRITE] [varchar](5) NOT NULL,
        [DELETE_SOURCE] [tinyint] NOT NULL,
        [MOVE_SOURCE] [tinyint] NOT NULL,
        [MOVE_SOURCE_SUCCESSDEST] [varchar](255) NULL,
        [MOVE_SOURCE_ERRORDEST] [varchar](255) NULL,
        [TRANSFER_ORDER] [varchar](20) NULL,
        [LOG_LOCATION] [varchar](255) NOT NULL,
        [LOG_FILENAME] [varchar](64) NOT NULL,
        [ARCHIVE] [tinyint] NOT NULL,
```

```
        [ARCHIVE_FILE_TYPE] [varchar](32) NULL,
        [ARCHIVE_LOCATION] [varchar](255) NULL,
        [ARCHIVE_ZIP] [tinyint] NULL,
        [ARCHIVE_ZIP_FILENAME] [varchar](255) NULL,
        [PRIMARY_ARCHIVE] [tinyint] NOT NULL,
        [PRIMARY_ARCHIVE_FILE_TYPE] [varchar](32) NULL,
        [PRIMARY_ARCHIVE_LOCATION] [varchar](255) NULL,
        [PRIMARY_ARCHIVE_ZIP] [tinyint] NULL,
        [PRIMARY_ARCHIVE_ZIP_FILENAME] [varchar](255) NULL,
        [START_TIME] [varchar](17) NOT NULL,
        [END_TIME] [varchar](17) NOT NULL,
        [SOURCE_PARTNER_ID] [varchar](128) NOT NULL,
        [SOURCE_PARTNER_TYPE] [varchar](32) NULL,
        [SOURCE_PARTNER_SAVED] [tinyint] NOT NULL,
        [SOURCE_TRANSPORT_METHOD] [varchar](32) NOT NULL,
        [SOURCE_SERVER_ADDRESS] [varchar](64) NULL,
        [SOURCE_SERVER_PORT] [varchar](16) NULL,
        [SOURCE_SERVER_ACCOUNT] [varchar](64) NULL,
        [SOURCE_SERVER_DIRECTORY] [varchar](255) NULL,
        [SOURCE_SERVER_TYPE] [varchar](32) NULL,
        [SOURCE_SERVER_PASSIVE] [tinyint] NULL,
        [SOURCE_FILE_LOCATION] [varchar](255) NULL,
        [ENCRYPT_DECRYPT] [tinyint] NOT NULL,
        [SIGN_AUTHENTICATE] [tinyint] NOT NULL,
        [ASCII_ARMORING] [tinyint] NOT NULL,
        [CANONICAL_TEXT] [tinyint] NULL,
        [COMPRESSION] [tinyint] NULL,
        [SOURCE_FTP_MODE] [varchar](32) NULL,
        [RUN_NOW] [tinyint] NOT NULL,
        [API] [tinyint] NOT NULL,
        [FILE_MONITOR] [tinyint] NOT NULL,
        [THIRD_PARTY] [tinyint] NOT NULL,
        [LINKED] [tinyint] NOT NULL,
        [SCRIPT_ARGUMENT1] [varchar](64) NULL,
        [SCRIPT_ARGUMENT2] [varchar](64) NULL,
        [SCRIPT_ARGUMENT3] [varchar](64) NULL,
        [SCRIPT_ARGUMENT4] [varchar](64) NULL,
        [SCRIPT_ARGUMENT5] [varchar](64) NULL,
        [POLLING_FREQUENCY] [varchar](32) NULL,
        [POLLING_INTERVAL] [varchar](16) NULL,
        [NUMBER_RETRIES] [tinyint] NULL,
        [TOTAL_ATTEMPTS] [tinyint] NULL,
        [BUSINESS_EMAIL] [tinyint] NOT NULL,
        [BUSINESS_EMAIL_ADDRESSES] [varchar](255) NULL,
        [IT_EMAIL] [tinyint] NOT NULL,
        [IT_EMAIL_ADDRESSES] [varchar](255) NULL,
        [PAGING_TYPE] [varchar](32) NOT NULL,
        [PAGING_LEVEL] [varchar](32) NULL,
        [PAGING_PIN] [varchar](32) NULL,
        [PAGING_ATTEMPTED] [tinyint] NULL,
        [PAGING_SUCCESSFUL] [tinyint] NULL,
        [PAGING_EMAIL_ADDRESS] [varchar](128) NULL,
        [PRIMARY_PAGING_LOCATION] [varchar](255) NULL,
        [SECONDARY_PAGING_LOCATION] [varchar](255) NULL,
        [PAGING_FILENAME] [varchar](64) NULL,
        [PRE_COMMAND] [varchar](255) NULL,
        [PRE_COMMAND_ATTEMPTED] [tinyint] NULL,
        [PRE_COMMAND_RTRN_CODE] [varchar](16) NULL,
        [PRE_COMMAND_FAILURE_OVERRIDE] [tinyint] NULL,
        [POST_COMMAND] [varchar](255) NULL,
        [POST_COMMAND_ATTEMPTED] [tinyint] NULL,
        [POST_COMMAND_RTRN_CODE] [varchar](16) NULL,
        [POST_COMMAND_FAILURE_OVERRIDE] [tinyint] NULL,
        [PRE_ZIP] [varchar](255) NULL,
        [POST_ZIP] [varchar](255) NULL,
        [LINK_STATUS] [varchar](128) NULL,
        [MACHINE] [varchar](64) NULL,
PRIMARY KEY CLUSTERED
(
        [JOB_AUDIT_ID] ASC
```

```
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF) ON [PRIMARY]
) ON [PRIMARY]
GO
/****** Object:  Table [dbo].[SFTP_FILE_OPERATION] ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[SFTP_FILE_OPERATION](
        [ID] [varchar](36) NULL,
        [SESSION_ID] [varchar](64) NULL,
        [TIMESTAMP] [varchar](17) NULL,
        [OPERATION] [varchar](16) NULL,
        [FILE_PATH] [varchar](128) NULL,
        [SRC_FILE_PATH] [varchar](128) NULL,
        [BYTES_TRANSFERRED] [varchar](32) NULL
) ON [PRIMARY]
GO
/****** Object:  Table [dbo].[SFTP_SERVER_CONNECTION] ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[SFTP_SERVER_CONNECTION](
        [ID] [varchar](64) NULL,
        [TIMESTAMP] [varchar](17) NULL,
        [CLIENTIP] [varchar](32) NULL,
        [USERNAME] [varchar](64) NULL,
        [AUTH_METHOD] [varchar](16) NULL,
        [OPERATION] [varchar](16) NULL
) ON [PRIMARY]
GO
/****** Object:  Table [dbo].[USER_ACTIVITY] ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[USER_ACTIVITY](
        [SEQUENCE_NUMBER] [varchar](9) NOT NULL,
        [TIMESTAMP] [varchar](17) NOT NULL,
        [USER_ID] [varchar](64) NOT NULL,
        [USER_IP_ADDRESS] [varchar](64) NOT NULL,
        [OBJECT_TYPE] [varchar](32) NOT NULL,
        [OBJECT_ID] [varchar](128) NULL,
        [ACTION] [varchar](32) NOT NULL,
        [COMMENT] [varchar](8000) NULL,
PRIMARY KEY CLUSTERED
(
        [SEQUENCE_NUMBER] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF) ON [PRIMARY]
) ON [PRIMARY]
GO
/****** Object:  Table [dbo].[USER_ACTIVITY_ARCHIVE] ******/
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[USER_ACTIVITY_ARCHIVE](
        [SEQUENCE_NUMBER] [varchar](9) NOT NULL,
        [TIMESTAMP] [varchar](17) NOT NULL,
        [USER_ID] [varchar](64) NOT NULL,
        [USER_IP_ADDRESS] [varchar](64) NOT NULL,
        [OBJECT_TYPE] [varchar](32) NOT NULL,
        [OBJECT_ID] [varchar](128) NULL,
        [ACTION] [varchar](32) NOT NULL,
        [COMMENT] [varchar](8000) NULL,
PRIMARY KEY CLUSTERED
(
        [SEQUENCE_NUMBER] ASC
```

```
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON, OPTIMIZE_FOR_SEQUENTIAL_KEY = OFF) ON [PRIMARY]
) ON [PRIMARY]
GO
ALTER TABLE [dbo].[FILE_DEST_AUDIT]  WITH CHECK ADD  CONSTRAINT [FILE_DEST_TO_JOB_DEST_FK]
FOREIGN KEY([JOB_DEST_AUDIT_ID])
REFERENCES [dbo].[JOB_DEST_AUDIT] ([JOB_DEST_AUDIT_ID])
ON DELETE CASCADE
GO
ALTER TABLE [dbo].[FILE_DEST_AUDIT] CHECK CONSTRAINT [FILE_DEST_TO_JOB_DEST_FK]
GO
ALTER TABLE [dbo].[FILE_DEST_AUDIT_ARCHIVE]  WITH CHECK ADD  CONSTRAINT
[FILE_DEST_TO_JOB_DEST_ARCHIVE_FK] FOREIGN KEY([JOB_DEST_AUDIT_ID])
REFERENCES [dbo].[JOB_DEST_AUDIT_ARCHIVE] ([JOB_DEST_AUDIT_ID])
ON DELETE CASCADE
GO
ALTER TABLE [dbo].[FILE_DEST_AUDIT_ARCHIVE] CHECK CONSTRAINT [FILE_DEST_TO_JOB_DEST_ARCHIVE_FK]
GO
ALTER TABLE [dbo].[FILE_SRC_AUDIT]  WITH CHECK ADD  CONSTRAINT [FILE_SRC_TO_JOB_SRC_FK] FOREIGN
KEY([JOB_AUDIT_ID])
REFERENCES [dbo].[JOB_SRC_AUDIT] ([JOB_AUDIT_ID])
ON DELETE CASCADE
GO
ALTER TABLE [dbo].[FILE_SRC_AUDIT] CHECK CONSTRAINT [FILE_SRC_TO_JOB_SRC_FK]
GO
ALTER TABLE [dbo].[FILE_SRC_AUDIT_ARCHIVE]  WITH CHECK ADD  CONSTRAINT
[FILE_SRC_TO_JOB_SRC_ARCHIVE_FK] FOREIGN KEY([JOB_AUDIT_ID])
REFERENCES [dbo].[JOB_SRC_AUDIT_ARCHIVE] ([JOB_AUDIT_ID])
ON DELETE CASCADE
GO
ALTER TABLE [dbo].[FILE_SRC_AUDIT_ARCHIVE] CHECK CONSTRAINT [FILE_SRC_TO_JOB_SRC_ARCHIVE_FK]
GO
ALTER TABLE [dbo].[JOB_DEST_AUDIT]  WITH CHECK ADD  CONSTRAINT [JOB_DEST_TO_JOB_SRC_FK] FOREIGN
KEY([JOB_AUDIT_ID])
REFERENCES [dbo].[JOB_SRC_AUDIT] ([JOB_AUDIT_ID])
ON DELETE CASCADE
GO
ALTER TABLE [dbo].[JOB_DEST_AUDIT] CHECK CONSTRAINT [JOB_DEST_TO_JOB_SRC_FK]
GO
ALTER TABLE [dbo].[JOB_DEST_AUDIT_ARCHIVE]  WITH CHECK ADD  CONSTRAINT
[JOB_DEST_TO_JOB_SRC_ARCHIVE_FK] FOREIGN KEY([JOB_AUDIT_ID])
REFERENCES [dbo].[JOB_SRC_AUDIT_ARCHIVE] ([JOB_AUDIT_ID])
ON DELETE CASCADE
GO
ALTER TABLE [dbo].[JOB_DEST_AUDIT_ARCHIVE] CHECK CONSTRAINT [JOB_DEST_TO_JOB_SRC_ARCHIVE_FK]
GO
```

5 Support

Installation and configuration support is provided under warranty for 30 days from initial purchase, as well as under annual maintenance agreements. Email and phone support is available from 9 a.m. ET to 5 p.m. CT weekdays. If you require assistance, contact Coviant Software Support as follows:

Voice: 210.985.0985 x2
Web: www.coviantsoftware.com
E-mail: support@coviantsoftware.com

Web: www.coviantsoftware.com
E-mail: support@coviantsoftware.com

Diplomat Managed File Transfer products interoperate with other software applications, such as FTP, STMP, SMS, and OpenPGP software. File transfer and encryption failures can occur during a job created by Diplomat Managed File Transfer for many reasons, including:

- Inaccurate transaction or setting data
- Connection problems with FTP, email, or local systems
- Wrong encryption or signature keys on incoming files
- Missing files or keys
- Mismatch between file format and FTP transfer settings
- Compatibility issues with older OpenPGP versions
- Incorrect or incompatible FTP server settings

Typically, these problems are NOT due to a malfunction of your Diplomat MFT product. Data to diagnose these problems and others are provided in the log files, debug email messages, and audit trail data generated when the job or jobs were run. These types of conditions are usually the user's responsibility. Please review the diagnostic information provided before contacting Coviant Software for support.

If you require support assistance that appears to be due to a malfunction of your Diplomat MFT software, please have the following items available before contacting a support representative.

- Diplomat MFT Edition name, version installed, and serial number located in Help > About Diplomat
- Current log file containing entries for the failed job(s)
- IT Support emails containing debug information for the failed job(s), if available
- Audit detail report for the failed job(s), if available

You may be asked to send some of the above information to the Coviant Software Support representative in order to resolve your problem in a timely manner.

6 Appendix A: Glossary

Additional Archive Directory – Directory on the network where backup files for a specific file transfer job are written.

Additional Encryption Key (AEK) – Public key used when the user wants to encrypt files to more than one key.

Active Window – Right-hand side of the main screen for Diplomat MFT Client that displays the active key, partner, or transaction that is being viewed or edited. Some data is displayed in panels that can be maximized for editing and then minimized to save screen space.

Business Users – Persons responsible for specific file transfers with trading partners or internal groups.

Debug – A setting that when activated inserts system messages into an email notification message. It is used primarily to troubleshoot problems in jobs.

Destination Directory – The directory on an FTP server or local network where a transaction file is to be written.

Diplomat MFT Administrator – Person administering the Diplomat MFT Service and Diplomat MFT Configuration Database.

Diplomat MFT Audit Database – Database containing detailed records of every job executed and user activity. The audit database is a set of XML files where each job has a single file or a SQL database with three tables to capture Job, File, and User Activity and three tables in which to archive Job, File, and User Activity records.

Diplomat MFT Client – Desktop application that enables creation and modification of key, partner, transaction information, and configuration settings, as well as license management, report generation, and job scheduling.

Diplomat MFT Configuration Database – Database containing all system-setting and transaction setting data. The configuration database is a single XML file.

Diplomat MFT Scripting Agent – Java application that submits for execution a specified transaction that has been created and saved in a Diplomat MFT transaction database that may require an optional password.

Diplomat MFT Service – Run-time engine that executes transactions stored in the Diplomat MFT transaction database and interfaces with FTP servers, mail servers, and other systems, as needed. The Diplomat MFT Service is a Windows service. After installation, the Windows operating system starts the Diplomat MFT Service, which then runs in the background creating jobs for each transaction. Plus, it creates a log file with system messages, an audit database, and archives transaction files, if desired.

Diplomat MFT Service Login – Windows login identity for the Diplomat MFT Service on the Diplomat MFT site. Defaults to Local Network.

Diplomat MFT Transaction Database – Contains all data needed to create and schedule jobs, including keys, partner profiles, and transaction data. The transaction database contains the Diplomat MFT keystore. The transaction database is comprised of a set of XML files that can be backed up and restored as a group.

Diplomat MFT Users – Persons setting up new keys, partners, and transactions that are allowed to automatically login to the Diplomat MFT Client, but do not have access to certain administrative functions.

Firewall – A software program that protects computers on a network from unauthorized Internet access.

FTP Server – A software program that allows the receipt and pick-up of files, which typically resides outside a corporate firewall.

Inbound Transaction – The process of receiving a file from another organization with optional decryption and verification.

IP Address – The numerical identification of a computer connected to a network. The IP Address appears with periods separating groups of numbers. (i.e. 192.168.0.1).

Job – A job is a particular execution of a transaction. For example, if a transaction is scheduled to run once a day, a new job will be created and executed once a day.

Job Monitor – A feature of Diplomat MFT that allows the real-time monitoring of job scheduling and execution.

License File –Diplomat MFT uses a license file named *diplomat.lic* to determine the number of keys you can have in your Diplomat MFT keystore and the expiration date of your license.

Log File – File containing chronological system messages generated as a result of Diplomat MFT operation.

Mail Server – A computer that acts as temporary recipient and storage for email messages sent to an individual.

Main Screen – Contains top menu bar, left-hand navigation tree, and active window for Diplomat MFT Client.

Menu Bar – Bar at the top of the main screen for Diplomat MFT Client that allows access to a variety of functions via sub-menus and pop-up dialog boxes.

Menu Item –Selection on the top menu bar of Diplomat MFT Client. When a menu item is selected either a sub-menu or a pop-up dialog box is displayed.

Navigation Tree – Left-hand side of the main screen for Diplomat MFT Client that displays folders, sub-folders, and objects with status indicators in a tree format for easy navigation

OpenPGP – Open PGP is one type of public key encryption technology. It is based on an asymmetric scheme that uses a pair of keys: a *public key*, which encrypts data, and a corresponding *private*, or *secret key* for decryption. The OpenPGP protocol, created by the Internet Engineering Task Force (IETF), defines standard formats for encrypted messages, signatures, private keys, and certificates for exchanging public keys.

OpenPGP Command Line Tool – OpenPGP products with a command line interface, such as PGP Command Line Server and McAfee e-Business Server.

Open PGP Key Pair – OpenPGP keys are always created as key pairs with a public key and a private key. The owner of a key pair keeps their key pair and gives their trading partner their public key.

OpenPGP Public Key – The OpenPGP key that is made available to an organization's trading partners to be used to encrypt data that is sent from the trading partner to the organization.

Outbound Transaction – The process of moving a file from within an organization to a receiving organization with optional encryption and signing of the file.

Paging Application – Software that converts email or files to a radio signal that is received by beepers.

Panel – Section of active window, usually surrounded by a blue border. Some larger panels can be maximized for editing and then minimized to save screen space.

Partner Profile – A set of information defining default parameters to be used when setting up a transaction with the trading partner.

Passphrase – Used by OpenPGP algorithms to encrypt your private key.

PGP – An acronym for Pretty Good Privacy, an encryption application developed by Phil Zimmerman that utilizes asymmetrical or public/key pairs to encrypt and decrypt files. Trademarked by PGP Corporation.

Pop-up Dialog Box – Window used to collect data for features accessed from the top menu bar in the Diplomat MFT Client.

Primary Archive Directory – Directory on the network where backup copies of files from all jobs are written.

Public Partners – Trading partners that provide you only their public keys for encryption and verification.

Signature Key– The OpenPGP key used to sign a file on encryption and authenticate/verify it on decryption.

Source Directory – The directory on an FTP server or local network where a transaction file is to be picked up.

SQL Audit Database – Contains two tables to capture Job and File records for each transaction and two tables in which to archive Job and File records, if desired.

Status Indicator – Colored icons that indicate scheduling status of transactions and suspend status of keys, partners, and transaction folders.

Trusted Partners – Trading partners that are considered part of your organization and can use key pairs for decryption or signing.

User Activity – Any action taken when using the Diplomat MFT Client, such as when a user creates, updates, or deletes records in the Diplomat MFT transaction database and associated configuration files.