COVIANT Software

USER GUIDE
DIPLOMAT MANAGED FILE TRANSFER
VERSION 9.2

V9.2

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 are available from 9 a.m. ET to 5 p.m. CT weekdays. If you require assistance, contact Coviant Software support as follows:

E-mail: support@coviantsoftware.com

Voice: +1-210-985-0985 x2

Web: www.coviantsoftware.com

Table of Contents

1 Welcome to Diplomat Managed File Transfer

When referring to this documentation, please remember that Diplomat MFT is available in several Editions and with available optional components. If you see a function here that you would find valuable, but it's not available to your license, please contact us at +1-210-985-0985 or via www.coviantsoftware.com to discuss your options.

1.1 Typical Customer Scenarios

Encryption and secure file transfer are technologies that can be used to safeguard files as they are transferred outside of a local area network. It can replace more expensive, traditional approaches to data security, such as leased lines or hardcopy tape shipments. These open technologies are especially popular in industries that face the twin challenges of privacy regulations and compression of financial margins – such as healthcare and financial services.

Encryption and secure file transfer can be chosen for internal security or forced upon the buyer by the requirements of a trading partner. A few typical customer scenarios include:

Meet Trading partner Requirement for OpenPGP

Key Need: A large trading partner or vendor has made a strategic decision to move to OpenPGP as its encryption standard and now requires your company to send and receive encrypted files in this format.

Solution: With Diplomat, you can automate file transfer jobs that send or pick up files at specific times from specific locations. No need to remember to encrypt and send files. Diplomat Managed File Transfer Basic Edition is an excellent choice for single trading partner implementations. It is simple to manage with all of the functionality you need to schedule file transfer jobs.

Centralize Secure File Transfer Management

Key Need: As part of your security policy, you have made a strategic decision to move to OpenPGP as your encryption standard and secure FTP for all file transfers with your trading partners.

Solution: With Diplomat MFT Enterprise Edition, you can set up profiles for each of your trading partners that include locations of source and destination files, FTP information, encryption and signature keys, and special handling information, such as ASCII armoring and canonical text. In addition, Diplomat MFT Enterprise Edition provides real-time job monitoring and the ability to respond immediately to security breaches by suspending file transfer jobs by key or by Partner. Plus, it simplifies regulatory compliance with an extensive SQL audit database with detailed information on every Admin Activity and file transfer job.

Automate File Transfers with Remote Sites

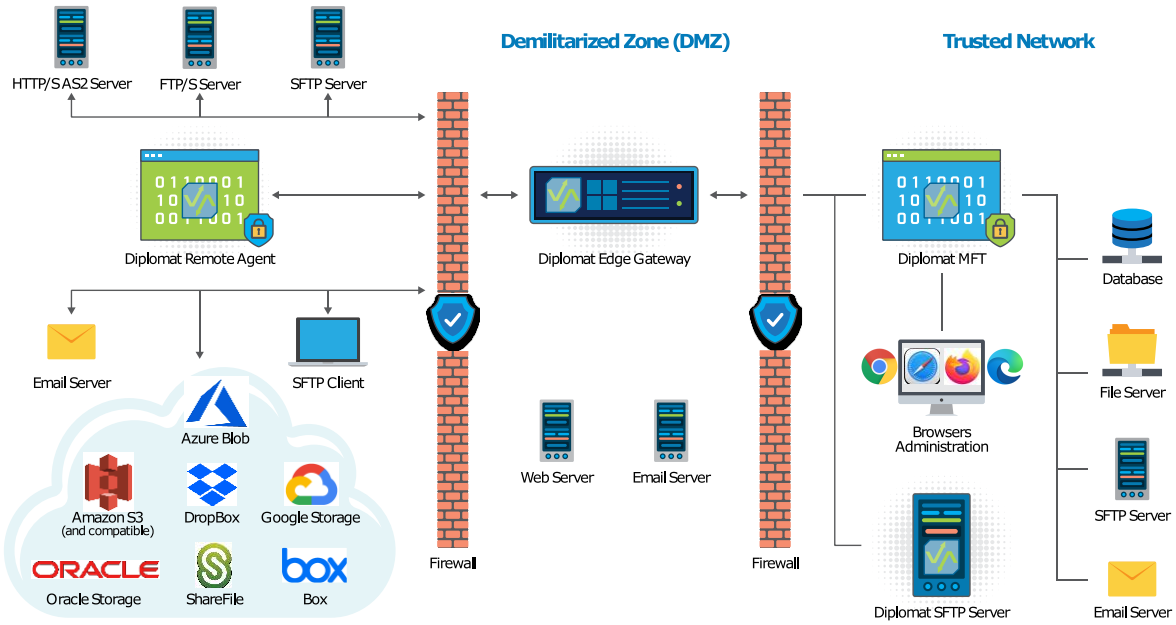
Key Need: Many businesses need to send files containing sensitive data between a central, corporate hub and multiple remote sites, such as branch offices, retail stores, sales offices, or distribution sites. As a rule, these remote sites do not have skilled IT personnel on site and the local users typically have limited technical skills.

Thus, a file transfer solution that is feasible for a corporate hub falls short of the level of simplicity required in a solution for a remote site.

Solution: Diplomat Remote Agent at the remote sites in conjunction with Diplomat MFT Enterprise Edition at the central hub is ideal for automation of file transfers with remote sites. Diplomat MFT Enterprise Edition initiates all the file transfer jobs without relying on any local IT expertise at the remote sites.

1.2 Deployment

Diplomat Managed File Transfer (Diplomat MFT or simply Diplomat) is an application that runs as a service on Windows and Linux systems. The following diagram shows a common network deployment for a Diplomat MFT solution:



Deployment Overview

The Diplomat Service is the runtime engine that executes transactions. It runs as a service and performs all the file transfer management activities. It should be located behind the corporate firewall and interoperates with FTP servers, HTTPS servers, mail servers, and other systems that may be in a corporate DMZ. It creates a log file with system messages, writes to an audit database, and archives of transaction files, if desired.

On Windows systems, the Diplomat service is set up as a Windows service, called *Diplomat MFT 64,* and on Linux systems as a daemon, called *diplomatServer*.

Each trading partner or other group that receives encrypted files from or sends encrypted files to a Diplomat MFT site must have an OpenPGP compatible application at their site. An installation of Diplomat MFT is **not** required at the trading partner site.

2 Installing Diplomat MFT

Diplomat components are supported on various ***64-bit*** platforms. Refer to Appendix B: Requirements for details.

2.1 Windows Installation

Diplomat uses a simple Next-Next-Finish executable installer file.

2.1.1 Important preparations

When installed on a Windows server, Diplomat runs as a service with a display name of ***Diplomat MFT 64*** and a service name of ***DiplomatServer64***. To view and modify the properties of the service or to stop and start it, run **services.msc** or navigate to the **Services** app in Windows per your preference**.** Services are listed in alphabetical order by default, so click on the list and start typing *d-i-p* or scroll down to get to *Diplomat MFT 64*.

2.1.1.1 Service Account

A service account is very strongly recommended and *may be **required** for proper operation*. In the *Diplomat MFT 64* service properties, select the **Log On** tab to set to a service account with the required privileges. This service account must have appropriate access to the local installation and configuration data folders, by default **C:\Program Files\Coviant Software** and **C:\ProgramData\Coviant Software**, respectively. To seamlessly use UNC paths in your Settings or Transactions you must also grant it appropriate access to all applicable network storage shares and their subfolders.

2.1.2 Initial Install

Use the following instructions **only** if you are installing Diplomat MFT components on a system on which no Diplomat MFT components are currently installed.

1. Log on to the system where Diplomat MFT components are to be installed. You must use a Windows account with administrator privileges if you are installing the Diplomat MFT Service.

2. Go to www.coviantsoftware.com and log on to the Support Portal using the credentials supplied by Coviant. Select the appropriate options to download the installer.

3. Double-click on the filename to start the installation. You can change an installation setting by selecting **Back** until you reach the previous window where the change is needed. Otherwise, select **Next** to continue to the next step. You can select **Cancel** at any time to stop the installation.

4. Scroll through the license agreement and review the terms and conditions. If you agree with the terms, select 'I accept the terms of the license agreement' and **Next** to continue. You may print a copy of the license agreement for your records using the **Print** button.

5. Choose the type of setup you would like. Select **Complete** to install the default Diplomat MFT components in the default location (C:\Program Files\Coviant Software\Diplomat-j, or for a trial installation C:\Program Files\Coviant Software\Diplomat-trial). Select **Custom** to **choose Diplomat MFT components to install** or to **change the installation location**.

6. Select a maximum memory limit for the Diplomat MFT service. For values greater than 8 GB, choose 'Other'. **NOTE:** Maximum memory should typically be set to no more than 80% of installed memory.

7. Select **Install** on the next screen to start the installation.

8. When the installation is complete, ***before*** you start the service for the first time you must:

    1. Copy your Diplomat license file to **C:\Program Files\Coviant Software\Diplomat-j**, delete the existing **diplomat.lic** file there, and rename your license file to **diplomat.lic** in its place.
    2. Modify the *Diplomat MFT 64* service properties. Refer to **Important Diplomat MFT service considerations and preparation**
    3. Ensure any OS, software, and network firewalls allow access to Diplomat on port 8080.

2.1.3 Modify

Use the following instructions only if you are **adding or removing** one or more Diplomat MFT components on a system on which at least one Diplomat MFT component is already installed.

1. Stop the Diplomat service. It may not stop immediately. Diplomat waits until all currently queued or running jobs are completed before stopping the service.

   NOTE: To be sure that no jobs are queued or running before you stop the service, suspend all transactions, and wait until an orange status indicator '🟧' is displayed next to the Transactions folder.

2. Double-click on the filename to start the installation. You can change an installation setting by selecting **Back** until you reach the previous window where the change is needed. Otherwise, select **Next** to continue to the next step. You can select **Cancel** at any time to stop the installation.

3. Select **Modify**.

4. To **ADD** a component, check all the currently installed components **AND** the new component. The new component will be installed in the directory in which each original component was installed. The default directory is C:\Program Files\Coviant Software\Diplomat-j. To **REMOVE** a component, uncheck the component to be removed **AND** check the components to be retained.

5. **CAUTION:** Leaving an installed component's box unchecked will uninstall that component.

2.1.4 Repair (Update Build)

Use the following instructions if you are updating to a newer build of the same version of Diplomat MFT.

1. Stop the Diplomat service. It may not stop immediately. Diplomat waits until all currently queued or running jobs are completed before stopping the service.

   NOTE: To be sure that no jobs are queued or running before you stop the service, suspend all transactions, and wait until an orange status indicator '🟧' is displayed next to the Transactions folder.

2. Double-click on the filename to start the installation and select **Repair**.

3. When complete, start the Diplomat service.

2.1.5 Remove

Use the following instructions only if you are **uninstalling ALL** Diplomat MFT components.

1. Stop the Diplomat service. It may not stop immediately. Diplomat waits until all currently queued or running jobs are completed before stopping the service.

   NOTE: To be sure that no jobs are queued or running before you stop the service, suspend all transactions, and wait until an orange status indicator '■' is displayed next to the Transactions folder.

2. Initiate the uninstallation through Windows. If running the installer instead, select **Remove**.

2.1.6 Version Upgrade

Use the following instructions only if you are **upgrading** Diplomat MFT to a newer version.

1. Go to www.coviantsoftware.com and log on to the Support Portal using the credentials supplied by Coviant. Select the appropriate options to download the installer.

2. Stop the Diplomat service. It may not stop immediately. Diplomat waits until all currently queued or running jobs are completed before stopping the service.

   NOTE: To be sure that no jobs are queued or running before you stop the service, suspend all transactions, and wait until an orange status indicator '■' is displayed next to the Transactions folder.

3. Double-click the file to start the upgrade. Read and accept the terms, pressing **Next** to continue. You may print a copy of the license agreement for your records using the **Print** button.

6. Start the Diplomat service.

   If you need to start the service with all jobs suspended, create a file called 'safestart' with NO file extension in the DiplomatData root folder. The content of the file does not get processed – only the name of the file matters.

   If a 'safestart' file exists when the Diplomat Service is started, the 'startup' file is deleted and the Transactions folder is suspended before any jobs are started. Right-click on the Transactions folder to unsuspend Transactions.

7. Release all transactions when ready to resume normal operations.

2.2 Linux Installation

The Linux installation of Diplomat Managed File Transfer supports installation of the Diplomat MFT Service. The Diplomat MFT Client is supported only on Windows systems.

NOTE: If you plan to use Diplomat MFT Scripting Agent, refer to *Diplomat MFT Scripting Agent User Guide* for instructions on how to install Diplomat MFT Scripting Agent. When you install the Diplomat MFT Service, the files you need to install the Diplomat MFT Scripting Agent on a UNIX system are written to /opt/coviant/diplomat-j/scriptingAgent or corresponding directory for your installation.

2.2.1 Diplomat MFT Service Initial Install

1. On the system where the Diplomat MFT Service is being installed, create an operating system account with username 'diplomat'. Log on with username 'diplomat'. Create directory /opt/coviant/diplomat-j to be used for installation and maintenance of the Diplomat MFT Service.

   NOTE: If you use UNC paths or mounted drives when setting up transactions and access to those paths or drives is restricted, the 'diplomat' account must have the required access privileges and you must set up the diplomatServer daemon to run as the 'diplomat' account.

2. Go to www.coviantsoftware.com and log on to the Support Portal using the credentials supplied by Coviant. Select the appropriate options to download the diplomatServer.tar.gz file.

3. Unzip diplomatServer.tar.gz in /opt/coviant/diplomat-j or corresponding directory for your installation to install the Diplomat MFT Service software, a Java Runtime Environment (JRE), and the Tomcat web server.

4. Review the license agreement in the file named *Coviant Software Clickwrap License Agreement.pdf* in /opt/coviant/diplomat-j/docs or corresponding directory for your installation. If you DO NOT agree with the license terms, DO NOT continue the installation. Continuing the installation indicates that you have accepted the license terms. You may want to print a copy of the license agreement for your records.

5. To set the diplomatServer daemon for the Tomcat web server to start automatically on system reboot, log on as 'root'. Execute the setup script at /opt/coviant/diplomat-j/install_systemd.sh or corresponding directory for your installation.
   NOTE: If you use UNC paths or mounted drives when setting up transactions and access to those paths or drives is restricted, the 'diplomat' account must have the required access privileges and you must set up the diplomatServer daemon to run as the 'diplomat' account.

6. Copy the Diplomat MFT license file, named *xxx.lic,* that you received from Coviant Software to /opt/coviant/diplomat-j or the corresponding directory for your installation. **Rename the *xxx.lic* file to *diplomat.lic* using all lowercase characters.**

   NOTE: The default username is 'Administrator' and the default password for all licenses is 'diplomat' for all licenses. You must reset this password using the Diplomat MFT Client immediately after you install a new license.

   NOTE: If you have not received a license file, you can rename the temporary *diplomat.templic* file in /opt/coviant/diplomat-j/startup or the corresponding directory for your installation to *diplomat.lic* and continue the installation. This license is a preview license only and transaction scheduling is not enabled. You must contact Coviant Software Support to receive a copy of your permanent license.

7. To start the diplomatServer daemon, reboot the Linux system or use the 'service diplomatServer start' command.

8. Open a browser window (not Internet Explorer) and navigate to https://***machine***:8080 (where "***machine***" is the name or IP address of the computer on which Diplomat MFT is installed), which should display the administrator login page. If the service is not running, see Appendix B: Windows Diplomat MFT Service.

   NOTE: The server port is set to 8080 by default. If port 8080 is already in use, contact Coviant Software Support for instructions on how to change the server port number.

   NOTE: You will receive a message from your browser indicating a problem with the web site's security, Select Continue to access the login page.

   If you do not see the login page , contact support@coviantsoftware.com for assistance.

9. Check to ensure that all firewall software is configured to allow the diplomatServer daemon access to the Internet.

10. A new directory structure is created during the installation of the Diplomat MFT Service. If you selected the default installation location, this directory structure is located under /opt/coviant/diplomat-j or the corresponding directory for your installation. These directories contain the Diplomat MFT Service and various Diplomat MFT databases. Changes to any of these files can affect the performance of Diplomat. **We strongly recommend that you set privileges on these directories to limit access** to only necessary applications, such as backup.

2.2.2 Diplomat MFT Service Version Upgrade

1. Open the Diplomat MFT Client and suspend all transactions by selecting **Jobs** > **Suspend** > **All Transactions Directly** from the top menu bar. To be sure that no jobs are queued or running before you stop the diplomatServer daemon, wait until an orange status indicator '🟧' is displayed next to the transaction folder in the job monitor. Exit from the Diplomat MFT Client.

2. On the system where the Diplomat MFT Service is being upgraded, log on as 'root' or other account with 'root' privileges. Stop the diplomatServer daemon by using the 'service diplomatServer stop' command.

   NOTE: When you stop the diplomatServer daemon manually, it may not stop immediately. The system waits until all currently running jobs are completed before stopping the daemon.

3. On the system where the Diplomat MFT Service is being upgraded, log on with username 'diplomat'.

4. Unzip the new diplomatServer.tar.gz in /opt/coviant/diplomat-j or a corresponding directory for your installation.

5. Review the license agreement in the file named *Coviant Software Clickwrap License Agreement.pdf* in the /opt/coviant/diplomat-j/docs directory or the corresponding directory for your installation. If you DO NOT agree with the license terms, DO NOT continue the installation. Continuing the installation indicates that you have accepted the license terms. You may want to print a copy of the license agreement for your records.

6. Log on as 'root' or other account with 'root' privileges. To restart the diplomatServer daemon, reboot the Linux system or use the 'service diplomatServer start' command.

7. To confirm that the diplomatServer daemon is operating correctly, open a web browser and navigate to the secure login page https://localhost:8080/.

2.2.3 Diplomat MFT Service Remove

1. Log on as 'root' or other account with 'root' privileges so you may stop the diplomatServer daemon by using the 'service diplomatServer stop' command.

   NOTE: When you stop the diplomatServer daemon manually, it may not stop immediately. The system waits until all currently queued or running jobs are completed before stopping the daemon.

2. Execute the uninstall script at /opt/coviant/diplomat-j/uninstall or the corresponding directory for your installation to remove the startup script for the diplomatServer daemon.

   NOTE: If you want to permanently uninstall Diplomat MFT Service, including the Diplomat MFT transaction database and other Diplomat MFT files, you can delete the /opt/coviant/diplomat-j directory and remove the 'diplomat' user account.

3 Diplomat Fundamentals

3.1 User Interface

Diplomat Managed File Transfer has a simple, intuitive user interface that combines a top menu bar for overall functions that initiate pop-up dialog boxes; a navigation tree for accessing specific Partner profiles, transactions, and/or keys, and an active window for editing and viewing keys, Partner profiles, and transactions.

The menus allow access to a variety of functions via sub-menus and pop-up dialog boxes:

- File – Backup, merge, restore configurations. View license details and log files. Check status of Diplomat and current admin logins.
- Keys – Import, create, modify, export, search/move, delete, and recover OpenPGP keys, SSH keys, and SSL server certificates.
- Partners – Create, save, delete, and search/move Partner profiles.
- Transactions – Create, save, delete, and search/move transactions.
- Settings – Set up system-wide parameters and defaults to be used in creating, running, and debugging transactions.
- Jobs – Release jobs, suspend jobs, and open the Job Monitor.
- Reports – Generate reports on configuration and activity.
- On the far right you'll see your username with options to sign out and other actions.

The main part of the screen is the active window on the right-hand side. It displays the details of the active key, Partner, transaction, or SFTP user that is being viewed or edited. Some details are displayed in panels that can be expanded for editing and then collapsed to save screen space.

The navigation tree on the left side of the main screen displays folders and objects in a tree format for easy navigation. The navigation tree also:

- Enables right-click menu actions such as Export, Save, Clone, Reset, Validate, View Logs, Run Now, Delete, Release, Suspend, or Search/Move.
- Displays a root folder with the name of the server where the Diplomat MFT Service is installed and the Diplomat MFT version number.
- Highlights the name of an object that is currently displayed in the active window for viewing or editing.
- Bolds the name of objects that have unsaved changes pending.
- Indicates suspend status of Keys, Partners, and Transaction folders by displaying an orange status indicator for items that have been suspended.
- Indicates when all transactions are suspended due to critical audit error by displaying a pink status indicator on the transaction folder.
- Indicates when all transactions are suspended due to a transaction database restore by displaying a purple status indicator on the transaction folder.

3.2 Databases

Diplomat Managed File Transfer Enterprise Edition retains data in three main databases:

- **Diplomat MFT transaction Database** is an embedded database which contains all data used to create and schedule jobs, including keys, Partner profiles, transaction, and configuration data.
- **Diplomat MFT Job History Database** is an embedded database which contains all job and file history records.
- **Audit Database** contains detailed records of every job executed and all attempted file transfers. The built-in audit database is a set of XML files where each job has a single file. An external SQL database server may be used instead.

3.3 Data Security

Diplomat ensures you can secure your data in various ways.

- Before files are transferred, use OpenPGP keys to encrypt and sign the files.
- During file transfer, choose secure protocols or the secure Diplomat Remote Agent to protect both login data and data in transit.
- After files are transferred, use OpenPGP keys to decrypt and verify files.

In addition, Diplomat works behind the scenes to improve your overall security:

- Does not require administrators to be granted access to remotely control the server machine itself.
- Only allows accounts with *Administrator* privileges to execute sensitive activities, such as updating licensing, managing administrator accounts, and database restores.
- Tracks all administrator activity, such as changes to the Diplomat MFT transaction database. Data for each administrator action is captured in the Diplomat MFT log files and the audit database, if desired.
- Displays on every screen the last date that the displayed data was updated and the Domain/User ID that performed the update.
- Automatically encrypts all sensitive data in the Diplomat MFT transaction database, including the passphrases or passwords associated with OpenPGP or SSH key pairs, FTP servers, and mail servers. Sensitive information is never written to disk in cleartext or unencrypted format.
- Uses a secure connection (TLS) for all administrative communications.
- Only requires the entry of passphrases to manage sensitive tasks related to key pairs, such as export, modify, delete, or recover. Passphrases do not need to be known by users setting up file transfer jobs.

4 Administering Diplomat

Diplomat is administered via a desktop browser. Current versions of Chrome, Edge, Firefox, and Safari work well. Internet Explorer is not supported.

Administrative sessions can be terminated after a period of inactivity. The session expiration period is set under **Settings** > **Session Management** from the menu bar.

Note that for parts of the graphical interface, some sections may be able to be collapsed or expanded at will. Click the chevron icon or to expand (⌄) or collapse (⌃) the view:

4.1 Sign In

When Diplomat is initially installed, the default username is ***Administrator*** with ***diplomat*** as the password. Upon first login, you will be required to change the default password to one of your own choosing.

From a workstation with connectivity to the Diplomat server, open a browser window and navigate to the Diplomat service. There is no need to remotely control the Diplomat server computer to launch a browser window.

For the URL, use **https://** before the **machine name or IP address** of the Diplomat server, and add **:8080** as the port. For example, let's use your browser to log in to Diplomat running on a server with the computer name of ExampleServer. In that case you would enter https://ExampleServer:8080 in the address bar.

> **NOTE:** You will receive a browser security warning, as Diplomat will use an unsigned unique certificate automatically generated during installation. You must choose to proceed to access the login page.

4.2 Change Your Password

You can change your password at any time by clicking your username at the far right of the menu bar and choosing the **Change Password** option.

4.3 Sign Out

Click your username at the far right of the menu bar and choose **Sign Out**.

You will be reminded if you have *Advanced Troubleshooting* turned on for any Transactions. You can leave it enabled or turn it off, if desired.

If the *Backup Reminder on Exit* setting is enabled, you will be asked if you would like to initiate a Diplomat backup.

4.4 Date Variables

There are a number of opportunities to use a <DATE> variable in Diplomat. The table below includes the list of each Date Variable element. Note that these elements are case sensitive. Additionally, there may be limitations on which elements may be used in which context. For example, Source Files fields may only have a single Year and Month element or are otherwise invalid.

Date Variable Elements		
Element Type	**Element**	**Element Description**
Year	<YY>	2-digit numeric year with zero padding added when necessary (e.g., 22)
	<YYYY>	4-digit numeric year (e.g., 2022)
Month	<MM> <M>	2-digit numeric month with zero padding added when necessary (e.g., 04) **NOTE:** <MM> must always be capitalized for a 2-digit month. Lowercase <mm> is always used to specify minutes. 1-digit numeric month, with no zero padding (e.g., "4" or "12")
	<MMM> <Mmm> <mmm>	3-character month with matching capitalization If all letters are capitalized, then all letters in the name of the month are capitalized (e.g., <MMM> for APR). If only the leading M is capitalized, then only the first letter of the month is capitalized (e.g., <Mmm> for Apr). If all letters are lowercase, then all letters in the name of the month are lowercase (e.g., <mmm> for apr). No other capitalization formats are allowed.
	<MMMM> <Mmmm> <mmmm>	Complete month's name with matching capitalization If all letters are capitalized, then all letters in the name of the month are capitalized (e.g., <MMMM> for APRIL). If only the leading M is capitalized, then only the first letter of the month is capitalized (e.g., <Mmmm> for April). If all letters are lowercase, then all letters in the name of the month are lowercase (e.g., <mmmm> for april). No other capitalization formats are allowed.
Day	<DD> <D>	2-digit numeric day of month with zero padding added when necessary (e.g., 04) 1-digit numeric day of the month; no zero-padding added. (e.g., "4" or "12")
Julian Day	<JJJ> <J>	3-digit numeric Julian day of the year with zero padding added when necessary (e.g., 014 for January 14) **NOTE:** A Julian day cannot be used with any other day or month element. 1-digit numeric Julian day of the year – no zero padding (e.g., "14" for January 14)
Hour	<hh>	2-digit hour using 24 hour clock with values from 0 to 23
Minute	<mm>	2-digit minutes **NOTE:** <mm> must always be lowercase for minutes. Uppercase <MM> is always used to specify a 2-digit month.
Second	<ss>	2-digit seconds
Millisecond	<ms>	3-digit milliseconds
Time Zone	<Z>	Short Time Zone, e.g., "PST" Long Time Zone, e.g., "Pacific Standard Time"
AM/PM	<AMPM>	The time of day indicator for 12-hour clocks; either "AM" or "PM"

5 File Menu

The File Menu allows you to backup and restore Diplomat's configuration as well as manage your license, view logs, and display the status of the Diplomat's service and system along with current administrative sessions.

5.1 Backup

Diplomat backups are a snapshot of the configuration in that moment in time, saved as a single file. You can manually back up the Diplomat MFT database at any time by selecting **File** > **Backup**. This backup feature is not intended to replace regular backups of the Diplomat MFT data as part of your overall backup process. See Backup settings to manage automatic backups.

For Windows systems, the default backup directory is C:\ProgramData\Coviant Software\Diplomat-j\backup. For Linux systems, the default directory is /opt/coviant/diplomat-j/backup. When creating a backup, you may browse to select a different directory or paste in a desired folder path. Use the **Test** button to determine whether the location is accessible and is read/write enabled for the Diplomat service.

The default backup filenames are in the form 'DiplomatBackup.version.year + month + day + hour (24-hour format) + minutes + seconds.dbu'. For example, a backup created on March 22, 2022 at 3:19:20 PM by Diplomat MFT v9.0 would be named 'DiplomatBackup.0.0.20220322.151920.dbu'. If desired, you can enter a different backup filename.

NOTE: All Diplomat MFT backup files have the file extension '.dbu' and merge files have the file extension '.dmrg'.

Check the "Remove passwords" option to securely omit all passwords from the backup file. This is only used when sharing a backup file with another party where passwords and passphrases may not be desirable to include, such as sending to the Coviant support team.

When creating a merge file, only the selected transactions and their related Partners and keys are retained in the merge file. Use the Filter Phrase field to limit the available transactions displayed to Transaction Names containing the filter phrase. Use the **Reset** button to display all available transactions.

NOTE: The Filter *Phrase* is case sensitive.

5.2 Merge

Merge is only available to accounts with administrator privileges. Among its various uses, it's highly helpful for promoting processes from development to test, test to production, and so on. A merge file contains selected transactions and their related Partners, keys and linked transactions, if any.

Use Merge **ONLY** if you need to **ADD** or **OVERWRITE** keys, Partners, or transactions from a backup or merge file to your current set of keys, Partners, and transactions. Otherwise Restore to replace an entire database with a backup copy.

Browse and select the backup file that you would like to merge with your active database. If the backup or merge file is encrypted, you must also enter the password used when the file was created.

When merging Diplomat MFT databases, you must decide how duplicate items are handled during the merge process. For example, if you have a key with the same name in both databases, your choice will determine which key is retained after the merge process is complete.

Diplomat MFT checks whether any of the transactions to be merged require overwriting an existing key, Partner, or transaction. If so, all job scheduling will be suspended and processing will wait for all currently queued or running jobs finish executing before starting the merge. All jobs are suspended during the merge operation. If you do not choose to release the suspended jobs when prompted at the end of the merge operation, all jobs remain suspended. A purple status indicator '■' is displayed next to the transaction folder in the navigation tree and an orange status indicator '■' is displayed next to all transaction objects in the tree. And as a safety precaution, Diplomat will attempt to take a backup to the default backup directory before initiating a database merge or restore operation.

You cannot complete a merge when other administrators are logged in. Instead, you will be prompted for what you would like to do. Click 'Cancel' or else 'Disconnect' to disconnect all other administrators and continue with the merge.

To release job suspension due to a Diplomat MFT database merge or restore, select **Jobs** > **Release** > **Release DB Merge/Restore Suspend** or right-click on the Transactions folder and select **Release DB Merge/Restore Suspend**.

If any items were already suspended in your active Diplomat MFT database prior to executing a merge, those items will remain suspended even after the Merge/Restore suspension is released.

NOTE: In addition, all individual keys, Partners or transactions that were added to the Diplomat MFT database during the merge process also remain suspended even after the Merge/Restore suspension is released.

5.3 Restore

Restore is only available to accounts with administrator privileges.

Use Restore to *replace* an entire Diplomat configuration with the details in the backup file.

All job scheduling will be suspended and processing will wait for all currently queued or running jobs finish executing before starting the restore. And as a safety precaution, Diplomat will attempt to take a backup to the default backup directory before initiating a database merge or restore operation.

Browse to select the backup file from which you would like to restore. If the backup file is encrypted, you must also enter the backup file password.

You have the option to restore server configurations settings in addition to the items in the tree view**. NOTE:** *Calendars* and *Proxy Servers* settings are always restored, even if you select not to restore the other configuration settings.

You cannot complete a restore when other users are connected. Click 'Cancel' or else 'Disconnect' to disconnect all users and continue with the restore.

When you restore a Diplomat MFT database, all jobs are suspended during the restore operation. If you do not choose to release the suspended jobs when prompted at the end of the restore operation, all jobs remain suspended. A purple status indicator '■' is displayed next to the transaction folder in the navigation tree and an orange status indicator '■' is displayed next to all transaction objects in the tree.

To release job suspension due to a Diplomat MFT database merge or restore, select **Jobs** > **Release** > **Release DB Merge/Restore Suspend** or right-click on the Transactions folder and select **Release DB Merge/Restore Suspend**.

If any items were already suspended in your active Diplomat MFT database prior to executing a merge, those items will remain suspended even after the Merge/Restore suspension is released.

5.4 License

License information is only available to accounts with administrator privileges.

Diplomat is licensed based on the details associated with your License ID. The License screen displays the information provided by your current license.

The ***Activate*** button is displayed when Diplomat senses a more recent license available than the current one. Click the button to switch to this newer license.

5.5 Logs

You can view the content of log files by selecting the log files that you would like to view. Only log files located in the configured logging directory are shown. Logging configuration can be viewed and managed in **Settings** > **Logging.** If you check the box for more than one log file, then all selected log files are appended together for viewing. Once the desired log files are chosen, you can take additional actions.

Log entries start with a line that identifies the level of the message (Debug, Informational, Warning, Error, or Critical Error) and a timestamp. The subsequent lines are the message content. The log file contains several types of entries:

- Administrator activity such as updating transactions, changing a password, or importing a public key
- Entries for each step in the execution of a job.
- Summary entry at the end of each job, the same as included in email notifications
- Error messages

If you would like to narrow down what is displayed, **Set Filter** allows you to select and view a sub-set of all log messages. If you have already set a filter and then select **Set Filter** again, your previous filter settings are displayed. For filtering, you can choose a minimum log verbosity level as well as choosing whether to filter by a phrase string or a Transaction name.

Minimum Filter Level limits the log messages selected to include only log messages with a particular log level or above. **Debug** is the default filter level, which shows all messages, except for large messages such as directory listings.
Search by Phrase allows you to select all log messages containing a specific phrase string. This feature is helpful when you are searching for a particular entry not necessarily related to given Transaction.

Search by Transaction Name allows you to select all log messages specifically related to a given Transaction. If no Transaction is selected, then all Transactions are displayed. This feature allows you to view all entries associated with a particular transaction in chronological order. Only transactions currently present in Diplomat are available.

If you do not filter by *Transaction Name*, entries from various transactions are likely to be intermingled, as log messages are written in chronological order.

Reset Filter reverts the log viewer session to the defaults, such that all messages are displayed.

Refresh reloads the current log file using the current filter settings and includes any additional messages added to the log file since the last refresh.

5.6 Diplomat Status

The **Diplomat MFT Service** panel displays information about the Diplomat service state, start time, service account, max memory, and version and build numbers. The **System** panel shows the Diplomat server's host name, IP address, operating system, and CPU architecture.

The **Connections** panel lists all current administrator session connections with checkboxes to select one or more active sessions. The first item on the list is always your own session and cannot be selected. **Logoff Selected** forcefully logs off all the selected connections.

Disable/Enable Logins is used to temporarily disable all new sessions. However, as a safety measure accounts with Administrator privileges are prompted about this status upon attempting to log in and can choose to disable it.

6 Keys

OpenPGP and SSH keys as well as SSL certificates are forms of public key encryption technology. They use key pairs, consisting of a private key and a public key. A private key can decrypt communications or files as well as sign a file, and as such it should be protected with a passphrase and kept securely stored internally. A public key is all that is needed to encrypt communications or files or to verify a signature. Thus, a private key must be kept private, while a public key may be freely distributed publicly. No one can derive or "guess" your private key, since a key pair cannot be deduced from the public key.

OpenPGP is used to protect files. You can create an OpenPGP key pair, export the public key to a file, and send the public key file to your trading partners or other remote sites while keeping your private key protected. When you send or receive a file, you must specify which key(s) to use to encrypt, decrypt, sign, or verify the file.

SSH keys may be used SFTP server authentication. You can create an SSH key pair, export the public key, and send the SSH public key file to a remote SFTP server administrator who associates your public key to your account. You may then use that SSH Key Pair to authenticate your login request. An SFTP server must always have a key pair in place, so you must create or import one before you can enable Diplomat to act as an SFTP Server. Connecting clients may wish to provide you with their own SSH public key for you to import and associate with their SFPT User account, and you may even choose to require them to do so.

SSH host keys are used to verify the SFTP server identity before connecting to it. SSH host keys are added when setting up a Partner profile. SSH host keys are added and deleted from Diplomat using **Keys** > **SSH Host Keys** from the menu bar.

SSL certificates are simply keys with some additional metadata included that may be validated and signed by a trusted Certificate Authority. They can be managed under **Keys > SSL Certificates** and for Diplomat's use are either **Server** or **Client** certificates. SSL server certificates are like SSH Host Keys, used to validate a remote server's certificate. This is **required** for AS2 transfers.

SSL client certificates are used by Diplomat when connecting to remote servers that require it. This is rare but not unheard-of for FTPS connections, though it is almost never used for HTTPS-based communications. However, this is **required** for AS2 transfers.

6.1 Keys Navigation Tree

The navigation tree shows the keys currently in Diplomat's key ring, listed by name. The keys are divided into sub-folders for OpenPGP keys, SSH Keys, and SSL Certificates.

Click to select a folder under OpenPGP Keys, SSH Key Pairs or SSL Certificates in the navigation tree and right-click to create or import keys, add a sub-folder, expand/collapse all sub-folders, rename the folder, delete the folder and/or search/move the folder.

Select a key in the navigation tree and right-click to save changes to the key, reset the key settings to the saved values, export the key to a file, rename the key, delete the key, move the key to a new sub-folder, release transactions using the key for scheduling or suspend transactions using the key.

The navigation tree also indicates the suspension status of keys. If a key is suspended, all transactions associated with that key are indirectly suspended as well. For example, you may need to suspend transactions for a key if a trading partner notifies you that an OpenPGP key or SFTP account may have been compromised.

When transactions associated with a key are suspended, an orange status indicator '■' is displayed next to the key in the navigation tree and next to all transactions that have been suspended due to the suspension of the key.

To suspend all transactions associated with a key, select the affected key in the navigation tree. Then right-click the key and select the option to suspend it. Alternatively, go to **Jobs** > **Suspend** > **Active Key**. Any jobs that are currently queued or running when a key is suspended will complete normally. No further jobs using the suspended key are scheduled until the key has been released.

To release suspension on all transactions associated with a key, select the suspended key. Then right-click the key and select the option to release it. Alternatively, go to **Jobs** > **Release** > **Active Key**.

6.2 OpenPGP Keys

OpenPGP keys can be used to encrypt/decrypt and to sign/verify files.

If you need to encrypt a file to send to someone else, you need to get their public key from them. If they need to encrypt a file for you to receive, you need to send them your public key, the public half of your key pair. If you need to exchange files in both directions, they you both need to share your respective public keys with each other.

If you do not already have an OpenPGP key pair, you can create one in Diplomat. You can then publish that public key to your trading partners or Diplomat MFT Remote Agents while retaining and protecting your private key. Anyone with a copy of your public key can encrypt files, and then only you can decrypt the files.

Diplomat MFT can import keys or key pairs created by other OpenPGP-compliant products and add them to its key ring. An individual key may be exported from the key ring into a file for use with other applications or for sending to third parties. For example, you will need to export your public key to send it to a trading partner.

When you establish a relationship with a trading partner, they may send you their public key. Each time they encrypt a file to send to you, they may choose to use their private key to sign the file. As part of the decryption process, you can determine whether your trading partner encrypted the file and whether the file integrity remains intact by using their public key to verify the signature. If verification fails, then you should assume that your trading partner was not the source of the encrypted file or that the file contents have been compromised. Signing and verifying the signature provides non-repudiation, which means that it prevents the sender from claiming that someone has tampered with the data or that someone else impersonating them is the source of the file.

The OpenPGP Working Group of the Internet Engineering Task Force (IETF) defines the standard methodologies and formats for encrypted messages, signatures, and keys, such as in RFC 2440 and RFC 4880.

6.2.1 OpenPGP Key Menu Items

Each OpenPGP public key and key pair in Diplomat's key ring has a unique key name, a label which is displayed throughout Diploamt. It is good practice to ensure these names are readily understandable. For example, you might choose the name 'Acme Foods' for the public key provided by Acme Foods, regardless of the key file's name.

Diplomat's OpenPGP key management allows you to:

- Create key pairs for signing and encryption.
- Add encryption sub-keys to existing key pairs.
- Import existing key rings, public keys, and key pairs created by other OpenPGP-compliant products.
- Export public keys and key pairs.
- Delete and recover keys.
- Search or move keys.

NOTE: All actions related to an OpenPGP key pair require the entry of the secret passphrase for that key pair.

6.2.1.1 OpenPGP Key Pairs

OpenPGP key pairs have a master key and one or more sub-key(s) for encryption. Although each key pair may have multiple encryption sub-keys, only one encryption sub-key should be valid at any time.

As long as the master key has not expired, encryption sub-keys can be added. You are prompted to add sub-keys when a master key is created. If you do not add encryption sub-keys at this time, you can add sub-keys later using **Keys** > **OpenPGP Key Pairs** > **Add Subkey** from the top menu bar.

Subkeys are a part of the OpenPGP standard. They are each essentially their own key pair (private and public both), but they are bound to the master private key. They can be given start and end validity periods, and OpenPGP-compatible applications support their use automatically. In this way, you can provide a single combined public key file to the trading partner, and they can use their application to encrypt files with whichever is the valid public subkey at the time. Diplomat will use only the currently valid subkey to decrypt those files and to sign files. That means that even determined bad actors hoping to crack your private key would have to start over with new public key every time the current subkey rotates out to be replaced with a new one.

Adding an encryption sub-key does not affect the master key. If you have given the public key from a key pair to trading partners for use in the verification of files sent by you, this key can still be used for signing and verification of files even if no encryption sub-keys are currently valid.

Regularly changing the sub-key used to encrypt files makes your key much more secure, as anyone trying to attack your key must break the algorithm used by the currently-valid sub-key. Generally, the more often you change your encryption sub-key the more secure your key is.

To maximize the benefits of using sub-keys, it is a good practice to create a set of encryption sub-keys that cover the ENTIRE PERIOD that you reasonably expect to use the master key, when you first create the master key and before any public keys are distributed to Partners. If you expect to use the key for 5 years, you may want to create 10 sub-keys each valid for consecutive 6 month periods or 20 sub-keys for consecutive 3 month periods. You get the benefit of a new encryption key every 3 to 6 months, without the hassle of continually redistributing public keys to all of your Partners.

6.2.1.1.1 Create Key Pair

When you create OpenPGP keys using Diplomat, you must provide several pieces of information:

Key Name

Each key pair and public key must have a unique *Key Name* in Diplomat. A *Key Name* is a label used only in Diplomat. You should choose a name that makes it easy for you to determine the intended use of the key when setting up transactions. For example, Acme Corporation might use 'Acme Decryption Key' to identify the private key from which it plans to export and send the public key portion to its trading partners for encrypting files. *Key Name* field length is limited to 64 characters.

NOTE: If you attempt to create a key with a *Key Name* that already exists in the Diplomat MFT database, you have the option to replace the existing key with the new key. If you choose to overwrite the existing key, you cannot recover the original key later. As a precaution, Diplomat MFT attempts to export a copy of the original key before it is overwritten. For Windows systems, the default key directory is C:\ProgramData\Coviant Software\Diplomat-j\keys. For Linux systems, the default directory is /opt/coviant/diplomat-j/keys. **To ensure you do not permanently delete a key, export the original key before you attempt to replace it.**

Key Type

OpenPGP supports two different key types: DH/DSS and RSA.

Bit Strength

Bit strength of a key is related to how difficult the algorithm is to break. The larger the bit strength of a key, the more difficult and time-consuming the code-breaking task would be. However, the larger the bit strength of the key, the longer it takes to encrypt, decrypt, sign, or verify a file. Keys sizes are generally 1024, 2048, or 4096.

NOTE: DH/DSS keys allow 1024, 2048, and 4096 for encryption sub-keys, but only 1024 for signature sub-keys.

User ID

Identifies the owner of the key. A common practice is to enter the corporate and/or division name and a good contact email address for potentially use by trading partners who will be receiving the public key. For example, a good *User ID* that would indicate that the owner of the key pair is the Payroll Department at Acme Foods might be 'Acme Foods Payroll <it.payroll@acmefoods.com>'. If you send a public key to a trading partner, they are likely to use the *User ID* to determine the owner of the key, and a working email address helps identify a good contact should there be a question, concern, or other type of communication required.

In fact, some encryption products actually *require* that the user ID be in the form 'Name <user@domain.com>' such as used in the example above.

Passphrase

OpenPGP uses a passphrase to encrypt your private key. A good passphrase should be difficult for others to guess.

You must provide the passphrase, when you import, create, modify, delete, or recover a key pair, but you do not need provide it when selecting the key in a Partner profile or Transaction. Once you have created a key pair in Diplomat, the passphrase is stored separately from the key pair in a special encrypted format. If you forget the passphrase, an account with *Administrator* privileges can recover it.

Expiration

You can set the expiration such that it never expires, expires in a certain number of days, or expires on a certain date.

Symmetric Algorithms are used for data encryption, while ***Hash Algorithms*** are used for protecting signatures.

6.2.1.1.2 Add Subkey

A sub-key can be added to a key pair at any time during the lifetime of the master key. When you create an encryption sub-key, you must set unique, non-overlapping usage periods for each one. Diplomat uses the currently-valid encryption sub-key to encrypt files.

To add a sub-key, select the key to which you would like to add a sub-key on the navigation tree. Go to **Keys** > **OpenPGP Key Pairs** > **Add Subkey** from the top menu bar.

Key Type and *Bit Strength* are the same for subkeys as they are for key pairs.

Start Date

The first date the sub-key is to be used for encrypting files. This defaults to the date following the most recently created sub-key expiration date.

Expiration

You can set the expiration such that it never expires, expires in a certain number of days, or expires on a certain date. Each expiration date for a sub-key created by Diplomat MFT cannot be later than the expiration date of the master key.

6.2.1.1.3 Import Key Pairs

Keys created by other OpenPGP-compliant products can be imported into the Diplomat MFT database. Key rings from other OpenPGP products can be imported directly or you can export a key into an individual file using your OpenPGP-compliant product and then import it into Diplomat. Go to **Keys** > **OpenPGP Key Pairs** > **Import Key Pairs** from the top menu bar.

Browse to the location of the key pair file or key ring file to be imported.

Import Checkbox
Check *Import* beside each key that you would like to import.

Key ID
Uniquely identifies a key. A public key always has the same *Key ID* as the key pair from which it was created. Two key pairs or two public keys may have the same *User ID*, but they must have different *Key ID*s.

NOTE: If a key pair to be imported has the same *Key ID* as a key pair in the Diplomat MFT database, the key cannot be imported. The *Import* checkbox and *Key Name* field will be disabled.

User ID(s)
Text string that helps identify the owner of the key. Two key pairs may have the same *User ID*, but they must have different *Key IDs*.

Diplomat Key Name
Diplomat Key Names are labels used only by Diplomat. All key pairs and public keys must have unique *Key Names* in Diplomat. The default value shown in the *Diplomat Key Name* field is the *User ID* from the OpenPGP key. *Diplomat Key Name* field length is limited to 64 characters.

Diplomat Key Names are not the same as *Key ID*s. Diplomat MFT allows a public key and a key pair to have the same *Diplomat Key Name*, but two public keys may **not** have the same *Diplomat Key Name*. You cannot import a public key that has the same internal *Diplomat Key Name* as an existing public key.

Since *User IDs* do not have to be unique in OpenPGP-compliant key rings, you may need to modify the default *Diplomat Key Name* before importing. You can choose a name that makes it easy to determine the intended use of the key when setting up transactions. For example, you might use 'Acme Verification Key' to identify the public key from Acme Corporation that you will use to verify signatures on files you receive.

A public key in Diplomat MFT and the key pair from which it was created share the same *Key ID*, but cannot share the same *Diplomat Key Name*.

If you attempt to import a key pair with a *Diplomat Key Name* that already exists in the Diplomat's key ring, you have the option to overwrite the existing key pair or to modify the *Diplomat Key Name* field. If you choose to overwrite the existing key pair from the screen below, the *Overwrite Checkbox* is checked automatically.

NOTE: You cannot import a key pair that has the same *Diplomat Key Name* as an existing public key.

If you choose to overwrite the existing key, you cannot recover the original key at a later time. As a precaution, Diplomat MFT attempts to export a copy of the original key before it is overwritten.

The ***Imported Key Passphrase*** field is required for key pairs. An ***Overwrite*** checkbox is only displayed for keys with a *Diplomat Key Name* that already exists in Diplomat. The ***Existing Key Passphrase*** field is only displayed for key pairs. OpenPGP uses a passphrase to encrypt each key pair. If you plan to overwrite an existing key in the Diplomat MFT database, you must enter the passphrase for the existing key.

6.2.1.1.4 Export Key Pair

Key pairs can be exported from Diplomat for secure backup or for use with other OpenPGP-compliant products. To export a key pair, select the key pair you plan to export from the navigation tree. Then go to **Keys** > **OpenPGP Key Pairs** > **Export Key Pair** from the top menu bar. Set the desired file name and browse to the location where you would like to save the file. You will be required to provide the previously defined passphrase is required to export the key pair.

6.2.1.1.5 Delete

Key pairs can be deleted from the Diplomat MFT database. To delete a key, select the key you plan to delete from the navigation tree. Then, select **Keys** > **OpenPGP Key Pairs** > **Delete** from the top menu bar or right-click and select **Delete**. You will be required to provide the passphrase before deletion will be completed.

If you have forgotten the passphrase and need to delete a key pair, accounts with *Administrator* privileges can force the deletion without a valid passphrase.

If a Partner profile or Transaction in Diplomat MFT references the key you are attempting to delete, Diplomat MFT does not immediately delete the key and you receive a message warning that all Partners and/or Transactions referencing that key will also be deleted.

> It is ***STRONGLY RECOMMENDED*** that you cancel that operation and manually remove references to the key before proceeding with the key deletion.
>
> ***ONLY*** proceed if you are certain that the key and all the related Partners and Transactions are no longer needed. For example, you might choose to delete a key and all its related Partners and Transactions if you are no longer doing business with the trading partner from which you received the key.

NOTE: A key specified in a Partner profile may or may not be used when the Partner profile is selected for a transaction. If you delete a key that is specified in a Partner profile, any transaction using that Partner profile will be deleted – even if the key is not used explicitly in the transaction.

If a key pair is deleted by another user while you are adding a sub-key, you can recover the key by selecting **Keys** > **OpenPGP Key Pairs** > **Recover** from the top menu bar.

6.2.1.1.6 Recover

Key pairs can be recovered if they were deleted within Diplomat. To recover a key, select **Keys** > **OpenPGP Key Pairs** > **Recover** from the top menu bar. You will be required to provide the passphrase.

Check *Recover* beside each key that you would like to recover. The *Key Type* Indicates whether the key available for recovery is a public key or a key pair. The *Key ID* uniquely identifies a key. The *User ID(s)* help identify the owner of the key. Two key pairs may have the same User ID, but they must have different *Key IDs*. *Diplomat Key Names* are labels used only by Diplomat. All key pairs and public keys must have unique *Diplomat Key Names*.

If you attempt to recover a key with a *Diplomat Key Name* that already exists in the Diplomat MFT database, you have the option to overwrite the existing key or to modify the *Diplomat Key Name* field. The *Recovered Key Passphrase* field is required. An *Overwrite* checkbox is displayed for keys with a *Diplomat Key Name* that already exists in the Diplomat MFT database. If you decide not to overwrite the existing key, simply uncheck the *Overwrite* checkbox before selecting *OK*.

The ***Existing Key Passphrase*** field is only displayed for key pairs. OpenPGP uses a passphrase to encrypt each key pair. If you plan to overwrite an existing key in the Diplomat MFT database, you must enter the passphrase for the existing key.

6.2.1.1.7 Search/Move

OpenPGP Key Search/Move is used to help locate OpenPGP keys containing specific phrases and keys that are not referenced by any Partner profile or transaction.

To select a key for editing, highlight the *Key ID* in the list and select OK. To move a key, highlight the Key ID and drag it to the target folder in the navigation tree. ***Search Criteria*** are used to find keys where the search field contains a specific phrase or keys that are not referenced by any Partner or transaction. The *phrase* field is case sensitive. Leaving the 'containing phrase' field blank displays an unfiltered list of objects. The ***Search*** button is used to initiate the search using the criteria in the *Search Criteria* panel and displays the number of keys found.

Search Results displays all the keys that match the search criteria. A status indicator is displayed to the left of each Key ID which indicates scheduling status of each key by displaying:

- Green status indicator for keys that are available for use in scheduled jobs,
- Yellow status indicator for keys that have been suspended directly, and
- Orange status indicator for keys that have been suspended indirectly.

Use the ***Export*** button to export search results to a .csv file.

6.2.1.2 OpenPGP Public Keys

6.2.1.2.1 Import Public Keys

Public keys and key rings created by other OpenPGP-compliant products can be imported into the Diplomat MFT database. Go to **Keys** > **OpenPGP Public Keys** > **Import Public Keys** from the top menu bar, and browse to the location of the public key or key ring to be imported.

Check ***Import*** beside each key in the key ring that you would like to import. A public key always has the same *Key ID* as the key pair from which it was created. Two key pairs or two public keys may have the same *User ID*, but they must have different *Key ID*s.

NOTE: If a public key to be imported has the same *Key ID* as a public key in the Diplomat MFT database, the key cannot be imported. The *Import* checkbox and *Diplomat Key Name* field will be disabled. The rollover message and the help message provide a reminder that the *Key ID* already exists in the Diplomat MFT transaction database.

Two key pairs may have the same *User ID*, but they must have different *Key IDs*. *Diplomat Key Names* are labels used only by Diplomat. All key pairs and public keys must have unique *Key Names* in Diplomat. The default value shown in the *Diplomat Key Name* field is the *User ID* from the OpenPGP key. *Diplomat Key Names* field length is limited to 64 characters.

If you attempt to import a public key with a *Diplomat Key Name* that already exists in the Diplomat MFT database, you have the option to overwrite the existing public key or to modify the *Diplomat Key Name* field. If you choose to overwrite the existing public key from the screen below, the *Overwrite Checkbox* is checked automatically.

NOTE: You cannot import a public key that has the same *Diplomat Key Name* as an existing key pair.

If you choose to overwrite the existing key, you cannot recover the original key later. As a precaution, Diplomat MFT attempts to export a copy of the original key before it is overwritten. An ***Overwrite*** checkbox is displayed only for keys with a *Diplomat Key Name* that already exists in Diplomat.

6.2.1.2.2 Export Public Key

OpenPGP public keys can be exported from Diplomat MFT for use with other OpenPGP-compliant products. To export a public key, select the key you plan to export on the navigation tree. You can export a public key directly or the public key portion of a key pair. Then go to **Keys** > **OpenPGP Public Keys** > **Export Public Key** from the top menu bar. Enter the desired filename and browse to the path to export the public key file.

6.2.1.2.3 Delete

To delete a key, select the key you plan to delete from the navigation tree and go to **Keys** > **OpenPGP Public Keys** > **Delete** from the top menu bar, or simply right-click it and select ***Delete***.

If a Partner profile or transaction in Diplomat MFT references the key you are attempting to delete, Diplomat MFT does not immediately delete the key and you receive a message warning that all Partners and/or Transactions referencing that key will also be deleted.

> It is ***STRONGLY RECOMMENDED*** that you cancel that operation and manually remove references to the key before proceeding with the key deletion.
>
> ***ONLY*** proceed if you are certain that the key and all the related Partners and Transactions are no longer needed. For example, you might choose to delete a key and all its related Partners and Transactions if you are no longer doing business with the trading partner from which you received the key.

NOTE: A key specified in a Partner profile may or may not be used when the Partner profile is selected for a transaction. If you delete a key that is specified in a Partner profile, any transaction using that Partner profile will be deleted – even if the key is not used explicitly in the transaction.

6.2.1.2.4 Recover

Public keys can be recovered, if they were deleted within Diplomat. To recover a public key, select **Keys** > **OpenPGP Public Keys** > **Recover** from the top menu bar. Check *Recover* beside each key that you would like to recover.

If a key to be recovered has the same *Key ID* as a key in the Diplomat MFT database, the key cannot be recovered. The *Recover* checkbox and *Diplomat Key Name* field will be disabled. An *Overwrite* checkbox is displayed for keys with a *Diplomat Key Name* that already exists in the Diplomat MFT database.

6.2.1.2.5 Search/Move

OpenPGP Key Search/Move is used to help locate OpenPGP keys containing specific phrases and keys that are not referenced by any Partner profile or transaction.

To select a key for editing, highlight the *Key ID* in the list and select OK. To move a key, highlight the Key ID and drag it to the target folder in the navigation tree. ***Search Criteria*** are used to find keys where the search field contains a specific phrase or keys that are not referenced by any Partner or transaction. The *phrase* field is case sensitive. Leaving the 'containing phrase' field blank displays an unfiltered list of objects. The ***Search*** button is used to initiate the search using the criteria in the *Search Criteria* panel and displays the number of keys found.

Search Results displays all the keys that match the search criteria. A status indicator is displayed to the left of each Key ID which indicates scheduling status of each key by displaying:

- Green status indicator for keys that are available for use in scheduled jobs,
- Yellow status indicator for keys that have been suspended directly, and
- Orange status indicator for keys that have been suspended indirectly.

Use the ***Export*** button to export search results to a .csv file.

6.2.2 OpenPGP Key Window

OpenPGP Key information about the selected key is displayed to the right of the tree view. None of the fields are editable. Public keys appear the same as key pairs.

In the ***Key Identification*** panel, the *Key Name* is a lable displayed any time you select a key for use in a Transaction or Partner. That *Key Name* is used only by Diplomat and is not exported if you export the key from Diplomat. The *User ID(s)* is a part of the key added by owner of the key to help identify it. You can also select whether to *Include in expiration email notifications*.

In the ***Master Key*** and ***Subkey(s)*** panels, the title of each Master or Sub-Key panel in the Key window indicates the functions that the key can perform (i.e., Sign or Encrypt/Sign). Each Master Key and Sub-Key displays the ***Algorithm***, ***Bit Strength***, the date the key was ***Created*** or the sub-key ***Starts*** to be valid, the date the key ***Expires***, the ***Key Fingerprint***, the ***Version*** of IETF OpenPGP specification to which the key conforms, and both the ***Symmetric*** and ***Hashing Algorithms*** that the private key of a key pair can use to decrypt a file encrypted using the matching public key.

The ***Related Partners and Transactions*** panel displays the status of each Partner and transaction using that key. To access a related Partner or transaction, click on the Partner Name or the Transaction Name in the table.

For Partners, the status symbols are as follows:

- Suspended indirectly '■'
- Actively being scheduled '■'

For transactions, the status symbols are as follows:

- Not scheduled '■'
- Allow external requests '■'
- File monitoring '■'
- Suspended indirectly '■'
- Suspended directly '■'
- Actively being scheduled '■'

NOTE: It is recommended that you suspend all transactions related to a key before you make any changes to it, like adding sub-keys. You can suspend all transactions using a key by highlighting the key in the navigation tree and selecting **Jobs** > **Suspend Active Key** from the top menu bar or right clicking on the key in the navigation tree and selecting the suspend option. Suspended transactions are displayed with a yellow or orange status indicator in the related transactions panel. To restart jobs once you are satisfied with the changes in the key, select Jobs > Release Active Key from the top menu bar or right click on the key in the navigation tree and select the release option.

6.3 SSH Keys

SSH keys are a public key encryption technology. SSH Key Pairs can assist in authenticating the user attempting to access an SFTP server. SSH host keys are used to validate the SFTP server, which ensures that the file transfer job is connected to the correct SFTP server.

SSH client or host keys are **not required** when connecting to an SFTP server. Contact the SFTP server administrator if you are unsure whether an SFTP client key is required for a connection. Verification of SSH host keys is always an optional step when connecting to an SFTP server.

6.3.1 SSH Key Menu Items

In Diplomat Managed File Transfer, each SSH key has a unique key name. This name is displayed when you select a key to be used in a Partner profile window or in the Partner profile panels in a transaction window. These names should be readily understandable. For example, you might name the SSH key for Acme Foods – 'Acme Foods SSH Key'.

Diplomat MFT SSH key management allows you to:

- Create SSH Key Pairs.
- Import existing SSH Key Pairs created by other SSH-compliant products. See *Appendix A: Configuration Requirement* for a list of compatible SSH-compliant products.
- Manually adding SSH host keys to the Diplomat MFT database.
- Export SSH client public keys.
- Delete SSH client or host keys.
- Recover, search for, or move SSH Key Pairs.

NOTE: All key menu items related to SSH Key Pairs require the entry of the secret passphrase for that key pair.

6.3.1.1 SSH Key Pairs

To use SSH Key Pairs, you must:

- Create an SSH Key Pair by selecting **Keys** > **SSH Key Pairs** > **Create Key Pair** from the top menu bar.
- Export the public key from the newly-created SSH Key Pair into a file by selecting **Keys** > **SSH Key Pairs** > **Export Public Key** from the top menu bar.
- Send the public key file to the SFTP server administrator.
- Once the server administrator attaches the public key to the account you use to access the SFTP server, you can use the SSH Key Pair to log into the SFTP server by selecting the correct SSH Key Pair on the SFTP panel in the Source or Destination Partner Profile when setting up transactions.

During a file transfer to an SFTP server, the SSH Key Pair is used **ONLY** to authenticate your login. A different key pair generated at run-time by the SFTP server is used to encrypt/decrypt the file being transmitted.

When you attempt to log into an SFTP server using an account that requires an SSH Key Pair, the SFTP server automatically uses the public key associated with your account to authenticate your login request. The SFTP server encrypts a random number using the public key associated with your account and sends it to Diplomat. Diplomat MFT uses the private SSH Key Pair specified in the transaction to decrypt the number and send it back to the SFTP server. If the SFTP server recognizes the number, it establishes a connection with Diplomat MFT to transfer the file. If the SFTP server does not recognize the number, it refuses the connection.

6.3.1.1.1 Create Key Pair

SSH key pairs must have a unique ***Key Name*** in Diplomat. *Key Names* are used only by Diplomat. You should choose a name that makes it easy for you to determine the intended use of the key when setting up transactions. *Key Name* field length is limited to 64 characters.

Select the ***Key Type***. Diplomat MFT supports two SSH Key Pair types: DH/DSS and RSA.

Bit Strength of a key is related to how difficult the algorithm is to break. The larger the bit strength of the key, the more difficult and time-consuming the code-breaking task would be. The larger the bit strength of the key, the longer it takes to generate the key. Keys sizes are generally 1024, 2048, and 4096. DS/DSS keys only support a 1024 key size. RSA keys support 1024, 2048, and 4096 key sizes.

SSH uses a ***Passphrase*** to encrypt your key pair. A passphrase should be difficult for others to guess.

You must provide the passphrase, when you import, create, export, delete, or recover an SSH Key Pair. Once you have created a key pair in Diplomat, the passphrase is stored in a special encrypted format separately from the key pair. When you set up a transaction in Diplomat, for security purposes, you do not need to re-enter the passphrase. If you forget the passphrase, an account with *Administrator* privileges can recover it.

NOTE: If you attempt to create a key with a *Key Name* that already exists in the Diplomat MFT database, you have the option to replace the existing key with the new key. **If you choose to overwrite the existing key, you cannot recover the original SSH key later.** To ensure that you do not permanently delete a key, you can delete the SSH key you want to replace. Then, create a new SSH Key Pair with the same name. The original SSH Key Pair can still be recovered later.

6.3.1.1.2 Import SSH Key Pair

SSH Key Pairs from other SSH-compliant products can be imported into Diplomat. You must export the key pair into an individual file using your SSH-compliant product and then import it into Diplomat.

NOTE: If you attempt to import a key with an *SSH Key Name* that already exists in the Diplomat MFT database, you have the option to replace the existing key with the new key. **If you choose to overwrite the existing key, you cannot recover the original SSH key later.** To ensure that you do not permanently delete a key, you can delete the SSH key you want to replace. Then, create a new SSH key with the same name. The original SSH key can still be recovered later.

Browse for or paste the path of the SSH Key Pair to be imported. Provide a ***Key Name*** that makes it easy to determine the intended use of the key when setting up transactions. Keys must have a unique *Key Name* in Diplomat. *Key Names* are labels used only by Diplomat. *Key Name* field length is limited to 64 characters. You must also provide the passphrase.

6.3.1.1.3 Export SSH Public Key

The public half of an SSH Key Pair can be exported from Diplomat MFT for use with other SSH-compliant products. To export a public key, select the key you would like to export on the navigation tree. Then, go to **Keys** > **SSH Key Pairs** > **Export Public Key** from the top menu bar.

Provide the desired file name with a *.pub* extension and browse to the desired output location.

6.3.1.1.4 Export SSH Private Key

The private half of an SSH Key Pair can be exported from Diplomat MFT for use with other SSH-compliant products. To export a private key, select the key you would like to export on the navigation tree. Then, go to **Keys** > **SSH Key Pairs** > **Export Secret Key** from the top menu bar.

Provide the desired file name, browse to the desired output location, and provide the passphrase.

Private Keys are exported in the OpenSSL PEM format, without password protection.

6.3.1.1.5 Delete

SSH Key Pairs can be deleted from the Diplomat MFT database. To delete a key, highlight the key you plan to delete in the navigation tree. Then, go to **Keys** > **SSH Keys** > **Delete** from the top menu bar or right-click the SSH Key Pair in the navigation tree and select **Delete**.

If a Partner or Transaction in references the key you are attempting to delete, Diplomat does not immediately delete the key, and you will receive warning that all Partners and/or Transactions referencing that key will also be deleted.

It is strongly recommended that you ***Cancel*** the operation and manually remove references to the key before proceeding with the key deletion.

6.3.1.1.6 Recover

SSH Key Pair can be recovered if they were deleted within Diplomat. To recover a key, go to **Keys** > **SSH Key Pairs** > **Recover** from the top menu bar.

Check *Recover* beside each key pair that you would like to recover, verify the *Fingerprint* and the *Diplomat Key Name*, and provide the *Passphrase*. If you attempt to recover an SSH Key Pair with a *Key Name* that already exists in the Diplomat, an *Overwrite* checkbox is displayed. If you decide not to overwrite the existing key pair, uncheck the *Overwrite* checkbox before selecting *OK*. You will be required to provide the *Existing Key Passphrase* to overwrite the existing key.

6.3.1.1.7 Search/Move

Search/Move is used to find SSH Key Pairs containing specific phrases and keys that are not referenced by any Partner or Transaction.

Use the ***Search Criteria*** to find keys where the search field contains a specific phrase or keys that are not referenced by any Partner or transaction. The *phrase* field is case sensitive.

Use the *Search* button initiate the search using your criteria and display the number of results. A status indicator is displayed to the left of each Key ID which indicates scheduling status of each key by displaying *Green* when available for use in scheduled jobs, *Yellow* for suspended directly, or *Orange* for suspended indirectly.

You can *Export* search results to a .csv file.

6.3.2 SSH Key Window

Click an SSH Key from the tree view to display information about it.

The *Name* is a label used by Diplomat each time you select a key for use in a Transaction or Partner. The *Algorithm* field indicates which algorithm the key will use for encryption or decryption. Bit Strength is the number of bits representing the key size, while the *Key Fingerprint* is the unique string of numbers and characters used to identify a key. Passphrase that was set during key creation.

The *Related Partners and Transactions* panel displays the status of each Partner and transaction using the key. To access a related Partner or transaction, click on the Partner Name or the Transaction Name in the table.

6.3.3 SSH Host Keys

When you connect to an SFTP server, you may choose to have Diplomat MFT verify the identity of the SFTP server by comparing the fingerprint supplied by the SFTP server with the fingerprints stored in Diplomat. You may add and remove SSH Host Keys as needed.

SFTP server administrators may provide the fingerprint prior to your first connection attempt, in which case you can go to **Keys** > **SSH Host Keys** and choose to **Add** the information provided. Alternatively, you may check the *Verify SSH host key* on the SFTP panel in the Partner or transaction and using the *Test* button. When you use the *Test* button on the Partner profile panel and the correct SSH host key is not in the SSH host key list, you will be prompted to add the SSH host key to the list.

6.4 SSL Certificates

SSL Server Certificates are used to validate the server identity for TLS-enabled protocols when a job runs. While rare, remote server administrators may require that that you have your own ***SSL Client Certificates*** as well. Options and actions are the same for both.

During a file transfer to an affected server, the SSL server certificate is only used to verify the identity of the FTPS server. A different key pair generated at run-time by the FTPS server is used for communications encryption.

6.4.1 SSL Certificate Menu Items

Each SSL certificate in Diplomat has a unique key name, a label displayed when you select a key to be used in a Partner or Transaction. Diplomat enables you to import, delete, and search for SSL certificates.

6.4.1.1 Import SSL Certificate

To import an SSL certificate, browse to the location of the SSL certificate and select it. If you attempt to import an SSL certificate with an *SSL Certificate Name* that already exists in the Diplomat MFT database, you have the option to replace the existing certificate with the new certificate. If you choose to overwrite the existing certificate, you cannot recover the original SSL certificate later.

6.4.1.2 Delete

To delete an SSL certificate, select the certificate you plan to delete from the navigation tree and choose to delete it from the top menu bar or right-click it and select ***Delete***.

If a Partner or Transaction references the key you are attempting to delete, Diplomat does not immediately delete it, and you will receive warning that all Partners and/or Transactions referencing that certificate will also be deleted. It is strongly recommended that you ***Cancel*** the operation and manually remove references to the certificate before proceeding with the deletion.

6.4.1.3 Search/Move

Search/Move is used to find certificates containing specific phrases and keys that are not referenced by any Partner or Transaction.

Use the ***Search Criteria*** to find keys where the search field contains a specific phrase or keys that are not referenced by any Partner or transaction. The *phrase* field is case sensitive.

Use the *Search* button initiate the search using your criteria and display the number of results. A status indicator is displayed to the left of each Key ID which indicates scheduling status of each key by displaying *Green* when available for use in scheduled jobs, *Yellow* for suspended directly, or *Orange* for suspended indirectly.

You can *Export* search results to a .csv file.

6.4.2 SSL Certificate Window

Click a certificate to display information about it.

The *Name* is a label used by Diplomat each time you select a certificate for use in a Transaction or Partner. All certificate details are set at the time the certificate was created.

You can also choose whether to *Include in expiration email notifications* that are sent to enabled **IT Support Email Notifications** recipients.

The *Related Partners and Transactions* panel displays the status of each Partner and transaction using the key. To access a related Partner or transaction, click on the Partner Name or the Transaction Name in the table.

7 Partners

Diplomat MFT Enterprise Edition provides the ability to define a Partner. Each Partner is an endpoint with which Diplomat can exchange files. The *Partner Name* as a unique label for each Partner and must be unique across all public and trusted profiles. Within each Transaction the *Source Partner Profile* and *Destination Partner Profile* may reference either a defined partner or one explicitly defined within that Transaction.

Once a Partner is defined, it may be used across one or many Transactions. Enter the Partner details once and reuse it in all transactions with that trading partner or site. A change to the Partner automatically updates all Transactions using that Partner. Any details can change such as a file server name, a host address, a password, or an OpenPGP key, and that change can be made once in one place to update all Transactions using that Partner.

A Partner under your control, whether on-premises or in the cloud, would be a 'Trusted' profile. A 'Public' profile is used for locations not under your control, such a trading partner's SFTP server. You can create a new Partner for each unique set of details that need to be reflected in a Transaction.

7.1 Partners Navigation Tree

The navigation tree displays the *Partner Name*s of all Partner profiles in the current Diplomat MFT transaction database. Partner profiles are divided into sub-folders for public profiles and trusted profiles. Public profiles are generally used for trading partners that provide you their public keys for encryption and verification. Trusted profiles should be used for profiles that are part of your local network.

Select a sub-folder under Partners in the navigation tree and right-click to create a new Partner, expand/collapse all sub-folders, add a sub-folder, rename the folder, delete the folder, or search the folder.

Select a Partner in the navigation tree and right-click to rename the Partner, delete the Partner, move the Partner to a new folder, release transactions using the Partner for scheduling or suspend transactions using the Partner.

The Partners navigation tree also indicates the suspend status of Partners. Diplomat allows you to immediately suspend a Partner and therefore all transactions associated with that Partner. For example, you may need to suspend transactions for a Partner during a maintenance window for their systems.

When transactions associated with a Partner are suspended, an orange status indicator '■' is displayed next to the Partner in the navigation tree and next to all transactions that have been suspended indirectly due to the suspension of the Partner. When transactions associated with a Partner are actively being scheduled, a green status indicator '■' is displayed next to the Partner profile in the navigation tree.

To suspend a Partner right-click it in the navigation tree and select *Suspend Partner*. Any jobs that are currently queued or running when the Partner is suspended will complete normally. No further jobs using the suspended Partner are run until they have been released.

To release a Partner, right-click it in the navigation tree and select *Release Partner*.

7.2 Partners Menu Items

The Partners menu in the top menu bar allows you to create, delete, or search Partner profiles.

7.2.1 Create Partner Profiles

New public and trusted Partner profiles can be created using the **Partners** menu. You will be prompted to enter a *Partner Name* label, which must be unique across all trusted and public profiles. If you attempt to create a new Partner using a name that already exists in the Diplomat MFT transaction database, you are warned before the existing Partner is overwritten.

You cannot overwrite a trusted Partner profile with the same name as a public profile or vice versa. For example, assume you have a Public Profile with a *Partner Name* of 'Trading partner 1'. You could not create a new Trusted Profile or save an existing Trusted Profile with the *Partner Name* of 'Trading partner 1'.

NOTE: You may not change the *Partner Name* of a Partner profile once it has been created, but you can it to save it under another name, then delete the original.

7.2.2 Clone

To clone a Partner, right-click it in the tree navigation and select *Clone* or via ***Partners*** > ***Clone*** and provide a new *Partner Name*. You must choose a unique name for the new Partner.

7.2.3 Delete

To delete a Partner, right-click it in the tree navigation and select *Delete* or via ***Partners*** > ***Delete***.

Deletion is permanent. The only way to recover a Partner profile is to recreate it manually. You may choose to restore a previously saved backup, but any other changes after the backup was taken will be lost.

If a Transaction references the Partner you are attempting to delete, Diplomat does not immediately delete it, and you will receive warning that all Transactions referencing that certificate will also be deleted. It is strongly recommended that you ***Cancel*** the operation and manually remove references to the Partner before proceeding with the deletion.

7.2.4 Search/Move

Partner Search/Move is used to locate Partner profiles containing specific phrases and Partners that are not referenced by any transactions. Go to ***Partners*** > ***Search/Move*** from the top menu bar or right-click a Partner folder in the tree navigation and select *Search/Move*.

To select a Partner profile for editing, highlight the Partner Name in the public or trusted list and select OK. To move a Partner, highlight the Partner Name and drag it to the target folder in the navigation tree.

The *Search Criteria* are used to find Partners where the search field contains a specific phrase or Partners that are not referenced by any transactions. The *phrase* field is case sensitive.

Use the *Search* button initiate the search using your criteria and display the number of results. A status indicator is displayed to the left of each Key ID which indicates scheduling status of each key by displaying *Green* when available for use in scheduled jobs, *Yellow* for suspended directly, or *Orange* for suspended indirectly.

You can *Export* search results to a .csv file.

7.3 Partners Window

7.3.1 Partner Identification

Click a certificate to display information about it.

The *Name* is a label used by Diplomat each time you select a Partner for use in a Transaction. You may also provide a *Description* to help document relevant information. You must also provide the details required for the Transport Method to be used for the Partner.

7.3.2 Transport Methods

A transport method describes how files are exchanged with that endpoint. See the section on Transport Methods for more information.

7.3.3 OpenPGP Keys

OpenPGP keys assigned to Partner profiles are used for encryption/decryption and signing/verification. Only keys appropriate for the task will be shown. In other words, Trusted Profiles only display key pairs, while Public Profiles display only public keys.

For Public Profiles, the ***Partner's Encrypt/Decrypt Key*** is the OpenPGP public key used to encrypt files sent to the trading partner. You must import the Partner's OpenPGP public key into Diplomat before you can set this parameter. For Trusted Profiles, the encryption key is the OpenPGP key pair used to decrypt files you receive.

For Public Profiles, the ***Partner's Sign/Verify Key*** is the OpenPGP public key used to verify a signed file from the Partner. You must import the Partner's OpenPGP key into your Diplomat MFT database before you can set this parameter. For Trusted Profiles, the signature key is the OpenPGP key pair used to sign files you are sending to a Partner.

7.3.4 Related Transactions

The Related Transactions panel displays the transactions using the Partner profile and their status, which is not scheduled '■', allow external requests '■', using file monitoring '■', suspended indirectly '■', suspended directly '■', or actively being scheduled '■'. To access a related transaction, click on the Transaction Name in the table.

NOTE: It is recommended that you suspend all transactions for a Partner before you make any changes to a Partner profile. You can suspend all transaction for a Partner by highlighting the Partner profile in the navigation tree and selecting Jobs > Suspend Active Partner from the top menu bar. Suspended transactions are displayed with an orange status indicator in the related transactions panel. To restart jobs once you are satisfied with the changes in the Partner profile, select Jobs > Release Active Partner from the top menu bar.

You cannot delete Partner profiles that are actively being used in transactions. If you attempt to delete a Partner profile that is used in related transactions, you will be reminded that the Partner profile is currently in use and all transactions using the profile will be deleted, as well.

7.3.5 Save/Reset Buttons

The **Save** and **Reset** buttons are displayed at the bottom of the active window. These buttons become selectable if changes have been made to any of the data fields, combo boxes, or checkboxes for the Partner profile. The **Save** button saves all changes to the Partner profile. The **Reset** button redisplays the previously saved version of the Partner profile data.

8 Transactions

Transactions are file transfers processes between endpoints, with or without encryption. Transactions are at the core of Diplomat MFT's automation and define all characteristics that govern a particular file transfer, including:

- Source name of the file being transferred and, if different, the destination filename
- Source and destination profiles, including file location, transport method (Amazon S3, Box, Citrix ShareFile, Diplomat Remote Agent, Dropbox, Email, FTP, FTPS (TLS), Google Cloud, HTTP, HTTPS, Local Network, Microsoft Azure, Oracle Cloud, SFTP (SSH2) or SMB), and associated login information
- OpenPGP keys to encrypt/decrypt and sign/verify
- File handling characteristics
- Job scheduling information, including use of file monitoring and external job execution requests
- Email notifications
- Transaction-specific additional archive location for storing copies of files
- Pre- and post-job command line execution for integration with other jobs streams
- Advanced troubleshooting

The transaction window contains all information needed to encrypt, sign, and send a file for outbound transactions or pick-up, decrypt, and verify a file for inbound transactions. You may create multiple transactions each encrypting and moving a single file or you may create one transaction to encrypt and move a group of files. Information entered in a transaction window is specific to an individual transaction and has no effect on any other transaction.

The Diplomat MFT transaction database is a SQL database that contains Partner, transaction, key, configuration, and job suspension data. You can back up or restore these files as a group by selecting File > Backup or File > Restore**.**

8.1 Inbound, Outbound, and Synchronization Transactions

Transactions are the heart of Diplomat MFT automation. A Transaction is the defined process by which files come from somewhere and are sent to somewhere, with or without encryption and additional actions and options.

Inbound and Outbound Transactions are similar except in the way you configure OpenPGP actions and the Pre- and Post-Job Processing and the effects on Archiving. Typically, Inbound Transactions are for processes where your company is retrieving files from a trading partner while Outbound Transactions are for processes where your company is sending files to a trading partner. Many real-world Transactions move or process data internally and even locally to the Diplomat server itself, of course, and whichever version makes more sense at the time may be used as needed.

Synchronization Transactions are for distributing or replicating data sources to or from endpoints. This will make the destination folder look exactly like the source folder, so that you can keep one or more destination folders in synch with the source folder. This is useful for scenarios such as distributed web servers – you have the primary copy of web content that is approved and published in one location, and you use a Synchronization transaction to keep other web servers in that web farm, or in collocated web farms across the globe, in sync with that primary web server. This includes removing content from destination locations that are not on the approved source server.

Synchronization configuration is somewhat different from the traditional Inbound or Outbound types. You must still define the Source and one or more Destinations along with desired notifications, pre- and post-job processing, archiving, linked transactions, and so on. Some functions such as OpenPGP encryption do not apply to the Synchronization concept, while others such as whether to *Remove destination items not present at source* apply only to Synchronization. Note that the Primary Archive is skipped by default for Synchronizations.

8.2 Transactions Navigation Tree

The navigation tree shows the *Transaction Name*s of all transactions currently in the Diplomat MFT transaction database. The transactions are divided into sub-folders for Inbound, Outbound, and Synchronization Transactions.

Select a sub-folder under Transactions in the navigation tree and right-click to create a new transaction in the folder, release all transactions (not otherwise suspended) in the folder for scheduling, suspend all transactions in the folder, add a sub-folder, collapse/expand all sub-folders, rename the folder, delete the folder and/or search/move the sub-folder to a new location.

Select a transaction in the navigation tree and right-click to save changes to the transaction, save the transaction with a new name, reset the settings in the transaction to the saved values, validate the transaction values, view log entries from the most recent job run, run a transfer job from the transaction, rename the transaction, delete the transaction, move the transaction to a new folder, release the transaction for scheduling or suspend the transaction.

Each transaction in the navigation tree displays a status indicator:

- Red for transactions that are disabled
- Green for transactions that use a Schedule and are active
- Light green status indicator for transactions that use File Monitoring
- Dark green for transactions that run *only* via external request or linking

- Yellow for transactions that have been suspended directly
- Orange for transactions that have been suspended indirectly

To suspend all transactions, all inbound, or all outbound transactions, right-click the transaction folder, the inbound transaction folder, or the outbound transaction folder in the navigation tree and select the *Suspend* option. For example, you may need to suspend all inbound transactions if your FTP server has been compromised.

Any jobs that are currently queued or running when the folder is suspended will complete normally. No further jobs in the suspended folder are scheduled until they have been released. To release all transactions, all inbound, or all outbound transactions for scheduling, right-click the transaction folder, the inbound transaction folder, or the outbound transaction folder in navigation tree and select *Release*.

When you restore a Diplomat MFT transaction database, all jobs are suspended during the restore operation. If you do not choose to release the suspended jobs when prompted at the end of the restore operation, all jobs remain suspended. A purple status indicator '■' is displayed next to the transaction folder in the navigation tree and an orange status indicator '■' is displayed next to all transactions in the tree.

To release job suspensions due to a Diplomat MFT transaction database merge or restore, select Jobs > Release > Release DB Restore/Suspend or right-click on the transactions folder and select *Release DB Restore/Suspend*.

When a critical audit trail error occurs, all jobs are suspended and a pink status indicator '■' is displayed next to the transaction folder. In addition, an orange status indicator '■' is displayed next to all transactions.

To release job suspensions due to a critical audit trail failure, select Jobs > Release > Release Critical Audit Suspend or right-click on the transactions folder and select *Release Critical Audit Suspend*.

NOTE: All transactions that are currently set to *Do Not Run* continue to display a red status indicator '■' at all times.

8.3 Transactions Menu Items

The drop-down menu from Transactions on the top menu bar allows you to create, save, delete, or search transactions.

8.3.1 Create

New transactions may be created using the drop-down menu from the Transaction button on the top menu bar. Newly created transactions are set automatically to *Do Not Run*.

You will be prompted to enter a *Transaction Name* or *Synchronization Name* which must be unique across all inbound and outbound transactions and may not contain any of the following characters: * ? / \ | " : < >.

NOTE: If you attempt to create a new transaction using a name that already exists in the Diplomat MFT transaction database, you will be warned before the existing transaction is overwritten.

NOTE: You cannot overwrite a transaction with the same name as a different type of transaction. For example, assume you have a Diplomat MFT database containing an inbound transaction with a *Transaction Name* of 'Transaction 1'. You could not create a new outbound transaction or save an existing outbound transaction with the *Transaction Name* of 'Transaction 1'.

8.3.2 Save

A transaction can be saved by clicking the SAVE button at the top of the transaction or by using the Transactions item on the top menu bar. If you have not already saved the transaction, you are prompted to save it upon signing out or moving to another item in the tree navigation.

8.3.3 Clone

Clone a transaction to create a new copy with a new name. If you attempt to use a name that already exists, you will be warned before the existing transaction is overwritten. A cloned Transaction is set to *Do Not Run*.

8.3.4 Reset

Undoes any changes since the last save.

8.3.5 Delete

Transaction deletions are permanent. The only way to recover a transaction is to restore a previously saved backup of the entire Diplomat MFT configuration. Any changes since the backup was saved are lost.

8.3.6 Search/Move

You can find specific transactions for viewing, editing, or moving. Use the ***Search Criteria*** to find transactions where the search field contains a specific phrase, that have not processed files for a specified number of days, or that have no records in the job history database. The *phrase* field is case sensitive.

Use the ***Search*** button to initiate the search using the *Search Criteria* display the number of results. The ***Search Results*** displays all the inbound and outbound transactions that match the search criteria. A status indicator is displayed to the left of each Transaction Name which indicates status of each transaction. Use the ***Export*** button to export search results to a .csv file.

To select a transaction for editing, double-click on the Transaction Name in the inbound or outbound list. To move a transaction, highlight the Transaction Name and drag it to the target folder in the navigation tree.

8.4 Transactions Window

The transaction window is separated into panels covering the types of information necessary to fully-specify a transaction, including transaction identification, file, source and destination, keys, job schedule, email notifications, and archive information.

Some of the panels can be maximized and minimized using the chevrons located in near the top-right corner of each panel.

The ***Validate***, ***Save***, and ***Reset*** buttons are displayed at the top of the active window. These buttons become selectable if changes have been made to any of the data fields, combo boxes, or checkboxes for the transaction. The **Validate** button tests the data displayed in the transaction window to ensure a valid transaction. If data is missing or invalid, a pop-up dialog describes the error. The **Save** button saves all changes to the transaction, and CTRL+S may be used in some browsers on some operating systems. The **Reset** button redisplays the previously-saved version of the transaction data.

In ***Transaction Identification***, the ***Transaction Name*** is the label used by Diplomat to identify the Transaction and must be unique. A *Transaction Name* may not contain any of the following characters: * ? / \ | " : < >. *Transaction*

Name field length is limited to 110 characters. The ***Description*** provides an opportunity to document relevant details and an overview to help recognize the transaction.

8.4.1 File Information

At run time, the fields in the *File Information* panel determine which files are to be processed and what actions are to be taken with the file(s) during or after transfer. Potential source files are filtered from all files in the source directory based on whether:

- Filenames match a naming template that allows wildcards for up to one (?) or multiple (*) characters in the ***Source File(s)*** fields.
- Filenames may be configured to contain dates and sequence numbers matching the date and sequence number parameters in the *Source File(s)* and the ***Source Date Format*** fields.
- Dates in the source filenames fall within the ***Source Date Range***.
- ***Use Modified Date*** falls within the ***Modified Date Range***.
- Advanced file name matchings options are configured using the icon button to the right of the Source File(s) input field. Any option which has been selected will show the respective icon in blue, otherwise gray means that option is not selected. The options are:
    - Case Sensitive – setting this on will cause the ***Source File(s)*** pattern to match file names with an exact case match. Setting this off means matching irrespective of case.
    - Regular Expression – setting this on means that the pattern specified in the ***Source File(s)*** field is a regular expression. Diplomat MFT uses Java 8 regular expression notation.
    - Recursive – setting this on will match the pattern in the source folder and all subfolders
    - Exclude – setting this on means that the pattern specified in ***Source File(s)*** will cause any matched file to be ***excluded*** from the list of matching files. Setting this value off (the default) means that matching files are ***included*** in the list of matching files.

If source files are found that match **all** specified criteria, destination filenames are determined for each file in the list of source files based on:

- A blank value for ***Destination File(s)*** field means that no changes are applied to file names matched at source; they will be named identically at destination.
- A naming template that interprets a pipe '|' wildcard in the ***Destination File(s)*** fields as the source filename. The '|' symbol can be placed anywhere in this field and it will be replaced with the original file name matched at the source location.
- Removal of dates from the filename if the ***Remove Source Date*** checkbox has been checked.
- Removal of sequence numbers from the filename if the ***Remove Source Sequence*** checkbox has been checked.
- Addition of dates and sequence numbers in the destination filenames based on date and sequence number parameters in the ***Destination File(s)*** fields. The ***Destination Date Format*** and the ***Destination Date*** fields determine the exact date and the format of the date string to be inserted.

If each source file has a unique destination filename, then processing continues, and a list of source and destination filenames is created. Then, the number of source and destination filename pairs is compared to the number of files specified. If the number found matches the number specified in the ***Number of Files*** box, the files are added to the list of files to be processed for the job.

If the number of source and destination filename pairs found does not match the number of files specified, Diplomat MFT checks to see if the files are required to continue processing. In that case, if the ***Required*** checkbox is **not** checked, then the file pairs are removed from the list to be processed and the job continues. If the *Required* checkbox is checked, then the processing of the job stops due to the wrong number of files being found. If the ***Fail***

If File(s) Not Found option is enabled, then the job is handled as failed. Otherwise, the job is simply scheduled for the next run.

Once the list of source and destination filename pairs has been validated, additional options and fields affect the processing of files. If the ***Ignore File Handling*** checkbox is checked, the associated source files are written to the destination with no actions taken as configured in the File Handling panel. If the ***Overwrite*** settings allow it, a file is written to the destination even if a file of the same name already exists there. If the ***Allow Zero Byte Files*** checkbox is checked, source files that have zero bytes on outbound jobs and destination files that have zero bytes on inbound jobs will continue to be processed. If the ***Fail if File(s) Not Found*** option is enabled, jobs that find an insufficient number of files to be processed (generally none) after the configured number of attempts will generate a Failure status, and configured notifications, alerts, and other related actions are taken.

The **Transfer Order** option controls the order of files as they are transferred from source to destination, as follows:

- Default order is order provided by the directory listing of the source location. This is typically in alphabetical order, but not necessarily always so.
- Alphabetical (A-Z) will sort the list of matched files alphabetically, and transfer in that order.
- Alphabetical (Z-A) will sort the list of matched files in reverse alphabetical order, and transfer in that order.
- Oldest first will sort the list of matched files by modified date in ascending order, and transfer in that order.
- Newest first will sort the list of matched files by modified date in descending order, and transfer in that order.

The ***Post-Transfer Action*** option determines what happens to files at the source location after they are processed and delivered successfully to the destination. The selected option will be applied to each file that is successfully transferred from source to destination, but not to any files that fail to transfer.

- ***Nothing*** means that source files are left alone after successful transfer.
- ***Delete*** causes Diplomat MFT attempts to delete the source file.
- ***Move*** will attempt to move (rename) the file into a subfolder of that source location. When selected, you can specify where to move files that are successfully transferred, and a different location for those files that experience error during transfer. If the "On Error" path is left blank, files that fail during transfer are not moved, leaving them in the original location to potentially be processed later.

  The values for the On Success and On Error location supports date/time parameters ("<YYYY>," "<MM>", and so on)., which will be replaced by the values derived from the job execution time.

If the ***Translate Invalid Windows Characters*** is checked, then source files names that contain characters which are invalid for the Windows file system, but may be valid in other operating systems (':', '*', '?', '"', '<', '>', '|') will be converted to a dash ('-') character when transferred.

8.4.1.1 Source File(s)

The *Source File(s)* fields contain the name(s) of file(s) to be picked up. Source files are processed in the order in which they are identified using the *Source File(s)* specification.

If multiple source files are found and any of the files fail to properly complete the transaction, FAILURE notifications are generated. The filename(s) of the specific file(s) that fail are listed in the notifications.

Fail if File(s) Not Found

Check *Fail if File Not Found*, if you expect one or more valid files to be found every time a job for this transaction is executed. Valid files conform to all the settings in the File Information panel, such as having a particular name, containing a date with a specified format, and finding the number of files specified.

If *Fail if File Not Found* is checked, all email addresses requesting notification for any 'Failure' or 'All Jobs' receive email each time a job runs and does not find a valid file. When *Fail if File Not Found* is not checked, jobs that do not find any files to transfer are simply rescheduled, no email or pages are sent, and no record is written to the Audit Trail. 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.

If a job fails unexpectedly due to *File Not Found*, check the log file for the exact listing of filenames in the source directory. Confirm that the file and directory names on the transaction are identical to the names on the source or destination system. All file and directory names are CASE SENSITIVE. If the names do not match exactly, the file will not be found.

Using Multiple Source File(s) Fields

Use the plus (+) and minus (-) icons to the right of the *Source File(s)* field to add or remove additional source file fields (***Enterprise Edition Only***). Enter unique filenames into each *Source File(s)* field. Each *Source File(s)* field may contain wildcards, a date parameter, and/or a sequence number parameter.

Specifying Sub-Directories to Source Filenames

A sub-directory can be prepended to the beginning of the filename using '/' or '\' as a delimiter between the sub-directory name and the filename. Do **not** add a delimiter at the beginning of the sub-directory name. Wildcard characters (* and ?), date parameters, and sequence parameters cannot be used as part of a sub-directory name in a *Source File(s)* field. **NOTE: Sub-directories are case sensitive.**

Using Wildcards in Source File(s) Fields

The asterisk '*', the question mark '?' and double asterisks '**' are the only wildcard characters recognized in *Source File(s)* fields when regular expressions are not used. Wildcards are not supported on HTTP/S due to lack of reliable directory listings nor by remote servers that do not allow directory listing.

To specify multiple files in a *Source File(s)* field, substitute a single '?' to wildcard single characters or an asterisk to wildcard multiple characters in the filename. For example, 'diplomat*.txt' returns all files starting with 'diplomat' that have a '.txt' extension.

Double asterisks indicate that all files and folders will be sent recursively to the destination. When using a double asterisk wildcard, no destination file renaming is enabled other than the default .pgp and .asc during file encryption, decryption, signing or verification. This automatic file renaming cannot be overridden.

Using Variables in Source File(s) Fields

Variables are specified in *Source File(s)* field as <%variable_name%>. Variables are case sensitive and can only be passed to a Diplomat MFT job using the "–vars" parameter in a Diplomat MFT Scripting Agent command or the "var" parameter in an API *RunNow Job* request.

Variables can be used in both the sub-directory and filename portion of the *Source File(s)* field. If any variables specified in a *Source File(s)* field are not defined in a Scripting Agent command or API request, then the Diplomat job fails.

Using Date and Sequence Number Parameters in Source File(s) Fields

Each *Source File(s)* field may contain one date parameter, which represents a date in the filename, and one sequence number parameter, which represents a numeric sequence in the filename.

In *Source File(s)* fields, the only valid date parameter is the string '<DATE>' and the only valid sequence number parameter is the string '<SEQ>'.

If a sequence number parameter is used as part of the filename, the wildcard character cannot be adjacent to the sequence number parameter. For example, '*abc<SEQ>.*' is a valid filename, but 'abc*<SEQ>.*' is not.

For the wildcard character '*', the wildcard string can be zero to 'n' digits long. For the wildcard character '?', the wildcard string can be zero to 1 digit long. For example, if 'abc*<DATE>.txt' or 'abc?<DATE>.txt' with a date format of '<MM><DD><YYYY>' was specified and two files named 'abcX01302007.txt' and 'abc01302007.txt' were in the target source directory, both files would be selected.

NOTE: HTTP/S transports do NOT support Sequence Number parameters. The Date parameter is supported ONLY when the result is a finite list of filenames (e.g., Source Date Range is set to "Today" or "Within Last Week) and does NOT CONTAIN time intervals less than a day. For example, the date format "<MM><DD><YY><hh><mm>" would not be supported.

Source Date Format

When a *Source File(s)* field contains a date parameter, the *Source Date Format* field which specifies the Date Variables for date parameter is enabled. If no date parameter is specified in any *Source File(s)* field, then the *Source Date Format* field is disabled. A <DATE> can be any combination of the Source Date Elements listed below. If a date parameter is specified and no source files are found that match the *Source Date Format* field, then the job continues as if no files were found.

Source Date Range

Specifies the range of valid values for the date parameter(s) in the *Source File(s)* fields.

NOTE: Unless the *Source Date Format* field contains a fully-specified date format such that a day, month, and year can be determined, the *Source Date Range* field is disabled. A fully-specified date format can contain any combination of day (DD), month (MM, MMM, Mmm, mmm, MMMM, Mmmm, or mmmm), and year (YY or YYYY) elements or a combination of a Julian day (JJJ) and a year (YY, YYYY) element.

The value of the date parameter in a source filename must be within the *Source Date Range* for the source file to be selected. For example, for a *Source File(s)* of '<DATE>*.txt', a job that runs at 11:00 AM on Tuesday, June 26, 2022, that has a source date range equal to 'Yesterday' and date format '<YYYY><MM><DD><hh><mm>' would pick up a file named '202206250800abc.txt' because that file matches a date (and time in this case) for yesterday.

NOTE: *Source Date Range* values starting with 'Within…' that include hours or minutes will **not** find files with dates that match the first day of the period and are earlier in the day than the runtime of the current job. For example, a job that runs at 11:00 a.m. on Tuesday, June 26, 2007, that has a source date range equal to 'With last week' and date format '<MM><DD><YYYY><hh><mm>' would **not** pick up a file named 'abc061920070800.txt', because the date in the filename occurred before 11:00 a.m. on the prior Tuesday, June 19, 2007 (i.e., not within the last week).

Advanced Source File Options

Advanced file name matchings options are configured using the icon button to the right of the Source File(s) input field. Any option which has been selected will show the respective icon in blue, otherwise gray means that option is not selected. The options are:

- Case Sensitive – setting this on will cause the ***Source File(s)*** pattern to match file names with an exact case match. Setting this off means matching irrespective of case.
- Regular Expression – setting this on means that the pattern specified in the ***Source File(s)*** field is a regular expression. Diplomat MFT uses Java 8 regular expression notation.
- Recursive – setting this on will match the pattern in the source folder and all subfolders
- Exclude – setting this on means that the pattern specified in ***Source File(s)*** will cause any matched file to be ***excluded*** from the list of matching files. Setting this value off (the default) means that matching files are ***included*** in the list of matching files.

8.4.1.2 Destination File(s)

Each *Destination File(s)* field is always associated with a matching *Source File(s)* field and determines the name(s) of file(s) as they are to be written to the location specified in the *Destination Partner Profile* panel. Enter data in this field only if you want the destination filename(s) to be different than the original source filename(s).

NOTE: After constructing destination filenames, if any 2 or more are identical INCLUDING capitalization, the file transfer job will fail.

Specifying Sub-Directories for Destination Filenames

A sub-directory can be prepended to the beginning of the filename using '/' or '\' as a delimiter between the sub-directory name and the filename. Do **not** add a delimiter at the beginning of the sub-directory name. If no characters follow the sub-directory name and '/' or '\', the destination file(s) will be written to the specified sub-directory with default names as described below. **NOTE: Sub-directories are case sensitive.**

NOTE: Any sub-directory name entered as part of the source filename is ignored in the default for the destination filename.

NOTE: Any sub-directory name entered as part of the destination filename may contain a <DATE> parameter. A <DATE> parameter in a sub-directory name has the same Destination Date and Destination Date Format as in a filename.

Default Destination Filenames

For inbound transactions, if a destination filename is not specified, the filename defaults to the original filename with the .pgp, .gpg, or .asc extension, if any, removed. For outbound transactions, file extensions are added depending on whether a file is encrypted, signed, and/or ASCII-armored.

Using Wildcards in Destination File(s) Fields

The pipe '|' character is the only wildcard recognized in *Destination File(s)* fields. The pipe '|' character indicates the original source filename when the destination filename is constructed. Additional characters may precede or be appended to the original source filename.

NOTE: When using a '|', check *Remove Source Date* or *Remove Source Sequence* if you want a source date or sequence number removed from the string represented by the pipe.

NOTE: On inbound transactions where a file is being decrypted, verified, and/or having ASCII-armoring removed, the '|' wildcard represents the incoming filename without a .pgp, .gpg, or .asc file extension, if any. If a file with .pgp, .gpg, or .asc extension is treated as transferred with no changes, the file extension is not removed.

NOTE: Only one '|' wildcard can be used in a *Destination File(s)* field.

Using Variables in Destination File(s) Fields

Variables are specified in *Destination File(s)* field as <%variable_name%>. Variables are case sensitive and can only be passed to a Diplomat MFT job using the "–vars" parameter in a Diplomat MFT Scripting Agent command or the "var" parameter in an API *RunNow Job* request.

Variables can be used in both the sub-directory and filename portion of the *Destination File(s)* field. If any variables specified in a *Destination File(s)* field are not defined in a Scripting Agent command or API request, then the Diplomat job fails.

Using Parameters in Destination File(s) Fields

Destination File(s) fields may each contain one <###>, <DATE>, <FILENAME>, <EXT> and, if specified in the *Source File(s)* field, one sequence number parameter.

Copy Number Parameter
Each *Destination File(s)* field may contain one copy number parameter. The copy number is determined at run time by looking for a file at the destination with the highest copy number. The next highest number is used at the destination file name.

If only one digit is specified, <#>, then it is replaced with the next highest value regardless of number of digits.

If more than one digit is specified, e.g. <###>, then it is replaced with the next highest value with zero padding used to have the specified number of digits, if necessary. If the next highest value has more than the specified number of digits it is used and a miscellaneous error is generated.

NOTE: HTTP, HTTPS and email transports do not support the use of the Copy Number parameter.

Date Parameters
Each *Destination File(s)* field may contain one date parameter, which represents a date in the filename. The value of the parameter is determined at run time based on the value of the *Destination Date* field.

The value of the <DATE> parameter in a destination filename or sub-directory is determined by the Destination Date and Destination Date Format fields described below.

NOTE: If the matching *Source File(s)* field does not contain a date parameter, then the *Destination Date* field cannot be set to 'Source Filename Date' as no source date was specified.

Filename and Extension Parameters
The values of the <FILENAME> and <EXT> parameters in a destination filename are determined by the source filename parsed as '<FILENAME>.<EXT>'. On inbound transfers with encrypted files (i.e., .pgp or .asc file extensions), the .pgp or .asc is ignored. For files named xxx.pgp or xxx.asc, <EXT> is set to 'null'.

Sequence Number Parameters
When the matching *Source File(s)* field contains a sequence parameter, the *Destination File(s)* field may contain one sequence number parameter. When a sequence number parameter is used in a *Destination File(s)* field, the sequence number from the source filename is always used, but may be reformatted using the <LLL> or <RRR> sequence number parameter.

Valid sequence number parameters are as follows:

Destination Sequence Number Parameters	
Parameter	**Parameter Description**
<SEQ>	Complete sequence number from the source filename
<LLL>	'n' digits starting at the left of the sequence number in the source filename, where the number of L's represents the number of digits to be inserted into the destination filename
<RRR>	'n' digits starting at the right of the sequence number in the source filename, where the number of R's represents the number of digits to be inserted into the destination filename

NOTE: If the sequence number in the source filename has less than 'n' digits and either <LLL> or <RRR> are used in the destination filename, then the sequence number in the destination filename is padded on the left with zeroes to make it 'n' digits long. For example, when a source file has a 3-digit sequence number of '104' and a destination

filename with a <LLLLLL> sequence number parameter that expects a 6-digit number, the sequence number inserted into the destination filename would be '000104'.

Use Modify Date
Each *Use Modify Date* checkbox is associated with a *Source File(s)* field. When *Use Modify Date* is checked, the modify date on each source file must match the time period specified in the *Modify Date Range* field for a files to be added to the valid file list.

Modify Date Range
Specifies the range of valid values for the modified dates of the source file(s). The Modified Date must be within the *Modify Date Range* for a source file to be selected. If the value is not within the modify date range, the file transfer job continues as if no files were found. Values are as follows: All Dates, Today, Yesterday, Since Last Successful Execution, Within last week, Within last 2 weeks, Within last month, Within last 3 months, Within last year, Oldest and Most Recent.

The "Since Last Successful Execution" means that Diplomat MFT will choose matching files from source that have a *modified date* value that is *newer* than the last time this job was executed successfully. A successful execution for a job is one in which at least one file was transferred to destination and the entire job finished with neither **warning** nor **error**. The job execution information is stored in the **Job History** database, and therefore will be remembered even if you restart the service.
This option is helpful when you cannot delete nor move files out of the source folder, but the files at destination are processed out of the destination folder and, therefore, you cannot rely solely on **overwrite conditions** to prevent transferring the source files again each time the job executes.

NOTE: If both *Source Date Range* and *Modify Date Range* are specified, then both conditions need to be satisfied for the file to be added to the valid file list.

Destination Date Format
When a *Destination File(s)* field contains a date parameter, *Destination Date Format* specifies the Date Variables to be used. If no date parameter is shown in any *Destination File(s)* field, then the *Destination Date Format* field is disabled.

NOTE: If 'Source Filename Date' is selected for *Destination Date* and *Destination Date Format* includes parameters not included in the associated *Source Date Format*, an error will occur as part of the validation process and the transaction cannot be saved. For example, if you have a *Source File(s)* field with 'abc<DATE>.txt' and a *Source Date Format* with '<MM><DD>' and you want to use the date from the source filename in the destination filename, you cannot have a *Destination Date Format* that includes <YYYY>, since no year was specified in the *Source Date Format* field.

NOTE: An explicit date string can be entered into the *Destination Date Format* field. For example, you might use *Run Now* with an explicit date string, if you needed to rerun a job that should have run yesterday and needs one or more filenames to reflect yesterday's date.

Destination Date
When a Destination File(s) field contains a date parameter, Destination Date determines the value of the date to be inserted into the destination filename(s). Values are as follows: Source Filename Date, Source Modified Date, Today, Tomorrow, Yesterday, Last Sunday, Last Monday, Last Tuesday, Last Wednesday, Last Thursday, Last Friday, Last Saturday, End of Last Month, End of Last Quarter, and End of Last Year.

NOTE: You cannot save a transaction with a *Destination Date* of 'Source Filename Date', if the associated *Source File(s)* field does **not** contain a date parameter.

NOTE: When multiple files are allowed by the *Source File(s)* field and the matching *Destination File(s)* field contains a date parameter but no pipe wildcard or sequence parameter, the values of *Destination Date* are limited to 'Source Filename Date' and/or 'Source Modified Date'.

NOTE: Source modified date may not be supported on some FTP servers. If you specify a value of 'Source Modified Date' in the *Destination Date* field and an FTP server does not provide a source modified date, Diplomat MFT will not be able to complete the file transfer and the file transfer job will fail.

Overwrite
Overwrite settings allow you to select the conditions under which you want to allow destination files to be overwritten. Default value is *Do Not Overwrite*.

NOTE: If *Do Not Overwrite* is selected and the destination directory contains a file with the same name as a file being transferred, the file is **not** overwritten, the job generates a warning, and WARNING email and pages are sent. If any other overwrite setting is selected and files are **not** overwritten, the job does **not** generate a warning and SUCCESS email and pages are sent.

Values are:

- Overwrite
- Overwrite if newer
- Overwrite if file size different
- Overwrite if newer or file size different
- Do not overwrite

Remove Source Date
When *Remove Source Date* is checked, the string matching the date parameter in the *Source File(s)* field is removed before creating destination filenames. Unless at least one *Source File(s)* field contains a date parameter and the associated *Destination File(s)* field is blank, contains a pipe '|' character or contains a <FILENAME> parameter, *Remove Source Date* field is disabled.

NOTE: Any sequence number or date values are removed before further file renaming occurs.

If the *Destination File(s)* field is blank and *Remove Source Date* is checked, a *Source File(s)* field of 'abc<DATE>.*' that finds 2 files named 'abc01022007.txt' and 'abc01022007.xls' that are encrypted as part of the file transfer process would become destination files named 'abc.txt.pgp' and 'abc.xls.pgp'.

If the *Destination File(s)* field is 'XYZ.|.pgp' and *Remove Source Date* is checked, the date value is removed from the string represented by the pipe wildcard '|'. In this case, a *Source File(s)* field of 'abc<DATE>.*' that finds 2 files named 'abc01022007.txt' and 'abc01022007.xls' that are encrypted as part of the file transfer process would become destination files named 'XYZ.abc.txt.pgp' and 'XYZ.abc.xls.pgp'.

A source file date can be removed and a new date can be inserted into a destination filename. For example, assume you have 2 source files named 'abc01022007.txt' and 'abc01022007.xls' that were created yesterday and you need destination files with today's date formatted as follows '02-01-07abc.txt' and '02-01-07abc.xls'. You would set up the fields in the File Information sub-panel as shown below:

Remove Source Sequence
When *Remove Source Sequence* is checked, the string matching a <SEQ> parameter in the *Source File(s)* field is removed before creating destination filenames. Unless at least one *Source File(s)* field contains a sequence

number parameter and the associated *Destination File(s)* field is blank, contains a pipe '|' wildcard or contains a <FILENAME> parameter, *Remove Source Sequence* field is disabled.

NOTE: Any sequence number or date values are removed before further file renaming occurs.

If the *Destination File(s)* field is blank and *Remove Source Sequence* is checked, a *Source File(s)* field of 'abc<SEQ>.*' that finds 2 files named 'abc00001.txt' and 'abc00001.xls' that are encrypted as part of the file transfer process would become destination files named 'abc.txt.pgp' and 'abc.xls.pgp'.

If the *Destination File(s)* field is 'XYX.|.pgp' and *Remove Source Sequence* is checked, the sequence number value is removed from the string represented by the pipe wildcard '|'. In this case, a *Source File(s)* field of 'abc<SEQ>.*' that finds 2 files named 'abc00001.txt' and 'abc00001.xls' that are encrypted as part of the file transfer process would become destination files named 'XYZ.abc.txt.pgp' and 'XYZ.abc.xls.pgp'.

Number of File(s)
Each *Number of File(s)* field is associated with a *Source File(s)* and a *Destination File(s)* field. When a wildcard, a date parameter, or a sequence number parameter is used as part of the source filename, the *Number of File(s)* field is enabled. If not, the *Number of File(s)* field is disabled and set to '1'.

If *Number of File(s)* is specified and a Diplomat MFT job does not find exactly the number of files specified, the transaction does not continue. If *Fail if File(s) Not Found* is checked, then the transaction fails. If *Fail if File(s) Not Found* is **not** checked, then the job is simply rescheduled.

You might use this feature if you always expect a single file for a particular transaction, but the incoming file changes names (e.g., a filename that includes a date) on a regular basis. For example, you might receive a weekly payroll file from your bank named 'payroll<DATE>.xls.pgp'. The application that uses this payroll file expects to receive a weekly file named 'payroll.xls'. To set up this transaction, you would enter 'payroll<DATE>.pgp' in the *Source File(s*) field and check *Remove Source Date*. Then, set *Number of File(s)* to '1'. Or, when only one file is expected, you could enter 'payroll*.pgp' in the source filename field and 'payroll.xls' in the destination filename field.

NOTE: When *Number of File(s)* is '1', you can enter a fixed, single filename in the *Destination File(s)* field in addition to using the pipe wildcard '|' in the field.

Required
Each *Required* checkbox is associated with a *Source File(s)* field, a *Destination File(s)* field, and a *Number of File(s)* field. *Required* checkboxes are typically used in combination with multiple *Source File(s)* fields.

When *Required* is checked, the exact number of files specified in the *Number of File(s)* field must be found for the corresponding *Source* and *Destination File(s)* fields for a valid file list to be created.

If *Required* is not checked and multiple sets of *Source* and *Destination File(s)* fields are specified, a valid list is created when Diplomat MFT finds the correct number of files for **any** of the *Source* and *Destination File(s)* fields.

For example, assume you have a remote office that sends payroll files every Thursday. Each remote office sends 2 encrypted files: the actual payroll file (e.g., Remote1payroll.xls.pgp) and a text file describing the characteristics of the payroll (e.g., Remote1payroll.txt.pgp). Both files need to be picked up and processed in a single job, but they do not need to be renamed. The Diplomat MFT job is set to run at 3 p.m. every Thursday. If both files are not available, then file transfer job would fail and Failure email would be generated. In this scenario, you would set up the fields in the File Information sub-panel as shown below:

NOTE: When only one *Source File(s)* field is used, at least one file must be found for the job to continue whether or not the *Required* checkbox is checked.

Ignore File Handling
Each *Ignore File Handling* checkbox is associated with a Source File(s) field, a Destination File(s) field, and a Number of File(s) field. When *Ignore File Handling* is checked, the source files found for the corresponding *Source* fields are transferred without modification. Any entries to encrypt/decrypt, sign/verify, and/or add/remove ASCII Armoring in the *File Handling* panel on the transaction are ignored for these files.

NOTE: If FTP or secure FTP is specified as the Transport Method for either the source or destination Partner profile, files that are set to 'ignore file handling' are transferred in binary mode.

Allow Zero Byte Files
If *Allow Zero Byte Files* is checked, source files that have zero bytes on outbound jobs and destination files that have zero bytes on inbound jobs will continue to be processed as if they were valid files. File renaming and file handling steps, such as encrypt, decrypt, sign, verify, and adding ASCII-armor, occur as if the file were not zero bytes.

NOTE: Zero byte files may cause some applications to fail. *Allow Zero Byte Files* should be checked only if the receiving application(s) can correctly handle zero byte files, including ones that may have been encrypted, signed, compressed, and/or ASCII-armored.

NOTE: Zero byte files that have been encrypted or signed by PGP Command Line Server or McAfee e-Business Server typically cannot be decrypted. If you or a trading partner uses a PGP command line tool to decrypt or verify files, test whether zero byte files can be successfully decrypted and verified before checking *Allow Zero Byte File(s)*.

Post-Transfer Action
After a transaction moves source files to the destination successfully, you can specify what to do with those original source files: nothing, delete them, or move them to a subfolder at the source.

- When ***None*** is selected, Diplomat MFT does nothing to the source files after they are transferred to the destination. To avoid processing these files again, you should ensure that either something else moves these files before the next scheduled execution of this transaction, or be sure that you are using date-related source filtering (such as the <DATE> param in the file name) to pick up only those files which you are interested in for each execution of the transaction.
- When ***Delete*** is selected, Diplomat MFT attempts to delete source file(s). Some FTP servers do not allow server-side delete. If so, files are not deleted. If you experience problems deleting files from an FTP server, contact the FTP server manager.
- When ***Move*** is selected, Diplomat MFT will attempt to move the source file to the folder specified in the text field to the right (which is only visible when "Move" is selected). No file renaming is supported, but you can use Date Parameters (such as <YYYY><MM><DD>) for folder names, which will be replaced at execution time with the values corresponding to the date/time at which the transaction is run. Here is an example of the MOVE configuration:

8.4.2 Source and Destination Partner Profiles

For Diplomat MFT Enterprise Edition, you can select from your saved Partners to set all information on the *Source Partner Profile* panel in a transaction. Once you select a saved Partner Profile, the fields are fixed with saved the Partner details. You can click ***Go To Partner*** if you need to modify the fields.

If you do not want to use a saved Partner, select ***<NONE>*** to explicitly define the source for the transaction. Select the appropriate *Transport Method* to access the source file(s). When complete, you may wish to ***Save As New Partner*** so that you can simply reference it later in other transactions.

In the "Destination Partners" panel, there will always be at least one destination partner profile option, labeled "Default". There is also a "+" icon to the right of this tab which can be used to add additional destination partners. Each destination partner is independently configured. Press "X" on any destination partner tab (other than "Default") to remove that partner.

When a transaction executes and matches files at the source partner location, each matching file will be delivered to all partners at the same time. Once all partner deliveries have finished, Diplomat will repeat with the next matching source file, and so on, until all source files have been transferred to all destination partners.

8.4.3 File Handling

The information in the File Handling panel determines how a file is transformed during a file transfer job. Options may change for inbound jobs versus outbound jobs. For example, an Inbound Transaction's *File Handling* section will contain the option to *Decrypt* and appropriate related configuration, while an Outbound Transaction will contain the option to *Encrypt*. Options such as *Compress* will be available only when applicable, such as when choosing to *Encrypt* a file in an Outbound Transaction; the option would not be relevant to the *Decrypt* action.

Before configuring these options, you must create or import the appropriate OpenPGP Keys.

Check the box to enable the ***Encrypt*** or ***Decrypt*** actions as part of the Transaction as desired. When enabled, select the appropriate ***OpenPGP Encryption Key*** or ***OpenPGP Decryption*** *Key*, noting that these keys may be automatically selected and enforced if defined as part of the associated Partner's OpenPGP Keys configuration. Only keys capable of being used to execute the desired action will be available to select. If desired, repeat the process for the ***Sign*** or ***Verify*** options to either sign or verify the signature of the OpenPGP-encrypted file, selecting the appropriate ***OpenPGP Signature/Verification Key***.

When *Encrypt* is enabled, you may use additional public keys to encrypt the file, such that any of the corresponding private keys may decrypt it later. When appropriate, select the relevant *Additional OpenPGP Encryption Keys (AEKs)* from the list. Multiple keys may be selected. When a *Default Additional Encryption Key* is specified in the OpenPGP Keys Settings, it will be automatically selected for all new Outbound Transactions with *Encrypt* enabled. **Note** that when one or more additional encryption keys are specified, the job will fail if any one of the selected encryption keys has expired. Additionally, enabling the ***One-Pass Signature*** option will process the target file in a single pass for both encryption and signing. One-pass signatures may not be supported by some older OpenPGP software implementations. This option is disabled by default.

ASCII-armored format represents binary data using only printable ASCII characters for compatibility with some exception legacy systems. The ***Add/Remove ASCII Armoring*** option, disabled by default, adds or removes ASCII armoring during the encryption or decryption process. For Outbound Transactions, enabling the ***Add ASCII Armoring*** option reveals a ***Comment*** field where relevant text can be added for processes that require it. For Inbound Transactions, the job will fail if set to *Remove ASCII Armoring* from a file that is not ASCII-armored or not set to *Remove ASCII Armoring* and the file is ASCII-armored.

For Outbound Transactions with *Encrypt* enabled, the OpenPGP standard provides for the inherent ability to ***Compress*** files to reduce size. Similarly, you may enable the option to ***Convert to Canonical Text*** for plain text-based files so that each line ends with a carriage return and linefeed (CRLF) before the file is encrypted, signed, or ASCII-armored, only used when required by a legacy system. The ***Source/Destination File Format*** indicates whether you expect to handle ***ASCII*** or ***Binary*** formatted source files and the corresponding destination files. This defaults to *Binary*, as used by nearly all modern systems, or is otherwise set by use of the *ASCII Armoring* option. Additionally, enable the option to ***Add Integrity Protected Packet*** to include an Integrity Protected Packet in a

PGP-encrypted file, occasionally referred to as MDC (Modification Detection Code) or Integrity Check in various OpenPGP software products. Refer to RFC4880, the OpenPGP specification, for additional details.

8.4.4 Job Execution

Job Execution parameters determine how frequently file transfer jobs run and on what schedule. File transfer jobs can be scheduled using the built-in scheduler, file monitoring or by an external request. When a file transfer job is initiated, it is placed in a scheduling queue and waits for an available slot to begin execution.

If ***Do Not Run*** is checked, then file transfer jobs based on the transaction information are NEVER scheduled to run using the built-in scheduler, file monitoring, the Diplomat MFT Scripting Agent or the Diplomat MFT API. *Do Not Run* is always checked for newly created transactions.

The ***Run Now*** button immediately executes a file transfer job using the current transaction information, even if the transaction is suspended or set to *Do Not Run*. When the job completes, the pop-up dialog box displays the same information that you would normally receive in SUCCESS or FAILURE email messages. *Run Now* uses the settings shown in the transaction window – even if the transaction has not been saved.

The ***Diplomat Scheduler*** panel contains the settings Diplomat uses to schedule file transfer jobs. ***Run Jobs Using*** sets whether jobs run on a pre-set schedule or by monitoring one or more source folders for new files. If *Run Jobs Using* is set to <NONE>, then Diplomat MFT does not on its own initiate any jobs for the transaction, running only if invoked manually by an administrator clicking *Run Now* or via the Scripting Agent or REST API.

Schedule
Schedule Settings are enabled only if *Run Jobs Using* is set to *Schedule*. The ***Recurrence Type*** defines how frequently jobs are scheduled. For every *Recurrence Type* you use ***Run Every*** to set the recurrence frequency and the ***Start Date*** and ***Start Time*** (or ***Start Date and Time***), and you can use the ***View*** button to examine the next 10 upcoming scheduled executions. You can also set an ***Expires On*** value if you need Diplomat to stop scheduling additional runs once a specific date is reached.

Exclusions are an important consideration for scheduling. For everything other than *Weekly*, you can select ***Daily Exclusions*** by checking the boxes of days you don't want Diplomat to run the transaction. If you have defined one or more Calendars to define non-business days, then you can set the ***Calendar Exclusions*** to the desried calendar's ***Name***. For *Daily*, *Weekly*, and *Monthly* schedules you can then chose the ***Rule*** for how excluded runs should be handled, whether ***Do Not Schedule*** to simply skip that run or else ***Schedule Next Business Day*** or ***Schedule Prior Business Day***.

For ***Seconds***, ***Minutes***, and ***Hours***, you can let it recur indefinitely starting at the *Start Time*, or you can select a ***Daily Window*** to recur at that frequency starting at the ***Begin*** time and ending at the ***End*** time.

For ***Weekly***, you must select the ***Day of Week*** to run. ***Monthly*** presents additional options, such as to ***Choose months*** to run, the numeric ***Days of Month*** to run, the ***Business Days***, the ***Weeks of Month***, and ***Days of Week***.

Retries provides the ability to not immediately Fail if File(s) Not Found but to instead extend an additional grace period for the total ***Number of Attempts*** and the ***Retry Interval*** in minutes. For certain critical Transactions, you may wish to enable the option to ***Send debug email to IT support on every attempt***, or else uncheck it to send only the result if needed, whether eventual success or failure when the *Number of Attempts* is exhausted.

File Monitoring
In Diplomat MFT Standard Edition and Enterprise Edition, File Monitoring sets up a "hot folder" that is continually monitored for the source files specified, at which point action is taken in only a few seconds at most. This option

will only work with the Local Network Transport Method. If multiple pairs of source and destination filename fields are shown in the *File Information* panel, Diplomat watches the source folder for those new files. When a new file is found, a file transfer job checks that all the criteria in the File Information panel are met before processing files.

A typical example of a file monitoring job would pick up any newly created files in the source folder and delete the source files after they are processed. File Monitoring only watches for newly created files. It does not watch for files that are modified or overwritten.

Generally, only one Diplomat transaction should be set to monitor a folder. When a file monitoring transaction is saved or the Diplomat MFT Service is restarted, a job is run to process any files already in the watched folder(s). If multiple transactions are monitoring the same folder, then multiple Diplomat jobs are started when a file is written to the folder.

Set the ***Disable/notify after*** field to the number of minutes to wait if target directory is not available before automatically checking the **Do Not Run** box for the Transaction and sending an urgent email to all IT support email addresses set to receive messages on *Warning*, *Failure* or *All Jobs*. The Transaction's *Do Not Run* box must be manually cleared to re-initiate *File Monitoring*.

You can also set the ***Start Date and Time*** in case you don't want Diplomat to start monitoring for files until a specific moment, and you can set an ***Expiration*** option so that it ***Expires On*** a given date, meaning Diplomat will stop monitoring for files.

External Requests
The Diplomat MFT Scripting Agent and REST API can be used to initiate Diplomat MFT file transfer jobs. They are each documented separately. Please refer to the Coviant Software Knowledge Base for more information. Transactions can be set to allow the Diplomat MFT Scripting Agent and/or API to initiate file transfer jobs either *instead of* or *in addition to* the built-in scheduler or file monitoring. Otherwise, to run a Transaction using *only* an *External Request*, set *Run Jobs Using* to *<NONE>*.

You can choose to ***Allow Diplomat MFT Scripting Agent requests*** as well as whether to require a ***Password*** to be provided upon attempted execution. The *Password* is optional and may be left blank. Otherwise any word or phrase or string of characters entered and will be required when a Diplomat MFT Scripting Agent job is executed. The *Password* is not associated with any password or passphrase for Admin User account, PGP key, any other usage.

If you would like to ***Allow Diplomat MFT API requests***, it leverages Admin User accounts and thus does not involve a generic *Password*.

You must enable ***Allow execution as a linked transaction*** if you plan to allow one or more other Transactions to link to it as a *Post-Job Process*.

High Priority Job Queue
Use high-priority job queue if execution of this transaction should take priority over other jobs. Jobs in the regular job queue do not execute unless the high-priority queue is empty. Note that jobs initiated by the *Run Now* button or as a linked transaction are processed immediately and do not go into either job execution queue.

8.4.5 Linking Transactions

A list of all other Transactions configured to specify this Transaction as a Linked Diplomat Transaction as part of the Post-Job Processes will be listed as *Transactions linking to this transaction*.

8.4.6 Notifications

Business Email Notifications provide an additional, separate mechanism for sending email notifications of job results to individuals not included in the global IT Support Email Notification list. Diplomat's Email settings must be configured properly before email notifications can be sent.

Notifications to *Business Recipients* contain an overview of the major steps in the file transfer job and a results summary. This is useful for notifying business recipients, such as those in Accounting, HR, or other departments. It is also helpful for notifying IT personnel who may be managing or interested in processes tangential to Diplomat but are not themselves Diplomat administrators. In those cases it may be inappropriate or even annoying to the recipient to add them to the global list for notifications on all Transactions.

For each ***Business Recipient***, provide their email address and select the appropriate ***Notification Type***. Use the plus (+) button to include additional recipients. Clicking the chevron to the right reveals the ***Business Addendum*** field, which provides the option of supplying additional text to be appended to all *Business Recipients*.

Messaging Notifications provide alerts to a Slack channel or a Microsoft Teams channel. Refer to the Knowledge Base for help setting this up. To enable a ***Slack Notification*** or a ***Teams Notification*** or both, check the corresponding box and supply the Webhook URL. Select which ***Notification Type*** should generate alerts.

When the option to ***Send Debug Email to IT Support*** is checked, each time the Transaction runs, an email message including debug logs about that job is sent to relevant IT Support Email Notification recipients. This option is enabled by default. The ***IT Addendum*** field provides the option of supplying additional text to be appended to all *IT Support* recipients.

For jobs that may be long and complex, you may wish to ***Use Abbreviated Notifications***. Lists all email notifications, Run Now windows, and summary messages in log files are truncated to 100 entries. These lists include source filenames, destination filenames, primary archive filenames, additional archive filenames, destination errors, archive errors and other non-fatal errors. Additionally, Debug Log entries in IT support email are also limited to the first and last 1,000 entries.

8.4.7 Archiving

Archive files are copies of the files that are transferred by a Diplomat MFT file transfer job. It is strongly recommended that users who want to create centralized, self-managing archives of transaction files, use Primary Archive to set the location and related parameters. Otherwise, use the ***Skip Primary Archiving*** option when retention of files in the primary archive location is not needed or desired.

For each Transaction you may also choose whether to provide a separate ***Additional Archive***, to be used instead of or in addition to the *Primary Archive*. Use **Test** to determine whether the location is accessible. You may decide whether to automatically ***Add transaction-specific sub-directories*** and whether to ***Zip Archive Files*** into a single zip file. Note that **if** zipping the files is not successful, the additional archive files are **not** deleted and can be found in the directory specified in the *Additional Location* field or a transaction-specific sub-directory. Select whether source, destination, or both ***File Types*** are to be archived.

File archiving occurs directly after each file transfer during a job. When a file transfer is completed, the source file, the destination file, or both files are archived. For files that fail to transfer, the original file(s) remain in the source directory. Typically, files are archived only when a file transfer has completed successfully without a fatal error. Use the settings in the ***Attempt Archive On*** field to archive files for file transfers that do not complete successfully.

8.4.8 Pre- and Post-Job Processes

Pre- and Post-Job Processes occur either before of after all other file transfer job steps have been completed. Custom and zip/unzip processes are supported.

Custom Processes
A custom pre-process can be run before either inbound or outbound jobs. For outbound jobs, files can also be zipped after the custom pre-process has completed.

The *Custom Process* panel allows you to specify a custom process that executes before a file transfer job is attempted or after it completes. For example, it might be used to rename files before processing or to validate an XML file's schema after it's received.

The *Custom Process* can be used to run any command supported by the OS, such as DOS commands, batch files, or shell scripts, or executables such as script parsers or utilities. DOS commands must always begin with 'cmd /c' followed by the command in the same form as you would enter at a DOS prompt. When executing batch or executable files on a Windows system, the 'cmd /c' is optional, but may provide additional debug information when used.

Provide *the complete pathname* for any file referenced in ***Execute Before/After File Transfer Job***, such as 'E:\path\to\example.bat'. This command is executed before any steps in the file transfer job begin or after they have all completed. It uses either the ***<DEFAULT>*** of Diplomat's installation directory *\tomcatWebserver\bin* subfolder or else whatever you provide, using ***Test*** to validate the path. The ***Execute*** button issues the command as entered to assist in confirming it works correctly before use in production jobs. The ***Timeout*** value is the maximum amount of time for Diplomat to wait for a reply from the process before marking the job as a Failure.

For *Pre-Job Processes* this command is executed *each time* a job is executed, no matter how often or frequently it's scheduled to run, regardless of whether any files are ready to be processed. If the command fails, the overall job fails, failure notifications are generated, and no further steps in the job are executed. To override this default, enable the option to ***Continue Job Execution on Command Failure***. You can also include the <TRANS_ID> parameter in this field to be set by Diplomat MFT during job execution.

For *Post-Job Processes* this command executes after all steps in the file transfer job have *successfully completed*. If any prior steps in the file transfer job have failed, this command is not executed. To override this default, check *Execute custom post-process on file transfer job failure*. Note that even with that box checked, when no files are processed by a given run of Transaction that does not use the option to Fail if File(s) Not Found, the command is not executed. These jobs are not classified as successes or failures by Diplomat MFT and are simply rescheduled.

You can also include the following parameters in this field to be set by Diplomat MFT during job execution:

- <TRANS_ID> is the Transaction Name. **NOTE:** The value of the Transaction Name parameter is case sensitive and is set exactly as the Transaction Name is displayed in the Transaction Name field on the transaction screen.
- <JOB_COMP_STATUS> is the job completion status.
- <NUM_FILES> is the total number of files found by the job – whether or not the files were processed successfully.
- <FILE_STATUS_LIST> is a list of the status of the each file found by the job.
- <SRC_FILE_LIST> is the list of source filenames found by the job.
- <DEST_FILE_LIST> is the list of destination filenames found by the job.
- <DEST_LIST_PATHNAME> is the full pathname including the name of the file that contains the list of destination files names and the status of each file. The path is set to C:\ProgramData\Coviant

Software\Diplomat-j\temp or the corresponding folder for your installation. The name of the file is filesxxxxx.tmp, where 'xxxxx' is a random number. The Diplomat job knows the exact filename created by the job. The file contains two lines for each file, with the file name on the first line and the status on the second line.

NOTE: These temp files are deleted whenever other temp files in the folder are deleted based on the schedule under Settings > Logging from the top menu.

List elements are separated by a single space, and filenames are enclosed in double quotation marks.

These values are also populated as **Environment Variables,** so your custom process can easily acquire the information using the environment variables, rather than passing along as a command line parameter.

- DMFT_TRANSID – the name of the executed transaction
- DMFT_JOB_COMP_STATUS is the job completion status (one of "Cancelled", "Critical", "Failure", "File(s) Not Found", "Incomplete", "Missed", "Required File(s) Not Found", Successful", "Terminated", or "Warning")
- DMFT_NUM_FILES is the number of files transferred during this job execution
- DMFT_SRC_FILENAME_x – for each transferred file, there is an entry with the source file name (e.g., "DMFT_SRC_FILENAME_1")
- DMFT_DEST_FILENAME_x – for each transferred file, there is an entry with the destination file name
- DMFT_FILE_STATUS_x – for each transferred file, there is an entry with the status of that file transfer
- DMFT_FILESIZE_x – for each transferred file, there is an entry with the size, in bytes, of that file.

Zip (Outbound)

For outbound jobs, files can be zipped after the Custom Pre-Process, if any, has completed. Zip can only be specified on transactions with source Transport Method set to Local Network. Take care to set the the *Source File(s)* field of your transaction to match the names of the resulting zip files for transfer, such as '*.zip' for all zipped files in the directory. The option to ***Delete Original Unzipped File(s)*** is enabled by default, and it will only act if the zip process succeeds.

Zip Type, if not set to ***None*** to disable zipping, sets either the Windows-style ***ZIP*** or Linux-style ***GZIP*** tar archives. You can choose whether to ***Zip Files Individually*** so you could have multiple zip files or else ***Together*** into a single file. You must provide the full path to the ***File(s)Location*** for the files to be zipped as well as the and name mask of the **File(s)** to be zipped, both of which may contain a <DATE> parameter. The name mask may also contain the wildcards *, ? and the special ** to recursively zip all files in the files location folder and any subfolders, though ** can only be used when *Zip Files Together* is selected.

If *Together* is specified, Provide the ***Zip File Path/Name*** of the zip file to be generated. It can contain a <DATE> parameter, in which case the ***Date Format*** field allows you to provide the desired Date Variables.

The ***Zip Encryption*** is available when the *Zip Type* is *ZIP*, providing the ability to encrypt the resulting zip files with traditional weak WinZip ***Zip2.0*** encryption supported by most operating systems, or the stronger ***AES-128*** and ***AES-256*** encryption not supported by Windows, only Diplomat itself and some 3rd party tools such as 7-Zip (https://www.7-zip.org/). If *Zip Encryption* is used, you must provide a ***Zip File Password***.

You may choose to ***Continue Job Execution on Zip Process Failure***, but only do so when the rest of the Transaction does not depend on the process completed. Otherwise, by default the job fails and stops further processing.

Unzip (Inbound)

For inbound jobs, files can be unzipped before a Custom Post-Process, if any, is initiated. Unzip can only be specified on transactions with source Transport Method set to Local Network. The option to ***Delete Original Zipped File(s)*** is enabled by default, and it will only act if the unzip process succeeds.

Set the ***Zip Type*** based on whether you're expecting ***ZIP*** or ***GZIP*** files, or use ***None*** to disable unzipping. *GZIP* assumes that files are standard UNIX tar archives. Use ***Zipped File(s) Template*** mask to provide the full path for the files should be unzipped, which can contain a <DATE> parameter. If required, provide the ***Zip File Password***. The ***Unzip to Directory*** optionally specifies one or more folders as the root location for any unzipping operation and can contain a <DATE> parameter. If the *Unzip to Directory* is not specified, the unzipping is done in-place at the destination location. The ***Date Format*** field allows providing Date Variables for the moment at which the processing occurs if a <DATE> parameter is contained in the *Zipped File(s) Template* or *Unzip to Directory* fields.

The ***Overwrite*** settings allow you to select the conditions under which unzipped files will overwrite existing files. The overall job status of SUCCESS, WARNING or FAILURE is not affected by whether a file is overwritten or not, regardless of setting.

You may choose to **Execute unzip process on file transfer job failure**, but do so only when the zip process does not rely on the transfer job to be complete.

Linked Diplomat Transaction

To invoke another Transaction to run when this Transaction has completed, you choose it in the ***Run After File Transfer Job*** drop-down which lists all Transactions with Allow execution as a linked transaction enabled. For a quick shortcut to view the linked transaction, use the ***Go to Transaction*** to button. You may choose to ***Run linked Diplomat MFT transaction on file transfer job failure***, but only do so if the linked Transaction does not depend on the primary linking transaction to have completed successfully.

A successfully linked Transaction will have its own job status based on its own results. If a Transaction cannot be linked successfully, an error is generated and the primary file transfer job fails. A transaction cannot be linked successfully if the linked transaction either does not exist, is not set to allow execution as a linked transaction, is set to Do Not Run, or is currently suspended.

NOTE: A linked transaction is not quite the same as using a Diplomat Scripting Agent command in the Custom Post-Process panel. The primary job does not wait for a linked transaction to execute before completing, which means that a primary file transfer job may be successful even if the linked transaction fails. Thus, linked transactions should be set to send email notifications, as needed, to anyone who needs to know the completion status of the linked transaction job.

8.4.9 Troubleshooting

Use ***Turn on Advanced Troubleshooting*** to capture additional debug and log information and prevent deletion of temporary files created during the execution of a transaction. It should be used **ONLY** when you need to debug a particular transaction, as the zip files in the *troubleshooting* directory are **not** automatically deleted by Diplomat. You MUST manually delete all troubleshooting files when you are finished using them.

Advanced Troubleshooting captures debug files, log entries and temporary files in a zip file. For Windows systems, the location is C:\ProgramData\Coviant Software\Diplomat-j\troubleshooting. For Linux systems, the default directory is /opt/coviant/diplomat-j/troubleshooting or the corresponding directory for your installation.

Troubleshooting files have names in the form 'DiplomatTS.TransactionName.year + month + day . hour + minutes + seconds.zip'. For example, a troubleshooting file for transaction 'Test2' created on January 4, 2004 at 3:17:53 p.m. would be named 'DiplomatTS.Test2.20040104.151753.zip'.

If *Turn on Advanced Troubleshooting* is checked on any transactions, you will be reminded when you exit the Diplomat MFT Client. You can click through to the transactions from the *Troubleshooting On* pop-up or check *Turn off troubleshooting on all transactions*, if desired.

NOTE: Debug files may contain sensitive information. Additionally, troubleshooting files only contain temporary files when they are created (e.g., during encryption, decryption, signing, or verification). If temporary files are not created and files are transferred using only Local Network as the source and destination, no temporary files are captured in the troubleshooting zip file.

9 Transport Methods

Every Transaction in Diplomat must have a source and a destination, where files are coming from and where they're going to. The transport method refers to how those files are retrieved from the source or written to the destination. Each method has its own capabilities and configuration items.

9.1 Amazon S3

The Amazon S3 transport can operate in ***S3*** mode, meaning that it natively communicates with the Amazon AWS S3 services, or it can operate in ***S3 Compatible*** mode, in which it utilizes the standard S3 API to communicate to a given storage endpoint other than Amazon AWS S3. Many storage vendors support the S3 API, both in the cloud and on-premises. Examples include Wasabi Systems, Backblaze, Carringo, Minio, and many more.

The fields that you must configure are slightly different for the two styles of S3. You choose which style of access using the radio button choices at the top of the transport configuration panel.

Enter the ***Key ID*** and ***Secret Key*** from your Amazon S3 authorization credentials. Then provide the name of the desired ***Bucket***, and if you intend to use a subfolder in the Bucket, provide the ***Directory*** path. The ***File Integrity Checking*** is enabled by default, where Diplomat validates that the **File Size** at the source and destination match when the transfer is complete, but you may choose to set it to ***None*** to disable it. You may also choose whether to ***Use server-side encryption***, enabling SSE-S3 protection of data at rest. If desired, enable the options for ***Bucket Owner Full Control***, and if you know you ***Expect Bucket owner***, check the box and provide the owner in the field.

For S3 ***Compatible*** connections, you must supply the full URL to the S3 API ***Endpoint***, such as *https://s3.wasabisystems.com*. You must also supply the ***Region*** for *Bucket* access. This *Region* item is also used as part of the header signing, a form of security on S3 API requests. If you are unsure, either use "us-east-1" or consult the documentation for your storage provider.

You may also select a ***Proxy Server*** through which to make connections. If desired, enable the option to ***Use temp filenames*** and provide the desired filename ***Prefix*** or ***Suffix*** or while writing files to the destination. When the entire file has been written, the filename is changed to the destination filename.

9.2 AS2

AS2 is an acronym that stands for "Applicability Standard 2," and is defined by RFC 4130. This transport is a message-oriented protocol that was designed to provide a mechanism for trading partners to send files to a server in a secure fashion, using both SSL/TLS for transport security, and OpenPGP and SMIME for data security. In

addition, the protocol supports digital receipts that can be signed using strong cryptography (sometimes referred to as MDNs, or "Message Digest Notifications"). By providing a receipt, the AS2 protocol is used in scenarios where acknowledgement of file receipt is important, and cryptographically strong proof of delivery is required – for example, purchase orders and shipments in a supply chain.

NOTE: AS2 can only be used to SEND files, and therefore it is only available as a Transport for the **Destination** of a transaction. When choosing a **Partner Profile** for a transaction, you may only choose AS2 Partners a **Destination** of a transaction.

NOTE: Diplomat MFT's AS2 implementation supports only **synchronous** receipts, meaning that immediately after a file is uploaded, the remote AS2 server will return a digitally signed receipt (which is audited by Diplomat MFT). Some AS2 implementations also support an **asynchronous** receipting mechanism, in which the remote AS2 server delivers the file receipt via an HTTPS connection back to the sending system – but Diplomat MFT does not support this..

Address
Enter the full URL to the HTTP or HTTPS endpoint that receives AS2 transfers. For example, https://as2.acmeserver.com/inbox. If the server uses a non-standard port, be sure to include it in the URL as well – for example, https://as2.acmeserver.com:8443/inbox.

Test Button
After entering the AS2 Server Address, Subject, Sender ID, Recipient ID, and choosing Client SSL Certificate, Server SSL Certificate, Encryption Algorithm, and Signing algorithm, you may press **Test** to:

- Test the connection to the AS2 Server.
- Send a small text file to the server using the AS2 protocol.

Enter the ***Username*** and ***Password*** that will be used to authenticate with the AS2 Server, along with the ***Subject*** and ***Email Address*** for the message envelope.

Your AS2 Identifier
Each partner in an AS2 transfer will have an assigned Identifier string that is unique to that partner. Enter your AS2 Identifier into this field. You will communicate this identifier to your trading partner so that they know from whom transfers are originating.

Recipient AS2 Identifier
Enter your partner AS2 Identifier into this field. Your trading partner should provide this information to you.

Your SSL Certificate
AS2 performs digital signing on the delivered message, so that the recipient may verify the identity of the sender. Supply your Client SSL Certificate in this field. You will need to deliver the Public portion of this Client SSL Certificate to your partner so that they can verify your digital signature.

Recipient SSL Certificate
Your partner will provide you with their public SSL Certificate, which you will import into your SSL Certificates, and choose in this field. The certificate is used for encrypting messages delivered to your trading partner, and for verifying the digital signature on signed receipts.

Encryption Algorithm
Choose an encryption algorithm to use for encrypting the message contents for your trading partner. Choose "<None Selected>" if you do not wish for the file(s) payload to be encrypted during transfer

Signature Algorithm

Choose a signature algorithm to request that your trading partner use to sign digital receipts which are returned to Diplomat MFT at the end of a file upload. Choose "<None Selected>" if you do not wish for the file(s) payload to be encrypted during transfer.

9.3 Biscom

Biscom provides a cloud hosted file transfer service. It provides secure file messaging and large file sharing for businesses. With Diplomat MFT, you can choose to send files to email recipients through Biscom Transit, which means that the recipient will get an email that has a hyperlink pointing back to the file for pickup. The sender receives notifications of download activities. Alternatively, you can use Diplomat MFT to upload files to the Biscom Transit folder system, which can be used for document sharing and collaboration.

NOTE: Biscom can only be used to SEND files, and therefore it is only available as a Transport for the **Destination** of a transaction. When choosing a **Partner Profile** for a transaction, you may only choose Biscom Partners a **Destination** of a transaction.

Account
Enter the account name for your Biscom Transit service. This is typically the first part of your Biscom Transit domain, such as “coviant” for “coviant.biscomtransit.com”

Type
Choose whether you are sending files as an email (Message) or uploading them to a Biscom Transit folder (Upload).

Test Button
Test the connection, including authentication with the provided username and password.

Username
Enter the username that can authenticate to the Biscom Transit service.

Password
Enter the password for authenticating to the Biscom Transit Service.

To
When sending the files as email attachments, supply the email address(s) for the recipients. You can specify multiple email addresses separated by commas.

CC
When sending the files as email attachments, supply the email address(s) for the CC recipients. You can specify multiple email addresses separated by commas.

BCC
When sending the files as email attachments, supply the email address(s) for the CC recipients. You can specify multiple email addresses separated by commas. Recipients will not see these addresses in the message envelope.

Subject
Specify the subject to be used when you are sending file(s) in a message. You can use Date Parameter values in the subject, such as “<YYYY>” and the job will replace those with the values when the job executed.

Folder
When sending the files as an upload, supply the folder path where you wish the files to go. For example, / is the root folder of your Biscom Transit “Files” area.

Email Notification
Enter the text which will be sent to the recipient in the email notification that they receive regarding files available on the Biscom Transit server. They read this email in order to follow a link to pick up the file(s). You can use Date Parameter values in the subject, such as "<YYYY>" and the job will replace those with the values when the job executed.

Secure Note
Enter the text which will be stored on the Biscom Transit server. A recipient of a message must follow the link and authenticate in order to read this text. You can use Date Parameter values in the subject, such as "<YYYY>" and the job will replace those with the values when the job executed. This field is only available if you check the box "Secure Message"

Secure Message (sign-in required)
Check this box if you wish to require the recipient to authenticate against Biscom Transit server in order to obtain the delivered file(s). Optionally, you can provide text in the Secure Note field that will be visible only after they authenticate to Biscom Transit.

Expiration Date
Optionally, choose when this message delivery expires. After expiration, recipients will no longer be able to download file(s) nor see any secure notes.

Proxy Server
Choose a proxy server for outbound HTTPS connections, if necessary.

Timeout
Specify the number of seconds to wait for a response from Biscom Transit before the job times out as an error.

9.4 Box

Provide the authorization ***Credentials*** file associated with your Box account, the ***User ID*** of the Box application, and, if needed, the specific ***Directory*** within the Box account to be used. Also choose whether to use ***File Integrity Checking*** after a transfer has completed, verifying the ***File Size*** at the source and destination. Use the ***Test*** button to test the connection and display the storage contents.

9.5 Citrix ShareFile

Provide the ***Address*** at which you access your ShareFile account along with the ***Username*** and ***Password*** and the ***Client ID*** and ***Client Secret*** generated for API access to your ShareFile account. Select whether the ***Folder Type*** is ***Personal***, or if it's ***Shared***, provide the name of the ***Shared Folder***. If desired, provide a specific ***Directory*** to be used. Also choose whether to use ***File Integrity Checking*** after a transfer has completed, verifying the ***File Size*** at the source and destination. Use the ***Test*** button to test the connection and display the storage contents.

9.6 Diplomat Remote Agent

Diplomat Remote Agent is a proprietary transport method that requires Diplomat Remote Agent to be installed at the target location. Refer to the *Diplomat Remote Agent Installation Guide* for more information on how to install and configure a Diplomat Remote Agent site.

Diplomat Remote Agent is a very secure file transport option with authentication using OpenPGP and data transmissions can optionally be automatically PGP encrypted before pick-up from the source location and automatically decrypted before being written to the destination location. It is based on TLS 1.3 encrypted HTTPS.

Address
IP address or domain name of Diplomat Remote Agent site where the source file(s) are found or destination files are written. The system running the Diplomat Remote Agent must have a permanent IP address or domain name.

Port
Specifies a port number to be used for communication with Diplomat Remote Agent. Default port is 8082. Contact the Diplomat Remote Agent administrator to obtain this information.

MFT Site Key
The OpenPGP private key to be used for session authentication and data encryption and decryption during a file transfer job. If you do not have a password to install the MFT site key automatically, export the OpenPGP public key from the MFT Site Key and name the file diplomatMFTPublicKey.asc. Email the diplomatMFTPublicKey.asc file to the Diplomat Remote Agent administrator for installation.

Install Button
The *Install* button initiates a process to install the OpenPGP public key associated with the MFT Site Key on the Diplomat Remote Agent site. You must enter the single-use password created when Diplomat Remote Agent was installed. If you do not have the correct password, the MFT site public key on the Diplomat Remote Agent site is not updated.

NOTE: Passwords are only created during a Windows installation process. When the Diplomat Remote Agent Site is installed on a Red Hat Linux system, the Diplomat MFT Site public key must be sent to the Diplomat Remote Agent administrator and copied to the Diplomat Remote Agent site.

NOTE: The password can be used only once to install a MFT site public key. If the MFT site public key needs to be refreshed, a new Diplomat MFT site public key can be sent to the Diplomat Remote Agent administrator and copied to the Diplomat Remote Agent site or the Diplomat Remote Agent administrator can perform a Repair install, enter a new password, and send the new password to the Diplomat MFT administrator.

Test Button
After entering the Diplomat Remote Agent information, press **Test** to:

- Test the connection to the Diplomat Remote Agent site
- Determine whether the OpenPGP public key at the Diplomat Remote Agent site matches the OpenPGP private key specified in the Partner profile
- Test whether the Diplomat MFT Service was able to authenticate and connect to the Diplomat Remote Agent site
- Display the default directory and its contents

Change Root Button
Sets the default directory for Diplomat Remote Agent site. Files being transferred are read from or written to this location if no directory or a relative path is specified in the Directory field. Updating the root directory changes the root directory for the entire Diplomat Remote Agent site and **affects all transactions sending files to or from the site.**

NOTE: If a relative path is specified in the Directory field or the Source File(s) or Destination File(s) fields in the File Information panel of a transaction, the relative path is appended to the directory shown in the Root Directory field.

NOTE: The root directory defaults to the documents directory of the network identity associated with the Diplomat Remote Agent Service. It is strongly recommended that you select a permanent directory to replace the default directory.

View Logs Button
Enables logs files from the Diplomat Remote Agent site to be displayed and filtered using the Diplomat Log Viewer. For further information refer to the *Logs* section of this guide.

Auto OpenPGP Encrypt/Decrypt
When checked, all data files are automatically compressed and encrypted before transfer and then automatically decompressed and decrypted before being written to the destination location. Files coming from the Remote Agent are encrypted with the Diplomat MFT public key and then decrypted with the Diplomat MFT private key pair. Files coming from Diplomat MFT are encrypted with the Remote Agent public key and then decrypted with the Remote Agent private key pair.

NOTE: A new Remote Agent private key pair is dynamically created each time the Remote Agent is restarted.

NOTE: The Diplomat Remote Agent public key is not stored on the Diplomat MFT site and is passed automatically to the Diplomat MFT site during the file transfer job after the Diplomat MFT site has been authenticated.

Attempt Checkpoint Restart on Transmission Failure
When checked and an error occurs while transferring a file, the Diplomat MFT site attempts to resume the file transfer by adding data to the partially completed file. Otherwise, the Diplomat MFT site attempts to restart the file transfer from the beginning of the file.

Directory
Directory on the Diplomat Remote Agent site where transaction file(s) are found or written. Values starting with a slash are interpreted as full path names. Other values are interpreted as sub-directories from the root directory shown in the Site Configuration panel.

NOTE: The root directory for the Diplomat Remote Agent site can be changed using the **Change Root** button in the Site Configuration panel. Updating the root directory changes the root directory for the entire Diplomat Remote Agent site and **affects all transactions sending files to or from the site.**

Set the ***Max # Retries*** and ***Retry Delay*** in seconds to decide how persistent Diplomat should be with transfers using this Remote Agent. Set the ***Chunk Size*** for the maximum file part size will be used and the ***Max Bandwidth*** in megabits per second to limit bandwidth utilization. Default *Chunk Size* is 100MB and may be set smaller but should not be set larger without consideration to the performance impact of increased memory (RAM) utilization.

File Integrity Checking
Choice of file integrity checking by File Size, Checksum (SHA-256), or no file checking after a file transfer. When File Integrity Checking is enabled, the size of the source file is compared to the size of the destination file. The size of the source file before the transfer is also compared to the size of the source file after the transfer to ensure that no additional data has been written to the source file.

Timeout
Sets the length of time a Diplomat MFT site waits for a response from Diplomat Remote Agent site.

Custom Post-Process
You may provide a process for the Remote Agent to run on its local machine after a Transaction has completed. For specific details, see Custom Processes.

9.7 Dropbox

Provide the ***Access Token*** associated with your Dropbox account, a specific ***Directory*** to be used, and whether to use ***File Integrity Checking*** after a transfer has completed, verifying the ***File Size*** at the source and destination. Use the ***Test*** button to test the connection and display the storage contents.

9.8 Email

Use the **Test** button to test the connection to the email server and determine whether the account and password on the Email Settings screen, if any, are valid.

When Sending, the ***Sender Account***, ***Sender Address***, and ***Sending Server*** are defined in the Email settings. Specify the desired ***Recipient Addresses***, ***Subject***, and ***Body***. If multiple email addresses are used, they are concatenated with semi-colons before being written to a single Email Address field in the audit trail database. Diplomat MFT can only store up to 255 characters in the Email Address field in the audit trail database. Address information after the first 255 characters will be truncated.

When receiving, the ***Recipient Account*** and ***Receiving Server*** are defined in the Email settings. Each time a job runs, all email messages addressed to *Recipient Address* on the *Receiving Server* are searched. A separate email account is recommended, rather than using an existing user's account. A separate email account reduces the risk that files are downloaded unintentionally because an attached file happens to have a name matching the *Subject* and *Source File(s)* information. It also reduces the risk that a user accesses and deletes an email message with a desired file attached before Diplomat MFT has processed the file.

The ***Sender Address*** and ***Subject*** may be used to narrow down which emails from which to retrieve attachments, though either or both may be ***<ANY>*** as they are by default. Wildcards for up to one (?) or multiple (*) characters are allowed in *Subject* and in the left portion if the *Sender Address* only (i.e., before the @ sign). Use wildcards when you expect email will be sent by more than one person at your trading partner. For example, you might use *@companyname.com in the *Sender Address* field, if you expect email to be sent by either Mary Smith (mary.smith@companyname.com) or John Doe (john.doe@companyname.com). Specifying the *Subject* and *Sender Address* as completely as possible reduces the time to review and download email attachments.

NOTE: If the sender is using Microsoft Outlook, they may need to send the email message using 'plain text' format to avoid having attached file(s) renamed to winmail.dat.

9.9 FTP/S

Provide the ***Address*** and ***Port*** of the FTP/S server along with the ***Username*** and ***Password*** details. Some legacy FTP/S servers require an ***Account*** ID in addition to a username and password. Provide a specific ***Directory*** to be used, if any, along with a ***Timeout***. Provide a custom ***SITE Command*** to be used after login and before the file transfer is initiated, rarely used but available, and choose whether to use ***File Integrity Checking*** after a transfer has completed, verifying the ***File Size*** at the source and destination. Use the Test button to test the connection, credentials, and display the folder contents.

For the ***Server Type***, leave the default ***Windows/Unix*** in place or select ***AS400/IFS***, ***AS400/Library***, or ***MVS/IFS***. Selecting *AS400/IFS* enables transactions with the Integrated File System (IFS) only, and the Directory will always be processed as starting with a forward slash '/' even if left blank. Selecting *AS400/Library* enables transactions with the *AS/400 Library* file system only. *AS/400 Library* systems do not support directories, so the *Directory* field must be left blank.

For ***Server Mode***, since most FTP/S servers operate most successfully in Passive (PASV) Mode, the default is ***Passive***. Select ***Active*** if desired, and review the active FTP settings.

For FTPS, if desired use ***SSL Server Certificate*** select an SSL Certificate to be validated upon connection, and select whether to use ***Explicit SSL*** (port 21) or ***Implicit SSL*** (port 990). Choose whether to allow a Clear Command Channel (***CCC***) to stop encryption after the user authentication is completed, ***Allow Self-Signed Certificates***, and ***Allow Expired Certificates***, all of which are disabled by default.

When used as a source, the ***File Ready Condition*** determines whether to transfer a file, helping ensure a file is only transferred when it is completed at the source. The ***File Idle Time*** condition checks that the file has not been created or modified within the last ***Idle seconds*** value, 30 by default. The ***Trigger Name*** condition looks for a trigger file (sometimes called a flag file) indicating the readiness of the actual file to be processed, allowing you to set the desired ***Trigger Pattern*** and choose what to do with the ***Trigger File Handling*** after the transaction completes successfully, to either ***Transfer*** or ***Delete*** the trigger file. An example of the typical ***Trigger Pattern*** would be **<FILENAME>.<EXT>.trg** where the trigger file name is simply the name of the actual file with a trigger-specific extension added, such as **.trg** in this case.

You may also choose a ***Proxy Server*** when connecting to FTP or FTPS servers. Proxy servers are defined in Proxy Servers settings.

9.10 Google Cloud

Provide the authorization ***Credentials*** file associated with your Google Cloud account, the name of the ***Bucket*** to be accessed, and, if needed, the specific ***Directory*** to be used. Also choose whether to use ***File Integrity Checking*** after a transfer has completed, verifying the ***File Size*** at the source and destination. Use the ***Test*** button to test the connection and display the storage contents.

9.11 HTTP/S

Provide the ***Address*** and ***Port*** of the HTTP/S server. If needed, provide a ***Username*** and ***Password*** as well as the specific ***Directory*** to be used. Choose and appropriate ***Timeout*** value and whether to use ***File Integrity Checking*** after a transfer has completed, verifying the ***File Size*** at the source and destination. You may also choose a ***Proxy Server*** from the list defined in Proxy Servers settings. Use the ***Test*** button to test the connection and display the storage contents.

For HTTPS, choose whether ***Allow Self-Signed Certificates*** and ***Allow Expired Certificates***, both of which are disabled by default.

NOTE: Some HTTP/S jobs may have a maximum file size of 2 GB.

9.12 Local Network

Local Network allows access to any attached storage or network shares to which Diplomat's Service Account has access. is the default selection for each Source and Destination partner profile, and it is the simplest and most direct option. Browse for attached storage or paste in a UNC path. **Use *Test* to confirm that the logon for the Diplomat MFT 64 service or diplomatServer daemon has the required privileges before contacting Coviant Software Support.**

Choose whether to use ***File Integrity Checking*** after a transfer has completed, verifying the ***File Size*** at the source and destination. Use the Test button to test the connection, credentials, and display the folder contents.

When used as a source, the ***File Ready Condition*** determines whether to transfer a file, helping ensure a file is only transferred when it is completed at the source. The ***File Idle Time*** condition checks that the file has not been

created or modified within the last ***Idle seconds*** value, 30 by default. The ***Trigger Name*** condition looks for a trigger file (sometimes called a flag file) indicating the readiness of the actual file to be processed, allowing you to set the desired ***Trigger Pattern*** and choose what to do with the ***Trigger File Handling*** after the transaction completes successfully, to either ***Transfer*** or ***Delete*** the trigger file. An example of the typical ***Trigger Pattern*** would be **<FILENAME>.<EXT>.trg** where the trigger file name is simply the name of the actual file with a trigger-specific extension added, such as **.trg** in this case.

9.13 Microsoft Azure

Choose your ***Storage Type***, including ***File***, ***Append Blob***, ***Block Blob***, or ***Page Blob***. Then provide your Account, select whether to use ***Key*** or ***SAS*** for ***Authentication***, and provide the access ***Key*** associated with your account or the ***SAS URL***. Specify the ***Container*** or share to be accessed and a ***Directory*** in that container, if needed. Also choose whether to use ***File Integrity Checking*** after a transfer has completed, verifying the ***File Size*** at the source and destination.

The **Account** and **Share** information can be found in Data Storage > File Shares when looking at your storage account in Azure. Both the account and share do not require any reference to the "file.core.windows.net", the way that you use to connect to SMB.

When configured to your liking, use the **Test** button to test the connection and details provided and show the file contents.

9.14 Oracle Cloud

The ***Username*** is the same as used to log into the MyServices Dashboard of your Oracle account, typically an email address, and must have a valid ***Password***. Provide the ***Service Name***, the ***Identity Domain*** name, and the ***Service URL*** of your Oracle Cloud Storage service along with the ***Container*** to be accessed. You may provide a ***Directory*** in that container or leave it blank to use the default directory.

Choose whether to use ***File Integrity Checking*** after a transfer has completed, including verifying the ***File Size*** at the source and destination or validating the ***Checksum (SHA-256)*** for a high degree of certainty that each file is truly identical.

When configured to your liking, use the **Test** button to test the connection and details provided and show the file contents. If the specified container does not exist, you will be prompted to create it or select an existing container.

9.15 SFTP

SFTP is part of the SSH2 protocol suite and is the de facto standard for secure, reliable file transfers.

When using SFTP in Diplomat, you must provide the ***Address*** and ***Port*** of the SFTP server, the ***Username***, and the ***Password*** and/or ***SSH Client Key***. You may optionally choose to ***Verify SSH host key*** to ensure it matches the list of known good options in the ***Show SSH Host Keys*** list.

Use the ***Directory*** field to provide an alternate absolute path or relative subfolder of the default home folder when connected to that SFTP server. Set the ***Timeout*** to a reasonable value in seconds, with a default of 30. You may need to use a ***Proxy Server*** from the list defined in the Proxy Servers settings.

When used as a source, the ***File Ready Condition*** determines whether to transfer a file, helping ensure a file is only transferred when it is completed at the source. The ***File Idle Time*** condition checks that the file has not been created or modified within the last ***Idle seconds*** value, 30 by default. The ***Trigger Name*** condition looks for a trigger file (sometimes called a flag file) indicating the readiness of the actual file to be processed, allowing you to set the desired ***Trigger Pattern*** and choose what to do with the ***Trigger File Handling*** after the transaction completes successfully, to either ***Transfer*** or ***Delete*** the trigger file. An example of the typical ***Trigger Pattern*** would be **<FILENAME>.<EXT>.trg** where the trigger file name is simply the name of the actual file with a trigger-specific extension added, such as **.trg** in this case.

Select the ***File Size*** option for ***File Integrity Checking*** to ensure the file size at the source and destination are the same.

When configured to your liking, use the **Test** button to test the connection to the SFTP server, determine whether the login credentials are valid, display the directory contents, and check that an *SSH host key* has been verified. If you have configured the transaction to *Verify SSH host key*, and *SSH host key* from the SFTP server is not already known, then you will be prompted whether to add the key details and retest the connection.

9.16 SMB

SMB (Server Message Block) is an alternate method of accessing network storage. Whenever possible, the default Local Network is recommended to be used instead. SMB may be used when you are attempting to access network storage to which you have connectivity but is outside of the security context of the Diplomat Service Account, such as when connected via VPN to a partner's network with an unrelated Active Directory with which a sufficient trust relationship has not been established. It is strongly recommended to NOT use this to leverage alternate internal user or service accounts in place of proper network share administration.

When configuring an SMB endpoint, you must provide the ***Address*** of the server and the ***Port*** number to be used for the SMB session. Contact the SMB server administrator to obtain this information. Also important are the ***Domain***, ***Username***, and ***Password*** used to access the SMB server. The ***Share*** is the folder shared by the SMB server administrator, and the ***Directory*** is the subfolder under that share which will be used for the Transaction. The File Integrity Checking option determines whether to check the file size at the source and destination to ensure they are the same.

When you have completed the fields, use the ***Test*** button to test the connection to the SMB server, determine whether the username and password are valid, to check that the storage location is accessible, and to display the folder and its contents.

When used as a source, the ***File Ready Condition*** determines whether to transfer a file, helping ensure a file is only transferred when it is completed at the source. The ***File Idle Time*** condition checks that the file has not been created or modified within the last ***Idle seconds*** value, 30 by default. The ***Trigger Name*** condition looks for a trigger file (sometimes called a flag file) indicating the readiness of the actual file to be processed, allowing you to set the desired ***Trigger Pattern*** and choose what to do with the ***Trigger File Handling*** after the transaction completes successfully, to either ***Transfer*** or ***Delete*** the trigger file. An example of the typical ***Trigger Pattern*** would be **<FILENAME>.<EXT>.trg** where the trigger file name is simply the name of the actual file with a trigger-specific extension added, such as **.trg** in this case.

Choose whether to use ***File Integrity Checking*** after a transfer has completed, verifying the ***File Size*** at the source and destination. Use the Test button to test the connection, credentials, and display the folder contents.

The **SMB Version** indicates the SMB libraries to be used. Two options are available, 6.1 which is compatible with SMB 1.0 and 7.3 which is compatible with SMB 1.0, 2.0 and 3.0. The default selection is 6.1.

9.17 Microsoft SharePoint

When configuring a SharePoint endpoint, you must provide some details that are available from the **App Registration** in **Azure Active Directory**. When registering the application, you must keep the **Client ID**, **Client Secret** and the **Tenant ID** of the registered application. The application can be registered in a Single Tenant mode to access only SharePoint in that Active Directory.

Your SharePoint **SiteName** is located in your SharePoint address. For example, if you are in company.sharepoint.com/site/YourSiteName the SiteName "YourSiteName". If you do not see /site/ you can leave the SiteName blank as you are on the default site.

From there your **Document Library** can be specified, otherwise the **first Document Library** will be selected. Note the URL when viewing your document library in a web browser is not the correct name for the document library, it is the name above the content listed.

After you've filled out the necessary fields and configured your settings, use the Test button to verify the connection with the SharePoint site, validate that the provided Client ID, Client Secret and Tenant ID are accurate, and display the contents of the specified folder.

10 SFTP Server

10.1 Settings

Diplomat can act as an SFTP server, in which case it listens for connections from SFTP clients, whether those client applications are driven by automated processes or interactive human users. A successfully connected SFTP User can then attempt actions such as uploading a file to Diplomat, downloading a file from Diplomat, or otherwise managing the files and folders to which they have access through Diplomat to whatever extent their permissions allow. SFTP is a specific part of the SSH protocol suite. By design, no other SSH functions are allowed, such as shell access or SCP.

> **NOTE:** Before enabling the SFTP Server, you must have both an SFTP Key Pair and a root folder prepared.

To enable the SFTP Server, slide the ***SFTP Server Status*** switch to the right to turn it on.

If desired, provide the specific IPv4 or IPv6 ***Listen IP*** address on the Diplomat server computer that you want Diplomat to use when listening for incoming client connections. The default is 0.0.0.0, which represents listening on all present and valid TCP/IP interfaces. For example, if the Diplomat server computer has two address assigned, 10.0.3.55 and 10.0.7.30, then 0.0.0.0 would mean Diploamt listens for connections on both the universal localhost loopback address of 127.0.0.1 as well as the 10.0.3.55 and addresses. Otherwise specifying 10.0.7.30 would mean Diplomat listens *only* on 10.0.7.30. Providing an invalid IP address will result in Diplomat not listening on any interface.

Provide the ***Port*** on which Diplomat should listen for incomign client connections. The default port is 22, the standard for SSH. You may specify any port between 1 and 65535 that is not already occupied by another application. It is a good practice to either use the standard port 22 or else a port greater than 1024. Technically any otherwise unused port below 1024 is valid as well, but you may encounter compatiblity issues with some firewall or NAT devices when choosing non-standard ports below 1024.

Select the ***SSH Host Key*** from your list of SSH Key Pairs available in Diplomat. This will be the key Diplomat uses when accepting connections, and clients will automatically receive the pair's public half and associated fingerprint.

The ***SFTP Root Folder*** will be the storage location in which all user home folders will be created. This is referred to as the "Virtual Filesystem" (or "VFS") within Diplomat MFT. You can browse through attached storage or paste in a local path or UNC path to shared storage. The Diplomat service account should have full acess to the storage location. If the Diplomat service account does not have sufficient access, SFTP users will encounter errors when attempting to perform tasks they have permission to do in Diplomat but that Diplomat itself doesn't have permission to do on the storage.

Select the ***Default Permissions*** you want for new SFTP users to have in their home folder. Changing these values only changes which permissions are assigned to new SFTP users created after the change; it does not modify permissions for existing SFTP users.

If desired, you may set a ***SFTP Server Data Retention*** policy by checking the box to ***Automatically Delete Old Files*** and specifying the maximum age in days for files under the *SFTP Root Folder*. This option is useful to prevent the SFTP Server from being used as a long-term data respository. SFTP users and processes can often neglect to remove files that are no longer needed, leading to excessive reduction in available storage space as unnecessary potential security risks when sensitive data is left in place longer than required. Consideration must be given to balancing the usefulness of the system against minimizing the risk of storage utilization and unnecessary sensitive data housing. The automatic daily removal of files older than the age specified includes any symlinks created under the *SFTP Root Folder*.

If desired, you may modify the ***Authentication Policies*** for connecting SFTP users. You can modify the ***Set Password Policies*** details to specify the minimum number of characters for an SFTP user's password as well as whether and how many upper-case, lower-case, numeric, and special characters are required in a password.

You have the option to choose choose whether and how to handle ***invalid logins***, useful to mitigate the risk of a login attack. You can decide how many invalid login attempts over how many minutes will trigger Diplomat to take action, either locking out the user for a specified number of minutes or else simply disabling the user. A lockout will automatically expire after the specified number of minutes have elapsed since the most recent triggering action, requiring no further administrative or user intervention. If a user is disabled, on the other hand, a Diplomat administrator must explicitly take action to re-enable the individual user account.

You may also choose to ***Disable user after*** a number of ***days of inactivity***. This helps ensure that unused accounts are not overlooked and left enabled inappropriately. Similarly, you may also choose to ***Require password change every*** specified ***number of days***, ensuring policy compliance.

In the ***Advanced Settings*** you may choose the cryptography and compression settings Diplomat will use when servicing connected clients. The default values are generally a good balance of high security and broad compatibility at the time of release, with no deprecated technologies enabled and the highest security items having preferred status high in the list. To modify the values for *Key Exchanges*, *Ciphers*, *HMAC*, and *Compression* settings, uncheck a box to disable the item or check the box to enable it, and drag and drop an item higher or lower on the list to set its priority level versus other options.

During the initial negotiation with a connecting SFTP user, Diplomat and the SFTP client application attempt to arrive at a mutually agreeable set of values, attempting to use the highest priority selections first and only proceeding down the list of enabled values as long as it takes to either find a mutually agreeable value or else terminate the connection with an error if no agreeable values are available.

10.1.1 Edge Gateway

The ***Edge Gateway Settings*** panel (available if licensed) contains the settings required to enable the Edge Gateway. To enable the Edge Gateway, slide the ***Edge Gateway Status*** switch to the right to turn it on. Supply the host name or IP address in the ***Edge Gateway Address*** field and provide the PNC listening ***Port*** to configure

Diplomat to establish a connection out to that Edge Gateway. The default listening port on the Edge Gateway is 26841. Supply a uniqe ***Connection Identifier*** string that can be used for logging and auditing purposes. The automatically provided default is recommended, taking the form of *GWConnector-[computer_name]*.

10.2 SFTP Users

SFTP Users are the accounts used by connecting clients when the SFTP Server functionality is enabled. The concept and execution of these users has been kept very straightforward and streamlined by design. Few administrators need more complexity, and that complexity breeds numerous potential pitfalls for misconfiguration and even data leakage.

In the tree view you may create folders to help organize SFTP Users, dragging users and dropping them on to a folder as desired. Click on an SFTP User in the tree view to see their properties in the main window.

Right-click an SFTP User to ***Rename***, ***Delete***, or ***Move*** that account.

10.2.1 Create an SFTP User

To create an SFTP User, right-click the SFTP Users folder or a subfolder in the tree and select ***Create SFTP User***. The only value you're required to provide will be the ***New SFTP User Name***. Note that the name provided will be used to automatically create or associate that user's home folder under the *SFTP Root Folder* location. All other properties, authentication settings, permissions, and IP restrictions will be set later.

10.2.2 User Properties

Each SFTP User can be disabled either automatically or manually by changing the state of the ***Enabled*** box. The ***Username*** field shows which user's details you're viewing. The ***Last Access Time*** field shows the most recent login date and time, and the ***Access from IP*** field shows the IPv4 or IPv6 address from which the account most recently connected.

The ***Home Folder*** field is editable and reflects the current setting. Use caution when modifying this field, as it is a relative virtual path from the ***SFTP Root Folder***. Importantly, you also have the option to ***Restrict to home folder***. This is a vital security option and is enabled by default. When enabled, the SFTP User cannot navigate any higher in the directory structure. If disabled, they have access to the entire directory structure, which would be appropriate only for rare instances of internal administrator users or processes.

To provide an SFTP User more controlled access to paths outside their *Home Folder*, you may consider leveraging symlinks on the file system to lead to any other location that Diplomat can access.

10.2.3 User Authentication

When an SFTP User connects, Diplomat does not know which account will attempt to log in and whether that client has the correct credentials. Setting those credentials is a fundamental requirement for connecting users. For authentication you may require an account to use a password, a public key, or both.

To assign a password, check the ***Password*** box and provide a valid password to be used. If a password is already in place, such as when a user forgot their password, click the pencil icon to reset the password value. To force the user to reset their password to one of their own choosing, enable the option to ***Require password change at next login***. Uncheck the *Password* box to remove it as an option for the user's authentication.

To assign an ***SSH Key*** for Public Key Authentication, you must have already imported the user's public key so that you may then check the *SSH Key* box and select their key from the list. Both SSH Public Keys and SSH Key Pairs will appear in the list.

It is bad practice to create a key pair for another user and provide it to them. It is quite possible doing so violates policies and goes against regulations. A key pair is essentially a proof of identity. Any user familiar with using key-based authentication should already have that identity in place or create one themselves. Not only is there a much greater security risk of that identity being stolen when providing a key to a user, but it's also very possible that the application may not accept the private key format provided by Diplomat, and that key must be converted to some other format using third-party tools. Any user not familiar is likely to cost a large amount of time and effort to help them get set up. With creating key pairs for connecting clients, the risks are high while the rewards are low.

10.2.4 User Permissions

Refer to "SFTP Filesystem" for more information on setting folder permissions for an SFTP user account.

10.2.5 User IP Whitelisting

You may choose to enable the option to ***Restrict to IP Address(es)***. There may be one or more comma separated IPv4 values in that field. Values may be individual IP addresses or provided in CIDR notation to describe a given range.

This capability can be helpful to establish a greater degree of security. For example, if two competing firms are your clients, you may have to allow both their corporate IP ranges through your firewall. But the ability to *Restrict to IP Address(es)* means that even if a user at one firm gets the credentials for the other firm, those credentials cannot be used except from the proper firm's network. Attempts to connect from the competing firm's network or elsewhere will fail even with the otherwise correct credentials.

10.3 SFTP Groups

SFTP groups provides a mechanism to easily group SFTP Users together to define common permissions on the SFTP Filesystem.

Use this menu item to create, move, or delete a Group in the default SFTP Group folder. You can also right-click on any SFTP Group folder, subfolder, or SFTP Group entry in the Tree Navigator to access the options at that exact location.

10.4 SFTP Filesystem

Each SFTP user has their own view of the Filesystem managed by the Diplomat MFT server. The root of the SFTP Filesystem is defined in the "SFTP Server" settings. The configured physical path becomes the root path "/" in the SFTP Server Filesystem.

Each physical subfolder of that physical root path has an entry in the Diplomat MFT SFTP Filesystem. You can create, rename, or delete these physical paths from within Diplomat MFT or from the underlying filesystem itself.

You can also create a "virtual folder" within Diplomat MFT, which is a folder within the SFTP Filesystem that points to any other arbitrary physical path on the Diplomat MFT Server. For example, you can create a virtual folder "shared" underneath the user "foo" which points to the physical path for the home folder of the user "bar". In this fashion, both "foo" and "bar" can see the same files via "/shared" and "/", respectively.

Permissions

At each level of the SFTP Fileystem, you have the opportunity to assign specific permissions for users and/or groups. By default, all subfolders will inherit permissions from its root folder ("/"). At any level, you can uncheck

the box for "inherit" to put specific permissions onto that path, breaking the inheritance. You will be prompted to either remove or copy whatever permissions had been inherited previously.

All permission entries are treated as "allow" entries. For any given SFTP user attempting to perform an operation on a given folder, Diplomat MFT will check if any permissions (user or group) allow that operation at that level. As long as one permission entry allows that operation, Diplomat MFT will proceed with that operation. If not, a "permission denied" will be returned to the connected SFTP user.

11 Settings

Settings items allow you to specify global (system-wide) Diplomat configurations. Settings apply across the board.

11.1 Audit

Audit Trail data includes all data related to each file transfer job executed by Diplomat that attempts to transfer files. Audit trail data is used to generate Activity Reports. If a SQL database is used, Admin Users activity data is also recorded, and an Admin Activity Report becomes available. Refer to the separate *Diplomat MFT SQL Administrator Guide* in the Knowledge Base for a complete list of all tables and data elements captured.

Audit Settings

The *Audit Settings* section provides fundamental choices regarding whether Diplomat captures audit data, what type of database is used, and whether to take action if an error occurs during an attempt to write an audit record. *Audit Settings* cannot be opened or saved when an audit archive process is running. If an audit archive process is in progress, you will be prompted to choose if you want to stop it.

If you choose to ***Skip Audit Trail***, no audit records will be written. Use the ***Audit Trail Type*** dropdown to choose either the ***Standard*** lightweight embedded database or a customizable ***SQL*** database external to Diplomat. Most Reports in Diplomat are available regardless of which you use. If you want to create custom reports or import the data into Splunk or for any other use, you must select a database external to Diplomat.

When a SQL database is configured but has a problem, any administrator activity that would otherwise be recorded displays an error message to the user, an error message is written to the Diplomat log, and job processing continues normally. The error is **not** treated as a critical error by email, paging, and logging

If the option to ***Treat Failures as Critical*** is enabled then Diplomat will **SUSPEND ALL JOBS**, effectively stopping all automation. Suspensions must be manually released once the problem has been addressed; they will not release automatically. Therefore, only enable that option if an audit record is required for every file transfer job.

When such critical failure has occurred and global job suspension is in place, a pink status indicator is displayed next to the Transactions folder in the navigation tree. In addition, an orange status indicator is displayed next to all Transactions in the tree, as they have been indirectly suspended. The failure is treated as a critical error by email, paging, and logging. 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 separately.

Once the problem has been resolved, test jobs can be executed using the Run Now Button to confirm. Once confirmed, you must manually Release suspended transactions to resume normal operations.

SQL Audit Database

If you use an external database for auditing, you must configure its properties. When setting up the external database itself, you must configure it allow Diplomat to truncate data being written to fields that are shorter than

the string to be written. If Diplomat does truncate data, log entries will be written with a warning message and the complete string.

Note that changing SQL Audit Database settings while jobs are executing risks potential audit data loss. You may therefore be asked whether to temporarily suspend all jobs before updating the settings. If the new settings are unsuccessful, all transactions will remain suspended.

Select the ***SQL Database Type*** you are providing, whether Microsoft ***SQL Server***, ***MySQL***, or another ANSI SQL-92 compliant database with a ***Custom JDBC*** driver. Note that Linux systems may not support *SQL Server*. Provide the ***SQL Database Name*** (schema name for MySQL). Enter the ***Username*** and ***Password*** for authentication, unless using the Service Account for against a SQL Server. Provide the ***Host*** name or IP address and ***Port*** of the database server. Use the ***Authentication*** drop-down to select whether to use standard ***SQL Server*** or ***Windows*** authentication.

If you need to use a *Custom JDBC* database, such from Oracle, obtain a JDBC jar file from your database vendor and copy it to the installation directory under **..\tomcatWebserver\webapps\diplomat\WEB-INF\lib**. Enter the JDBC driver class name from the JDBC jar in the ***Custom Driver*** field. Refer to the documentation from your database vendor for more information if needed. Then provide the ***Custom URL*** associated with the specified *Custom Driver.* In that URL you may optionally use <HOST>, <PORT>, and <DBNAME> for your parameters, as they will then be replaced at run-time with the values in their respective *SQL Audit Database* fields. At run-time, authentication uses data from the *Username* and *Password* fields.

After entering the SQL Audit Database information, use the ***Test*** button to verify connectivity. The test button only tests that the specified *Host* and *Port* respond. It does not test authentication.

The ***Do Not Attempt Table Creation*** option is enabled by default. When first configuring Diplomat's Audit Trail Settings, uncheck that box to have Diplomat check for existence of the latest schema and attempt table creation for you if needed. Leave it checked if you have manually created and configured the tables beforehand, or for normally daily operations.

SQL Audit Archive Schedule
Archiving audit records is available when using an external database and may help increase both run-time job performance and Reports performance. When archiving, affected records are transferred to the archive tables in the database and deleted from the active tables. Use these options to determine whether and how to archive automatically.

Enabling ***Do Not Schedule*** disables archival. Disabling it enables archive. When enabled, an automatic daily process archives records based on the settings for **Archive By Days** or **Archive By Records** and written to the archive tables in the SQL audit database. When *Archive By Days* is selected, records older than the specified number of days are moved. If *Archive by Records* is selected, any records beyond the number specified are moved. All records for a given day are moved as a block to the archive tables in the database, even when *Archive by Records* is selected. Thus, the active and the archive audit databases never contain a partial day of records, and records for the current day are never archived.

When scheduled archival is enabled, you may also invoke that process using the ***Archive Now*** button. If an audit archive process is already in progress when you use the *Archive Now* Button, you are asked if you want to stop it.

11.2 Backup

Backup settings determine the backup directory and encryption options, whether Admin Users are prompted to perform a backup when signing out, and whether automatic daily backups are enabled.

To be prompted to perform a backup when signing out, enable the ***Backup Reminder on Exit*** option. Browse localh storage for where to use as the ***Backup Directory*** or paste in a UNC path to which Diplomat has access. Use the **Test** button to confirm the location is accessible.

The option to ***Encrypt Backup Files*** is disabled by default. If you choose to use it, the time and storage space taken by a backup file increase. Provide a ***Backup Password*** and again to confirm. Backup files created during the period between the start and end dates require entry of the associated password to merge or restore. You can use the Show Password History to view each backup password used and its associated start and end dates.

Unless you choose to ***Turn Off Daily Backup*** Diplomat will take a backup every day at midnight. You can change the ***Time of day*** the backup files are created and specify the desired number of days to ***Retain Backup Files For***. All files ending in .dbu in the active *Backup Directory* modified date older than the configured number of days are deleted each daily.

11.3 Calendars

Calendars are optional and used to specify dates that require special handling by the Diplomat Scheduler. Calendars can be used to exclude specified dates. For jobs that recur on a daily, weekly, or monthly schedule, calendars can also be used to run jobs the business day before the specified date or the next business day after the specified date.

You can ***Add***, ***Delete***, ***Edit***, or ***View*** selected calendars. The ***Calendar Name*** is the name that appears when selecting a calendar for a transaction, while the The ***Description*** field allows for short in-app documentation.

When you *Add*, *Edit*, or *View* a Calendar, you can choose the *Non-Business Days* days of the week. The *Holidays* table displays the name and dates of currently specified holidays, if any. When creating a calendar, a combination of non-business days and holidays may be specified. You may *Add* a new holiday name and date to the holidays table, or use the ***Add US Holidays*** button to add all official US holidays for the specified year. You may also *Delete* individual holidays from the Holidays table or *Delete Past Dates*.

In main Calendars view, you can select and *Edit* a previously created calendar or *Delete* it. Otherwise you may simply wish to View the names and dates of the non-business days and holidays in the selected calendar along with any Transactions using the selected calendar.

11.4 Email

In order to send email notifications or use Email as a Transport Method, you must provide Diplomat with the details of the email server(s) to be used.

The ***Receiving*** settings are only used to retrieve attachments in Transactions. To do so, select the ***Server Type***, the ***Email Server*** host name or IP address and ***Port*** to use, provide the ***Account*** username and ***Password***, and specify the ***Encryption*** to use. When complete, use the ***Test*** button to test the connection and authentication.

The ***Sending/Notification*** SMTP settings are required to send email notifications and to send attachments in Transactions. Set the SMTP ***Email Server*** host name or IP address and ***Port***, the ***Sender Address*** for the FROM field, and the ***Encryption*** to use. Consult your mail server administrator for assistance. If ***Authentication Required*** to send through that mail server, enable that option and provide the ***Account*** username and ***Password***. You may also set the ***Delay Time*** between sending email messages to avoid overwhelming the mail server or even getting blocked as a suspicious actor. You may also modify the ***Max Email Size*** supported by the sending mail server. When an outgoing message is near that size, a non-fatal error will be written to the Diplomat log. Beyond that size, email notifications will be truncated. The total size of email message, including attachments, must be less than the *Max Email Size*. You may encounter a circumstance where a 3rd party recipient's mail server has lower limits.

When configured fully, press the ***Test*** button to confirm connectivity and, if required, authentication.

The ***Job Status Notification Subject*** field to is used for notification emails to both Business Recipients and IT Support. The default template is '<STATUS>: <TRANS_ID> <STATUS_TEXT> at <Mmmm> <DD>, <YYYY> <hh>:<mm>:<ss> <AMPM>'. Beyond the Date Variables, available parameters are <Trans ID> for the name of the Transaction, <STATUS> for the final status of the job, and <STATUS_TEXT> for a description of the final job status.

Values for status and status text parameters include:

Status	<STATUS>	<STATUS_TEXT>
Cancelled	FAILURE	was cancelled
Critical	CRITICAL FAILURE	failed
Failure	FAILURE	failed
File(s) Not Found	RETRY	N/A
Successful	SUCCESS	was successful
Terminated	FAILURE	was terminated
Warning	WARNING	was successful with a warning

11.5 FTP

The FTP protocol requires multiple connections to complete a directory listing or file transfer, causing additional complications. Diplomat will typically use Passive (PASV) mode, while there may be occasions where the older Active (PORT) mode is needed. In Active mode, the FTP server attempts an outbound connection to an IP address and port provided by Diplomat. Therefore leaving the option enabled to automatically Use Default IP Address and Use Default Port will nearly always fail in FTPS and is unreliable with cleartext FTP.

To use this option, you must configure your NAT and Firewall devices with static rules to explicitly forward incoming connections on a specific range of ports to the Diplomat server. Then specify the proper external ***IP Address*** and ***Port Range*** in Diplomat, with the ***Start*** of the range to the ***End*** of the range.

11.6 IT Support Email Notification

Email notifications to IT personnel are a crucial means of both visibility and quick access to troubleshooting information. They are intended for use in diagnosing system and network problems that are causing jobs to fail. They may be sent to individual inboxes, group aliases, or the inbox for ticketing and other systems to automatically open a new trouble ticket when messages are received with debug logs generally included. Note that when the total email size exceeds the *Max Email Size*, the email is truncated while the complete job log is written to a file referenced in the email message in the Troubleshooting folder.

Provide the ***Email Addresses*** to be notified, select the desired Notification Type, and choose whether to ***Send Status Email*** in case of ***Service Restart*** or ***Key Expiration***. For key expirations, notifications are sent 90 days, 60 days, 30 days, and 7 days prior to expiration, then daily thereafter.

Use the ***Add Notification*** (+) button to add and configure as many email notification recipients as you need.

11.7 Job Monitor

The ***Job Monitor Settings*** control and count the number of job history records available for display by the Job Monitor. The records are stored for a number of jobs per transaction or a specific number of days. Specify the desired number of ***Jobs per Transaction*** or ***Days*** to retain the records. You can also keep an eye on the ***Total Job History Records Available***. The option to ***Display Detailed File Status*** determines whether the Job Monitor shows only basic Getting Source and Complete status in parenthesis or a more detailed sub-status, adding Preparing File, Putting Destination File, and Archiving File.

Setting the ***Job Monitor Update Rate*** value controls the number of seconds between refreshes of data displayed in the Job Monitor. Too small an interval could increase the load on the server.

NOTE: Job History is stored in an embedded database. You can execute runJobHistoryDb at the command line on the Diplomat MFT server to manually view the contents of this database.

11.8 Job Queue

Job Queue settings affect the scheduling and execution of Diplomat file transfer jobs.

When the Diplomat MFT Service starts, all Diplomat Transactions are scheduled based on the information provided in the Job Execution settings of the Transaction. Transactions that are scheduled to run Daily or Monthly start at the exact time provided whenever possible. Those scheduled by Seconds, Minutes, or Hours run the initial job shortly after the Diplomat Service starts. To avoid a glut of jobs running at once and a long queue of jobs awaiting execution, the default is to add one second between job starts. To increase or reduce the time between job starts, change the ***Delay between initial job starts*** setting. Changes take effect on the next Diplomat service start.

If needed to optimize performance, change the ***Maximum number of concurrently running jobs***. The default setting is 50. Diplomat jobs are spawned in separate threads and distributed across all processors on the server. Only increase this setting if the Diplomat server has the resources needed for additional concurrent jobs.

11.9 Logging

Diplomat creates log files with chronological entries about every action that Diplomat Managed File Transfer takes during its operation. Log files are text files and can be viewed using File Menu or third-party tools. You can set the level of information to capture, the location of the log files, and archival/retention parameters. Certain types of errors impacting all transactions *cannot* be logged, such as if the Diplomat service is killed or terminates unexpectedly.

Log filenames are in the form: 'Diplomat.year + month + day + hour + minutes + seconds.log'. For example, a log file created on September 22, 2004 at 1:19:20 p.m. would be named 'Diplomat.20040922.131920.log'.

To set the ***File Location*** of the log files, browse the attached storage or paste the desired UNC path. Use the **Test** button to verify the location is accessible. Note that if the folder does not exist, Diplomat attempts to create it. If Diplomat MFT is successful in creating the directory, the job continues as if the directory had already existed. You can also set the level at which system messages are logged. Levels are described below.

- ***Full*** includes *all* system messages.
- ***Debug*** includes all system messages, except for large messages such as directory listings.
- ***Informational*** includes all informational notations. This is the recommended minimum setting.
- ***Warning*** includes any problem that might have affected the integrity of the file(s) being transferred for *an individual job*, such as:
    - Error closing a file

  - Error deleting an uploaded file after a problem during transmission
  - Decryption or verification key is not valid for current date
  - ASCII file size not within tolerance
- ***Error*** includes only a problem that causes a failure of an individual job. For example, the FTP server specified in the transaction does not exist or the specified key pair did not decrypt a downloaded file.
- ***Critical Error*** only includes problems that impacts the encryption, decryption, or file transfer *of all jobs*. Action must be taken immediately. For example, if the audit file is marked as Treat as Critical on the Audit settings screen and the specified audit database does not exist.

The ***Archival and Retention*** options set the log rotation parameters and how long Diplomat waits to delete old log files. When a log file is archived, Diplomat MFT automatically creates a new log file. Diplomat can automatically archive log files that are larger than a specified size or older than a number of days. The current log file is always archived each time the Diplomat service starts.

Set the ***Archive Log Files Over*** value to automatically archive the current log file when it grows too large. The ***Archive Log Files Every*** value automatically archives the current log file when it's too old but has not yet become too large. Use ***Retain Archived Log Files For*** to purge all archived log files that are too old. Only log files with names conforming to 'Diplomat.*.log' are deleted, and only in the currently configured *File Location*.

You may also use the ***Performance Logging*** value to adjust the interval to write performance information to the Diplomat log file. That performance information consists of details such as a list of active threads, the number of jobs running or queued, and memory usage. Select '0' to disable *Performance Logging*.

11.10 OpenPGP Keys

The ***Default Decryption Key*** is the OpenPGP Key Pair used to pre-fill the *OpenPGP Decryption Key* field in all new Inbound Transactions when the Destination Partner Profile doesn't already have such key information defined.

The ***Default Signature Key*** is the OpenPGP Key Pair used to pre-fill the *OpenPGP Signature Key* field in all new Outbound Transactions when the Destination Partner Profile doesn't already have such key information defined.

The ***Default Additional Encryption Key (AEK)*** is used to pre-fill the *Additional OpenPGP Encryption Key(s)* field in all new outbound transactions. This can be useful when you want all *Encrypt* actions to include your key so that they may be stored encrypted for security reasons. The AEK will be a secondary key that can decrypt the files later.

11.11 Paging Notification

The Paging Notification screen allows you to send a pager notice if the Diplomat has a problem during its operation. Paging notification is triggered when an event occurs that meets or exceeds the *Minimum Level to Page*. The default ***Paging Type*** is ***No Paging***, disabling this function. Select *Email* if your paging application generates pages from email messages and you have configured your Sending/Notification Email settings. Otherwise choose *File* if your paging application generates pages from files.

The Minimum Level to Page defaults to ***Critical Error***, for any problem that impacts the encryption, decryption, or file transfer *of all jobs* such that Action NEEDS to be taken immediately. ***Error*** will also initiate a page for any problem that causes a failure *of an individual job.* ***Warning*** adds a page for any problem that might have affected the integrity of a file being transferred such as a problem closing a file, deleting a source file, an ASCII file size is not within tolerance, and other such errors. ***Success*** adds pages for all jobs except those with a status of Cancelled or Terminated, while ***All*** adds those in as well.

For the ***Email*** *Paging Type*, set the target ***Email Address*** used by your paging application and the desired ***Email Subject*** for the messages sent. You can also choose whether to ***Use Custom Message*** as defined in the *Custom Messages* section or leave it disabled as per the default. If not checked, Diplomat will send the auto-generated <MESSAGE TEXT> as the body of the email message.

For the ***File*** *Paging Type*, you must define the ***Primary Location*** and ***Secondary Location*** where your paging application looks for files during normal operations or when the primary location is not available, such as in a disaster recovery scenario. When a secondary location is provided, Diplomat writes paging files to both the primary and the secondary location. The filename used defaults to 'DiplomatPage.<TIMESTAMP>.txt', and you may also choose to include the Transaction Name with '<TRANS_ID>' or the completion status as '<JOB_COMP_STATUS>' in the filename.

The ***Custom Message*** allows you to provide a ***PIN Number*** or PID belonging to an on-call recipient of the paging message, set the ***Max Message Length*** allowed in a paging message, including '0' for unlimited, and the ***Message Template***. You can include any text you would like in the message as well as the <PIN Number>. The <Message Text> is the same text as contained in the body of a debug email message, truncated to *Max Message Length*, and is included by default.

11.12 Primary Archive

Diplomat can create an archive copy of all files that are transferred by a Transaction. The *Primary Archive Settings* allow you to choose whether and how those archives function. The default configuration enables the *Primary Archive* for the original Destination versions of files for Inbound Transactions and Source versions for Outbound Transactions. These files will be zipped together for each successful job, and any files that fail to transfer will not be included since they will be archived later if they are successfully completed. Archiving occurs directly after each file transfer during a job. When each file transfer is complete, the source file, the destination file, or both files are archived.

Enable the option to ***Turn Off Primary Archiving*** ONLY if you want to skip this entire archive process.

You may specify a desired ***Primary Location***, which can be an attached storage or network share to which the Diplomat service has access. It should contain ONLY files archived by Diplomat. Use the ***Test*** button to determine whether the location is accessible. You may also choose whether to ***Add transaction-specific sub-directories***, which is enabled by default to assist with organization and prevent the *Primary Location* from accumulating an excessively large number of files.

Default names for individual archive files, whether or not they're contained in a zip, include the original file name and extension along with which version of the file was archived and the date and time at which the archive copy was created. A destination archive file is '<FILENAME>.<EXT>.dest.<YYYY><MM><DD>.<hh><mm><ss>.<ms>.da' while source archive files is '<FILENAME>.<EXT>.srce.<YYYY><MM><DD>.<hh><mm><ss>.<ms>.da' with the .da extension simply being an indicator they are a Diplomat Archived file. For example, an archive of the destination version of the file 'Example.txt' created on February 11, 2022 at 2:41:38.017 PM would be named 'Example.txt.dest.20220411.144138.017.da'.

Zipped archive files have default names 'DiplomatArchive.<TRANS_ID>.<YYYY><MM><DD>.<hh><mm><ss>.<ms>.zip'. For example, a zipped archive file for transaction 'Example Bank Transfer' created on February 11, 2022 at 2:41:38.021 PM would be named 'DiplomatArchive.Example Bank Transfer.20220411.144138.021.zip'.

Because these file names are designed by default to be unique, ***Do Not Overwrite*** is enabled by default. If archive files cannot be written because an existing file has the same name, the job processes the files, but ends with a FAILURE status. If this occurs, you should recheck the filename parameters to ensure that unique names are

generated. If *Do Not Overwrite* is unchecked and the parameters in the *Source*, *Destination* or *Zip* Filename fields allow it, then jobs with multiple files could write different archive files with the same name and only the last file would be archived.

In the ***Primary Archive File Selection*** panel, you can choose whether source, destination, or both types of files are to be archived. For ***Inbound File Types*** the default is the original file as it came from the ***Destination***, while ***Outbound File Types*** archive the original file as it was in the ***Source***. If all Outbound Transactions use Encrypt, *and* you use your own private key as an AEK, then you may choose to archive only *Destination* files for Outbound. All primary archive files would be encrypted, but you can then decrypt them as needed with your own key. Regardless, Diplomat will ***Zip Archive Files*** generated by the job into a single zip file by default. If zipping the files is not successful, the individual archive files are **not** deleted.

The ***Primary Archive Handling*** section lets you choose to ***Attempt Archive on*** which job result, with a default value of 'Success and Warning'. However, the option to ***Delete source files on primary or additional archive failure*** controls whether source files themselves are allowed to be deleted by the Transaction's *Post-transfer action* when Diplomat MFT is unable to write archive files to either the primary or additional archive location. When enabled, source files are allowed to be deleted only if destination files were written successfully and the only job error is the archive failure. This option is disabled by default.

The ***Primary Archive Retention*** options ONLY affect files in from the primary archive location and its sub-directories. Files archived in an individual transaction to an additional location other than the *Primary Location* are **not** deleted automatically. For the *Primary Location*, this option helps minimize concerns of continually increasing storage utilization and help prevent unnecessary retention of sensitive data. However, because this is destructive and could be undesirable for some, the option to ***Automatically Delete Archive Files*** is disabled by default. If enabled, use the ***Retain Files For*** field set the number of days that you would like to keep primary archive files. The default value is 30 days. **All files** in the currently specified *Primary Location* older than the specified number of days are deleted, so only Diplomat archive files should be stored there.

11.13 Proxy Servers

The Proxy Server settings screen displays a list of proxy server definitions available for use when setting up Partners and transactions. An asterisk indicates which, if any, of the proxy servers is the default proxy server.

Use the ***Add Proxy Server*** button to create new proxy server definitions. Specify the desired display ***Name*** and ***Description*** to be used for the proxy server. Then provide the ***Address***, ***Port***, ***Username***, and ***Password*** for the proxy server. The ***Proxy Protocol*** used to establish a connection to the proxy server is set to HTTP. If desired, check the box to make it the ***Default Proxy Server***.

In the main ***Proxy Servers*** window, you can use the ***Delete***, ***Edit***, and ***View*** buttons to perform their respective actions on the selected proxy server from the list.

11.14 Session Management

Set the Diplomat MFT Client session expiration time in minutes. If you do not want Diplomat MFT Client sessions to expire, set the expiration time to "0" minutes. Default is 9 minutes.

11.15 Admin Users

In Diplomat MFT Enterprise Edition, the ***Admin Users*** settings displays user account information and enables the creation and management of Admin Users that can manage Diplomat MFT and access the Job Monitor.

The ***Contact Name*** is the given full name of Admin User associated with the account. The ***Privilege Level*** denotes whether the user is an *Administrator, Manager* or *Reviewer*. ***Administrator*** privilege level includes the ability to change server settings, activate a new Diplomat MFT license, and perform merge or restore functions. A ***Manager*** privilege level allows only access to the tree navigation, such as for the set-up and running of file transfer jobs and associated objects. A ***Reviewer*** has read-only access to the tree navigation, without the ability to run file transfer jobs.

The ***Username*** is the actual name used to login with that account. When choosing to ***Add*** a new Admin User, it is required to set their initial password. If a user forgets their password, *Administrators* can select an account and use the ***Edit*** button to set a new password for them. Otherwise when an account is no longer needed, the ***Delete*** button will remove them.

The ***Authentication Policies*** allow specifying whether Admin User accounts will *Use Case-Insensitive Authentication* when signing in. Only disable this option if you require that entered usernames be case sensitive. In versions prior to 9.0, this option was disabled by default. In 9.0 this was changed by popular request to be enabled by default.

Password Policies define the fundamental requirements for Admin User passwords. The ***Minimum Password Change Frequency*** applies to all Diplomat MFT Admin Users and can be set to 3 months, 6 months, or 1 year. If you do not want users to be prompted for regular password updates, select ***None***. You may choose the ***Password Format*** requirements for any future Admin User creation or password changes, including the ***Minimum Number of Characters***, whether ***Passwords must contain both uppercase and lowercase letters***, whether ***Passwords must contain both alpha and numeric characters***, and whether ***Passwords must contain at least 1 special character***.

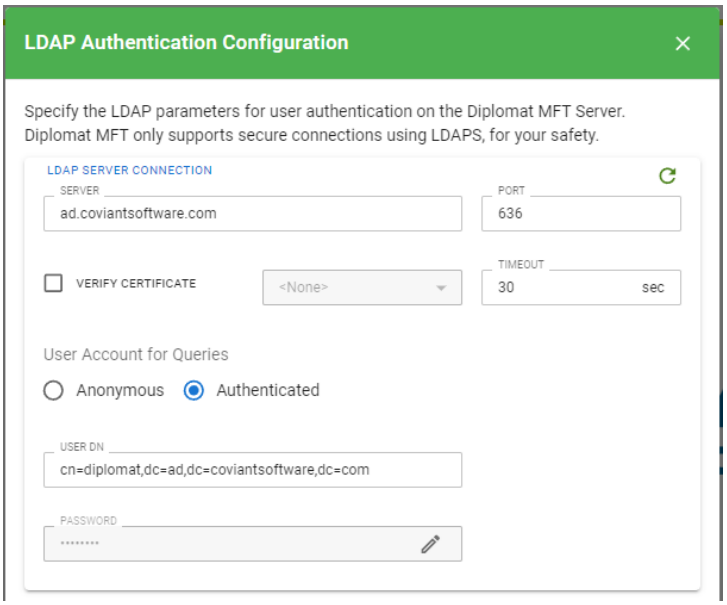
NOTE: Password format changes do not affect existing passwords and are used to validate new passwords only.

11.16 LDAP

Diplomat MFT can connect to an LDAP server, such as Microsoft Active Directory (AD), to authenticate users. You can configure this option for Admin users, SFTP users, or both. When configuring Diplomat MFT to use LDAP authentication, you specify the LDAP server configuration once, and then specify the LDAP query parameters for Admin Users and SFTP Users separately. This is useful, for example, if you have created on group on AD to hold the Diplomat MFT Admin users, and another group on AD to hold the SFTP users.

When Diplomat MFT attempts to authenticate a user account that comes from AD, the authentication request is passed to the LDAP server as a **bind** operation. This **bind** operation will use the full dn of the entity where the supplied username matches the LDAP Username attribute configured in the settings. If the username and password supplied to Diplomat MFT during an authentication attempt are approved by the AD server, then Diplomat MFT will authorize that user and apply whatever permissions to that user account which are configured in Diplomat MFT.

11.16.1 LDAP Server Connection



Supply the LDAP server connectivity details for Diplomat MFT to connect to and make queries from the LDAP server.

Server
Provide the domain name or the IP address for the LDAP Server.

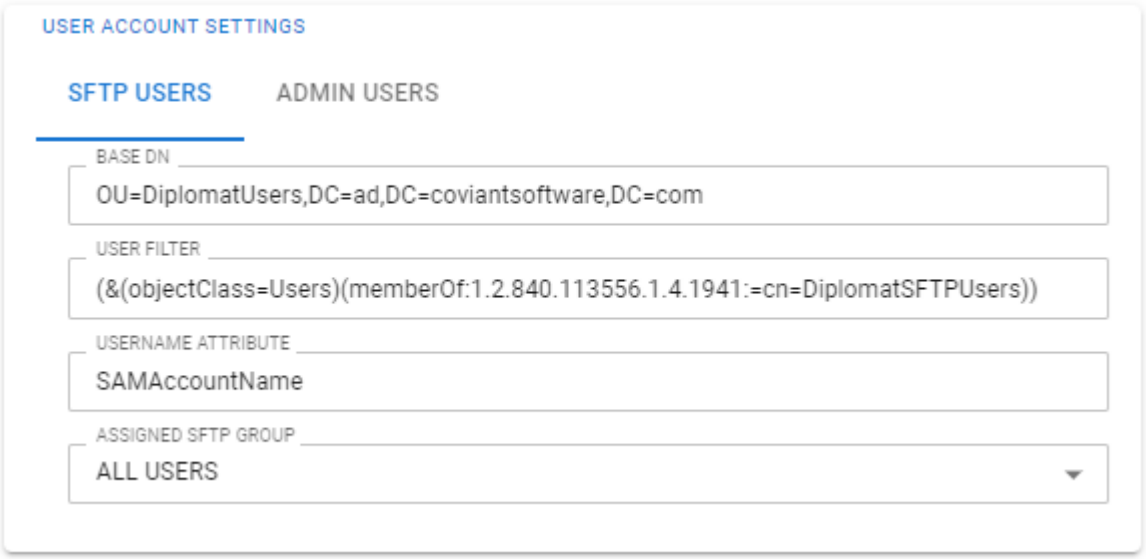
Port
Provide the port on the LDAP server to which Diplomat MFT will connect. Diplomat MFT only supports LDAP over SSL (LDAPS) for the highest levels of security. The default port for LDAPS is "636".

Verify Certificate
If you wish to verify the SSL Certificate provided by the LDAPS server, check this box and choose the matching server SSL Certificate from this list. You will need to first **import** that server SSL Certificate into the appropriate "Keys" folder for it to appear in this list. See "Import SSL Certificate" for more details.

Timeout
The number of seconds Diplomat MFT will wait for a connection or query response before timing out the operation and logging an error.

Authentication
To make authenticated queries against the LDAP server, provide the authentication details here. When supplied, Diplomat MFT will authenticate ("bind") to the LDAP server as this account when making the user queries specified in the SFTP and Admin Users settings.

11.16.2 SFTP User and Admin Account Settings



The "User Account Settings" configuration applies to both "SFTP Users" and "Admin Users." Both sets of configuration contain nearly identical configuration options. They are separated to provide you the ability to assign LDAP users to either SFTP or Admin user accounts, and to vary the LDAP query that is used for each (for example, you create two different groups in AD, one for SFTP users and one for Admin users).

Base DN
Specify the Base DN for all queries to the LDAP server. Diplomat MFT will search for matching entities at this level and below (i.e., a *subtree* search)

User Filter
The filter is used to identify which LDAP entities are to be included in Diplomat MFT as SFTP Users. For example, in Active Directory, to add all AD members of the group "DiplomatSFTPUsers" to Diplomat MFT as SFTP users, you can use a filter such as:

```
(&(objectClass=Users)(memberOf:1.2.840.113556.1.4.1941:=cn=DiplomatSFTPUsers,
ou=Groups,ou=Users,dc=ad,dc=coviantsoftware,dc=com))
```

(the "1.2.840.113556.1.4.1941" attribute is a handy trick that tells Microsoft AD to look into nested groups as well).

Username Attribute
Specify which attribute from the LDAP server will represent the SFTP username within Diplomat MFT. A common value is "sAMAccountName", which is what most AD users will use to log into an AD server. Other values that might be used is "userPrincipalName", which looks like an email address (e.g., "testuser@coviantsoftware.com").

Assigned SFTP Group (SFTP Users only)
Select which group to which we add the SFTP users that are pulled from the LDAP server.

Assigned Role (Admin Users only)
Select which Diplomat MFT Admin role to which we add the Admin users that are pulled from the LDAP server.

12 Jobs

12.1 Jobs Overview

A job is a particular execution of a Transaction. For example, if a Transaction is scheduled to run each day, a new job is executed every day. In Diplomat MFT Enterprise Edition, you can suspend jobs or release suspension and enjoy the visibility provided by the Job Monitor. The Jobs menu provides access to enhanced real-time job control features with the ability to suspend, monitor, cancel, terminate, and/or run jobs.

12.2 Jobs Menu Items

12.2.1 Release

The Release menu items re-enable job execution after one or more Transactions have been suspended either directly or indirectly. All *Release* choices can be executed by right-clicking on the object to be released in the navigation tree.

You can release jobs for ***All Transaction Directly*** for any directly suspended transactions, the ***Transaction Folder*** for all transactions indirectly suspended by folder, including specifically the ***Inbound Transactions Folder*** or ***Outbound Transactions Folder***.

When you suspend a Key or Partner, all Transactions using that Key or Partner are suspended. Release the selected ***Active Key*** or ***Active Partner*** to enable processing of all associated Transactions. Similarly, if a selected Transaction has been suspended directly, re-enable processing with ***Active Transaction***.

As a special case, when *Treat Failure as Critical* is selected in the Audit Settings, an audit trail error suspends all job processing, and a pink status indicator '■' is displayed next to the Transactions folder in the navigation tree with an orange status indicator '■' for all Transaction objects. Once the problem has been resolved, restart suspended transactions using ***Release Critical Audit Suspend***. Other existing direct or indirect suspensions will remain.

When you merge or restore from a Backup, all jobs are suspended during the operation. For Diplomat MFT Enterprise Edition, you have the choice of whether to release that suspension or wait until later. This is especially helpful when migrating servers or as part of a disaster recovery exercise. In this case a purple status indicator '■' is displayed next to the Transactions folder in the navigation tree with an orange status indicator '■' for all Transaction objects. When you're ready, you can choose to ***Release DB Merge/Restore Suspend***. Other existing direct or indirect suspensions from the backup will remain.

12.2.2 Suspend

The Suspend menu items stop job scheduling. Any jobs that are currently queued or running when a Suspend action is taken still complete normally, but no further jobs are scheduled until suspension is released. An orange status indicator '■' denotes indirect suspension while yellow '■' denotes direct suspension. Not that all disabled Transactions continue to display a red status indicator '■'. The indicator in the Job Monitor for an actively running or queued Transaction does not change until the job completes. All *Suspend* choices may also be executed by right-clicking on the object to be suspended in the navigation tree.

When suspending ***All Transaction Directly***, each transaction is individually directly suspended. Otherwise you can suspend the entire ***Transactions Folder***, the ***Inbound Transactions Folder***, or the ***Outbound Transactions Folder*** to indirectly suspend all relevant Transactions.

You may instead suspend the selected ***Active Key*** which directly suspends all Partners or Transactions that use it, the ***Active Partner*** which indirectly suspends all Transactions that use it, or the ***Active Transaction*** itself.

12.2.3 Job Monitor

See Job Monitor

13 Job Monitor

In Diplomat MFT Enterprise Edition the Job Monitor allows you to view current scheduling status and the job history of all transactions. The amount of job history data available for display by the job monitor is determined by the **Job Monitor Settings.**

The job monitor main screen shows an Inbound Transactions table, an Outbound Transactions table, and a Summary table. The Inbound and Outbound Transactions tables show current data on each transaction. The summary table provides a snapshot of the status and the last completion status of all jobs. At the bottom of the main screen, a ticker field displays the most recent refresh time for the values in the job monitor tables and a *Pause* button that can temporarily suspend the refresh of the values in the job monitor tables. The time displayed in this field is based on the system clock of the system running the Diplomat MFT Service.

13.1 Inbound/Outbound Transactions Table

Each table displays the ***Transaction Name***, transaction status, start time, elapsed time, job status, number of files found/processed, job execution attempt, time the next attempt is scheduled, and the time the next job is scheduled. Each table can be sorted by clicking on the title bar of the column by which you would like to sort. Ascending or descending sort order is indicated by up or down arrows in the title bar.

To run a job, right-click on the *Transaction Name* cell and select ***Run Now***. Run Now is available only if a job is not already executing. When *Run Now* is executed from the Job Monitor, any unsaved changes to the Transaction are ignored.

To cancel a job, right-click on the Transaction Name cell and select ***Cancel Job***. If a job is already canceling, a red slash appears across the icon. *Cancel Job* is available only if a job is currently executing. If you have requested that a job be cancelled and the job is still executing, you can take an additional step to terminate the job. To terminate a job, right-click on the Transaction Name cell of a transaction that is 'Canceling' and select ***Terminate Job***. If a job is terminating, a red 'X' appears across the icon. *Terminate Job* is only enabled if a job is currently cancelling.

> **NOTE:** Terminating a job attempts to stop execution immediately. Some or all files may not have been transferred completely or at all. Email notifications may not be sent, and audit trail records may not be written. Also, terminating a job may leave system resources locked. **Terminate a job only if necessary.**

If you need detailed debugging information for a job, right-click on the *Transaction Name* cell and select ***View Log***. The *Diplomat MFT Log Viewer* opens and displays the most recent log entries for the transaction. To adjust the log entries displayed, select *Set Filter* and reset the filter parameters as described in Logs. *View Log* is only displayed when a transaction has run within the window available to the Job Monitor.

If you need information on earlier jobs from a transaction, right-click on the Transaction Name cell and select ***View Job History***. A *Job History* window opens and displays all job records for the transaction in the job history database. Each job execution shows start time, elapsed time, job status, total bytes transferred, number of files found, number of files transferred successfully, number of files that did not transfer successfully, and the number of executions that were attempted by the job.

If you need more information on the files in a particular job, right-click on the Transaction Name and select ***View File History***. A *File History* window opens and displays all file records for the transaction in the job history database. Each row displays source filename, destination filename, start time, elapsed time, file status, source file size, and the number of attempts that were made to transfer the file successfully.

The ***Transaction Status*** indicates the current scheduling status of the transaction. Valid values are:

- *Not Scheduled*: Do Not Run checked and/or no job scheduling types are set/allowed on the Job Execution panel.
- *Directly Suspended*: Key, Partner, or transaction individually suspended.
- *Indirectly Suspended*: Key, Partner, or individual transaction suspended because:
  - Key or Partner used by the transaction is suspended
  - Folder is suspended.
  - Critical audit database problem has suspended all transactions.
  - Database merge or restore has suspended all transactions.
- *External Request*: Allow Diplomat MFT Scripting Agent requests or Allow Diplomat MFT API requests checked on the Job Execution panel of the transaction.
- *Scheduled*: Job scheduled to run at a specific time.
- *Monitoring*: Job set to use file monitoring.

NOTE: Only transactions that display a *Transaction Status* of *External Request, Scheduled or Monitoring* will execute.

Start Time
The date and time that the most recent job began execution for this transaction. If no job history exists for the transaction and a job is not currently executing, this field is blank.

Elapsed Time
The length of time in seconds that the current or most recently completed job has run. If no job history exists for the transaction and a job is not currently executing, this field is blank.

Job Status
Job Status displays status of the most recent execution of the transaction. If no job history exists for the transaction and a job is not currently executing, this field is blank.

If a job is currently executing, valid values are:

- **Delayed** — Job executed using a Diplomat MFT Scripting Agent command with a <delay> parameter.
- **Queued** — Job waiting in queue for execution.
- **Running** — Job actively executing. This value has sub-status shown in parentheses of:
  - Building File List
  - Verifying File List
  - Processing Files
  - Sending Emails
  - Sending Pages
  - Waiting for Retry
  - Writing Audit Trail
- **Cancelling** — Request to cancel job occurred, but job is still executing.
- **Terminating** — Request to terminate job occurred, but job is still executing.
- **Aborting** — Unrecoverable error encountered.

If a job is not currently executing, valid values are:

- **File(s) not Found** — No files were found on the most recent execution and transaction was **not** set to Fail if File(s) Not Found.
- **Required File(s) Not Found** — Some files were found on the most recent execution, but one or more required files were **not** found and transaction was **not** set to Fail if File(s) Not Found.
- **Successful** — Most recent execution completed successfully. Email and other notifications indicate the job was *Successful*.
- **Warning** — Job completed successfully, but had at least one error that might have affected the integrity of the file(s) being transferred. Examples of problems generating a Warning status, include:
  - Error closing a file
  - Error deleting an uploaded file after a problem during transmission
  - Decryption or verification key is not valid for current date
  - ASCII file size not within tolerance

  NOTE: Source files with a Warning status are NOT deleted.
- **Failure** — Most recent job execution did not complete successfully. Email and other notifications indicate the job was *Failure*.
- **Critical** — Job failed due to a problem with the audit database and audit trail settings set to T*reat Failures as Critical*.
- **Cancelled** — Job manually cancelled on most recent execution.
- **Terminated** — Job manually terminated on most recent execution.
- **Incomplete** — Diplomat MFT Service stopped during job execution.
- **Missed** — Jobs are flagged as missed, when *Fail if File(s) Not Found* is checked and:
  - Diplomat MFT Service not running when last job execution scheduled.
  - Job queued, but execution had not started, when Diplomat MFT Service stopped unexpectedly.

Number of Files Found/Processed

Number of files found for the current or most recent job execution and the number of files that has been processed by the job. For jobs that complete successfully, the number of files found should be the same as the number of files processed.

Job Execution Attempt

For transactions that are scheduled daily or monthly and have retries specified, each time the job reattempts to find files the number of job execution attempts increases.

For example, a job is scheduled to run at 1PM each day and to make 4 attempts with a 15 minute retry intervals if it does not find files. If the job started at 1PM and the current time was 1:35PM, the job would have made an attempt at 1PM, 1:15PM, and 1:30PM and would be waiting for final attempt at 1:45PM. The number of job execution attempts shown at 1:35PM in the job monitor would be 3.

NOTE: This field is always '1' for jobs that are schedule by minutes or hours.

Next Attempt Scheduled

For transactions that are scheduled daily or monthly and have retries specified, when a job does not find files a new attempt is scheduled. Next Attempt Scheduled displays the date and time the next attempt is scheduled.

Next Job Scheduled

For transactions with a Transaction Status of Scheduled, the Next Job Scheduled field displays the date and time the next job is scheduled to begin execution.

13.2 Summary Table

The summary table provides a snapshot of the current status and the last completion status of all jobs broken down by inbound and outbound jobs.

Current Job Status

- **Total** — Total number of inbound and outbound jobs in Diplomat MFT transaction database.
- **Executing** — Number of inbound and outbound jobs currently executing.
- **Queued** — Number of inbound and outbound jobs queued to run as soon as less than 50 jobs are executing
- **Scheduled** — Number of inbound and outbound jobs scheduled to run, but not currently executing.
- **Suspended** — Number of inbound and outbound jobs directly or indirectly suspended.
- **External Request** — Number of inbound and outbound jobs set to be executed by an external request.
- **Not Scheduled** — Number of inbound and outbound jobs not currently scheduled to run.

Last Job Completion Status

- **Success** — Most recent execution completed successfully.
- **Failure** — Most recent job execution did not complete successfully. Numbers include incomplete jobs, missed jobs, cancelled jobs, terminated jobs, jobs with critical audit trail errors, or attempts to run with a preview license.
- **Warning** — Most recent job completed successfully, but had at least one error that might have affected the integrity of the file(s) being transferred. Examples of problems generating a Warning status, include:
  - Error closing a file
  - Error deleting an uploaded file after a problem during transmission
  - Decryption or verification key is not valid for current date
  - ASCII file size not within tolerance

  NOTE: Source files with a Warning status are NOT deleted.
- **File(s) Not Found** — No files were found OR one or more required files were not found on the most recent execution and transaction was **not** set to Fail if File(s) Not Found.

13.3 Job History Viewer

Start Time
The date and time that the most recent job began execution for this transaction. If no job history exists for the transaction and a job is not currently executing, this field is blank.

Elapsed Time
The length of time in seconds that the current or most recently completed job has run. If no job history exists for the transaction and a job is not currently executing, this field is blank.

Job Status

If a job is currently executing, valid values are:

- **Delayed** — Job executed using a Diplomat MFT Scripting Agent command with a <delay> parameter.
- **Queued** — Job waiting in job queue for execution.
- **Running** — Job actively executing. This value has sub-status shown in parentheses of:
  - Building File List
  - Verifying File List
  - Processing Files
  - Sending Emails
  - Sending Pages
  - Waiting for Retry
  - Writing Audit Trail
- **Cancelling** — Request to cancel job occurred, but job is still executing.
- **Terminating** — Request to terminate job occurred, but job is still executing.
- **Aborting** — Unrecoverable error encountered.

If a job is not currently executing, valid values are:

- **Preview License** — Job attempted to run, but was stopped due to no valid license.
- **File(s) not Found** — No files were found on the most recent execution and transaction was **not** set to Fail if File(s) Not Found.
- **Required File(s) Not Found** — Some files were found on the most recent execution, but one or more required files were **not** found and transaction was **not** set to Fail if File(s) Not Found.
- **Successful** — Most recent execution completed successfully. Email and other notifications indicate the job was *Successfu*l.
- **Warning** — Job completed successfully, but had at least one error that might have affected the integrity of the file(s) being transferred. Examples of problems generating a Warning status, include:
  - Error closing a file
  - Error deleting an uploaded file after a problem during transmission
  - Decryption or verification key is not valid for current date
  - ASCII file size not within tolerance

  NOTE: Source files with a Warning status are NOT deleted.
- **Failure** — Most recent job execution did not complete successfully. Email and other notifications indicate the job was *Failure*.
- **Critical** — Job failed due to a problem with the audit database and audit trail settings set to T*reat Failures as Critical*.
- **Cancelled** — Job manually cancelled on most recent execution.
- **Terminated** — Job manually terminated on most recent execution.
- **Incomplete** — Diplomat MFT Service stopped during job execution.
- **Missed** — Jobs are flagged as missed, when *Fail if File(s) Not Found* is checked and:
  - Diplomat MFT Service not running when last job execution scheduled.
  - Job queued, but execution had not started, when Diplomat MFT Service stopped unexpectedly.

Source Files Total Size
Total size of all source files found by the job.

Number of Files Found
Number of files selected for file transfer.

Number of Files Successful
Number of files successfully transferred.

Number of Files Failed
Number of files that did not transfer successfully.

Job Execution Attempt
For transactions that are scheduled daily or monthly and have retries specified, each time the job reattempts to find files the number of job execution attempts increases.

13.4 File History Viewer

The file history for each job contains one row for each file found by the job – whether it was successfully processed or not. The File Status column displays information about whether the file was processes successfully.

File Status
If a file is currently being processed, then valid values are:

▪ **Pending**	File has been found, validated and added to list of source files for processing, but has not actively started running.
▪ **Processing**	File actively being processed. This value has sub-status shown in parentheses of: ▪ Getting source ▪ Preparing file ▪ Putting destination file ▪ Archiving file ▪ Complete **NOTE:** Preparing file, putting destination file and archiving file are shown only when Display Detailed File Status is checked on the Settings > Job Monitor screen.

If a file is not currently being processed, valid values are:

▪ **Not Processed**	File never started processing.
▪ **Successful**	File processing completed successfully.
▪ **Warning**	File processing completed but had at least one error that might have affected the integrity of the file. Examples of problems generating a Warning status, include: ▪ Error closing a file ▪ Error deleting an uploaded file after a problem during transmission ▪ Decryption or verification key is not valid for current date ▪ ASCII file size not within tolerance **NOTE:** Source files with a Warning status are NOT deleted.
▪ **Failure**	▪ File processing did not complete successfully.

The ***Transaction Name*** is the name of the transaction as shown in the Transaction Name field on the transaction screen. The ***Source Filename*** is the name of the file picked up at the source location, while the Destination Filename is the name of the file dropped off at the destination location. The ***Job Start Time*** is when that the job began execution, the ***Start Time*** is when the file itself began processing, and the ***Elapsed Time*** is the total elapsed time to process the file. The ***Source File Size*** is provided in bytes. The ***File Transfer Attempt*** denotes the number of the last attempt to transfer the file.

14 Reports

Diplomat MFT provides a set of standard reports on Diplomat's configuration as well as various activities from the Audit database. Reports are generated in PDF format, requiring a PDF reader to view.

14.1 OpenPGP Key Report

The OpenPGP key detail report allows you to print a standard report that includes all information for each OpenPGP key in the Diplomat MFT database. The OpenPGP key report is based on the data in the current Diplomat MFT transaction database.

14.2 SSH Key Pair Report

The SSH Key Pair detail report allows you to print a standard report that includes all information for each SSH Key Pair in the Diplomat MFT database. The SSH Key Pair report is based on the data in the current Diplomat MFT transaction database.

14.3 SSL Certificate Report

The SSL Certificate detail report allows you to print a standard report that includes all information for each SSL Certificate in the Diplomat MFT database. The SSL Certificate report is based on the data in the current Diplomat MFT transaction database.

14.4 Partner Report

The Partner report allows you to print a standard report that includes all information for each Partner in the Diplomat MFT transaction database. The Partner report is based on the data in the current Diplomat MFT transaction database.

14.5 Transaction Report

The transaction report allows you to print a standard report that includes all information for each transaction in the Diplomat MFT transaction database. The transaction report is based on the data in the current Diplomat MFT transaction database.

14.6 Job Detail Report

The Job Detail report allows you to print a standard report that includes all information for each job in the built-in Diplomat MFT audit database or SQL audit database.

You may generate a report with all audit records or any combination of only inbound transactions, only outbound transactions, transaction name, jobs on specific dates, jobs transferring files with specific names, or audit records containing a specified string.

NOTE: When you search for records containing a string, **ONLY** the transaction name, transaction type (inbound/outbound), job status (successful/failure), source and destination Partner name, source and destination filenames, encryption/decryption key name, signature/verification key name, and pre- and post-command fields are searched.

NOTE: The Job Detail report is generated from the data in the Diplomat MFT audit database shown under Settings > Audit**.**

NOTE: If you are using a SQL audit database, you can also choose to *Include Archived Records*, if you want archived audit records included in a report.

14.7 Job Summary Report

The Job Summary report allows you to print a standard report that summarizes the success and failures of jobs that ran during a specified period.

You may generate a report with all audit records or any combination of only inbound transactions, only outbound transactions, transaction name, jobs on specific dates, jobs transferring files with specific names, or audit records containing a specified string.

NOTE: When you search for records containing a string, **ONLY** the transaction name, transaction type (inbound/outbound), job status (successful/failure), source and destination Partner name, source and destination filenames, encryption/decryption key name, and signature/verification key name fields are searched.

Each column shows whether a particular action completed successfully for the entire job. For example, an inbound transaction with 5 files might have 4 files decrypt successfully and 1 file that fails to decrypt. The report would indicate 'No' in the Encrypt/Decrypt column for the job, since not all files were decrypted successfully.

NOTE: The Job Summary report is generated from the data in the Diplomat MFT audit database shown under Settings > Audit**.**

NOTE: If you are using a SQL audit database, you can also choose to *Include Archived Records*, if you want archived audit records included in a report.

14.8 Admin Activity Report

Admin Activity Reports are only available when a SQL database is used for the audit trail.

You may generate reports with all records or any combination of User IDs, User IP Address, Object Type, Date, or Object ID. You can check *Include Archived Records*, if you want archived audit records included in a report.

NOTE: The Admin Activity Report is generated from the data in the SQL Diplomat MFT audit database shown under Settings > Audit**.**

14.9 SFTP Users Report

Report containing configured SFTP Users in Diplomat MFT if the SFTP Server is enabled.

14.10 SFTP Activity Report

Report containing file transfer activity undertaken by SFTP Users in Diplomat MFT if the SFTP Server is enabled.

14.11 Scheduled Reports

Use *Scheduled Reports* to automate the generation of any built-in report.

The *Scheduled Reports* table displays all reports currently scheduled to execute at a future time. The table shows the Report Type, Report Name, and the time a report is scheduled to be generated. Click the pencil icon to edit an

existing scheduled report or the trashcan icon to delete it. Use ***Add Report*** to create a new schedule for generating a report.

When adding or editing a report, choose the ***Report Type*** and set the ***Audit Parameters*** along with the ***Report Name*** to be displayed.

Specify the output ***Report Directory*** and ***File Name*** for the report. You can use the ***Test*** button to ensure the directory is accessible. **Note** that reports written to the same directory with the same name automatically overwrite the earlier version of the report. Date Variables can be used in the *Report Directory* and *File Name* to ensure unique file names and even sort them into folder structures.

Set the ***First Scheduled Report*** date and time and choose how often that report ***Repeats***. For anything other than *Never*, use the ***Repeats Every*** field to select how frequently the report is generated. For monthly and yearly reports, select the day of the month to run.

15 Help Menu

15.1 Diplomat Help

Diplomat Help provides an online interface to the contents of this Diplomat Managed File Transfer Enterprise Edition User Guide to assist you in using the product.

15.2 Diplomat Release Notes

Use this option to navigate to a web page with release notes.

15.3 About Diplomat

You will need the information on this screen if you contact Coviant Software for support. It contains information about the Diplomat Edition and license, including who it's licensed to, the License ID, the license expiration date, and the machine name on which it's installed. The version and build numbers are also important to know.

Diplomat MFT is subject to certain export restrictions outside of the United States. Click the ***Export Restrictions*** button for more details.

16 Appendix A: Support

If you hold a current license of Diplomat MFT with active Premium Support or Extended Hours Support, our support team is available from 9AM to 5PM Central Time, Monday through Friday, except holidays. If you require assistance, contact the Coviant Software Support Team as follows:

E-mail: support@coviantsoftware.com

Phone: +1-210-985-0985 x2

If you require support assistance that appears to be due to a malfunction of your Diplomat MFT software, please review the diagnostic information provided before contacting Coviant Software for support. If you are unable to solve the problem, please include or have the following items available when seeking support:

- Diplomat MFT Edition name, version with build number, and License ID, all located in **Help** > **About**
- Current log file containing entries for the failed job(s)
- IT Support Notification emails containing debug information for the failed job(s)

Diplomat MFT interoperates with other software applications, such as SFTP and OpenPGP software. File transfer and encryption failures can occur during a job created by Diplomat Managed File Transfer for many reasons unrelated to the Diplomat service itself, including:

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

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 issues are outside our ability to fix for you. We do not control your firewalls.

17 Appendix B: Requirements

Supported Operating Systems and Databases	
Diplomat MFT Service	Windows Server 2012 R2 through 2022 64-bit Linux distribution with glibc 2.5 or higher
Diplomat Remote Agent	Windows Server 2012 R2 through 2022 64-bit *nix with glibc 2.5 or higher.
Diplomat Scripting Agent	Windows 10 (64-bit) and Windows Server 2012 R2 through 2022 64-bit *nix with glibc 2.5 or higher.
SQL Database	MySQL Server 5.1 or higher Microsoft SQL Server 2005 v9.0 or higher Most ANSI SQL-92 compliant databases with JDBC support

18 Appendix C: Uncommon Configurations

Diplomat typically runs very well with the configuration deployed at installation time for most cases; however, in some situations, you will want to control a variety of advanced options that are not available in the Diplomat administrative interface**.** This appendix documents these advanced options and how to configure them.

18.1 High Frequency Scheduler

By default, the Diplomat checks every 5 seconds for transactions that need to run. In certain specific situations, a Diplomat MFT installation must check more frequently for jobs that must execute. For those situations, you can pass the Java Virtual Machine (JVM) property "HighFrequencyScheduler" to the Diplomat MFT Service.

Edit the JVM properties using tomcat8w.exe and ensure that the "Java Options" on the "Java" tab include the line:

```
-DHighFrequencyScheduler=true
```

18.2 In-Memory Job History Database

By default, the Diplomat MFT service records the recent history of executed transactions in an embedded database referred to as the ***Job History*** database. This embedded database saves data to the filesystem under Diplomat's data directory at **..\db\derby\jobHistory**. The Job History database is used when tracking the run-time activity of Transactions, which feeds data into the Job Monitor. This information augments the long-term audit history stored in the Audit Trail database, which is either another embedded database or an external database provided by Microsoft SQL Server, MySQL, or others.

Under heavy loads, the Job History database can grow quickly, which may result in degraded job scheduling performance over time. In these situations, it may be desirable to embed the Job History database in memory rather than relying on storage operations. Memory access dramatically faster than even the fastest modern storage I/O, resulting in increased performance. When in memory, the Job History database will be cleared out at Service restart time, resulting in faster performance and freeing up memory resources. The net result is a faster system when executing tens of thousands of jobs throughout the day.

To switch the Job History database to run from memory rather than the default storage-based operations, edit the JVM properties using tomcat8w.exe and ensure that the "Java Options" on the "Java" tab include the line:

```
-DInMemoryJobHistory=true
```