COVIANT Software

USER GUIDE
DIPLOMAT MANAGED FILE TRANSFER
WEB LAUNCH
VERSION 8.1

V8.1

Web Launch

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 Overview

Diplomat MFT Web Launch runs Diplomat MFT components without needing to install Diplomat MFT Client, Scripting Agent or Job Monitor software on a user's local network. The Diplomat MFT Administrator configures a Diplomat MFT Web Launch page and provides the URL to each user needing to run a Diplomat MFT component.

2 Deployment

Diplomat Managed File Transfer is a Java-based, client-server application that runs on Windows and Linux systems.

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, SMB 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 MFT'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.

NOTE: Diplomat MFT Web Launch is ONLY supported with a Diplomat MFT Standard or Enterprise Edition license.

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

3 Configuration

Use the following instructions to configure Diplomat MFT Web Launch.

1. Decide which Diplomat MFT components you would like to have accessible via Diplomat MFT Web Launch.

   By default, the Diplomat MFT Client and Scripting Agent are enabled for web launch in Diplomat MFT Standard Edition. With Diplomat MFT Enterprise Edition, the Diplomat MFT Job Monitor is also enabled.

   NOTE: Diplomat MFT Job Monitor is only available with Diplomat MFT Enterprise Edition.

2. If you have not already, install the Diplomat MFT Service and the components you want to access via Diplomat MFT Web Launch.

   If you need assistance, please refer to the *Quick Start Instructions*.

3. Identify the IP address or domain name of the system running the Diplomat MFT Service.

   It is the same IP address or domain name that is used with an installed copy of any Diplomat MFT component. The IP address or domain name is entered by each user when attempting to start a Diplomat MFT component with web launch. Thus, this IP address or domain name must be accessible from the user's system (e.g., on the same network).

4. Decide which port will be used by Diplomat MFT Web Launch to access the Diplomat MFT Service.

   It is the same port that would be used with an installed copy of any Diplomat MFT component.

   The default ports are 8080 for an SSL-encrypted connection and 8443 for an HTTP connection. We recommend that you support only SSL-encrypted connections with Diplomat MFT Web Launch. If you want to change the default ports, refer to *Changing Diplomat Services Port Numbers FAQ*.

   NOTE: If you change the default ports, please note the port you have selected. You will need to make this change each time you install a new version of Diplomat MFT.

5. Customize the JNLP (Java Network Launch Protocol) file for each component you want to enable.

   By default, three JNLP files are located in the C:\Program Files\Coviant Software\Diplomat-j\tomcatWebserver\webapps\diplomat directory for Windows and opt/Coviant Software/Diplomat-j/tomcatWebserver/webapps/diplomat for Red Hat Linux as follows:

Diplomat Component	JNLP File
Client	sampleDiplomatClient.jnlp
Scripting Agent	sampleDiplomatScriptingAgent.jnlp
Job Monitor	sampleDiplomatJobMonitor.jnlp

   For each component you plan to use, you must customize the Diplomat MFT Web Launch URL in each JNLP file.

   - Open each JNLP file for editing.
   - Locate the following line of code "codebase=https://localhost:8080/diplomat".
   - Replace *localhost* with the IP address or domain name of the system identified above.
   - Replace *8080* with the port number identified above. Diplomat MFT Client, Job Monitor and Scripting Agent use the same port to communicate with the Diplomat MFT Service.
   - If you have selected an unencrypted port, change *https* to *http*.

     NOTE: If you select an SSL-encrypted port, users will see a dialog at the beginning of each web launch session stating that the web site's certificate cannot be verified.
   - Save each JNLP file with a new name that does not include "sample" to prevent the file from being overwritten by a future upgrade.

6. Customize the Diplomat MFT Web Launch page, if desired.

   The default Diplomat MFT Web Launch page, samplediplomatWebLaunch.html, is located in the same directory as the JNLP files. It includes links to the Diplomat MFT Client, Scripting Agent and Job Monitor JNLP files. If you want to disable any of the default Diplomat MFT components from web launch, edit the samplediplomatWebLaunch.html file to remove the links to the Diplomat MFT components you do not want to support.

   You may also customize the web page with your company logo or other content. For additional security, you may choose to change the name of the Diplomat MFT Web Launch page.

   NOTE: The html files are only intended as examples. **You must change the name of the html file before you use it.** If you do not change the filename, it will be overwritten the next time you update Diplomat MFT and any changes you have made will be lost.

7. Send the Diplomat MFT Web Launch URL to users.

   By default, the Diplomat MFT Web Launch URL is https://localhost:8080/diplomat/diplomatWebLaunch.html. If you have changed the IP address/domain, port number or the name of the Diplomat MFT Web Launch page, you would make those changes in the URL you send to users.

   To test the URL, try accessing it from a browser on a system where the Diplomat MFT Service is NOT installed.

   When a user attempts to launch a Diplomat MFT component, they receive the same connection and authentication screen as if the Diplomat MFT component were installed locally.

   NOTE: Users must enter a username and password for authentication when using Diplomat MFT Web Launch. Automatic authentication with the Domain and User ID of the current user without entering username and password is not supported with Diplomat MFT Web Launch.

4 User Set-up

Each user should review the following set-up instructions before attempting to use Diplomat MFT Web Launch.

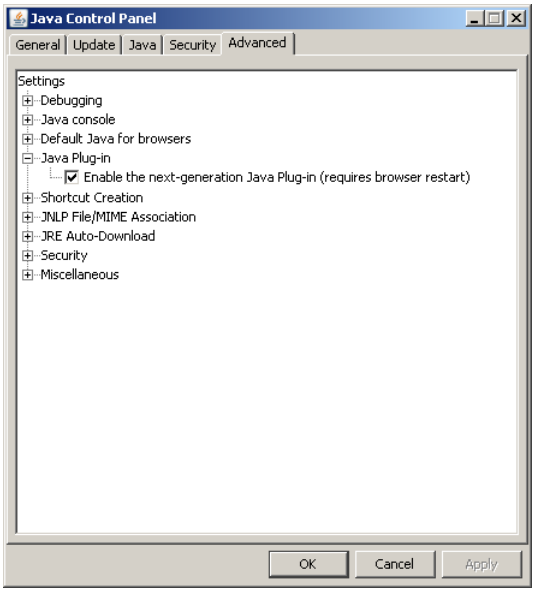
1. Open a browser on a Microsoft Windows system. Diplomat MFT Web Launch has been tested for compatibility with Internet Explorer 9, Chrome v26 and Firefox v20.
2. Check that the Java plug-in for the browser is enabled.

   To confirm the Java plug-in for Firefox, select Tools > Add-Ons from the top menu bar. Select Plugins in the left-hand navigation tree. Confirm that the Java(TM) Platform Next Generation Java Plug-in is enabled.

   To confirm the Java plug-in for Chrome, enter chrome://plugins/ in the URL field. Confirm that the Java(TM) Platform Next Generation Java Plug-in is enabled.

   To confirm the Java plug-in for Internet Explorer, go to the Java Control Panel. In the Java Control Panel, select the Advanced tab. Expand the Java Plug-in and confirm that it has been enabled.

   NOTE: Refer to http://www.java.com/en/download/help/enable_panel.xml if you need assistance locating the Java Control Panel.



3. Check that the user has a Java Runtime Environment (JRE) version 1.8 or later installed on their local system – typically under …/Program Files/Java. To install or update Java, download it from the Oracle Java web site.
4. Each user must define an environment variable named 'DiplomatWebData', which points to a pre-existing, writeable directory. Create a writable directory, such as C:\Coviant Software\DiplomatWebData, before setting the environment variable.

   NOTE: Close all browser windows before updating the environment variable. Changes to environment variables do not take effect until all browser windows have been closed and the browser is restarted.

NOTE: Environment variables can be accessed under Control Panel > System. Select the Advanced tab and then the Environment Variables… button. Add the 'DiplomatWebData' environment variable to the User or System variables table.

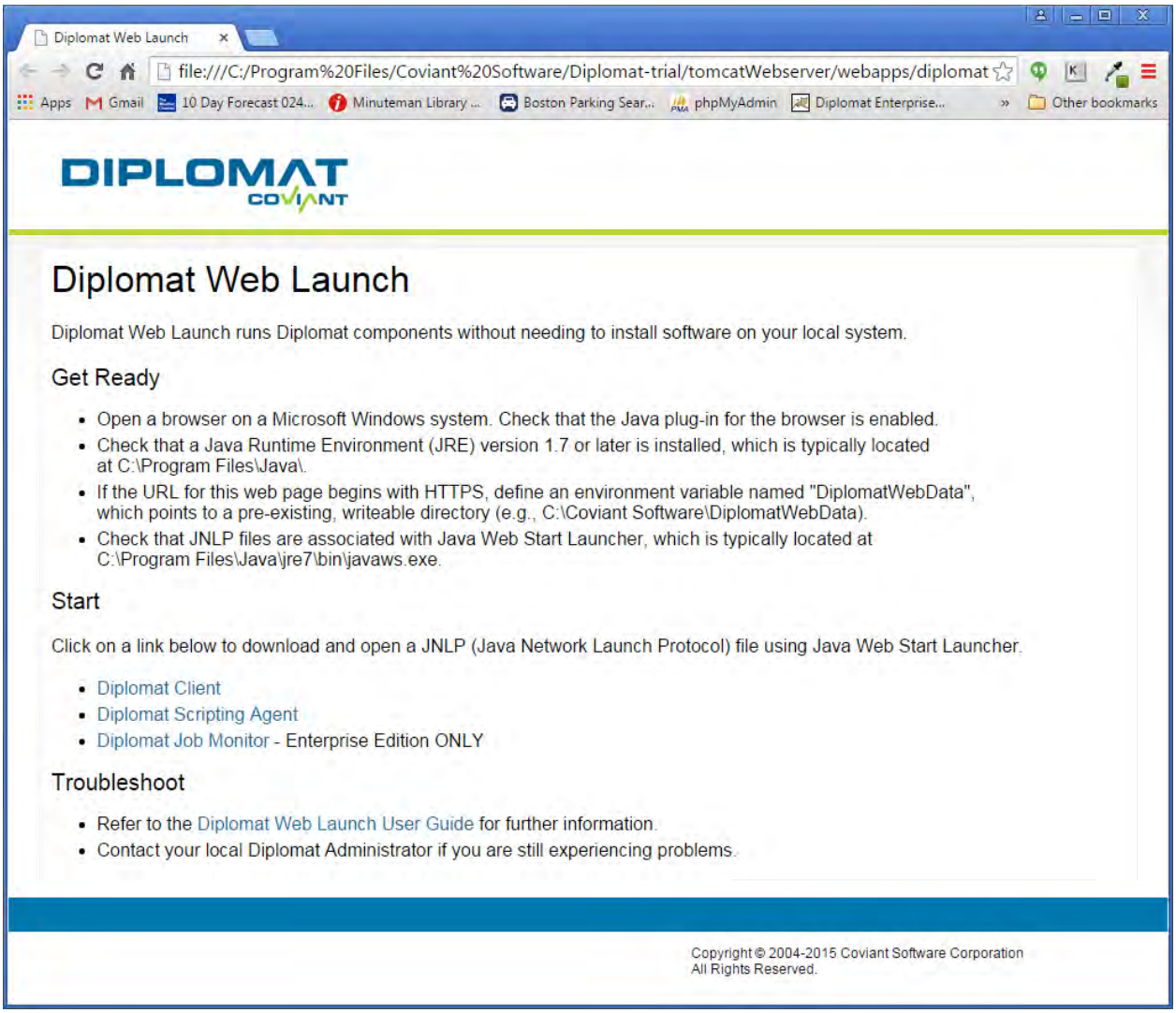
NOTE: Names of environment variables are case sensitive.

5. Check that JNLP files are associated with Java Web Start Launcher, which is typically located at C:\Program Files\Java\jre7\bin\javaws.exe, on the user's local system.

   - For XP, select Start > Control Panel > Tools > Folder Options > File Types. Find the JNLP file type and associate it with Java Web Start Launcher, if needed.
   - For Windows 7, select Start > Default Programs > Associate a file type with a specific program. Find the JNLP file type and associate it with Java Web Start Launcher, if needed.

5 Starting Web Launch

1. Open a browser from a system on the internal network where the Diplomat MFT Service is running. Navigate to the Diplomat MFT Web Launch URL provided by your Diplomat MFT Administrator. The default web page is shown below. Your Diplomat MFT Administrator may have customized your web page.



2. Click on the link for the Diplomat MFT component you would like to start. The JNLP file associated with the Diplomat MFT component is downloaded to your local system and executed using Java Web Start Launcher.

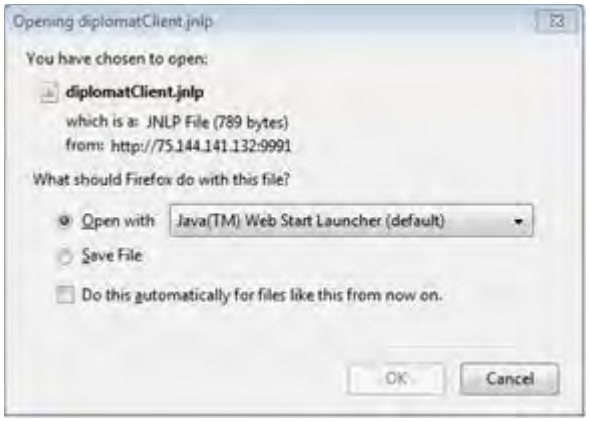
   If you used an SSL-encrypted connection to the Diplomat MFT Web Launch page and an SSL-encrypted port for connections to the Diplomat MFT Service, you will see two warning screens as part of downloading and verifying the JNLP file.

   Examples of starting Diplomat MFT Web Launch from Firefox, Google Chrome, and MS Internet Explorer are provided below. The examples may not match the exact screens displayed when you download a Diplomat MFT Web Launch JNLP file.

5.1 Firefox

Firefox displays the following screens when starting Diplomat MFT Web Launch.

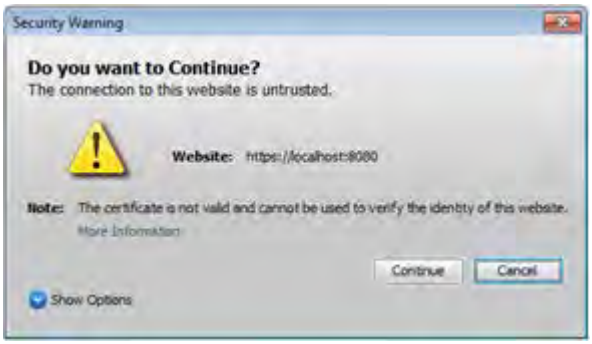
Select "*I Understand the Risks*" to continue.



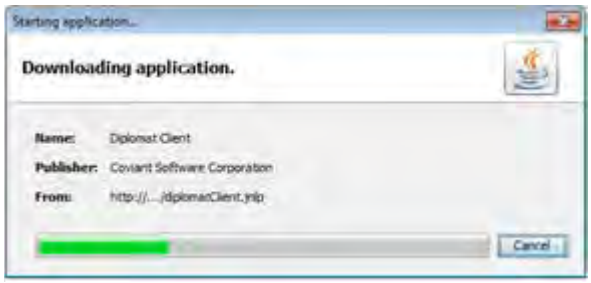
Be sure that Java Web Start Launcher is displayed next to the "*Open with*" button.

You can also check "*Do this automatically for files like this from now on.*" to skip this screen in the future.

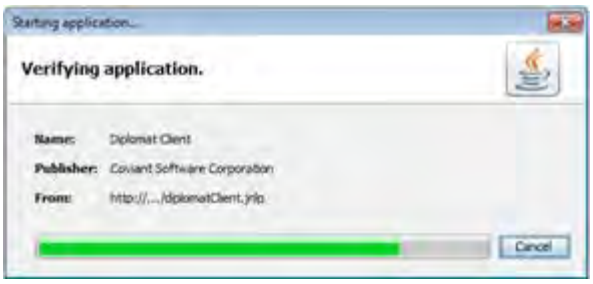
Then, select "*OK*" to continue.



Select "*Continue*".



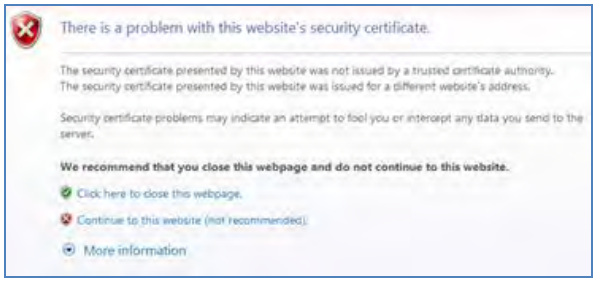
No action needed.



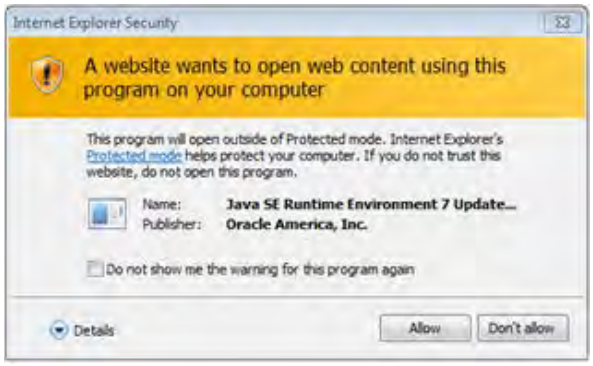
No action needed.

5.2 Internet Explorer

Internet Explorer displays the following screens when starting Diplomat MFT Web Launch.

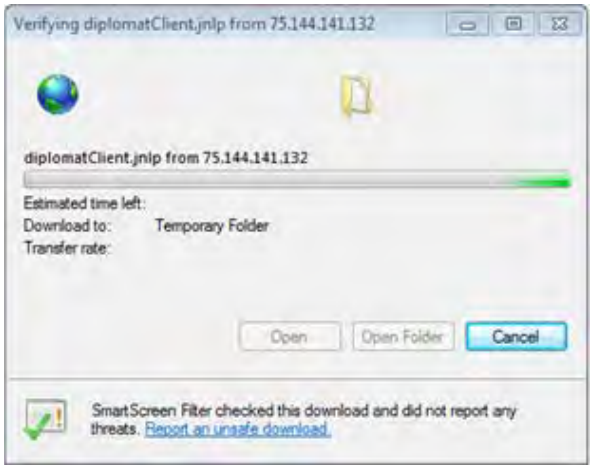


Select "*Continue to this website (not recommended)*".

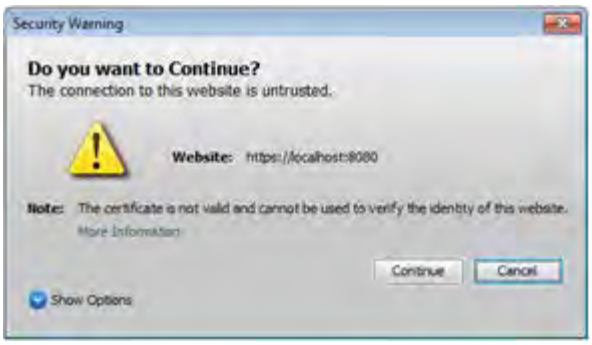


You can check "*Do not show me the warning for this program again*" to skip this screen in the future.

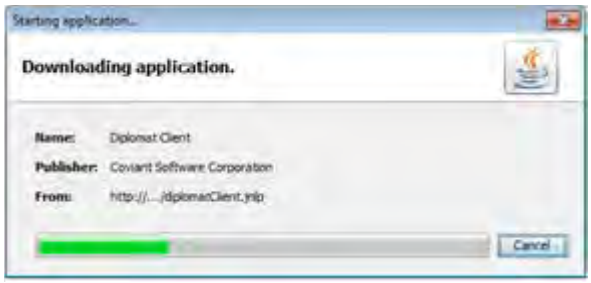
Then, select "*Allow*" to continue.



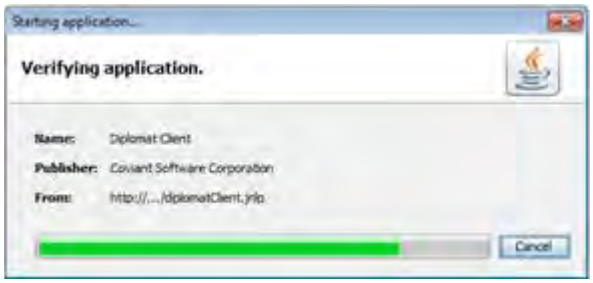
Select "*Open*" to continue.



Select "*Continue*".



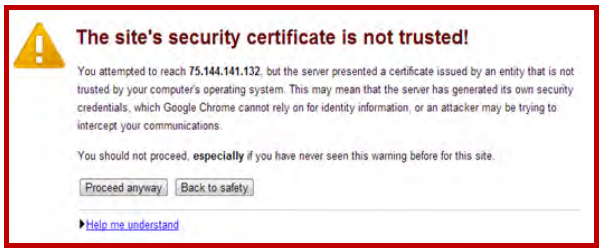
No action needed.



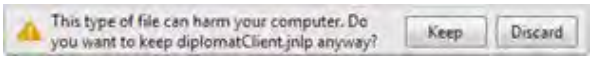
No action needed.

5.3 Chrome

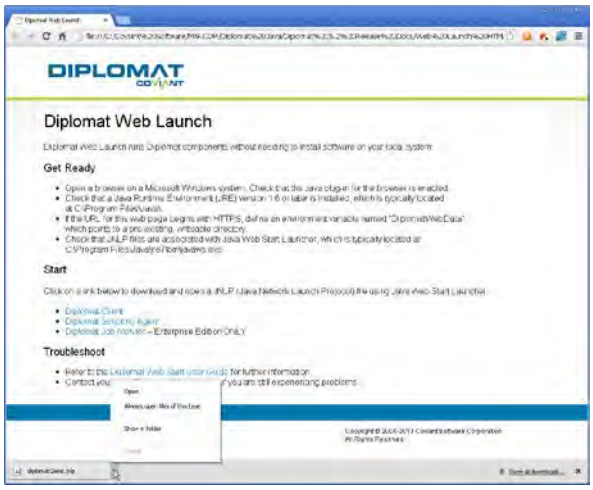
Chrome displays the following screens when starting Diplomat MFT Web Launch.



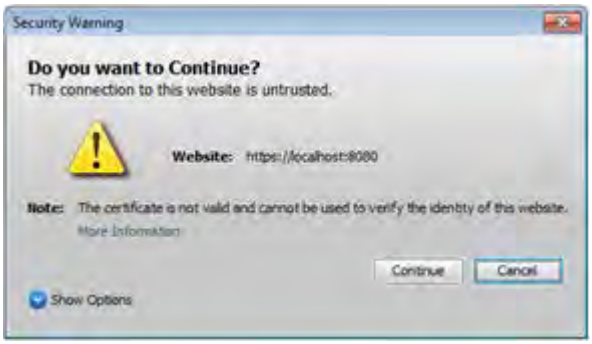
Select "*Proceed anyway*" to continue.



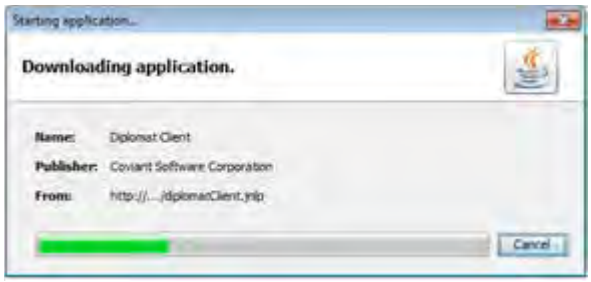
Select "*Keep*" to download the JNLP file.



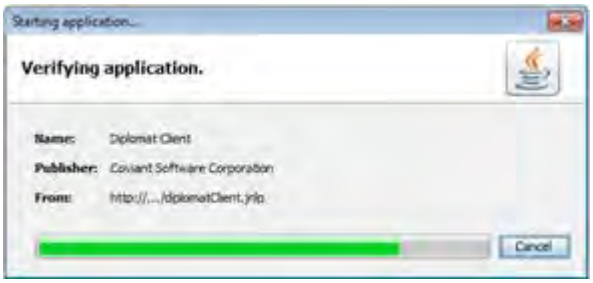
Select "*Open*" to open the JNLP file.



Select "*Continue*".

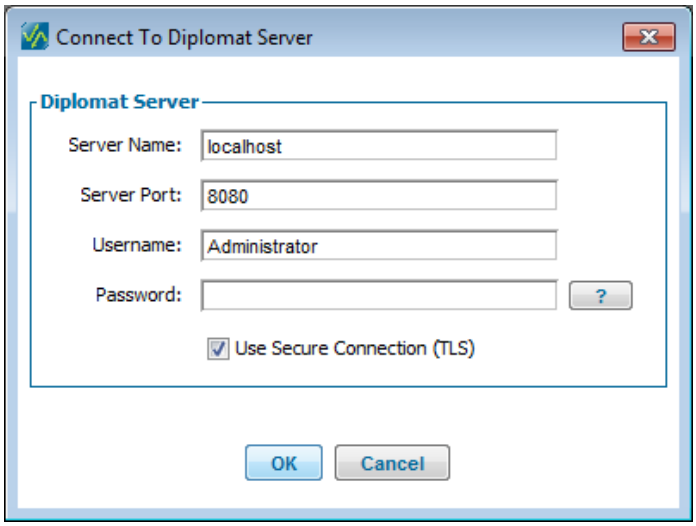


No action needed.



No action needed.

6 Logging On



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

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

6.1 Server Name

Server Name is the IP address or domain of the system running the Diplomat MFT Service or the diplomatServer daemon and configured in the JNLP file.

6.2 Server Port

Server Port is the port configured in the JNLP file.

6.3 Username and Password

Login to the Diplomat MFT component using Diplomat MFT Web Launch requires a username and password combination.

NOTE: Automatic authentication with the Domain and User ID of the current user without entering username and password is not supported with Diplomat MFT Web Launch.

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

NOTE: Passwords are case sensitive.

6.4 Secure Connection

Use Secure Connection (SSL) protects all communication between the Diplomat MFT Service and each Diplomat MFT component using Secure Socket Layer (SSL). Check *Use Secure Connection (SSL)* if the "codebase" is configured to use HTTPS in the JNLP file.

7 Troubleshooting

Most issues with Diplomat MFT Web Launch can be resolved by reviewing the User Set-up instructions above or contacting your Diplomat MFT Administrator.

If a user has trouble downloading the JNLP file from the web page, the file can be sent to them directly. Once the JNLP file is on the local system, the Diplomat MFT component can be started by double-clicking on the file name. The user can also set up a desktop icon to execute the file.

If the user is having trouble executing the file (e.g., the JNLP association to Java Web Start Launcher is not working), the file can be executed at the command line (e.g., "C:\Program Files\Java\jre6\bin\javaws.exe" "C:\Program Files\Coviant Software\Diplomat-trial\tomcatWebserver\webapps\diplomat\sampleDiplomatClient.jnlp").

8 Appendix A: Configuration Requirements

Diplomat MFT components accessed through Diplomat MFT Web Launch have the same configuration requirements as if they were installed applications. Specific software versions tested for Diplomat Managed File Transfer are shown below.

Supported Software	
Diplomat MFT Client[1] Diplomat MFT Job Monitor	Windows 7[2], 8 and 10 (64-bit) Windows Server 2008 R2[2], 2012 R2[2] and 20162 (64-bit)
Diplomat MFT Scripting Agent	Windows 7[2], 8 and 10 (64-bit) Windows Server 2008 R2[2], 2012 R2[2] and 2016[2] (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 later

The hardware configurations shown are based on approximately 50 simultaneous file transfer jobs with associated keys. Your production environment may require less or more memory/disk space depending on the numbers of transactions and keys you use.

Minimum Hardware Configurations		
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

[1] Unix operating systems are not currently supported. Contact Coviant Software Support for further information.

[2] 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.

9 Appendix B: Glossary

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

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

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

Allow Diplomat MFT Scripting Agent or API– Allows an external process to initiate execution of an existing Diplomat MFT transaction.

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

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

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

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

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

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

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

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

Diplomat MFT transaction Database – Contains all data needed to create and schedule jobs, including keys, partner profiles, transaction, and configuration data. The transaction database is comprised of a SQL database.

Diplomat 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.

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.

JNLP File – JNLP (Java Network Launching Protocol) files are used to run Java applications from the web. JNLP files launch Java Web Start software automatically when a Java application using Java Web Start technology is downloaded for the first time. The Diplomat MFT Client, Job Monitor, and Scripting Agent can be started using the JNLP files associated with each Diplomat component.

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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