COVIANT Software

USER GUIDE
DIPLOMAT MANAGED FILE TRANSFER
ENTERPRISE EDITION
VERSION 6.2

v6.2
ENTERPRISE EDITION

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

Voice: 781.210.3310 x2

Fax: 781.210.3313

Web: www.coviantsoftware.com

E-mail: support@coviantsoftware.com

Table of Contents

1 Welcome to Diplomat Managed File Transfer

1.1 What is Diplomat Managed File Transfer?

The Diplomat® suite of managed file transfer products enables easy creation and management of secure file transfers. You can purchase the edition you need today and seamlessly upgrade to other editions with a simple license file replacement.

Basic Edition	**Automate secure FTP and PGP encryption in one application.** > File transfers using any combination of local network, FTP, SFTP (SSH2), and FTPS (TLS) > Intuitive transaction set-up with extensive job scheduling options > Central, encrypted transaction database to protect passwords and passphrases > Creation, import, and export of PGP keys for compatibility with OpenPGP-compliant tools > OpenPGP to encrypt, decrypt, sign, verify, ASCII-armor, and/or compress files > Create, import, and export SSH client keys for key authentication with SFTP file transfers > Ability to recover from transient file transfer errors without restarting file transfer jobs > Backup, merge, and restore of transaction database for fast recovery > Automated clean-up of archived data and log files > Capture of advanced troubleshooting data > Comprehensive tracking of user activity on screen and in log files > Multi-threaded, client-server design for flexible deployment and high performance
Standard Edition	**Integrate secure file transfers into business processes.** Offers all the capabilities of Basic Edition plus: > File transfers to and from email, HTTP, HTTPS and SMB servers > Email error notifications for immediate follow-up and problem resolution > Emergency paging notifications > Import pre-existing public and secret key rings from OpenPGP-compatible tools > Built-in audit database to track job statistics for improved regulatory compliance > Standard audit, key, and transaction reports for easy oversight > Ability to archive data files and log files to multiple locations > Use of Additional Encryption Keys (AEKs) for easy decryption of archived files > Diplomat MFT Scripting Agent and (optional) Diplomat MFT REST API for initiating Diplomat MFT jobs > Folder monitoring to trigger file transfer jobs when new files arrive > Administration of user login identities for easy, secure authentication of multiple concurrent users
Enterprise Edition	**Provide a single point of control for business-critical secure file transfers.** Offers all the capabilities of Standard Edition plus: > Monitor scheduled and live file transfer jobs using Diplomat MFT Job Monitor > File transfers using Diplomat Cloud Connector with built-in PGP encryption and checkpoint restart > Execute specified programs before or after a file transfer job > Save source, destination and PGP key settings for use in multiple file transfer jobs > Identify unused keys, partners and transactions for fast system clean-up > Capture job history and user activity data in a SQL audit database for compliance and custom reporting > Enhanced specification, selection, and naming of source and destination files > Temporarily suspend file transfers to immediately respond to security breaches > On-screen status icons show file transfers as actively scheduled, suspended, or set to allow external requests > Easily merge new file transfer jobs from test systems onto production systems > Manage job queue settings > Access Diplomat components without installing locally using Diplomat MFT Web Launch

1.2 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 user activity and file transfer job.

Automate File Transfers with Remote Sites

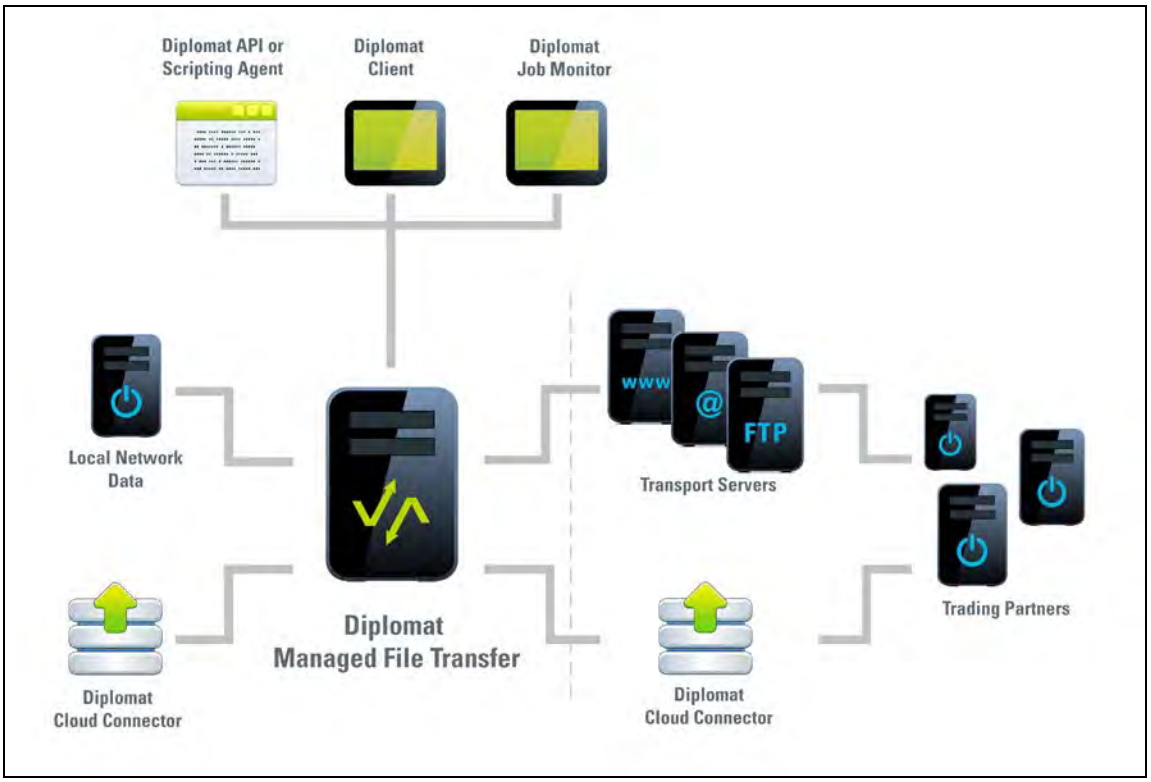
Key Need: Many businesses need to send files containing sensitive data between a central, corporate hub and multiple remote sites, such as branch offices, retail stores, sales offices, or distribution sites. As a rule, these remote sites do not have skilled IT personnel on site and the local users typically 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 Cloud Connector 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 of the file transfer jobs without relying on any local IT expertise at the remote sites.

1.3 Deployment

Diplomat Managed File Transfer is a Java-based, client-server application that runs on Windows and Linux systems. The following diagram shows a network deployment for a Diplomat MFT solution:



Deployment Overview

The Diplomat MFT Client is a user application that enables the creation and modification of transaction, key, partner, and other data. It captures transaction information and administrative settings in the Diplomat MFT transaction database for use by the Diplomat MFT Service. The Diplomat MFT Client is located behind the corporate firewall in a secure datacenter or elsewhere on the local network.

The Diplomat MFT Service is the runtime engine that executes transactions stored in the Diplomat MFT transaction database. It runs as a service and performs all of the file transfer management activities specified in the Diplomat MFT transaction database. The Diplomat MFT Service is located behind the corporate firewall (typically in a secure datacenter) and interoperates with FTP servers, HTTP/S servers, mail servers, and other systems that may be in a corporate DMZ. It creates a log file with system messages, an audit database, and archives of transaction files, if desired.

Diplomat MFT Service requires that a Java-enabled Web server be installed on the same system. The Tomcat web server from The Apache Software Organization (www.apache.org) is automatically installed during the Diplomat MFT Service installation. On Windows systems, the Tomcat web server is set up as a Windows service, called *Diplomat MFT 64,* and on Linux systems as a daemon, called *diplomatServer*.

The Diplomat MFT Scripting Agent can be used to send a request to the Diplomat MFT Service to immediately schedule a specific file transfer job that was previously set up using the Diplomat MFT Client. Many system/user events, scheduled tasks, or specific application events can be set to trigger a job to run that executes a Diplomat MFT Scripting Agent command. Diplomat MFT Scripting Agent is located behind the corporate firewall on any system that wants to kick off a secure file transfer job without using Diplomat's built-in scheduler.

The Diplomat MFT Job Monitor is installed behind the corporate firewall and can be started from the Diplomat MFT Client or in stand-alone mode.

Diplomat MFT Web Launch can start the Diplomat MFT Client, Scripting Agent or Job Monitor from a browser located behind the corporate firewall.

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

2 Installing Diplomat Managed File Transfer

Diplomat Managed File Transfer is supported on various platforms as follows:

	Diplomat MFT Service	Diplomat MFT Client	Diplomat MFT Scripting Agent	Diplomat MFT Job Monitor	Diplomat Cloud Connector
Windows 7[1] (64-bit)	X	X	X	X	X
Windows 8[1] (64-bit)	X	X	X	X	X
Windows Server 2008 R2[1] (64-bit)	X	X	X	X	X
Windows Server 2012 R2[1] (64-bit)	X	X	X	X	X
Red Hat Linux (64-bit)	X		X		X
Other Unix			X		

Refer to *Appendix A: Configuration Requirements* for exact operating system releases supported.

NOTE: If you plan to use Diplomat MFT Scripting Agent, refer to *Diplomat MFT Scripting Agent User Guide* for instructions on how to install and configure the Diplomat MFT Scripting Agent.

NOTE: If you plan to use Diplomat MFT Job Monitor as a standalone application, refer to *Diplomat MFT Job Monitor User Guide* for instructions on how to separately install the Diplomat MFT Job Monitor.

NOTE: If you have data in a Diplomat MFT trial copy that you would like to retain, use File > Backup to create a backup file. Install a Diplomat MFT paid copy and use File > Restore to import the data from your trial copy. Then, uninstall the Diplomat MFT trial copy.

2.1 Windows Installation

Diplomat Managed File Transfer uses a single Windows installation module to install all Diplomat MFT components.

NOTE: The Diplomat MFT Service must be installed and started before other Diplomat MFT components can be used.

In addition to performing an initial installation, you can:

Modify
- Add one or more components to an existing installation
- Uninstall a component from an existing installation

Repair
- Reinstall all previously installed components

Remove
- Uninstall all Diplomat MFT components

[1] When running Windows 7, Windows Server 2008 or follow-on products, the Diplomat Cloud Connector service cannot run as a local system account. A logon account with administrator privileges must be specified.

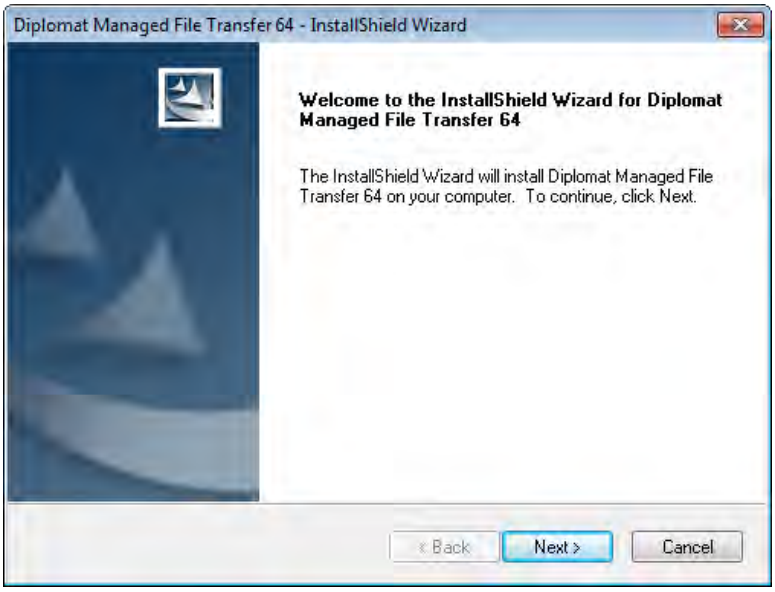
2.1.1 Initial Install

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

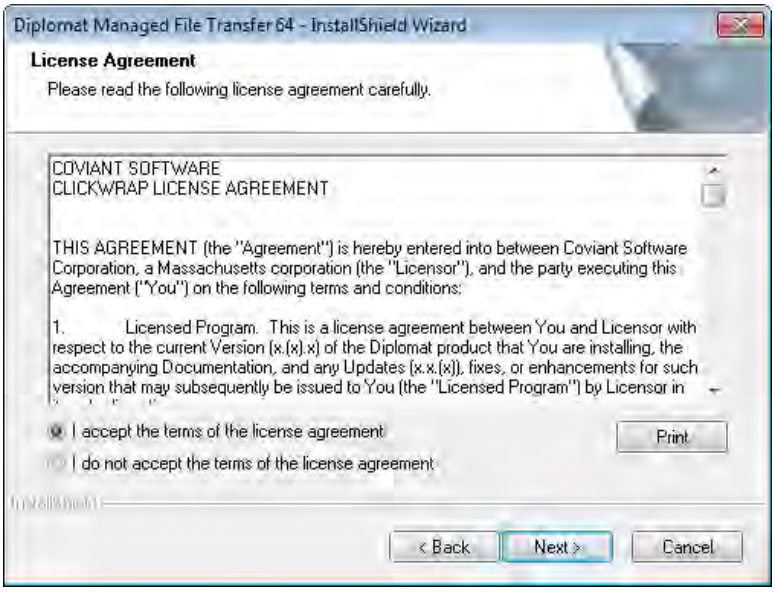
1. Log on to the system where Diplomat MFT components are to be installed. You must use a Windows account with administrator privileges if you are installing the Diplomat MFT Service.

2. Go to www.coviantsoftware.com and log on using the username and password supplied by Coviant Software Support. Navigate to http://www.coviantsoftware.com/support-portal.php. Download and unzip the DiplomatSetup file for the correct edition of Diplomat Managed File Transfer.

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.

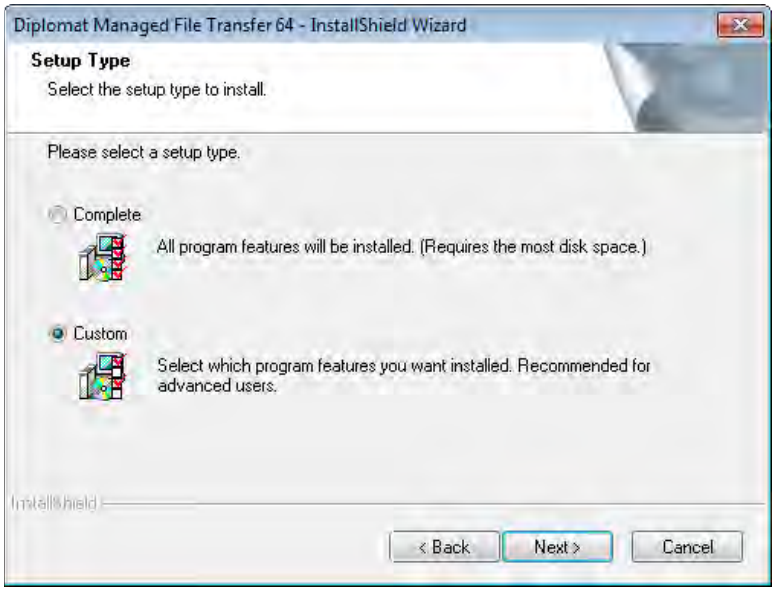


4. Scroll through the license agreement and review the terms and conditions. If you agree with the terms, select 'I accept the terms of the license agreement' and **Next** to continue. You may print a copy of the license agreement for your records using the **Print** button.



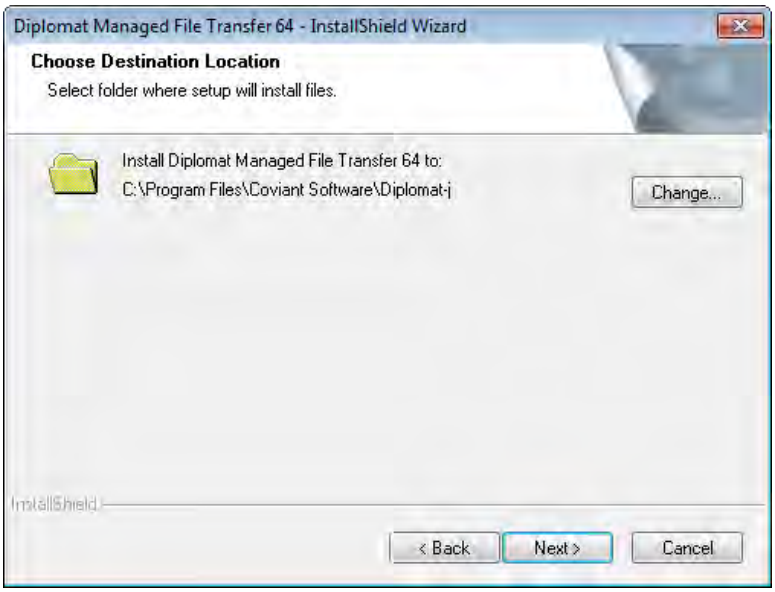
5. Choose the type of setup you would like. Select **Complete** to install the default Diplomat MFT components in the default location (C:\Program Files\Coviant Software\Diplomat-j). Select **Custom** to **choose Diplomat MFT components to install** or to **change the installation location**.

   NOTE: A complete installation installs the Diplomat MFT Service, Diplomat MFT Client and Diplomat MFT Scripting Agent. **You must select Custom to install the Diplomat MFT Job Monitor.**

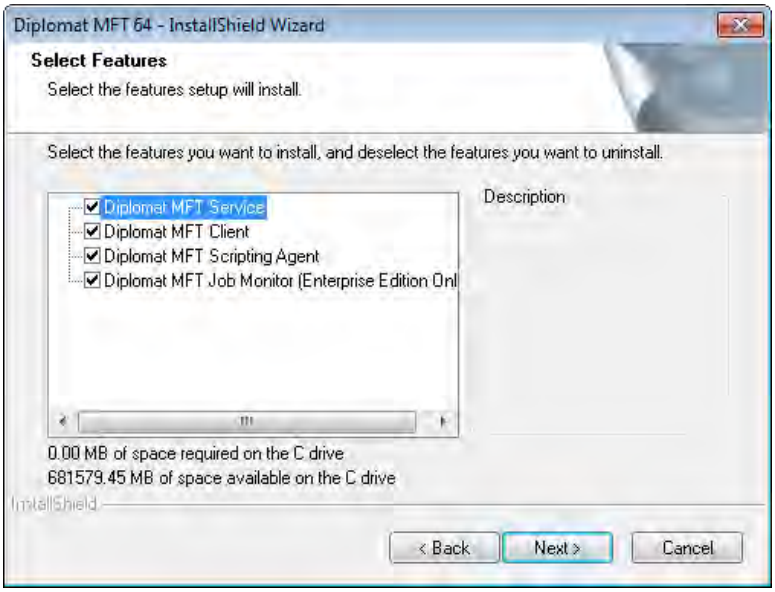


6. If you chose **Custom**, select **Next** to accept the default location (C:\Program Files\Coviant Software\Diplomat-j) or **Change…** to identify a new installation directory.

   NOTE: The default location for a Diplomat MFT trial copy is C:\Program Files\Coviant Software\Diplomat-trial.

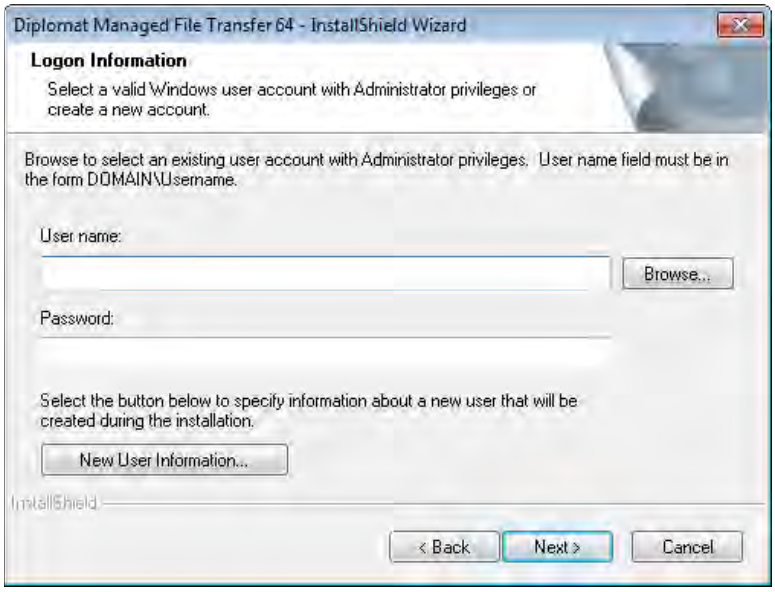


7. If you selected **Custom**, check which components to install on the next screen.

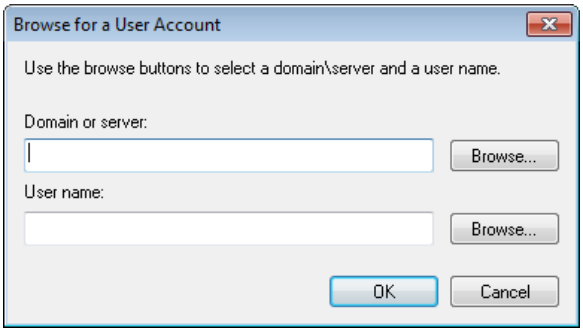


8. If you chose to install the Diplomat MFT Service, follow the instructions below:

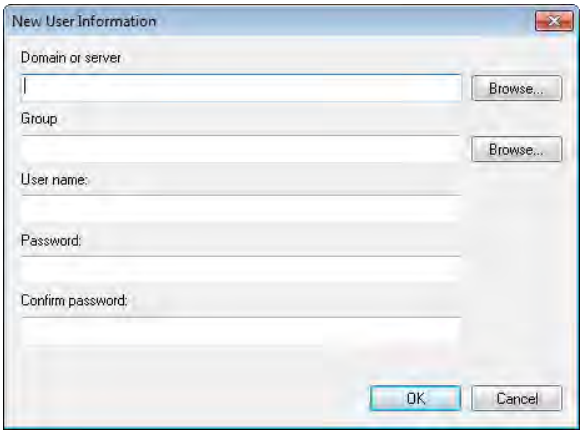
   - Enter the logon information for the Windows account to be used with the Diplomat MFT Service or select **New User Information…** to create a new Windows account.



   - Using **Browse…** to select a DOMAIN and Username ensures that DOMAIN/Username is entered correctly. **NOTE:** A Windows logon account with Administrator privileges is REQUIRED when running on Windows 7, Windows 8, Windows Server 2008 or follow-on products.

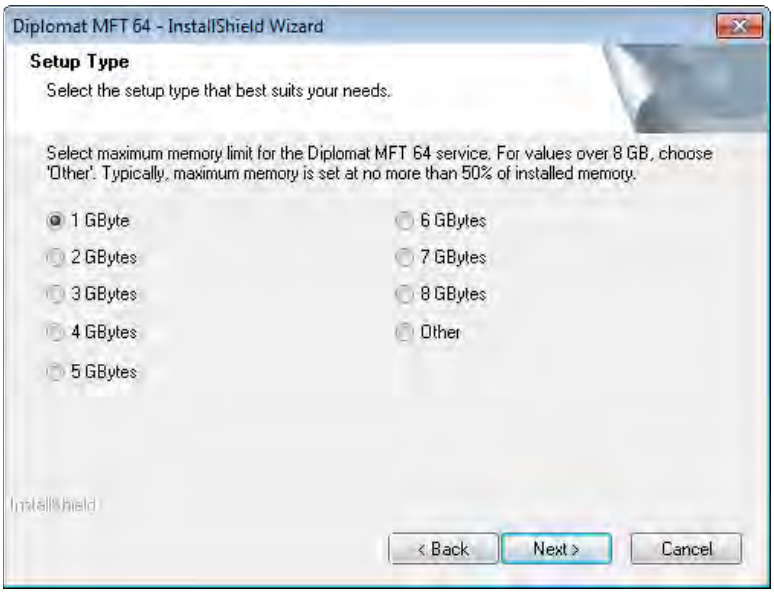


   - If you are creating a new user, **ensure that 'Administrator' is selected in the Group field** to ensure that the new Windows account has administrator privileges.

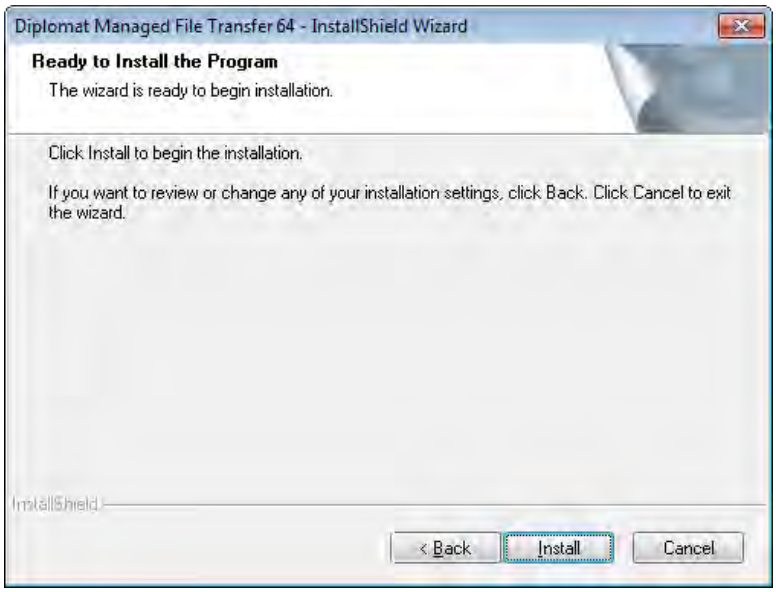


- If you plan to use mapped drives or UNC paths when setting up transactions and access to the source and destination directories is restricted, you must assign the logon account for the Diplomat MFT Service the required privileges. See *Appendix B: Windows Diplomat MFT Service* for more information.

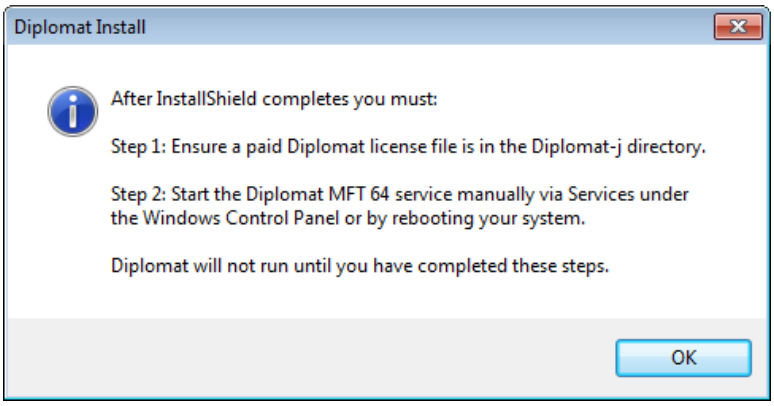
9. Select a maximum memory limit for the Diplomat MFT service. For values greater than 8 GB, choose 'Other'.
   NOTE: Maximum memory should typically be set to no more than 50% of installed memory.



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



11. When the installation is complete, you must:



- Copy the Diplomat license file (i.e., *.lic) that you received from Coviant Software Support to C:\ProgramData\Coviant Software\Diplomat-j.

  NOTE: The default username is 'Administrator' and the default password for all licenses is 'diplomat' for all licenses. You are prompted to reset this password when you start the Diplomat MFT Client.

  NOTE: The ProgramData directory is a system folder and may be hidden by the operating system. To display the ProgramData directory and sub-directories, open Windows Explorer. Select 'Organize > Folder and search options' from the top menu. Select the View tab. Select 'Show hidden files, folders, and drives'.

  NOTE: If you are using a user-defined data location, the license file must be copied to the <DiplomatData>\Coviant Software\Diplomat-j directory, where <DiplomatData> is the directory defined by the DiplomatData environment variable. Refer to *Setting a User-Defined Data Location FAQ* for further information.

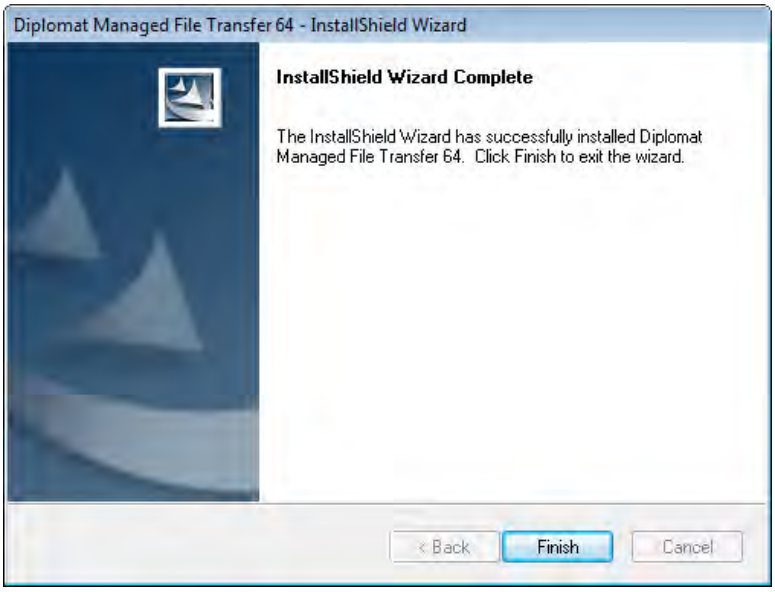
  NOTE: The default location for Diplomat MFT trial licenses is …\Diplomat-trial.

- Before attempting to start the Diplomat MFT Client or Job Monitor, start the Windows service named *Diplomat MFT 64*, which starts and stops the Tomcat web server. The Diplomat MFT Service is set to start automatically on reboot. You can manually start the service through **Services** under the Windows **Control Panel.**
- If needed, you can confirm that the Diplomat MFT Service is working properly by opening a browser window and navigating to https://localhost:8080 which should display the Tomcat home page. If the Tomcat server 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 may receive a message from your browser indicating a problem with the web site's security, Select *Continue* in order to access the Tomcat home page.

12. The final screen indicates that you have successfully completed the component install or uninstall.



13. If firewall software is running on the Diplomat MFT site, check to ensure that it is configured to allow Internet access for the Diplomat MFT processes. The service name is *Diplomat MFT 64* and the process name is *tomcat*_64.exe*. These files are located in the …\Diplomat-j\tomcatWebserver\bin directory or your corresponding install directory. The process name that the Diplomat MFT Client uses to access the Internet is *javaw.exe*, which is located in the …\Diplomat-j\jre\bin or your corresponding install directory.

14. A new directory structure is created during the installation of the Diplomat MFT site. If you selected the default installation location, this directory structure is located under C:\Program Files\Coviant Software\Diplomat-j. These directories contain the Diplomat MFT Service. Diplomat MFT data files are located either under the install directory or under C:\ProgramData\Coviant Software\Diplomat-j for Windows systems that enforce the User Access Control model. 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.

2.1.2 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. Log on to the system where Diplomat MFT components are to be added or removed. You must use a Windows account with administrator privileges if you are adding the Diplomat MFT Service.

2. Open the Diplomat MFT Client and suspend all transactions by selecting Jobs > Suspend > All Transactions Directly from the top menu bar. Exit from the Diplomat MFT Client.

3. If you are removing the Diplomat MFT Service, you must stop the Diplomat MFT Service. You can access the Diplomat MFT Service through **Services** under the Windows **Control Panel.**

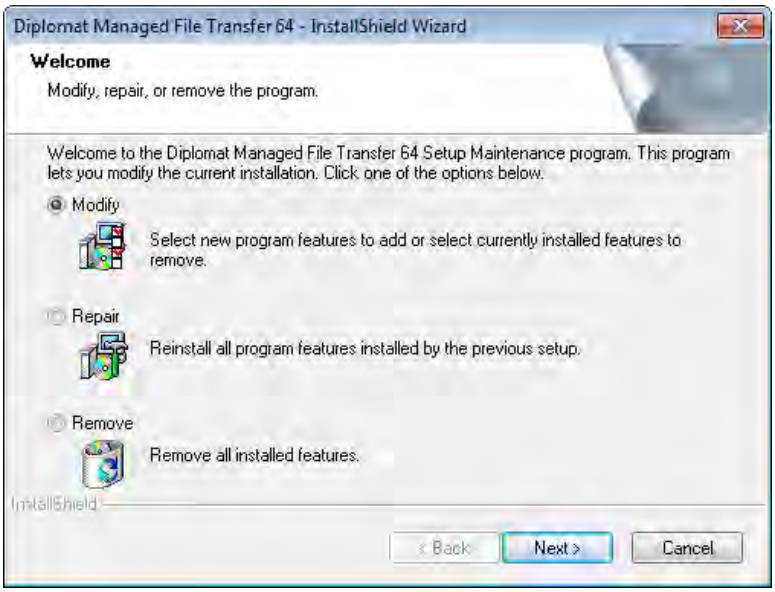
   To ensure that no jobs are queued or running before you stop the service, suspend all transactions in the Diplomat MFT Client and wait until an orange status indicator '■' is displayed next to the transaction folder in the job monitor.

   NOTE: When you stop the Diplomat MFT Service manually, it may not stop immediately. The system waits until all currently queued or running jobs are complete before stopping the service. You will be reminded to confirm that the Diplomat MFT Service is not running.

4. Go to www.coviantsoftware.com and log on using the username and password supplied by Coviant Software Support. Navigate to http://www.coviantsoftware.com/support-portal.php. Download and unzip the DiplomatSetup file for the correct edition of Diplomat Managed File Transfer.

5. 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.

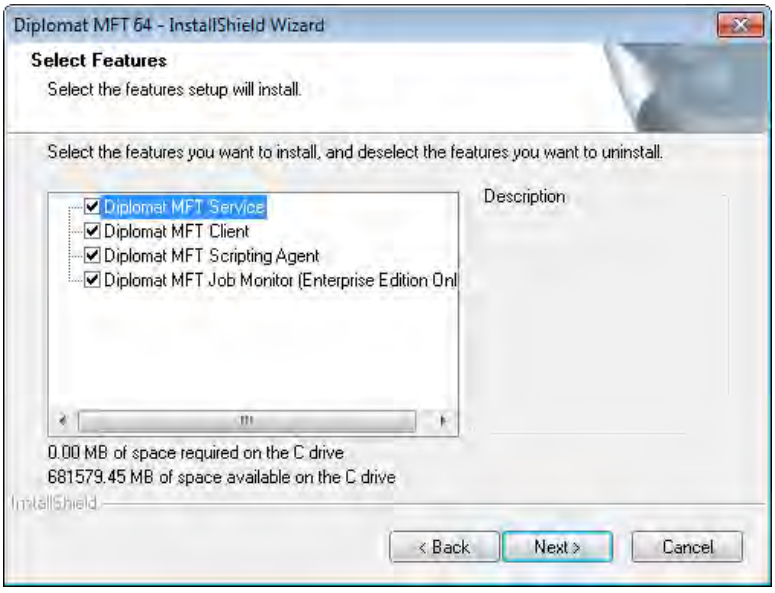
6. Select **Modify**.



7. To **ADD** a component, check all of 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.

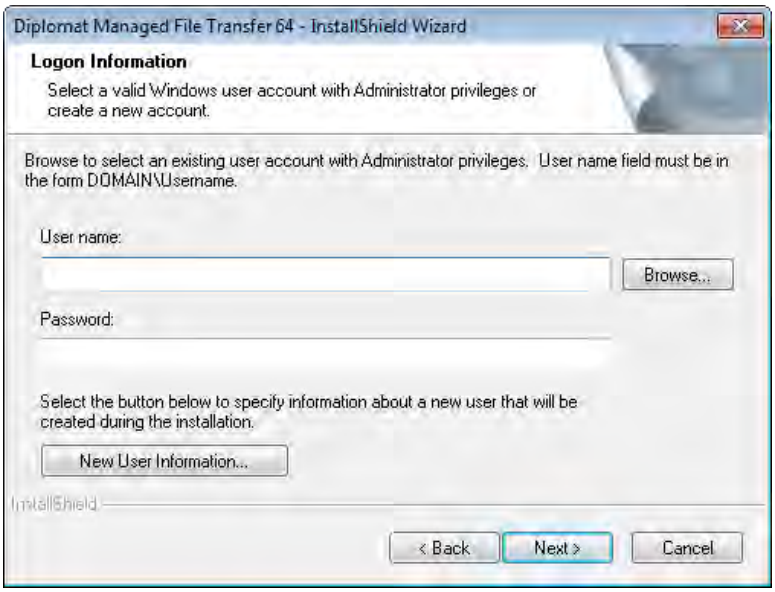
   NOTE: The default location for Diplomat MFT trial licenses is …\Diplomat-trial.

   CAUTION: DO NOT leave a component that is already installed unchecked. If you do, the unchecked component will be uninstalled.

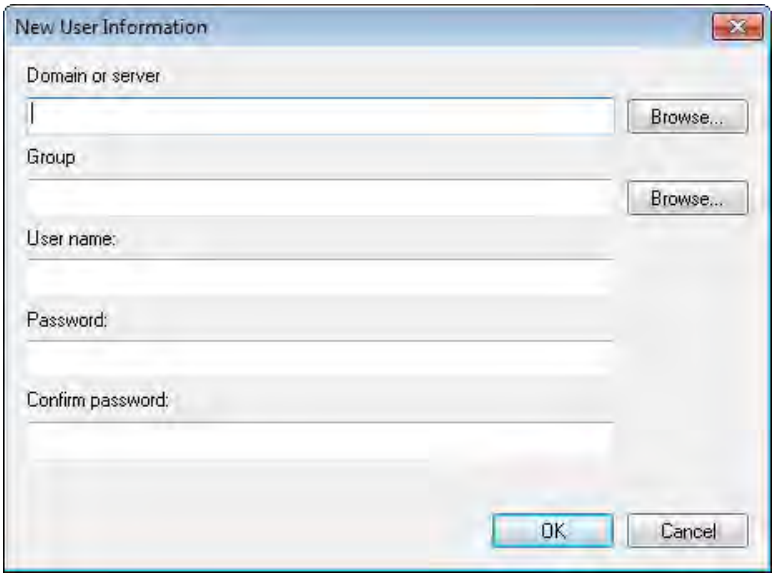


8. If you chose to install the Diplomat MFT Service, follow the instructions below:

   - Enter the logon information for the Windows account to be used with the Diplomat MFT Service or select **New User Information…** to create a new Windows account. Using **Browse…** to select a DOMAIN and Username ensures that DOMAIN/Username is entered correctly. **NOTE:** A Windows logon account with Administrator privileges is REQUIRED when running on Windows 7, Windows 8, Windows Server 2008 or follow-on products.

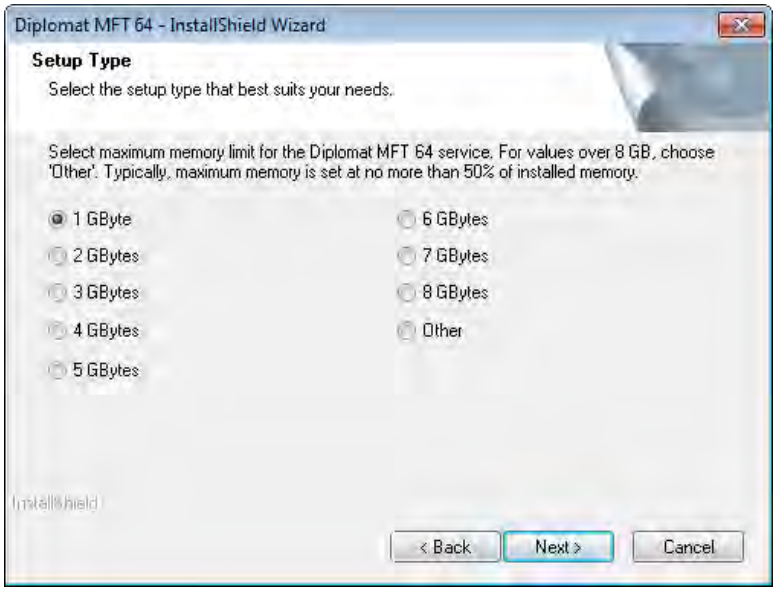


- If you are creating a new user, **ensure that 'Administrator' is selected in the Group field** to ensure that the new Windows account has administrator privileges.

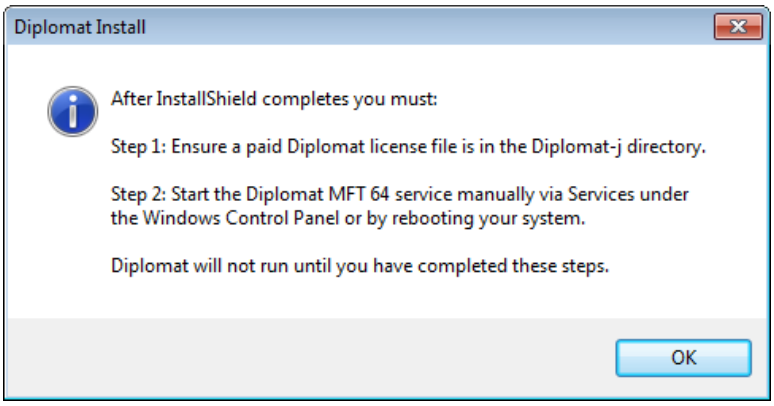


- If you plan to use mapped drives or UNC paths when setting up transactions and access to the source and destination directories is restricted, you must assign the Windows logon account for the Diplomat MFT Service the required privileges. See *Appendix B: Windows Diplomat MFT Service* for more information.

9. 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 50% of installed memory.



10. Select **Install** on the next screen to start the installation. When the installation is complete, you must:



- If you installed the Diplomat MFT Service, copy the Diplomat MFT license file (i.e., *.lic) that you received from Coviant Software Support to C:\ProgramData\Coviant Software\Diplomat-j.

  NOTE: The default username is 'Administrator' and the default password for all licenses is 'diplomat' for all licenses. You will be prompted to reset this password when you start the Diplomat MFT Client.

  NOTE: The ProgramData directory is a system folder and may be hidden by the operating system. To display the ProgramData directory and sub-directories, open Windows Explorer. Select Organize > Folder and search options from the top menu. Select the View tab. Select Show hidden files, folders, and drives.

  NOTE: If you are using a user-defined data location, the license file must be copied to the <DiplomatData>\Coviant Software\Diplomat-j directory, where <DiplomatData> is the directory defined by the DiplomatData environment variable. Refer to *Setting a User-Defined Data Location FAQ* for further information.

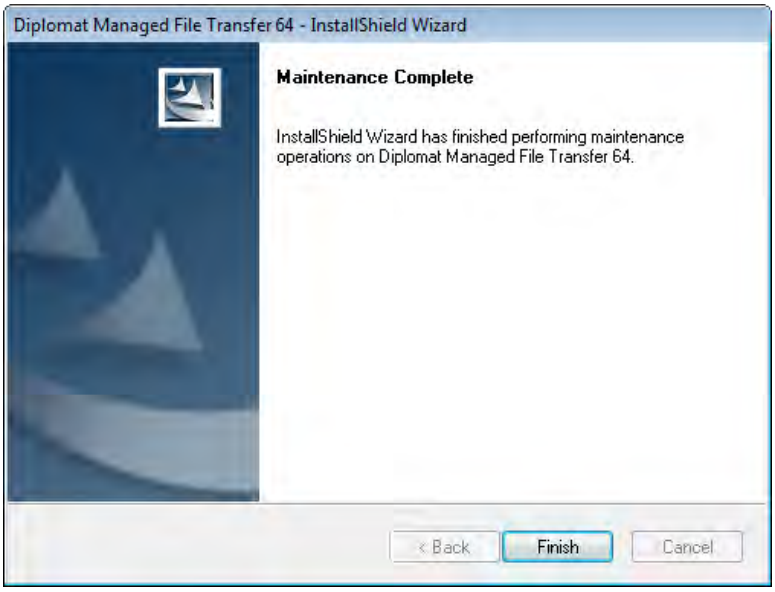
  NOTE: The default location for Diplomat MFT trial licenses is …\Diplomat-trial.

- Before attempting to start the Diplomat MFT Client or Job Monitor, start the Windows service named *Diplomat MFT 64*, which starts and stops the Tomcat web server. The Diplomat MFT Service is set to start automatically on reboot. You can manually start the service through **Services** under the Windows **Control Panel.**
- If needed, you can confirm that the Diplomat MFT Service is working properly by opening a browser window and navigating to https://localhost:8080 which should display the Tomcat home page. If the Tomcat server 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 may receive a message from your browser indicating a problem with the web site's security, Select *Continue* in order to access the Tomcat home page.

11. The final screen indicates that you have successfully completed the component install or uninstall.



12. If firewall software is running on the Diplomat MFT site, check to ensure that it is configured to allow Internet access for the Diplomat MFT processes. The server service name is *Diplomat MFT 64* and the process name is *tomcat*_64.exe*. These files are located in the …\Diplomat-j\tomcatWebserver\bin directory or your corresponding install directory. The process name that the Diplomat MFT Client uses to access the Internet is *javaw.exe*, which is located in the …\Diplomat-j\jre\bin or your corresponding install directory.

13. 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 C:\Program Files\Coviant Software\Diplomat-j. These directories contain the Diplomat MFT Service. Diplomat MFT data files are located either under the install directory or under C:\ProgramData\Coviant Software\Diplomat-j for Windows systems that enforce the User Access Control model. 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.

2.1.3 Repair

Use the following instructions if you are reinstalling **ALL** current Diplomat MFT components.

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

2. Open the Diplomat MFT Client and suspend all transactions by selecting Jobs > Suspend > All Transactions Directly from the top menu bar. Exit from the Diplomat MFT Client.

3. If you are repairing the Diplomat MFT Service, you must stop the Diplomat MFT Service. You can access the Diplomat MFT Service through **Services** under the Windows **Control Panel.**

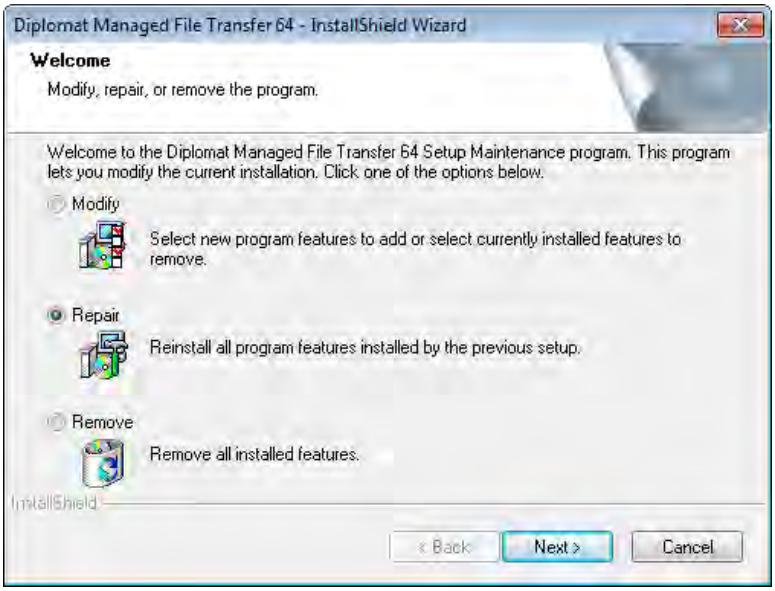
   To be sure that no jobs are queued or running before you stop the service, suspend all transactions in the Diplomat MFT Client and wait until an orange status indicator '■' is displayed next to the transaction folder in the job monitor.

   NOTE: When you stop the Diplomat MFT Service manually, it may not stop immediately. The system waits until all currently queued or running jobs are completed before stopping the service. During the repair, you will be reminded to reconfirm that the Diplomat MFT Service is not running.

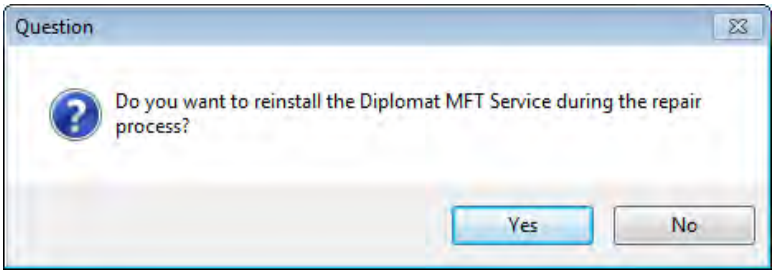
4. Go to www.coviantsoftware.com and log on using the username and password supplied by Coviant Software Support. Navigate to http://www.coviantsoftware.com/support-portal.php. Download and unzip the DiplomatSetup file for the correct edition of Diplomat Managed File Transfer.

5. 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.

6. Select **Repair**.

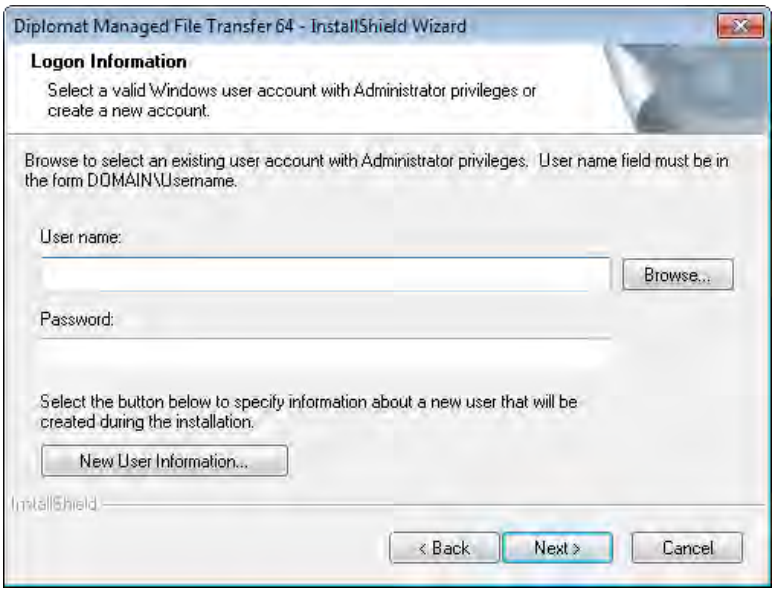


7. If the Diplomat MFT Service component is installed, choose whether to reinstall it.

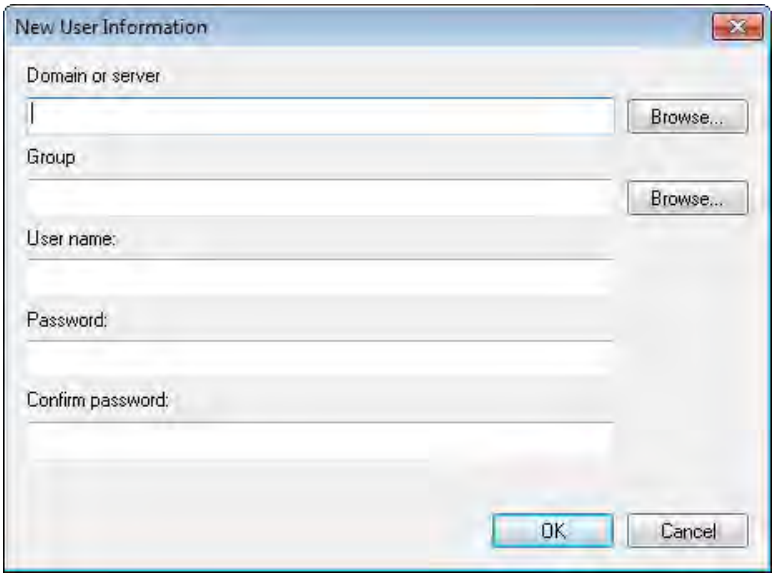


8. If you chose to reinstall the Diplomat MFT Service, follow the instructions below:

   - Enter the logon information for the Windows account to be used with the Diplomat MFT Service or select **New User Information…** to create a new Windows account. Using **Browse…** to select a DOMAIN and Username ensures that DOMAIN/Username is entered correctly. **NOTE:** A Windows logon account with Administrator privileges is REQUIRED when running on Windows 7, Windows 8, Windows Server 2008 or follow-on products.



- If you are creating a new user, **ensure that 'Administrator' is selected in the Group field** to ensure that the new Windows account has administrator privileges.

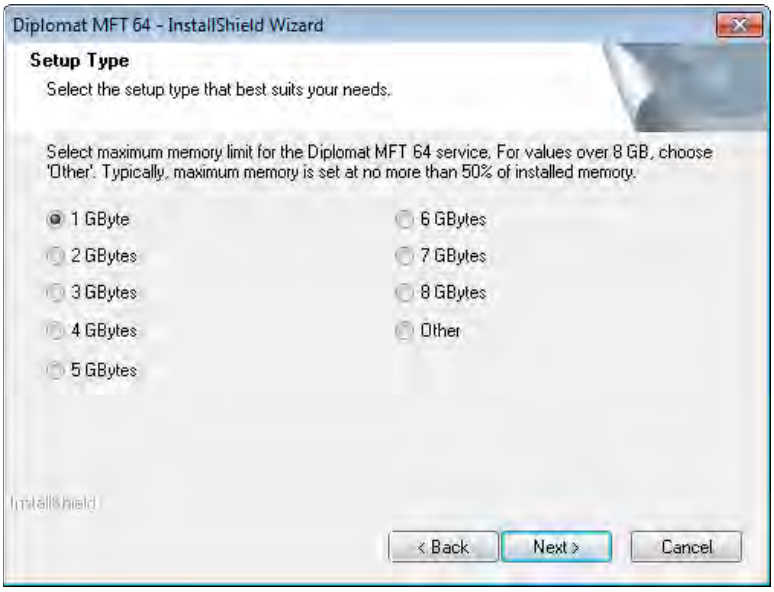


- If you plan to use mapped drives or UNC paths when setting up transactions and access to the source and destination directories is restricted, you must assign the Windows logon account for the Diplomat MFT Service the required privileges. See *Appendix B: Windows Diplomat MFT Service* for more information.
- Before attempting to start the Diplomat MFT Client or Job Monitor, start the Windows service named *Diplomat MFT 64*, which starts and stops the Tomcat web server. The Diplomat MFT Service is set to start automatically on reboot. You can manually start the service through **Services** under the Windows **Control Panel.**
- If needed, you can confirm that the Diplomat MFT Service is working properly by opening a browser window and navigating to https://localhost:8080 which should display the Tomcat home page. If the Tomcat server is not running, see *Appendix B: Windows Diplomat MFT Service*.

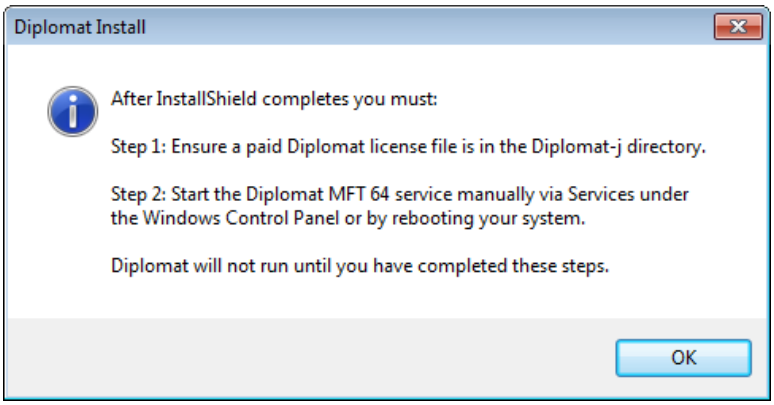
NOTE: The server port is set to 8080 by default. If port 8080 is already in use, contact Coviant Software Support for instructions on how to change the server port number.

NOTE: You may receive a message from your browser indicating a problem with the web site's security, Select *Continue* in order to access the Tomcat home page.

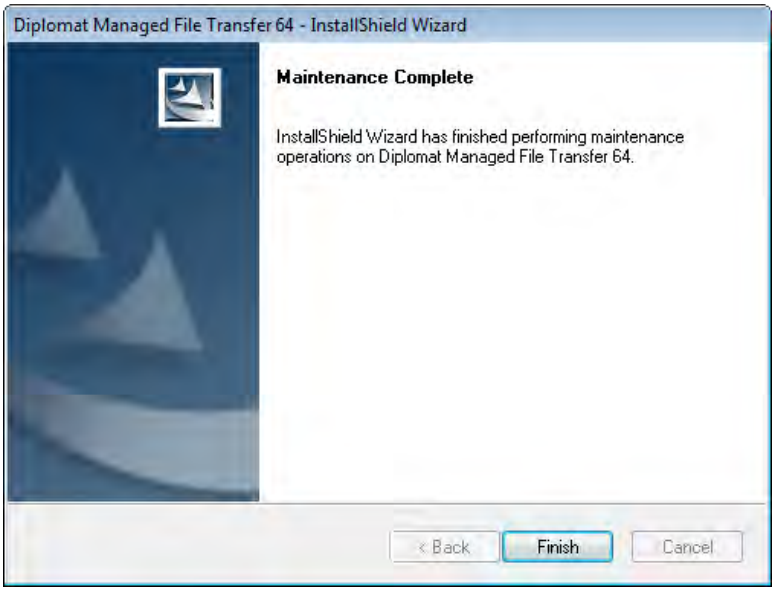
9. Select a maximum memory limit for the Diplomat MFT service. For values greater than 8 GB, choose 'Other'. **NOTE:** Maximum memory should typically be set to no more than 50% of installed memory.



10. Select **Install** on the next screen to start the installation. When the installation is complete, you must:



11. The final screen indicates that you have successfully completed the repair.



2.1.4 Remove

Use the following instructions only if you are **uninstalling ALL** Diplomat MFT components. If you want to uninstall one or more components (e.g., the Diplomat MFT Client or the Diplomat MFT Service), review the previous section on *Modify Installation*.

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

2. Open the Diplomat MFT Client and suspend all transactions by selecting Jobs > Suspend > All Transactions Directly from the top menu bar. Exit from the Diplomat MFT Client.

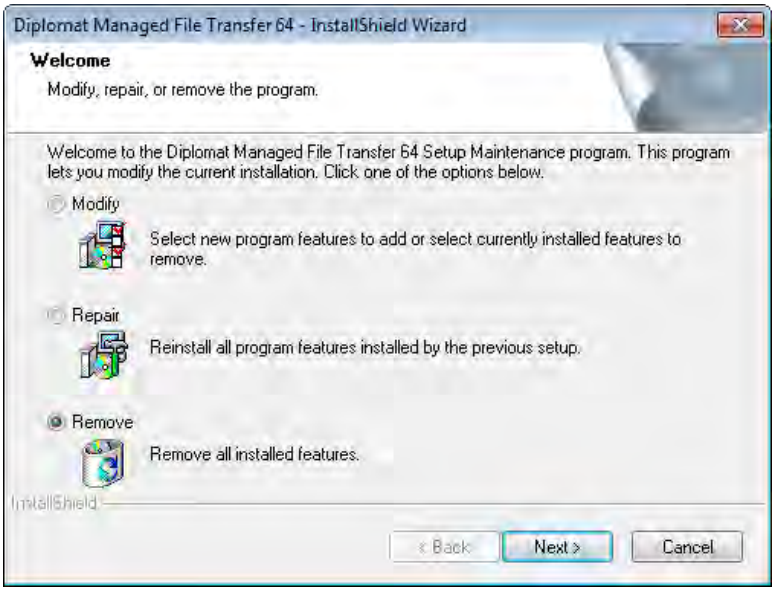
3. If you are uninstalling the Diplomat MFT Service, you must stop the Diplomat MFT Service. You can access the Diplomat MFT Service through **Services** under the Windows **Control Panel.**

   To be sure that no jobs are queued or running before you stop the service, suspend all transactions in the Diplomat MFT Client and wait until an orange status indicator '■' is displayed next to the transaction folder in the job monitor.

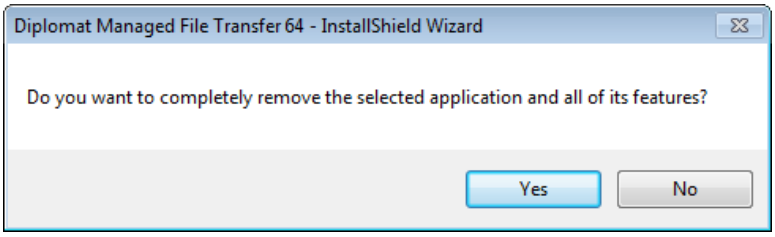
   NOTE: When you stop the Diplomat MFT Service manually, it may not stop immediately. The system waits until all currently queued or running jobs are completed before stopping the service. During the uninstall, you will be reminded to reconfirm that the Diplomat MFT Service is not running.

4. Select Windows **Start** button and then Control Panel > Add/Remove Programs > Diplomat Managed File Transfer**.**

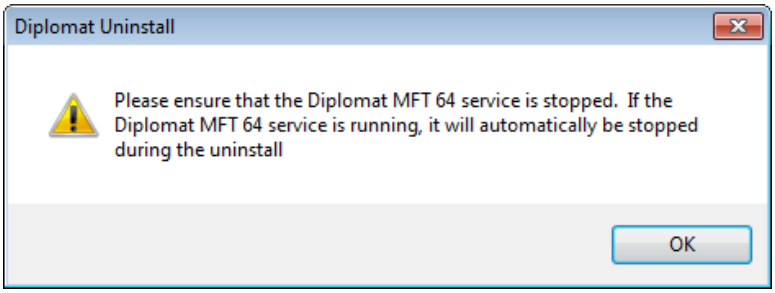
5. Select **Remove**.



6. Confirm that you want to completely remove all Diplomat MFT components.



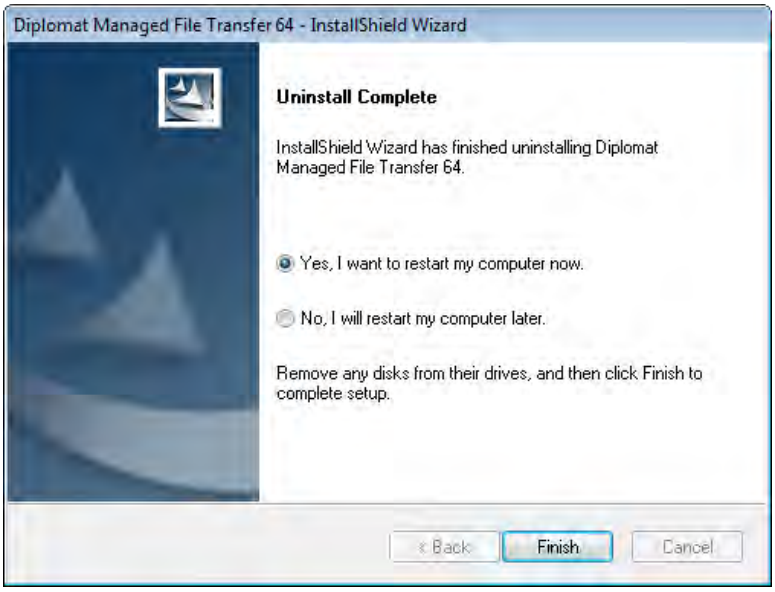
7. If prompted, confirm that the Diplomat MFT Service is stopped.



8. The final screen indicates that you have successfully uninstalled Diplomat MFT.

   When you uninstall the Diplomat MFT Service, the Diplomat MFT Service may be deleted automatically or marked for deletion and set to disabled. Check the status of the Diplomat MFT Service through **Services** under the Windows **Control Panel.** If the Startup Type is set to disabled, you must reboot your system to complete the uninstall.

   NOTE: If you are planning to reinstall the Diplomat MFT Service on the same system, you must complete the deletion of the service by rebooting before attempting the reinstall.



2.1.5 Version Upgrade

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

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

2. Open the Diplomat MFT Client. Create a backup file under File > Backup in the top menu bar.

3. Suspend all transactions by selecting Jobs > Suspend > All Transactions Directly from the top menu bar. Exit from the Diplomat MFT Client.

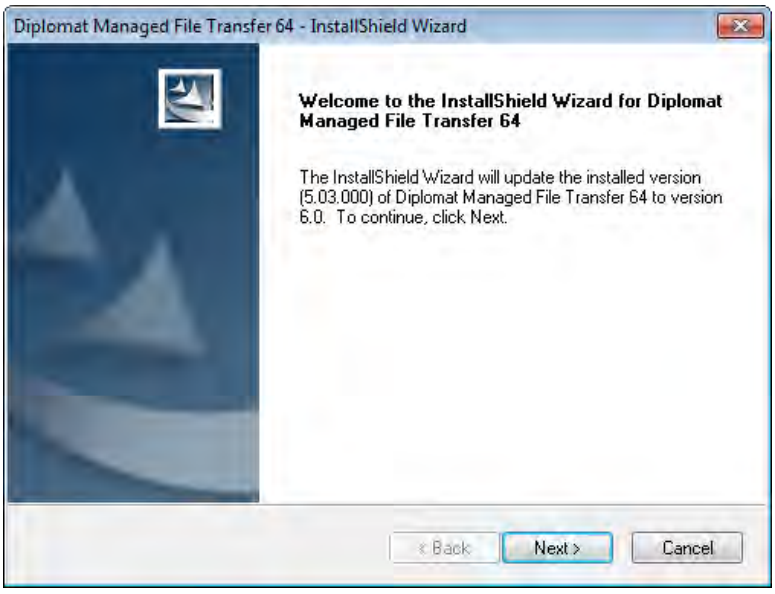
4. If you are upgrading the Diplomat MFT Service, you must stop the current Diplomat MFT Service. You can access the Diplomat MFT Service through **Services** under the Windows **Control Panel.**

   To be sure that no jobs are running before you stop the service, suspend all transactions in the Diplomat MFT Client and wait until an orange status indicator '■' is displayed next to the transaction folder in the job monitor.

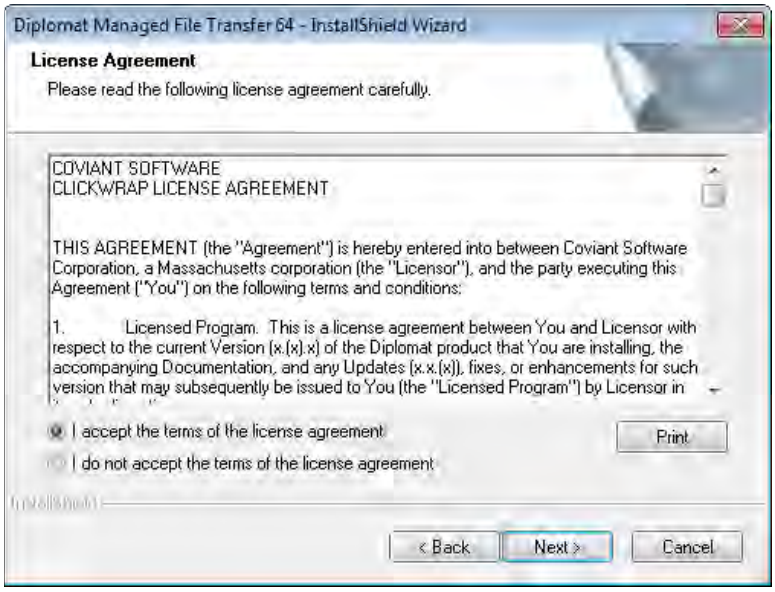
   NOTE: When you stop the Diplomat MFT Service manually, it may not stop immediately. The system waits until all currently queued or running jobs are completed before stopping the service. During the uninstall, you will be reminded to reconfirm that the Diplomat MFT Service is not running.

5. Go to www.coviantsoftware.com and log on using the username and password supplied by Coviant Software Support. Navigate to http://www.coviantsoftware.com/support-portal.php. Download and unzip the DiplomatSetup file for the correct edition of Diplomat Managed File Transfer.

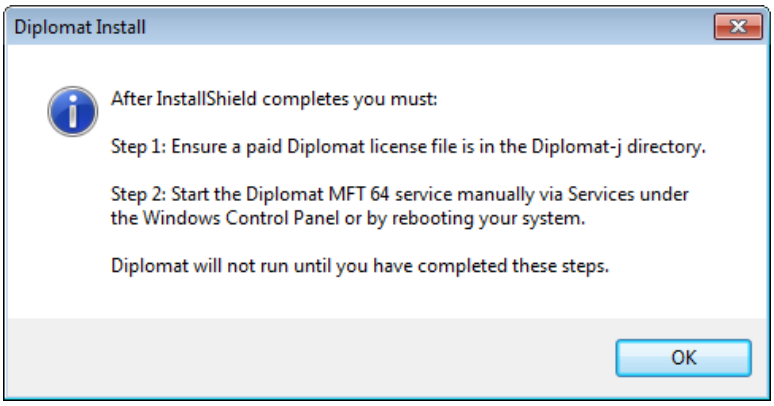
6. Double-click on the filename to start the upgrade. You can change an upgrade setting by selecting **Back** until you reach the previous window where the change is needed. Otherwise, select **Next** to continue to the next step. You can select **Cancel** at any time to stop the upgrade.



7. 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.



8. If you are upgrading the Diplomat MFT Service, when the upgrade is complete, you must:



- Start the Windows service named *Diplomat MFT 64*, which starts and stops the Tomcat web server, before attempting to start the Diplomat MFT Client. The Diplomat MFT Service is set to start automatically on reboot. You can manually start the service through **Services** under the Windows **Control Panel.**

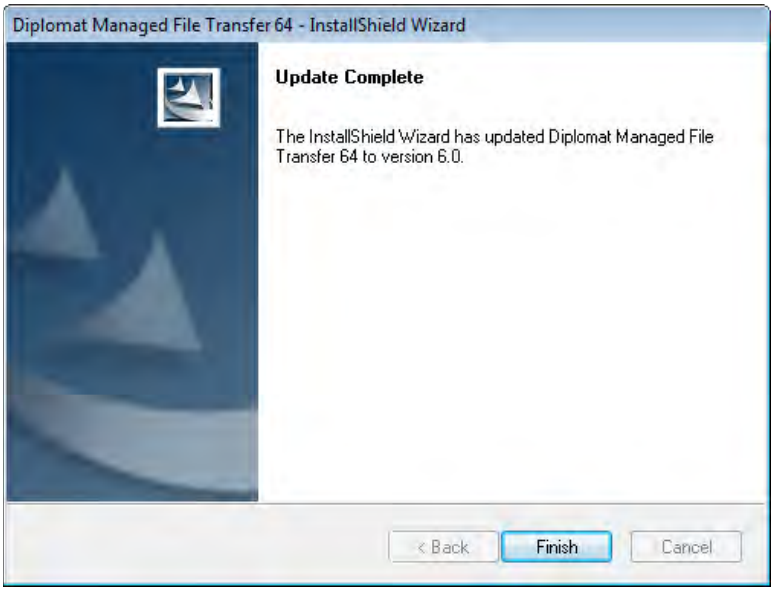
  NOTE: When possible, the Diplomat MFT Service Windows logon account is retained after the upgrade.

- Confirm that the Tomcat web server is working properly. Open a browser window and navigate to the secure page https://localhost:8080/. You should see the Tomcat home page. If the Tomcat server 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 may receive a message from your browser indicating a problem with the web site's security, Select *Continue* in order to access the Tomcat home page.

9. The final screen indicates that you have successfully completed the upgrade.



NOTE: After the upgrade, be sure to release all transactions in the Diplomat MFT Client.

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 user name 'diplomat'. Log on with user name '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 using the username and password supplied by Coviant Software Support. Navigate to http://www.coviantsoftware.com/support-portal.php. Download diplomatServer.tar.gz for the correct edition of Diplomat Managed File Transfer.

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/setup or corresponding directory for your installation. This script copies the diplomatServer daemon into the /etc/rc.d/init.d directory, which starts the diplomatServer daemon on system startup.

   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.

   You can use the following commands to check the status of or change the diplomatServer daemon:

Command	Action
chkconfig --list	Display status of daemons, including diplomatServer
chkconfig diplomatServer on	Configure the diplomatServer daemon to start automatically on reboot
chkconfig diplomatServer off	Disable automatic start of diplomatServer daemon on reboot
chkconfig --del diplomatServer	Permanently delete diplomatServer daemon
service diplomatServer start	Manually start the diplomatServer daemon
service diplomatServer stop	Manually stop the diplomatServer daemon
service diplomatServer status	Check status of the diplomatServer daemon

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. To confirm that the diplomatServer daemon is operating correctly, open a web browser and navigate to the secure page https://localhost:8080. You should see the Tomcat home page.

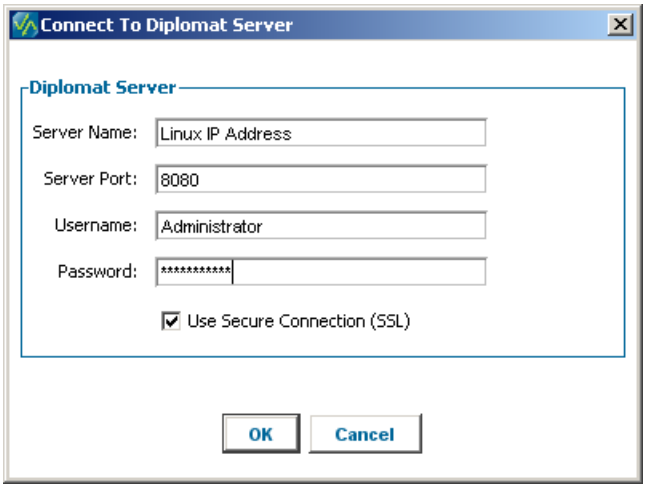
   If you do not see the Tomcat home page, log on as 'root' or other account with 'root' privileges.

   Check whether the diplomatServer daemon was successfully created using the 'chkconfig --list' command. If you do not see the diplomatServer daemon in the list of daemons, repeat the setup for the diplomatServer daemon.

   If the diplomatServer daemon does appear in the list, check the status of the diplomatServer daemon using the 'service diplomatServer status' command. If the diplomatServer daemon is not running, restart the daemon using the 'service diplomatServer start' command.

   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.

9. Check that the Diplomat MFT Service is functioning by starting the Diplomat MFT Client on a Windows system. Connect to the Diplomat MFT Service using the IP address or domain name of the Linux system and the port number '8080'. The default username is 'Administrator' and the default password for all licenses is 'diplomat' for all licenses. You must reset this password immediately after you install a new license.



NOTE: The Diplomat MFT Client must be the same version as the Diplomat MFT Service. If the Diplomat MFT Service and Client are not the same version, you will receive a message similar to the following one:

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

11. 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 user name 'diplomat'.

4. Go to www.coviantsoftware.com and log on using the username and password supplied by Coviant Software Support. Navigate to http://www.coviantsoftware.com/support-portal.php. Download diplomatServer.tar.gz for the correct edition of Diplomat Managed File Transfer.

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

6. 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.

7. 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.

8. To confirm that the diplomatServer daemon is operating correctly, open a web browser and navigate to the secure page https://localhost:8080/. You should see the Tomcat home page.

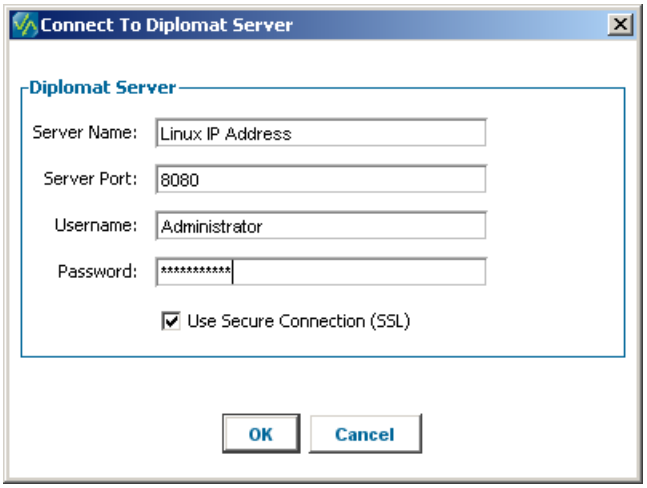
   If you do not see the Tomcat home page, log on as 'root' or other account with 'root' privileges.

   Check whether the diplomatServer daemon was successfully created using the 'chkconfig --list' command. If you do not see the diplomatServer daemon in the list of daemons, repeat the setup for the diplomatServer daemon.

   If the diplomatServer daemon does appear in the list, check the status of the daemon using the 'service diplomatServer status' command. If the diplomatServer daemon is not running, restart the daemon using the 'service diplomatServer start' command.

   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.

9. Check that the Diplomat MFT Service is functioning by starting the Diplomat MFT Client on a Windows system. Connect to the Diplomat MFT Service using the IP address or domain name of the Linux system and the port number '8080'. The default username is 'Administrator' and the default password is 'diplomat' for all licenses. You must reset this password immediately after you install a new license.



NOTE: The Diplomat MFT Client must be the same version as the Diplomat MFT Service. If the Diplomat MFT Service and Client are not the same version, you will receive a message similar to the following:

2.2.3 Diplomat MFT Service Remove

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. Log on as 'root' or other account with 'root' privileges.

3. 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.

4. 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.

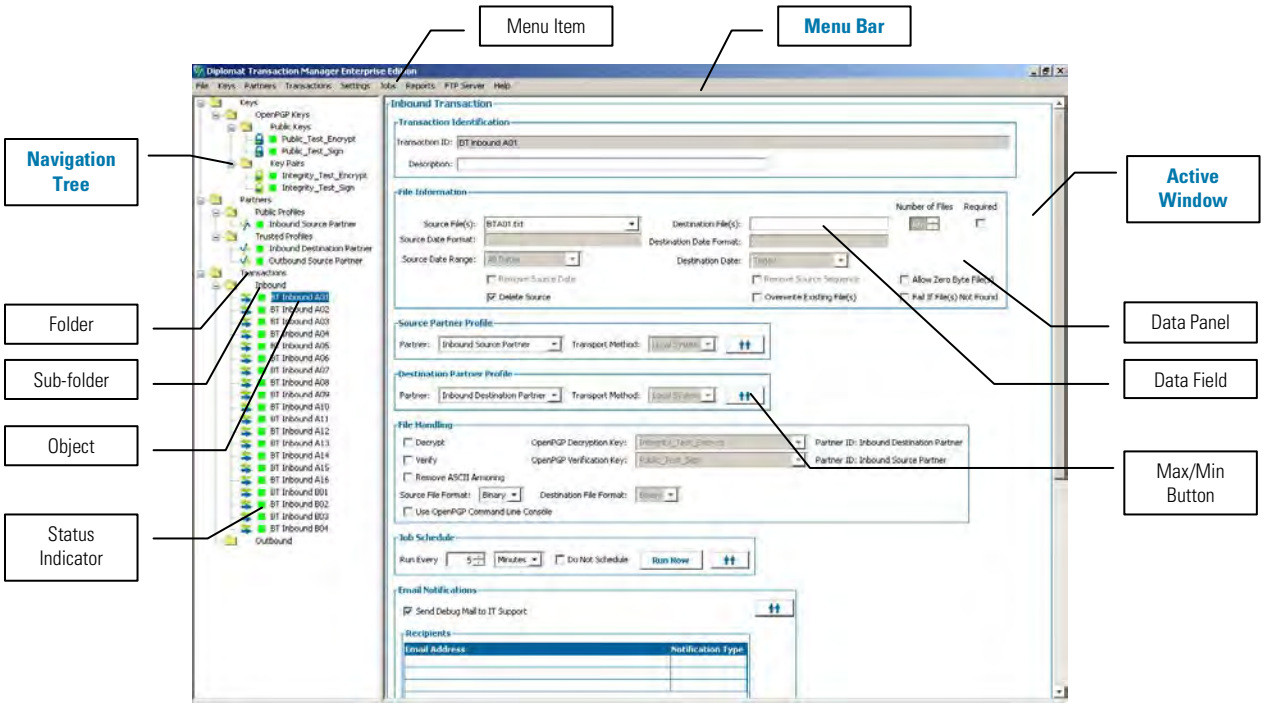
2.3 Web Launch

Diplomat MFT Web Launch enables the user to run the Diplomat MFT Client, Scripting Agent and Job Monitor from a browser on Windows systems without needing to install the Diplomat MFT components on their local system. Contact your local Diplomat MFT administrator for instructions on whether Diplomat Web Start is supported and how to access it. Refer to the Diplomat MFT Web Start User Guide for further information.

3 Basics

3.1 User Interface Overview

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.



Diplomat MFT Enterprise Edition Client Main Screen

Menu Bar allows access to a variety of functions via sub-menus and pop-up dialog boxes:

- File – Control license management, check status of Diplomat MFT service and current connections, password updates, backup, merge, restore, view log files, and exit.
- 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 to view job history, execute, cancel, and/or terminate jobs.
- Reports – Generate key, partner, transaction, or audit reports.
- FTP Server Administration (Optional) – Create integrated access to or FTP server management consoles, if desired.

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

Navigation Tree on the left-hand side of the main screen displays folders, sub-folders, and objects in a tree format for easy navigation. The navigation tree also:

- Displays root folder name, which is the name of the server where the Diplomat MFT Service is installed and the Diplomat MFT version number. On rollover, the domain and username set as the Diplomat MFT Service logon is displayed. If no logon is set, then a generic logon, such as NT AUTHORITY/SYSTEM is shown on rollover.
- Displays partner profiles and keys that are available for use in defining transactions.
- Highlights the name of the partner profile, transaction, or key that is currently displayed in the active window for viewing or editing.
- Bolds the name of any partner profiles, transactions, and keys that have changes pending before being saved.
- Indicates scheduling status of transactions by displaying:
    - Red status indicator for transactions that are not scheduled to run,
    - Green status indicator for transactions that have a job currently scheduled for execution,
    - Dark green status indicator for transactions that are set to allow external requests.
    - Light green status indicator for transactions that are set to use the file monitor.
    - Yellow status indicator for transactions that have been suspended directly, and
    - Orange status indicator for transactions that have been suspended indirectly.
- 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.
- Allows functions, such as Export, Save, Save As, Reset, Validate, View Logs, Run Now, Delete, Release, Suspend, or Search/Move, by right-clicking transactions, keys, partners, and/or folders.

3.2 Database Overview

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

- **Diplomat MFT transaction Database** is an embedded SQL database which contains all data used to create and schedule jobs, including keys, partner profiles, transaction, and configuration data.

  NOTE: You can execute *runDiplomatTransactionDb* at the command line on the Diplomat MFT site to manually view the contents of this database or to create a backup file of the database. Refer to *Transaction Database Viewer FAQ* for more detailed instructions.

- **Diplomat MFT Job History Database** is an embedded SQL database which contains all job and file history records.

  NOTE: You can execute *runJobHistoryDb* at the command line on the Diplomat MFT site to manually view the contents of this database. Refer to *Job History Database Viewer FAQ* for more detailed instructions.

- **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 or an external SQL database with job, file, and user table.

3.3 Diplomat MFT Security Model

Diplomat MFT ensures the security of your data at all times.

- Before files are transferred, use OpenPGP keys to encrypt and sign the files.
- During file transfer, choose HTTPS, SFTP (SSH2), FTPS (TLS/SSL) or Diplomat Cloud Connector to protect both login data and data in transit.
- After files are transferred, use OpenPGP keys to decrypt and verify files.

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

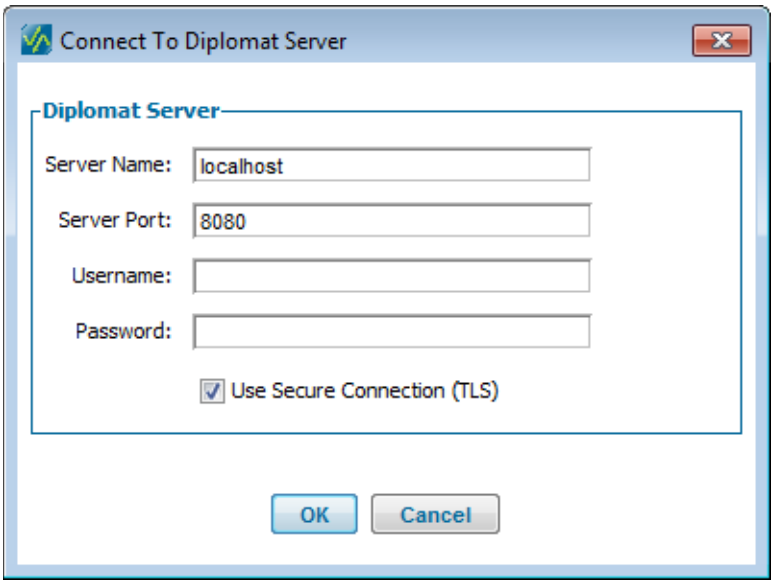
- Provides additional protection by allowing only accounts with *Administrator* privileges to execute sensitive activities, such as updating user account and other settings, Diplomat MFT licenses, and database restores.
- Tracks all user activity, such as changes to the Diplomat MFT transaction database, by the User ID provided by the operating system where the Diplomat MFT Client is running. Data on each user activity 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 plaintext (i.e., unencrypted) format.
- Uses a secure connection (TLS) for all communications between the Diplomat MFT Client and the Diplomat MFT Service.
- Executes transactions using the Diplomat MFT Service or the diplomatServer daemon – which does not require that the Diplomat MFT Client be running.
- Only requires the entry of passphrases to manage 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.

3.4 Security Best Practices

You can improve the security of your Diplomat MFT implementation by following a few security practices:

- Install and run both Diplomat MFT Service and Diplomat MFT Client behind a firewall.
- Limit the number of OpenPGP key pairs that you create, so that you remember the correct passphrase associated with each key without writing it down.
- Sign all outbound transactions to ensure that your trading partner knows the files have not been tampered with and that they went sent by you.
- Verify all inbound transactions to ensure that you know the source of the encrypted file.
- Set Diplomat MFT to require changing passwords used to access the Diplomat MFT Client every 3 months.
- Set Diplomat MFT to encrypt backup files of the Diplomat MFT transaction database.
- Create multiple encryption sub-keys covering different time periods when you create new key pairs. Your trading partners use your same public key to encrypt, but the encryption sub-key changes on a regular basis – making your transactions more secure. (See Section 6.3.1.1.2 *Add Subkeys* for a more detailed explanation of this approach.)

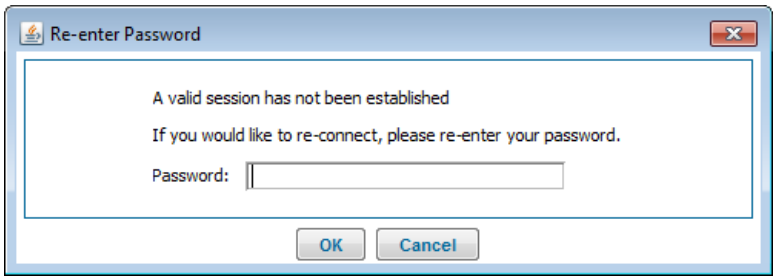
4 Logging On



When the Diplomat MFT Client starts, you are prompted to provide information so the Diplomat MFT Client can access the Diplomat MFT Service.

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

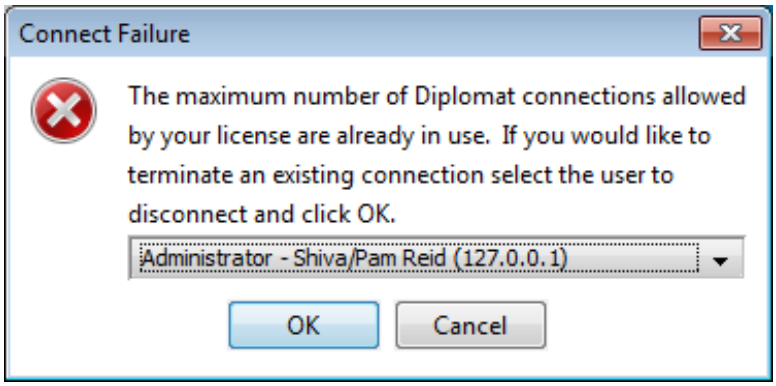
When the session limit is reached, the Diplomat MFT Client is automatically logged out and the number of active Diplomat MFT Client logins on the Diplomat MFT Service is decremented by 1. The terminated Diplomat MFT Client remains open but can no longer communicate with the Diplomat MFT Service until the password for the session has been re-entered.



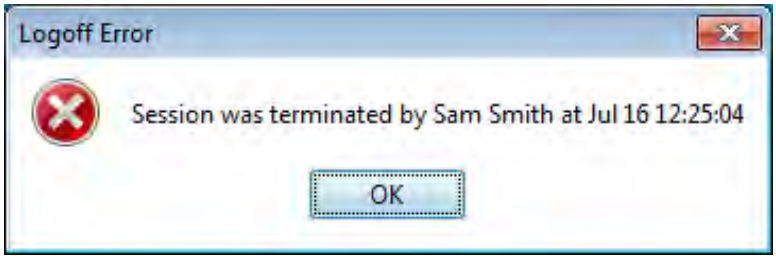
The Diplomat MFT Client must be the same version as the Diplomat MFT Service. If the Diplomat MFT Service and Client are not the same version, you will receive a message similar to the following one:

Diplomat MFT requires different license types for trial and paid copies. If your license type is not valid with this copy, the following error message is displayed. You must either uninstall all Diplomat Managed File Transfer components and install the correct copy or obtain the correct type of license.

If the maximum number of concurrent Diplomat MFT Client connections is already in use, the Username and Domain/User IDs of the connected users are displayed and you are prompted whether or not to terminate one or more existing connections. An account with Reviewer privileges can log off other accounts with Reviewer privileges. An account with *Administrator* or *Manager* privileges can log off any other user.



If you terminate an existing connection, the terminated Diplomat MFT Client session remains open but can no longer communicate with the Diplomat MFT Service and a dialog is displayed indicating which user terminated the session.



4.1 Server Name

Server Name is the network address of the system running the Diplomat MFT Service or the diplomatServer daemon. If the Diplomat MFT Client and the Diplomat MFT Service are installed on the same system, the server name can be 'localhost'. If the Diplomat MFT Service is located on a different system than the Diplomat MFT Client, the server name is the network IP address or domain name of the system running the Diplomat MFT Service.

4.2 Server Port

Server Port is set to 8080 by default. If you uncheck *Use Secure Connection*, *Server Port* automatically resets to 8443. If port 8080 or 8443 is already in use, contact Coviant Software Support for instructions on how to change the server port number or refer to the *Changing Diplomat Services Port Numbers FAQ* on changing Diplomat MFT Service port numbers.

4.3 Username and Password

When the Diplomat MFT Client is initially installed, the default password for the username 'Administrator' is set to 'diplomat'. Use the Change Password feature under File > Password to update the password for the current user.

Login to the Diplomat MFT Client and Job Monitor may require:

- Username and password combination
- Automatic authentication with the Domain and User ID of the current user without entering username and password
- Both a username/password combination and authentication with the Domain/User ID

The login requirements for each user are set under Settings > User Accounts from the top menu.

When a password is updated, the new password must be a minimum of 6 characters and include both alpha and non-alpha characters.

NOTE: Passwords are case sensitive.

It is very important to change your password regularly. Although an uninvited user cannot import, modify, export, delete, or recover key pairs without the matching passphrase, anyone who can log on to Diplomat MFT can set up transactions using your key pairs. By default, passwords must be updated at least every 6 months.

4.4 Secure Connection

Use Secure Connection (TLS) protects all communication between the Diplomat MFT Service and the Diplomat MFT Client using Transport Layer Security (TLS). If you uncheck *Use Secure Connection*, *Server Port* automatically resets to 8443.

5 File Menu

5.1 File Overview

The File Menu allows you to backup and restore the Diplomat MFT transaction database, manage your Diplomat MFT license, view log files, update your login password, display the status of the Diplomat MFT Service and the underlying system, display current connections, and exit the Diplomat MFT Client.

5.2 File Menu Items

5.2.1 Backup

This backup feature is not intended to replace regular backups of the Diplomat MFT data as part of your overall backup process.

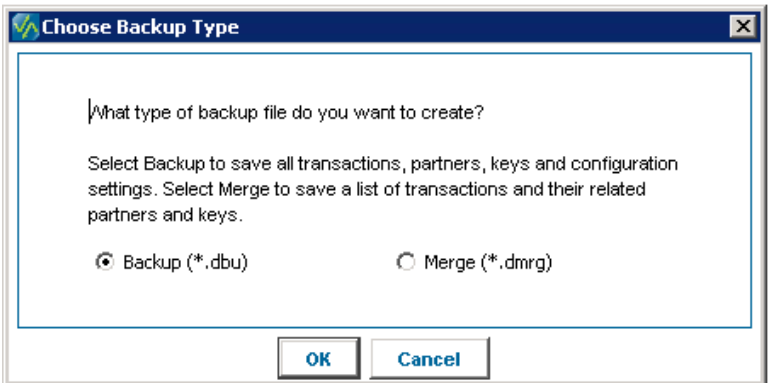
Backup creates a single file snapshot of the Diplomat MFT transaction database.

You can manually back up the Diplomat MFT database by selecting File > Backup and, unless you override the default under Settings > Backup, you are prompted on **Exit** to back up your database.

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. Use **Browse** to select a different directory. Use **Test** to determine whether the location is accessible and is read/write enabled for the logon identity used by the Diplomat MFT Service.

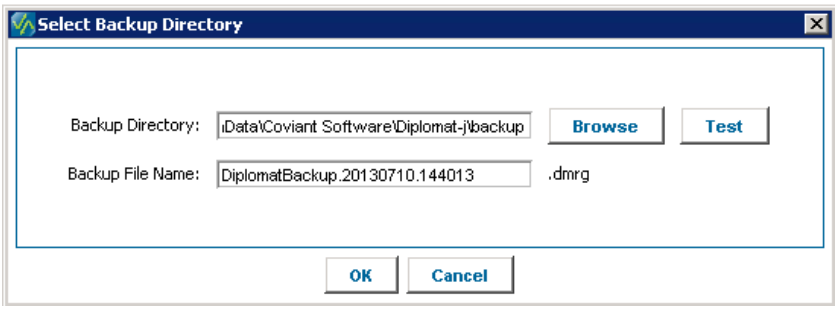
NOTE: Select Settings > Backup to edit all Backup Settings.

A backup copy of the database contains the key, transaction, partner, configuration settings, and job suspension data as of the time the backup was done. A merge copy of the database contains selected transactions and their related partners and keys.



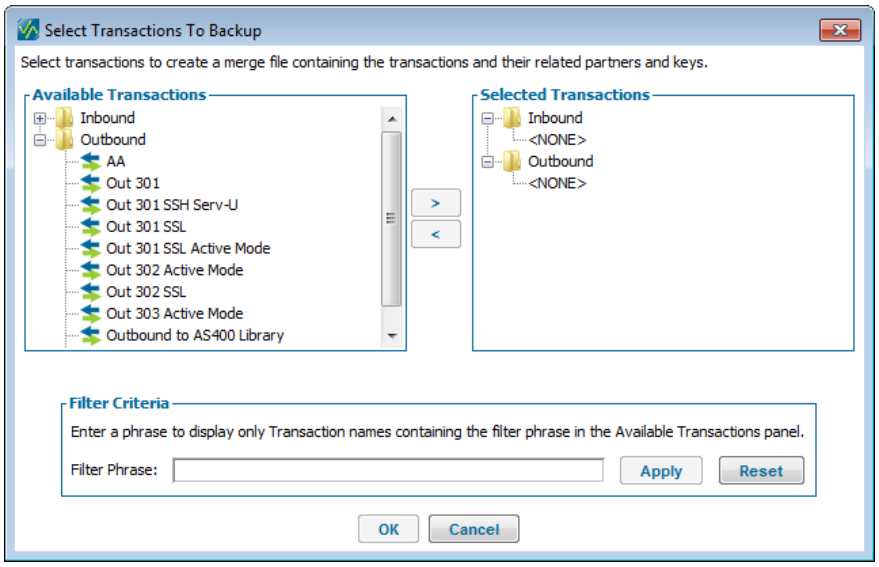
The default backup filenames are in the form 'DiplomatBackup.version.year + month + day + hour + minutes + seconds.dbu'. For example, a backup created on September 22, 2004 at 1:19:20 p.m. by Diplomat MFT v6.0 would be named 'DiplomatBackup.6.0.20040922.131920.dbu'. If desired, you can enter a different backup filename.

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



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.



5.2.2 Merge

NOTE: *Merge* is only available to accounts with administrator privileges.

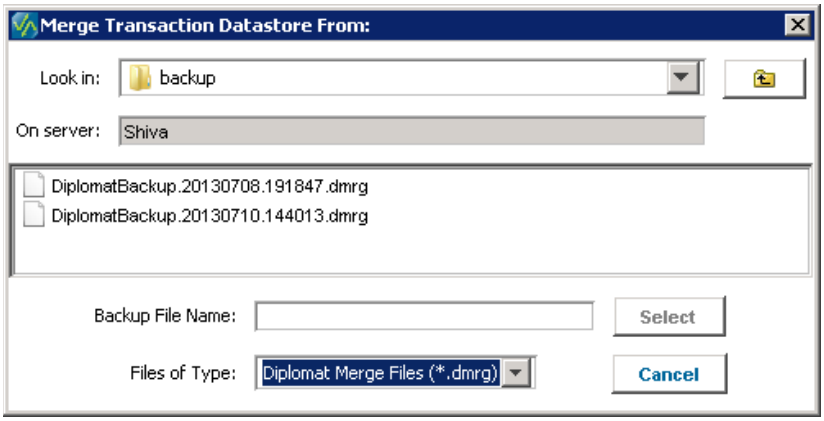
Use Merge **ONLY** if you need to **ADD** or **OVERWRITE** keys, partners, or transactions from a backup or merge file to your current set of keys, partners, and transactions. Use Restore to replace an entire database with a backup copy.

NOTE: Even if transactions in the active database are overwritten during a merge or restore with transactions using the same Transaction Name, the job history data is not deleted for Transactions Names in the active database and the job monitor may display data for jobs that ran prior to the merge or restore operation.

You can merge your Diplomat MFT database by selecting File > Merge.

NOTE: Diplomat MFT attempts to write a backup copy of the Diplomat MFT database to the default backup directory before initiating a database merge or restore operation.

Browse and select the backup file that you would like to merge with your active database.

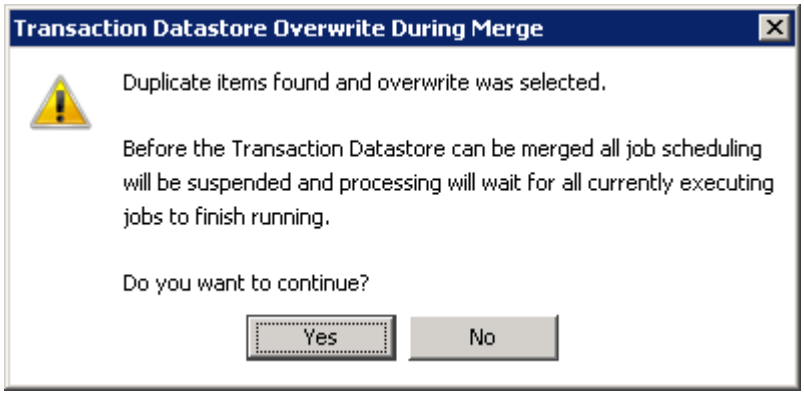


If the backup or merge file is encrypted, you must also enter the password used when the file was created.

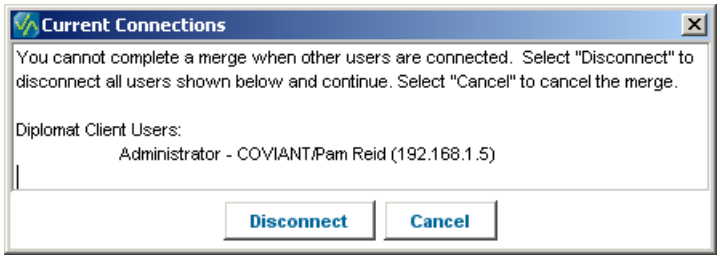
When merging Diplomat MFT databases, you must decide how duplicate items are handled during the merge process. For example, if you have a key with the same name in both databases, you must choose which key you would like retained in the database after the merge process is complete.

If you want the items in your active database retained, indicate that duplicate items should **not** be overwritten during the merge. If you want the items from the Diplomat MFT backup file to be retained, then indicate that duplicate items should be overwritten during the merge.

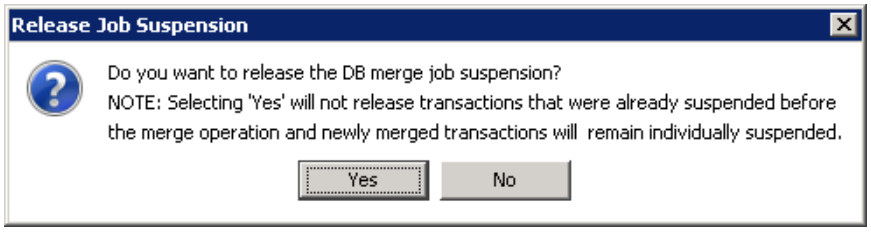
Diplomat MFT checks whether any of the transactions to be merged require an existing key, partner or transaction to be overwritten. If so, all job scheduling will be suspended and processing will wait for all currently queued or running jobs finish executing before starting the merge.



You cannot complete a merge when other users are connected. Select 'Disconnect' to disconnect all users and continue with the merge. Select 'Cancel' to cancel 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.



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*.

NOTE: If any keys, partners, or transactions were already suspended in your active Diplomat MFT database prior to executing a merge, these keys, partners, and transactions remain suspended after you select *Release DB Merge/Restore Suspend*.

NOTE: In addition, all individual keys, partners or transactions that were added to the Diplomat MFT database during the merge process also remain suspended after you select *Release DB Merge/Restore Suspend*.

CAUTION: Recoverable keys are not considered during a Diplomat MFT database merge. Recoverable keys are OpenPGP or SSH client keys which have been deleted, but are still available for recovery. Recoverable keys in the active database remain available for recovery after the merge. Recoverable keys in a Diplomat MFT backup or merge file being merged with a live database are ignored during the merge and do not appear in the active Diplomat MFT database after the merge.

To merge a recoverable key from a Diplomat MFT backup file into an active database, you must either:

- Restore the Diplomat MFT backup file containing the recoverable key and keep a backup of the active database. Recover the desired key. Export the key. Restore the active database. Import the key into the active database.
- Restore the Diplomat MFT backup file containing the recoverable key and keep a backup of the active database. Recover the desired key. Backup the Diplomat MFT database containing the recovered key. Restore the active database. Merge the active database with the newly saved Diplomat MFT backup file.

5.2.3 Restore

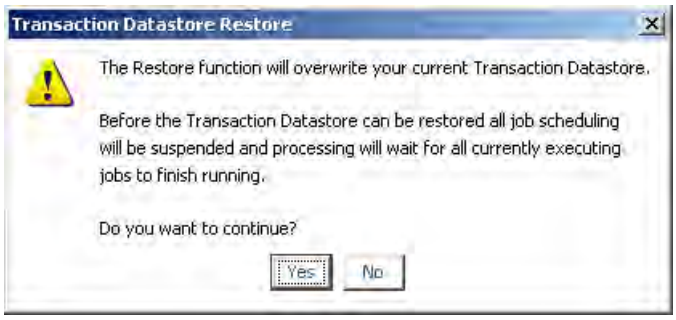
NOTE: *Restore* is only available to accounts with *Administrator* privileges.

Use Restore to replace an entire Diplomat MFT database with a backup copy. After completing a Restore, the Diplomat MFT database contains the key, transaction, partner, and job suspension data as of the time the backup was done. Any changes to the database since the backup was done will be lost.

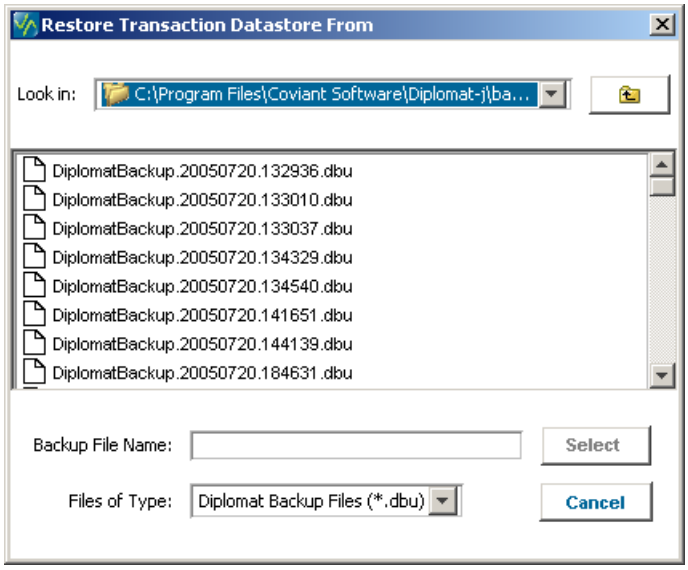
NOTE: Even if transactions in the active database are overwritten during a merge or restore with transactions using the same Transaction Name, the job history data is not deleted for Transactions Names in the active database and the job monitor may display data for jobs that ran prior to the merge or restore operation.

You can restore your Diplomat MFT database by selecting File > Restore. All job scheduling will be suspended and processing will wait for all currently queued or running jobs finish executing before starting the restore.

NOTE: Diplomat MFT attempts to write a backup copy of the Diplomat MFT database to the default backup directory before initiating a database merge or restore operation.



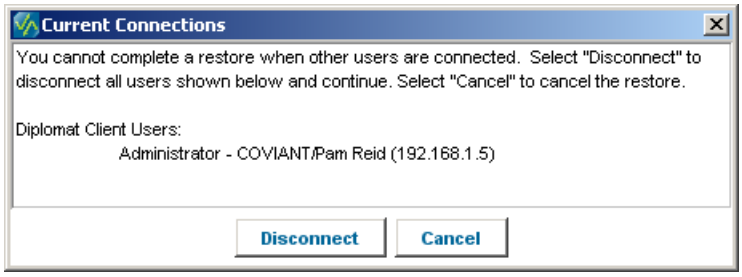
Then, you can browse and select the backup of the database that you would like to restore.



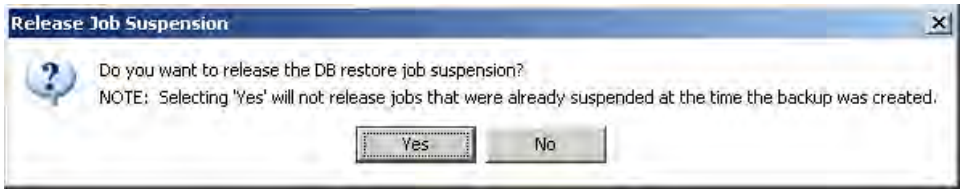
If the backup file is encrypted, you must also enter the backup file password.

You have the option to restore configurations settings, as well as the Diplomat MFT transaction database**. NOTE:** Only backup files created with Diplomat v3.5 or later contain configuration settings. When backup files created prior to v3.5 are restored, no configuration settings can be restored.

You cannot complete a restore when other users are connected. Select 'Disconnect' to disconnect all users and continue with the restore. Select 'Cancel' to cancel 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*.

NOTE: If any keys, partners, or transactions were already suspended prior to a restore occurring, these keys, partners, and transactions remain suspended after you select *Release DB Merge/Restore Suspend*.

5.2.4 License

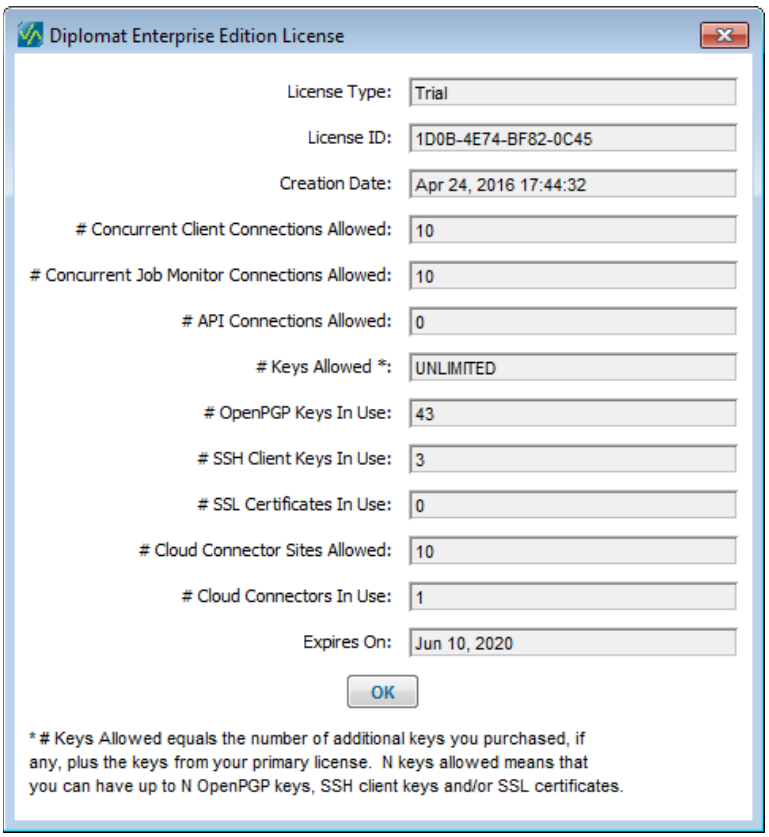
NOTE: *License* information is only available to accounts with *Administrator* privileges.

Diplomat Managed File Transfer is licensed based on the total number of OpenPGP, SSH client keys, and/or SSL certificates, the number of concurrent client connections, the number of concurrent job monitor connections, the number of Diplomat Cloud Connector sites, and the number of API connections associated with your License ID. The number of allowable keys, client connections, job monitor connections, Diplomat Cloud Connector sites and API connections equals the number you purchased. The License screen displays the information contained in your current license file, *diplomat.lic*.

NOTE: If no *diplomat.lic* file was found when the Diplomat MFT Service started, a 'Server initialization failed: No License' error message is generated when the Diplomat MFT Client attempts to start. To correct this problem, stop the Diplomat MFT Service. Navigate to the license file directory. For Windows systems, the default license directory is C:\ProgramData\Coviant Software\Diplomat-j. For Linux systems, the default directory is the installation directory, usually opt/coviant/diplomat-j. Copy a valid license file into the directory. Rename the license file to *diplomat.lic* and restart the Diplomat MFT Service.

NOTE: For more information on license file locations on Windows systems, please refer to *Windows Systems with User Account Control FAQ*.

NOTE: If the *diplomat.lic* license file has expired and the Diplomat MFT Client attempts to start, a 'License has expired' error message is generated. If you do not have a new license file, contact Coviant Software Support to request one. To install the new license, stop the Diplomat MFT Service. Navigate to the license file directory. For Windows systems, the default license directory is C:\ProgramData\Coviant Software\Diplomat-j. For Linux systems, the default directory is the installation directory, usually opt/coviant/diplomat-j. Copy a valid license file into the directory. Delete the existing *diplomat.lic* file. Rename the new license file to *diplomat.lic* and restart the Diplomat MFT Service.



License Type

License Type is Preview, Trial, or Paid. Preview licenses do not allow PGP encryption or file transfer job execution. Trial licenses are time-limited with full product functionality. Paid licenses enable full product functionality. Preview and trial licenses work with trial installations. Paid licenses work with paid installations.

License ID

License ID, a 16-digit number, is used to track your license and any related maintenance services. This number appears on your maintenance agreement and the About Diplomat MFT screen under Help.

Creation Date

Date and time license file created.

Number of Concurrent Client Connections Allowed

Number of concurrent Diplomat MFT Client logins allowed by the Diplomat MFT license. **NOTE:** The Diplomat MFT Service can support multiple concurrent Diplomat MFT Client logins. Contact Coviant Software Support for information on how to license additional concurrent Diplomat MFT Client logins.

Number of Concurrent Job Monitor Connections Allowed

Number of concurrent job monitor connections allowed by the Diplomat MFT license. **NOTE:** The Diplomat MFT Service can support multiple concurrent job monitor connections. Contact Coviant Software Support for information how to license additional job monitor connections.

Number of API Connections Allowed

The number of Diplomat MFT API connections allowed is determined by whether you purchased a Diplomat MFT API license.

Number of Keys Allowed
Diplomat Managed File Transfer is licensed based on the number of OpenPGP keys you are allowed to use to encrypt/decrypt and sign/verify files, SSH client keys used to validate login to an SFTP (SSH2) server, and/or SSL certificates to validate login to an FTPS (TLS/SSL) server.

NOTE: You can have up to the number of keys allowed of EACH OpenPGP keys, SSH client keys, and SSL certificates.

The number of keys allowed is equal to the number of additional keys you purchased plus the keys from your primary edition license. You must purchase an additional key for each trading partner or an unlimited key license. If you purchased an unlimited key license, the value of this field is 'UNLIMITED'.

Number of OpenPGP Keys in Use
The number of OpenPGP keys in use equals the number of OpenPGP keys that you have created or imported into Diplomat. The total number of OpenPGP public keys and key pairs in use equals the number of OpenPGP keys displayed in the navigation tree.

Number of SSH Client Keys in Use
The number of SSH client keys in use equals the number of SSH client keys that you have created or imported into Diplomat. The number of SSH client keys in use equals the number of SSH client keys displayed in the navigation tree.

Number of SSL Certificates in Use
The number of SSL certificates in use equals the number of SSL certificates that you have created or imported into Diplomat. The number of SSL certificates in use equals the number of SSL certificates displayed in the navigation tree.

Number of Cloud Connector Sites Allowed
The number of Diplomat Cloud Connector sites allowed is equal to the number of additional Diplomat Cloud Connector site licenses you purchased plus the Diplomat Cloud Connector sites from your primary edition license, if any.

Number of Cloud Connector Sites in Use
The number of Diplomat Cloud Connector sites in use equals the number of unique hostname/port combinations in all partner profiles and transactions.

Expires On
Date your Diplomat MFT license expires. You will not be able to run the Diplomat MFT Service or the Diplomat MFT Client after this date. If you purchased a perpetual license, the value of this field is 'Never'.

Activate Button
The *Activate Button* is displayed when the directory that contains the current *diplomat.lic* file also contains a file with a .lic file extension with a creation date/time field that is more recent than the current license file.

NOTE: You can typically check the create date in the file properties to determine this date.

For Windows systems, the default license directory is C:\ProgramData\Coviant Software\Diplomat-j. For Linux systems, the default directory is the installation directory, usually opt/coviant/diplomat-j.

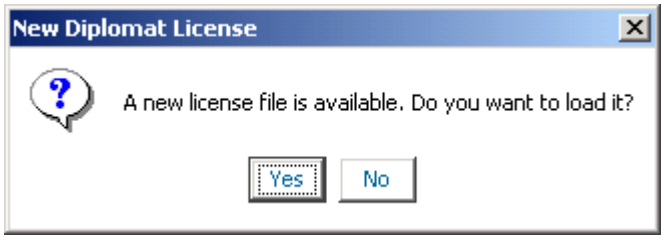
NOTE: The Activate Button is displayed only when the new license file is for the same Diplomat MFT Edition. If you need to update your license to a different Diplomat MFT Edition, follow the directions in the next section.

NOTE: The Activate Button is displayed when it matches the type of license required by the Diplomat MFT copy installed. For a trial installation, only preview and trial licenses are displayed. For a paid installation, only paid licenses are displayed.

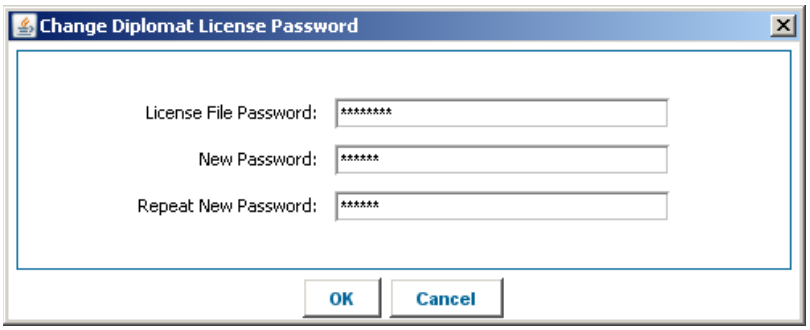
5.2.5 License Update

To update your license to a new Diplomat MFT Edition, you must place the new license file in the directory where the current license, *diplomat.lic*, is located. For Windows systems, the default license directory is C:\ProgramData\Coviant Software\Diplomat-j. For Linux systems, the default directory is /opt/coviant/diplomat-j.

Once the new license file has been copied to the correct directory, you can update your license by restarting the Diplomat MFT Client. You are notified that a new license is available and prompted whether you would like to accept it.



When your license is updated, the current *diplomat.lic* file is deleted and the new license file is renamed to *diplomat.lic*. Log into the Diplomat MFT Client using your current password. You can reset your password using the File > Password menu option which displays the Change Diplomat License Password screen.



NOTE: The date/time field in the new license must be more recent than the date/time field in the current *diplomat.lic* file. If the new license file is older than the current license, Diplomat MFT does not prompt you to update your license. You can typically check the create date in the file properties to determine this date.

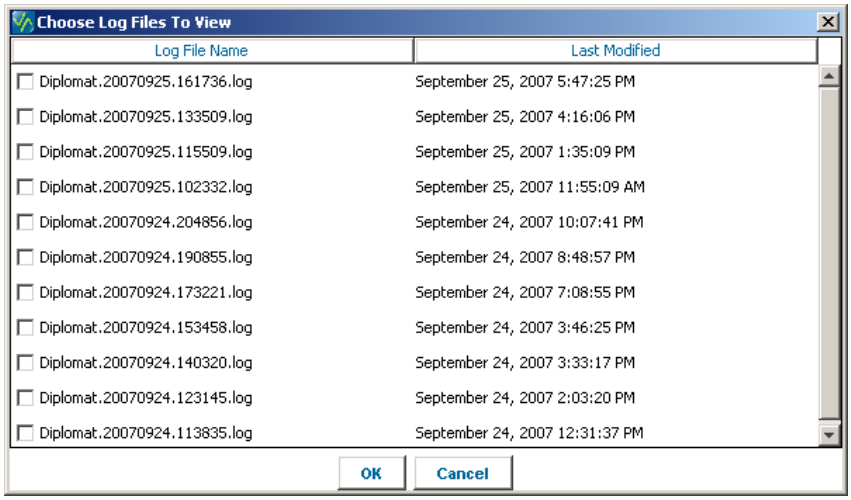
5.2.6 Logs

You can view the content of log files by selecting File > Logs, then choosing the log files that you would like to view. If you check more than one log file on the Choose Log Files to View screen, then all selected log files are appended into one screen for viewing.

NOTE: Only log files located in the directory specified under Settings > Logging are shown. For Windows systems, the default location is C:\ProgramData\Coviant Software\Diplomat-j\logs. For Linux systems, the default directory is /opt/coviant/diplomat-j/logs.

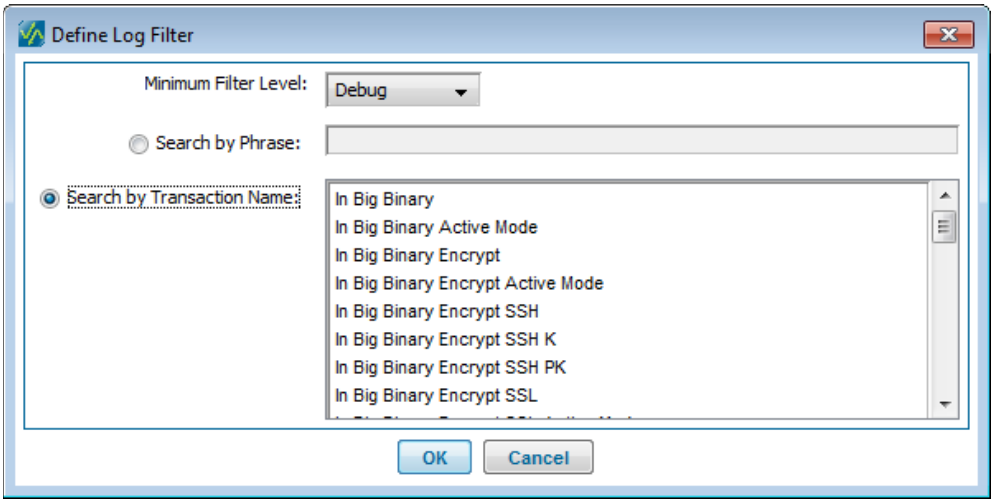
NOTE: To view Diplomat Cloud Connector log files, use the *View Logs* button in a Cloud Connector Partner Profile panel.

NOTE: Logging settings can be updated under Settings > Log File**.**



Set Filter

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.



Minimum Filter Level

Limits the log messages selected to include only log messages with a particular log level or above. The filter levels correspond to the log levels that can be set under Settings > Log File. 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. This feature is helpful when you are searching for a particular entry (e.g., 'audit database failure') unrelated to a particular transaction.

Search by Transaction Name

Allows you to select all log messages related to a particular transaction. If no transaction is selected, then all transactions are displayed, which is the default. This feature allows you to view all entries associated with a particular transaction in chronological order.

NOTE: If you do not filter by *Transaction Name*, entries from various transactions are likely to be mixed together as Diplomat MFT uses a multi-threaded job execution process and log messages are written in chronological order.

NOTE: Only transactions in the current Diplomat MFT transaction database are displayed in the transactions drop-down.

Reset Filter

Resets the log viewer to the default, such that all messages are displayed.

Refresh

Re-displays the current log file using the current filter settings and includes any additional messages added to the log file since the last refresh.

Done

Closes the Diplomat MFT Log Viewer.

5.2.7 Sample Log File

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, including:

- Entries for user activity that affects the content of the Diplomat MFT transaction database, such as updating transactions, changing a password, or importing a public key from a trading partner.
- Entries for each step in the execution of a file transfer job.
- Summary entry at the end of each job containing the same overview information that is included in email sent to business users.
- Error messages.

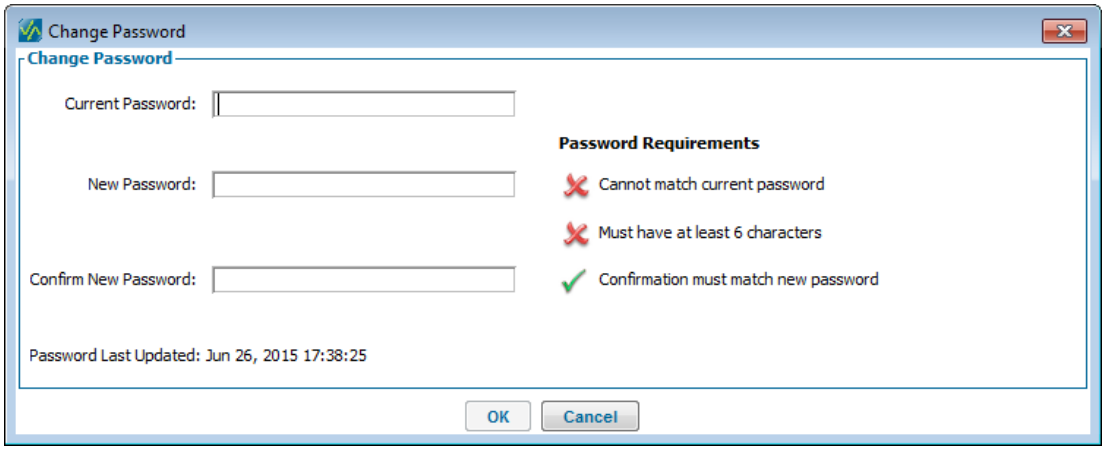
```
>Informational          November 12, 2007 5:01:38 PM EST
Transaction "Out 308": Begins execution

>Informational          November 12, 2007 5:01:38 PM EST
Transaction "Out 308": Outbound job started

>Informational          November 12, 2007 5:01:38 PM EST
Transaction "Out 308": Directory: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Outbound RT Source
            304.txt
            305.txt
            306.txt
            307.txt
            308.txt

>Informational          November 12, 2007 5:01:38 PM EST
Transaction "Out 308": Source/destination file pair added to processing list:
308.txt
308.txt.asc

>Informational          November 12, 2007 5:01:38 PM EST
Transaction "Out 308": 1 source files found

>Debug     November 12, 2007 5:01:38 PM EST
Transaction "Out 308": Source filename: 308.txt          Last modified: 20050214.165846

>Debug     November 12, 2007 5:01:38 PM EST
Transaction "Out 308": Unencrypted file created and locked: C:\Program Files\Coviant Software\Beta Test
Files\AsciiBinary\GlobalScape\Outbound RT Source\308.txt

>Debug     November 12, 2007 5:01:38 PM EST
Transaction "Out 308": Signed file created: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-
INF\temp\sig58783.tmp

>Debug     November 12, 2007 5:01:38 PM EST
Transaction "Out 308": Encrypted file created for: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-
INF\temp\enc58785.tmp

>Debug     November 12, 2007 5:01:39 PM EST
Transaction "Out 308": Connected to 75.144.141.131:21
With userID coviant

>Debug     November 12, 2007 5:01:39 PM EST
Transaction "Out 308": FTP connection verified

>Debug     November 12, 2007 5:01:39 PM EST
```

```
Transaction "Out 308": File type set to ASCII

>Debug     November 12, 2007 5:01:39 PM EST
Transaction "Out 308": Successfully stored file 308.txt.asc

>Debug     November 12, 2007 5:01:39 PM EST
Transaction "Out 308": Primary archiving skipped

>Debug     November 12, 2007 5:01:39 PM EST
Transaction "Out 308": Unencrypted file closed

>Debug     November 12, 2007 5:01:39 PM EST
Transaction "Out 308": Encrypted file closed

>Debug     November 12, 2007 5:01:39 PM EST
Transaction "Out 308": Temp signed file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-
INF\temp\sig58783.tmp

>Debug     November 12, 2007 5:01:39 PM EST
Transaction "Out 308": Temp encrypted file deleted: C:\Program Files\Coviant Software\Diplomat-
beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\enc58785.tmp

>Debug     November 12, 2007 5:01:39 PM EST
Transaction "Out 308": Beginning end-of-job processing

>Debug     November 12, 2007 5:01:39 PM EST
Transaction "Out 308": FTP session disconnected

>Informational          November 12, 2007 5:01:39 PM EST
Transaction "Out 308": Transaction terminated successfully

>Informational          November 12, 2007 5:01:39 PM EST
Transaction "Out 308" Summary:

SUCCESS: Out 308 was successful at November 12, 2007 5:01:39 PM

Outbound transaction

Source files obtained from C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Outbound RT Source
          308.txt       Last modified: 20050214.165846 File size: 44

Encryption key(s): Public_Test_Encrypt
Encryption key(s) used: Public_Test_Encrypt_sub0
Signature key: Integrity_Test_Sign
Signature key used: Integrity_Test_Sign

Destination files FTP'd to 75.144.141.131:21/
          308.txt.asc File size before xfer: 680          File size after xfer: 680

Primary archiving skipped

Additional archiving skipped

No audit record written

>Debug     November 12, 2007 5:01:39 PM EST
Transaction "Out 308": Job ended
```

NOTE: In addition to the Diplomat MFT logs, the Tomcat web server generates a separate log file each time the Diplomat MFT Service or the diplomatServer daemon is started. These logs are located in the …\tomcatWebserver\logs directory, which defaults to C:\Program Files\Coviant Software\diplomat-j\tomcatWebserver\logs for Windows systems or /opt/coviant/diplomat-

j/tomcatWebserver/logs for Linux installations. Tomcat log filenames are in the form: 'jakarta_service_ year-month-day.log'. For example, a Tomcat log file created on July 15, 2006 would be named 'jakarta_service_20060715.log'.

5.2.8 Password



Current Password
The current password is the password associated with the current Diplomat MFT Client login.

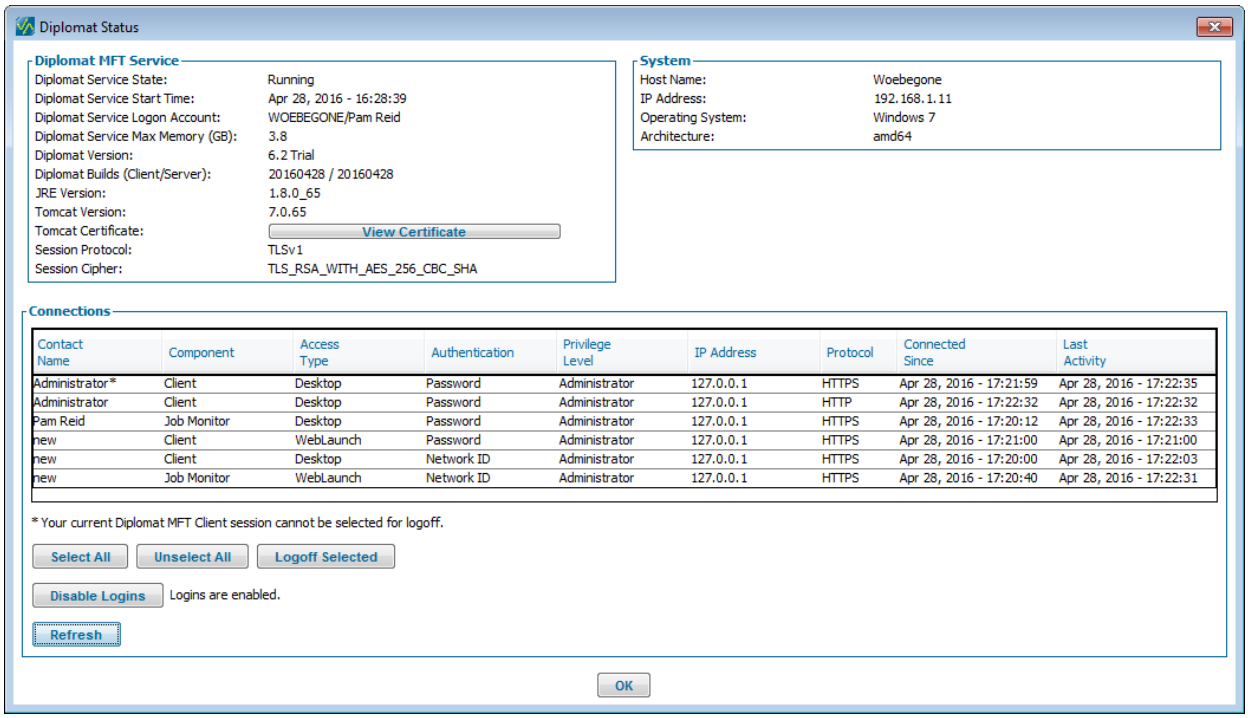
NOTE: To update passwords for other Diplomat MFT users, select Settings > User Accounts from the top menu bar. You must be logged as a user with Diplomat MFT *Administrator* privileges to update user account settings.

New Password/Confirm New Password
You must enter your new password twice to confirm your password change. Once you change the password, you must use the new password to log in to the Diplomat MFT Client.

NOTE: User accounts with *Administrator* privileges can change the password policies under Settings > User Accounts from the top menu bar.

NOTE: Passwords are case sensitive.
NOTE: When the Diplomat MFT Client is initially installed, the default password for the username 'Administrator' is set to 'diplomat'. You must reset this password immediately after you install a new license.

5.2.9 Diplomat Status



Diplomat MFT Service

The *Diplomat MFT Service* panel displays information about the currently installed Diplomat MFT Service, including service state, start time, the domain and username associated with the Diplomat MFT Service, the maximum memory allocated to the Diplomat MFT Service, Diplomat MFT version and build numbers, JRE version, Tomcat version and certificate, session protocol and session cipher,

System

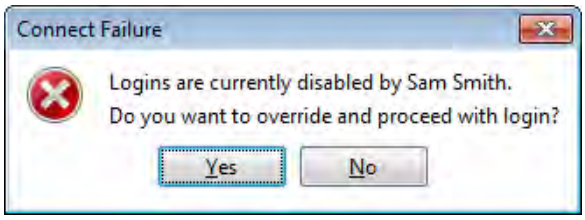
The *System* panel shows the host name, IP address, operating system and architecture of the system where the Diplomat MFT Service is running.

Connections

The *Connections* panel lists all current Diplomat MFT Client and Job Monitor connections to the Diplomat MFT Service. The first item on the list is the Diplomat MFT Client connection of the current Diplomat user account. This account cannot be selected for logoff.

The *Select/Unselect All* buttons select all connections in the list other than the current Diplomat MFT Client connection. The *Logoff Selected* button logs off all of the selected connections.

The *Disable/Enable Logins* button is used to disable all new connections to the Diplomat MFT Service by the Diplomat MFT Client or Job Monitor. Accounts with *Administrator* privileges can still log in when logins are disabled by overriding the setting.



The *Refresh* button refreshes the list of current Diplomat MFT Client and Job Monitor connections.

5.2.10 Exit

Exit closes the Diplomat MFT Client. You are reminded to save any partner profiles or transactions that have changed, but have not been saved, during the session. If you have not turned off *Backup On Exit*, you are asked if you would like to backup your Diplomat MFT database.

NOTE: The state of job scheduling is saved automatically when you exit from the Diplomat MFT Client. If you have suspended some or all transactions, they remain suspended when you reopen the Diplomat MFT Client.

6 Working with Keys

6.1 Keys Overview

OpenPGP and SSH keys are forms of public key encryption technology. Both OpenPGP and SSH keys are built on key pairs. Only a public key is needed to encrypt data. Decryption requires a key pair, which includes a private key in addition to a public key. A public key can be freely distributed without fear that someone will 'guess' your private key, since a key pair cannot be deduced from the associated public key.

When you want to use OpenPGP to protect file transfers, you 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 retaining and protecting your key pair. Each time you send or receive a file, you must specify which key(s) to use to encrypt, decrypt, sign, or verify the file.

SSH keys are used when you log into an SFTP server. With SSH client keys, you create an SSH key pair, export the public key, and send the SSH client public key file to the SFTP server administrator. The server administrator attaches the public key to the account you use to access the SFTP server. When you log into the SFTP server, the SFTP server automatically uses the public key to authenticate your login request.

SSH host keys are used to verify the SFTP server identity before connecting to it. SSH host keys are imported into the Diplomat MFT database and selected when setting up a Diplomat partner profile. SSH host keys are added and deleted from Diplomat MFT using Keys > SSH Host Keys from the top menu bar.

SSL server certificates are also displayed in the navigation tree under *Keys*. SSL server certificates are used when the FTPS server administrator requires them for file transfer jobs using FTPS as the transport method. When an SSL certificate is required, the FTPS server administrator sends you a server certificate file (usually ending in .crt). SSL certificate files are imported into Diplomat MFT from the top menu under Keys > SSL Certificates > Import SSL Certificate.

6.2 Keys Navigation Tree

The navigation tree shows the *Key Name*s of keys currently in the Diplomat MFT transaction database. The keys are divided into sub-folders for OpenPGP keys, SSH Client Keys, and SSL Certificates. OpenPGP keys can be public keys or key pairs. Key pairs are your company's private keys. Public keys are typically keys that you have received from trading partners or remote sites.

Select a sub-folder under OpenPGP Keys, SSH Client Keys 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 text 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 suspend status of keys. Diplomat MFT allows you to immediately suspend all transactions associated with a key. 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 indirectly due to the suspension of the key.

To suspend all transactions associated with a key:

- Select the affected key in the navigation tree.
- Select Jobs > Suspend > Active Key or right-click on the key in the navigation tree and select *Suspend 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 all transactions associated with a key, right-click the key in the navigation tree and select *Release Key*.

NOTE: All transactions that are currently set to *Do Not Run* on the transaction continue to display a red status indicator '■' regardless of suspension status.

6.3 OpenPGP Keys

OpenPGP is a public key encryption technology. You publish your public key to your trading partners or remote sites while retaining and protecting your key pair. Anyone with a copy of your public key can encrypt files using your public key, but only you can decrypt the files.

OpenPGP keys are usually kept in files called key rings or keystores, where keys are stored in encrypted form. If you lose or delete your key ring, you will be unable to decrypt any files encrypted with the keys that were on the ring.

Individual keys can be exported from key rings into single files. For example, you will need to export a key when you send it to a trading partner or if you need to use the key with a different OpenPGP application. Many OpenPGP products keep their public keys and their key pairs in separate key rings. Diplomat MFT keeps all of its keys in a single database. Diplomat MFT can import keys created by other OpenPGP-compliant products and add them to its database.

OpenPGP keys can be used to encrypt/decrypt and to sign/verify files. When you receive a file signed by a private OpenPGP key pair, you can determine the authenticity of the file's origin and verify that the file is intact. Verifying the signature on a file provides non-repudiation, which means that it prevents the sender from claiming that he or she is not the source of the information.

When a file is signed with a key pair, only the public key that matches the private key in the key pair can be used to verify the signature. When you establish a relationship with a trading partner, they send you their public key. Each time they encrypt a file to send to you, they use their private key to sign the file. When you decrypt the file, you determine whether your trading partner encrypted the file by using their public key to verify the signature. If you cannot verify the signature, then you should assume that your trading partner was not the source of the encrypted file.

Here is an example of which keys are used to encrypt/sign and decrypt/verify an inbound file from your trading partner:

- You create a key pair to be used for encryption and decryption and give your trading partner the public key.
- Your trading partner creates a key pair for signing and verification and gives you the public key.
- Your trading partner encrypts the file with your public key, signs it with their key pair, and sends the encrypted/signed file to you.
- You decrypt the file with your key pair and verify their signature with their public key.

The keys used by your company to encrypt/sign and decrypt/verify an outbound file to your trading partner work in a similar way:

- Your trading partner creates a key pair to be used for encryption and decryption and gives you the public key.
- You create a key pair for signing and verification and give your trading partner your public key.
- You encrypt the file with your trading partner's public key, sign it with your key pair, and send the encrypted/signed file to them.
- Your trading partner decrypts the file with their key pair and verifies your signature with your public key.

The OpenPGP protocol defines standard formats for encrypted messages, signatures, and private keys. The OpenPGP encryption standard is defined by the OpenPGP Working Group of the Internet Engineering Task Force (IETF) Proposed Standard RFC 2440 and RFC 4880, which can be found at http://www.ietf.org/rfc/rfc2440.txt.

For current information on OpenPGP, go to www.pgpi.org – an international PGP Web site that promotes the use of PGP worldwide and a resource pool for information on the PGP program and the OpenPGP standard.

The following books provide further technical and historical information on OpenPGP:

- *The Official PGP User's Guide* by Phil Zimmermann, MIT Press, 1995, ISBN: 0-262-74017-6.
- *PGP: Source Code and Internals* by Phil Zimmermann, MIT Press, 1995, ISBN: 0-262-24039-4.
- *PGP: Pretty Good Privacy* by Simson Garfinkel, O'Reilly & Associates, 1994, ISBN: 1-56592-098-8.
- *Protect Your Privacy - A Guide for PGP Users* by William Stallings. Prentice-Hall, 1994, ISBN: 0-13-185596-4.
- *Crypto - How the Code Rebels Beat the Government, Saving Privacy in the Digital Age* by Steven Levy, Viking Penguin Putnam, 2001, ISBN: 0-670-85950-8.
- *Applied Cryptography: Protocols, Algorithms, and Source Code in C* by Bruce Schneier, John Wiley & Sons, 1995, ISBN: 0471117099.
- *Handbook of Applied Cryptography* by Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, CRC Press, 1996, ISBN: 0849385237.

6.3.1 OpenPGP Key Menu Items

In Diplomat Managed File Transfer, each OpenPGP public key and key pair has a unique key name, which is displayed when you select keys to be used in a partner profile or for encryption, decryption, signing, or verification in a transaction. These names should be readily understandable. For example, you might name the public key for Acme Foods – 'Acme Foods Public Key'.

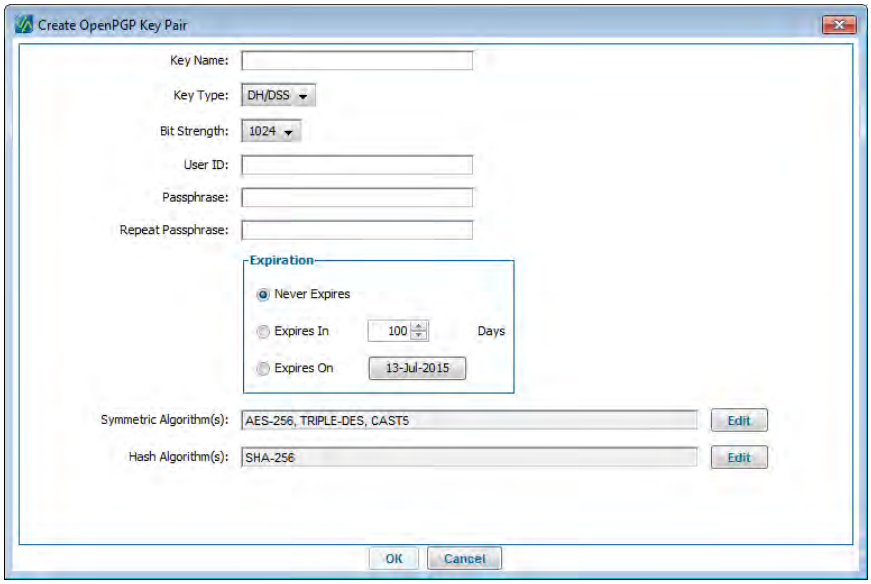
Diplomat MFT OpenPGP key management allows you to:

- 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 key menu items related to OpenPGP key pairs require the entry of the secret passphrase for that key pair.

6.3.1.1 OpenPGP Key Pairs

6.3.1.1.1 Create Key Pair



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 a 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. See the following section on *Adding Subkeys* for instructions on how to add an encryption sub-key.

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

Key Name

All key pairs and public keys must have unique *Key Names* 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. 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 at a later time. 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.

NOTE: RSA legacy keys use an older algorithm that is no longer used by most OpenPGP products. Diplomat MFT can import and use RSA legacy keys for encryption/decryption and signing/verification, but it does not support RSA legacy key creation.

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. The larger the bit strength of the key, the longer it takes to generate and the longer it takes to encrypt, decrypt, sign, or verify a file. Keys sizes are generally 1024, 2048, and 4096.

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

User ID

Identifies the owner of the key. A commonly used practice with OpenPGP keys for personal use is to use your email address as the User ID. As most keys in Diplomat MFT are used for corporate transactions, you may want to use the corporate and/or division name using the key or the email address that you use when you set up your email server under Settings > Email Server. For example, payroll@acmefoods.com might be a good *User ID* that would indicate that the owner of the key pair is the Payroll Department at Acme Foods. 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.

NOTE: Some OpenPGP products require that *User IDs* be in the form 'FirstName LastName <username@domain_name.com>', such as 'John Smith <jsmith@acmefoods.com>'.

Passphrase

OpenPGP uses a passphrase to encrypt your private key. A passphrase should be hard for you to forget and difficult for others to guess.

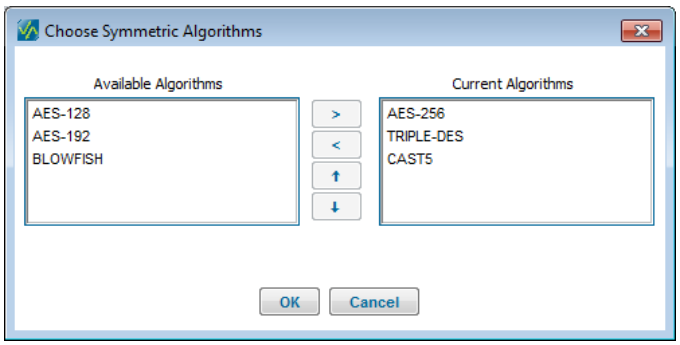
You must provide the passphrase, when you import, create, modify, delete, or recover a key pair. Once you have created a key pair in Diplomat, the passphrase is stored separately from the key pair in a special encrypted format. When you set up a transaction in Diplomat, for security purposes, you do not need to re-enter the passphrase.

If you forget the passphrase, an account with *Administrator* privileges can recover it.

Expiration

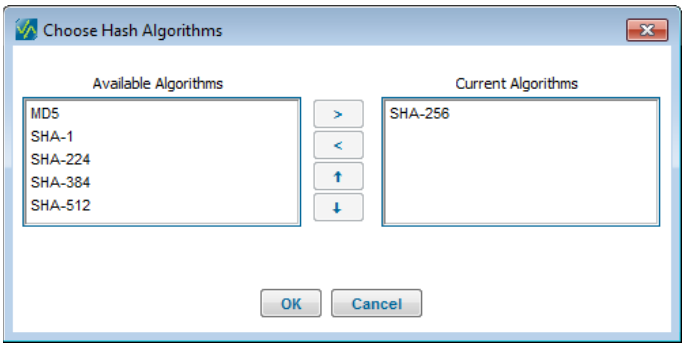
You can set the expiration of the master key such that it never expires, expires in XX days, or expires on a particular date.

Symmetric Algorithm(s)



Symmetric Algorithms are used for data encryption.

Hash Algorithm(s)



Hash Algorithms are used for protecting signatures.

6.3.1.1.2 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 MFT uses the currently-valid encryption sub-key to encrypt files.

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.

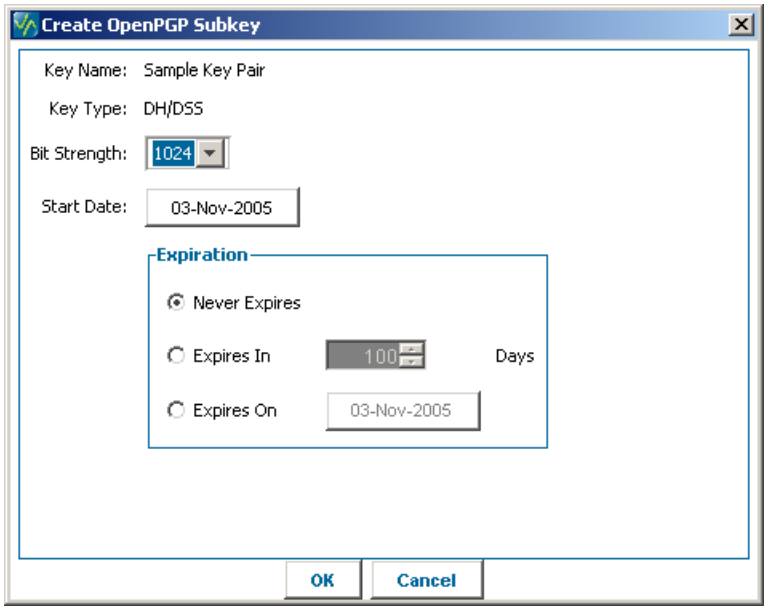
Regularly changing the sub-key used to encrypt files makes your key much more secure, as anyone trying to attack your key must break the algorithm used by the currently-valid sub-key. Generally, the more often you change your encryption sub-key the more secure your key is.

To maximize the benefits of using sub-keys, we recommend you 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 redistributing public keys to all of your partners.

NOTE: If a key has encryption sub-keys with overlapping usage periods, Diplomat MFT uses the sub-key with the most recent creation date to encrypt files.

NOTE: OpenPGP uses a passphrase to encrypt your private key. You must provide the passphrase, when you import, create, delete, or recover a key pair. **If you forget the passphrase, an account with *Administrator* privileges can recover it.**

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



Key Type

Key Type for sub-keys is the same key type as the master key and is not editable.

Bit strength

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 and the longer it takes to encrypt, decrypt, sign, or verify a file. Keys sizes are generally 1024, 2048, and 4096.

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

Start Date

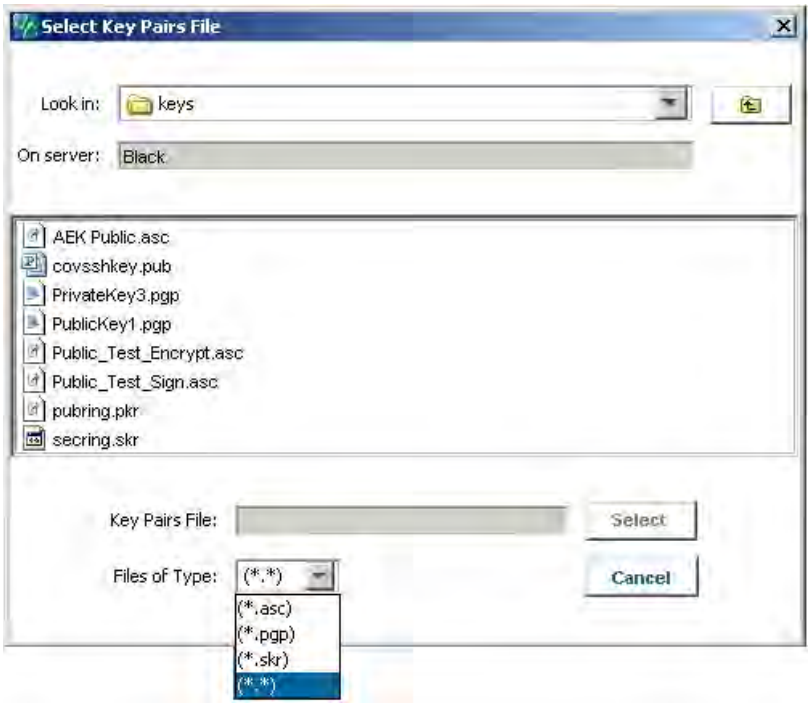
The first date the sub-key is used for encrypting files. Defaults to the date following the most recently created sub-key expiration date.

Expiration

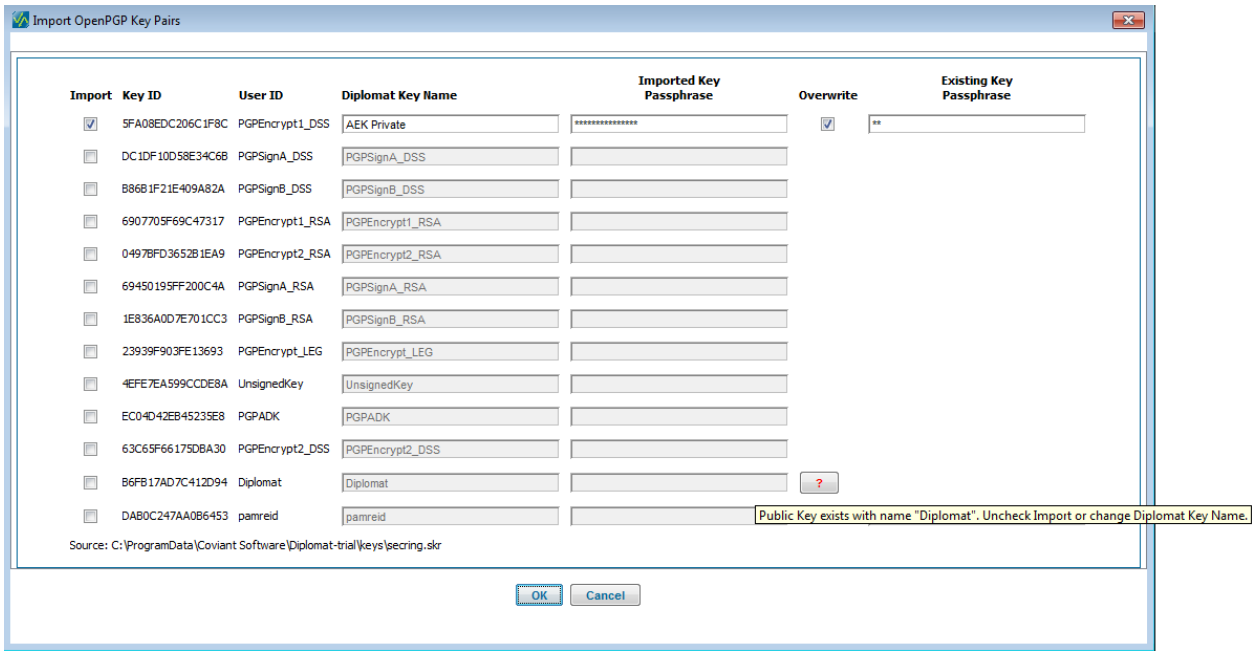
You can set the expiration of a sub-key such that it never expires, expires in XX days, or expires on a particular date. Each expiration date for a sub-key created by Diplomat MFT cannot be later than the expiration date of the master key.

6.3.1.1.3 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. Select Keys > OpenPGP Key Pairs > Import Key Pairs from the top menu bar.



Browse to the location of the key ring to be imported. 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.



Import Checkbox

Check *Import* beside each key in the key ring that you would like to import.

NOTE: Prior to Diplomat MFT v4.0, you were required to indicate if a key to be imported needed to be compatible with PGP5.x or PGP 6.x. Compatibility is now determined automatically and no longer needs to be specified.

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 *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.

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 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.

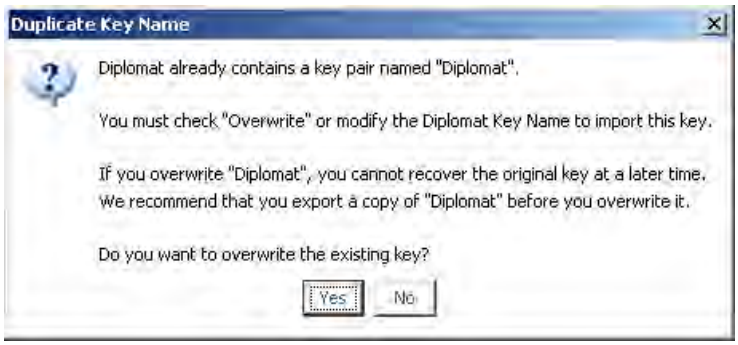
NOTE: Since *User IDs* do not have to be unique in OpenPGP-compliant key rings, you may need to modify the default *Diplomat Key Name* before importing. You can choose a name that makes it easy to determine the intended use of the key when setting up transactions. For example, you might use 'Acme Verification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

NOTE: *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 ID*, but two public keys may **not** have the same *Key ID*. You cannot import a public key that has the same internal *Key ID* as an existing public key.

NOTE: 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 MFT database, 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.



NOTE: 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. For Windows systems, the default key directory is either C:\Program Files\Coviant Software\Diplomat-j\keys or 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.**

Imported Key Passphrase

The *Imported Key Passphrase* field is only displayed for key pairs. OpenPGP uses a passphrase to encrypt each key pair. The imported key passphrase is the passphrase for the key you plan to import.

Overwrite Checkbox

An *Overwrite* checkbox is only displayed for keys with a *Diplomat Key Name* that already exists in the Diplomat MFT database.

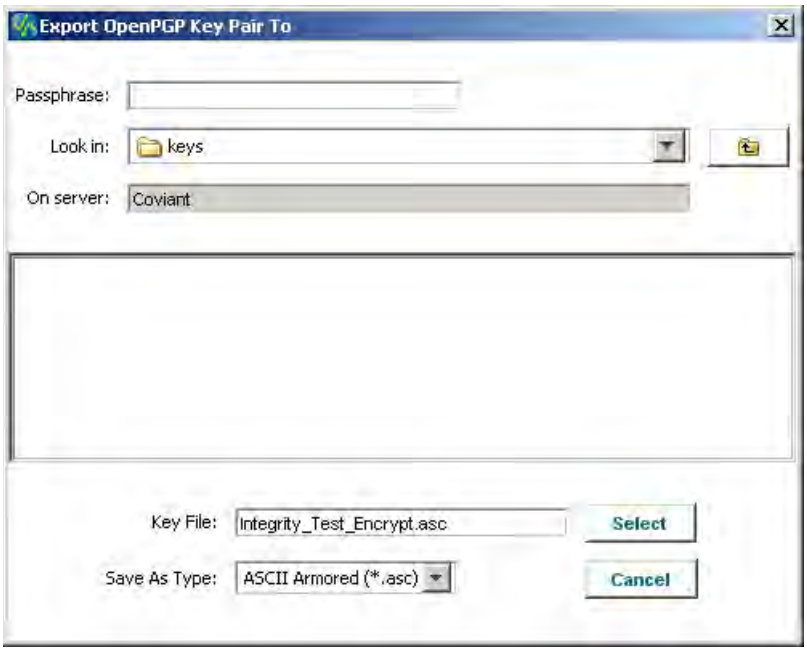
NOTE: If you decide not to overwrite the existing key, simply uncheck the *Overwrite* checkbox before selecting *OK*.

Existing Key Passphrase

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.

6.3.1.1.4 Export Key Pair

Key pairs can be exported from Diplomat MFT 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, select Keys > OpenPGP Key Pairs > Export Key Pair from the top menu bar.



Passphrase
OpenPGP uses a passphrase to encrypt your private key. A pop-up dialog box requests the passphrase, when you import, create, delete, or recover a key pair. **If you forget the passphrase, an account with *Administrator* privileges can recover it.**

On Server
Displays the name of the system running the Diplomat MFT Service with which the Diplomat MFT Client currently has an active session.

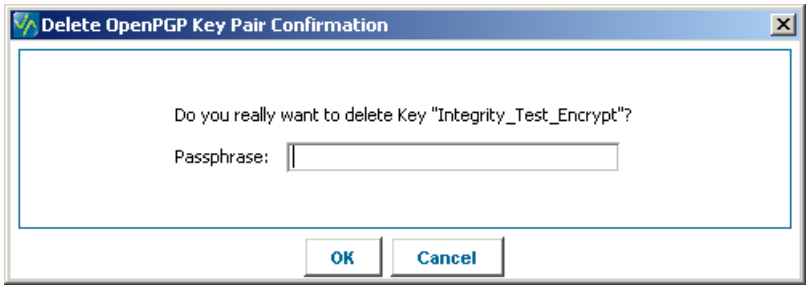
Key File
Enter the filename you plan to use for the key pair file. You may enter a path as part of the filename or browse to locate the directory to which the key pair will be exported. For Windows systems, the default key directory is C:\ProgramData\Coviant Software\Diplomat-j\keys. For Linux systems, the default directory is /opt/coviant/diplomat-j/keys.

Save as File Type
Select a file type of either ASCII-armored (*.asc) or OpenPGP (.pgp).

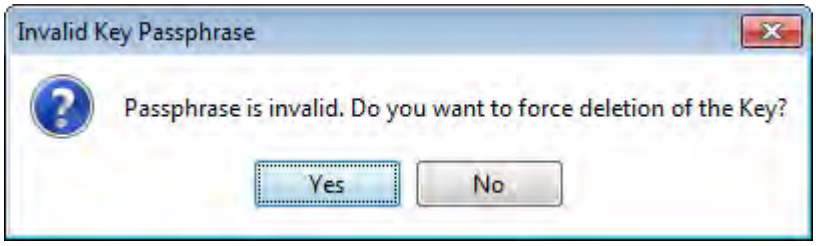
6.3.1.1.5 Delete

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, enter <Ctrl+D>, or right-click and select Delete.

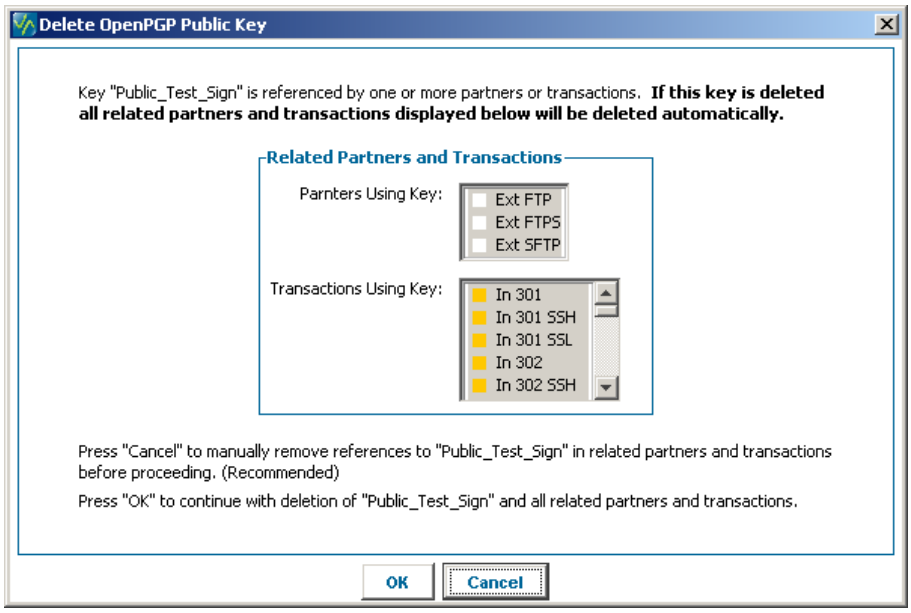
NOTE: OpenPGP uses a passphrase to encrypt your private key. You must provide the passphrase, when you import, create, delete, or recover a key pair. **If you forget the passphrase, an account with *Administrator* privileges can recover it.**



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 the message shown below.



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

Only press 'OK' if you are certain that the key and all of the related partners and transactions are no longer needed. For example, you might choose to delete a key and all of 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.

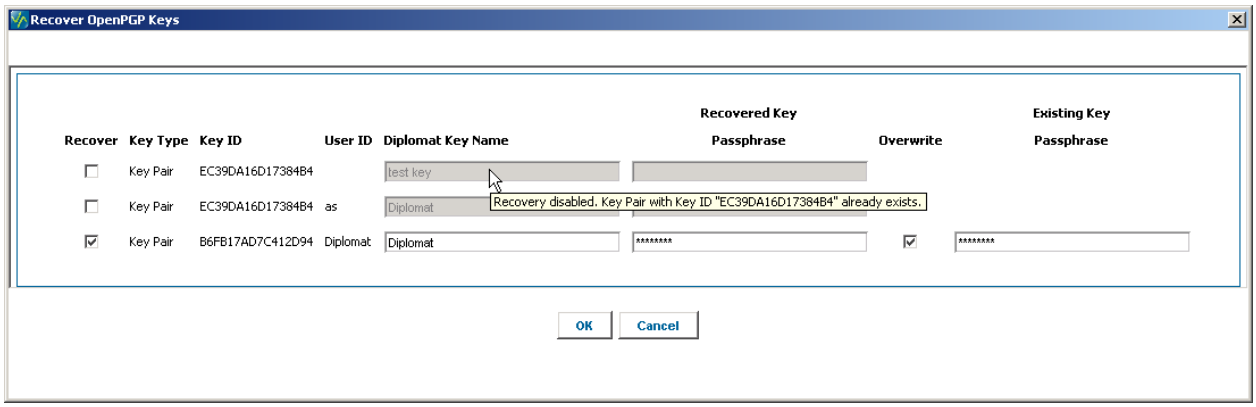
For example, assume you want to delete a private key pair named 'Private Key 1'. 'Private Key 1' is specified in 'Private Partner 1' as the Sign/Verify key. If an outbound transaction 'Out Transaction 1' uses the 'Private Partner 1' as the source partner profile but the transaction does not require a signature, then 'Private Key 1' is not actually used in 'Out Transaction 1'. Since 'Out Transaction 1' uses 'Private Partner 1', if 'Private Key 1' is deleted, the 'Out Transaction 1' will also be deleted.

NOTE: 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.

6.3.1.1.6 Recover

Key pairs can be recovered, if they were deleted by Diplomat. To recover a key, select Keys > OpenPGP Key Pairs > Recover from the top menu bar.

NOTE: OpenPGP uses a passphrase to encrypt your private key. You must provide the passphrase, when you import, create, delete, or recover a key pair. **If you forget the passphrase, an account with *Administrator* privileges can recover it.**



Recover Checkbox

Check *Recover* beside each key that you would like to recover.

Key Type

Indicates whether the key available for recovery is a public key or a key pair.

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 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. The rollover message and the help message provide reminders that the Key ID already exists in the Diplomat MFT transaction database.

User ID(s)

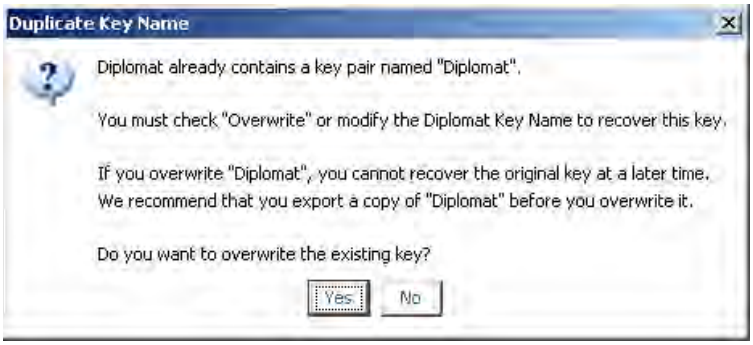
Text string that helps identify the owner of the key. Two key pairs may have the same *User ID*, but they must have different *Key IDs*.

Diplomat Key Name

Diplomat Key Names are 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.

NOTE: Only one copy of a deleted key is retained. If you delete a key with the same *Diplomat Key Name* as a key that has already been deleted, only the most recently deleted key is available for recovery. For example, assume you have a key pair named 'Test' and you delete it. The key pair named 'Test' is available for recovery. Then, you import a public key named 'Test' and delete it. The original key pair named 'Test' is no longer available for recovery. The public key 'Test' is available.



NOTE: 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 to the default keys directory 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.**

Recovered Key Passphrase

The *Recovered Key Passphrase* field is only displayed for key pairs. OpenPGP uses a passphrase to encrypt each key pair. The recovered key passphrase is the passphrase for the key you plan to recover.

Overwrite Checkbox

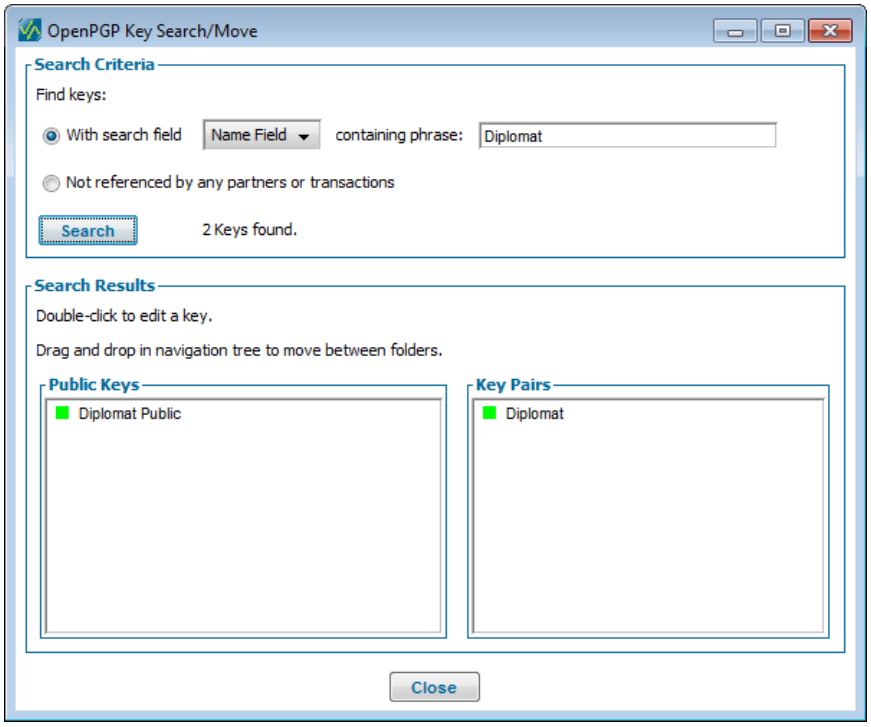
An *Overwrite* checkbox is displayed for keys with a *Diplomat Key Name* that already exists in the Diplomat MFT database.

NOTE: If you decide not to overwrite the existing key, simply uncheck the *Overwrite* checkbox before selecting *OK*.

Existing Key Passphrase

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.

6.3.1.1.7 Search/Move



OpenPGP Key Search/Move is used to 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

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.

NOTE: The *phrase* field is case sensitive.

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

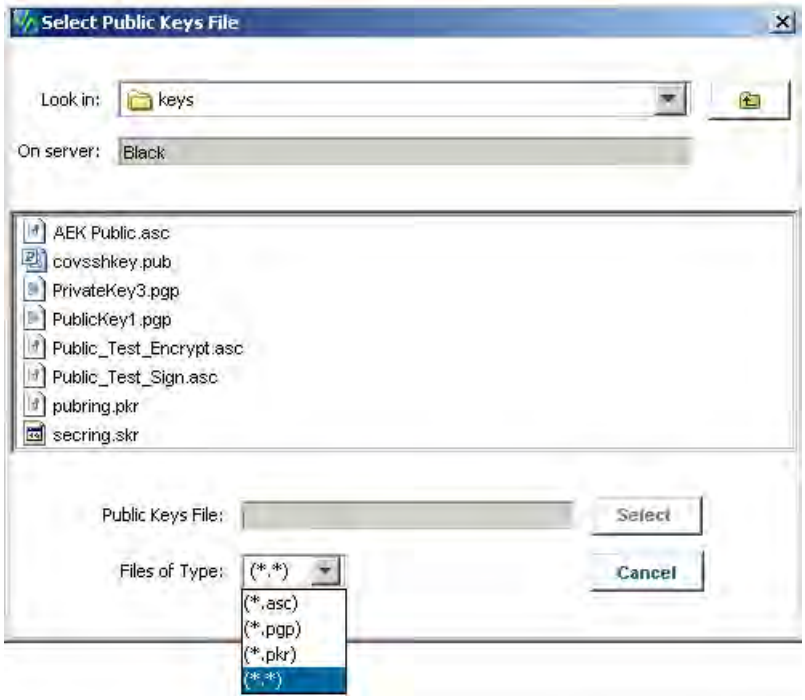
Search Results displays all of the keys that match the search criteria. A status indicator is displayed to the left of each Key ID which indicates scheduling status of each key by displaying:

- 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.

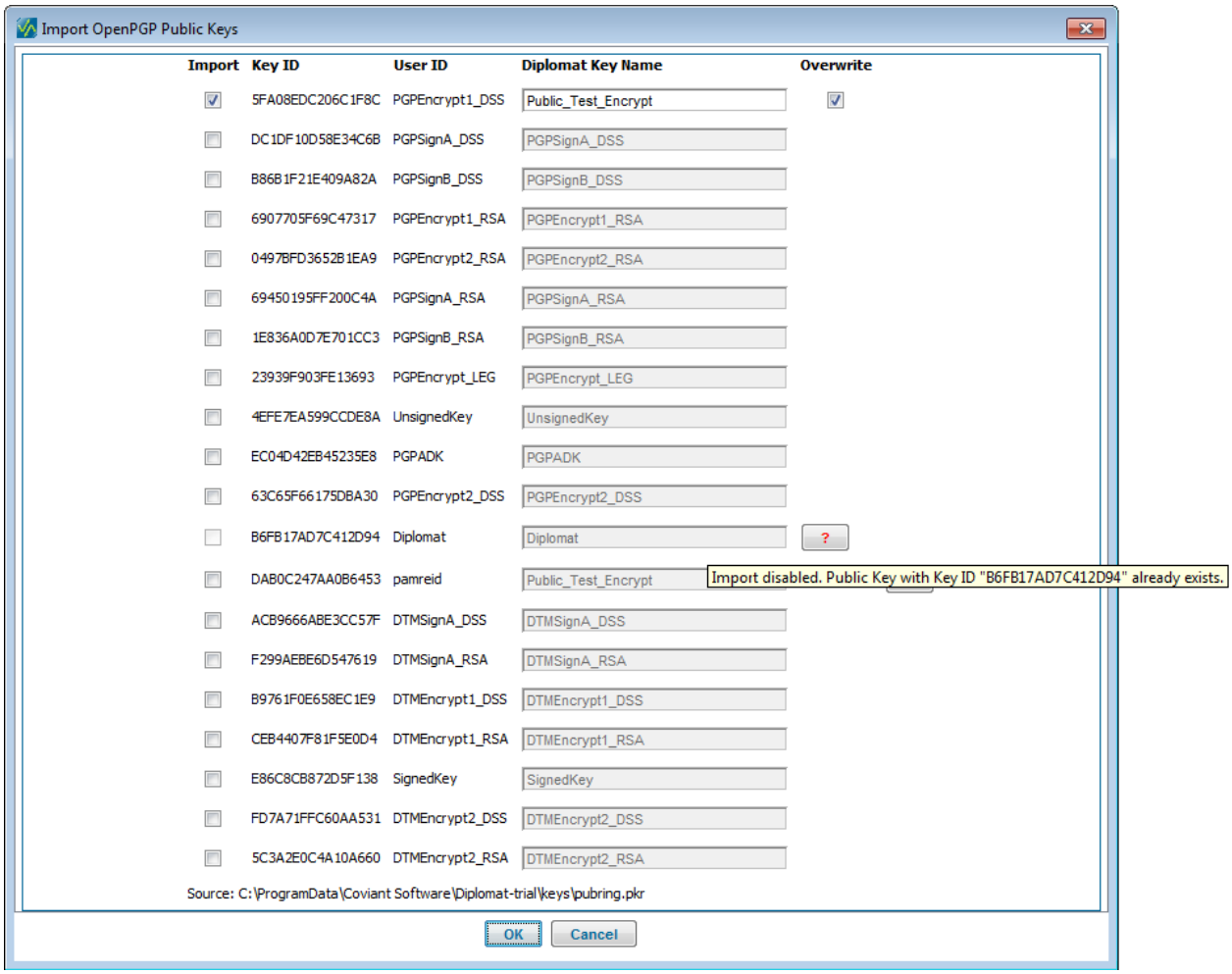
6.3.1.2 OpenPGP Public Keys

6.3.1.2.1 Import Public Keys

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 the OpenPGP-compliant tool that created it and then import it into Diplomat. Select Keys > OpenPGP Public Keys > Import Public Keys from the top menu bar.



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



Import Checkbox

Check *Import* beside each key in the key ring that you would like to import.

NOTE: Prior to Diplomat MFT v4.0, you were required to indicate if a key to be imported needed to be compatible with PGP5.x or PGP 6.x. Compatibility is now determined automatically and no longer needs to be specified.

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 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.

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 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.

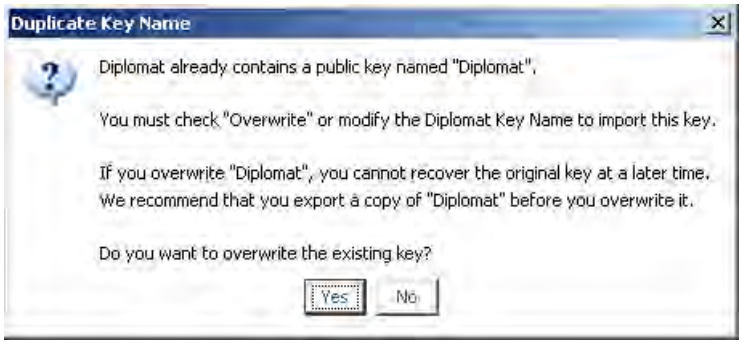
NOTE: Since *User IDs* do not have to be unique in OpenPGP-compliant key rings, you may need to modify the default *Diplomat Key Name* before importing. You can choose a name that makes it easy to determine the intended use of the key when setting up transactions. For example, you might use 'Acme Verification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

NOTE: *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 *Key ID*, but two public keys may **not** have the same *Key ID*. You cannot import a public key that has the same internal *Key ID* as an existing public key in the Diplomat MFT database.

NOTE: 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 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.



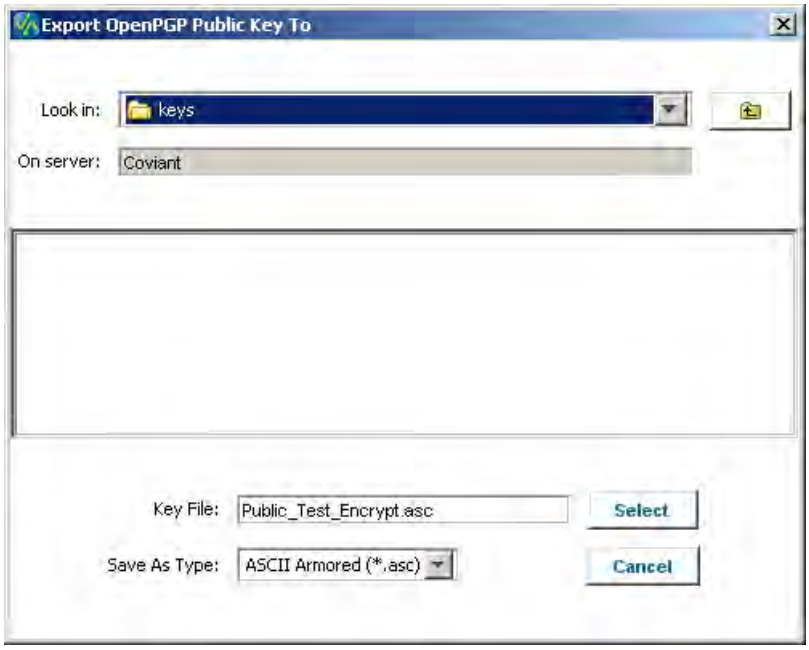
NOTE: If you choose to overwrite the existing key, you cannot recover the original key at a later time. As a precaution, Diplomat MFT attempts to export a copy of the original key before it is overwritten. For Windows systems, the default key directory is C:\ProgramData\Coviant Software\Diplomat-j\keys. 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.**

Overwrite Checkbox

An *Overwrite* checkbox is displayed only for keys with a *Diplomat Key Name* that already exists in the Diplomat MFT database.

NOTE: If you decide not to overwrite the existing key, simply uncheck the *Overwrite* checkbox before selecting *OK*.

6.3.1.2.2 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, select Keys > OpenPGP Public Keys > Export Public Key from the top menu bar.

For example, you might have a key pair named Pinnacle Bank Key Pair for your company to be used for transactions with your bank. To export the public key from the key pair to send to Pinnacle Bank, select Pinnacle Bank Key Pair in the navigation tree. Then, select Keys > OpenPGP Public Keys > Export Public Key from the top menu bar to export the public key from the key pair. Then, send the public key file to Pinnacle Bank or via email or through your web site.

On Server

Displays the name of the system running the Diplomat MFT Service with which the Diplomat MFT Client currently has an active session.

Key File

Enter the filename you plan to use for the public key file. You may enter a path as part of the filename or browse to locate the directory to which the public key will be exported. 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.

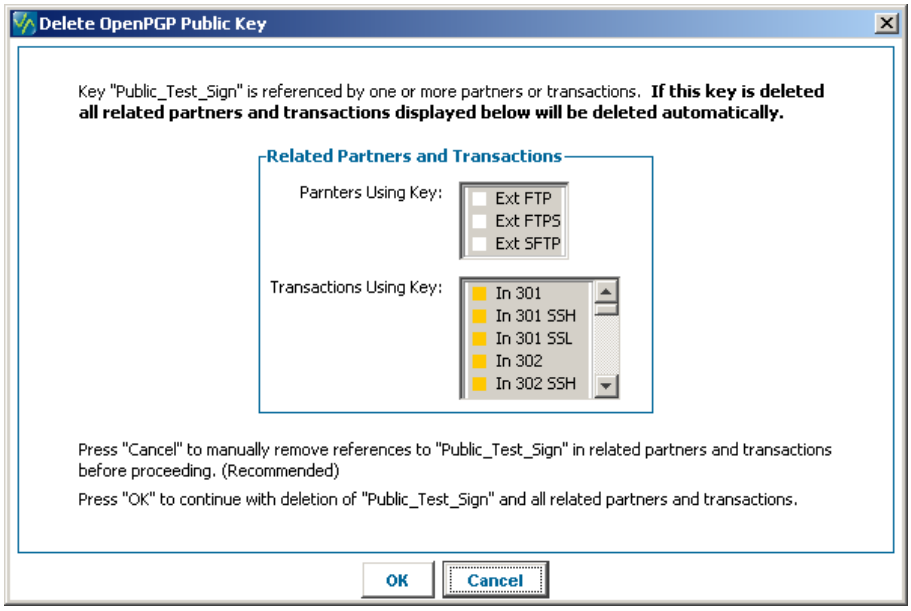
Save as File Type

Select a file type of either ASCII-armored (*.asc) or OpenPGP (.pgp).

6.3.1.2.3 Delete

Public keys and 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 Public Keys > Delete from the top menu bar, enter <Ctrl+D>, or right-click 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 the message shown below.



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

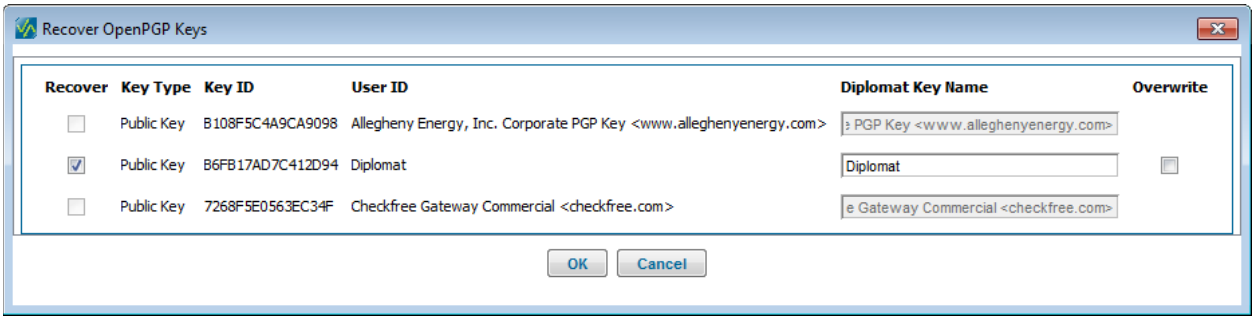
Only press 'OK' if you are certain that the key and all of the related partners and transactions are no longer needed. For example, you might choose to delete a key and all of its related partners and transactions if you are no longer doing business with the trading partner from which you received the 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.

For example, assume you want to delete a private key pair named 'Private Key 1'. 'Private Key 1' is specified in 'Private Partner 1' as the Sign/Verify key. If an outbound transaction 'Out Transaction 1' uses the 'Private Partner 1' as the source partner profile but the transaction does not require a signature, then 'Private Key 1' is not actually used in 'Out Transaction 1'. Since 'Out Transaction 1' uses 'Private Partner 1', if 'Private Key 1' is deleted, the 'Out Transaction 1' will also be deleted.

6.3.1.2.4 Recover

Public keys can be recovered, if they were deleted by Diplomat. To recover a public key, select Keys > OpenPGP Public Keys > Recover from the top menu bar.



Recover Checkbox

Check *Recover* beside each key that you would like to recover.

Key Type

Indicates whether the key available for recovery is a public key or a key pair.

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 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. The rollover message and the help message provide a reminder that the Key ID already exists in the Diplomat MFT transaction database.

User ID(s)

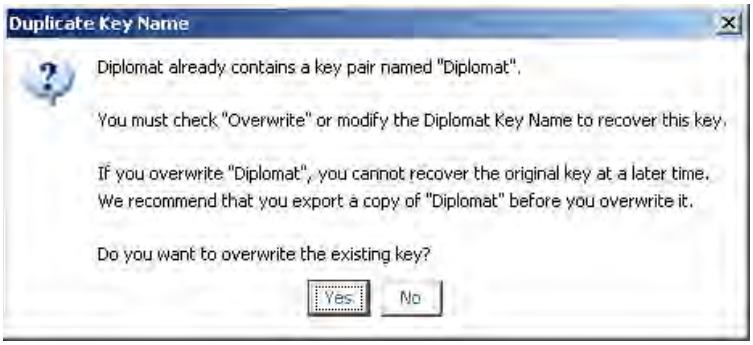
Text string that helps identify the owner of the key. Two key pairs may have the same *User ID*, but they must have different *Key IDs*.

Diplomat Key Name

Diplomat Key Names are 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.

NOTE: Only one copy of a deleted key is retained. If you delete a key with the same *Diplomat Key Name* as a key that has already been deleted, only the most recently deleted key is available for recovery. For example, assume you have a key pair named 'Test' and you delete it. The key pair named 'Test' is available for recovery. Then, you import a public key named 'Test' and delete it. The original key pair named 'Test' is no longer available for recovery. The public key 'Test' is available.



NOTE: 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 to the default keys directory 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.**

Recovered Key Passphrase

The *Recovered Key Passphrase* field is only displayed for key pairs. OpenPGP uses a passphrase to encrypt each key pair. The recovered key passphrase is the passphrase for the key you plan to recover.

Overwrite Checkbox

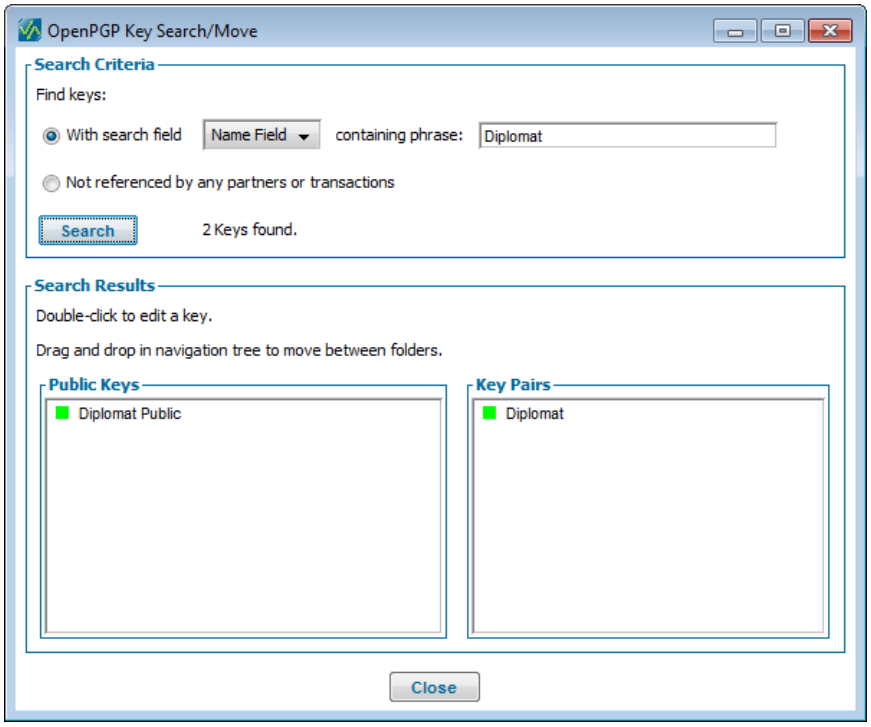
An *Overwrite* checkbox is displayed for keys with a *Diplomat Key Name* that already exists in the Diplomat MFT database.

NOTE: If you decide not to overwrite the existing key, simply uncheck the *Overwrite* checkbox before selecting *OK*.

Existing Key Passphrase

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.

6.3.1.2.5 Search/Move



OpenPGP Key Search/Move is used to 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

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.

NOTE: The *phrase* field is case sensitive.

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

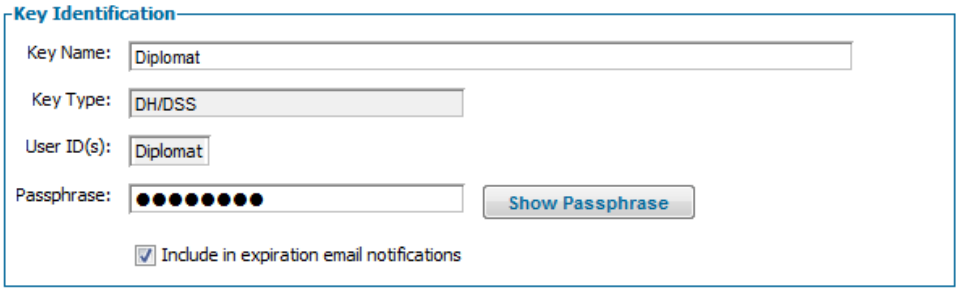
Search Results displays all of the keys that match the search criteria. A status indicator is displayed to the left of each Key ID which indicates scheduling status of each key by displaying:

- 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.

6.3.2 OpenPGP Key Window

The OpenPGP Key Window displays information about the selected key. None of the fields are editable. Public keys appear the same as key pairs.

6.3.2.1 Key Identification



Key Name
Displayed by Diplomat MFT each time you select a key for use in a transaction or partner profile. *Key Name* is used only by Diplomat.

NOTE: If you export a key, the *Key Name* is not exported.

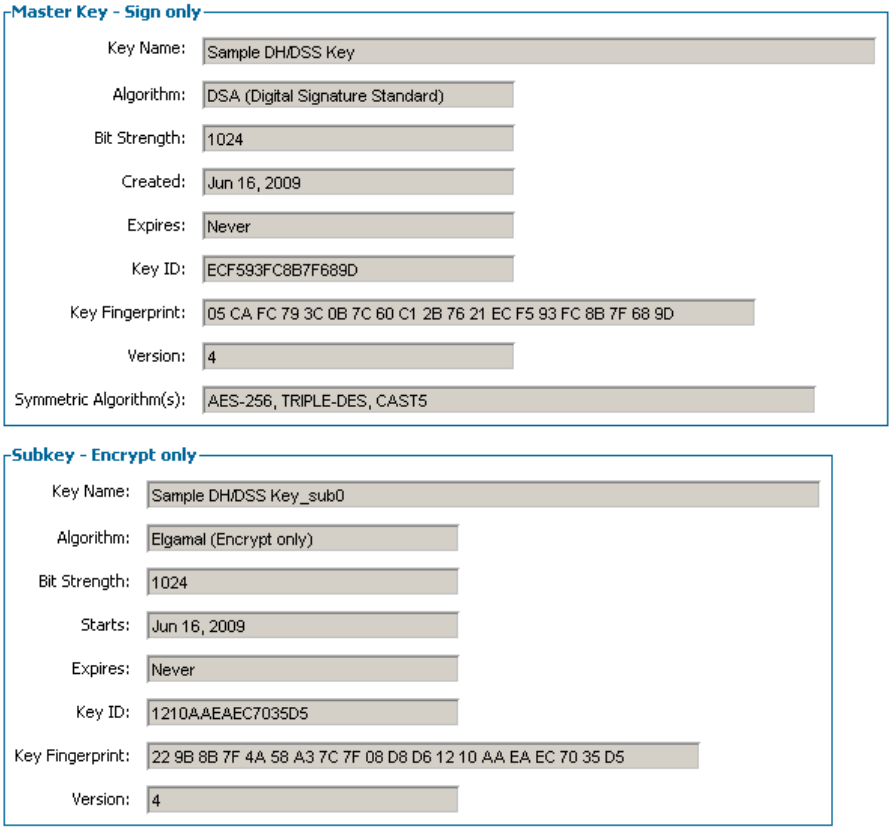
Key Type
OpenPGP keys have three different types: DH/DSS, RSA, and RSA Legacy. This field displays either DH/DSS or RSA as the key type. If an RSA key is an RSA Legacy key, version '3' is displayed in the version field of the master key or sub-key.

User ID(s)
Text string that helps identify the owner of the key. Some OpenPGP products allow you to specify multiple *User IDs* for a single key. If you export a key, the *User IDs* are exported. Users of other OpenPGP products will have visibility to the *User IDs* of a key.

Key Passphrase
Passphrase that was set during key creation. Accounts with *Administrator* privileges can select the *Show Passphrase* button to display the passphrase.

Include in expiration email notifications
Check *Include in expiration email notifications* to receive email notifications about key expiration. Recipients are set under Settings > IT Support Email Notifications.

6.3.2.2 Master Key and Subkey(s)



When Diplomat MFT creates a new OpenPGP key using the DH/DSS algorithm, the master key is designated as Sign Only and sub-keys are designated as Encrypt Only. When the RSA algorithm is selected, the master key and the sub-keys are able to encrypt and sign files. Keys created by other OpenPGP products may have master or sub-keys that can be used for both signing and encryption.

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 following characteristics:

Algorithm
Name of the algorithm the master key or sub-key uses at runtime to encrypt/decrypt or sign/verify files. Each master key and sub-key can use a different algorithm.

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. The larger the bit strength of a key, the longer it takes to generate and the longer it takes to encrypt, decrypt, sign, or verify a file. Keys sizes are generally 1024, 2048, and 4096.

Created/Starts
For a Master Key, date key was created. For Encryption Sub-keys, date the sub-key becomes effective.

Expires
Date master key or sub-key expires. Most keys are set to Never. **NOTE:** Keys created by OpenPGP-compliant products other than Diplomat MFT may have sub-keys that expire after the master key expiration date.

Key ID

Uniquely identifies a key pair. Two key pairs may have the same *User ID*, but they must have different *Key ID*s.

NOTE: A public key that is exported from a key pair has the same *Key ID* as the original key pair. Diplomat MFT allows a public key and a key pair to have the same *Key ID*, but two key pairs or two public keys may **not** have the same *Key ID*.

Key Fingerprint

Unique string of numbers and characters used to authenticate a public key. For example, you might send a trading partner your public key. To authenticate that the public key is yours, they might telephone you and read you the key fingerprint. You can confirm whether it is the same fingerprint and, therefore, a valid key or not.

Version

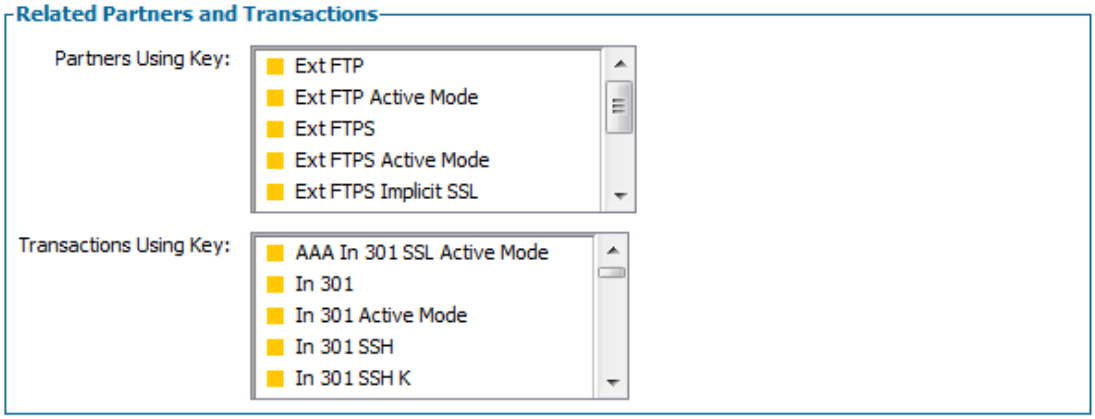
Version of IETF OpenPGP specification to which the key conforms. RSA legacy keys display version '3'.

Symmetric Algorithm(s)

Symmetric algorithms that the private key of a key pair can use to decrypt a file encrypted using the matching public key. The list is in the preferred order of the key creator (i.e., the first algorithm on the list is the most preferred). At run-time, Diplomat MFT compares the symmetric algorithms listed in the key to the list of algorithms currently supported by Diplomat. Diplomat MFT uses the first algorithm that it supports to encrypt files with the key. Diplomat MFT currently supports AES-256, Triple-DES, and CAST5 for file encryption.

NOTE: When a key with no algorithm specified is imported, the symmetric algorithm field on the key screen is blank. When Diplomat MFT uses the key, it defaults to using Triple-DES – even though it is NOT displayed on the Open PGP Key Pair screen.

6.3.2.3 Related Partners and Transactions



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.

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.

6.4 SSH Keys

SSH keys are a public key encryption technology. SSH client keys can assist in authenticating the user attempting to access an SFTP server. SSH host keys are used to authenticate 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.

6.4.1 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 client key pairs.
- Import existing SSH client 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 or move SSH client keys.

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

6.4.1.1 SSH Client Keys

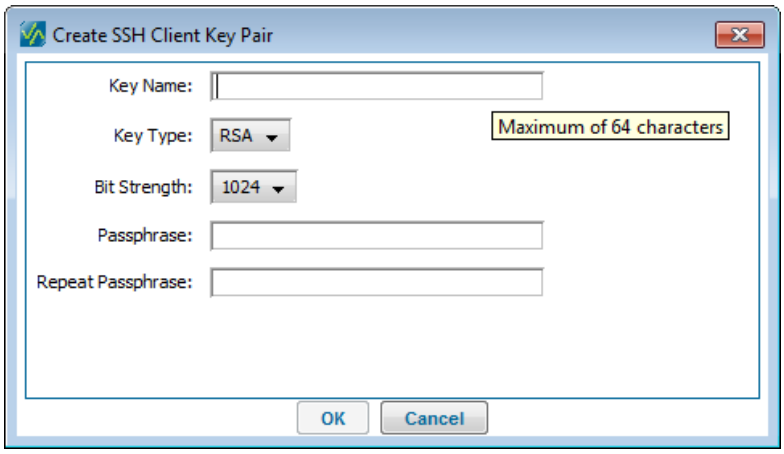
To use SSH client keys, you must:

- Create an SSH client key pair by selecting Keys > SSH Client Keys > Create Key Pair from the top menu bar.
- Export the public key from the newly-created SSH Client key pair into a file by selecting Keys > SSH Client Keys > 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 client key to log into the SFTP server by selecting the correct SSH client key 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 client key 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 client key, 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 client 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.

6.4.1.1.1 Create Key Pair



Key Name

SSH key pairs must have unique *Key Names* 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.

Key Type

Diplomat MFT supports two SSH client 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 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.

Passphrase

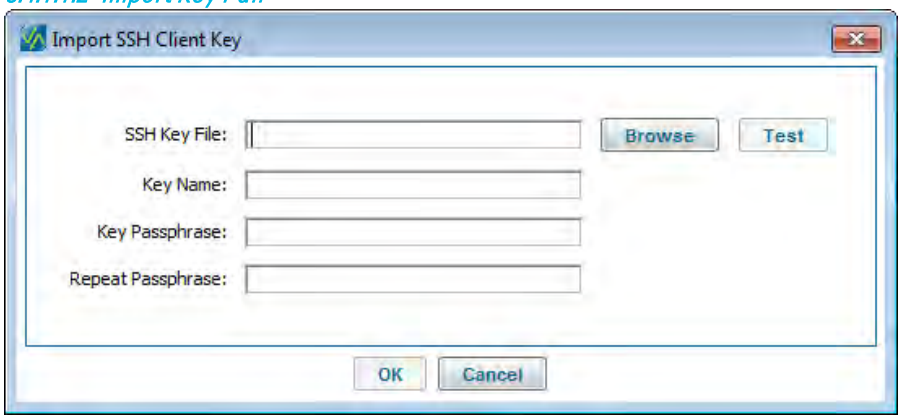
SSH uses a passphrase to encrypt your key pair. A passphrase should be hard for you to forget and difficult for others to guess.

You must provide the passphrase, when you import, create, export, delete, or recover an SSH client 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 at a later time.** 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 client key with the same name. The original SSH client key can still be recovered at a later time.

6.4.1.1.2 Import Key Pair



SSH client 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 at a later time.** 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 at a later time.

SSH Key File

Enter the filename and location of the SSH client key pair. 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. Use **Browse** to select a different directory. Use **Test** to determine whether the location is accessible and is read/write enabled for the logon identity used by the Diplomat MFT Service.

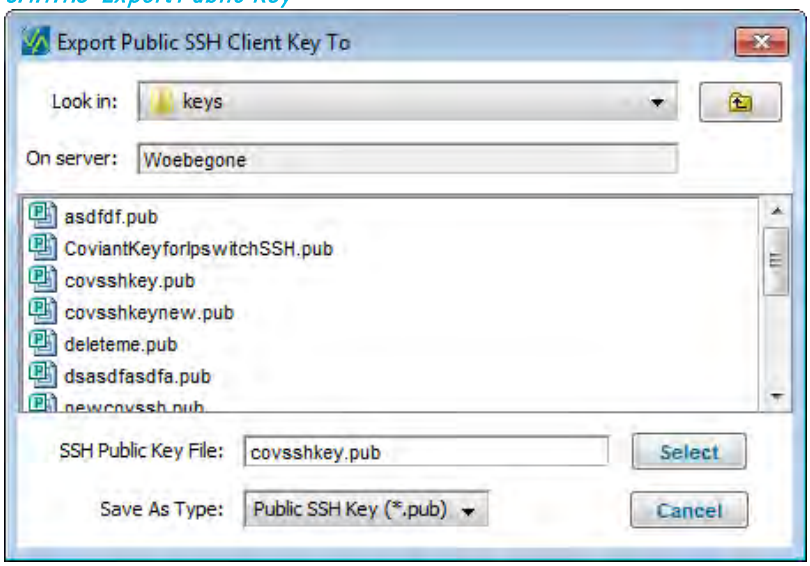
Key Name

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

Passphrase

SSH uses a passphrase to encrypt your private key. You must provide the passphrase, when you import, create, delete, or recover a key pair.

6.4.1.1.3 Export Public Key



Public SSH client keys 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, select Keys > SSH Client Keys > Export Public Key from the top menu bar.

To use SFTP for file transfers, you must create an SSH client key pair for use by Diplomat MFT when logging on to a particular SFTP server. Then, you must export the public key from your newly-created SSH client key pair into a file and send it to the SFTP server administrator. The SFTP server administrator must then attach the public key to your SFTP account.

NOTE: Some older SSH1-based SFTP servers use a different key format when exported to a file. The SFTP (SSH1) server may appear to import Diplomat MFT SSH client keys correctly, but login fails. If you have created a new SFTP public key and cannot connect to an SFTP server, contact Coviant Software Support for assistance.

SSH Client Public Key File

Browse to the file you plan to use for the public key file. 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.

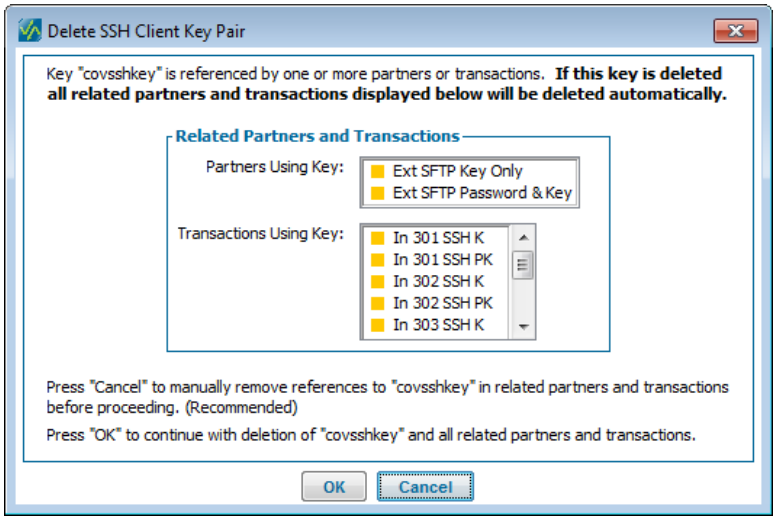
Save as File Type

SSH public keys exported by Diplomat MFT have a '.pub' file extension.

6.4.1.1.4 Delete

SSH client 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, select Keys > SSH Keys > Delete from the top menu bar or highlight the SSH client key pair in the navigation tree. Enter <Ctrl+D> or right-click and select Delete. .

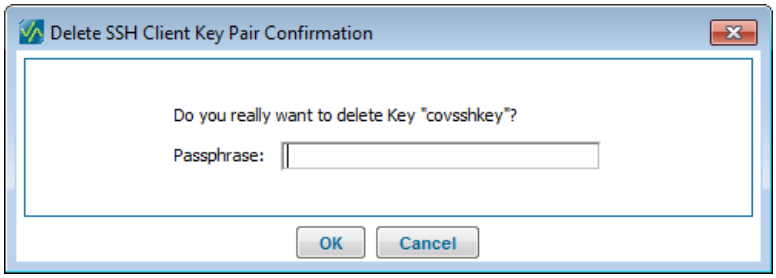
If a partner profile or transaction in Diplomat MFT references the key you are attempting to delete, Diplomat MFT does not immediately delete the key and you receive the message shown below.



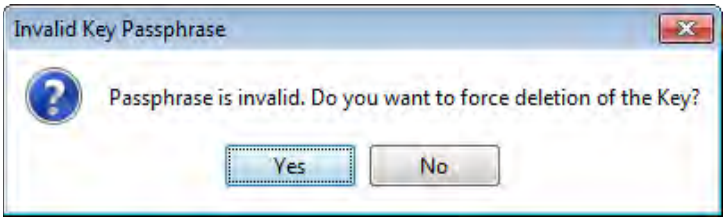
It is strongly recommended that you press 'Cancel' and manually remove references to the key before proceeding with the key deletion.

Only press 'OK' if you are certain that the key and all of the related partners and transactions are no longer needed. For example, you might choose to delete a key and all of its related partners and transactions if you are no longer doing business with the trading partner for which you created the key.

NOTE: SSH uses a passphrase to encrypt your private key. You must provide the passphrase, when you import, create, delete, or recover a key pair.



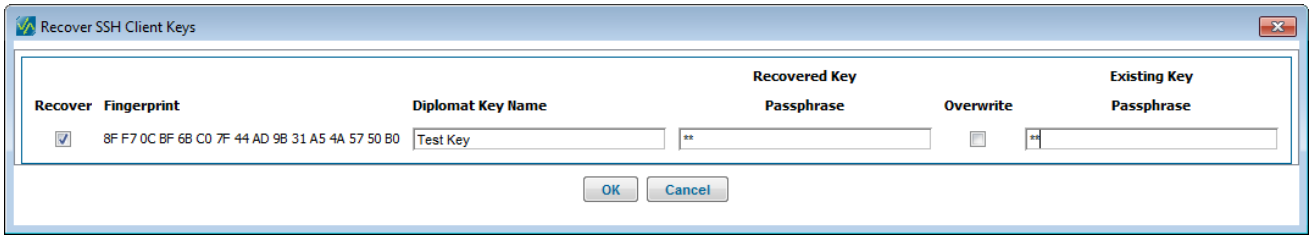
If you have forgotten the passphrase and need to delete a key pair, accounts with *Administrator* privileges can force the deletion without a valid passphrase.



6.4.1.1.5 Recover

SSH client key pairs can be recovered, if they were deleted by Diplomat. To recover a key, select Keys > SSH Client Keys > Recover from the top menu bar.

NOTE: SSH uses a passphrase to encrypt your private key. You must provide the passphrase, when you import, create, delete, or recover a key pair.

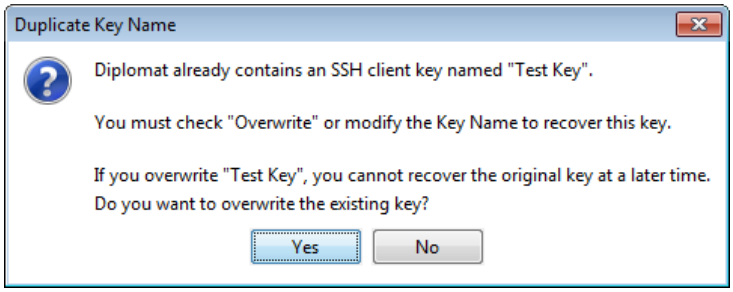


Recover Checkbox
Check *Recover* beside each key pair that you would like to recover.

Fingerprint
Uniquely identifies an SSH client key pair.

Diplomat Key Name
Diplomat Key Names are used only by Diplomat. All SSH client key pairs must have unique *Diplomat Key Names*.

If you attempt to recover an SSH client key pair with a *Diplomat Key Name* that already exists in the Diplomat MFT database, you have the option to overwrite the existing key pair or to modify the *Diplomat Key Name* field.



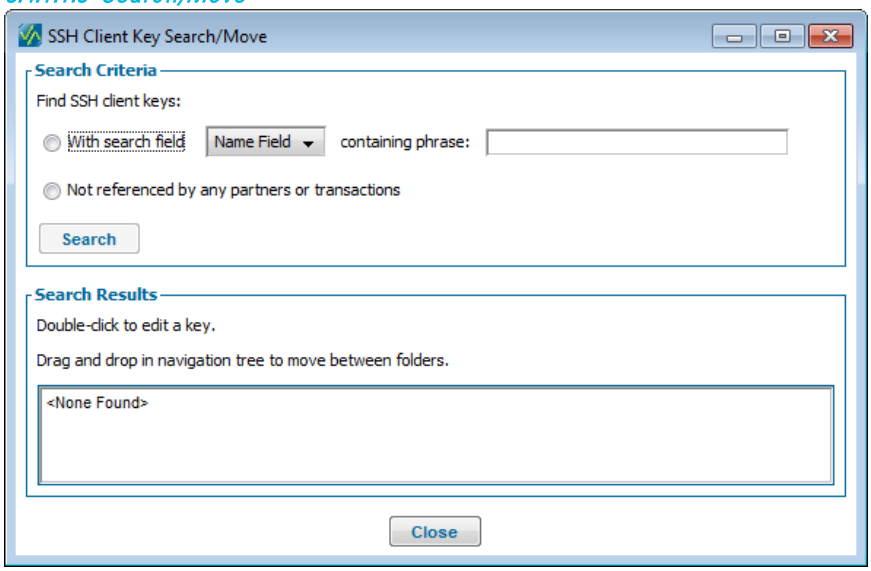
Recovered Key Passphrase
Recovered Key Passphrase is the passphrase for the SSH client key pair you plan to recover.

Overwrite Checkbox
An *Overwrite* checkbox is displayed for each SSH client key pair with *Diplomat Key Name* that already exists in the Diplomat MFT database.

NOTE: If you decide not to overwrite the existing key pair, uncheck the *Overwrite* checkbox before selecting *OK*.

Existing Key Passphrase
If you plan to overwrite an existing SSH client key pair in the Diplomat MFT database, you must enter the *Existing Key Passphrase* for the existing key.

6.4.1.1.6 Search/Move



SSH client key Search/Move is used to locate SSH client 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

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.

NOTE: The *phrase* field is case sensitive.

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

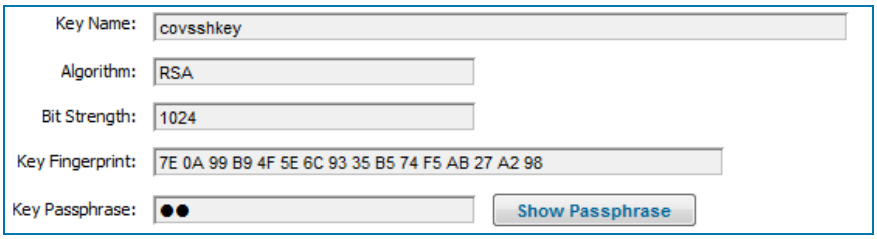
Search Results displays all of the keys that match the search criteria. A status indicator is displayed to the left of each Key ID which indicates scheduling status of each key by displaying:

- 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.

6.4.2 SSH Client Key Window

The SSH Client Keys Window displays information about the selected key.

6.4.2.1 Key Identification



Key Name
Displayed by Diplomat MFT each time you select a key for use in a transaction or partner profile. *Key Name* is used only by Diplomat.

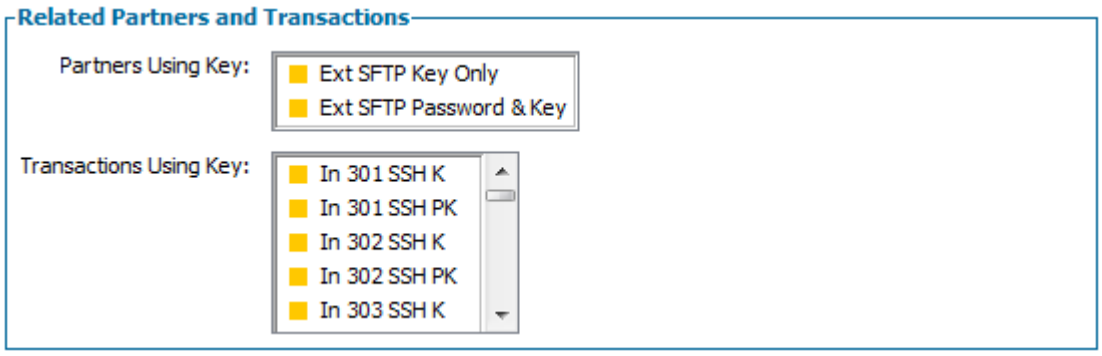
Algorithm
SSH client keys can use two algorithms: DH/DSS and RSA. This field indicates which algorithm the key will use for encryption or decryption.

Bit Strength
Number of bits representing the key size. The difficulty of breaking a key increases as bit strength increases.

Key Fingerprint
Unique string of numbers and characters used to authenticate a public key. For example, you would be likely to export a public key and send to an SFTP server administrator. To authenticate that the public key is yours, the administrator might telephone you and read you the key fingerprint. You can confirm whether it is the same fingerprint and, therefore, the correct key.

Key Passphrase
Passphrase that was set during key creation. Accounts with *Administrator* privileges can select the *Show Passphrase* button to display the passphrase.

6.4.2.2 Related Partners and Transactions



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.

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 ' '
- Use 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 deletion. 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.

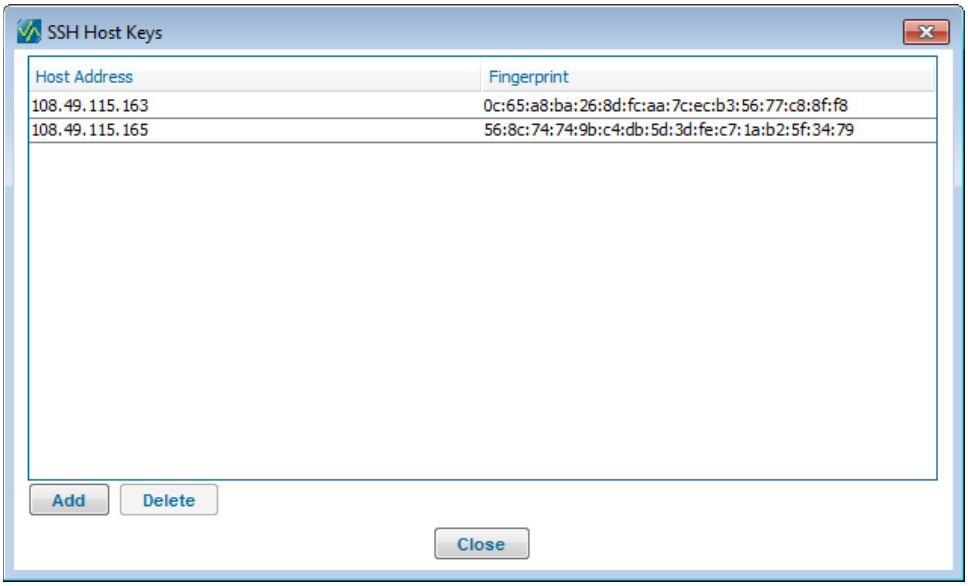
6.4.3 SSH Host Keys

When you attempt to log into an SFTP server, you can have Diplomat MFT verify the identity of the SFTP server by comparing the fingerprint supplied by the SFTP server with the fingerprints in the Diplomat MFT database.

To use SSH host keys, you must:

- Add the host address and fingerprint of the SFTP server to the SSH host key list in Diplomat MFT under Keys > SSH Host Keys from the top menu or when using the Test button in a partner profile.
- Check *Verify SSH host key* on the SFTP panel in the Source or Destination Partner Profile when setting up transactions.
- Use the Show SSH Host Keys on the same panel to verify that the host address and fingerprint are shown in the SSH host key list.

NOTE: 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.



Select the *Add* button to enter host addresses and fingerprints for SSH Host Keys. Select the *Delete* button to remove the host address and fingerprint from the Diplomat MFT database.

6.5 SSL Certificates

SSL Certificates are used to confirm the identity of an FTPS (TLS/SSL) server when a file transfer job runs. The FTPS server administrator decides whether an SSL certificate is required. And, if so, they send a certificate file to you that must be imported into Diplomat.

If an SSL certificate is required, you must:

- Request an SSL certificate file from the FTPS server administrator. Typically, this file can be emailed to you.
- Import the SSL certificate by selecting Keys > SSL Certificates > Import SSL Certificate from the top menu bar.
- Select the certificate from the *SSL Server Certificate* drop-down list in the FTPS(TLS/SSL) Server sub-panel on the Transaction screen.

During a file transfer to an FTPS 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 to encrypt/decrypt the file being transmitted.

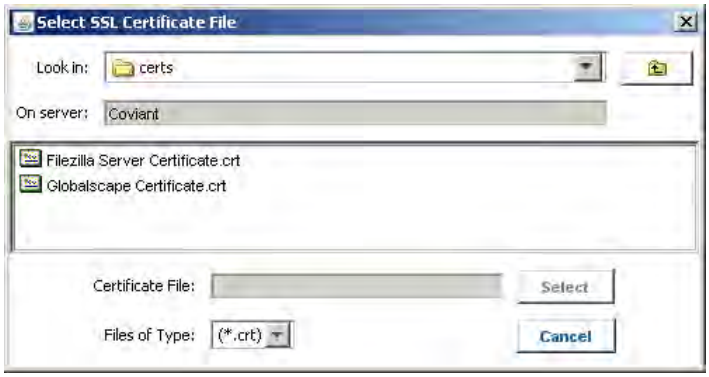
6.5.1 SSL Certificate Menu Items

In Diplomat Managed File Transfer, each SSL certificate 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 SSL Certificate for Acme Foods FTPS server– 'Acme Foods SSL Cert'.

Diplomat MFT SSL certificate management allows you to:

- Import existing SSL certificates.
- Delete SSL certificates.
- Search or move SSL certificates.

6.5.1.1 Import SSL Certificate



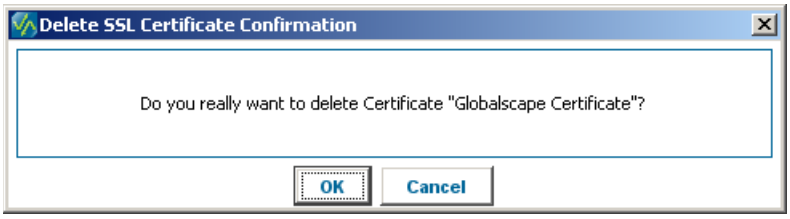
SSL certificates can be imported into Diplomat. Typically, you would receive an SSL certificate file from the FTPS server administrator.

NOTE: 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 at a later time.**

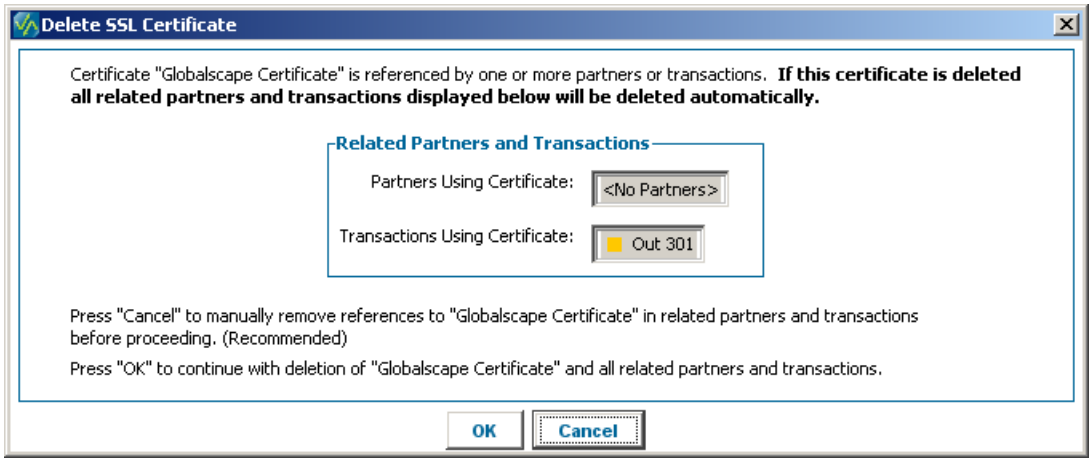
Browse to the location of the SSL certificate file and select the filename. For Windows systems, the default directory is C:\ProgramData\Coviant Software\Diplomat-j\certs. For Linux systems, the default directory is /opt/coviant/diplomat-j/certs.

6.5.1.2 Delete

SSL certificates can be deleted from the Diplomat MFT database. To delete an SSL certificate, highlight the certificate you plan to delete from the navigation tree. Then, select Keys > SSL Certificates > Delete from the top menu bar. Enter <Ctrl+D> or right-click and select Delete.



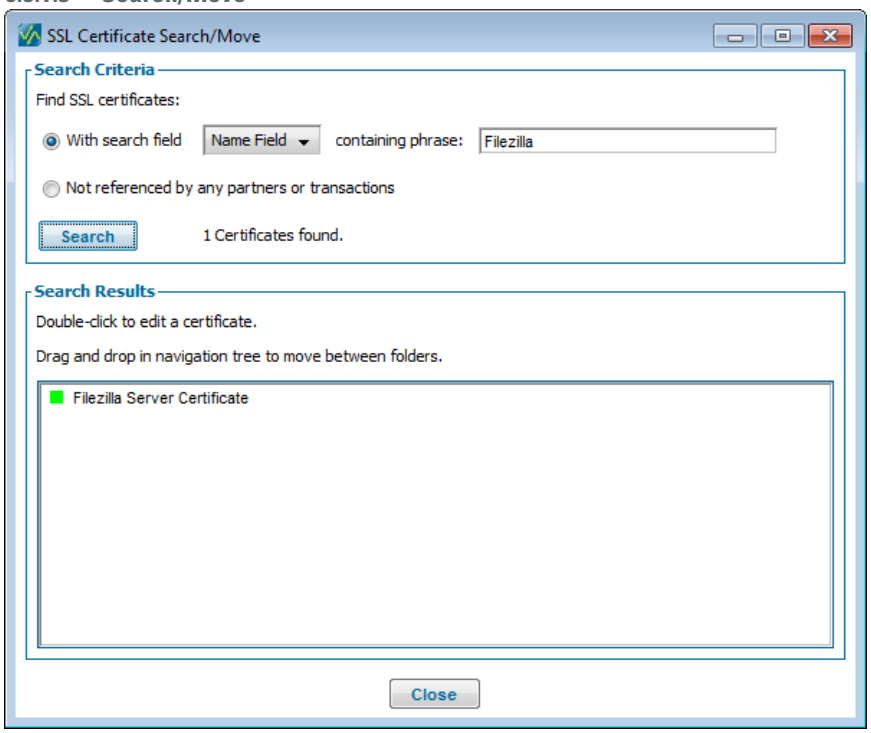
If a partner profile or transaction in Diplomat MFT references the certificate you are attempting to delete, Diplomat MFT does not immediately delete the certificate and you receive the message shown below.



It is strongly recommended that you press 'Cancel' and manually remove references to the certificate before proceeding with the deletion.

Only press 'OK' if you are certain that the certificate and all of the related partners and transactions are no longer needed. For example, you might choose to delete a certificate and all of its related partners and transactions if you are no longer doing business with the trading partner from which you received the certificate.

6.5.1.3 Search/Move



SSL Certificate Search/Move is used to locate SSL certificates containing specific phrases and keys that are not referenced by any partner profile or transaction. To select a certificate for editing, highlight the Key ID in the list and select OK. To move a certificate, highlight the Key ID and drag it to the target folder in the navigation tree.

Search Criteria

Search Criteria are used to find certificates where the search field contains a specific phrase or keys that are not referenced by any partner or transaction.

NOTE: The *phrase* field is case sensitive.

The Search Button is used to initiate the search using the criteria in the Search Criteria panel and displays the number of certificates found.

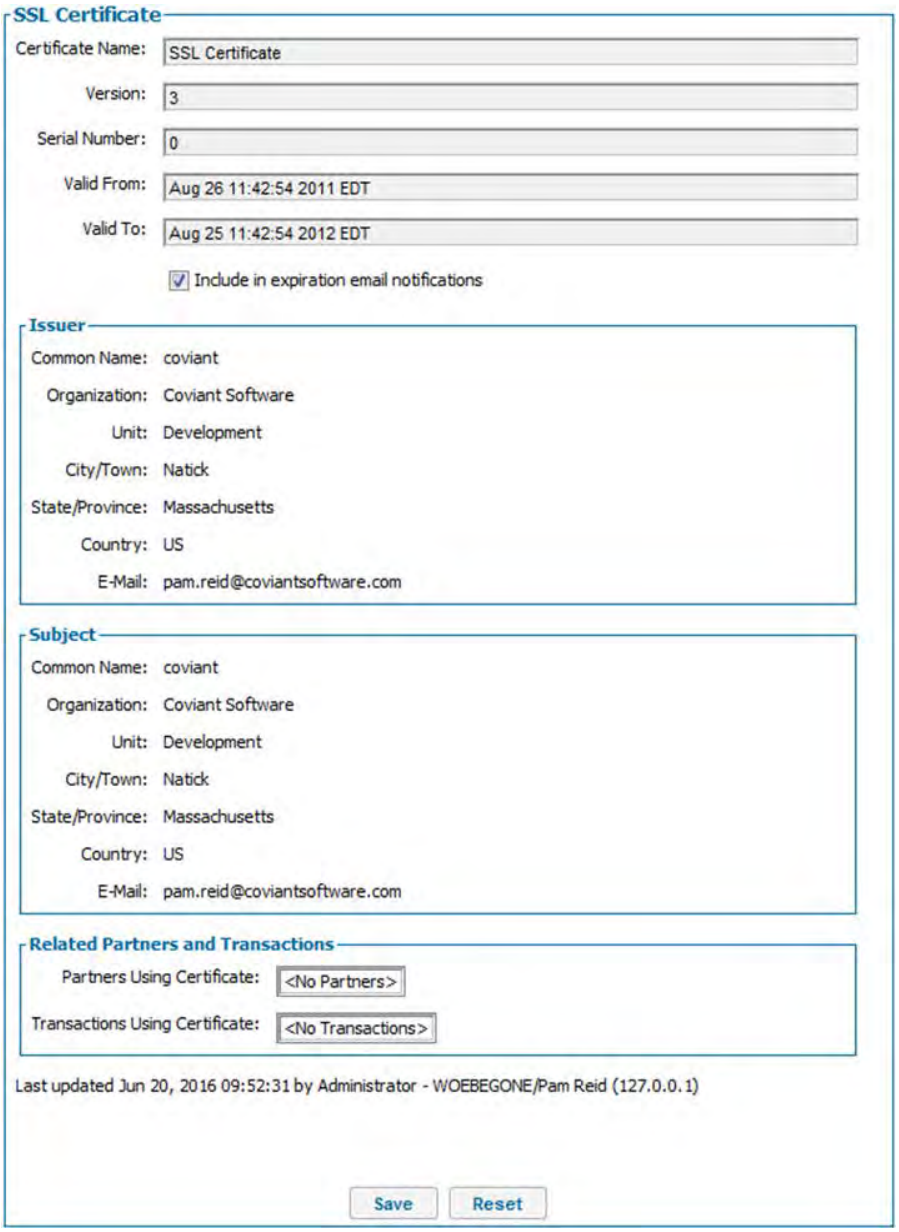
Search Results

Search Results displays all of the certificates 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 certificates that are available for use in scheduled jobs,
- Yellow status indicator for certificates that have been suspended directly, and
- Orange status indicator for certificates that have been suspended indirectly.

6.5.2 SSL Certificate Window

The SSL Certificate displays information about the selected certificate.



Certificate Name

Displayed by Diplomat MFT each time you select a certificate for use in a transaction or partner profile. *Certificate Name* is used only by Diplomat MFT.

Include in expiration email notifications

Check *Include in expiration email notifications* to receive email notifications about key expiration. Recipients are set under Settings > IT Support Email Notifications.

Version, Serial Number, Valid From/To, Issuer and Subject

SSL Version, *Serial Number*, *Valid From/To*, *Issuer* and *Subject* are set at the time the certificate was created.

Related Partners and Transactions

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.

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 '
- Use file monitoring '
- Suspended indirectly '
- Suspended directly '
- Actively being scheduled '

NOTE: It is recommended that you suspend all transactions related to a certificate before you make any changes to it, like deletion. You can suspend all transactions using a certificate by highlighting the certificate in the navigation tree and selecting Jobs > Suspend Active Key from the top menu bar or right clicking on the certificate 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.

7 Understanding Partner Profiles

7.1 Partners Overview

Diplomat MFT Enterprise Edition uses *Partner Name* as a unique identifier for each partner profile. *Partner Name* must be unique across all public and trusted profiles.

When you need to set up more than one transaction with a particular trading partner or remote site, Diplomat MFT allows you to create a partner profile that can be referenced by all of the transactions. You enter the partner profile information once and reuse it in all transactions with that trading partner or site.

If the information on a partner profile changes, you enter the new data once on the profile and it automatically updates all transactions with that partner. For example, a partner may install a new FTP server, change the username or password to their current FTP server, or change their encryption or signature key. In each of these cases, you can update the partner profile and all transactions with that partner will reflect the changes.

A partner profile may be a location inside your corporate firewall, a 'Trusted' profile. Or, it may be a 'Public' profile for locations outside your corporate firewall, such as your own or your trading partner's FTP server. You can create new profiles for partners or particular departments or divisions of partners that have their own FTP servers, passwords, or other unique characteristics that need to be reflected in a transaction.

7.2 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 and/or search/move the folder to a new location.

Select a partner in the navigation tree and right-click to save changes to the partner, save the partner with a new name, reset the settings in the partner to the saved values, 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 MFT allows you to immediately suspend all transactions associated with a partner. For example, you may need to suspend transactions for a partner if a trading partner notifies you that their FTP server may have been compromised.

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 all transactions associated with a partner:

- Highlight the desired partner in the navigation tree.
- Select Jobs > Suspend > Active Partner or right-click on the partner 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 scheduled until they have been released. To release all transactions associated with a partner, right-click the partner in the navigation tree and select *Release Partner*.

NOTE: All transactions that are currently set to *Do Not Run* on the transaction continue to display a red status indicator '■'.

7.3 Partners Menu Items

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

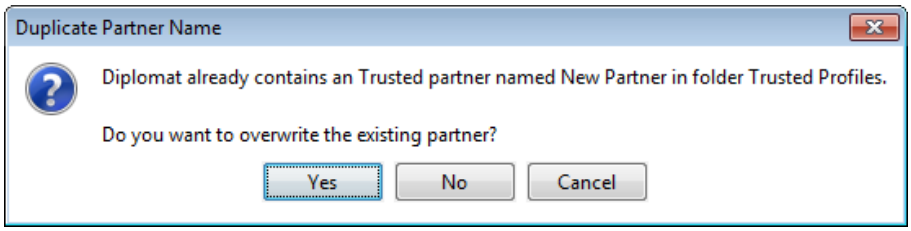
7.3.1 Create Public/Trusted Profiles

New public and trusted partner profiles are created using the drop-down menu from the **Partners** button on the top menu bar. You will be prompted to enter *Partner Name*, which must be unique across all trusted and public profiles.

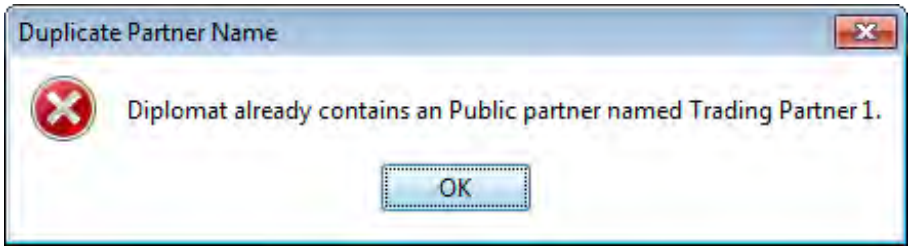
Trusted profiles should be used for partners that are considered part of your organization. **Trusted partner profiles use only key pairs to encrypt/decrypt or sign/verify**. Typically, you would have only a small number of trusted profiles.

Public profiles are used for trading partners or remote sites that provide only their public keys for encryption and verification. Typically, you would have more public profiles, as you would need one for each trading partner.

NOTE: 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.



NOTE: You cannot overwrite a trusted partner profile with the same name as a public profile or vice versa. For example, assume you have a Diplomat MFT database containing 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'.



7.3.2 Save/Save As

To save a partner profile, highlight the partner profile you would like to save in the navigation tree. Then, select Partners > Save from the top menu bar, enter <Ctrl+S>, or right-click and select Save. If you have not already saved a partner profile, you are prompted to save it upon exit from the Diplomat MFT Client. You must save the partner profile before you exit from the Diplomat MFT Client in order to retain information entered during the client session.

You may not change the *Partner Name* of a partner profile once it has been created, but you can use *Save As* on the **Partners** drop-down or right-click to save it under another name, then delete the original partner profile using Delete on the same drop-down menu.

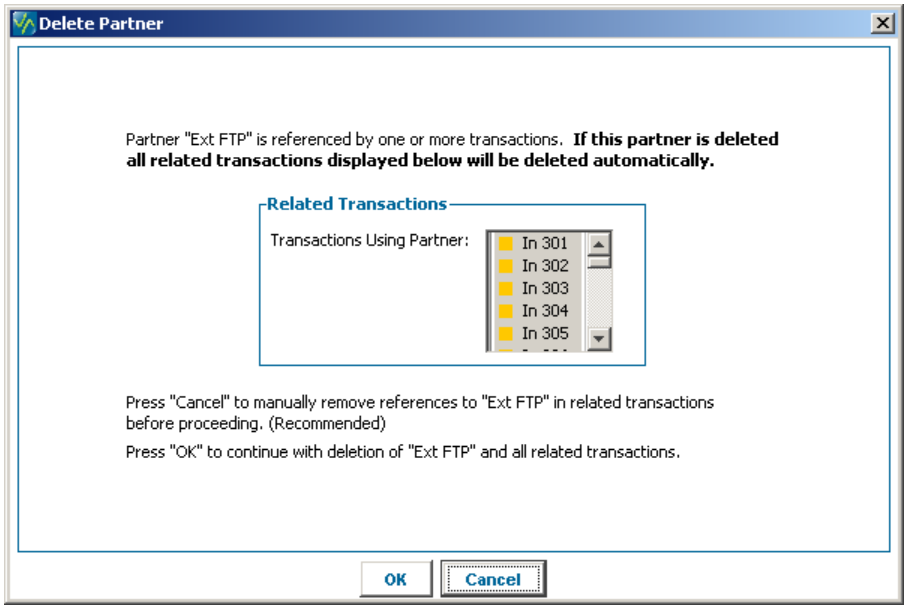
NOTE: If you attempt to create a new partner using *Save As* with a name that already exists in the Diplomat MFT transaction database, you are warned before the existing partner is overwritten.

7.3.3 Delete

To delete a partner profile, highlight the partner profile you would like to delete in the navigation tree. Then, select Partners > Delete from the top menu bar, enter <Ctrl+D>, or right-click and select Delete.

Deletions of partner profiles are permanent. The only way to recover a partner profile is to restore a previously saved backup of the entire Diplomat MFT transaction database. This database contains the key, transaction, partner, and configuration data as of the date the backup was done. Any changes to the database are lost.

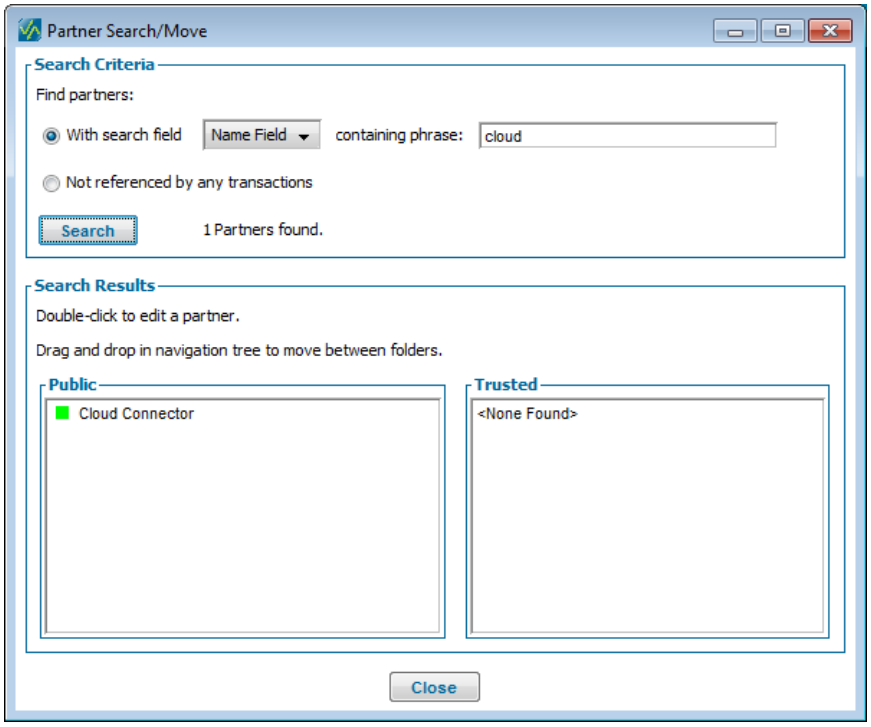
If a transaction in Diplomat MFT references the partner you are attempting to delete, Diplomat MFT does not immediately delete the partner and you receive the message shown below.



It is strongly recommended that you press 'Cancel' and manually remove references to the partner before proceeding with the partner deletion.

Only press 'OK' if you are certain that the partner and all of the related transactions are no longer needed. For example, you might choose to delete a partner and all of its related transactions if you are no longer doing business with the trading partner.

7.3.4 Search/Move



Partner Search/Move is used to locate partner profiles containing specific phrases and partners that are not referenced by any transactions. 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.

Search Criteria

Search Criteria are used to find partners where the search field contains a specific phrase or partners that are not referenced by any transactions.

NOTE: The *phrase* field is case sensitive.

The Search Button is used to initiate the search using the criteria in the Search Criteria panel and displays the number of partners found.

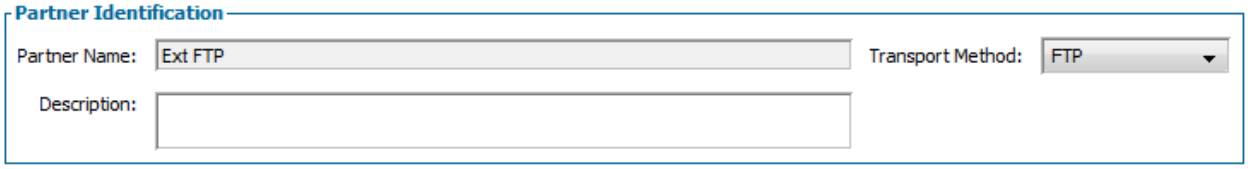
Search Results

Search Results displays all of the public and trusted partner profiles that match the search criteria. A status indicator is displayed to the left of each Partner Name which indicates scheduling status of each transaction by displaying:

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

7.4 Partners Window

7.4.1 Partner Identification



Partner Name

Name of the partner. Must be a unique name across all trusted and public profiles. *Partner Name* field length is limited to 64 characters.

NOTE: Partner Profiles created prior to Diplomat v3.5 may contain Partner Names that exceed the 64 character limit. If so, some data may be truncated when written to a SQL audit database. You can manually shorten older *Partner Names* by using *Save As* and deleting the original partner profile.

Description

Descriptive overview to help recognize the partner.

Transport Method

Determines the location of the source or destination file(s). *Transport Method* is Cloud Connector, email, FTP, SFTP (SSH2), FTPS (TLS/SSL), HTTP, HTTPS, Local Network, or SMB (Server Message Block) Server. The selected *Transport Method* determines the sub-panel displayed as described in the next sections.

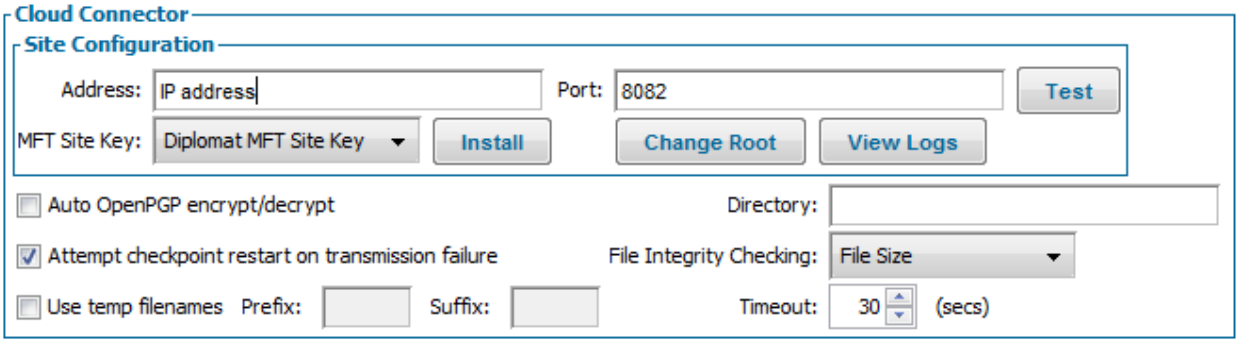
NOTE: SFTP (SSH2) is **not** supported for AS/400 systems. If you select SFTP (SSH2), *Server Type* is set to Windows/Unix and disabled.

7.4.2 Transport Methods

Diplomat MFT offers the following transport methods:

- Diplomat Cloud Connector
- Email
- FTP/S
- HTTP/S
- Local Network
- SFTP (SSH2)
- SMB (Server Message Block) Server

7.4.2.1 Cloud Connector Transport Method



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

Diplomat Cloud Connector 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.

Address

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

Port

Specifies a port number to be used for communication with Diplomat Cloud Connector. Default port is 8082. Contact the Diplomat Cloud Connector 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 Cloud Connector 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 Cloud Connector site. You must enter the single-use password created when Diplomat Cloud Connector was installed. If you do not have the correct password, the MFT site public key on the Diplomat Cloud Connector site is not updated.

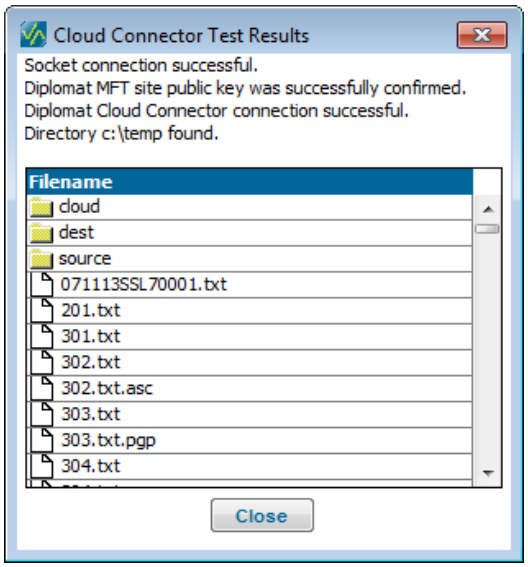
NOTE: Passwords are only created during a Windows installation process. When the Diplomat Cloud Connector Site is installed on a Red Hat Linux system, the Diplomat MFT Site public key must be sent to the Diplomat Cloud Connector administrator and copied to the Diplomat Cloud Connector site.

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 Cloud Connector administrator and copied to the Diplomat Cloud Connector site or the Diplomat Cloud Connector administrator can perform a Repair install, enter a new password and send the new password to the Diplomat MFT administrator.

Test Button

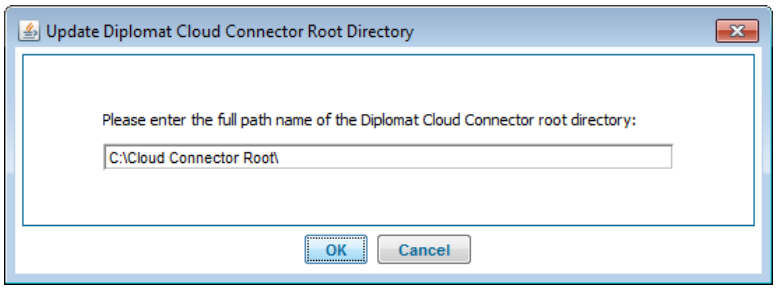
After entering the Diplomat Cloud Connector domain or IP address, port number and installing the Diplomat MFT site key on the Cloud Connector site, press **Test** to:

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



Change Root Button

Sets the default directory for Diplomat Cloud Connector 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.



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: Updating the root directory changes the root directory for the entire Diplomat Cloud Connector site and **affects all transactions sending files to or from the site.**

NOTE: The root directory defaults to the documents directory of the network identity associated with the Diplomat Cloud Connector 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 Cloud Connector 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 encrypted before transfer and decrypted before being written to the destination location. Files coming from the Diplomat Cloud Connector site are encrypted with the Server public key and decrypted with the Server private key pair. Files coming from the Diplomat MFT site are encrypted with the Diplomat Cloud Connector public key and decrypted with the Diplomat Cloud Connector private key pair.

NOTE: A new Diplomat Cloud Connector private key pair is created each time Diplomat Cloud Connector is restarted.

NOTE: The Diplomat Cloud Connector public key is not stored on the Diplomat MFT site and is passed 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 Cloud Connector 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 Cloud Connector 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 Cloud Connector site and **affects all transactions sending files to or from the site.**

File Integrity Checking
Choice of file integrity checking by file size, checksum 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.

Use Temp Filenames
A temporary filename is used while writing files to the destination. When the entire file has been written, the filename is changed to the destination filename. By default, the temporary filename is a random number. A prefix and/or suffix can be appended using the associated **Prefix** and **Suffix** settings.

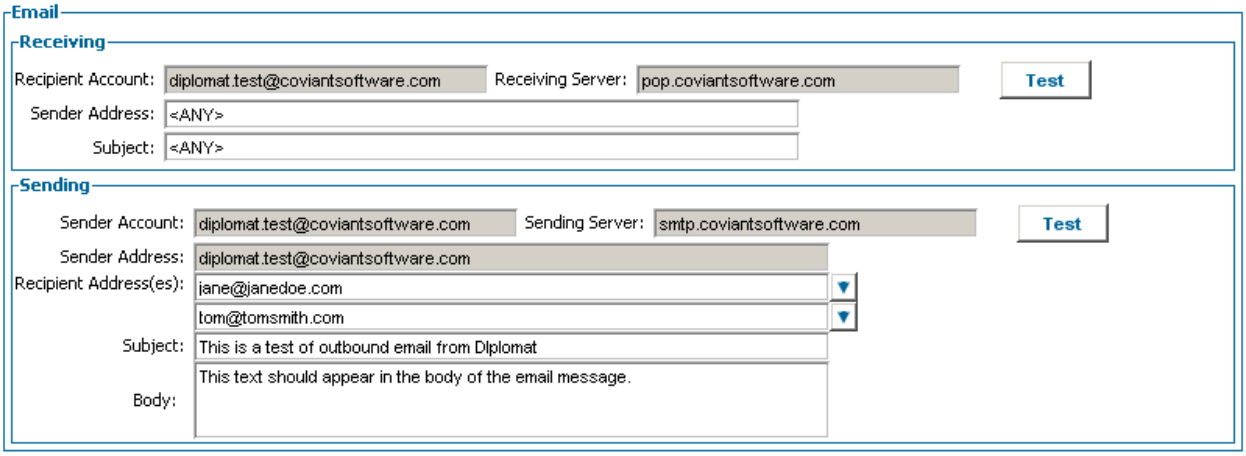
NOTE: Temporary filenames can only be used with Cloud Connector, FTP, FTPS, SFTP, local network or SMB destinations. FTP, FTPS and SFTP servers must support the RENAME command. Temporary filenames are not supported on HTTP, HTTPS or email destinations.

Prefix
String to be added before the default temporary filename.

Suffix
String to be added after the default temporary filename.

Timeout
Sets the length of time a Diplomat MFT site waits for a response from Diplomat Cloud Connector site.

7.4.2.2 Email Transport Method



Receiving

Recipient Account

Receives all email messages with attachments to be picked up by Diplomat Managed File Transfer. *Recipient Account* is defined on the Email Settings screen under Settings > Email from the top menu bar. The recipient account information can only be changed on the Email Settings screen.

Receiving Server

Stores all email messages with attachments to be picked up by Diplomat Managed File Transfer. *Receiving Server* is defined on the Email Settings screen under Settings > Email from the top menu bar. The receiving server information can only be changed on the Email Settings screen.

Test Button

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

Sender Address

Email address from which incoming files are sent. Diplomat MFT searches all email on the *Receiving Server* from the *Sender Address* for attachments that match the *Subject* and the *Source File(s)* information in the File Information panel. If *Sender Address* is <ANY>, all attachments that match the *Subject* and the *Source File(s)* information in the File Information panel are picked up.

Wildcards for up to one (?) or multiple (*) characters are allowed 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).

Each time a job runs, all email messages addressed to *Recipient Account* 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.

NOTE: Specifying the *Sender Address* as completely as possible reduces the time to review and download email attachments.

NOTE: The *Recipient Account* and *Receiving Server* are defined on the Email Settings screen under Settings > Email.

Subject

Incoming email messages can also be selected based on the content of the subject line of the email. If incoming email subject is **NOT** <ANY>, Diplomat MFT selects files that match the *Source File(s)* information in the File Information panel **AND** have a subject line that contains the specified string. Wildcards for up to one (?) or multiple (*) characters are allowed in the *Subject* field.

NOTE: Specifying the *Subject* as completely as possible reduces the time to review and download email attachments.

NOTE: If attached files are to be picked up by Diplomat MFT based on the name of the file and the sender is using Microsoft Outlook as the email client, the sender may need to send the email message using 'plain text' to avoid having attached file(s) renamed to winmail.dat.

Sending Email

Sender Account

Account used to log into the *Sending Server*. *Sender Account* is defined on the Email Settings screen under Settings > Email from the top menu bar. Sender account information can only be changed on the Email Settings screen.

Sending Server

Email server that sends all email messages with attachments created by Diplomat Managed File Transfer. *Sending Server* is defined on the Email Settings screen under Settings > Email from the top menu bar. Sending server information can only be changed on the Email Settings screen.

Sender Address

Address that identifies sender of email messages sent by Diplomat Managed File Transfer. *Sending Address* is defined on the Email Settings screen under Settings > Email from the top menu bar. Sending server information can only be changed on the Email Settings screen.

Test Button

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

Recipient Address(es)

Email address(es) to which outgoing files are sent. Use the drop-down arrow on the right-hand side of the *Recipient Address(es)* field to add or delete additional recipient address fields. Enter unique recipient addresses into each *Recipient Address(es)* field.

NOTE: Diplomat MFT uses the Destination/Notification Server defined on the Email Settings screen under Settings > Email to send outbound email messages.

NOTE: 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.

Subject

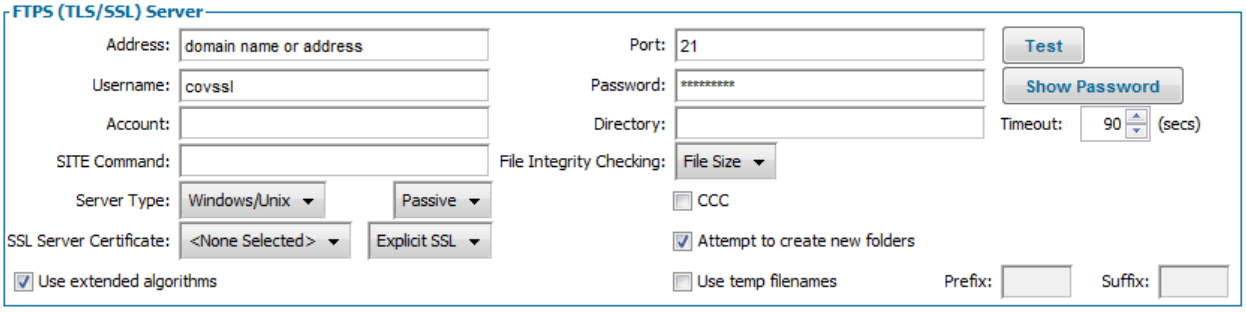
Outgoing email subject is the exact string that Diplomat MFT uses as the subject line of the outgoing email message.

Body

Outgoing email body is the exact text sent as the body of the email message.

NOTE: Some email servers may convert the body text to an attachment before sending.

7.4.2.3 FTP/S Transport Method



Address

Address of the FTP/S server where the source file(s) are found or destination files are written.

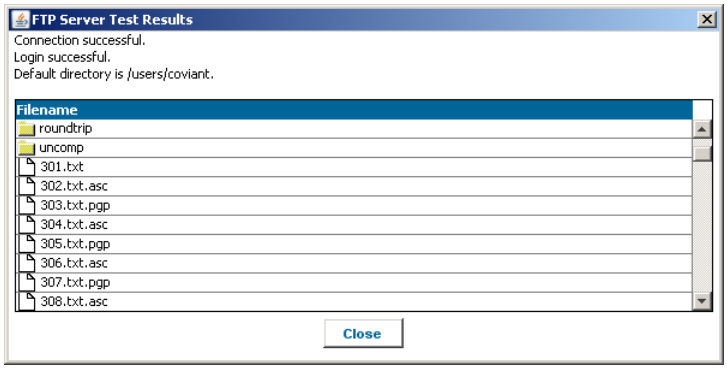
Port

Specifies a port number as required by the FTP/S server to be used for the FTP/S session. Contact the FTP/S server administrator to obtain this information.

Test Button

After entering the FTP/S server information, press **Test** to:

- Test the connection to the FTP/S server
- Determine whether the username and password are valid
- Display the default directory and its contents



Username

Name used to log in to the FTP/S server. Logging in under a username defaults to a particular directory on the FTP/S server.

NOTE: Some FTP/S servers allow anonymous login. If so, enter 'anonymous' in this field. It is *recommended* that FTP/S servers require a username and password before gaining access to the server for uploading or downloading files.

Password

Password used to log in to the FTP/S server. If you are using anonymous login, enter your email address or other identifier. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

Account

Some FTP/S servers require an account ID in addition to a username and password. If required by the FTP/S server, enter the account ID. Otherwise, leave the field blank. Contact the FTP/S server administrator to obtain this information.

Directory

Directory on the FTP/S Server where transaction file(s) are found or written. When an FTP/S session is initiated, a change directory command (CWD) is issued with this string as the argument. If the FTP/S server is set up to automatically point to the directory required by this transaction, leave this field blank.

NOTE: If the directory entered in the Directory field does not exist, Diplomat MFT attempts to create it.

NOTE: For AS/400 IFS systems, this directory path must always start with a '/'. If a directory path for an AS/400 IFS system is entered that does not start with a slash, Diplomat MFT processes the transaction as if a '/' were prepended to the beginning of the directory path. For AS/400 IFS systems, if the field is blank, Diplomat MFT uses '/' as the directory.

NOTE: For AS/400 Library systems, this field must be blank. AS/400 Library systems do not support directories.

NOTE: Except for AS/400 Library systems, you may specify a sub-directory from this directory in the *Source* or *Destination File(s)* fields for an individual transaction.

Timeout
Sets the length of time the Diplomat MFT Service waits for a response from the FTP/S server.

SITE Command
Specifies the content of SITE command to be issued after login on an FTP/S server and before file transfer is initiated.

NOTE: SITE commands are unique to each FTP/S server. Contact the FTP/S server administrator to determine which SITE commands are supported and/or required.

Server Type
Select Windows/Unix, AS400/IFS, AS400/Library, or MVS/IFS. Selecting AS400/IFS enables transactions with the Integrated File System (IFS) only. Selecting AS400/Library enables transactions with the AS/400 Library file system only.

SSL Server Certificate (FTPS only)
Select an SSL server certificate if you want to validate the certificate sent by an FTPS server when an FTPS session is initiated. This setting applies to FTPS(TLS/SSL) transport method only. If FTP or SFTP is selected, this field is disabled.

NOTE: Typically, you need to request the SSL server certificate from the FTPS server administrator. Then, you must import the certificate into Diplomat. Select Keys > SSL Server Certificates > Import SSL Certificate and browse to the file containing the SSL server certificate received from the FTPS server administrator.

Passive/Active
Since most FTP servers operate in passive mode, the default for this parameter is *Passive*. If the FTP server operates in active mode, select *Active* and review the active FTP settings under Settings > FTP from the top menu bar.

NOTE: FTPS (TLS/SSL) servers seldom operate in active mode, since firewalls are often not able to correctly route FTP traffic that has been encrypted via TLS/SSL.

Explicit/Implicit SSL (FTPS only)
Option when using FTPS (TLS/SSL) as the Transport Mode. When *Explicit SSL* selected for FTPS (TLS/SSL) transactions, Diplomat MFT uses the default FTP port, usually 21, and establishes the TLS/SSL link by issuing a command after establishing a connection. When *Implicit SSL* is selected, Diplomat MFT begins a TLS/SSL connection as soon as it logs in to an FTP/S server. The FTP/S server must define a specific port for implicit SSL, usually port 990. Default is *Explicit SSL*.

CCC (Clear Command Channel) (FTPS only)
Check *Clear Command Channel* to encrypt sensitive information including your username and password then transmit other information such as port and IP information in plaintext. This setting applies to FTPS(TLS/SSL) transport method only.

File Integrity Checking

Choice of file integrity checking by file size 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.

Attempt to Create New Folders

Check *Attempt to Create New Folder*s if you are writing to an FTP or FTPS server and want Diplomat MFT to create a new folder or folders under the default directory. Uncheck this setting to prevent Diplomat MFT from attempting to create new folders.

Use Temp Filenames

A temporary filename is used while writing files to the destination. When the entire file has been written, the filename is changed to the destination filename.

NOTE: Temporary filenames can only be used with FTP, FTPS, SFTP, local network or SMB destinations. And, FTP, FTPS and SFTP servers must support the RENAME command. Temporary filenames are not supported on HTTP, HTTPS or email destinations.

By default, the temporary filename is a random number. A prefix and/or suffix can be appended using the associated **Prefix** and **Suffix** settings.

Prefix

String to be added before the default temporary filename.

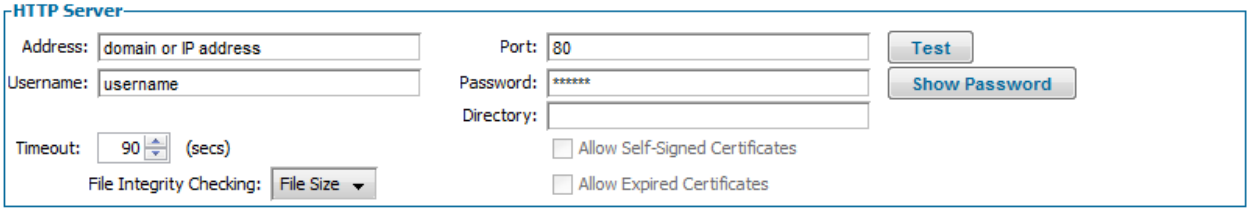
Suffix

String to be added after the default temporary filename.

Use Extended Algorithms

Defaults to checked. If you are having difficulty connecting to an FTP or FTPS server, be sure *Use Extended Algorithms* is checked to expand the number of algorithms attempted during the connection process.

7.4.2.4 HTTP/S Transport Method



NOTE: HTTP/S transport has a maximum file size of 2 GB.

Address
Address of the HTTP/S server where source files are found or destination file(s) are written.

Port
Specifies a port number as required by the HTTP/S server for the HTTP/S session. Contact the HTTP/S server administrator to obtain this information. Default for HTTP is 80. Default for HTTPS is 443.

Test Button
Use the **Test** button to attempt to access the directory on the system at the specified address using the specified port. For example, if *Address* is 'coviantsoftware.com', *Port* is '80' and *Directory* is 'test', Diplomat MFT issues a request for 'http://coviantsoftware.com:80/test'.

If the HTTP/S server requests authentication, Diplomat MFT provides the *Username* and *Password*. Typically, an HTTP/S server responds with a '401' code when authentication fails.

NOTE: The HTTP/S server controls whether authentication is required. Even if *Username* and *Password* are entered, the HTTP/S server may not request it. Thus, a successful connection and a '200' HTTP response code does not necessarily mean that a username and password were successfully authenticated.

NOTE: Diplomat MFT indicates when a connection fails because the HTTP/S server certificate is expired or not signed by a valid Certificate Authority. If you want to allow the connection to the HTTP/S server to proceed, check the *Allow Self-Signed Certificates* or *Allow Expired Certificates* checkbox, as needed.

Username
Name needed to authenticate access to the directory on the HTTP/S server where transaction file(s) are to be found or written.

Password

Password needed to authenticate access to the directory on the HTTP/S server where transaction file(s) are to be found or written. Accounts with *Administrator* privileges can select the *Show Passphrase* button to display the passphrase.

Directory
Sub-directory on the HTTP/S Server where source files are found or destination file(s) are written. This sub-directory is appended to the root directory associated with the HTTP/S server. Contact the HTTP/S server administrator to obtain this information.

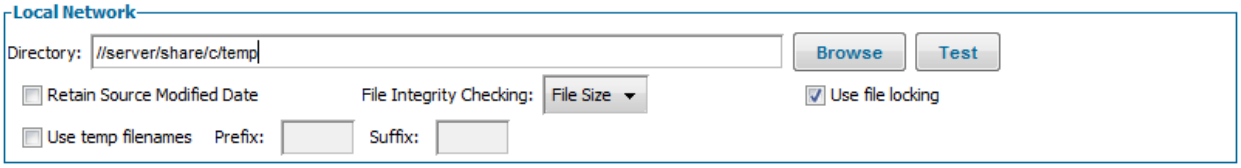
Timeout
Sets the length of time the Diplomat MFT Service waits for a response from the HTTP/S server.

File Integrity Checking
Choice of file integrity checking by file size 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.

Allow Self-Signed Certificates
Check *Allow Self-Signed Certificates* to allow a connection to an HTTPS server using an SSL certificate that is not signed by a valid Certificate Authority. Only enabled for HTTPS servers. Default is unchecked.

Allow Expired Certificates
Check *Allow Expired Certificates* to allow a connection to an HTTPS server using an SSL certificate that has expired. Only enabled for HTTPS servers. Default is unchecked.

7.4.2.5 Local Network Transport Method



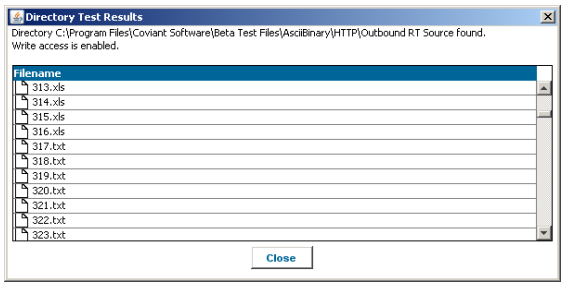
Directory

Directory on local network where source file(s) are found or destination files are written. If needed, use the **Browse** button to select a directory.

Test Button

After entering the local network directory information, press **Test** to:

- Verify that the directory can be found
- Read and/or write access are enabled
- Display the contents of the directory



CAUTION: If you have trouble running a transaction in which you specified a UNC path or a mapped drive, the logon for the Diplomat MFT Service or diplomatServer daemon may not have the privileges to access the specified directory. Please use **Test** to confirm that the logon for the Diplomat MFT Service or diplomatServer daemon has the required privileges before contacting Coviant Software Support.

Retain Source Modified Date

Check *Retain Source Modified Date* to make the modified date of the destination file the same as the modified date of the source file.

File Integrity Checking

Choice of file integrity checking by file size 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.

Use File Locking

Check Use File Locking to attempt to lock the target file during processing.

Use Temp Filenames

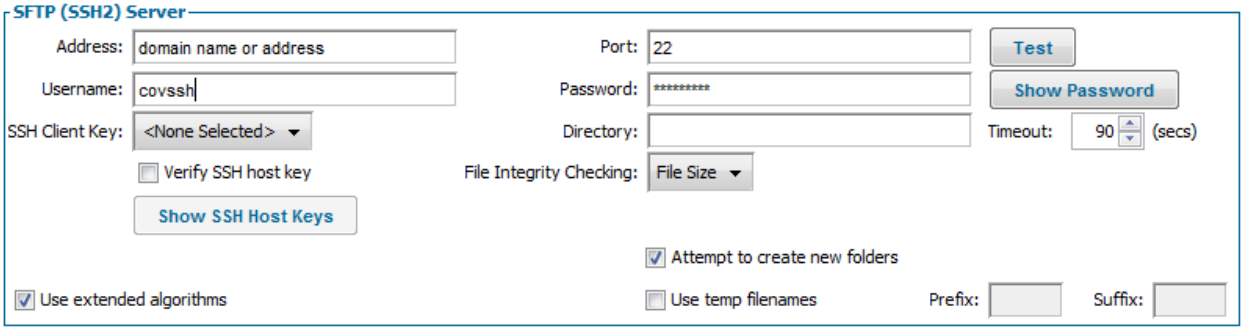
A temporary filename is used while writing files to the destination. When the entire file has been written, the filename is changed to the destination filename.

NOTE: Temporary filenames can only be used with Cloud Connector, FTP, FTPS, SFTP, local network or SMB destinations. FTP, FTPS and SFTP servers must support the RENAME command. Temporary filenames are not supported on HTTP, HTTPS or email destinations.

By default, the temporary filename is a random number. A prefix and/or suffix can be appended using the associated **Prefix** and **Suffix** settings.

Prefix/Suffix
String to be added before/after the default temporary filename.

7.4.2.6 SFTP Transport Method



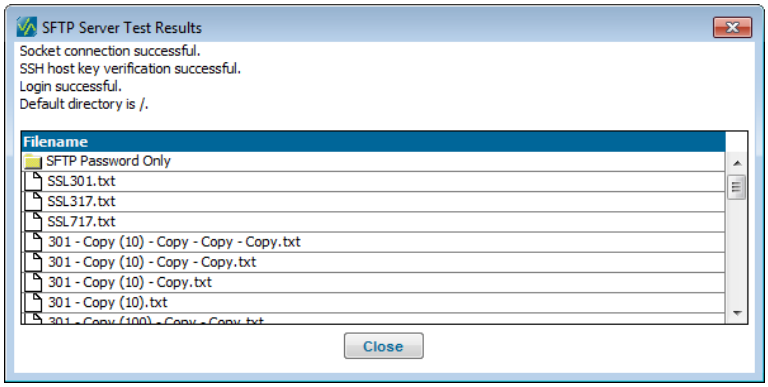
Address

Address of the SFTP server where the source file(s) are found or destination files are written.

Port

Specifies a port number as required by the SFTP server to be used for the SFTP session. Contact the SFTP server administrator to obtain this information.

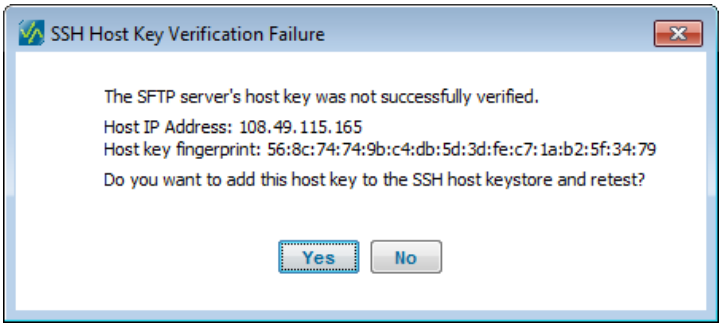
Test Button



After entering the SFTP server information, press **Test** to:

- Test the connection to the SFTP server.
- Check that an SSH host key has been verified.

  NOTE: If the SSH host key from the SFTP server is not in the Diplomat MFT database, then you are prompted to add the SSH host key and retest the connection.



- Determine whether the username, password and SSH client key are valid.
- Display the default directory and its contents.

Username
Name used to log in to the SFTP server. Logging in under a username defaults to a particular directory on the SFTP server.

Password
Password used to log in to the SFTP server. If you are using anonymous login, enter your email address or other identifier. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

SSH Client Key
SSH client private key associated with an SFTP account login.

Verify SSH Host Key
Check *Verify SSH Host Key* to check that the SSH Host Key associated with the SFTP server matches an SSH Host Key in the list displayed by the *Show Host Key*s button.

Show Host Keys Button
Use the *Show Host Keys* button to display the list domains and fingerprints associated with the SFTP server. *Show Host Keys* button is disabled when Verify SSH host key is not checked.

Directory
Directory on the SFTP Server where transaction file(s) are found or written. When an SFTP session is initiated, a change directory command (CWD) is issued with this string as the argument. If the SFTP server is set up to automatically point to the directory required by this transaction, leave this field blank.

Timeout
Sets the length of time the Diplomat MFT Service waits for a response from the SFTP server.

File Integrity
Choice of file integrity checking by file size 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.

Attempt to Create New Folders
Check Attempt to Create New Folders if you are writing to an SFTP server and want Diplomat MFT to create a new folder or folders under the default directory. Uncheck this setting to prevent Diplomat MFT from attempting to create new folders.

Use Temp Filenames
A temporary filename is used while writing files to the destination. When the entire file has been written, the filename is changed to the destination filename.

NOTE: Temporary filenames can only be used with FTP, FTPS, SFTP, local network or SMB destinations. And, FTP, FTPS and SFTP servers must support the RENAME command. Temporary filenames are not supported on HTTP, HTTPS or email destinations.

By default, the temporary filename is a random number. A prefix and/or suffix can be appended using the associated **Prefix** and **Suffix** settings.

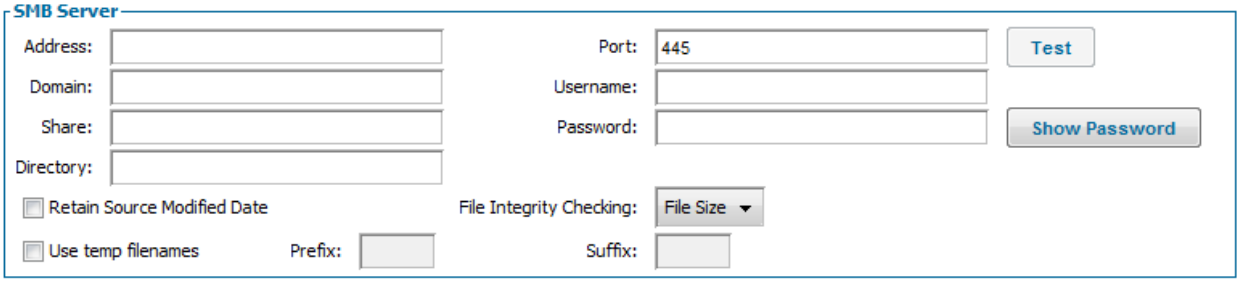
Prefix
String to be added before the default temporary filename.

Suffix
String to be added after the default temporary filename.

Use Extended Algorithms

Defaults to checked. If you are having difficulty connecting to an SFTP server, be sure *Use Extended Algorithms* is checked to expand the number of algorithms attempted during the connection process.

7.4.2.7 SMB Server Transport Method



Address

Address of the SMB (Server Message Block) server where the source file(s) are located.

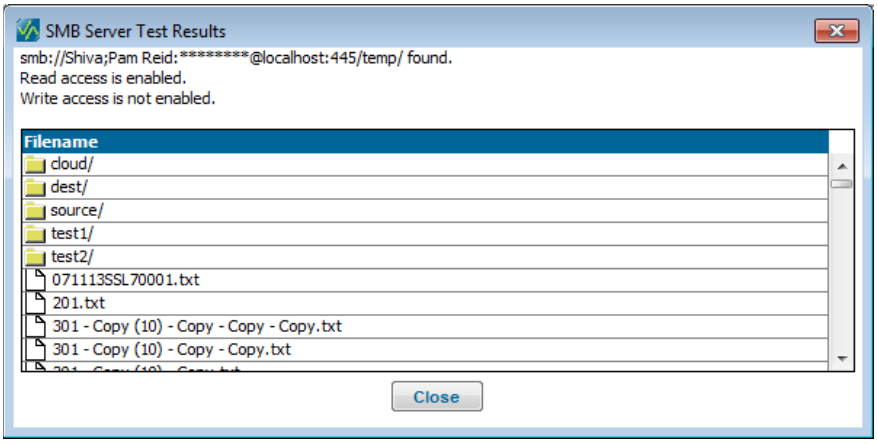
Port

Specifies a port number as required by the SMB server to be used for the SMB session. Contact the SMB server administrator to obtain this information.

Test Button

After entering the SMB server information, press **Test** to:

- Test the connection to the SMB server
- Determine whether the username and password, if any, are valid
- Display the default directory and its contents



Domain

Name used to log in to the SMB server where transaction file(s) are to be found. Logging in under a username defaults to a particular directory on the SMB server

Username

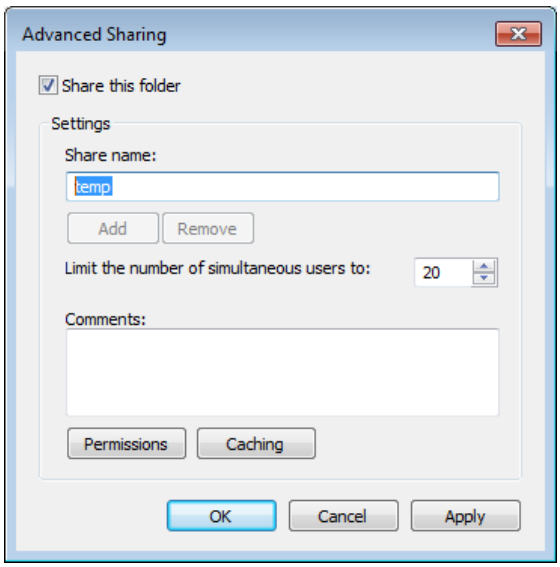
Name used to log in to the SMB server where transaction file(s) are to be found. Logging in under a username defaults to a particular directory on the SMB server.

Password

Password used to log in to the SMB server. If you are using anonymous login, enter your email address or other identifier. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

Share

Directory on the SMB server that has been set up as a network share. On most Windows systems, network shares can be set up from Properties > Sharing > Advanced Sharing for the target directory.



If you do not know how to specify a network share, contact the system manager of the SMB server for assistance.

Directory
Sub-directory in the share on the SMB server where transaction file(s) are found.

Retain Source Modified Date
Check *Retain Source Modified Date* to make the modified date of the destination file the same as the modified date of the source file.

File Integrity Checking
Choice of file integrity checking by file size 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.

Use Temp Filenames
A temporary filename is used while writing files to the destination. When the entire file has been written, the filename is changed to the destination filename.

NOTE: Temporary filenames can only be used with Cloud Connector, FTP, FTPS, SFTP, local network or SMB destinations. FTP, FTPS and SFTP servers must support the RENAME command. Temporary filenames are not supported on HTTP, HTTPS or email destinations.

By default, the temporary filename is a random number. A prefix and/or suffix can be appended using the associated **Prefix** and **Suffix** settings.

Prefix
String to be added before the default temporary filename.

Suffix
String to be added after the default temporary filename.

7.4.3 OpenPGP Keys

OpenPGP keys assigned to partner profiles are used for encryption/decryption and signing/verification. **The drop-down for the key fields in Trusted Profiles only displays key pairs. The drop-down for the key fields in Public Profiles displays only public keys.**

Partner's Encrypt/Decrypt Key

For Public Profiles, the encryption 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 your Diplomat MFT database before you can set this parameter.

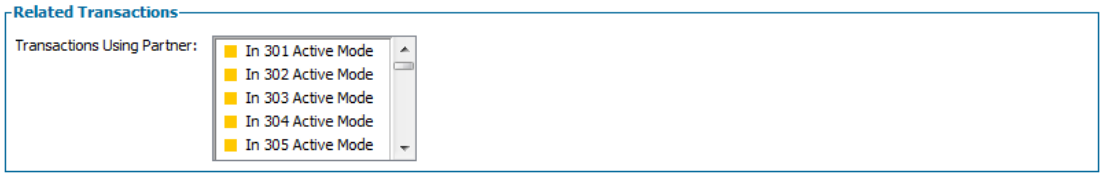
For Trusted Profiles, the encryption key is the OpenPGP key pair used to decrypt files you receive.

Partner's Sign/Verify Key

For Public Profiles, the signature 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.

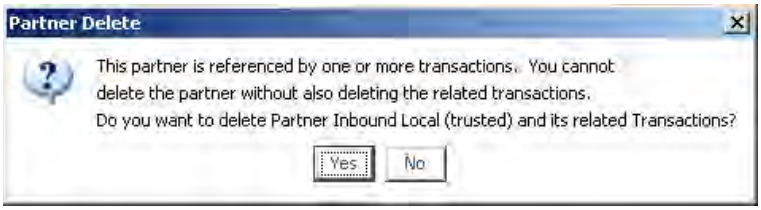
7.4.4 Related Transactions



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.



7.4.5 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 Understanding Transactions

8.1 Transactions Overview

Transactions are file transfers that are either outbound to a trading partner/remote site or inbound from a trading partner/remote site.

Transactions are at the core of Diplomat MFT functionality 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 (Cloud Connector, Email, FTP, FTPS, SFTP, HTTP/S, local network 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 backup or restore these files as a group by selecting File > Backup or File > Restore.

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 and outbound transactions. Typically, inbound transactions are for file transfers where your company is receiving files from a trading partner. Outbound transactions are for file transfers where your company is sending files to a trading partner.

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 at all times based on the Job Execution panel settings:

- When *Do Not Run* is checked and/or no job scheduling types are set/allowed, a red status indicator '■' is displayed.
- When *Do Not Run* is **not** checked and transactions are actively being scheduled, a green status indicator '■' is displayed.
- When *Allow Diplomat MFT Scripting Agent or API requests* is checked, a dark green status indicator '■' is displayed.
- When *File Monitoring* is selected, a light green status indicator '■' is displayed.
- When a key, partner, or folder associated with the transaction is suspended, an orange status indicator '■' is displayed next to the transaction.
- When an individual transaction is suspended, a yellow status indicator '■' is displayed next to the transaction.

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

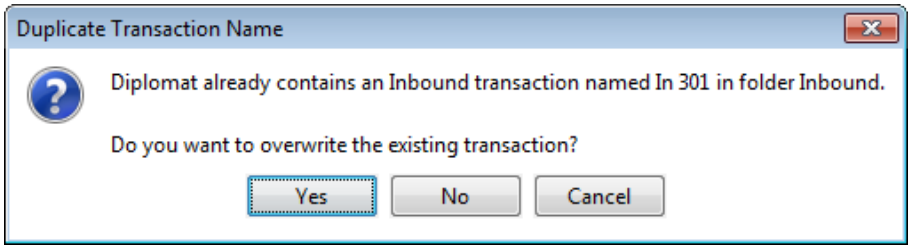
The drop-down menu from Transactions on the top menu bar allows you to create, save, delete, or search transactions.

8.3.1 Create Inbound/Outbound

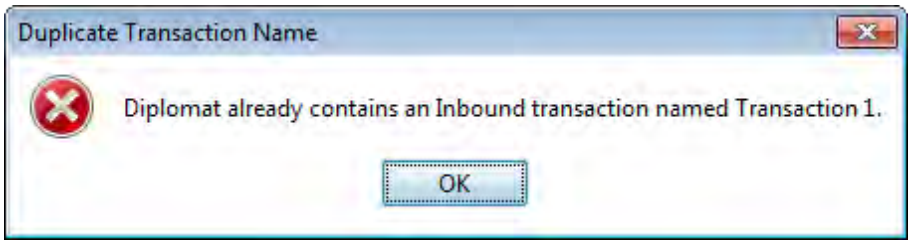
New inbound and outbound transactions are created using the drop-down menu from the Transaction button on the top menu bar. Newly created transactions are set automatically to *Do Not Run*.

You will be prompted to enter a *Transaction Name*, which must be unique across all inbound and outbound transactions. A *Transaction Name* 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 an inbound transaction with the same name as an outbound transaction or vice versa. 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/Save As

A transaction can be saved using the drop down menu from the Transaction menu item on the top menu bar or by entering <Ctrl+S>. If you have not already saved the transaction, you are prompted to save it upon exit from Diplomat. You must save a transaction before you exit from the Diplomat MFT Client in order to retain information entered during the session.

You may not change the *Transaction Name* of a transaction once it has been created, but you can use *Save As* on the transaction drop-down to save it under another name, then delete the original transaction using *Delete* on the same drop-down menu. When using *Save As*, the new *Transaction Name* may not contain any of the following characters: * ? / \ | " : < >.

New transactions created using *Save As* are set to *Do Not Run*.

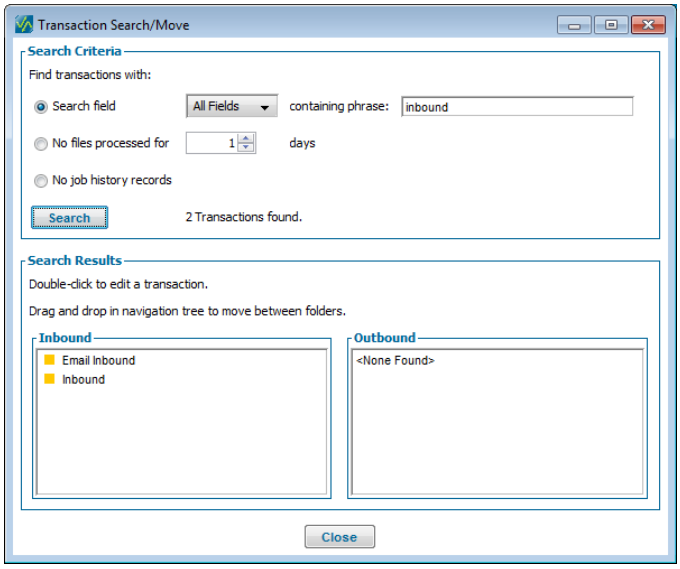
NOTE: If you attempt to create a new transaction using *Save As* with a name that already exists in the Diplomat MFT transaction database, you will be warned before the existing transaction is overwritten.

8.3.3 Delete

You may delete a transaction using the drop down menu from the Transactions menu item on the menu bar or by entering <Ctrl+D>, or right-click and select Delete.

Transaction deletions are permanent. The only way to recover a transaction is to restore a previously saved backup of the entire Diplomat MFT transaction database. The database contains only the keys, transactions, and partners as of the date the backup was done. Any changes to the database since the backup was saved are lost.

8.3.4 Search/Move



Transaction Search/Move dialog is used to locate and move or edit specific transactions.

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.

Search Criteria

Search Criteria are used 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.

NOTE: The *phrase* field is case sensitive.

The Search Button is used to initiate the search using the criteria in the Search Criteria panel and displays the number of transactions found.

Search Results

Search Results displays all of the inbound and outbound transactions that match the search criteria. A status indicator is displayed to the left of each Transaction Name which indicates scheduling status of each transaction by displaying:

- Red status indicator for transactions that are not scheduled to run,
- Green status indicator for transactions that have a job currently scheduled for execution,
- Dark green status indicator for transactions that are set to allow external requests.
- Light green status indicator for transactions that are set to use file monitoring.
- Yellow status indicator for transactions that have been suspended directly, and
- Orange status indicator for transactions that have been suspended indirectly.

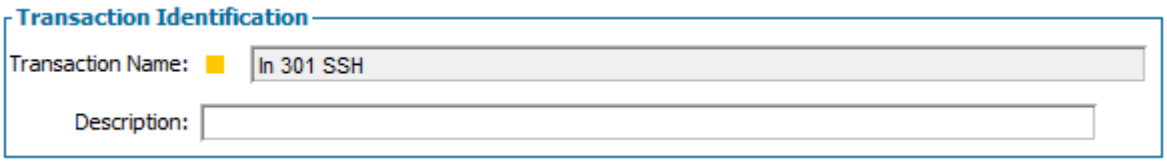
8.4 Transactions Window

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  and  buttons located in the top, right corner of each panel.

NOTE: Newly created transactions are displayed with all panels maximized. Previously-saved transactions are displayed with all panels minimized.

8.4.1 Transaction Identification



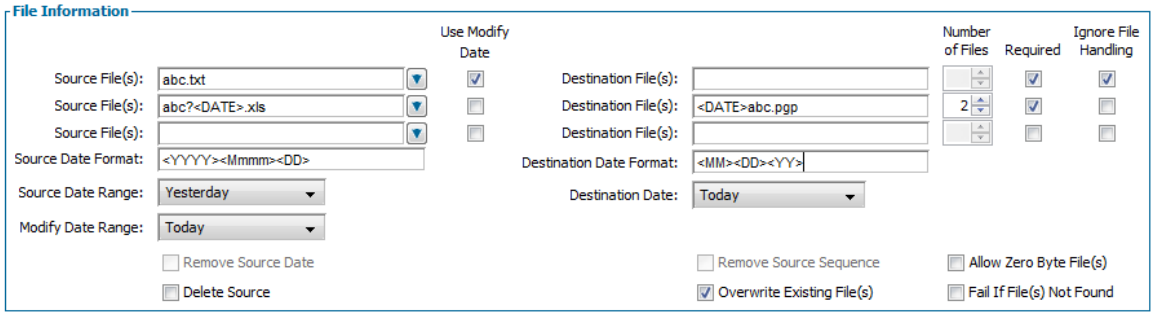
Transaction Name
Name of the transaction. Must be a unique name across all inbound and outbound transactions. A *Transaction Name* may not contain any of the following characters: * ? / \ | " : < >. *Transaction Name* field length is limited to 110 characters.

The icon to the left of the Transaction Name indicates the status of the transaction, which is not scheduled '■', allow external requests '■', use file monitoring '■', suspended indirectly '■', suspended directly '■', or actively being scheduled '■'.

NOTE: Transactions created prior to Diplomat v3.5 may contain *Transaction Names* that exceed the 110 character limit. If so, some data may be truncated when written to the SQL audit database. You can manually shorten older *Transaction Names* by using *Save As* and deleting the original transaction.

Description
Descriptive overview to help recognize the transaction.

8.4.2 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 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*.
- Modified date falls within the *Modified Date Range*.

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

- A naming template that interprets a pipe '|' wildcard in the *Destination File(s)* fields as the source filename.
- 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, 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* drop-down, the files are added to the list of files to be processed by 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. If the *Required* checkbox is checked, then the files are required and processing of the job stops due to the wrong number of files being found. If the *Required* checkbox is **not** checked, then the files for a particular *Source File(s)* field are not required, the file pairs are removed from the list to be processed and the job continues.

Once the list of source and destination filename pairs has been validated, the following 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 changes. Any encryption, decryption, signing, verification, or other actions specified in the *File Handling* panel are ignored.
- If the *Overwrite Existing Files* checkbox is checked, a file is written to the destination directory even if a pre-existing file in the directory has the same name.
- 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 *Delete Source* checkbox is checked and a file is transferred successfully, Diplomat MFT attempts to delete the source file.
- If the *Fail if File(s) Not Found* checkbox is checked, jobs that find no files to be processed generate a status of 'Failure', failure notifications are sent, and other related actions are taken.

Source File(s)

Source File(s) fields contain the name(s) of file(s) to be picked up. **NOTE: Filenames are case sensitive.**

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

NOTE: Source files are processed in the order in which they are identified using the *Source File(s)* specification.

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 '*' and the question mark '?' are the only wildcard characters recognized in *Source File(s)* fields. 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.

NOTE: HTTP and HTTPS transports do not support the use of wildcards.

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>'.

NOTE: HTTP and HTTPS transports do NOT support Sequence Number parameters.

NOTE: HTTP and HTTPS transports support the Date parameter ONLY when the result is a single filename (e.g., Source Date Range is set to "Today").

NOTE: 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.

NOTE: 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.

Using Multiple Source File(s) Fields

Use the drop-down arrow on the right-hand side of the *Source File(s)* field to add or delete additional source file fields. Enter unique filenames into each *Source File(s)* field. Each *Source File(s)* field may contain wildcards, a date parameter, and a sequence number parameter.

Source Date Format

When a *Source File(s)* field contains a date parameter, the *Source Date Format* field which specifies the elements of the 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. **NOTE:** Each parameter must be enclosed in angle brackets. **NOTE: Source date elements are case sensitive.**

Source Date Elements		
Element Type	**Element**	**Element Description**
Year[2]	<YY>	2-digit numeric year with zero padding added when necessary (e.g., 07)
	<YYYY>	4-digit numeric year (e.g., 2007)
Month[2]	<MM>	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.
	<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>	2-digit numeric day of month with zero padding added when necessary (e.g., 04)
Julian Day	<JJJ>	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.
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

[2] *Source Date Format* can contain only 1 (one) year element and only 1 (one) month element.

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. If the value is not within the source date range, the file transfer job continues as if no files were found. Values are as follows: All Dates, Today, Yesterday, Within last week, Within last 2 weeks, Within last month, Within last 3 months, and Within last year.

For example, a job that runs at 11:00 a.m. on Tuesday, June 26, 2007, that has a source date range equal to 'Yesterday' and date format '<MM><DD><YYYY><hh><mm>' would pick up a file named 'abc062520070800.txt'.

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).

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).

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

NOTE: Filenames are case sensitive.

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.

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'.

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 as summarized below:

File Processing	Extension
No encryption or signature	<none>
Encrypt or sign	.pgp
ASCII armor (with or without encrypt or sign)	.asc

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 Date Parameters in Destination File(s) Fields

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.

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.

Using Sequence Number Parameters in Destination File(s) Fields

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.

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, Within last week, Within last 2 weeks, Within last month, Within last 3 months, Within last year, Oldest and Most Recent.

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 elements of the date parameter. 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.

NOTE: Each parameter must be enclosed in angle brackets. **NOTE: Destination date elements are case sensitive.**

Destination Date Elements		
Element Type	**Element**	**Element Description**
Year	<YY>	2-digit numeric year with zero padding added when necessary (e.g., 07)
	<YYYY>	4-digit numeric year (e.g., 2007)
Month	<M>	Numeric month that allows a minimum of 1 digit (e.g., 4)
	<MM>	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.
	<MMM> <Mmm> <mmm>	3-character month with matching capitalization. ▪ If all letters are capitalized, then all letters in the name of the month will be capitalized (e.g., <MMM> for APR). ▪ If only the leading M is capitalized, then only the first letter of the month will be capitalized (e.g., <Mmm> for Apr). ▪ If all letters are lowercase, then all letters in the name of the month will be lowercase (e.g., <mmmm> 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 will be capitalized (e.g., <MMMM> for APRIL). ▪ If only the leading M is capitalized, then only the first letter of the month will be capitalized (e.g., <Mmmm> for April). ▪ If all letters are lowercase, then all letters in the name of the month will be lowercase (e.g., <mmmm> for april). ▪ No other capitalization formats are allowed.
Day	<D>	Numeric day of the month with a minimum of 1 digit (e.g., 4)
	<DD>	2-digit numeric day of month with zero padding added when necessary (e.g., 04)
Julian Day	<J>	Numeric Julian day of the year with a minimum of 1 digit (e.g., 14 for January 14)
	<JJJ>	3-digit numeric Julian day of the year with zero padding added when necessary (e.g., 014 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

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.

Remove Source Date

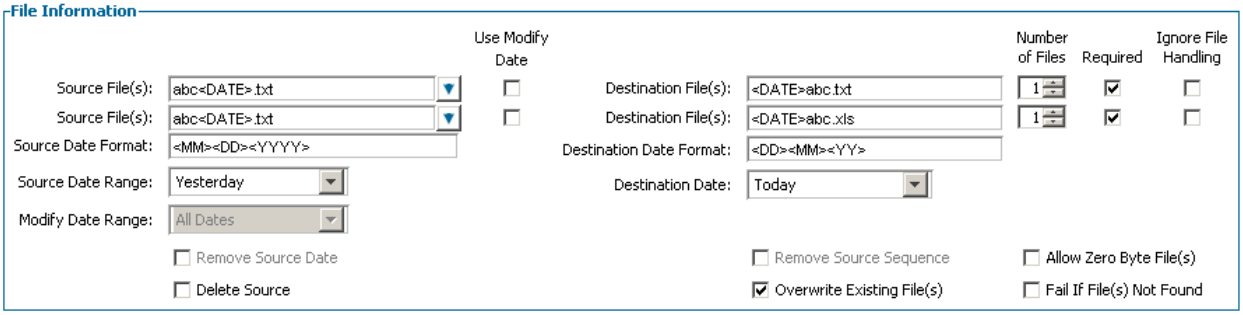
When *Remove Source Date* is checked, the string matching the date parameter in the *Source File(s)* field is removed before creating destination filenames. Unless at least one *Source File(s)* field contains a date parameter and the associated *Destination File(s)* field is blank, contains a pipe '|'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

Delete Source

If *Delete Source* is checked, 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.

Overwrite Existing File(s)

If *Overwrite Existing File(s)* is checked, any existing file in the destination directory with the same name as the file being transferred is overwritten. If *Overwrite Existing File(s)* is not checked 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.

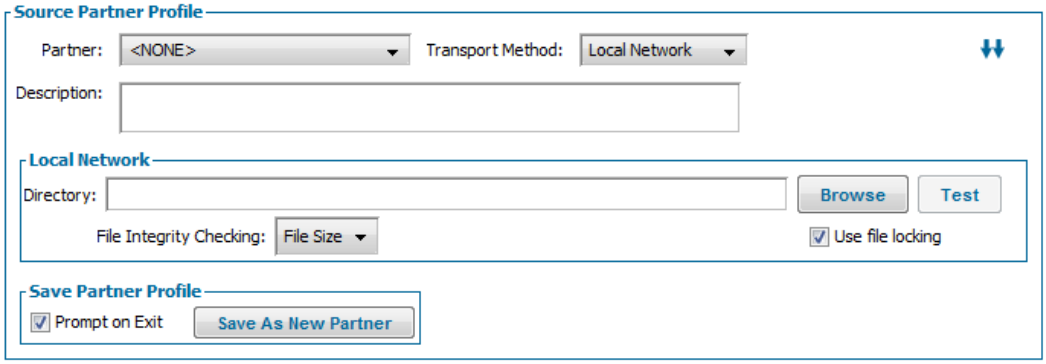
Fail if File(s) Not Found

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 of 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.

NOTE: 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.

8.4.3 Source Partner Profile



Partner
You can select a saved Partner Profile to be used to set all information on the Source Partner Profile panel in a transaction. If you do not want to use a saved Partner Profile, select <NONE> and you can make changes to the source partner profile on the transaction.

NOTE: Once you select a saved Partner Profile, you cannot make changes to the fields in the Source Partner Profile panel in the transaction.

NOTE: Changes made to the source partner profile in the transaction do not change the saved Partner Profile. If desired, use **Save As New Partner** in the Save Partner Profile panel to save the current information on the Source Partner Profile panel as a new partner for use in other transactions.

Transport Method
Determines the location of the source file(s). *Transport Method* is Cloud Connector, email, FTP, SFTP (SSH2), FTPS (TLS/SSL), HTTP, HTTPS, Local Network or SMB (Server Message Block) server. The selected *Transport Method* determines the sub-panel displayed as described in the next sections.

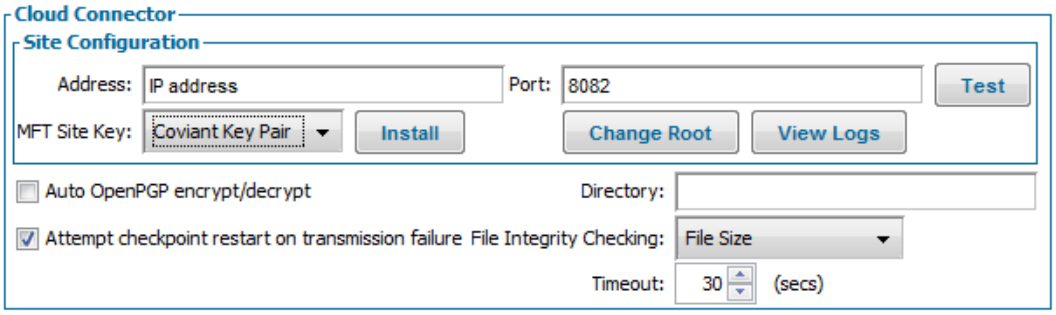
Description
Descriptive overview to help recognize the partner profile.

Save Partner Profile
NOTE: The fields in the Save Partner Profile panel are only active if you have selected <NONE> for your source partner profile.

Prompt on Exit
Check Prompt on Exit to be prompted before exiting the Diplomat MFT Client to save the current information in the Source Partner Profile panel as a new partner for use in other transactions. Prompt on Exit defaults to checked.

Save As New Partner
Select **Save As New Partner** to save the current information on the Source Partner Profile panel as a new partner for use in other transactions.

8.4.3.1 Cloud Connector Transport Method



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

Diplomat Cloud Connector 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.

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

Port
Specifies a port number to be used for communication with Diplomat Cloud Connector. Default port is 8082. Contact the Diplomat Cloud Connector 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 Cloud Connector 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 Cloud Connector site. You must enter the single-use password created when Diplomat Cloud Connector was installed. If you do not have the correct password, the MFT site public key on the Diplomat Cloud Connector site is not updated.

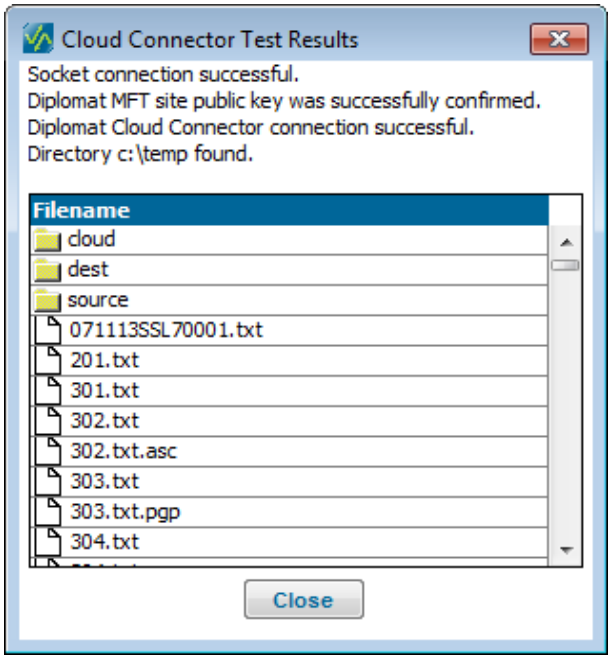
NOTE: Passwords are only created during a Windows installation process. When the Diplomat Cloud Connector Site is installed on a Red Hat Linux system, the Diplomat MFT Site public key must be sent to the Diplomat Cloud Connector administrator and copied to the Diplomat Cloud Connector site.

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 Cloud Connector administrator and copied to the Diplomat Cloud Connector site or the Diplomat Cloud Connector administrator can perform a Repair install, enter a new password and send the new password to the Diplomat MFT administrator.

Test Button

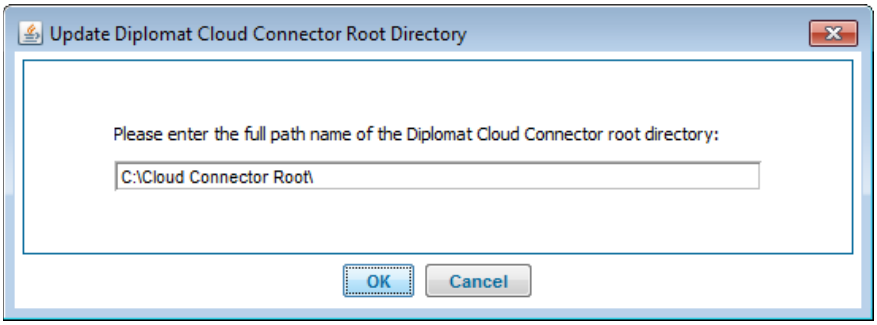
After entering the Diplomat Cloud Connector information, press **Test** to:

- Test the connection to the Diplomat Cloud Connector site
- Determine whether the OpenPGP public key at the Diplomat Cloud Connector 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 Cloud Connector site
- Display the default directory and its contents
-



Change Root Button

Sets the default directory for Diplomat Cloud Connector 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.



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: Updating the root directory changes the root directory for the entire Diplomat Cloud Connector site and **affects all transactions sending files to or from the site.**

NOTE: The root directory defaults to the documents directory of the network identity associated with the Diplomat Cloud Connector 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 Cloud Connector 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 encrypted before transfer and decrypted before being written to the destination location. Files coming from the Diplomat Cloud Connector site are encrypted with the Server public key and decrypted with the Server private key pair. Files coming from the Diplomat MFT site are encrypted with the Diplomat Cloud Connector public key and decrypted with the Diplomat Cloud Connector private key pair.

NOTE: A new Diplomat Cloud Connector private key pair is created each time Diplomat Cloud Connector is restarted.

NOTE: The Diplomat Cloud Connector public key is not stored on the Diplomat MFT site and is passed 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 Cloud Connector site where transaction file(s) are found or written.

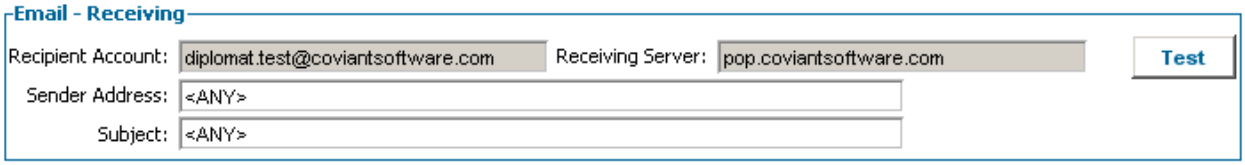
Values starting with a slash are interpreted as full path names. Other values are interpreted as sub-directories from the root directory shown in the Site Configuration panel.

NOTE: The root directory for the Diplomat Cloud Connector 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 Cloud Connector site and **affects all transactions sending files to or from the site.**

File Integrity Checking
Choice of file integrity checking by file size, checksum 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 Cloud Connector site.

8.4.3.2 Email Transport Method



Recipient Account

Receives all email messages with attachments to be picked up by Diplomat Managed File Transfer. *Recipient Account* is defined on the Email Settings screen under Settings > Email from the top menu bar. The recipient account information can only be changed on the Email Settings screen.

Receiving Server

Stores all email messages with attachments to be picked up by Diplomat Managed File Transfer. *Receiving Server* is defined on the Email Settings screen under Settings > Email from the top menu bar. The receiving server information can only be changed on the Email Settings screen.

Test Button

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

Sender Address

Email address from which incoming files are sent. Diplomat MFT searches all email on the *Receiving Server* from the *Sender Address* for attachments that match the *Subject* and the *Source File(s)* information in the File Information panel. If *Sender Address* is <ANY>, all attachments that match the *Subject* and the *Source File(s)* information in the File Information panel are picked up.

Wildcards for up to one (?) or multiple (*) characters are allowed 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).

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.

NOTE: Specifying the *Sender Address* as completely as possible reduces the time to review and download email attachments.

NOTE: The *Recipient Address* and *Receiving Server* are defined on the Email Settings screen under Settings > Email.

Subject

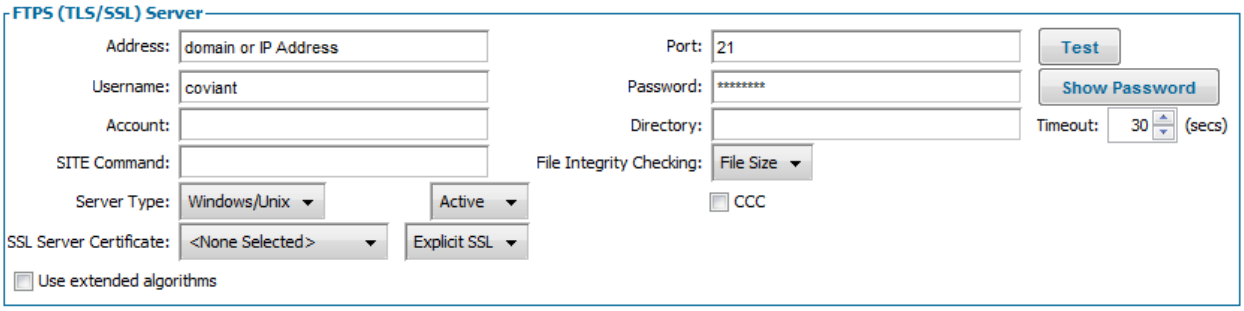
Incoming email messages can also be selected based on the content of the subject line of the email. If incoming email subject is **NOT** <ANY>, Diplomat MFT selects files that match the *Source File(s)* information in the File Information panel **AND** have a

subject line that contains the specified string. Wildcards for up to one (?) or multiple (*) characters are allowed in the *Subject* field.

NOTE: Specifying the *Subject* as completely as possible reduces the time to review and download email attachments.

NOTE: If attached files are to be picked up by Diplomat MFT based on the name of the file and the sender is using Microsoft Outlook as the email client, the sender may need to send the email message using 'plain text' to avoid having attached file(s) renamed to winmail.dat.

8.4.3.3 FTP/S Transport Method

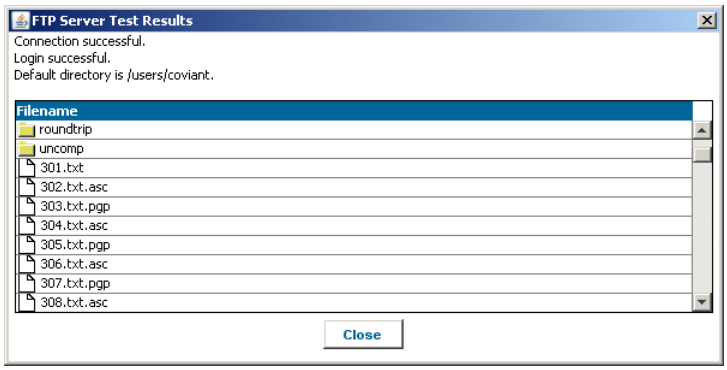


Address
Address of the FTP/S server where the source file(s) are found.

Port
Specifies a port number as required by the FTP/S server to be used for the FTP/S session. Contact the FTP/S server administrator to obtain this information.

Test Button
After entering the FTP/S server information, press **Test** to:

- Test the connection to the FTP/S server
- Determine whether the username and password are valid
- Display the default directory and its contents



Username
Name used to log in to the FTP/S server where transaction file(s) are to be found. Logging in under a username defaults to a particular directory on the FTP/S server.

NOTE: Some FTP/S servers allow anonymous login. If so, enter 'anonymous' in this field. It is *recommended* that FTP/S servers require a username and password before gaining access to the server for uploading or downloading files.

Password
Password used to log in to the FTP/S server. If you are using anonymous login, enter your email address or other identifier. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

Account
Some FTP/S servers require an account ID in addition to a username and password. If required by the FTP/S server, enter the account ID. Otherwise, leave the field blank. Contact the FTP/S server administrator to obtain this information.

Directory
Directory on the FTP/S server where transaction file(s) are found. When an FTP/S session is initiated, a change directory command (CWD) is issued with this string as the argument. If the FTP/S server is set up to automatically point to the directory required by this transaction, leave this field blank.

NOTE: For AS/400 IFS systems, this directory path must always start with a '/'. If a directory path for an AS/400 IFS system is entered that does not start with a slash, Diplomat MFT processes the transaction as if a '/' were prepended to the beginning of the directory path. For AS/400 IFS systems, if the field is blank, Diplomat MFT uses '/' as the directory.

NOTE: For AS/400 Library systems, this field must be blank. AS/400 Library systems do not support directories.

NOTE: Except for AS/400 Library systems, you may specify a sub-directory from this directory in the *Source* or *Destination File(s)* fields for an individual transaction.

Timeout
Sets the length of time the Diplomat MFT Service waits for a response from the FTP/S server.

SITE Command
Specifies the content of SITE command to be issued after login on an FTP/S server and before file transfer is initiated.

NOTE: SITE commands are unique to each FTP/S server. Contact the FTP/S server administrator to determine which SITE commands are supported and/or required.

Server Type
Select Windows/Unix, AS400/IFS, AS400/Library, or MVS/IFS. Selecting AS400/IFS enables transactions with the Integrated File System (IFS) only. Selecting AS400/Library enables transactions with the AS/400 Library file system only.

SSL Server Certificate (FTPS only)
Select an SSL server certificate if you want to validate the certificate sent by an FTPS server when an FTPS session is initiated. This setting applies to FTPS(TLS/SSL) transport method only. If FTP is selected, this field is disabled.

NOTE: Typically, you need to request the SSL server certificate from the FTPS server administrator. Then, you must import the certificate into Diplomat. Select Keys > SSL Server Certificates > Import SSL Certificate and browse to the file containing the SSL server certificate received from the FTPS server administrator.

Passive/Active
Since most FTP/S servers operate in passive mode, the default for this parameter is *Passive*. If the FTP/S server operates in active mode, select *Active* and review the active FTP settings under Settings > FTP from the top menu bar.

NOTE: FTPS (TLS/SSL) servers seldom operate in active mode, since firewalls are often not able to correctly route FTP traffic that has been encrypted via TLS/SSL.

Explicit/Implicit SSL (FTPS only)
Option when using FTPS (TLS/SSL) as the Transport Mode. When *Explicit SSL* selected for FTPS (TLS/SSL) transactions, Diplomat MFT uses the default FTP port, usually 21, and establishes the TLS/SSL link by issuing a command after establishing a connection. When *Implicit SSL* is selected, Diplomat MFT begins a TLS/SSL connection as soon as it logs in to an FTP server. The FTP server must define a specific port for implicit SSL, usually port 990. Default is *Explicit SSL*.

CCC (Clear Command Channel) (FTPS only)
Check *Clear Command Channel* to encrypt sensitive information including your username and password then transmit other information such as port and IP information in plaintext. This setting applies to FTPS(TLS/SSL) transport method only.

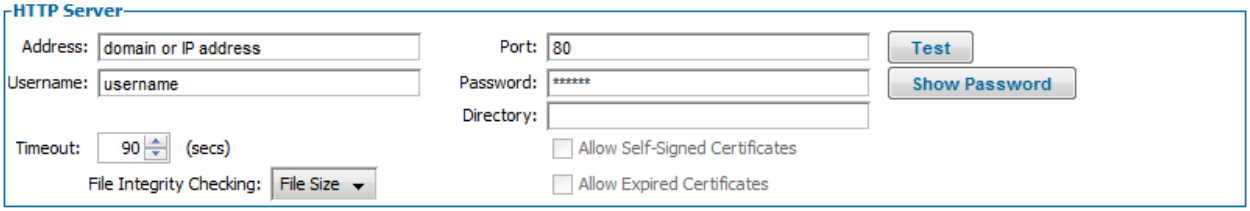
File Integrity Checking

Choice of file integrity checking by file size 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.

Use Extended Algorithms

Defaults to checked. If you are having difficulty connecting to an FTP or FTPS server, be sure *Use Extended Algorithms* is checked to expand the number of algorithms attempted during the connection process.

8.4.3.4 HTTP/S Transport Method



NOTE: HTTP/S transport has a maximum file size of 2 GB.

Address
Address of the HTTP/S server where the source file(s) are found.

Port
Specifies a port number as required by the HTTP/S server for the HTTP/S session. Contact the HTTP/S server administrator to obtain this information. Default for HTTP is 80. Default for HTTPS is 443.

Test Button
Use the **Test** button to attempt to access the directory on the system at the specified address using the specified port. For example, if *Address* is 'coviantsoftware.com', *Port* is '80' and *Directory* is 'test', Diplomat MFT issues a request for 'http://coviantsoftware.com:80/test'.

If the HTTP/S server requests authentication, Diplomat MFT provides the *Username* and *Password*. Typically, an HTTP/S server responds with a '401' code when authentication fails.

NOTE: The HTTP/S server controls whether authentication is required. Even if *Username* and *Password* are entered, the HTTP/S server may not request it. Thus, a successful connection and a '200' HTTP response code does not necessarily mean that a username and password were successfully authenticated.

NOTE: Diplomat MFT indicates when a connection fails because the HTTP/S server certificate is expired or not signed by a valid Certificate Authority. If you want to allow the connection to the HTTP/S server to proceed, check the *Allow Self-Signed Certificates* or *Allow Expired Certificates* checkbox, as needed.

Username
Name needed to authenticate access to the directory on the HTTP/S server where transaction file(s) are to be found.

Password

Password needed to authenticate access to the directory on the HTTP/S server where transaction file(s) are to be found. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

Directory
Sub-directory on the HTTP/S Server where source file(s) are found. This sub-directory is appended to the root directory associated with the HTTP/S server. Contact the HTTP/S server administrator to obtain this information.

Timeout
Sets the length of time the Diplomat MFT Service waits for a response from the HTTP/S server.

File Integrity Checking
Choice of file integrity checking by file size 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.

Allow Self-Signed Certificates
Check *Allow Self-Signed Certificates* to allow a connection to an HTTPS server using an SSL certificate that is not signed by a valid Certificate Authority. Only enabled for HTTPS servers. Default is unchecked.

Allow Expired Certificates
Check *Allow Expired Certificates* to allow a connection to an HTTPS server using an SSL certificate that has expired. Only enabled for HTTPS servers. Default is unchecked.

8.4.3.5 Local Network Transport Method

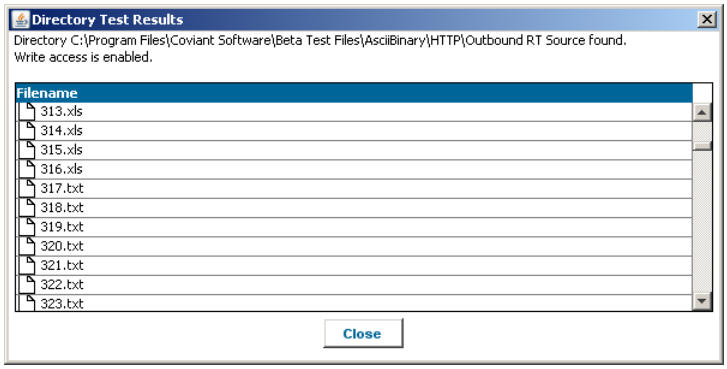
Directory

Directory on the local network where the source file(s) are found. If needed, use the **Browse** button to select a directory.

Test Button

After entering the local network directory information, press **Test** to:

- Verify that the directory can be found
- Read and/or write access are enabled
- Display the contents of the directory



CAUTION: If you have trouble running a transaction in which you specified a UNC path or a mapped drive, the logon for the Diplomat MFT Service or diplomatServer daemon may not have the privileges to access the specified directory. Please use **Test** to confirm that the logon for the Diplomat MFT Service or diplomatServer daemon has the required privileges before contacting Coviant Software Support.

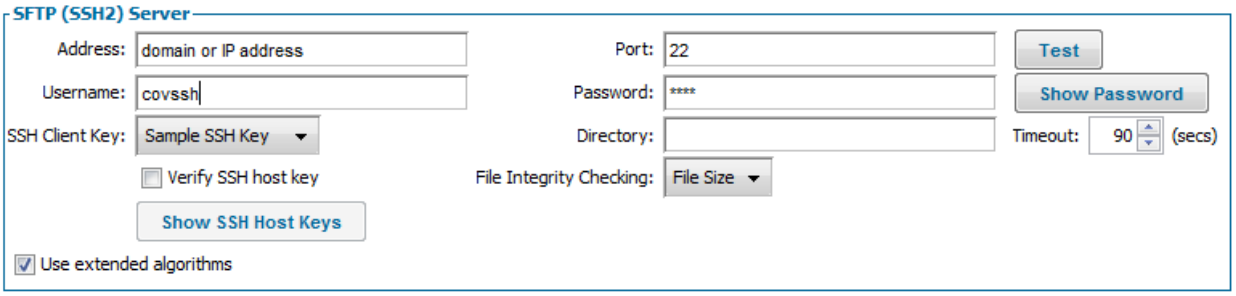
File Integrity Checking

Choice of file integrity checking by file size 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.

Use File Locking

Check Use File Locking to attempt to lock the target file during processing.

8.4.3.6 SFTP Transport Method



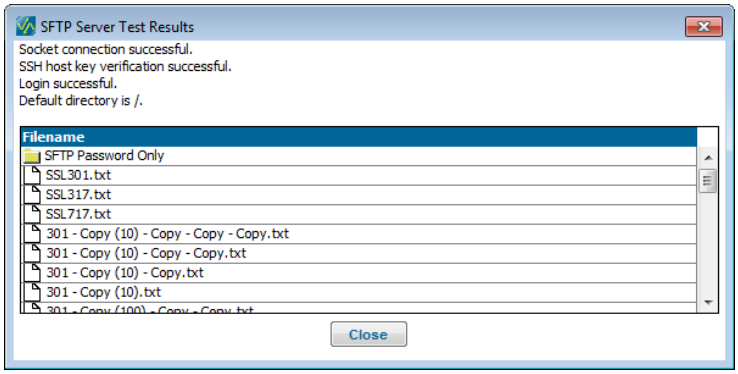
Address

Address of the SFTP server where the source file(s) are found.

Port

Specifies a port number as required by the SFTP server to be used for the SFTP session. Contact the SFTP server administrator to obtain this information.

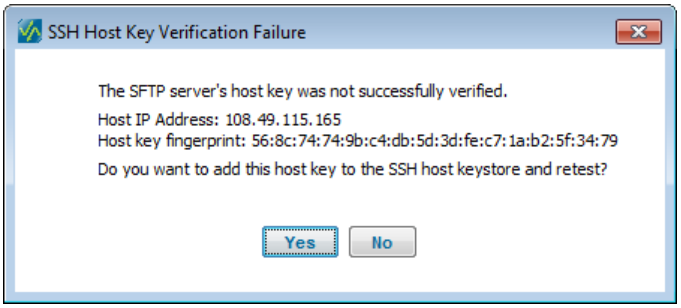
Test Button



After entering the SFTP server information, press **Test** to:

- Test the connection to the SFTP server.
- Check that an SSH host key has been verified.

  NOTE: If the SSH host key from the SFTP server is not in the Diplomat MFT database, then you are prompted to add the SSH host key and retest the connection.



- Determine whether the username, password and SSH client key are valid.
- Display the default directory and its contents.

Username
Name used to log in to the SFTP server. Logging in under a username defaults to a particular directory on the SFTP server.

Password
Password used to log in to the SFTP server. If you are using anonymous login, enter your email address or other identifier. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

SSH Client Key
SSH private key associated with an SFTP account login.

Verify SSH Host Key
Check *Verify SSH Host Key* to check that the SSH Host Key associated with the SFTP server matches an SSH Host Key in the list displayed by the *Show Host Key*s button.

Show Host Keys Button
Use the *Show Host Keys* button to display the list domains and fingerprints associated with the SFTP server. *Show Host Keys* button is disabled when Verify SSH host key is not checked.

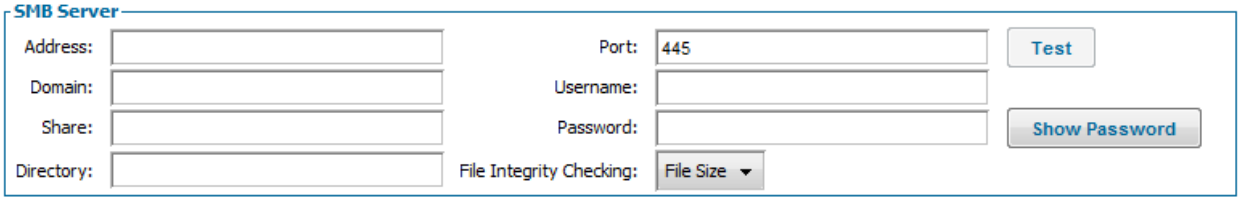
Directory
Directory on the SFTP Server where transaction file(s) are found or written. When an SFTP session is initiated, a change directory command (CWD) is issued with this string as the argument. If the SFTP server is set up to automatically point to the directory required by this transaction, leave this field blank.

Timeout
Sets the length of time the Diplomat MFT Service waits for a response from the SFTP server.

File Integrity
Choice of file integrity checking by file size 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.

Use Extended Algorithms
Defaults to checked. If you are having difficulty connecting to an SFTP server, be sure *Use Extended Algorithms* is checked to expand the number of algorithms attempted during the connection process.

8.4.3.7 SMB Server Transport Method



Address

Address of the SMB (Server Message Block) server where the source file(s) are located.

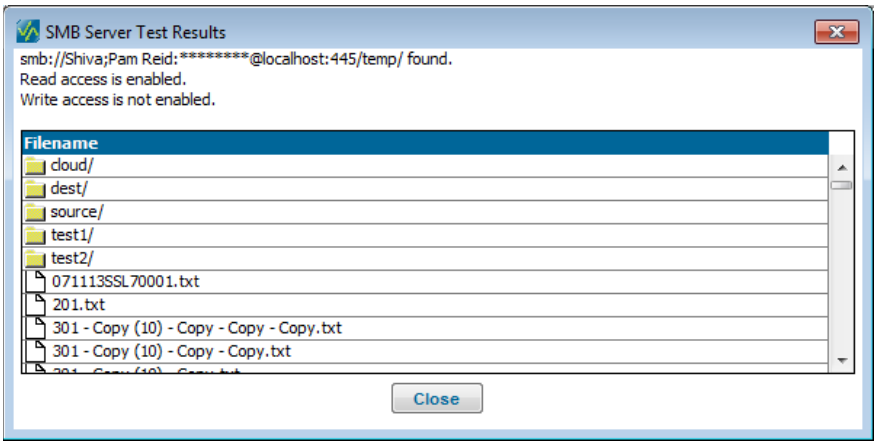
Port

Specifies a port number as required by the SMB server to be used for the SMB session. Contact the SMB server administrator to obtain this information.

Test Button

After entering the SMB server information, press **Test** to:

- Test the connection to the SMB server
- Determine whether the username and password, if any, are valid
- Display the default directory and its contents



Domain

Name used to log in to the SMB server where transaction file(s) are to be found. Logging in under a username defaults to a particular directory on the SMB server

Username

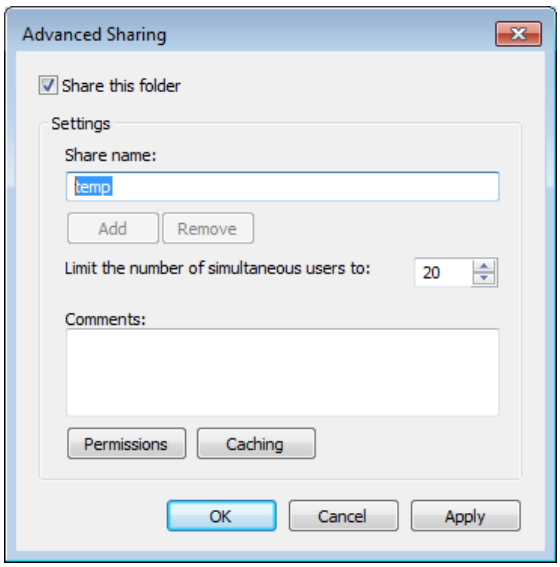
Name used to log in to the SMB server where transaction file(s) are to be found. Logging in under a username defaults to a particular directory on the SMB server.

Password

Password used to log in to the SMB server. If you are using anonymous login, enter your email address or other identifier. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

Share

Directory on the SMB server that has been set up as a network share. On most Windows systems, network shares can be set up from Properties > Sharing > Advanced Sharing for the target directory.



If you do not know how to specify a network share, contact the system manager of the SMB server for assistance.

Directory

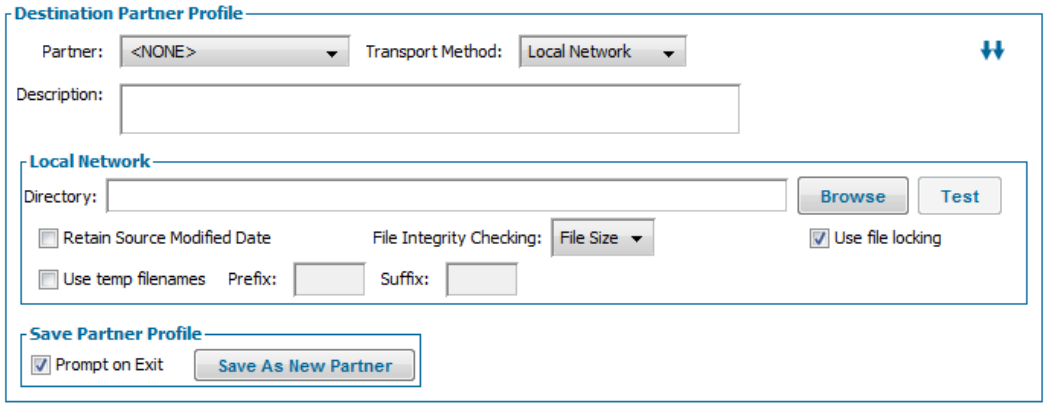
Sub-directory in the share on the SMB server where transaction file(s) are found.

File Integrity Checking

Choice of file integrity checking by file size 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.

.

8.4.4 Destination Partner Profile



Partner

You can select a saved Partner Profile to be used to set all default information for the *Destination Partner Profile* panel. If you do not want to use a saved Partner Profile, select <NONE>. No defaults are pre-filled and you can make changes to the destination partner profile on the transaction.

NOTE: Once you select a saved *Partner Profile*, you cannot make changes to the fields in the *Destination Partner Profile* panel in the transaction.

NOTE: Changes made to the destination partner profile in the transaction do not change the saved Partner Profile. If desired, use **Save As New Partner** in the Save Partner Profile panel to save the current information on the Destination Partner Profile panel as a new partner for use in other transactions.

Transport Method

Determines the location of the destination file(s). *Transport Method* is Cloud Connector, email, FTP, SFTP (SSH2), FTPS (TLS/SSL), HTTP, HTTPS, Local Network or SMB (Server Message Block) server. The selected *Transport Method* determines the sub-panel displayed as described in the next sections.

Description

Descriptive overview to help recognize the partner profile.

Save Partner Profile

NOTE: The fields in the Save Partner Profile panel are only active if you have selected <NONE> for your destination partner profile.

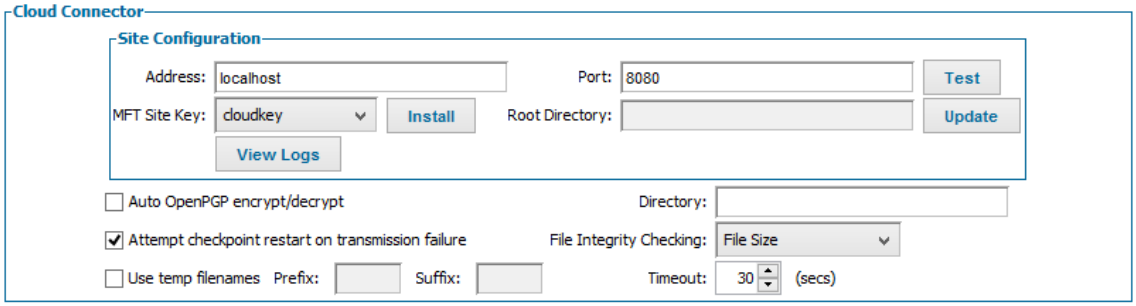
Prompt on Exit

Check Prompt on Exit to be prompted before exiting the Diplomat MFT Client to save the current information in the *Destination Partner Profile* as a new partner for use in other transactions. Prompt on Exit defaults to checked.

Save As New Partner

Select **Save As New Partner** to save the current information on the *Destination Partner Profile* panel as a new partner for use in other transactions.

8.4.4.1 Cloud Connector Transport Method



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

Diplomat Cloud Connector 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.

Address

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

Port

Specifies a port number to be used for communication with Diplomat Cloud Connector. Default port is 8082. Contact the Diplomat Cloud Connector 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 Cloud Connector 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 Cloud Connector site. You must enter the single-use password created when Diplomat Cloud Connector was installed. If you do not have the correct password, the MFT site public key on the Diplomat Cloud Connector site is not updated.

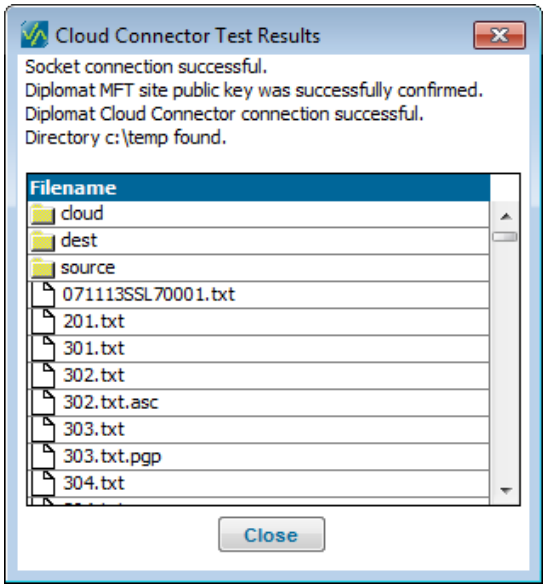
NOTE: Passwords are only created during a Windows installation process. When the Diplomat Cloud Connector Site is installed on a Red Hat Linux system, the Diplomat MFT Site public key must be sent to the Diplomat Cloud Connector administrator and copied to the Diplomat Cloud Connector site.

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 Cloud Connector administrator and copied to the Diplomat Cloud Connector site or the Diplomat Cloud Connector administrator can perform a Repair install, enter a new password and send the new password to the Diplomat MFT administrator.

Test Button

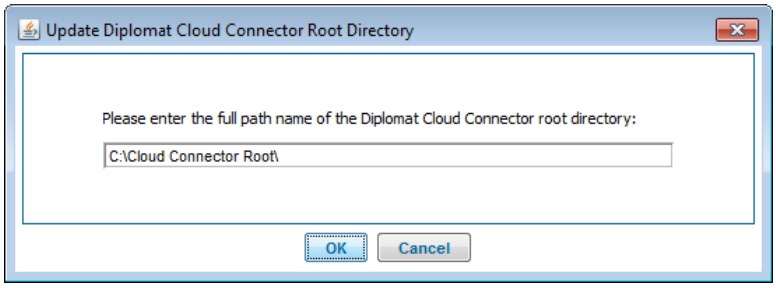
After entering the Diplomat Cloud Connector information, press **Test** to:

- Test the connection to the Diplomat Cloud Connector site
- Determine whether the OpenPGP public key at the Diplomat Cloud Connector 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 Cloud Connector site
- Display the default directory and its contents
- Refresh the Root Directory field



Change Root Button

Sets the default directory for Diplomat Cloud Connector 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.



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: Updating the root directory changes the root directory for the entire Diplomat Cloud Connector site and **affects all transactions sending files to or from the site.**

NOTE: The root directory defaults to the documents directory of the network identity associated with the Diplomat Cloud Connector 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 Cloud Connector 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 encrypted before transfer and decrypted before being written to the destination location. Files coming from the Diplomat Cloud Connector site are encrypted with the Server public key and decrypted with the Server private key pair. Files coming from the Diplomat MFT site are encrypted with the Diplomat Cloud Connector public key and decrypted with the Diplomat Cloud Connector private key pair.

NOTE: A new Diplomat Cloud Connector private key pair is created each time Diplomat Cloud Connector is restarted.

NOTE: The Diplomat Cloud Connector public key is not stored on the Diplomat MFT site and is passed 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 Cloud Connector 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 Cloud Connector 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 Cloud Connector site and **affects all transactions sending files to or from the site.**

File Integrity Checking
Choice of file integrity checking by file size, checksum 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.

Use Temp Filenames
A temporary filename is used while writing files to the destination. When the entire file has been written, the filename is changed to the destination filename.

NOTE: Temporary filenames can only be used with Cloud Connector, FTP, FTPS, SFTP, local network or SMB destinations. FTP, FTPS and SFTP servers must support the RENAME command. Temporary filenames are not supported on HTTP, HTTPS or email destinations.

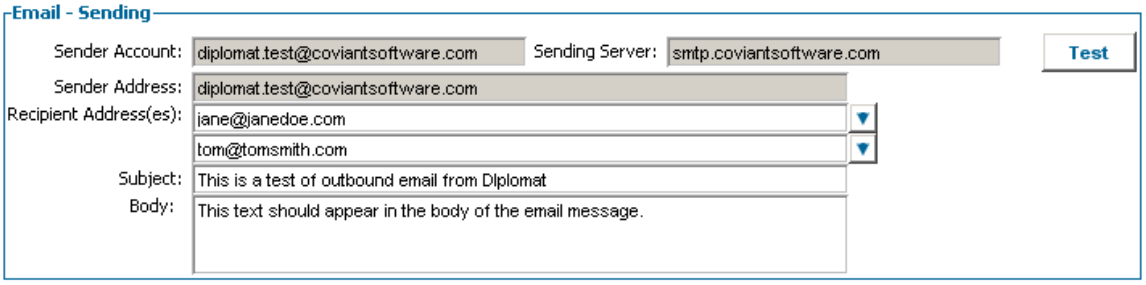
By default, the temporary filename is a random number. A prefix and/or suffix can be appended using the associated **Prefix** and **Suffix** settings.

Prefix
String to be added before the default temporary filename.

Suffix
String to be added after the default temporary filename.

Timeout
Sets the length of time a Diplomat MFT site waits for a response from Diplomat Cloud Connector site.

8.4.4.2 Email Transport Method



Sender Account

Account used to log into the *Sending Server*. *Sender Account* is defined on the Email Settings screen under Settings > Email from the top menu bar. Sender account information can only be changed on the Email Settings screen.

Sending Server

Email server that sends all email messages with attachments created by Diplomat Managed File Transfer. *Sending Server* is defined on the Email Settings screen under Settings > Email from the top menu bar. Sending server information can only be changed on the Email Settings screen.

Sender Address

Address that identifies sender of email messages sent by Diplomat Managed File Transfer. *Sending Address* is defined on the Email Settings screen under Settings > Email from the top menu bar. Sending server information can only be changed on the Email Settings screen.

Test Button

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

Recipient Address(es)

Email address(es) to which outgoing files are sent. Use the drop-down arrow on the right-hand side of the *Recipient Address(es)* field to add or delete additional recipient address fields. Enter unique recipient addresses into each *Recipient Address(es)* field.

NOTE: Diplomat MFT uses the Destination/Notification Server defined on the Email Settings screen under Settings > Email to send outbound email messages.

NOTE: 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.

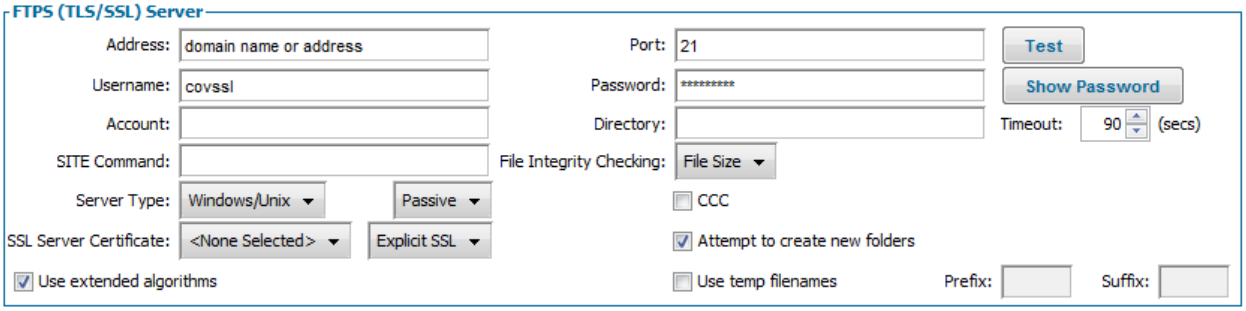
Subject

Outgoing email subject is the exact string that Diplomat MFT uses as the subject line of the outgoing email message.

Body

Outgoing email body is the exact text sent as the body of the email message. **NOTE:** Some email servers may convert the body text to an attachment before sending.

8.4.4.3 FTP/S Transport Method



Address

Address of the FTP/S server where the destination file(s) are written.

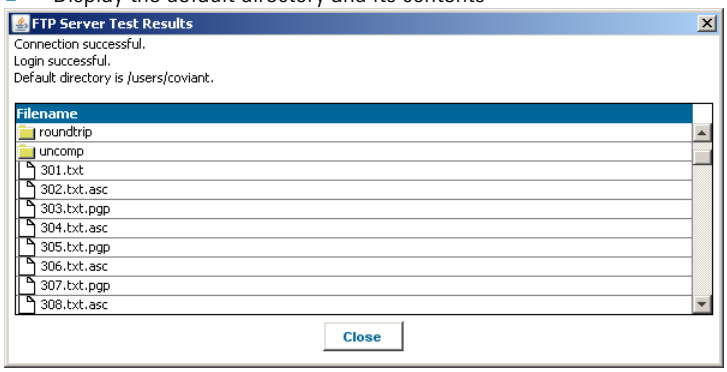
Port

Specifies a port number as required by the FTP/S server to be used for the FTP/S session. Contact the FTP/S server administrator to obtain this information.

Test Button

After entering the FTP/S server information, press **Test** to:

- Test the connection to the FTP/S server
- Determine whether the username and password, if any, are valid
- Display the default directory and its contents



Username

Name used to log in to the FTP/S server where destination file(s) are written. Logging in under a username defaults to a particular directory on the FTP/S server.

NOTE: Some FTP servers allow anonymous login. If so, enter 'anonymous' in this field. It is *recommended* that FTP servers require a username and password before gaining access to the server for uploading or downloading files.

Password

Password used to log in to the FTP/S server. If you are using anonymous login, enter your email address or other identifier. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

Account

Some FTP servers require an account ID in addition to a username and password. If required by the FTP server, enter the account ID. Otherwise, leave the field blank. Contact the FTP server administrator to obtain this information.

Directory
Directory on the FTP/S Server where transaction file(s) are written. When an FTP/S session is initiated, a change directory command (CWD) is issued with this string as the argument. If the FTP/S server is set up to automatically point to the directory required by this transaction, leave this field blank.

NOTE: If the directory entered in the Directory field does not exist, Diplomat MFT attempts to create it.

NOTE: For AS/400 IFS systems, this directory path must always start with a '/'. If a directory path for an AS/400 IFS system is entered that does not start with a slash, Diplomat MFT processes the transaction as if a '/' were prepended to the beginning of the directory path. For AS/400 IFS systems, if the field is blank. Diplomat MFT uses '/' as the directory.

NOTE: For AS/400 Library systems, this field must be blank. AS/400 Library systems do not support directories.

NOTE: Except for AS/400 Library Systems, you may specify a sub-directory from this directory in the *Source* or *Destination File(s)* fields for an individual transaction.

Timeout
Sets the length of time the Diplomat MFT Service waits for a response from the FTP/S server.

SITE Command
Specifies the content of SITE command to be issued after login on an FTP/S server and before file transfer is initiated.

NOTE: SITE commands are unique to each FTP/S server. Contact the FTP/S server administrator to determine which SITE commands are supported and/or required.

Server Type
Select Windows/Unix, AS400/IFS, AS400/Library, or MVS/IFS. Selecting AS400/IFS enables transactions with the Integrated File System (IFS) only. Selecting AS400/Library enables transactions with the AS/400 Library file system only.

SSL Server Certificate (FTPS only)
Select an SSL server certificate if you want to validate the certificate sent by an FTPS server when an FTPS session is initiated. This setting applies to FTPS(TLS/SSL) transport method only. If FTP or SFTP is selected, this field is disabled.

NOTE: Typically, you need to request the SSL server certificate from the FTPS server administrator. Then, you must import the certificate into Diplomat. Select Keys > SSL Server Certificates > Import SSL Certificate and browse to the file containing the SSL server certificate received from the FTPS server administrator.

NOTE: Diplomat MFT does **not** support SFTP (SSH2) for AS/400 or MVS systems. If you select SFTP (SSH2), *Server Type* is set to Windows/Unix and disabled.

Passive/Active
Since most FTP servers operate in passive mode, the default for this parameter is *Passive*. If the FTP server operates in active mode, select *Active* and review the active FTP settings under Settings > FTP from the top menu bar.

NOTE: FTPS (TLS/SSL) servers seldom operate in active mode, since firewalls are often not able to correctly route FTP traffic that has been encrypted via TLS/SSL.

NOTE: SFTP (SSH2) does not support the concept of active/passive mode. If you select SFTP (SSH2), *Passive* is selected and disabled.

Explicit/Implicit SSL (FTPS only)
Option when using FTPS (TLS/SSL) as the Transport Mode. When *Explicit SSL* selected for FTPS (TLS/SSL) transactions, Diplomat MFT uses the default FTP port, usually 21, and establishes the TLS/SSL link by issuing a command after establishing a

connection. When *Implicit SSL* is selected, Diplomat MFT begins a TLS/SSL connection as soon as it logs in to an FTP server. The FTP server must define a specific port for implicit SSL, usually port 990. Default is *Explicit SSL*.

CCC (Clear Command Channel) (FTPS only)
Check *Clear Command Channel* to encrypt sensitive information including your username and password then transmit other information such as port and IP information in plaintext. This setting applies to FTPS(TLS/SSL) transport method only.

File Integrity Checking
Choice of file integrity checking by file size 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.

Attempt to Create New Folders
Check *Attempt to Create New Folder*s if you are writing to an FTP, FTPS, or SFTP server and want Diplomat MFT to create a new folder or folders under the default directory. Uncheck this setting to prevent Diplomat MFT from attempting to create new folders.

Use Temp Filenames
A temporary filename is used while writing files to the destination. When the entire file has been written, the filename is changed to the destination filename.

NOTE: Temporary filenames can only be used with Cloud Connector, FTP, FTPS, SFTP, local network or SMB destinations. And, FTP, FTPS and SFTP servers must support the RENAME command. Temporary filenames are not supported on HTTP, HTTPS or email destinations.

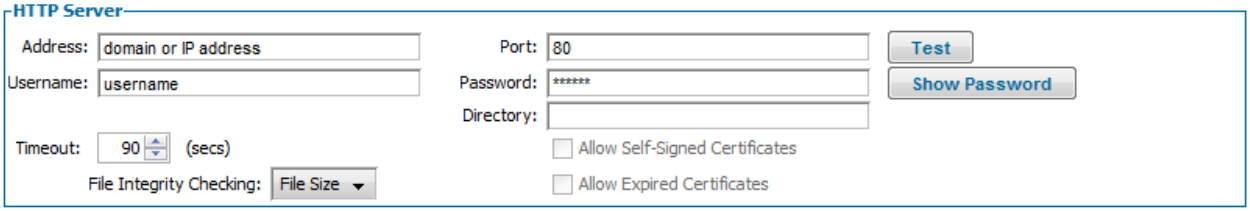
By default, the temporary filename is a random number. A prefix and/or suffix can be appended using the associated **Prefix** and **Suffix** settings.

Prefix
String to be added before the default temporary filename.

Suffix
String to be added after the default temporary filename.

Use Extended Algorithms
Defaults to checked. If you are having difficulty connecting to an FTP or FTPS server, be sure *Use Extended Algorithms* is checked to expand the number of algorithms attempted during the connection process.

8.4.4.4 HTTP/S Transport Method



NOTE: HTTP/S transport has a maximum file size of 2 GB.

Address
Address of the HTTP/S server where the destination file(s) are written.

Port
Specifies a port number as required by the HTTP/S server for the HTTP/S session. Contact the HTTP/S server administrator to obtain this information. Default for HTTP is 80. Default for HTTPS is 443.

Test Button
Use the **Test** button to attempt to access the directory on the system at the specified address using the specified port. For example, if *Address* is 'coviantsoftware.com', *Port* is '80' and *Directory* is 'test', Diplomat MFT issues a request for 'http://coviantsoftware.com:80/test'.

If the HTTP/S server requests authentication, Diplomat MFT provides the *Username* and *Password*. Typically, an HTTP/S server responds with a '401' code when authentication fails.

NOTE: The HTTP/S server controls whether authentication is required. Even if *Username* and *Password* are entered, the HTTP/S server may not request it. Thus, a successful connection and a '200' HTTP response code does not necessarily mean that a username and password were successfully authenticated.

NOTE: Diplomat MFT indicates when a connection fails because the HTTP/S server certificate is expired or not signed by a valid Certificate Authority. If you want to allow the connection to the HTTP/S server to proceed, check the *Allow Self-Signed Certificates* or *Allow Expired Certificates* checkbox, as needed.

Username
Name needed to authenticate access to the directory on the HTTP/S server where transaction file(s) are to be written.

Password

Password needed to authenticate access to the directory on the HTTP/S server where transaction file(s) are to be written. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

Directory
Sub-directory on the HTTP/S Server where destination file(s) are written. This sub-directory is appended to the root directory associated with the HTTP/S server. Contact the HTTP/S server administrator to obtain this information.

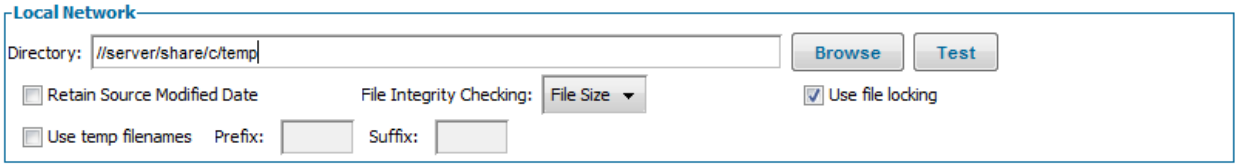
Timeout
Sets the length of time the Diplomat MFT Service waits for a response from the HTTP/S server.

File Integrity Checking
Choice of file integrity checking by file size 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.

Allow Self-Signed Certificates
Check *Allow Self-Signed Certificates* to allow a connection to an HTTPS server using an SSL certificate that is not signed by a valid Certificate Authority. Only enabled for HTTPS servers. Default is unchecked.

Allow Expired Certificates
Check *Allow Expired Certificates* to allow a connection to an HTTPS server using an SSL certificate that has expired. Only enabled for HTTPS servers. Default is unchecked.

8.4.4.5 Local Network Transport Method



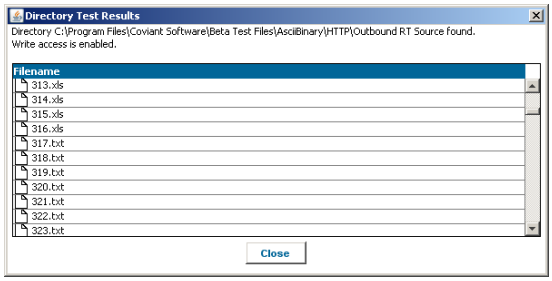
Directory

Directory on the local network where the destination file(s) are written. If the directory does not exist, Diplomat MFT attempts to create a directory as part of a file transfer job. If Diplomat MFT is successful in creating the directory, the job continues as if the directory had already existed. If needed, use the **Browse** button to select a directory.

Test Button

After entering the local network directory information, press **Test** to:

- Verify that the directory can be found
- Read and/or write access are enabled
- Display the contents of the directory



CAUTION: If you have trouble running a transaction in which you specified a UNC path or a mapped drive, the logon for the Diplomat MFT Service or diplomatServer daemon may not have the privileges to access the specified directory. Please use **Test** to confirm that the logon for the Diplomat MFT Service or diplomatServer daemon has the required privileges before contacting Coviant Software Support.

Retain Source Modified Date

Check *Retain Source Modified Date* to make the modified date of the destination file the same as the modified date of the source file.

File Integrity Checking

Choice of file integrity checking by file size 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.

Use File Locking

Check Use File Locking to attempt to lock the target file during processing.

Use Temp Filenames

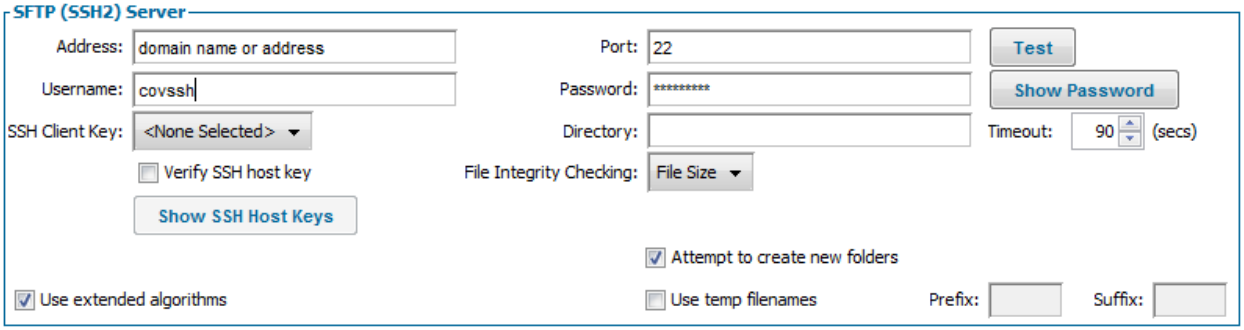
A temporary filename is used while writing files to the destination. When the entire file has been written, the filename is changed to the destination filename.

NOTE: Temporary filenames can only be used with Cloud Connector, FTP, FTPS, SFTP, local network or SMB destinations. And, FTP, FTPS and SFTP servers must support the RENAME command. Temporary filenames are not supported on HTTP, HTTPS or email destinations.

By default, the temporary filename is a random number. A prefix and/or suffix can be appended using the associated **Prefix** and **Suffix** settings.

Prefix/Suffix
String to be added before/after the default temporary filename.

8.4.4.6 SFTP Transport Method



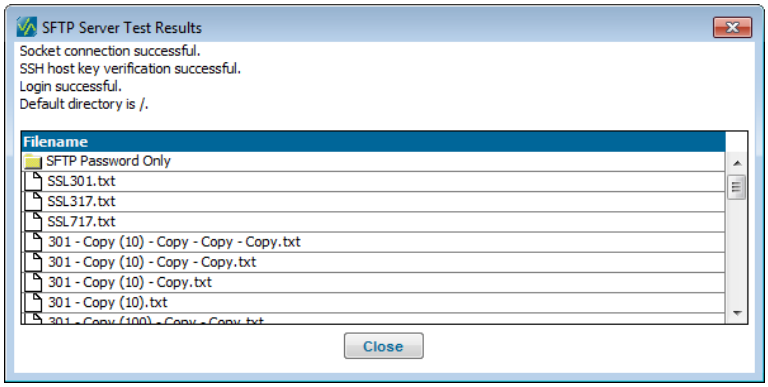
Address

Address of the SFTP server where the destination files are written.

Port

Specifies a port number as required by the SFTP server to be used for the SFTP session. Contact the SFTP server administrator to obtain this information.

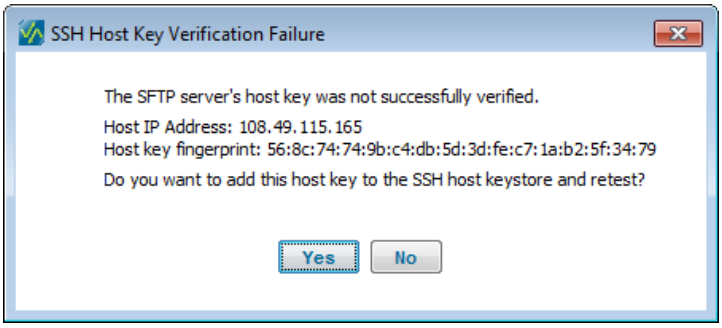
Test Button



After entering the SFTP server information, press **Test** to:

- Test the connection to the SFTP server.
- Check that an SSH host key has been verified.

  NOTE: If the SSH host key from the SFTP server is not in the Diplomat MFT database, then you are prompted to add the SSH host key and retest the connection.



- Determine whether the username, password and SSH client key are valid.
- Display the default directory and its contents.

Username
Name used to log in to the SFTP server. Logging in under a username defaults to a particular directory on the SFTP server.

Password
Password used to log in to the SFTP server. If you are using anonymous login, enter your email address or other identifier. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

SSH Client Key
SSH private key associated with an SFTP account login.

Verify SSH Host Key
Check *Verify SSH Host Key* to check that the SSH Host Key associated with the SFTP server matches an SSH Host Key in the list displayed by the *Show Host Key*s button.

Show Host Keys Button
Use the *Show Host Keys* button to display the list domains and fingerprints associated with the SFTP server. *Show Host Keys* button is disabled when Verify SSH host key is not checked.

Directory
Directory on the SFTP Server where transaction file(s) are found or written. When an SFTP session is initiated, a change directory command (CWD) is issued with this string as the argument. If the SFTP server is set up to automatically point to the directory required by this transaction, leave this field blank.

Timeout
Sets the length of time the Diplomat MFT Service waits for a response from the SFTP server.

File Integrity
Choice of file integrity checking by file size 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.

Attempt to Create New Folders
Check Attempt to Create New Folders if you are writing to an SFTP server and want Diplomat MFT to create a new folder or folders under the default directory. Uncheck this setting to prevent Diplomat MFT from attempting to create new folders.

Use Temp Filenames
A temporary filename is used while writing files to the destination. When the entire file has been written, the filename is changed to the destination filename.

NOTE: Temporary filenames can only be used with FTP, FTPS, SFTP, local network or SMB destinations. And, FTP, FTPS and SFTP servers must support the RENAME command. Temporary filenames are not supported on HTTP, HTTPS or email destinations.

By default, the temporary filename is a random number. A prefix and/or suffix can be appended using the associated **Prefix** and **Suffix** settings.

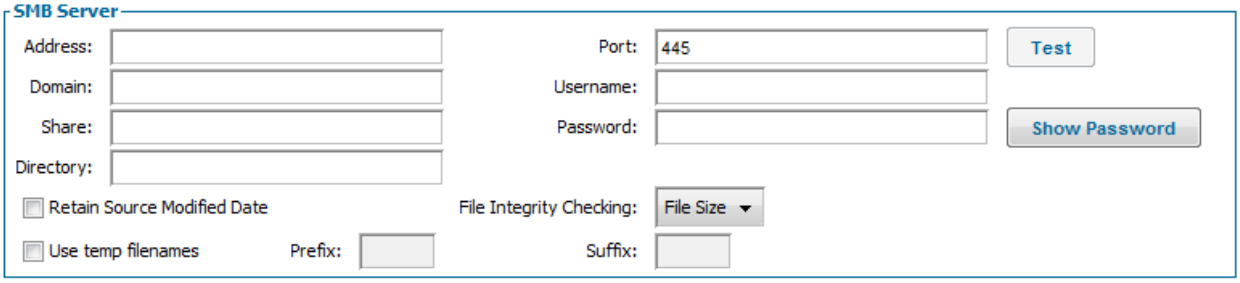
Prefix
String to be added before the default temporary filename.

Suffix
String to be added after the default temporary filename.

Use Extended Algorithms

Defaults to checked. If you are having difficulty connecting to an SFTP server, be sure *Use Extended Algorithms* is checked to expand the number of algorithms attempted during the connection process.

8.4.4.7 SMB Server Transport Method



Address

Address of the SMB (Server Message Block) server where the source file(s) are located.

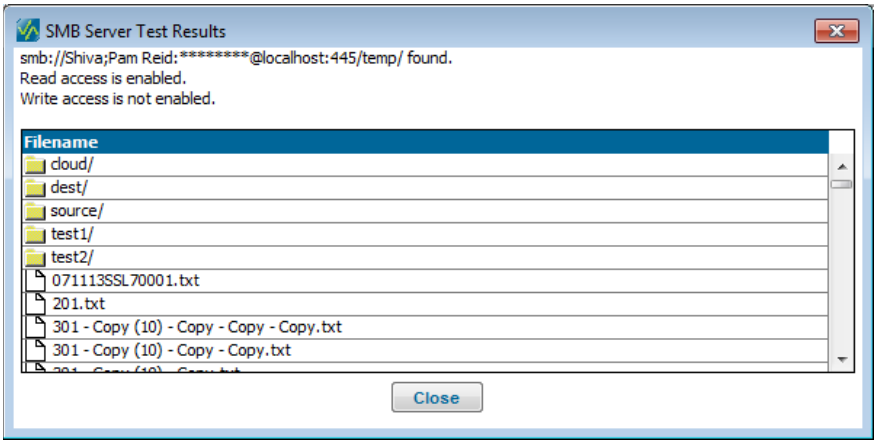
Port

Specifies a port number as required by the SMB server to be used for the SMB session. Contact the SMB server *Administrator* to obtain this information.

Test Button

After entering the SMB server information, press **Test** to:

- Test the connection to the SMB server
- Determine whether the username and password, if any, are valid
- Display the default directory and its contents



Domain

Name used to log in to the SMB server where transaction file(s) are to be found. Logging in under a username defaults to a particular directory on the SMB server

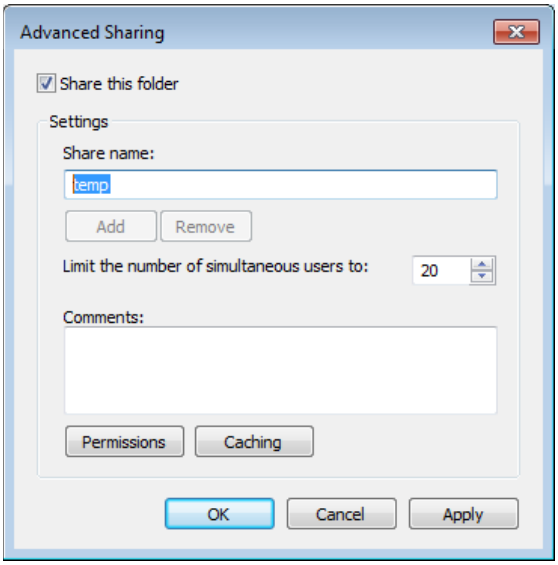
Username

Name used to log in to the SMB server where transaction file(s) are to be found. Logging in under a username defaults to a particular directory on the SMB server.

Password

Password used to log in to the SMB server. If you are using anonymous login, enter your email address or other identifier. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

Share
Directory on the SMB server that has been set up as a network share. On most Windows systems, network shares can be set up from Properties > Sharing > Advanced Sharing for the target directory.



If you do not know how to specify a network share, contact the system manager of the SMB server for assistance.

Directory
Sub-directory in the share on the SMB server where transaction file(s) are found.

Retain Source Modified Date
Check *Retain Source Modified Date* to make the modified date of the destination file the same as the modified date of the source file.

File Integrity Checking
Choice of file integrity checking by file size 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.

Use Temp Filenames
A temporary filename is used while writing files to the destination. When the entire file has been written, the filename is changed to the destination filename.

NOTE: Temporary filenames can only be used with Cloud Connector, FTP, FTPS, SFTP, local network or SMB destinations. FTP, FTPS and SFTP servers must support the RENAME command. Temporary filenames are not supported on HTTP, HTTPS or email destinations.

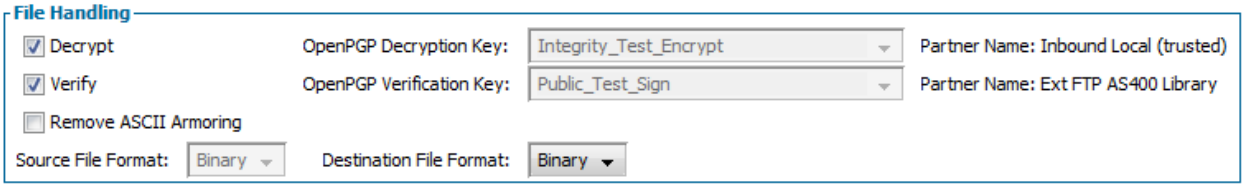
By default, the temporary filename is a random number. A prefix and/or suffix can be appended using the associated **Prefix** and **Suffix** settings.

Prefix
String to be added before the default temporary filename.

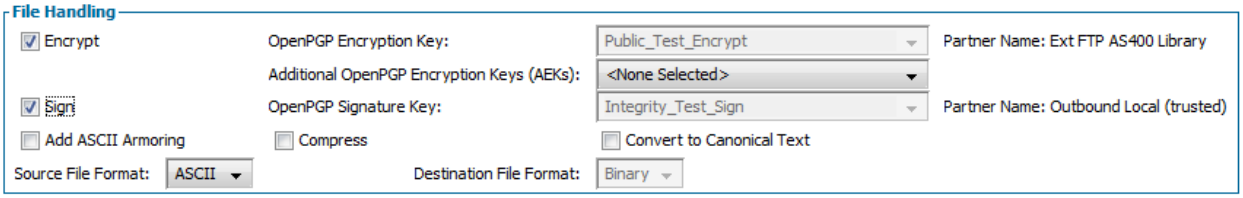
Suffix
String to be added after the default temporary filename.

8.4.5 File Handling

The information in the File Handling panel determines how a file is transformed during a file transfer job.



Inbound Transaction



Outbound Transaction

Encrypt/Decrypt
If *Encrypt* or *Decrypt* is **not** checked, the encryption or decryption step of the transaction is omitted and the *OpenPGP Encryption Key* or *OpenPGP Decryption Key* field is disabled. Default value is checked.

OpenPGP Encryption/Decryption Key
Either the public encryption key of the entity receiving the encrypted file or the key pair used to decrypt the file. Contact your trading partner to obtain their public key for encryption.

The drop-down menu displays only keys that have a currently valid encryption sub-key. For decryption, only key pairs are available for selection.

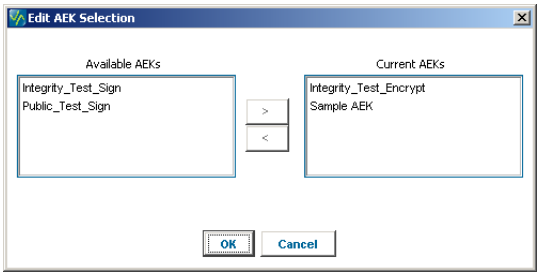
NOTE: If you selected a default decryption key in the Settings > OpenPGP Keys pop-up dialog box, the *OpenPGP Decryption Key* field for newly created inbound transactions is pre-filled with the default decryption key name. If you then select a saved partner profile in the destination partner profile panel, the *Encrypt/Decrypt Key* information from the profile overrides the default decryption key.

NOTE: If you select saved partner profiles in the *Source Partner Profile* or the *Destination Partner Profile* panels, the key information from the profiles overrides any key information and the key fields are disabled. The *Partner Name* of the saved partner profile is displayed to the right of the key information field. If you need to change the key information, go to the *Source Partner Profile* panel or the *Destination Partner Profile* panel and change the *Partner* field to '<NONE>'.

Additional OpenPGP Encryption Keys (AEKs)
Additional OpenPGP Encryption Keys (AEKs) are used when you want to encrypt files with more than one key. The additional keys could be your own key pair or the public key of an additional recipient.

If a *Default Additional Encryption Key* is specified on the OpenPGP Settings screen under Settings > OpenPGP Keys from the top menu bar, it is used to pre-fill the *Additional OpenPGP Encryption Key(s)* field in all new outbound transactions.

For example, most outbound files are encrypted with a public key from a trading partner. If you want to archive only encrypted files for security reasons, you would need to encrypt the files using your own key pair as an AEK that could always be used to decrypt all of the archived files.



AEKs are added to the list by selecting 'Edit AEKs…' from the *Additional Encryption Keys (AEKs)* drop-down, which displays the Edit AEK Selection screen. Highlight the key in the Available AEKs list that you would like to add to the Current AEKs list. Then, select the > button to move the selected key to the current list. You can reverse the process using the < button to remove keys from the current list.

NOTE: When one or more additional encryption keys are specified, the Diplomat MFT job fails if any one of the encryption keys has expired.

Sign/Verify

If *Sign* or *Verify* is **not** checked, the signature or verification step of a file transfer job is omitted and the *Signature* or the *Verification Key* field is disabled. Default value is checked.

OpenPGP Signature/Verification Key

Either your OpenPGP key pair to be used to sign the file or the OpenPGP public key that matches the key pair your trading partner used to sign the file.

The drop-down menu displays only OpenPGP keys that have a currently valid signing sub-key. For signature keys, only key pairs are available for selection.

NOTE: If you selected a default signature key in the Settings > OpenPGP Keys pop-up dialog box, the *OpenPGP Signature Key* field for newly created outbound transactions is pre-filled with the default signature key name. If you then select a saved partner profile in the source partner profile panel, the Sign/Verify key information from the profile overrides the default signature key.

NOTE: If you select saved partner profiles in the *Source Partner Profile* or the *Destination Partner Profile* panels, the key information from the profiles overrides any key information and the key fields are disabled. The *Partner Name* of the saved partner profile is displayed to the right of the key information field. If you need to change the key information, go to the *Source Partner Profile* panel or the *Destination Partner Profile* panel and change the *Partner* field to '<NONE>'.

Add/Remove ASCII Armoring

Adds/removes ASCII armoring during the encryption/decryption process. This format represents binary data using only printable ASCII characters and enables you to send encrypted files to or receive encrypted files from systems that do not support binary files.

NOTE: If an inbound transaction is set to *Remove ASCII Armoring* and an inbound file is **not** ASCII-armored, the file transfer job will fail. If an inbound transaction is **not** set to *Remove ASCII Armoring* and the file is ASCII-armored, the file transfer job will fail.

Compress

Compresses files as part of the encryption, signing, and/or ASCII-armoring process to reduce file size for transfer or storage. If a file is not being encrypted, signed, or ASCII-armored, the *Compress* field is disabled.

This field is available only for outbound transactions. On inbound transactions, files are automatically decompressed as part of the decryption and/or verification process.

Convert to Canonical Text

Converts an ASCII source file such that each line ends with a carriage return and linefeed before the file is encrypted, signed, or ASCII-armored.

This field is available only for outbound transactions.

Canonical text assists in ensuring that your file is readable by the system that receives it. You need to check *Canonical Text* when your expected files contain ASCII text, since ASCII text is represented differently on different systems. For example, on an MSDOS system, all lines of ASCII text are terminated with a carriage return followed by a linefeed. On a UNIX system, all lines end with just a linefeed. On a Macintosh, all lines end with just a carriage return. Canonical text has a carriage return and a linefeed at the end of each line of text and is readable by all systems.

Source/Destination File Format

Indicates ASCII or Binary as the format of the source files before they are picked up by Diplomat MFT and as the format of the destination files when they are dropped off by Diplomat.

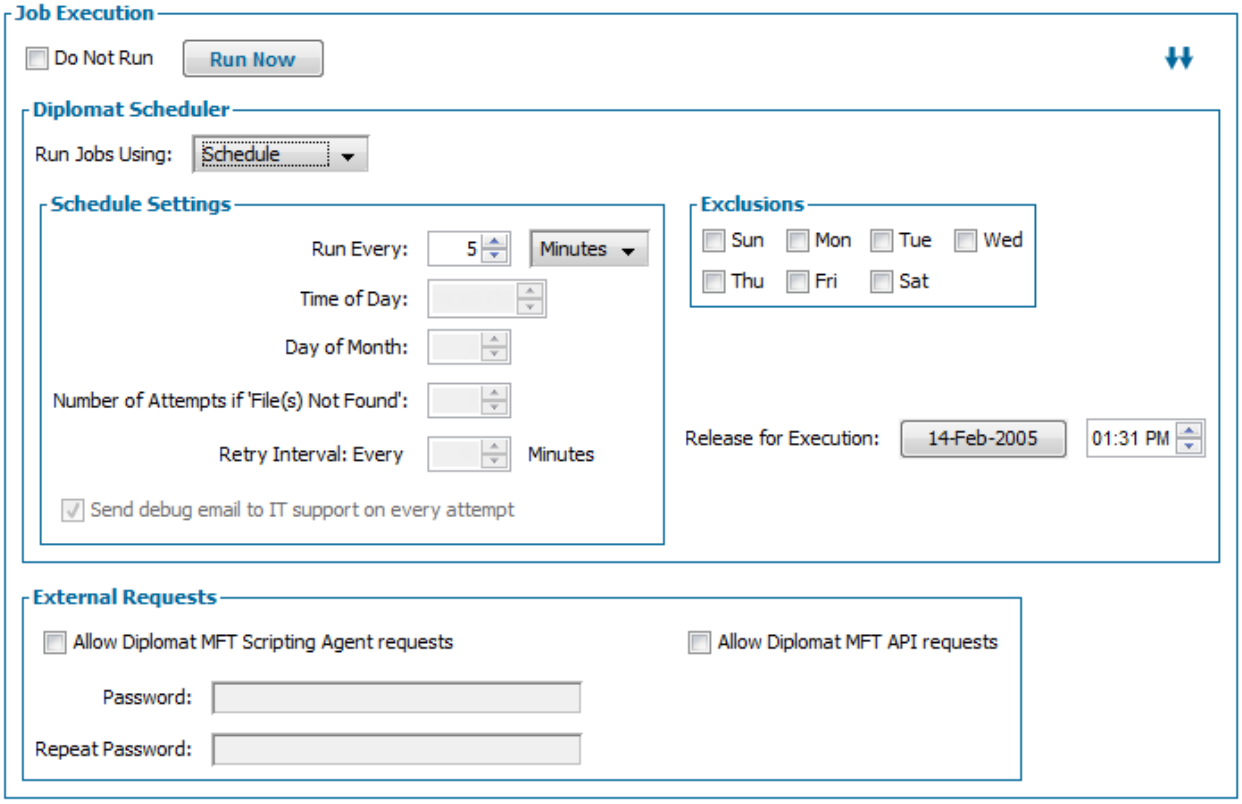
These fields default to Binary.

Diplomat MFT automatically updates the default values of the *Source* and *Destination File Format* fields based on other file handling parameters, as follows:

- If an inbound transaction is set to decrypt or verify files with no ASCII-armoring, source file format is always set to Binary.
- If an inbound transaction is set to remove ASCII-armoring, source file format is always set to ASCII.
- If an outbound transaction is set to encrypt or sign files with no ASCII-armoring, destination file format is always set to Binary.
- If an outbound transaction is set to add ASCII-armoring, destination file format is always set to ASCII.
- On all transactions where no file transformation is indicated, the source and destination file must always be the same format.

NOTE: Diplomat MFT uses the *Source* and *Destination File Format* fields to set FTP transfer type on file transfer jobs using FTP. If an ASCII file is transferred using FTP with a file format of 'Binary', the receiving system may not be able to read the file properly. If a Binary file is transferred with a file format of ASCII, the FTP server may automatically add carriage return or linefeed characters and corrupt the file.

8.4.6 Job Execution



The Job Execution parameters determine how frequently file transfer jobs will be 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.

Do Not Run

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.

NOTE: *Do Not Run* is always checked for newly created transactions.

Run Now Button

Run Now immediately executes a file transfer job using the current transaction information. 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.

NOTE: *Run Now* executes a job immediately – even if a transaction is suspended.

NOTE: *Run Now* is disabled when using a preview license.

8.4.6.1 Diplomat Scheduler

The *Diplomat Scheduler* panel contains the settings Diplomat uses to schedule file transfer jobs.

Run Jobs Using

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 initiate any jobs for the transaction.

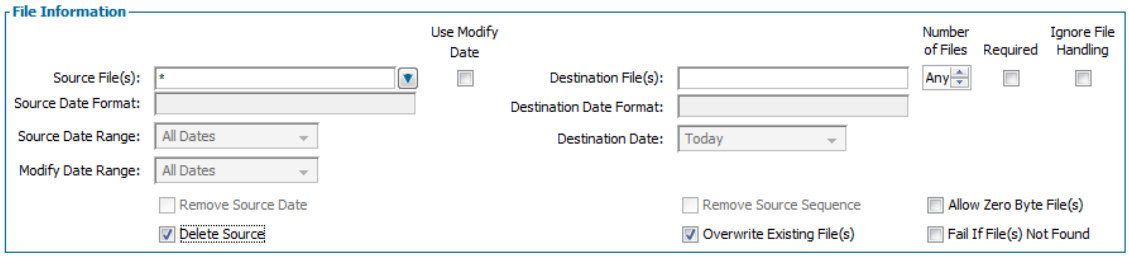
NOTE: If *File Monitoring* is selected, then only the *Exclusions* and *Release for Execution* settings in the *Diplomat Scheduler* panel are enabled.

File monitoring sets up a "watch folder" request for each folder specified in the File Information panel. For example, if multiple pairs of source and destination filename fields are shown in the File Information panel, the Diplomat MFT Service watches each of these folders for new files. When a new file is found, a file transfer job checks that all of the criteria in the File Information panel are met before processing files.

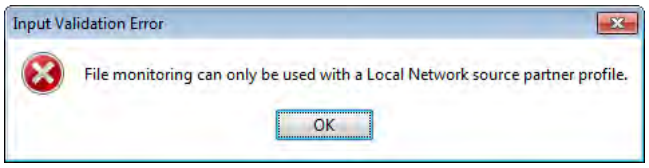
NOTE: *File Monitoring* only watches for newly created files. It does not watch for files that are modified or overwritten.

NOTE: *File Monitoring* can only be used when the source partner profile is a local network folder.

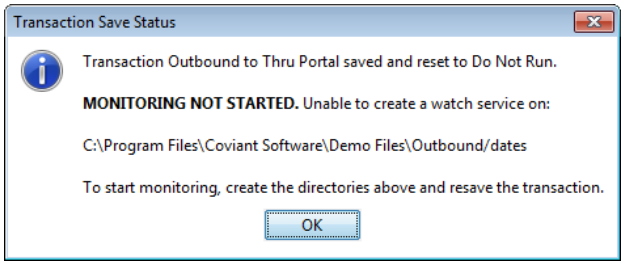
A typical example of a file monitoring job would pick up any newly created files in the source folder and delete the source files after they are processed. In this example, the File Information panel would have a wildcard'*' in the *Source File(s)* field, *Delete Source* would be checked and *Fail If File(s) Not Found* would be unchecked.



NOTE: File Monitoring can only be used with a Local Network source partner profile.



NOTE: The Diplomat MFT service cannot monitor folders that do not exist. When you save a Diplomat MFT transaction that is set to monitor a folder that does not exist, the transaction is saved and set to Do Not Run. To start monitoring, create the folders listed in the pop-up dialog and resave the transaction.



8.4.6.1.1 Schedule Settings

Schedule Settings are enabled only if *Run Jobs Using Schedule* is selected.

Run Every
Run Every settings define how frequently jobs are scheduled. You can specify:

- Every XX Minutes
- Every XX Hours
- Every XX Days
- Every XX Months

NOTE: The Diplomat MFT Service checks the system time every 5 minutes to determine whether the system clock differs from the expected time by more than 15 minutes. If so, the Diplomat MFT Service reschedules all file transfer jobs using the new system time.

NOTE: At a "spring forward" time when clocks lose the hour between 2am and 3am, daily and monthly jobs normally scheduled during that hour will run between 3am and 4am. At a "fall back" time change when clocks have two time periods between 1am and 2am, daily and monthly jobs will run once in the second hourly period.

Time of Day
Time of day to drop off or pick up the file(s) in the form hh:mm AM/PM.

Day of Month to Run
Select the number of the day of the month to run or select 'Last' for the last calendar day of each month.

Number of Attempts if File(s) Not Found
Total number of times that Diplomat MFT tries to complete a daily or monthly job when files are not found before declaring an error and rescheduling the job.

Retry Interval

Number of minutes Diplomat MFT waits before attempting to run the same file transfer job. Send Mail to IT Support on Every Attempt
Check if you want IT support email addresses to receive a FAILURE email message every time Diplomat MFT attempts to run a daily or monthly job.

NOTE: Checking *Send Mail to IT Support on Every Attempt* does not affect email to business users. Business users receive FAILURE emails only after all attempts have failed.

CAUTION: If the Diplomat MFT Service is not running or jobs are suspended at the time set for a daily or monthly file transfer, then the file transfer job is simply rescheduled when the Diplomat MFT Service is restarted or the job is released for scheduling. For example, if a file transfer job is scheduled monthly on the 1st of the month at 1:30PM and the Diplomat MFT Service was not running on the 1st at 1:30PM, then when the Diplomat MFT Service is restarted or jobs are released, the next file transfer job for this transaction would be scheduled at 1:30PM on the 1st of the following month.

8.4.6.1.2 Exclusions
File transfer jobs are not scheduled on days of the week that are checked.

NOTE: Jobs are scheduled at the time specified in *Time of Day* on the first day that is not excluded and every XX days or months afterwards. *Release for Execution* can be used to delay the first run until after a specified date and time. Jobs scheduled by the minute, hour or file monitoring are scheduled as soon as the Diplomat MFT Service starts or at 12:01AM on the first day that is not excluded.

8.4.6.1.3 Release for Execution

Sets the earliest date and time that Diplomat MFT allows a file transfer job for this transaction to be run by either the built-in scheduler or file monitoring.

NOTE: The exact date and time of first execution of the transaction is determined by the type of scheduler selected.

You might use this field to delay the release of a transaction into production. For example, you might have set up and tested a transaction such that it is ready for release into production. The file transfer job is scheduled to run every day, but you know that the production files will not be ready for another week. You can set this transaction to start running on the day that the production files are expected to show up – which would prevent FAILURE email from being sent each time a job runs until the files show up.

8.4.6.2 External Requests

The Diplomat MFT Scripting Agent and API can be used to initiate Diplomat MFT file transfer jobs.

NOTE: Transactions can be set to allow the Diplomat MFT Scripting Agent and/or API to initiate file transfer jobs in addition to either the built-in scheduler or file monitoring.

Allow Diplomat MFT Scripting Agent requests

Check *Allow Diplomat MFT Scripting Agent requests*, if you plan to initiate file transfer jobs using the Diplomat MFT Scripting Agent. Refer to the *Diplomat MFT Scripting Agent User Guide* for more information.

If you want to ONLY allow Diplomat MFT Scripting Agent requests, then set *Run Jobs Using* in the Job Execution panel to <NONE>.

NOTE: When upgrading from Diplomat MFT v6.1.x or earlier, transactions set to *Use 3rd Party Scheduler* are converted to *Allow Diplomat MFT Scripting Agent requests*.

Password/Repeat Password

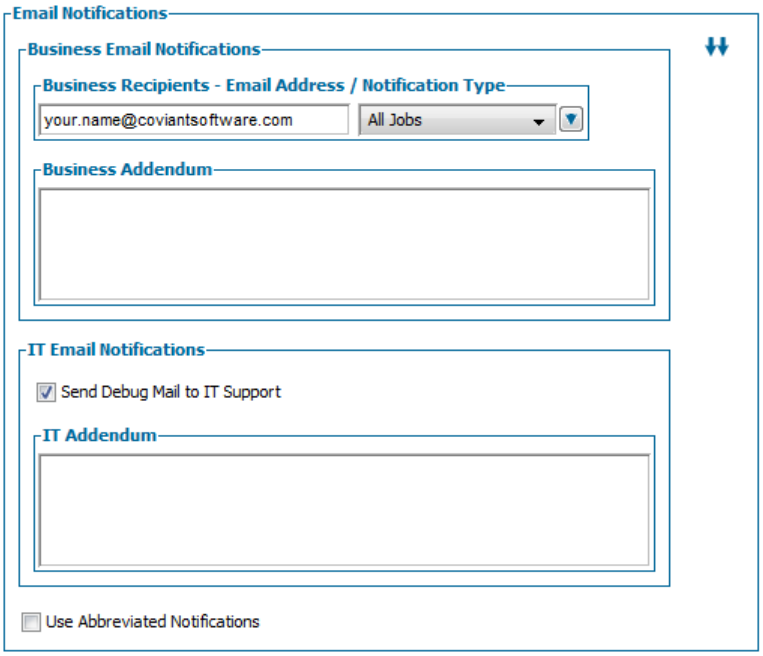
Password entered as an argument when executing a Diplomat MFT job using the Diplomat MFT Scripting Agent. If a password is entered in the Job Execution panel, it will be required when a Diplomat MFT Scripting Agent job is executed. Refer to the *Diplomat MFT Scripting Agent User Guide* for more information.

Allow Diplomat MFT API requests

Check *Allow Diplomat MFT API requests*, if you plan to initiate or monitor jobs using the Diplomat MFT API. Refer to the *Diplomat MFT REST API User Guide* for more information.

If you want to ONLY allow Diplomat MFT API requests, then set *Run Jobs Using* in the Job Execution panel to <NONE>.

8.4.7 Email Notifications



Business Email Notifications

Email Address

Email address(es) to receive automatic email notifications. Enter as many email addresses as desired for each transaction. Use the drop-down arrow on the right-hand side of the *Email Address* field to add or delete additional email address fields. Enter unique email addresses into each *Email Address* field. Notifications to business email addresses contain a summary of the major steps in the file transfer job.

NOTE: When total email size exceeds the Max Email Size under Settings > Email Settings, email is truncated and the complete job log is written to a file referenced in the email message in the /troubleshooting directory.

NOTE: Sample email messages are provided in *Appendix C: Sample Email Messages*.

Notification Type

Determines when an email message is sent to the associated email address. Choose any combination of the following from the drop down menu:

- Success — Email sent if job is successful
- Warning — Email sent if job is successful, but generated at least one error that might have affected the integrity of the file(s) being transferred
- Failure — Email sent if job fails for any reason
- All jobs — Email sent for all jobs

Business Addendum

Text added to email notifications to business recipients. Text entered here is appended to the end of email notifications for all email sent to business recipient email addresses.

IT Email Notifications

Send Debug Email to IT Support

When checked, an email message with debug information included is sent to all addresses listed on the Settings > IT Support Email Notification screen. The default for newly created transactions is checked.

IT Addendum

Text added to email notifications to IT support recipients. Text entered here is appended to the end of email notifications for all email sent to IT support recipient email addresses on the Settings > IT Support Email Notification screen.

NOTE: The level of detailed debug information included in IT Support Email is independent of the settings for the *Minimum Logging Level* in the Settings > Logging screen.

NOTE: If you check *Send Debug Email to IT Support*, but have not set up at least one email address under Settings > IT Support Email Notification, you will be reminded that no IT email addresses are defined when you attempt to save the transaction.

Use Abbreviated Notifications

When Use Abbreviated Notifications is checked, lists in business user email, IT support email, summary messages in Run Now windows and summary messages in log files are truncated to 100 entries. Lists include source filenames, destination filenames, primary archive filenames, additional archive filenames, destination errors, archive errors and other non-fatal errors.

NOTE: Only check Use Abbreviated Notifications for jobs that regularly process very large numbers of files, where list lengths may cause a memory overflow.

8.4.8 Additional Archive

Archive files are copies of the files that are transferred by a Diplomat MFT file transfer job. Diplomat MFT allows you to write copies of files for all jobs to a primary archive location and files for each specific transaction to an additional location.

For example, you may want to retain primary archive file copies in a central location, which is regularly backed up to a permanent location and is accessible to the IT group that manages file transfers. Business users may also need a copy of transferred files. You could specify an additional location accessible by the business users that are sending or receiving the files.

NOTE: It is strongly recommended that users who want to create centralized, self-managing archives of transaction files, use Settings > Primary Archive to set the primary archive location and related parameters.

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.

Individual archive files have names in the form 'source_filename.srce.year + month + day . hour + minutes + seconds.milliseconds.da' or 'destination_filename.dest.year + month + day . hour + minutes + seconds.milliseconds.da'. For example, an archive of the source version of the file 'TEST.txt' created on January 4, 2004 at 3:17:53:8769 p.m. would be named 'TEST.txt.srce.20040104.151753.8769.da'.

NOTE: All individual Diplomat MFT archive files have the file extension '.da' for easy lookup.

Zipped archive files have names in the form 'DiplomatArchive.TransactionName.year + month + day . hour + minutes + seconds.milliseconds.zip'. For example, a zipped archive file for transaction 'Test' created on January 4, 2004 at 3:17:53:8769 p.m. would be named 'DiplomatArchive.Test.20040104.151753.8769.zip'.

Additional Location

A second location, in addition to the primary archive location, where archive files for this transaction are written. Use **Browse** to select a directory. Use **Test** to determine whether the location is accessible and is read/write enabled for the logon identity used by the Diplomat MFT Service.

Add transaction-specific sub-directories

If *Add Transaction-specific Sub-directories* is checked, all archive files for each job are written to a sub-directory with the same name as the *Transaction Name* from the directory shown in the *Additional Archive Location* field.

Zip Archive Files

Check *Zip Archive Files* to zip all additional archive files generated by the job into a single zip file. *Zip Archive Files* is checked by default.

NOTE: 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.

File Types

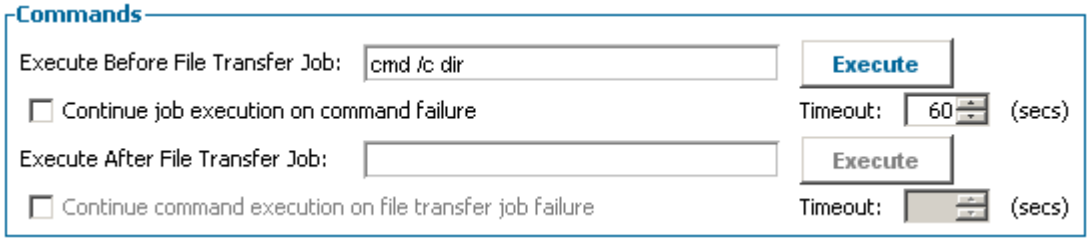
Select whether source, destination, or both types of files are to be archived.

Attempt Archive On

Determines when files are archived. Default value is 'Success and Warning'. Choose any combination of the following from the drop down menu:

- Success — Archive files if job is successful
- Warning — Archive files if job is successful, but generated at least one error that might have affected the integrity of the file(s) being transferred
- Failure — Archive files if job fails for any reason
- All jobs — Archive files for all jobs

8.4.9 Commands



The *Commands* panel allows you to specify commands that execute either before or after a file transfer job. These commands can be used to integrate the file transfer job into another job scheduling process. For example, assume you receive time and attendance files from 20 branch offices and a Diplomat MFT file transfer job checks every 30 minutes for incoming files. When files arrive and are decrypted, you could use the *Execute After File Transfer Job* field to start a payroll application to process the time and attendance files.

The command fields can be used to run any executable, such as DOS commands, batch files, or Unix shell scripts. DOS commands must always begin with 'cmd /c' followed by the command in the same form as you would enter at the 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.

The *Execute* buttons issue the command as entered, so you can confirm that the command works correctly before running production jobs.

NOTE: The complete pathname must be used for any file referenced in the command field, e.g., '\\domain_name\C\Program Files\Coviant Software\Diplomat-j\test.bat'.

Execute Before File Transfer Job

This command is executed before any steps in the file transfer job begin. If the command fails, the Diplomat MFT job fails. No further steps in the job are executed. Failure email and paging messages are generated. To override this default, check *Continue Job Execution on Command Failure*. **NOTE:** This command is executed each time a job is executed. If you have a job that is set to execute every 5 minutes, this command will execute every 5 minutes – whether or not files are ready to be processed.

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.

Pre-command Timeout

Time in seconds that Diplomat MFT waits for a reply from the pre-command process. If a pre-command process does not reply within the timeout period, the Diplomat MFT job has a Failure status and Diplomat MFT terminates the pre-command process. Return code shown in Diplomat MFT log and email messages is -1. Default is 60 seconds.

Continue Job Execution on Command Failure

Continue Job Execution on Command Failure overrides the default setting and allows the file transfer job to proceed when the initial command fails.

Execute After File Transfer Job

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 *Continue Command Execution on File Transfer Job Failure*.

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.

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

NOTE: If you select the *Execute* button when parameters are used in the post-command, only the <TRANS_ID> parameter will be resolved successfully and most likely an error will be shown in the Command Result pop-up window.

Continue Command Execution on File Transfer Job Failure

Continue Command Execution on File Transfer Job Failure overrides the default setting and ensures that the command is executed both for successful jobs and jobs that failed one or more steps during the file transfer.

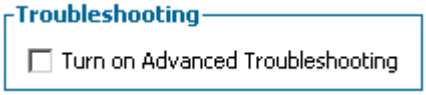
NOTE: Multi-file jobs may fail because only one or a subset of files had a problem or because a system problem was encountered, e.g., the audit database was unavailable. If you check *Continue Command Execution on File Transfer Job Failure,* no files or only a subset of the intended files may be available for further processing.

NOTE: When *Fail if File Not Found* is **not** checked on a transaction and a job does not find any files, the command in the *Execute After File Transfer Job* field is NEVER executed. Even if *Continue Command Execution on File Transfer Job Failure* is selected, these jobs are not classified as successes or failures by Diplomat MFT and are simply rescheduled.

Post-command Timeout

Time in seconds that Diplomat MFT waits for a reply from the post-command process. If a post-command process does not reply within the timeout period, the Diplomat MFT job has a Failure status and Diplomat MFT terminates the post-command process. Return code shown in Diplomat MFT log and email messages is -1. Default is 60 seconds.

8.4.10 Troubleshooting



Check *Turn on Advanced Troubleshooting* to create additional debug files and prevent deletion of temporary files created during the execution of a transaction. Advanced Troubleshooting captures both FTP debug 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.

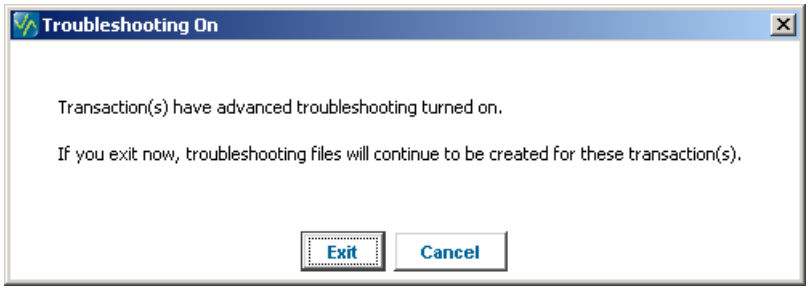
NOTE: FTP debug files may contain sensitive information such as user names and passwords that are passed in plaintext to an FTP server.

NOTE: All references to filenames in FTP debug files use the filename as it exists on the FTP server. When FTP, FTPS, or SFTP are specified in the *Destination Partner Profile* panel, each filename is the destination filename. When FTP, FTPS, or SFTP are specified in the *Source Partner Profile* panel, each filename is the source filename.

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'.

NOTE: *Turn on Advanced Troubleshooting* is unchecked by default. 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.

If *Turn on Advanced Troubleshooting* is checked on any transactions, you will be reminded when you exit the Diplomat MFT Client. To turn off troubleshooting, select **Cancel** and uncheck *Turn on Advanced Troubleshooting*.



NOTE: Troubleshooting files are only created if temporary files are created (e.g., during encryption, decryption, signing, or verification) or the source or destination is FTP, FTPS, SFTP, email, or HTTP/S. If temporary files are not created and files are transferred using only Local Network as the source and destination, no troubleshooting files are captured.

8.4.11 Validate/Save/Reset Buttons

The **Validate**, **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 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. The **Reset** button redisplays the previously-saved version of the transaction data.

9 Settings Menu

9.1 Settings Overview

NOTE: *Settings* are only available to accounts *Administrator* privileges.

The Settings menu items allow you to configure system-wide settings (e.g., email server information, primary archive information, audit database information, and log file location) and to set defaults for some data fields on newly-created transactions (e.g., default keys). Settings apply to all transactions. For example, all emails are sent using the email server information entered under Settings > Email.

9.2 Settings Menu Items

NOTE: Settings are only available to accounts with *Administrator* privileges.

Settings allow you to configure settings that apply to all transactions.

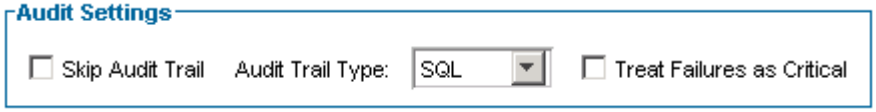
- Audit settings allow you to determine whether you want an audit database to be created and, if so, whether it is Built-in or SQL.
- Backup settings determine the default backup directory, whether or not backup files are encrypted, whether or not Diplomat MFT prompts for a backup to be created each time a user exits the Diplomat MFT Client, and whether automatic daily backups are enabled.
- Email settings allow you to set up the email server used to send email notifications on the status of each job.
- FTP settings enable configuration of IP address and ports to be used for active FTP file transfers.
- IT Support Email Notification settings allow you to identify the email addresses that you would like to receive email notifications of the status of all jobs.
- Job Monitor settings control the number of job history records available for display by the Diplomat MFT Job Monitor.
- Job Queue settings affect the scheduling execution of Diplomat file transfer jobs.
- Logging settings allow you to set the directory where log files are written, the minimum logging level, how often to create log files, and when to archive and delete old log files.
- OpenPGP Key settings are the default decryption, signing and additional encryption keys for new transactions.
- Paging Notification settings allow you to set up email or file-based pages to be sent when warnings, errors, or critical errors occur.
- Primary Archive settings allow you to archive files for every file transfer job.
- Session Management settings determine session expiration time for the Diplomat MFT Client.
- User Accounts settings allow a Diplomat MFT administrator with the Diplomat MFT password to create and manage a list of user identities that can access the Diplomat MFT Client without entering a separate password and set the system-wide minimum password update frequency.

9.2.1 Audit

NOTE: *Audit* settings are only available to accounts with *Administrator* privileges.

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

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



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

Skip Audit Trail

Check *Skip Audit Trail*, if you do not want audit records to be written. By default, *Skip Audit Trail* is checked and no audit trail records are written. If you uncheck *Skip Audit Trail,* an audit trail record is written for every job that is not automatically rescheduled due to File(s) Not Found (i.e., with a status of 'Success', 'Failure', or 'Warning', 'Error', or 'Critical Error').

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

Audit Trail Type

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

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

NOTE: When a SQL audit database is selected but the database is not currently accessible, any action by the Diplomat MFT Client that attempts to write a record to the USER_ACTIVITY table displays an error message to the user and generates an error message in the Diplomat MFT log.

Treat Failures as Critical

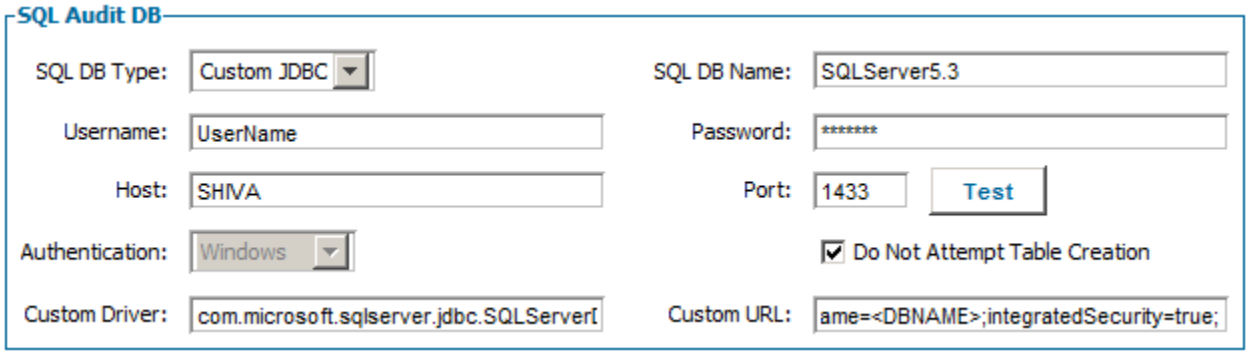
Select *Treat Failure as Critical* to **SUSPEND ALL JOBS** when an audit trail problem occurs. Only select *Treat Failure as Critical* if an audit record is required for every file transfer job.

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

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

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

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



SQL Audit DB

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

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

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

When setting up your SQL database, you must decide whether Diplomat MFT will be allowed to truncate data being written to character fields that are shorter than the string to be written. If Diplomat MFT does truncate data, a warning message and the complete string are written to the log file. **NOTE:** This setting is **not** a Diplomat MFT setting, but must be made in the SQL database set-up.

SQL DB Type

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

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

SQL DB Name

Name of SQL database used to capture audit records.

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

Username

If required, enter the username needed to access the SQL audit database. **NOTE:** *Username* and *Password* fields are disabled when Windows Authentication is selected. The logon account specified in the Diplomat MFT Service is used for Windows authentication. For detailed instructions on how to update the Diplomat MFT Service, see http://coviantsoftware.com/setting-windows-login.php.

Password

If required, enter the password needed to access the SQL audit database. **NOTE:** *Username* and *Password* fields are disabled when Windows Authentication is selected. The logon account specified in the Diplomat MFT Service is used for Windows authentication. For detailed instructions on how to update the Diplomat MFT Service, see http://coviantsoftware.com/setting-windows-login.php.

Host

Host name or IP address of the system where the SQL database is located. **NOTE:** A logon account on the Diplomat MFT Service must be specified when accessing SQL Server on a remote system. For detailed instructions on how to update the Diplomat MFT Service, see http://coviantsoftware.com/setting-windows-login.php.

Port

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

Test Button

After entering the host and port information, press **Test** to test the connection to the SQL database. **NOTE:** The test button only tests that the specified port is open on the host systems. It does **not** test the username and password for login to the database.

Authentication

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

Do Not Attempt Table Creation

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

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

Custom Driver

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

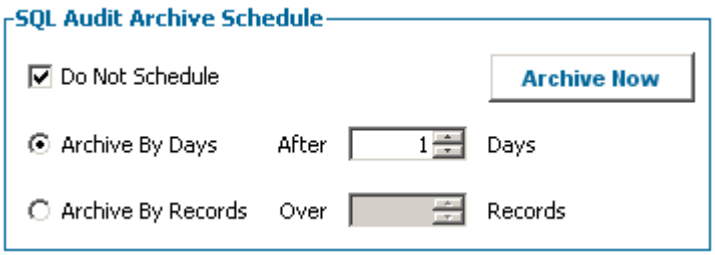
Enter the JDBC driver class name in the JDBC jar (e.g., com.microsoft.sqlserver.jdbc.SQLServerDriver) in the *Custom Driver* field. Refer to the documentation from your SQL database vendor for more information.

Custom URL

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

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

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



SQL Audit Archive Schedule

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

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

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

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

Do Not Schedule

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

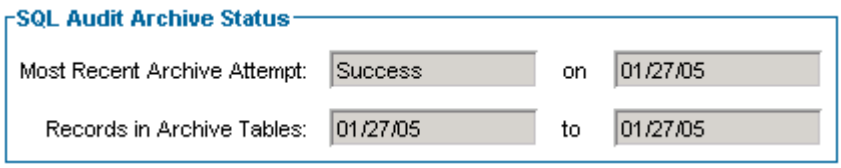
Archive Now Button

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

Archive by Days or Archive by Records

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

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



SQL Audit Archive Status

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

Most Recent Archive Attempt

Date of the most recent attempt to transfer records to the archive tables in the SQL audit database and indicates whether the transfer was successful.

Records in Archive Tables

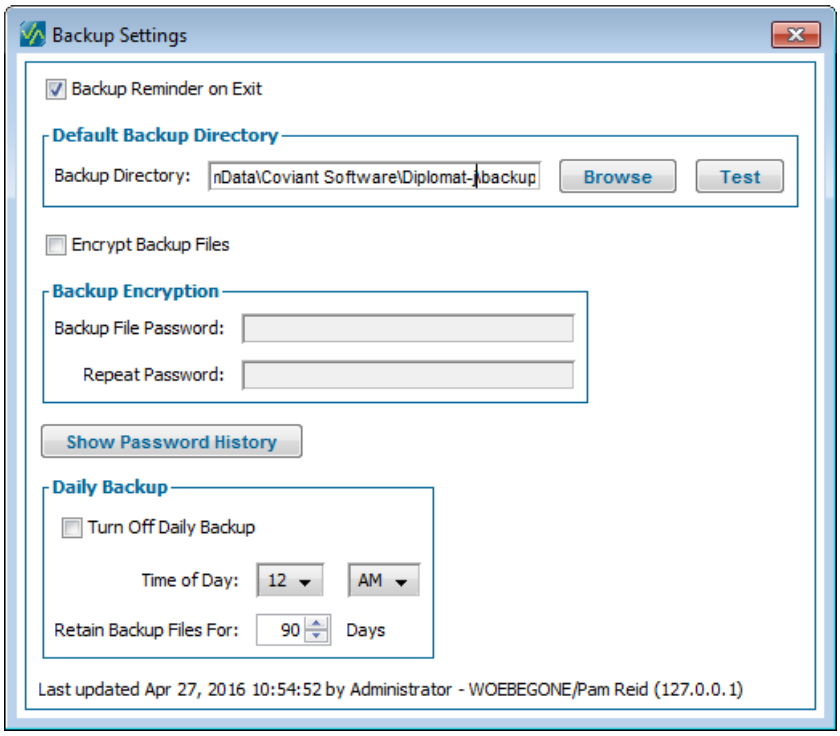
Range of creation dates for records in the archive tables in the SQL audit database. If no records are found in the archive tables, then 'No Records Archived' is displayed.

Audit Database Notices Button

Displays table with scheduled updates to SQL database fields. This table includes any fields scheduled for deletion. Fields scheduled for deletion in a subsequent release are typically no longer written in the current release.

9.2.2 Backup

NOTE: *Backup* settings are only available to accounts with *Administrator* privileges.



Backup settings determine the default backup directory, whether or not backup files are encrypted, whether or not Diplomat MFT prompts for a backup to be created each time the user exits the Diplomat MFT Client, and whether automatic daily backups are enabled

Backup Reminder on Exit

Check ***Backup Reminder on Exit***, if you want to be reminded to backup the Diplomat MFT databases when you exit the Diplomat MFT Client. ***Backup Reminder on Exit*** is checked by default. By backing up the databases each time you exit, you ensure the ability to 'roll-back' to earlier versions.

Default Backup Directory

Backup Directory

For Windows systems, the default backup location is C:\ProgramData\Coviant Software\Diplomat-j\backup. For Linux systems, the default directory is /opt/coviant/diplomat-j/backup. Use **Browse** to select a different directory. Use **Test** to determine whether the location is accessible and is read/write enabled for the logon identity used by the Diplomat MFT Service.

Encrypt Backup Files

Check ***Encrypt Backup Files***, if you want to encrypt every backup file when it is created. By default, ***Encrypt Backup Files*** is not checked and backup files are not encrypted.

Note: If you choose to encrypt backup files, the time to create a backup file and the size of the backup file increase.

Backup Encryption

If a backup file is encrypted, the backup file password is required to merge or restore the backup file.

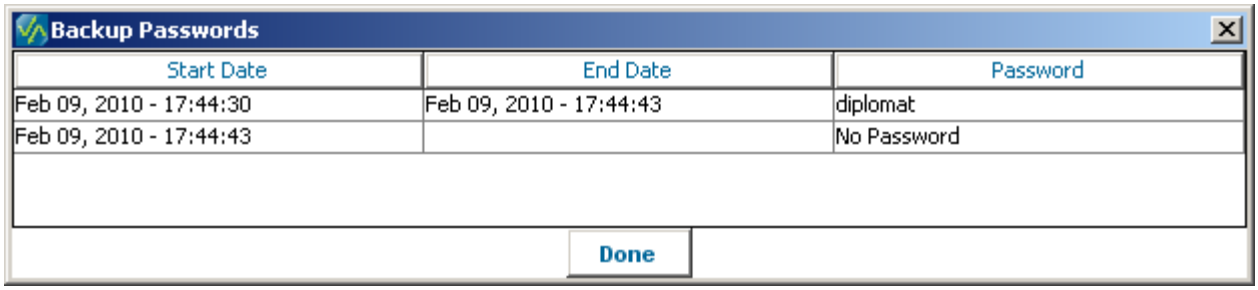
Backup File Password/Repeat Password

You must enter your backup file password twice to confirm your backup encryption password.

NOTE: Backup passwords are case sensitive.

Show Password History

Password history shows each backup password used and its associated start and end dates. Backup files created during the period between the start and end dates require entry of the associated password to merger or restore.



NOTE: *Show Password History* is displayed only when *Encrypt Backup Files* has been used to specify at least one password.

Daily Backup

Turn Off Daily Backup

Check *Turn Off Daily Backup* if you do not want backup files created automatically every day. By default, *Turn Off Daily Backup* is NOT checked and daily backup files are automatically created and deleted after 90 days.

Time of Day

Time of day that new daily backup files are created and older backup files are deleted. Default is midnight.

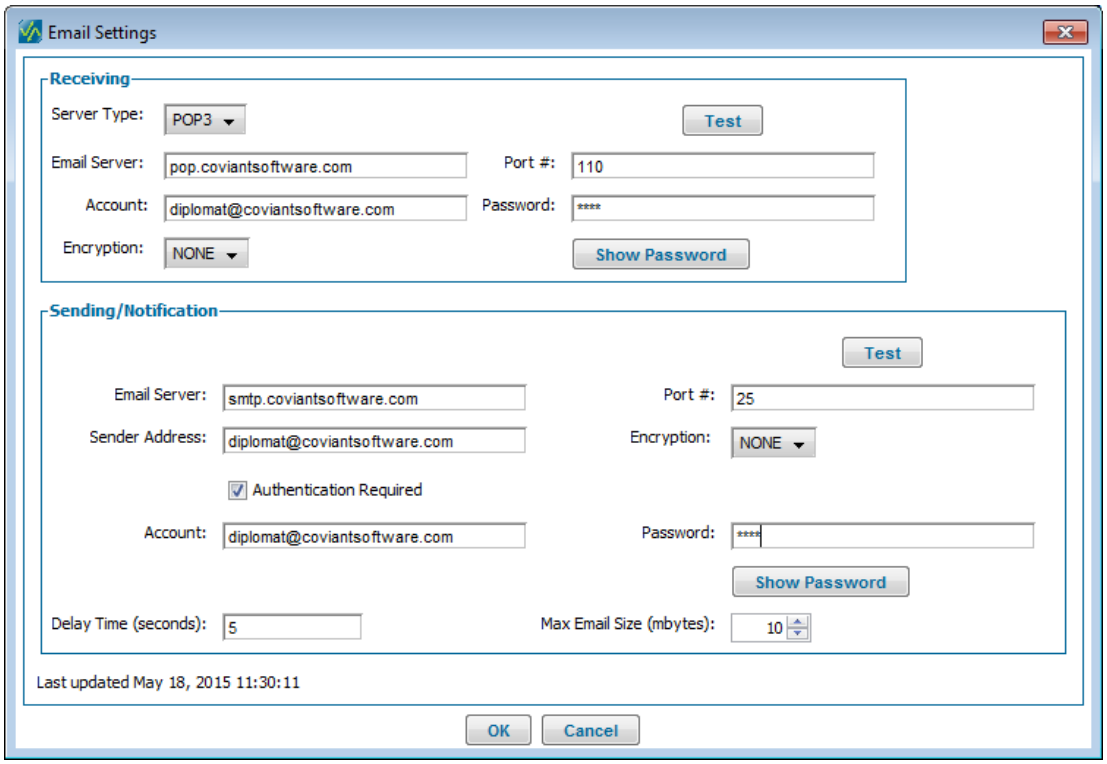
Retain Backup File for XX Days

Number of days backup files are retained. Default is 90 days.

NOTE: All files ending in .dbu in the current default backup directory with a last modified date older than XX days are deleted each day. To permanently retain a backup file, you must manually move a copy of the file to a location other than the default backup directory.

9.2.3 Email

NOTE: *Email* settings are only available to accounts with *Administrator* privileges.



The Email Settings screen identifies the email server to be used when sending email notifications to business users and IT support and the email server(s) to be used when Email is specified as a *Transport Method* in a source or destination partner profile. Sample email notification messages are provided in *Appendix C: Sample Email Messages*.

Receiving Server

Receiving Server settings are used to pick up files that specify Email as the *Transport Method* in the source partner profile.

Server Type

Select POP3 or IMAP as the type of mail server. Default is POP3.

Email Server

IP address or DNS name of the mail server.

Port #

Port used to connect to the mail server. Default is 110.

Account

Required by mail server to send an email message as part of the authentication process.

Password

Required by mail server to send an email message as part of the authentication process. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

Encryption

Select None, SSL, or TLS for level of encryption to use during authentication and transmission.

Test Button

After entering the mail server address and port number, press **Test** to test the connection to the receiving server and attempt to authenticate using the account and password.

Sending/Notification Server

Sending/Notification Server settings are used to send email notifications and to send files that specify Email as the *Transport Method* in the destination partner profile.

Email Server

IP address or DNS name of the mail server.

Port #

Port used to connect to the mail server. Default is 25.

Sender Address

Email address that appears in the FROM field on all email messages sent by Diplomat, which are also used by most email applications to generate the return mail address. **NOTE:** It is recommended that you set up a unique email username for use by Diplomat, so recipients can easily recognize email from your Diplomat MFT application. Consult your mail server administrator for assistance.

Encryption

Select None, SSL, or TLS for level of encryption to use during authentication and transmission.

Authentication Required

Indicates whether to use 'None' or 'Login' as the authentication on the mail server.

Account

Required by mail server to send an email message as part of the authentication process.

Password

Required by mail server to send an email message as part of the authentication process. Accounts with *Administrator* privileges can select the *Show Password* button to display the password.

Delay Time

Number of seconds Diplomat MFT waits between sending email messages.

NOTE: To prevent customers from sending spam, most public ISPs block emails when a large number of emails with the same sender or recipient are sent within a short period of time. If you use a public ISP for your mail server and expect to process several file transfers concurrently, you may need to increase the delay time to 20 seconds or more to prevent emails being blocked by your ISP.

Max Email Size (mbytes)

Maximum size of email message supported by *Sending Email Server*. Total size of email message, including attachments, must be less than the *Max Email Size*.

NOTE: Even if an email message is less than the maximum size supported on the Sending Email Server, delivery may fail if the email message is larger than the maximum supported on the email server receiving the message.

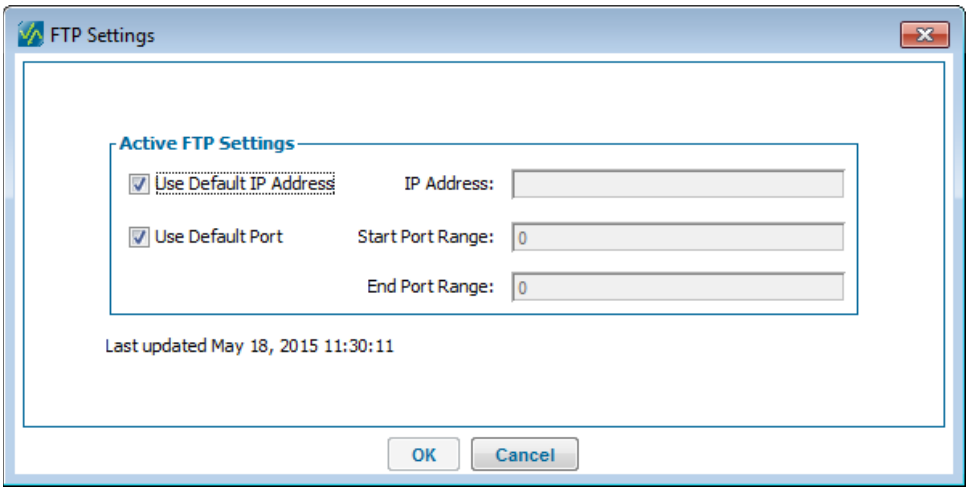
NOTE: If an email message is close to the *Max Email Size* limit, a non-fatal error is included in the Diplomat MFT log and email notifications about the job.

Test Button

After entering the server address and port number, press **Test** to test the connection to the sending server. If *Authentication Required* is checked, Diplomat MFT attempts to authenticate using the account and password.

9.2.4 FTP

NOTE: *FTP* settings are only available to accounts with *Administrator* privileges.



Active FTP Settings

Active FTP settings are needed when the FTP server operates in active mode. Typically, FTP servers operate in passive mode. In active mode, the FTP server attempts to connect to an IP address and port specified by the Diplomat MFT Service. Since a Diplomat MFT site is typically installed inside a firewall, the FTP server is often blocked from making a direct connection to the site by firewall software. In this case, the FTP server needs to be given an externally visible IP address and port number. Then, the port on the externally visible system needs to be forwarded to the Diplomat MFT site's IP address and the correct port.

NOTE: Some routers are pre-configured to use port 20 for explicit SSL data connections and port 989 for implicit SSL data connections. If so, these ports need to be opened and forwarded to the Diplomat MFT site.

Use Default IP Address
Check *Use Default IP Address* if the IP address for the Diplomat MFT site is externally visible.

IP Address
Enter the IP address that the FTP server connects to at run-time.

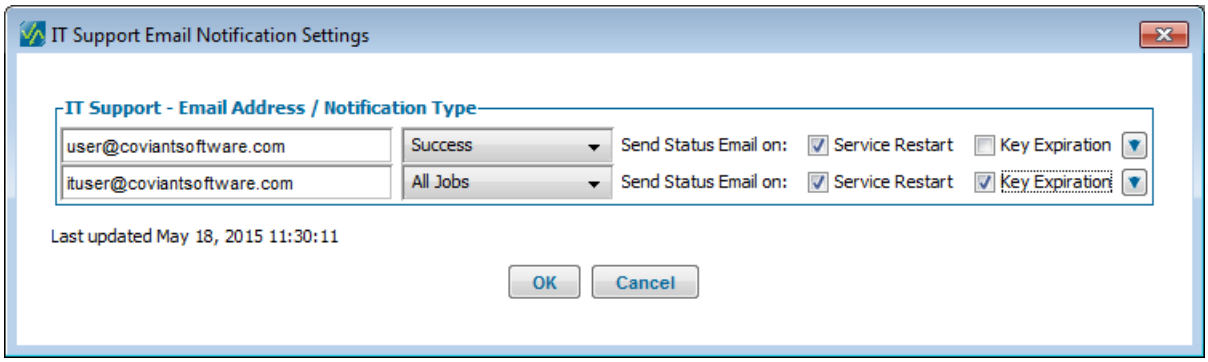
Use Default Port
Check *Use Default Port* if ports >1023 on the Diplomat MFT site are externally visible.

Start Port Range
Enter the beginning of the range of port numbers on the system that are externally visible and are forwarded to the correct port on the Diplomat MFT site.

End Port Range
Enter the last of the range of port numbers on the system that are externally visible and are forwarded to the correct port on the Diplomat MFT site.

9.2.5 IT Support Email Notification

NOTE: *IT Support Email Notification* settings are only available to accounts with *Administrator* privileges.



IT Support email notifications are sent to IT support personnel, network operations managers, or other individuals with similar responsibilities within your organization. They are intended for use in diagnosing system and network problems that are causing jobs to fail. Therefore, these email notifications are typically only sent when a file transfer job generates a warning or fails.

When *Send Debug Email to IT Support* is checked for an individual transaction, an address entered here receives an email message with the same content as the email to business users with additional debugging information appended (i.e., the same log entries as when the log level setting is "Debug").

NOTE: When total IT Support email size exceeds the Max Email Size under Settings > Email Settings, email is truncated and the complete job log is written to a file referenced in the email message in the /troubleshooting directory.

Sample email messages, including debugging information, are provided in *Appendix C: Sample Email Messages*.

NOTE: If *Send Debug Email to IT Support* is checked on the Email Notifications panel in a transaction and *Send Mail to IT Support on Failed Attempts* is checked on the Job Execution panel in a transaction, IT support addresses receive a FAILURE email message for each attempt. Business users receive FAILURE emails only after all attempts have failed.

Email Address

Email addresses of the IT support personnel to be notified.

Notification Type

Determines when an email message is sent to the associated email address. Choose any combination from the drop down menu:

- Success — Email sent if job is successful
- Warning — Email sent if job is successful, but generated at least one error that might have affected the integrity of the file(s) being transferred
- Failure — Email sent if job fails for any reason
- All jobs — Email sent for all jobs

Send Status Email on Service Restart

Check *Send Status Email on Service Restart* to send email when the Diplomat MFT Service starts that contains:

- Information about any debugging files that may have been created if the Diplomat MFT Service or Diplomat MFT Client shut down unexpectedly.
- List of incomplete jobs that were running when the Diplomat MFT Service shut down. **NOTE:** Queued jobs that have not begun execution are not included in the list of incomplete jobs.
- List of jobs that may have missed a scheduled execution. This list of missed jobs includes only transactions that were set to *Fail if File(s) Not Found* in the File Information panel on the Transaction screen or job was queued but execution had not

started when Diplomat MFT Service stopped unexpectedly. **NOTE:** Suspended transactions and transactions set to *Do Not Run*, file monitoring or allow external requests are not included in the list of missed jobs.

Send Status Email on Key Expiration

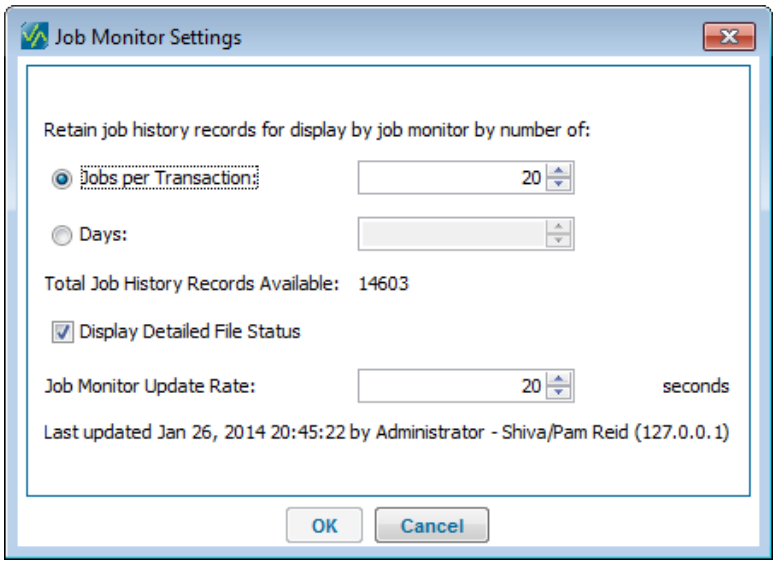
Check *Send Status Email on Key Expiration* to send email when OpenPGP keys or SSL certificates are about to expire. Emails are sent 90 days, 60 days, 30 days and 7 days prior to expiration, then daily thereafter.

NOTE: Email notifications are only sent if *Include in expiration email notifications* is checked on the key or certificate screen. The default setting is for email notifications to be sent.

NOTE: SSH keys do not have an expiration date.

9.2.6 Job Monitor

NOTE: *Job Monitor* settings are only available to accounts with *Administrator* privileges.



Job monitor settings control the number of job history records available for display by the Diplomat MFT Job Monitor. Job records can be stored for a specified number of jobs per transaction or for a specific number of days.

Retain Job Records by Jobs
Number of job executions retained for each transaction in the job history database.

Retain Job Records by Days
Number of days of job executions to retain in the job history database.

Total Job History Records Available
Total number of stored records available for display by the job monitor.

Display Detailed File Status
When not checked, the File Status column in the File History Viewer table in the Diplomat MFT Job Monitor displays sub-status in parentheses of getting source and complete

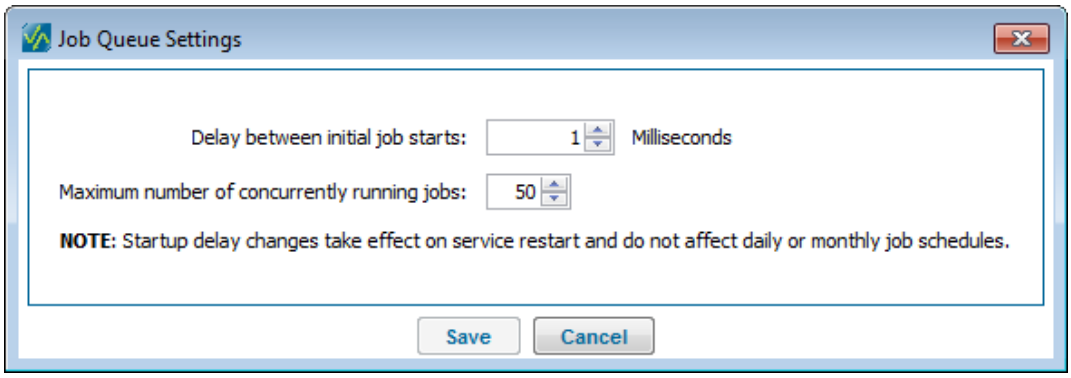
When checked, the File Status column in the File History Viewer table displays more detailed sub-status in parentheses of getting source, preparing file, putting destination file, archiving file, and complete.

Job Monitor Update Rate
Sets the number of seconds between refreshes of data displayed in the Diplomat MFTJob Monitor.

NOTE: Even if transactions in the active database are overwritten during a merge or restore with transactions using the same Transaction Name, the job history data is not deleted for Transactions Names in the active database and the job monitor may display data for jobs that ran prior to the merge or restore operation.

NOTE: Job and file records are stored in an embedded SQL database. You can execute runJobHistoryDb at the command line on the Diplomat MFT site to manually view the contents of this database. Refer to *Job History Database Viewer FAQ* for more detailed instructions.

9.2.7 Job Queue



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

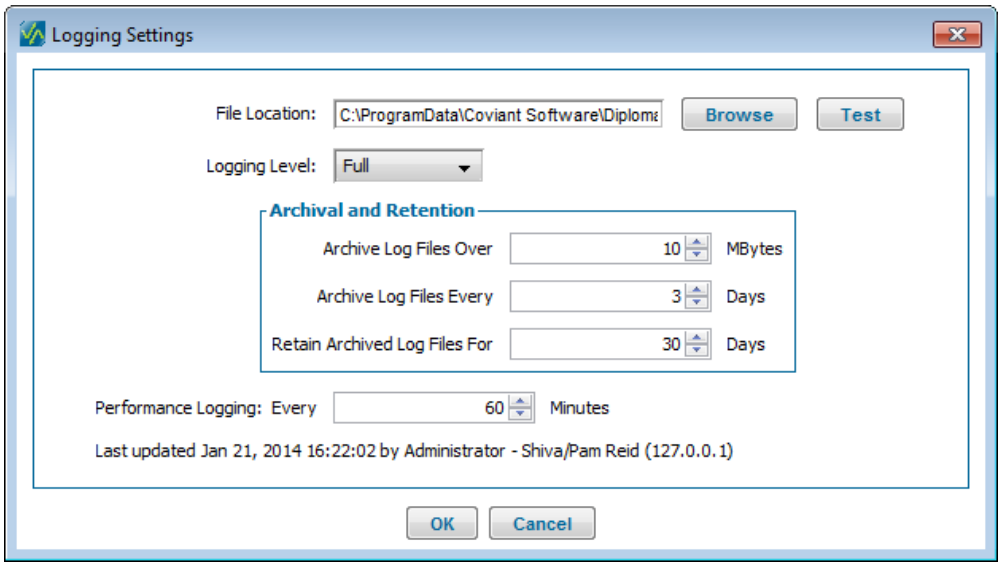
Delay between initial job starts (in Milliseconds)
When the Diplomat MFT Service starts, all Diplomat transactions are scheduled based on the information provided in the File Handling panel in the transaction. Transactions that are scheduled to run Daily or Monthly start at the exact time provided. Transactions that are scheduled Every XX Minutes or Hours run the initial job shortly after the Diplomat MFT Service starts. To avoid a long queue of jobs awaiting execution, the default is to add one second between job starts. To reduce the time between job starts, decrease the *Delay between initial job starts* setting.

NOTE: Changes to the *Delay between initial job starts* setting do not take effect until the Diplomat MFT Service restarts.

Maximum number of concurrently running jobs
The *Maximum number of concurrently running jobs* restricts the number of jobs that can execute at the same time. The default setting is 50 jobs. Diplomat file transfer jobs are spawned in separate threads and distributed across all processors on the system running the Diplomat MFT Service. **Only increase this setting if you can confirm that the system running the Diplomat MFT Service has the resources needed for additional concurrent jobs.**

9.2.8 Logging

NOTE: *Logging* settings are only available to accounts with *Administrator* privileges.



Diplomat MFT creates log files with chronological entries about every action that Diplomat Managed File Transfer takes during its operation. You can set the level of information to capture, the location of the log files, and archival/retention parameters.

Log files are text files and can be viewed using File > Logs or a variety of tools, including Wordpad or Notepad.

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'.

File Location
To change the default location of the log files, enter the pathname for the desired directory. For Windows systems, the default log file location is C:\ProgramData\Coviant Software\Diplomat-j\logs. For Linux systems, the default directory is /opt/coviant/diplomat-j/logs or the corresponding directory for your installation.

Use **Browse** to select a different directory. Use **Test** to determine whether the location is accessible and is read/write enabled for the logon identity used by the Diplomat MFT Service.

If the directory does not exist, Diplomat MFT attempts to create a directory as part of the job. If Diplomat MFT is successful in creating the directory, the job continues as if the directory had already existed.

Logging Level
Sets level at which system messages are logged from 'Full' to 'Critical Errors'. The Full level generates the most entries and Critical Errors the least.

Full
Includes all system messages.

Debug
Includes all system messages, except for large messages such as directory listings.

Informational
Includes all informational notations. Recommended setting to reduce log file sizes.

Warning

Any problem that might have affected the integrity of the file(s) being transferred for *an individual job*. Action may need to be taken. 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

Error

Any problem that causes a failure *of an individual job*. Action may need to be taken. 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

Any problem that impacts the encryption, decryption, or file transfer *of all jobs*. Action NEEDS to 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, a critical error is generated.

NOTE: Certain types of errors impacting all transactions *cannot* be logged. For example, if the Diplomat MFT Service or diplomatServer daemon stops running, all jobs stop. Diplomat MFT is unable to write to the log file, as it relies on the Diplomat MFT Service or diplomatServer daemon to do so.

Archival and Retention

When a log file is archived, Diplomat MFT automatically creates a new log file. You can automatically archive log files that are larger than a specified size or aged more than a specified number of days. Also, the current log file is archived automatically each time the Diplomat MFT Service or diplomatServer daemon is restarted.

If you do not change the default values for these fields, a new log file will be created each time the current log file reaches 1 MB or after 3 days and any log files older than 30 days are automatically deleted.

NOTE: Only log files in the currently specified *File Location* shown on this screen will be deleted.

Archive Log Files Over XX Mbytes

Set this value to automatically archive the current log file and create a new log file when the current log file reaches a maximum size. Default value is 1 MB.

Archive Log Files After XX Days

Set this value to automatically archive the current log file and create a new log file when the current log file has aged a specified number of days. Default value is 3 days.

Retain Archived Log Files For XX Days

Set this value to automatically delete all archived log files after a specified number of days. Default value is 30 days.

NOTE: Only log files with names conforming to 'Diplomat.*.log' are deleted.

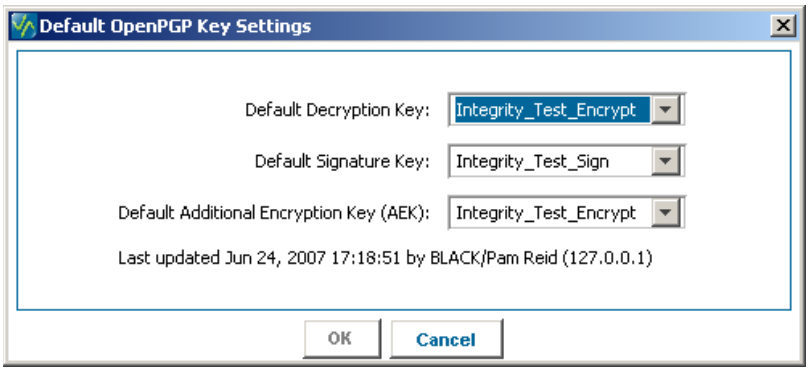
NOTE: Any temporary files created by a Diplomat MFT job that were unintentionally not deleted at the end of a Diplomat MFT job are deleted on the same schedule as archived log files.

Performance Logging

Sets interval in minutes to write performance information, such as a list of names of active threads, number of jobs running or queued, and memory usage, to the Diplomat log file. Select '0' to disable performance logging.

9.2.9 OpenPGP Keys

NOTE: *OpenPGP Keys* settings are only available to accounts with Diplomat MFT *Administrator* privileges.



Default Decryption Key

Default Decryption Key is used to pre-fill the *OpenPGP Decryption Key* field in all new inbound transactions. You would send your trading partners the public key associated with this OpenPGP key, so they can encrypt files to send to you.

Default Signature Key

Default Signature Key is used to pre-fill the *OpenPGP Signature Key* field in all new outbound transactions. You would send your trading partners the public key associated with this OpenPGP key, so they can verify the signatures on files that you send to them.

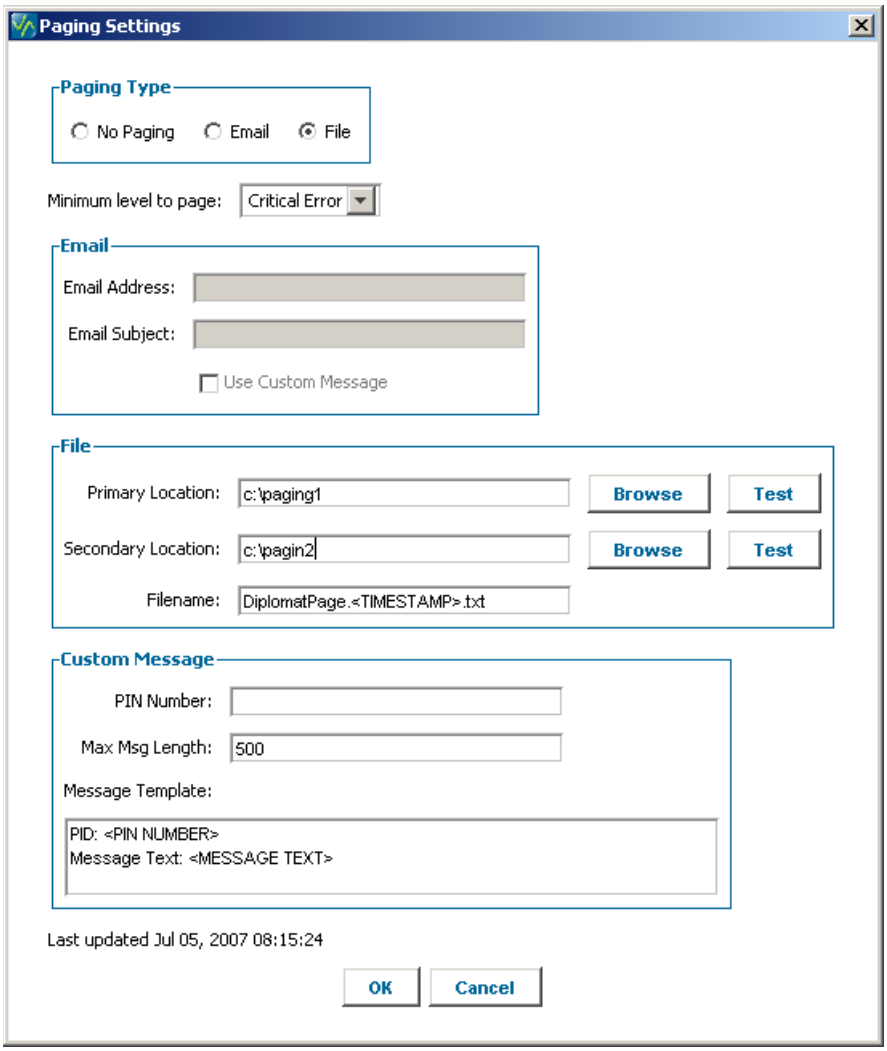
Default Additional Encryption Key (AEK)

Default Additional Encryption Key is used to pre-fill the *Additional OpenPGP Encryption Key(s)* field in all new outbound transactions. Use a *Default Additional Encryption Key* when you want to encrypt all files to a single key.

For example, most outbound files are encrypted with public keys from your trading partners. If you want to archive only encrypted files for security reasons, you would need to encrypt the files with an AEK as a secondary key that could be used to decrypt the archived files as needed.

9.2.10 Paging Notification

NOTE: *Paging Notification* settings are only available to accounts with *Administrator* privileges.



The Paging Notification screen allows you to assign a network on-call person to receive a pager notice if the Diplomat MFT Service has a problem during its operation. Paging notification is triggered when an event occurs that meets or exceeds the *Minimum Level to Page*.

Paging Type

Select *No Paging* if you want to skip all paging. Default is 'No Paging'.

Select *Email*, if your paging application generates pages from email messages. **NOTE:** Email paging requires that you set up the email server information under Settings > Email.

Select *File*, if your paging application generates pages from files.

Minimum Level to Page

Level at which paging notices are created:

Warning

Any problem that might have affected the integrity of the file(s) being transferred for *an individual job*. Action may need to be taken. 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.

Error

Any problem that causes a failure *of an individual job*. Action may need to be taken. 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

Any problem that impacts the encryption, decryption, or file transfer *of all jobs*. Action NEEDS to 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, a critical error is generated.

NOTE: Certain types of errors *cannot* be paged. For example, if the Diplomat MFT Service or diplomatServer daemon stops running, all jobs stop. Diplomat MFT is unable to send paging messages, as it relies on the Diplomat MFT Service or diplomatServer daemon to do so.

Email

Email Address

Address to send emails for use by your paging application in generating paging notices.

Email Subject

String to be displayed in the subject line of the email message sent to your paging application.

Use Custom Message

If checked, send the *Custom Message* as defined below as the body of the email message. If not checked, send the auto-generated <MESSAGE TEXT>, as defined below, as the body of the email message. Default for Use *Custom Message* is not checked.

File

Primary Location

Network location where your paging application looks for files. Use **Browse** to select a different directory. Use **Test** to determine whether the location is accessible and is read/write enabled for the logon identity used by the Diplomat MFT Service.

Secondary Location

Standby network location where your paging application looks for files when the primary location is not available. If a secondary location is entered, Diplomat MFT writes paging files to both the primary and the secondary location. Use **Browse** to select a different directory. Use **Test** to determine whether the location is accessible and is read/write enabled for the logon identity used by the Diplomat MFT Service.

Filename

Name of the file(s) written to the primary and secondary locations.

Unless you override the default, paging filenames are in the form 'DiplomatPage.year + month + day + hour + minutes + seconds.txt'. For example, a paging file created on September 22, 2004 at 1:19:20 p.m. would be named 'DiplomatPage.20040922.131920.txt'.

If you override the default, you can use <TIMESTAMP> in the filename to include a timestamp as part of the filename or <TRANS_ID> to include the Transaction Name as part of the filename. <TIMESTAMP> is replaced with a current timestamp when the paging file is written.

Custom Message

PIN Number

PIN number belonging to the on-call recipient of the paging message.

Max Message Length

Maximum number of characters allowed in a paging message. Default is 500 characters. Max message length of '0' is interpreted as 'unlimited'.

Message Template

Template for the text of the paging message to either be sent by email or captured in a file. You can include any text you would like in the message. You can also include the following fields to be filled in by Diplomat:

- <PIN Number> is the value of the *PIN Number* field from the *Custom Message* panel.
- <Message Text> is the same text as contained in the body of a debug email message and truncated to *Max Message Length*.

For example, let's assume you created a message template as follows:

```
PID: <PIN Number>
Message Text: <Message Text>
```

A paging message generated using that template might look like:

```
PID: 999 999 9999
Message Text: Outbound transaction
FTP Error
Source files obtained from C:\Program Files\Coviant Software\Diplomat-j\tomcat\Webserver\webapps\diplomat\WEB-
INF\Integrity\Outbound Source using filter BTB07.txt
        BTB07.txt File size: 44
Encryption key: Public_Test_Encrypt
Encryption key used: Public_Test_Encrypt_sub0
Signature key: Integrity_Test_Sign
Signature key used: Integrity_Test_Sign
Destination files FTP'd to coviant.biztechsource.com:21/Beta Test Files
        None
```

9.2.11 Primary Archive

NOTE: *Primary Archive* settings are only available to accounts with *Administrator* privileges.

Primary archive files are copies of the files that are transferred by Diplomat MFT file transfer jobs. The Primary Archive Settings allow you to archive files for every job in one centralized location.

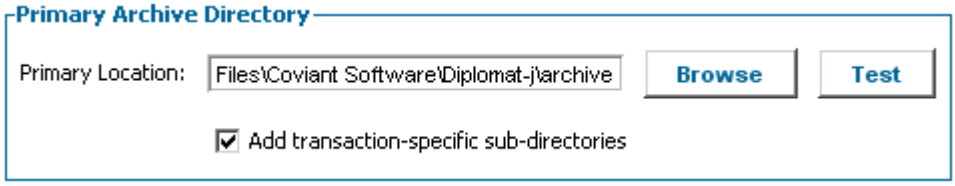
Archiving occurs directly after each file transfer step of a job. When each file transfer is complete, the source file, the destination file, or both files are archived and, if requested, the source files are deleted. By default, any files that fail to transfer are not archived and the original file(s) remain in the source directory. If desired, files can be archived for all jobs or any combination of Success, Failure, or Warning statuses.

Individual archive files have names in the form 'source_filename.srce.year + month + day . hour + minutes + seconds.milliseconds.da' or 'destination_filename.dest.year + month + day . hour + minutes + seconds.milliseconds.da'. For example, an archive of the source version of the file 'TEST.txt' created on January 4, 2004 at 3:17:53:8769 p.m. would be named 'TEST.txt.srce.20040104.151753.8769.da'. **NOTE:** All individual Diplomat MFT archive files have the file extension '.da' for easy lookup.

Zipped archive files have names in the form 'DiplomatArchive.TransactionName.year + month + day . hour + minutes + seconds.milliseconds.zip'. For example, a zipped archive file for transaction 'Test' created on January 4, 2004 at 3:17:53:8769 p.m. would be named 'DiplomatArchive.Test.20040104.151753.8769.zip'.

Turn Off Primary Archiving

Check *Turn Off Primary Archiving* to skip archiving files to one central location. When *Turn Off Primary Archiving* is checked, no files from any file transfer job are written to the primary archive location.



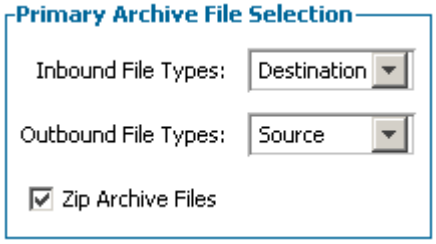
Primary Archive Directory

Primary Location

Directory where primary archive copies of all transaction files are written. For Windows systems, the default directory is C:\ProgramData\Coviant Software\Diplomat-j\archive. For Linux systems, the default directory is /opt/coviant/diplomat-j/archive. Use **Browse** to select a different directory. Use **Test** to determine whether the location is accessible and is read/write enabled for the logon identity used by the Diplomat MFT Service.

Add transaction-specific Sub-directories

If *Add Transaction-specific Sub-directories* is checked, then all primary archive files for each job are written to a sub-directory with the same name as the *Transaction Name* from the directory shown in the *Primary Location* field.



Primary Archive File Selection

Inbound File Types

Select whether source, destination, or both types of files are to be archived. Default is Destination files only.

Outbound File Types

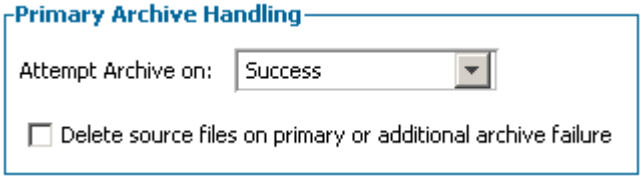
Select whether source, destination, or both types of files are to be archived. Default is Source files only.

NOTE: If you use your own private key as an AEK, you may choose to archive only destination files for outbound jobs. All primary archive files would be encrypted, but could be decrypted as needed.

Zip Archive Files

Check *Zip Archive Files* to zip all individual archive files generated by the job into a single zip file. *Zip Archive Files* is checked by default.

NOTE: If zipping the files is not successful, the individual archive files are **not** deleted.



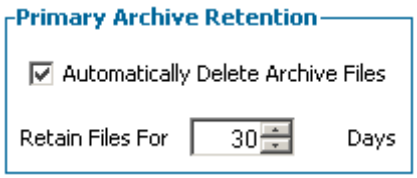
Primary Archive Handling

Attempt Archive on field determines when primary archive files are written. Default value is 'Success and Warning'. Choose any combination of the following from the drop down menu:

- Success — Archive files if job is successful
- Warning — Archive files if job is successful, but generated at least one error that might have affected the integrity of the file(s) being transferred
- Failure — Archive files if job fails for any reason
- All jobs — Archive files for all jobs

Delete source files on primary or additional archive failure controls whether source files are deleted when Diplomat MFT is unable to write archive files to either the primary or additional archive location. Default is unchecked.

NOTE: Source files are deleted only if destination files were written successfully and the only job error is the archive failure.



Primary Archive Retention

Archive files are **ONLY** automatically deleted from the primary archive location and its sub-directories. Files archived in an individual transaction to an additional location other than the *Primary Archive Location* are **not** deleted automatically.

Archive file deletion attempts occur each time the Diplomat MFT Service is restarted and daily starting 24 hours thereafter.

Automatically Delete Archive Files

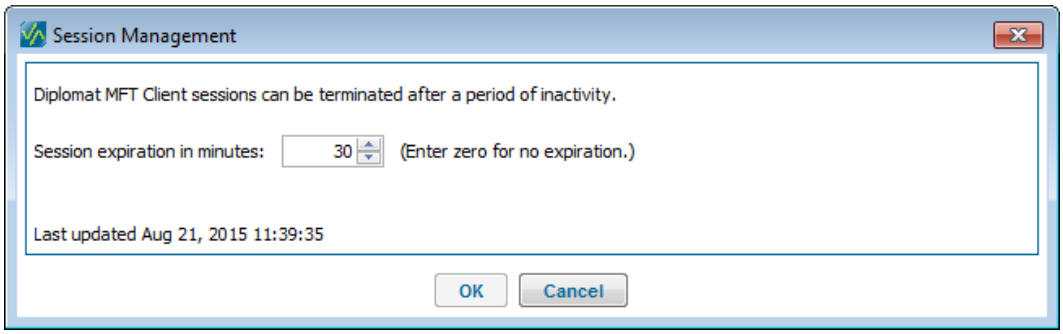
Check *Automatically Delete Archive Files*, if you would like Diplomat MFT to automatically delete primary archive files. Default is unchecked.

Retain Files for XX Days

Enter the number of days that you would like to keep primary archive files. This field is disabled if you have not checked *Automatically Delete Archive Files*. Default 30 days.

NOTE: Only archive files in the currently specified *Primary Archive Location* will be deleted.

9.2.12 Session Management

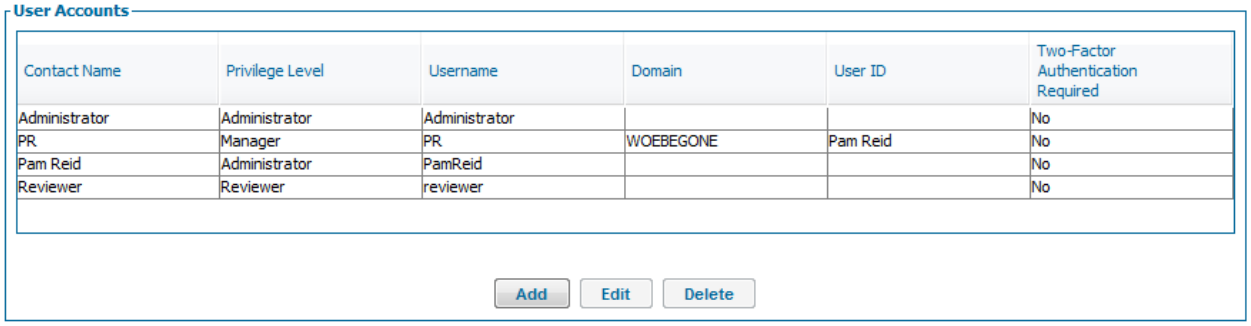


Set the Diplomat MFT Client session expiration time in minutes. If you do not want Diplomat MFT Client sessions to expire, set the expiration time to "0" minutes. Default is 30 minutes.

9.2.13 User Accounts

NOTE: *User Accounts* settings are only available to accounts with Diplomat MFT *Administrator* privileges.

The User Accounts settings screen displays current user account information and enables the creation and management of user accounts that can access the Diplomat MFT Client and Job Monitor. Only user accounts with *Administrator* privileges can update User Accounts settings.



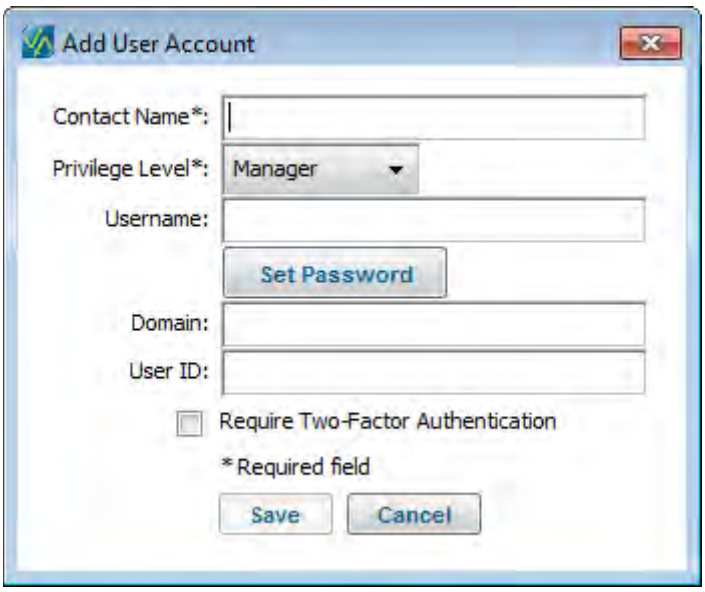
Accounts with *Manager* privileges have limited access to Diplomat MFT features. *Manager* privileges do not display the following selections from the top menu bar:

- Settings
- File > Merge
- File > Restore
- File > License

NOTE: Diplomat MFT does not limit the number of user accounts that can be created. The number of users that can connect concurrently to the Diplomat MFT Client is determined by the number of concurrent client connections allowed by the Diplomat MFT license. Accounts with an *Administrator* privilege level can check the number of concurrent client connections allowed by selecting File > License from the top menu.

NOTE: If you cannot access the Diplomat MFT Client because you do not have any valid username/password or domain/user ID combinations, contact Coviant Software Support to generate a recovery license. A recovery license is identical to your original license – except it will automatically create a user account with 'Administrator' as the username/contact name and 'diplomat' as the password. If an account with 'Administrator' already exists, the password will be changed to 'diplomat'.

NOTE: Highlight a user account in list to display the last date it was updated and the last date the password was updated.



Contact Name
Name of user associated with the account. **Required field.**

Privilege Level
Privilege level of user account. **Required field**. Valid values are *Administrator, Manager* and *Reviewer*. An *Administrator* privilege level includes the ability to change settings (including access/modify user account settings), activate a new Diplomat MFT license, and perform merge or restore functions. A *Manager* privilege level allows the set-up and running of file transfer jobs. A *Reviewer* privilege level provides read-only privileges without the ability to run file transfer jobs.

Username/Password
Username and *Password* allow users to access the Diplomat MFT Client and Job Monitor regardless of the network domain and user ID associated with their current network login. Each *Username* and *Password* combination must be unique.
After a user account has been created, users can change the password on their account under File > Password from the top menu. **NOTE:** If a user forgets their password, an account with *Administrator* privileges must set a new password for them.

NOTE: If user accounts with only *Domain* and *User ID* exist when upgrading from Diplomat MFT v4.x to Diplomat MFT v5.x, these accounts are imported into Diplomat MFT with no *Username* or *Password* data.

NOTE: When a Diplomat MFT license is installed for the first time, one user account is created with 'Administrator' as the username/contact name and 'diplomat' as the password. On the initial login, Diplomat MFT will prompt the user to change the password for user account 'Administrator'.

Domain and User ID
When a user attempts to open the Diplomat MFT Client or Job Monitor, Diplomat MFT queries the system to determine the current domain and user identity. Each *Domain* and *User ID* combination must be unique. Identities that are not on the *User Account Settings* list cannot access the Diplomat MFT Client or Job Monitor without entering a username and password.

Domain and *User ID* fields are case sensitive. Enter the domain and user ID exactly as it appears when the user is logged in.

NOTE: A domain is typically required on Windows systems.

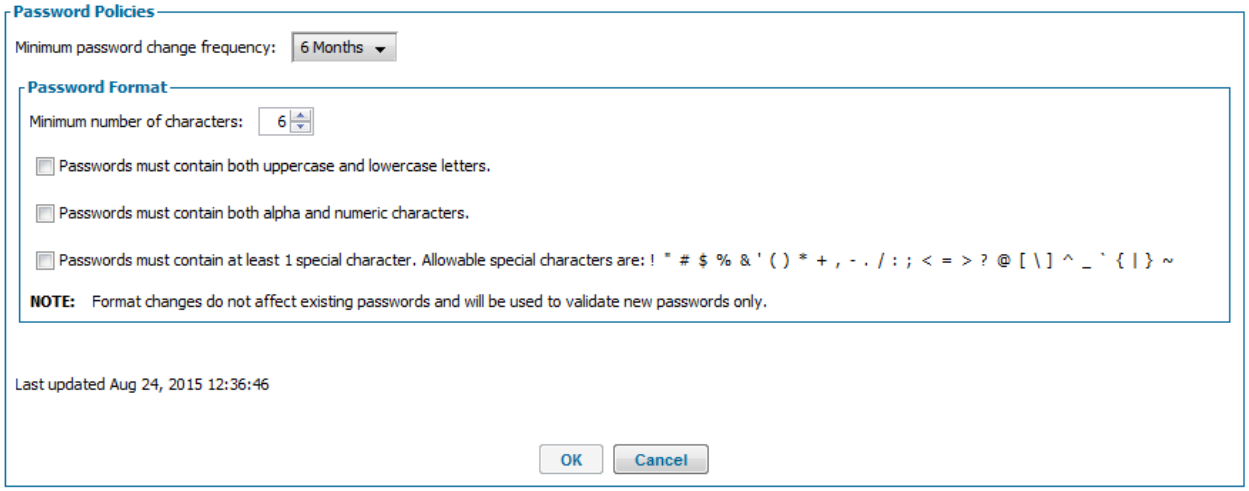
To validate the domain and user ID, follow the process below:

- Log in with the network identity on the system where the Diplomat MFT Client is installed or where the Diplomat MFT Client is running via Web Launch.
- Open a command window and enter the command 'set user'. The response will look like:
  USERDOMAIN=BLACK
  USERNAME=John Doe
- Enter the USERDOMAIN value exactly as shown in the *Domain* field.
- Enter the USERNAME value exactly as shown in the *User ID* field.

NOTE: Both fields are case sensitive.

Require Two-Factor Authentication

Check *Require Two-Factor Authentication* to require both a Username/Password and Domain/UserID combination before allowing access to the Diplomat MFT Client or Job Monitor.



Password Policies

Minimum Password Change Frequency

Minimum password change frequency can be set to 3 months, 6 months, or1 year and applies to all Diplomat MFT user accounts. If you do not want users to be prompted for regular password updates, select *None*.

NOTE: The update information at the bottom of the screen reflects the last time the *Minimum Password Change Frequency* was changed.

Password Format

Password format settings are the minimum requirements for creating a new password for all user accounts.

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

10 Managing Jobs

10.1 Jobs Overview

A Diplomat MFT file transfer 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.

The Jobs menu provides access to enhanced real-time job control features with the ability to suspend, monitor, cancel, terminate, and/or run jobs.

10.2 Jobs Menu Items

10.2.1 Release

The Release Jobs menu items restart job scheduling. When jobs are being scheduled, green status indicators are displayed in the navigation tree for jobs scheduled with the Diplomat Scheduler, dark green status indicators are displayed for jobs set to allow external requests and light green status indicators are displayed for jobs set to use file monitoring.

NOTE: All release choices can be executed by right-clicking on the object to be released in the navigation tree, as well as from the Jobs menu.

NOTE: Release Jobs menu items are disabled if the items are already being scheduled.

NOTE: When a release menu item is selected, the status indicators next to transactions in the navigation tree may change to:

- Green icons ', ' or ' to indicate they are now being scheduled or
- Orange icons ' to indicate that the transactions are still indirectly suspended.

Jobs can be released as follows:

All Transactions Directly
Release All Transaction Directly releases any directly suspended transactions. When a transaction is suspended directly, a yellow status indicator ' is displayed next to it in the navigation tree.

Transaction Folder
Release Transaction Folder releases all transactions indirectly suspended by using the *Suspend Transaction Folder* menu item.

Inbound Transaction Folder

Release Inbound Transaction Folder releases all transactions indirectly suspended by using the Suspend Inbound Transaction Folder menu item. Outbound Transaction Folder
Release Outbound Transaction Folder releases all transactions indirectly suspended by using the *Suspend Outbound Transaction Folder* menu item.

Active Key
To start all transactions associated with a key, select the suspended key in the navigation tree. Then, select Jobs > Release > Active Key.

Active Partner
To start all transactions associated with a partner profile, select the suspended partner profile in the navigation tree. Then, select Jobs > Release > Active Partner.

Active Transaction
Select the suspended transaction in the navigation tree. Then, select Jobs > Release > Active Transaction.

Release Critical Audit Suspend

When *Treat Failure as Critical* is selected on the Audit Trail Settings menu and an audit trail error occurs, all job processing is suspended. A pink status indicator '■' is displayed next to the transactions folder in the navigation tree and an orange status indicator '■' is displayed next to all transaction objects in the tree.

To release job suspensions due to a critical audit trail failure, select Jobs > Release > Release Critical Audit Suspend.

Test jobs can be executed using '*Run Now*' to determine if an audit problem has been resolved. Once the problem has been resolved, restart suspended transactions by selecting Jobs > Release > Release Critical Audit Suspend.

NOTE: If any keys, partners, or transactions were already suspended prior to a critical audit suspend occurring, these keys, partners, and transactions will remain suspended after you select Release Critical Audit Suspend.

Release DB Merge/Restore Suspend

When you merge or restore a Diplomat MFT transaction database, all jobs are suspended during the merge/restore operation. If you do not choose to release the suspended jobs when prompted at the end of the 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 suspensions due to a Diplomat MFT transaction database merge or restore, select Jobs > Release > Release DB Merge/Restore Suspend.

NOTE: When merging databases, if any keys, partners, or transactions were already suspended in your current Diplomat MFT transaction database prior to executing the merge, these keys, partners, and transactions will remain suspended after you select Release DB Merge/Restore Suspend. In addition, any keys, partners, folders, or transactions that were suspended in the backup database and were added to Diplomat MFT transaction database during the merge process will also remain suspended after you select Release DB Merge/Restore Suspend.

NOTE: When restoring a database, if any keys, partners, or transactions were already suspended prior to the restore, these keys, partners, and transactions will remain suspended after you select Release DB Merge/Restore Suspend.

10.2.2 Suspend

The Suspend menu items stop job scheduling. Any jobs that are currently queued or running when a Suspend menu item is selected complete normally and no further jobs are scheduled until a Release menu item is selected. An orange status indicator '■' is displayed next to a suspended folder, sub-folder, partner, or key, and the associated transactions in the navigation tree. When a transaction is directly suspended, a yellow status indicator '■' is displayed next to it.

NOTE: All transactions that are not currently being scheduled continue to display a red status indicator '■'.

NOTE: All release choices can be executed by right-clicking on the object to be released in the navigation tree, as well as from the Jobs menu.

NOTE: Suspend menu items are disabled if the items are already suspended.

NOTE: If a job is queued or running at the time a transaction is suspended, an orange or yellow status icon is displayed next to the transaction in the navigation tree. The job status indicator in the job monitor does not display a yellow or orange icon until the job completes.

Jobs can be suspended as follows:

All Transactions Directly

Suspend All Transaction Directly suspends each transaction individually. When a transaction is suspended directly, a yellow status indicator '■' is displayed next to it in the navigation tree.

Transaction Folder
*Suspend Transaction Folde*r indirectly suspends all transactions in the transaction folder.

Inbound Transaction Folder
*Suspend Inbound Transaction Folde*r indirectly suspends all transactions in the inbound transaction folder.

Outbound Transaction Folder
*Suspend Outbound Transaction Folde*r indirectly suspends all transactions in the outbound transaction folder.

Active Key
To suspend all transactions associated with a key, select a key in the navigation tree. Then, select Jobs > Suspend > Active Key.

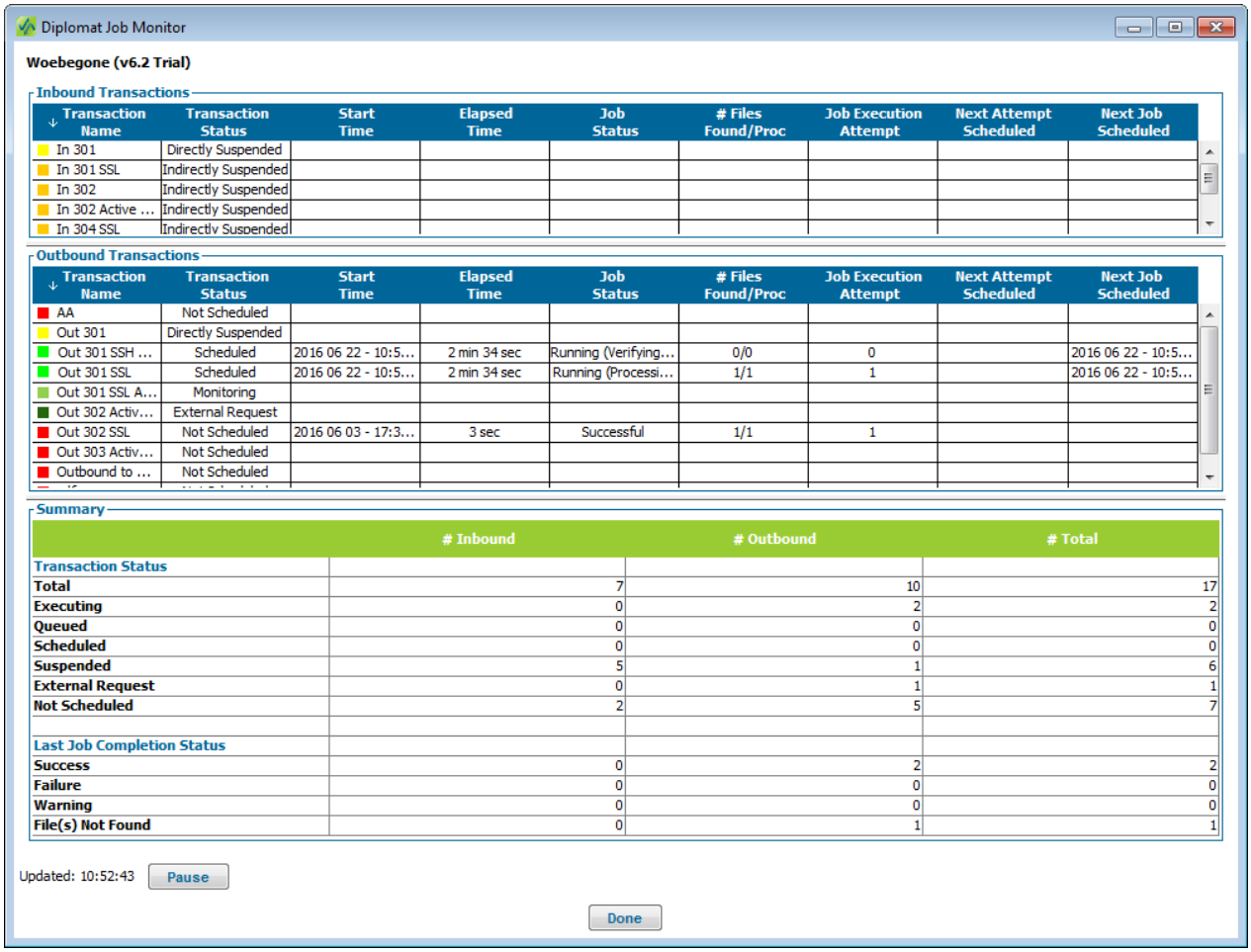
Active Partner
To suspend all transactions associated with a partner profile, select a partner profile in the navigation tree. Then, select Jobs > Suspend > Active Partner.

Active Transaction
Select the transaction in the navigation tree. Then, select Jobs > Suspend > Active Transaction.

10.2.3 Job Monitor

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* at Settings > Job Monitor.

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 current status and the last completion status of all jobs.



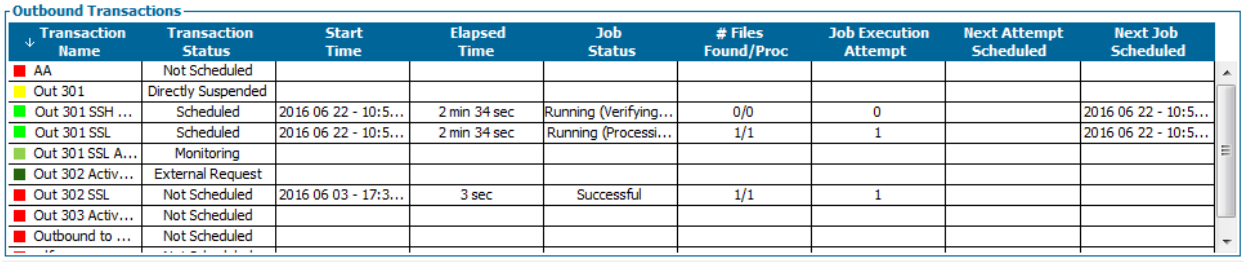
At the bottom of the main screen, a ticker field displays the most recent refresh time for the values in the job monitor tables and a *Pause* button that can temporarily suspend the refresh of the values in the job monitor tables.

NOTE: The time displayed in this field is based on the system clock of the system running the Diplomat MFT Service.

NOTE: If an error occurs when the Diplomat MFT Job Monitor is communicating with the Diplomat MFT Service, this field displays any error message returned from the Diplomat MFT Service.

Inbound/Outbound Tables

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.



Transaction Name

The transaction Name is the name of the transaction as shown in the Transaction Name field on the transaction screen. The colored icon to the left of the transaction Name is a visual indicator of job status, as follows:

	Green icon	Job scheduled or queued for execution by Diplomat MFT scheduler. Do Not Run is not checked on the Job Execution panel in the transaction.
	Blinking, green icon	Job using built-in Diplomat MFT scheduler actively executing.
	Light green icon	Job scheduled or queued for execution by the file monitor. *File monitoring* is selected on the Job Execution panel of the transaction.
	Blinking, light green icon	Job initiated by file monitoring actively executing.
	Dark green icon	Job scheduled or queued for execution by an external request. *Allow Diplomat MFT Scripting Agent requests* or *Allow Diplomat MFT API requests* checked on the Job Execution panel of the transaction.
	Blinking, dark green icon	Job initiated with the Diplomat MFT Scripting Agent or API actively executing.
	Blinking, green icon with red '/'	Request to cancel job occurred but job is still queued or running.
	Blinking, green icon with red 'X'	Request to terminate job occurred but job is still queued or running.
	Yellow icon	Individual transaction suspended.
	Orange icon	Key, partner, or folder suspended.
	Red icon	*Do Not Run* checked and/or no job scheduling types are set/allowed on the Job Execution panel.

When a file transfer job for the transaction is executing a blinking, green icon is displayed. Dark green icons indicate that the job was initiated using the Diplomat MFT Scripting Agent or API. Light green icons indicate that the job was initiated using the file monitor.

Run Now

To run a job, right-click on the Transaction Name cell and select Run Now. Run Now is enabled if a job is not currently executing.

NOTE: When Run Now is executed from the Job Monitor, the settings in the saved transaction are used. Any pending changes to the transaction in the Diplomat MFT Client are ignored.

Cancel Job

To cancel a job, right-click on the Transaction Name cell and select Cancel Job. If a job is canceling, a red slash appears across the blinking, green icon '«»'. Cancel Job is enabled if a job is currently executing.

Terminate Job

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 blinking, green icon '«»'. *Terminate Job* is enabled if a job is currently cancelling.

NOTE: Terminating a job attempts to stop execution immediately (i.e., Diplomat MFT issues a java stop thread command). Some or all files may or may not have been transferred. Email notifications may not be sent and audit trail records may not be written. Also, terminating a job may leave system resources (e.g., sockets or files) locked. **You should choose to terminate a job only if absolutely necessary.**

NOTE: As long as a job is not actively executing, *Run Now* is also an available choice when right-clicking on the Transaction Name cell.

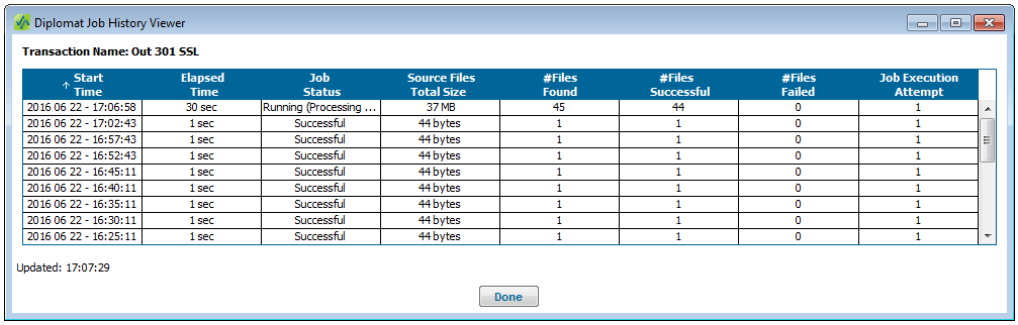
NOTE: If a job is queued or running at the time a transaction is suspended, an orange or yellow status icon is displayed next to the transaction in the navigation tree. The job status indicator in the job monitor does not display a yellow or orange icon until the job completes.

View Log

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.

NOTE: *View Log* is displayed when a job has run at least one time since the most recent time the Diplomat MFT Service started.

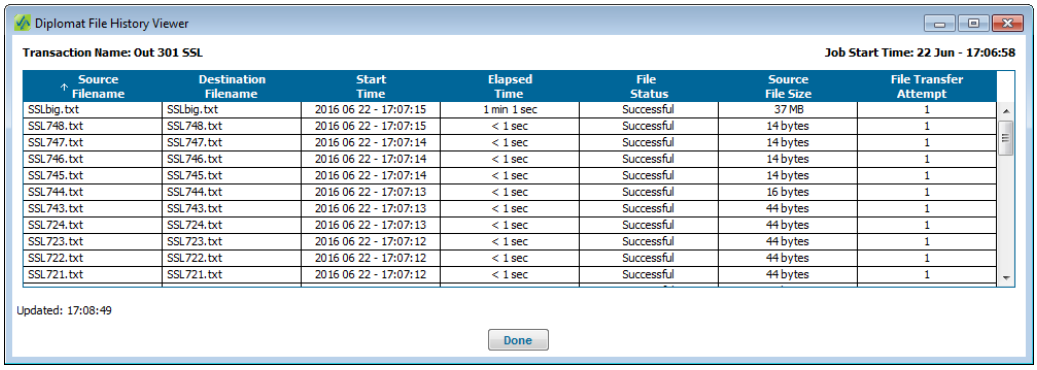
View Job History



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.

For more information on the files in a particular job, right-click on the Transaction Name cell and select *View File History*.

View File History



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.

Transaction Status

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:

- **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 *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.

Summary Table

Summary

	# Inbound	# Outbound	# Total
Transaction Status			
Total	7	10	17
Executing	0	2	2
Queued	0	0	0
Scheduled	0	0	0
Suspended	5	1	6
External Request	0	1	1
Not Scheduled	2	5	7
Last Job Completion Status			
Success	0	2	2
Failure	0	0	0
Warning	0	0	0
File(s) Not Found	0	1	1

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

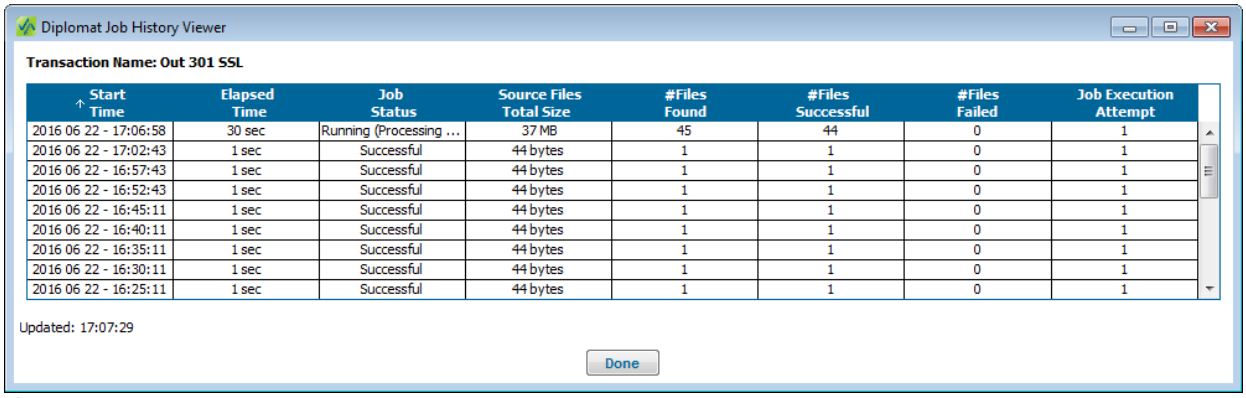
- **Total** — Total number of inbound and outbound jobs in Diplomat MFT transaction database.
- **Executing** — Number of inbound and outbound jobs currently executing.
- **Queued** — Number of inbound and outbound jobs queued to run as soon as less than 50 jobs are executing
- **Scheduled** — Number 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.

10.2.3.1 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 *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.

Source Files Total Size
Total size of all source files found by the job.

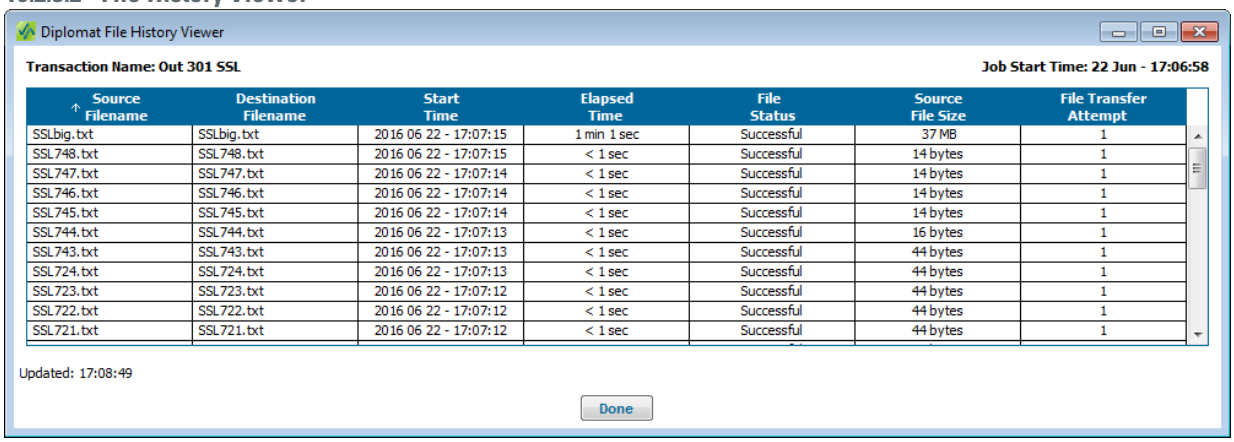
Number of Files Found
Number of files selected for file transfer.

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.

10.2.3.2 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.

Transaction Name
Transaction Name is the name of the transaction as shown in the Transaction Name field on the transaction screen.

Job Start Time
Date and time that the job began execution.

Source Filename
Name of the file picked up at the source location.

Destination Filename
Name of the file dropped off at the destination location.

Start Time
Date and time the file began processing.

Elapsed Time
Total elapsed time to process the file.

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.

Source File Size

Size of the source file in bytes.

File Transfer Attempt

Number of the last attempt to transfer the file.

11 Reports Menu

11.1 Reports Overview

Diplomat MFT provides a set of simple standard reports using the Diplomat MFT transaction database and the Diplomat MFT audit database. These reports are intended to give an overview of keys, partners, transactions, and jobs.

If further reporting of job information is required, use the SQL option for the Diplomat MFT audit database for more extensive reporting capabilities.

11.2 Reports Menu Items

11.2.1 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.

11.2.2 SSH Client Key Report

The SSH client key detail report allows you to print a standard report that includes all information for each SSH client key in the Diplomat MFT database. The SSH client key report is based on the data in the current Diplomat MFT transaction database.

11.2.3 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.

11.2.4 Partner Report

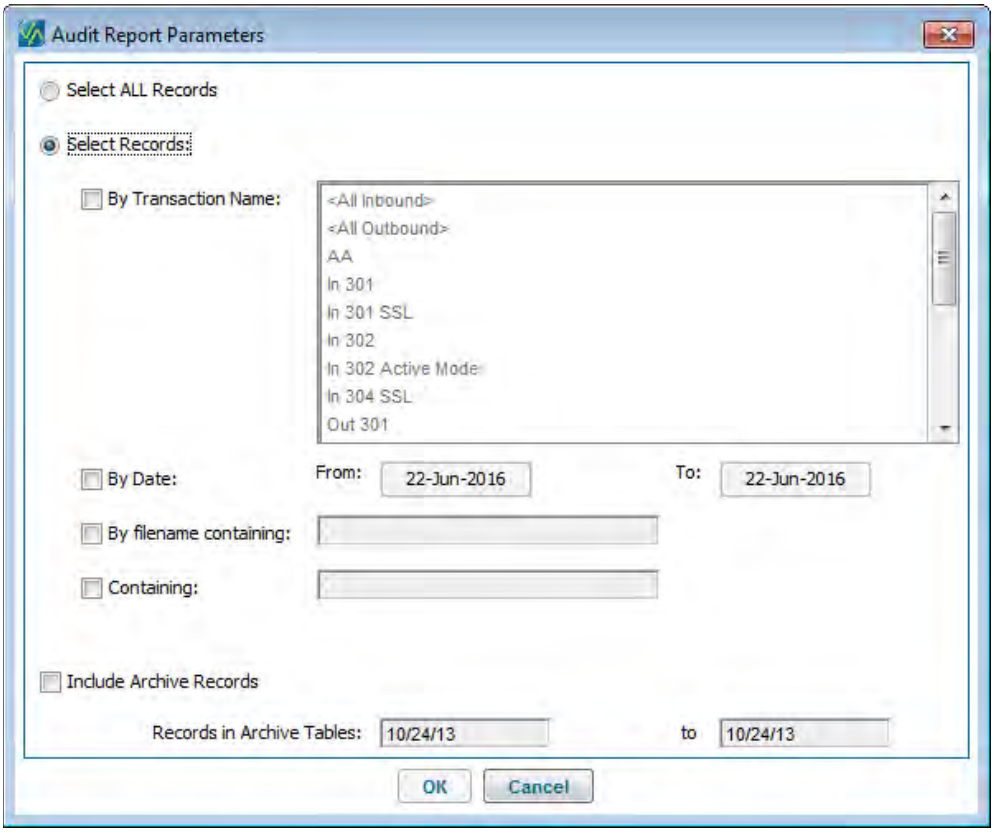
The partner report allows you to print a standard report that includes all information for each partner in the Diplomat MFT transaction database. The partner report is based on the data in the current Diplomat MFT transaction database.

11.2.5 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.

11.2.6 Audit Detail Report

The audit 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 runs on specific dates, jobs transferring files with specific names, or audit records containing a specified string.

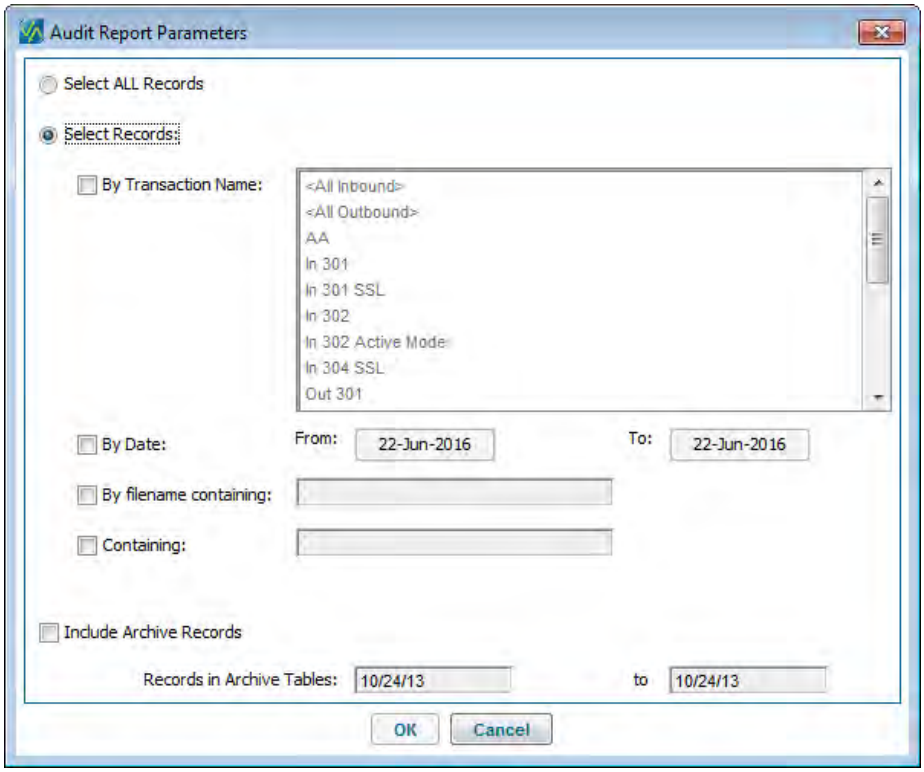
NOTE: When you search for records containing a string, **ONLY** the transaction name, transaction type (inbound/outbound), job status (successful/failure), source and destination partner name, source and destination filenames, encryption/decryption key name, signature/verification key name, and pre- and post-command fields are searched.

NOTE: The audit 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.

11.2.7 Audit Summary Report

The audit summary report allows you to print a standard report that summarizes the success and failures of jobs that ran during a specified period of time.



You may generate a report with all audit records or any combination of only inbound transactions, only outbound transactions, transaction name, jobs runs 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.

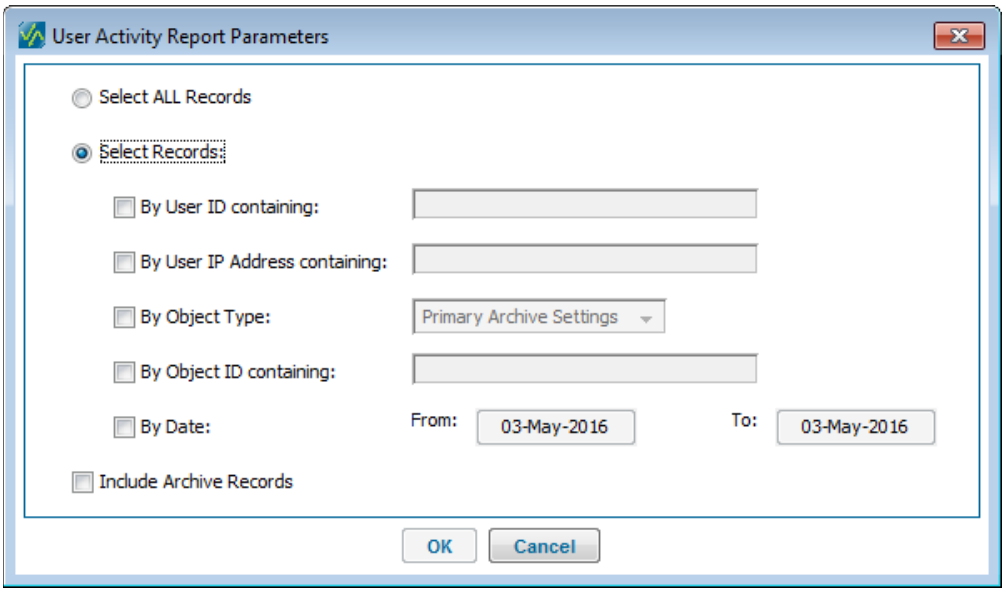
Each column shows whether a particular action completed successfully for the entire job. For example, an inbound transaction with 5 files might have 4 files decrypt successfully and 1 file that fails to decrypt. The report would indicate 'No' in the Encrypt/Decrypt column for the job, since not all files were decrypted successfully.

NOTE: The audit 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.

11.2.8 User Activity Report

User activity reports are only available when a SQL database is used for the audit trail.



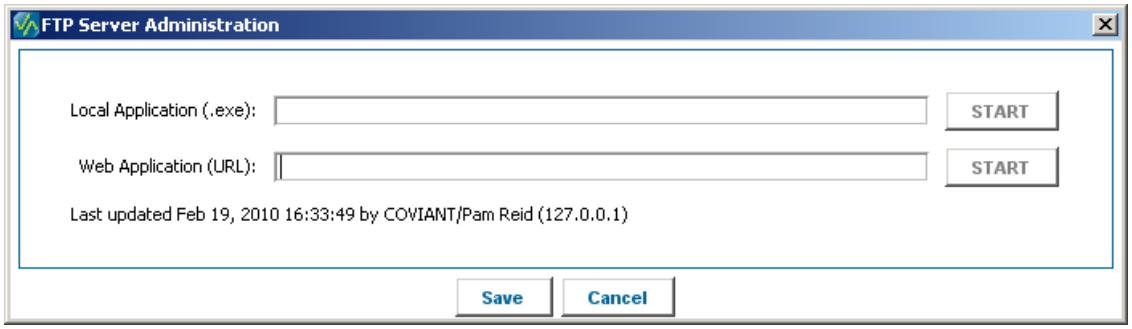
You may generate reports with all records or any combination of User IDs, User IP Address, Object Type, Date, or Object ID. You can check *Include Archived Records*, if you want archived audit records included in a report.

NOTE: The user activity report is generated from the data in the SQL Diplomat MFT audit database shown under Settings > Audit**.**

12 FTP Server Administration Menu (Optional)

Contact Coviant Software Support to activate this feature.

The FTP Server Administration settings enable immediate access to FTP server administrator consoles from within the Diplomat MFT Client. You can manage your file transfers and your FTP server with one application.



Local Application (.exe)
Set Local Application with the path to a local executable on the same system as the Diplomat MFT Client. For example, GlobalSCAPE FTP Server Administrator typically uses 'cftpsai.exe'. The **Start** button starts the FTP server administrator application on the same system as the Diplomat MFT Client.

NOTE: The FTP server must be set up to allow remote administration and the correct port must be open for the local FTP server administrator to access the FTP server.

Web Application (URL)
Set Web Application with the path to the url for the FTP server administrator web page. For example, Ipswitch WS_FTP Server Manager typically uses http://domain_name /wsftpsvr/login.asp, where 'domain_name' is associated with the system running the WS_FTP Server. The **Start** button starts the FTP server administrator in the default browser on the same system as the Diplomat MFT Client.

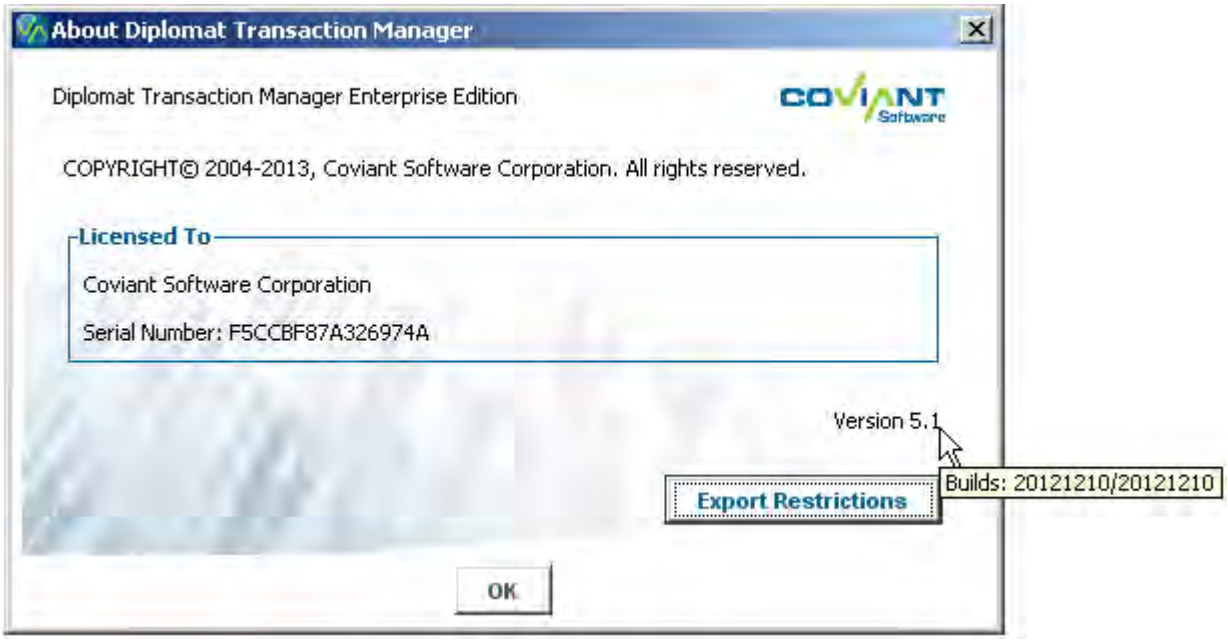
NOTE: The FTP server must be set up to allow remote administration and the correct port must be open for the FTP server administrator to access the web application.

13 Help Menu

13.1 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.

13.2 About Diplomat



You will need the information on this screen if you contact Coviant Software Support.

Licensed To

The Licensed To panel displays the name of the license owner and the serial number for this copy of Diplomat Managed File Transfer.

Version Number

The exact version and build numbers of the currently installed Diplomat MFT product. In addition to the version number, Build IDs are displayed in the form 'Diplomat MFT Client/Diplomat MFT Service' when you roll the cursor over the version number. You may need to provide the Build ID for the Diplomat MFT Client or Diplomat MFT Service to assist Coviant Software Support in diagnosing problems.

Export Restrictions

Diplomat Managed File Transfer Standard Edition may **not** be downloaded or otherwise exported or re-exported to any parties in Cuba, Iran, North Korea, Sudan, or Syria. You agree not to directly or indirectly export or re-export (including by transmission) this product to any parties in the above countries without first obtaining any required export license or governmental approval.

Select **Export Restrictions** to review detailed export restrictions.

14 Support

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

Voice:	781.210.3310 x2
Fax:	781.210.3313
Web:	www.coviantsoftware.com
E-mail:	support@coviantsoftware.com

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

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

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

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

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

Some sample debug email messages for common errors are provided in *Appendix D: Sample Email Messages*.

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

15 Appendix A: Configuration Requirements

Your environment may include not only the computer systems to run Diplomat, but other systems that provide functionality that co-exists with or is used by Diplomat, such as ftp servers, mail servers, paging servers, and OpenPGP software for key import/export. Specific software versions tested for Diplomat Managed File Transfer are shown below.

Supported Software	
Diplomat MFT Service	Windows 7[1](64-bit) Windows 8[1] (64-bit) Windows Server 2008 R2[1] (64-bit) Windows Server 2012 R2[1] (64-bit) Red Hat Enterprise Linux v6.3 Intel x86 (64-bit)
Diplomat MFT Client[3] Diplomat Cloud Connector Diplomat MFT Job Monitor	Windows 7[1] (64-bit) Windows 8[1] (64-bit) Windows Server 2008 R2[1] (64-bit) Windows Server 2012 R2[1] (64-bit)
Diplomat MFT Scripting Agent	Windows 7[1] (64-bit) Windows 8[1] (64-bit) Windows Server 2008 R2[1] (64-bit) Windows Server 2012 R2[1] (64-bit) Red Hat Enterprise Linux v6.3 Intel x86 (64-bit) Other Unix systems running Java Runtime Environment (JRE) 1.8 or higher
Diplomat MFT Web Launch	Any system supporting Java Runtime Environment (JRE) 1.8 or higher
FTP Server	Any FTP server compliant with FTP (RFC 959), FTPS (RFC 2228 with Secure FTP Using TLS), or SFTP (SSH-2; Secure Shell Charter); FTP file transfers tested with Windows, UNIX, AS400/Library, and AS400/IFS systems; SFTP and FTPS tested with Windows systems
Mail Server	Any SMTP (RFC 2821), POP3 (RFC 1939) or IMAP (RFC 3501) compliant server
HTTP/S Server	Any HTTP or HTTPS (RFC 2616) compliant server
Paging Server (Optional)	Generic file and email-based communications to paging systems; no specific paging server products are explicitly supported.
SQL Database (Optional)	MySQL Server 5.1 or higher Microsoft SQL Server 2005 v9.0 and 2008 v10.0 Most ANSI SQL-92 compliant databases with JDBC support
OpenPGP Software[4] (Optional)	OpenPGP compliant (RFC 2440, RFC 4880) products, such as McAfee E-business Server v8.0 – v8.5.2 and PGP Command Line v9.0 – v10.2.
SSH Software (Optional)	OpenSSH SSH Tectia Server from SSH Communications Security

[1] When running Windows 7, Windows Server 2008 or follow-on products, the Diplomat MFT Service cannot run as a local system account. A logon account with administrator privileges must be specified. For detailed instructions on how to update the Diplomat MFT Service, see http://coviantsoftware.com/setting-windows-login.php.

[3] Unix operating systems are not currently supported. Contact Coviant Software Support for further information.

[4] Diplomat has been tested with the listed software products, but should be compatible with any OpenPGP product compliant with RFC 2440 and RFC 4880.

The hardware configurations shown are based on approximately 50 simultaneous file transfer jobs with associated keys and partners. Your production environment may require less or more memory/disk space depending on the numbers of transactions, keys, and partners you use.

Minimum Hardware Configurations		
Diplomat MFT Service	Memory	1 GB
	Disk Space	250 MB
Diplomat MFT Client	Memory	512 MB
	Disk Space	170 MB
Diplomat MFT Scripting Agent	Memory Usage	512 MB
	Disk Space	160 MB
Diplomat MFT Job Monitor	Memory Usage	512 MB
	Disk Space	170 MB
Diplomat Cloud Connector	Memory Usage	512 MB
	Disk Space	170 MB

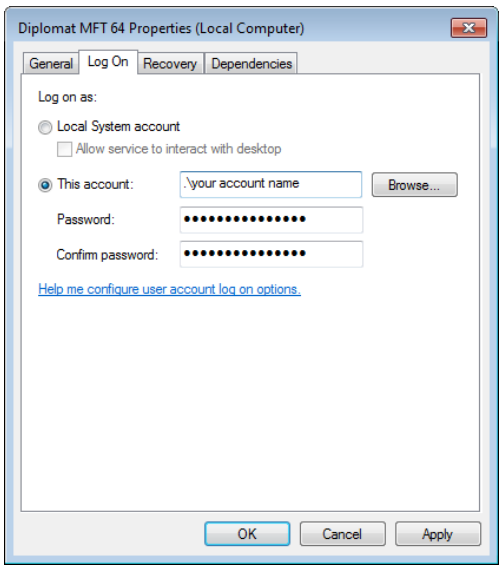
16 Appendix B: Windows Diplomat MFT Service

Access the Diplomat MFT Service through **Services** under the Windows **Control Panel.**

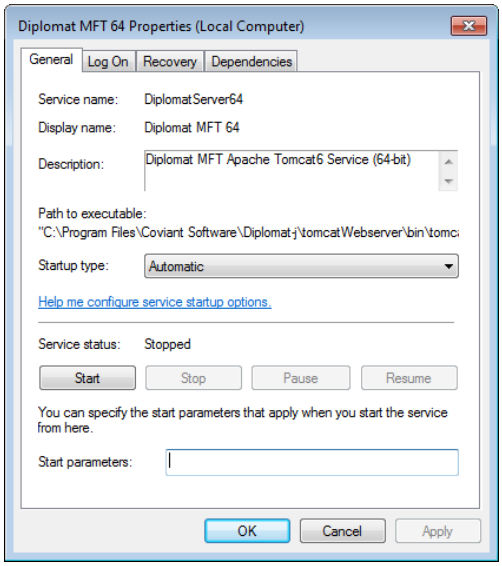
16.1 Start Diplomat MFT Service

On the **Diplomat MFT Service Properties** screen under the **Log On** tab, confirm that 'Log on as:' is set to a logon account with the required privileges. **NOTE:** A logon account is REQUIRED when running on Windows 7, Windows Server 2008 or follow-on products.

NOTE: If you use mapped drives or UNC paths when setting up transactions and access to those directories is restricted, you must set up a specific logon account for the Diplomat MFT Service with the required privileges and enter the logon account information on the **Diplomat MFT Service Properties** screen under the **Log On** tab.



Once the logon account has been set up, go to the **General** tab. The Diplomat MFT 64 service can be started or stopped using the buttons under 'Service Status'.

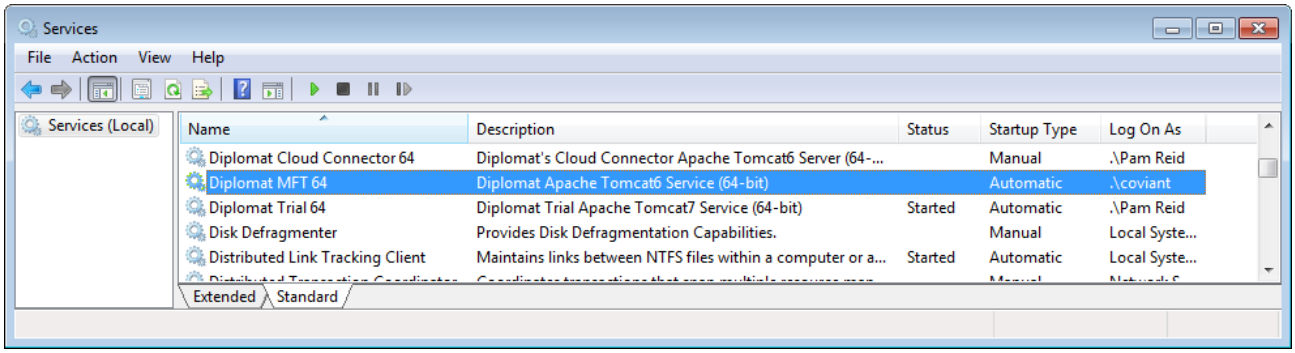


16.2 Delete Diplomat MFT Service

When you uninstall the Diplomat MFT Service, the Diplomat MFT Service may be deleted automatically or may be marked for deletion and set to disabled. If the service has been disabled, you must reboot your system to complete the deletion.

Check the status of the Diplomat MFT Service through **Services** under the Windows **Control Panel.** If Startup Type is set to disabled, you must reboot your system to complete the deletion.

NOTE: If you are planning to reinstall the Diplomat MFT Service on the same system, you must complete the deletion of the service by rebooting before attempting the reinstall.



17 Appendix C: Sample Email Messages

The following email messages are samples of email messages that are generated by various success or failure conditions. These messages include the system messages contained in email messages to IT Support.

17.1 Successful Transactions

A success email is generated any time all steps in an inbound or outbound transaction are completed properly.

17.1.1 Encrypt and Sign

Date: Thu 10/18/2007 4:49 PM
From: diplomat@coviantsoftware.com
To: ITsupport@coviantsoftware.com
Subject: SUCCESS: Out 307 was successful at October 18, 2007 4:49:16 PM

Outbound transaction

Source files obtained from C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Outbound RT Source
307.txt Last modified: 20050214.165846 File size: 44

Encryption key(s): Public_Test_Encrypt
Encryption key(s) used: Public_Test_Encrypt_sub0 Signature key: Integrity_Test_Sign Signature key used: Integrity_Test_Sign

Destination files FTP'd to 75.144.141.131:21/
307.txt.pgp File size before xfer: 431 File size after xfer: 431

Primary archiving skipped

Additional archiving skipped

Audit record written. Record ID = Out 30720071018164915343

Log Entries:
Informational October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": Begins execution

Informational October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": Outbound job started

Informational October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": Directory: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Outbound RT Source
302.txt
303.txt
304.txt
305.txt
306.txt
307.txt
308.txt

Informational October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": Source/destination file pair added to processing list:
307.txt
307.txt.pgp

Informational October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": 1 source files found

Debug October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": Source filename: 307.txt Last modified: 20050214.165846

Debug October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": Unencrypted file created and locked: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Outbound RT

Source\307.txt

Debug October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": Signed file created: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\sig19251.tmp

Debug October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": Encrypted file created for: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\enc19253.tmp

Debug October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": Connected to 75.144.141.131:21 With userID coviant

Debug October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": FTP connection verified

Debug October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": File type set to ASCII

Debug October 18, 2007 4:49:15 PM EDT
Transaction "Out 307": File type set to BINARY

Debug October 18, 2007 4:49:16 PM EDT
Transaction "Out 307": Successfully stored file 307.txt.pgp

Debug October 18, 2007 4:49:16 PM EDT
Transaction "Out 307": Primary archiving skipped

Debug October 18, 2007 4:49:16 PM EDT
Transaction "Out 307": Additional archiving skipped

Debug October 18, 2007 4:49:16 PM EDT
Transaction "Out 307": Unencrypted file closed

Debug October 18, 2007 4:49:16 PM EDT
Transaction "Out 307": Encrypted file closed

Debug October 18, 2007 4:49:16 PM EDT
Transaction "Out 307": Temp signed file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\sig19251.tmp

Debug October 18, 2007 4:49:16 PM EDT
Transaction "Out 307": Temp encrypted file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\enc19253.tmp

Debug October 18, 2007 4:49:16 PM EDT
Transaction "Out 307": FTP session disconnected

Debug October 18, 2007 4:49:16 PM EDT
Transaction "Out 307": Beginning end-of-job processing

Debug October 18, 2007 4:49:16 PM EDT
Transaction "Out 307": FTP session already disconnected

Informational October 18, 2007 4:49:16 PM EDT
Transaction "Out 307": Transaction terminated successfully

Debug October 18, 2007 4:49:16 PM EDT
Transaction "Out 307": Job ended

17.1.2 Decrypt and Verify

Date: Thu 10/18/2007 4:53 PM
From: diplomat@coviantsoftware.com
To: ITsupport@coviantsoftware.com
Subject: SUCCESS: In 307 was successful at October 18, 2007 4:52:51 PM

Inbound transaction

Source files FTP'd from 75.144.141.131:21/
307.txt.pgp Last modified: 20071018.124853
File size before xfer: 431 File size after xfer: 431

Decryption key: Integrity_Test_Encrypt
Decryption key used: Integrity_Test_Encrypt_sub Verification key specified: Public_Test_Sign Verification key used: Public_Test_Sign

Destination files moved to C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\Globalscape\Inbound RT Destination
307.txt File size: 44

Primary archiving skipped

Additional archiving skipped

Audit record written. Record ID = In 30720071018165250421

Log Entries:
Informational October 18, 2007 4:52:50 PM EDT
Transaction "In 307": Begins execution

Informational October 18, 2007 4:52:50 PM EDT
Transaction "In 307": Inbound job started

Debug October 18, 2007 4:52:50 PM EDT
Transaction "In 307": Connected to 75.144.141.131:21 With userID coviant

Debug October 18, 2007 4:52:50 PM EDT
Transaction "In 307": FTP connection verified

Debug October 18, 2007 4:52:50 PM EDT
Transaction "In 307": File type set to ASCII

Informational October 18, 2007 4:52:50 PM EDT
Transaction "In 307": Directory: /Usr/coviant
303.txt.pgp
304.txt.asc
305.txt.pgp
306.txt.asc
306.txt.pgp
307.txt.pgp
308.txt.asc
308.txt.pgp
309.xls
310.xls.asc

Informational October 18, 2007 4:52:50 PM EDT
Transaction "In 307": Source/destination file pair added to processing list:
307.txt.pgp
307.txt

Informational October 18, 2007 4:52:50 PM EDT
Transaction "In 307": 1 source files found

Debug October 18, 2007 4:52:50 PM EDT
Transaction "In 307": Source filename: 307.txt.pgp Last modified: 20071018.124853

Debug October 18, 2007 4:52:50 PM EDT
Transaction "In 307": FTP connection verified

Debug October 18, 2007 4:52:50 PM EDT
Transaction "In 307": File type set to BINARY

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": Encrypted file created and locked: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19254.tmp

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": Sensed armoring: false

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": Verified file created for transaction: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19255.tmp

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPCompressedData

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPSignatureList

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPLiteralData

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": File moved for transaction: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Inbound RT Destination\307.txt

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": Primary archiving skipped

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": Additional archiving skipped

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": Encrypted file closed

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": Verified file closed

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": Temp encrypted file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19254.tmp

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": Temp verified file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19255.tmp

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": FTP session disconnected

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": Beginning end-of-job processing

Debug October 18, 2007 4:52:51 PM EDT
Transaction "In 307": FTP session already disconnected

Informational October 18, 2007 4:52:51 PM EDT
Transaction "In 307": Transaction terminated successfully

```
Debug       October 18, 2007 4:52:51 PM EDT
Transaction "In 307": Job ended
```

17.1.3 Multi-file Decrypt and Verify

Date: Thu 10/18/2007 5:04 PM
From: diplomat@coviantsoftware.com
To: ITsupport@coviantsoftware.com
Subject: SUCCESS: In 307 was successful at October 18, 2007 5:03:40 PM

Inbound transaction

Source files FTP'd from 75.144.141.131:21/
307.txt.pgp Last modified: 20071018.130233
File size before xfer: 431 File size after xfer: 431
306.txt.pgp Last modified: 20071018.130233
File size before xfer: 431 File size after xfer: 431
308.txt.pgp Last modified: 20071018.130234
File size before xfer: 431 File size after xfer: 431

Decryption key: Integrity_Test_Encrypt
Decryption key used: Integrity_Test_Encrypt_sub Verification key specified: Public_Test_Sign Verification key used: Public_Test_Sign

Destination files moved to C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\Globalscape\Inbound RT Destination
307.txt File size: 44
306.txt File size: 44
308.txt File size: 44

Primary archiving skipped

Additional archiving skipped

Audit record written. Record ID = In 30720071018170335437

Log Entries:
Informational October 18, 2007 5:03:35 PM EDT
Transaction "In 307": Begins execution

Informational October 18, 2007 5:03:35 PM EDT
Transaction "In 307": Inbound job started

Debug October 18, 2007 5:03:35 PM EDT
Transaction "In 307": Connected to 75.144.141.131:21 With userID coviant

Debug October 18, 2007 5:03:35 PM EDT
Transaction "In 307": FTP connection verified

Debug October 18, 2007 5:03:35 PM EDT
Transaction "In 307": File type set to ASCII

Informational October 18, 2007 5:03:35 PM EDT
Transaction "In 307": Directory: /Usr/coviant
304.txt.asc
305.txt.pgp
306.txt.asc
306.txt.pgp
307.txt.pgp
308.txt.asc
308.txt.pgp
309.xls

Informational October 18, 2007 5:03:35 PM EDT
Transaction "In 307": Source/destination file pair added to processing list:
307.txt.pgp
307.txt

Debug October 18, 2007 5:03:36 PM EDT

```
Transaction "In 307": FTP connection verified

Informational          October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Directory: /Usr/coviant
          304.txt.asc
          305.txt.pgp
          306.txt.asc
          306.txt.pgp
          307.txt.pgp
          308.txt.asc
          308.txt.pgp
          309.xls

Informational          October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Source/destination file pair added to processing list:
306.txt.pgp
306.txt

Debug     October 18, 2007 5:03:36 PM EDT
Transaction "In 307": FTP connection verified

Informational          October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Directory: /Usr/coviant
          304.txt.asc
          305.txt.pgp
          306.txt.asc
          306.txt.pgp
          307.txt.pgp
          308.txt.asc
          308.txt.pgp
          309.xls

Informational          October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Source/destination file pair added to processing list:
308.txt.pgp
308.txt

Informational          October 18, 2007 5:03:36 PM EDT
Transaction "In 307": 3 source files found

Debug     October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Source filename: 307.txt.pgp          Last modified: 20071018.130233

Debug     October 18, 2007 5:03:36 PM EDT
Transaction "In 307": FTP connection verified

Debug     October 18, 2007 5:03:36 PM EDT
Transaction "In 307": File type set to BINARY

Debug     October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Encrypted file created and locked: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-
INF\temp\ftp19265.tmp

Debug     October 18, 2007 5:03:36 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug     October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Sensed armoring: false

Debug     October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Verified file created for transaction: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-
INF\temp\auth19266.tmp

Debug     October 18, 2007 5:03:36 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug     October 18, 2007 5:03:36 PM EDT
```

Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPCompressedData

Debug October 18, 2007 5:03:36 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPSignatureList

Debug October 18, 2007 5:03:36 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPLiteralData

Debug October 18, 2007 5:03:36 PM EDT
Transaction "In 307": File moved for transaction: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\Globalscape\Inbound RT Destination\307.txt

Debug October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Primary archiving skipped

Debug October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Additional archiving skipped

Debug October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Encrypted file closed

Debug October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Verified file closed

Debug October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Temp encrypted file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19265.tmp

Debug October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Temp verified file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19266.tmp

Debug October 18, 2007 5:03:36 PM EDT
Transaction "In 307": Source filename: 306.txt.pgp Last modified: 20071018.130233

Debug October 18, 2007 5:03:37 PM EDT
Transaction "In 307": FTP connection verified

Debug October 18, 2007 5:03:37 PM EDT
Transaction "In 307": Encrypted file created and locked: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19267.tmp

Debug October 18, 2007 5:03:37 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug October 18, 2007 5:03:37 PM EDT
Transaction "In 307": Sensed armoring: false

Debug October 18, 2007 5:03:38 PM EDT
Transaction "In 307": Verified file created for transaction: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19268.tmp

Debug October 18, 2007 5:03:38 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug October 18, 2007 5:03:38 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPCompressedData

Debug October 18, 2007 5:03:38 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPSignatureList

Debug October 18, 2007 5:03:38 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPLiteralData

Debug October 18, 2007 5:03:39 PM EDT
Transaction "In 307": File moved for transaction: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\Globalscape\Inbound RT Destination\306.txt

Debug October 18, 2007 5:03:39 PM EDT

Transaction "In 307": Primary archiving skipped

Debug October 18, 2007 5:03:39 PM EDT
Transaction "In 307": Additional archiving skipped

Debug October 18, 2007 5:03:39 PM EDT
Transaction "In 307": Encrypted file closed

Debug October 18, 2007 5:03:39 PM EDT
Transaction "In 307": Verified file closed

Debug October 18, 2007 5:03:39 PM EDT
Transaction "In 307": Temp encrypted file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19267.tmp

Debug October 18, 2007 5:03:39 PM EDT
Transaction "In 307": Temp verified file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19268.tmp

Debug October 18, 2007 5:03:39 PM EDT
Transaction "In 307": Source filename: 308.txt.pgp Last modified: 20071018.130234

Debug October 18, 2007 5:03:39 PM EDT
Transaction "In 307": FTP connection verified

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": Encrypted file created and locked: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19269.tmp

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": Sensed armoring: false

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": Verified file created for transaction: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19270.tmp

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPCompressedData

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPSignatureList

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPLiteralData

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": File moved for transaction: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\Globalscape\Inbound RT Destination\308.txt

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": Primary archiving skipped

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": Additional archiving skipped

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": Encrypted file closed

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": Verified file closed

Debug October 18, 2007 5:03:40 PM EDT

Transaction "In 307": Temp encrypted file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19269.tmp

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": Temp verified file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19270.tmp

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": FTP session disconnected

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": Beginning end-of-job processing

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": FTP session already disconnected

Informational October 18, 2007 5:03:40 PM EDT
Transaction "In 307": Transaction terminated successfully

Debug October 18, 2007 5:03:40 PM EDT
Transaction "In 307": Job ended

17.1.4 Transfer Only – No Encrypt or Sign

Date: Thu 10/18/2007 5:00 PM
From: diplomat@coviantsoftware.com
To: ITsupport@coviantsoftware.com
Subject: SUCCESS: Out 301 was successful at October 18, 2007 5:00:11 PM

Outbound transaction

Source files obtained from C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Outbound RT Source
301.txt Last modified: 20050214.165846 File size: 44

Encryption not required
Signature not required

Destination files FTP'd to 75.144.141.131:21/
301.txt File size before xfer: 44 File size after xfer: 44

Primary archiving skipped

Additional archiving skipped

Audit record written. Record ID = Out 30120071018170010421

Log Entries:
Informational October 18, 2007 5:00:10 PM EDT
Transaction "Out 301": Begins execution

Informational October 18, 2007 5:00:10 PM EDT
Transaction "Out 301": Outbound job started

Informational October 18, 2007 5:00:10 PM EDT
Transaction "Out 301": Directory: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Outbound RT Source
301.txt
302.txt
303.txt
304.txt
305.txt

Informational October 18, 2007 5:00:10 PM EDT
Transaction "Out 301": Source/destination file pair added to processing list:
301.txt
301.txt

Informational October 18, 2007 5:00:10 PM EDT
Transaction "Out 301": 1 source files found

Debug October 18, 2007 5:00:10 PM EDT
Transaction "Out 301": Source filename: 301.txt Last modified: 20050214.165846

Debug October 18, 2007 5:00:10 PM EDT
Transaction "Out 301": Unencrypted file created and locked: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Outbound RT Source\301.txt

Debug October 18, 2007 5:00:10 PM EDT
Transaction "Out 301": Connected to 75.144.141.131:21 With userID coviant

Debug October 18, 2007 5:00:10 PM EDT
Transaction "Out 301": FTP connection verified

Debug October 18, 2007 5:00:10 PM EDT
Transaction "Out 301": File type set to ASCII

Debug October 18, 2007 5:00:11 PM EDT

```
Transaction "Out 301": Successfully stored file 301.txt

Debug       October 18, 2007 5:00:11 PM EDT
Transaction "Out 301": Primary archiving skipped

Debug       October 18, 2007 5:00:11 PM EDT
Transaction "Out 301": Additional archiving skipped

Debug       October 18, 2007 5:00:11 PM EDT
Transaction "Out 301": Unencrypted file closed

Debug       October 18, 2007 5:00:11 PM EDT
Transaction "Out 301": Encrypted file closed

Debug       October 18, 2007 5:00:11 PM EDT
Transaction "Out 301": FTP session disconnected

Debug       October 18, 2007 5:00:11 PM EDT
Transaction "Out 301": Beginning end-of-job processing

Debug       October 18, 2007 5:00:11 PM EDT
Transaction "Out 301": FTP session already disconnected

Informational               October 18, 2007 5:00:11 PM EDT
Transaction "Out 301": Transaction terminated successfully

Debug       October 18, 2007 5:00:11 PM EDT
Transaction "Out 301": Job ended
```

17.2 Failed Transactions

When a transaction fails, email is generated any time the file was not delivered, encrypted/decrypted, or archived successfully. The first section of the message states the primary reason failure email was generated.

17.2.1 No Source File and 'Fail if File(s) Not Found' Checked

```
Date:      Thu 10/18/2007 5:09 PM
From:      diplomat@coviantsoftware.com
To:        ITsupport@coviantsoftware.com
Subject:  FAILURE: In 307 failed at October 18, 2007 5:08:51 PM
```

```
Inbound transaction

No source files found  and 'Fail if File(s) Not Found' is checked.

Source files FTP'd from 75.144.141.131:21/
        None

Decryption key: Integrity_Test_Encrypt
Message was not encrypted
Verification key specified: Public_Test_Sign Message was not signed

Destination files moved to C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Inbound RT Destination
        None

Primary archiving skipped

Additional archiving skipped

Audit record written.  Record ID = In 30720071018170850703


Log Entries:
Informational        October 18, 2007 5:08:50 PM EDT
Transaction "In 307": Begins execution

Informational        October 18, 2007 5:08:50 PM EDT
Transaction "In 307": Inbound job started

Debug    October 18, 2007 5:08:50 PM EDT
Transaction "In 307": Connected to 75.144.141.131:21 With userID coviant

Debug    October 18, 2007 5:08:50 PM EDT
Transaction "In 307": FTP connection verified

Debug    October 18, 2007 5:08:50 PM EDT
Transaction "In 307": File type set to ASCII

Informational        October 18, 2007 5:08:51 PM EDT
Transaction "In 307": Directory: /Usr/coviant
        301.txt
        302.txt.asc
        303.txt.pgp
        304.txt.asc
        305.txt.pgp

Error    October 18, 2007 5:08:51 PM EDT
Transaction "In 307": No source files found  and 'Fail if File(s) Not Found' is checked.

Debug    October 18, 2007 5:08:51 PM EDT
Transaction "In 307": FTP session disconnected

Debug    October 18, 2007 5:08:51 PM EDT
```

```
Transaction "In 307": Beginning end-of-job processing

Debug        October 18, 2007 5:08:51 PM EDT
Transaction "In 307": FTP session already disconnected

Informational              October 18, 2007 5:08:51 PM EDT
Transaction "In 307": Transaction terminated with an error

Debug        October 18, 2007 5:08:51 PM EDT
Transaction "In 307": Job ended
```

17.2.2 FTP Error

Date: Thu 10/18/2007 5:13 PM
From: diplomat@coviantsoftware.com
To: ITsupport@coviantsoftware.com
Subject: FAILURE: Out 307 failed at October 18, 2007 5:13:21 PM

Outbound transaction

FTP Error: FTP Error: 530 Not logged in.

Source files obtained from C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\Globalscape\Outbound RT Source
307.txt Last modified: 20050214.165846 File size: 44

Encryption key(s): Public_Test_Encrypt
Encryption key(s) used: Public_Test_Encrypt_sub0 Signature key: Integrity_Test_Sign Signature key used: Integrity_Test_Sign

Destination files FTP'd to 75.144.141.131:21/
None

Destination file errors:
307.txt.pgp: FTP error - FTP Error: 530 Not logged in.

Primary archiving skipped

Additional archiving skipped

Audit record written. Record ID = Out 30720071018171140875

Log Entries:
Informational October 18, 2007 5:11:40 PM EDT
Transaction "Out 307": Begins execution

Informational October 18, 2007 5:11:40 PM EDT
Transaction "Out 307": Outbound job started

Informational October 18, 2007 5:11:40 PM EDT
Transaction "Out 307": Directory: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\Globalscape\Outbound RT Source
301.txt
302.txt
303.txt
304.txt
305.txt
306.txt
307.txt
308.txt

Informational October 18, 2007 5:11:40 PM EDT
Transaction "Out 307": Source/destination file pair added to processing list:
307.txt
307.txt.pgp

Informational October 18, 2007 5:11:40 PM EDT
Transaction "Out 307": 1 source files found

Debug October 18, 2007 5:11:40 PM EDT
Transaction "Out 307": Source filename: 307.txt Last modified: 20050214.165846

Debug October 18, 2007 5:11:40 PM EDT
Transaction "Out 307": Unencrypted file created and locked: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\Globalscape\Outbound RT Source\307.txt

Debug October 18, 2007 5:11:40 PM EDT
Transaction "Out 307": Signed file created: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\sig19271.tmp

Debug October 18, 2007 5:11:40 PM EDT
Transaction "Out 307": Encrypted file created for: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\enc19273.tmp

Debug October 18, 2007 5:11:41 PM EDT
Transaction "Out 307": FTP connect error (attempt #1): 530 Not logged in.

Debug October 18, 2007 5:11:41 PM EDT
Transaction "Out 307": FTP session disconnected after failure

Debug October 18, 2007 5:12:01 PM EDT
Transaction "Out 307": FTP connect error (attempt #2): 530 Not logged in.

Debug October 18, 2007 5:12:01 PM EDT
Transaction "Out 307": FTP session disconnected after failure

Debug October 18, 2007 5:12:21 PM EDT
Transaction "Out 307": FTP connect error (attempt #3): 530 Not logged in.

Debug October 18, 2007 5:12:21 PM EDT
Transaction "Out 307": FTP session disconnected after failure

Debug October 18, 2007 5:12:41 PM EDT
Transaction "Out 307": FTP connect error (attempt #4): 530 Not logged in.

Debug October 18, 2007 5:12:41 PM EDT
Transaction "Out 307": FTP session disconnected after failure

Debug October 18, 2007 5:13:01 PM EDT
Transaction "Out 307": FTP connect error (attempt #5): 530 Not logged in.

Debug October 18, 2007 5:13:01 PM EDT
Transaction "Out 307": FTP session disconnected after failure

Debug October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": FTP connect error (attempt #6): 530 Not logged in.

Debug October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": FTP session disconnected after failure

Debug October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": FTP Exception (connect): 530 Not logged in.

Error October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": FTP Error: FTP Error: 530 Not logged in.

Cause: java.io.IOException - FTP Error: 530 Not logged in.

diplomat.server.ftp.FTPJscape.initializeConnection(FTPJscape.java:987)
diplomat.server.ftp.FTPJscape.connect(FTPJscape.java:92)
diplomat.server.filetransfer.FtpDirectoryAgent.connectForWriting(FtpDirectoryAgent.java:99)
diplomat.server.job.DiplomatOutboundJob.moveEncryptedFile(DiplomatOutboundJob.java:580)
diplomat.server.job.DiplomatOutboundJob.run(DiplomatOutboundJob.java:153)
java.lang.Thread.run(Thread.java:595)

Debug October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": Primary archiving skipped

Debug October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": Additional archiving skipped

Debug October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": Unencrypted file closed

Debug October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": Encrypted file closed

Debug October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": Temp signed file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\sig19271.tmp

Debug October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": Temp encrypted file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\enc19273.tmp

Debug October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": FTP session already disconnected

Debug October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": Beginning end-of-job processing

Debug October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": FTP session already disconnected

Informational October 18, 2007 5:13:21 PM EDT
Transaction "Out 307": Transaction terminated with an error

Debug October 18, 2007 5:13:22 PM EDT
Transaction "Out 307": Job ended

17.2.3 No Overwrite Allowed

Date: Thu 10/18/2007 5:31 PM
From: diplomat@coviantsoftware.com
To: ITsupport@coviantsoftware.com
Subject: FAILURE: Out 301 failed at October 18, 2007 5:31:01 PM

Outbound transaction

File 301.txt already exists on remote server and overwrite is not specified

Source files obtained from C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Outbound RT Source
301.txt Last modified: 20050214.165846 File size: 44

Encryption not required
Signature not required

Destination files FTP'd to 75.144.141.131:21/
None

Destination file errors:
File 301.txt already exists on remote server and overwrite is not specified

Primary archiving skipped

Additional archiving skipped

Audit record written. Record ID = Out 30120071018173101250

Log Entries:
Informational October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Begins execution

Informational October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Outbound job started

Informational October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Directory: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Outbound RT Source
301.txt
302.txt
303.txt
304.txt
305.txt
306.txt
307.txt

Informational October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Source/destination file pair added to processing list:
301.txt
301.txt

Informational October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": 1 source files found

Debug October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Source filename: 301.txt Last modified: 20050214.165846

Debug October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Unencrypted file created and locked: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Outbound RT Source\301.txt

Debug October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Connected to 75.144.141.131:21 With userID coviant

```
Debug         October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": FTP connection verified

Debug         October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": File type set to ASCII

Error         October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": File 301.txt already exists on remote server and overwrite is not specified

Debug         October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Primary archiving skipped

Debug         October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Additional archiving skipped

Debug         October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Unencrypted file closed

Debug         October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Encrypted file closed

Debug         October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": FTP session disconnected

Debug         October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Beginning end-of-job processing

Debug         October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": FTP session already disconnected

Informational                October 18, 2007 5:31:01 PM EDT
Transaction "Out 301": Transaction terminated with an error

Debug         October 18, 2007 5:31:02 PM EDT
Transaction "Out 301": Job ended
```

17.2.4 Decrypt of Multiple Files – File Encrypted with Wrong Key

Date: Thu 10/18/2007 5:38 PM
From: diplomat@coviantsoftware.com
To: ITsupport@coviantsoftware.com
Subject: FAILURE: In 307 failed at October 18, 2007 5:37:39 PM

Inbound transaction

Error during decryption or verification

Source files FTP'd from 75.144.141.131:21/
306.txt.pgp Last modified: 20071018.133643
File size before xfer: 431 File size after xfer: 431
307.txt.pgp Last modified: 20071018.130233
File size before xfer: 431 File size after xfer: 431
308.txt.pgp Last modified: 20071018.133628
File size before xfer: 431 File size after xfer: 431

Decryption key: Integrity_Test_Encrypt
Decryption key used: Integrity_Test_Encrypt_sub Verification key specified: Public_Test_Sign Verification key used: Public_Test_Sign

Decryption or Verification Errors:
306.txt.pgp: Error during decryption or verification - Key with ID 830652EEC97C419B cannot decrypt message with key ID(s): 07C82864FF7B8193

Destination files moved to C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\GlobalScape\Inbound RT Destination
307.txt File size: 44
308.txt File size: 44

Primary archiving skipped

Additional archiving skipped

Audit record written. Record ID = In 30720071018173736359

Log Entries:
Informational October 18, 2007 5:37:36 PM EDT
Transaction "In 307": Begins execution

Informational October 18, 2007 5:37:36 PM EDT
Transaction "In 307": Inbound job started

Debug October 18, 2007 5:37:36 PM EDT
Transaction "In 307": Connected to 75.144.141.131:21 With userID coviant

Debug October 18, 2007 5:37:36 PM EDT
Transaction "In 307": FTP connection verified

Debug October 18, 2007 5:37:36 PM EDT
Transaction "In 307": File type set to ASCII

Informational October 18, 2007 5:37:36 PM EDT
Transaction "In 307": Directory: /Usr/coviant
304.txt.asc
305.txt.pgp
306.txt.asc
306.txt.pgp
307.txt.pgp
308.txt.asc
308.txt.pgp
309.xls

Informational October 18, 2007 5:37:36 PM EDT
Transaction "In 307": Source/destination file pair added to processing list:

306.txt.pgp
306.txt

Debug October 18, 2007 5:37:36 PM EDT
Transaction "In 307": FTP connection verified

Informational October 18, 2007 5:37:37 PM EDT
Transaction "In 307": Directory: /Usr/coviant
304.txt.asc
305.txt.pgp
306.txt.asc
306.txt.pgp
307.txt.pgp
308.txt.asc
308.txt.pgp
309.xls

Informational October 18, 2007 5:37:37 PM EDT
Transaction "In 307": Source/destination file pair added to processing list:
307.txt.pgp
307.txt

Debug October 18, 2007 5:37:37 PM EDT
Transaction "In 307": FTP connection verified

Informational October 18, 2007 5:37:37 PM EDT
Transaction "In 307": Directory: /Usr/coviant
304.txt.asc
305.txt.pgp
306.txt.asc
306.txt.pgp
307.txt.pgp
308.txt.asc
308.txt.pgp
309.xls

Informational October 18, 2007 5:37:37 PM EDT
Transaction "In 307": Source/destination file pair added to processing list:
308.txt.pgp
308.txt

Informational October 18, 2007 5:37:37 PM EDT
Transaction "In 307": 3 source files found

Debug October 18, 2007 5:37:37 PM EDT
Transaction "In 307": Source filename: 306.txt.pgp Last modified: 20071018.133643

Debug October 18, 2007 5:37:37 PM EDT
Transaction "In 307": FTP connection verified

Debug October 18, 2007 5:37:37 PM EDT
Transaction "In 307": File type set to BINARY

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": Encrypted file created and locked: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19293.tmp

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": Sensed armoring: false

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": Verified file created for transaction: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19294.tmp

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Error October 18, 2007 5:37:38 PM EDT
Transaction "In 307": Error during decryption or verification

Cause: diplomat.common.DiplomatException - Key with ID 830652EEC97C419B cannot decrypt message with key ID(s): 07C82864FF7B8193

diplomat.server.pgp.bc.BcUtil.findActualDecryptionKey(BcUtil.java:268)
diplomat.server.pgp.bc.BcDecrypter.decryptAndAuthenticateFile(BcDecrypter.java:150)
diplomat.server.job.DiplomatInboundJob.getDecryptedAuthenticatedFile(DiplomatInboundJob.java:350)
diplomat.server.job.DiplomatInboundJob.run(DiplomatInboundJob.java:128)
java.lang.Thread.run(Thread.java:595)

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": Primary archiving skipped

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": Additional archiving skipped

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": Encrypted file closed

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": Verified file closed

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": Temp encrypted file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19293.tmp

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": Temp verified file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19294.tmp

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": Source filename: 307.txt.pgp Last modified: 20071018.130233

Debug October 18, 2007 5:37:38 PM EDT
Transaction "In 307": FTP connection verified

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Encrypted file created and locked: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19295.tmp

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Sensed armoring: false

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Verified file created for transaction: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19296.tmp

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPCompressedData

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPSignatureList

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPLiteralData

Debug October 18, 2007 5:37:39 PM EDT

Transaction "In 307": File moved for transaction: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\Globalscape\Inbound RT Destination\307.txt

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Primary archiving skipped

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Additional archiving skipped

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Encrypted file closed

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Verified file closed

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Temp encrypted file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19295.tmp

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Temp verified file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19296.tmp

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Source filename: 308.txt.pgp Last modified: 20071018.133628

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": FTP connection verified

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Encrypted file created and locked: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19297.tmp

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Sensed armoring: false

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Verified file created for transaction: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19298.tmp

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPEncryptedDataList

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPCompressedData

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPSignatureList

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": PGPObject: org.bouncycastle.openpgp.PGPLiteralData

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": File moved for transaction: C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\Globalscape\Inbound RT Destination\308.txt

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Primary archiving skipped

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Additional archiving skipped

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Encrypted file closed

Debug October 18, 2007 5:37:39 PM EDT

Transaction "In 307": Verified file closed

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Temp encrypted file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\ftp19297.tmp

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Temp verified file deleted: C:\Program Files\Coviant Software\Diplomat-beta\tomcatWebserver\webapps\diplomat\WEB-INF\temp\auth19298.tmp

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": FTP session disconnected

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Beginning end-of-job processing

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": FTP session already disconnected

Informational October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Transaction terminated with an error

Debug October 18, 2007 5:37:39 PM EDT
Transaction "In 307": Job ended

17.3 Audit Failures

17.3.1 Audit Error Set to Critical

If Treat Failures as Critical is selected, the failure email sent to IT Support includes the full contents of the records that would have been written to the audit database for the transaction in an XML format. If you have a stringent audit requirement, the data from this email can be entered manually into your SQL audit database.

Date: Thu 10/18/2007 5:45 PM
From: diplomat@coviantsoftware.com
To: ITsupport@coviantsoftware.com
Subject: CRITICAL Audit Trail Failure on transaction In 301

October 18, 2007 5:44:42 PM - Error encountered writing audit record for transaction In 301:

SQL Error:

```
<audit id="In 3012007101817444 1406" version="3.5 Beta" buildNumber="20071017" osVersion="">
  <transactionRecord>
    <transactionId>In 301</transactionId>
    <transactionType>Inbound</transactionType>
    <status>Successful</status>
    <statusReason></statusReason>
    <overwrite>true</overwrite>
    <deleteSource>false</deleteSource>
    <logLocation>C:\Program Files\Coviant Software\Diplomat-beta\logs</logLocation>
    <logFilename>Diplomat.20071018.161648.log</logFilename>
    <archive>false</archive>
    <primaryArchive>false</primaryArchive>
    <startTime>1192743881406</startTime>
    <endTime>1192743882125</endTime>
    <sourcePartnerId>Ext FTP</sourcePartnerId>
    <sourcePartnerType>Public</sourcePartnerType>
    <sourcePartnerSaved>true</sourcePartnerSaved>
    <sourceTransportMethod>FTP</sourceTransportMethod>
    <sourceServerAddress>75.144.141.131</sourceServerAddress>
    <sourceServerPort>21</sourceServerPort>
    <sourceServerDirectory></sourceServerDirectory>
    <sourceServerAccount></sourceServerAccount>
    <sourceServerType>Windows/Unix</sourceServerType>
    <sourceServerPassive>true</sourceServerPassive>
    <destinationPartnerId>Inbound Local (trusted)</destinationPartnerId>
    <destinationPartnerType>Trusted</destinationPartnerType>
    <destinationPartnerSaved>true</destinationPartnerSaved>
    <destinationTransportMethod>Local Network</destinationTransportMethod>
    <destinationFileLocation>C:\Program Files\Coviant Software\Beta Test Files\AsciiBinary\Globalscape\Inbound RT Destination</destinationFileLocation>
    <encryptDecrypt>false</encryptDecrypt>
    <signAuthenticate>false</signAuthenticate>
    <asciiArmoring>false</asciiArmoring>
    <sourceFileType>ASCII</sourceFileType>
    <runNow>true</runNow>
    <thirdParty>false</thirdParty>
    <businessEmail>false</businessEmail>
    <itEmail>false</itEmail>
    <pagingType>No Paging</pagingType>
    <clServer>false</clServer>
  </transactionRecord>
  <fileRecord>
    <jobAuditId>In 3012007101817444 1406</jobAuditId>
    <sourceFilename>301.txt</sourceFilename>
    <sourceXferred>true</sourceXferred>
    <sourceFileSize>44</sourceFileSize>
    <sourceAsciiArmored>false</sourceAsciiArmored>
```

```
    <sourceSigned>false</sourceSigned>
    <sourceEncrypted>false</sourceEncrypted>
    <sourceDeleted>false</sourceDeleted>
    <sourceAttemptUnarmor>false</sourceAttemptUnarmor>
    <sourceAttemptDecrypt>false</sourceAttemptDecrypt>
    <sourceAttemptVerify>false</sourceAttemptVerify>
    <destinationWriteAttempted>true</destinationWriteAttempted>
    <destinationWritten>true</destinationWritten>
    <destinationFilename>301.txt</destinationFilename>
    <destinationFileSize>44</destinationFileSize>
    <destinationOverwrite>true</destinationOverwrite>
    <fileStatus>Successful</fileStatus>
    <fileStatusReason></fileStatusReason>
  </fileRecord>
</audit>


diplomat.server.db.sql.DiplomatSqlDB.insert(DiplomatSqlDB.java:511)
diplomat.server.AuditTrailManager.insert(AuditTrailManager.java:129)
diplomat.server.job.DiplomatJob.done(DiplomatJob.java:742)
diplomat.server.job.DiplomatInboundJob.run(DiplomatInboundJob.java:224)
java.lang.Thread.run(Thread.java:595)

sun.jdbc.odbc.JdbcOdbc.createSQLException(JdbcOdbc.java:6958)
sun.jdbc.odbc.JdbcOdbc.standardError(JdbcOdbc.java:7115)
sun.jdbc.odbc.JdbcOdbc.SQLDriverConnect(JdbcOdbc.java:3074)
sun.jdbc.odbc.JdbcOdbcConnection.initialize(JdbcOdbcConnection.java:323)
sun.jdbc.odbc.JdbcOdbcDriver.connect(JdbcOdbcDriver.java:174)
java.sql.DriverManager.getConnection(DriverManager.java:525)
java.sql.DriverManager.getConnection(DriverManager.java:171)
diplomat.server.db.sql.DiplomatTransaction.<init>(DiplomatTransaction.java:67)
diplomat.server.db.sql.DiplomatSqlDB.createTransaction(DiplomatSqlDB.java:889)
diplomat.server.db.sql.DiplomatSqlDB.insert(DiplomatSqlDB.java:484)
diplomat.server.AuditTrailManager.insert(AuditTrailManager.java:129)
diplomat.server.job.DiplomatJob.done(DiplomatJob.java:742)
diplomat.server.job.DiplomatInboundJob.run(DiplomatInboundJob.java:224)
java.lang.Thread.run(Thread.java:595)
```

17.3.2 Audit Error NOT Set to Critical

Date: Thu 10/18/2007 5:43 PM
From: diplomat@coviantsoftware.com
To: ITsupport@coviantsoftware.com
Subject: Audit Trail Failure on transaction In 301

October 18, 2007 5:42:12 PM - Error encountered writing audit record for transaction In 301:

SQL Error:

diplomat.server.db.sql.DiplomatSqlDB.insert(DiplomatSqlDB.java:511)
diplomat.server.AuditTrailManager.insert(AuditTrailManager.java:129)
diplomat.server.job.DiplomatJob.done(DiplomatJob.java:742)
diplomat.server.job.DiplomatInboundJob.run(DiplomatInboundJob.java:224)
java.lang.Thread.run(Thread.java:595)

sun.jdbc.odbc.JdbcOdbc.createSQLException(JdbcOdbc.java:6958)
sun.jdbc.odbc.JdbcOdbc.standardError(JdbcOdbc.java:7115)
sun.jdbc.odbc.JdbcOdbc.SQLDriverConnect(JdbcOdbc.java:3074)
sun.jdbc.odbc.JdbcOdbcConnection.initialize(JdbcOdbcConnection.java:323)
sun.jdbc.odbc.JdbcOdbcDriver.connect(JdbcOdbcDriver.java:174)
java.sql.DriverManager.getConnection(DriverManager.java:525)
java.sql.DriverManager.getConnection(DriverManager.java:171)
diplomat.server.db.sql.DiplomatTransaction.<init>(DiplomatTransaction.java:67)
diplomat.server.db.sql.DiplomatSqlDB.createTransaction(DiplomatSqlDB.java:889)
diplomat.server.db.sql.DiplomatSqlDB.insert(DiplomatSqlDB.java:484)
diplomat.server.AuditTrailManager.insert(AuditTrailManager.java:129)
diplomat.server.job.DiplomatJob.done(DiplomatJob.java:742)
diplomat.server.job.DiplomatInboundJob.run(DiplomatInboundJob.java:224)
java.lang.Thread.run(Thread.java:595)

18 Appendix D: Glossary

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

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

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

Allow Diplomat MFT Scripting Agent or API– Allows an external process to initiate execution of an existing Diplomat MFT transaction.

ASCII Armoring – Data added to an OpenPGP encrypted file to appear that it is an ASCII file.

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

CCC (Clear Command Channel) – Allows login information to be passed in plaintext to FTPS servers.

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

Destination Directory – The directory on a Diplomat Cloud Connector site, a transport server or local network where a transaction file is to be written.

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

Diplomat Cloud Connector –Diplomat Cloud Connector is a very secure, proprietary file transport option with authentication always 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.

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

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

Diplomat MFT REST API – HTTP/S API that enables development or extension of third-party applications to run file transfer jobs and obtain job status from the Diplomat MFT Service.

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

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

Diplomat MFT Service Logon – Windows logon identity for the Diplomat MFT Service on the Diplomat MFT site. Defaults to Local Network.

Diplomat MFT transaction Database – Contains all data needed to create and schedule jobs, including keys, partner profiles, transaction, and configuration data. The transaction database is comprised of a SQL database.

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

Diplomat MFT Web Launch – Diplomat MFT Web Launch runs Diplomat MFT components without needing to install Diplomat MFT Client, Scripting Agent or Job Monitor software on the user's local system.

Encryption Subkey – OpenPGP key used to encrypt or decrypt files.

File Monitoring – Job scheduling type that watches one or more source directories for new files. When a new file is found, a Diplomat job is initiated.

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

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

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

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

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

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

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

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

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

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

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

Merge – Merges data from a Diplomat MFT backup file into the current Diplomat MFT database.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Restore – Restores a Diplomat MFT database from a backup file.

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

SITE Command – Command issued to FTP server before file transfer begins.

SMB (Server Message Block) Server – A network file sharing protocol that allows Diplomat MFT to read and write to files on another computer in same network.

Source Directory – The directory on a Diplomat Cloud Connector site, a transport server or local network where a transaction file is to be picked up.

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

SSH Client Key Pair – Key pair created by Diplomat MFT to be used when FTP over SSH is selected for a partner profile. The SSH public key is exported and sent to the FTP administrator as part of setting up the FTP login account.

SSH Host Key – Fingerprint of SFTP server that can be verified when establishing an SFTP session.

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

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

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