

DATA SHEET

DIPLOMAT® EBUSINESS SOLUTION

OVERVIEW



McAfee® no longer directly supports E-Business Server. If your business relies on McAfee E-Biz Server, try Diplomat eBusiness Solution to replace PGP command line and simplify encryption and file transfer.

Simplify batch scripts and reduce the complexity of PGP encryption with a one-to-one command replacement for an easy transition to a new OpenPGP command line solution. Diplomat commands execute OpenPGP encryption and additional tasks, such as secure file transfer, file archiving, audit trail and email messages.

FULL OPENPGP SECURITY

Switching to a Diplomat eBusiness Solution (EBS) requires no software changes for your trading partners. PGP keys imported by Diplomat EBS use the preferred algorithms specified in the signature block of the original PGP key for full compatibility with existing trading partners. And, you can import, create and manage OpenPGP keys from a user-friendly administrator console.

You can import your full private and public key rings or import only the PGP keys you need by selecting your key ring and then checking each key you would like to import. And, since Diplomat EBS manages your OpenPGP keys, you no longer need a PGP configuration file or a “PGP home” location.

When you need new OpenPGP keys, Diplomat EBS creates keys with strengths of up to 4096 bits. You can specify the expiration dates of master and sub-keys, including multiple encryption sub-keys which are valid for specific periods of time. The more often your encryption sub-keys change the more secure your data will be, since anyone attacking your key must break the currently-valid sub-key. With multiple encryption sub-keys, your encryption algorithms change on a predefined schedule without reissuing new public keys to your trading partners.

Diplomat eBusiness Solution protects your data by encrypting sensitive data before writing to disk. No

sensitive data is stored in registry entries or batch files. Since Diplomat commands only require a Transaction ID, your pass-phrases, passwords and account logins are decrypted and held in memory only while a file encryption job is running.

For additional security, Diplomat EBS supports secure file transfer protocols, such as FTPS, SFTP and HTTP/S, to protect data in transit.

Import	Key ID	User ID	Diplomat Key Name	Import Key Passphrase
<input checked="" type="checkbox"/>	5FA08EDC206C1F8C	PGPEncrypt1_DSS	PGPEncrypt1_DSS	
<input checked="" type="checkbox"/>	DC1DF10D58E34C6B	PGPSignA_DSS	PGPSignA_DSS	
<input checked="" type="checkbox"/>	886B1F21E409A82A	PGPSignB_DSS	PGPSignB_DSS	
<input checked="" type="checkbox"/>	6907705F69C47317	PGPEncrypt1_RSA	PGPEncrypt1_RSA	
<input checked="" type="checkbox"/>	04978FD3652B1EA9	PGPEncrypt2_RSA	PGPEncrypt2_RSA	
<input checked="" type="checkbox"/>	69450195FF200C4A	PGPSignA_RSA	PGPSignA_RSA	
<input checked="" type="checkbox"/>	1E836A0D7E701CC3	PGPSignB_RSA	PGPSignB_RSA	
<input checked="" type="checkbox"/>	23939F903FE13693	PGPEncrypt_LEG	PGPEncrypt_LEG	
<input checked="" type="checkbox"/>	4EFE7EA599CCDEBA	UnsignedKey	UnsignedKey	
<input checked="" type="checkbox"/>	EC04D42EB45235E8	PGPADK	PGPADK	
<input checked="" type="checkbox"/>	63C65F66175DBA30	PGPEncrypt2_DSS	PGPEncrypt2_DSS	
<input checked="" type="checkbox"/>	B6FB17AD7C412D94	Diplomat	Diplomat	
<input checked="" type="checkbox"/>	DA80C247A0B6453	parreid	parreid	

Source: C:\Program Files\Coviant Software\Diplomat-beta\keys\secring.skr

OK Cancel

Import PGP Keys

FAST MIGRATION

Diplomat eBusiness Solution can be installed in one central location as a hub to encrypt or decrypt files anywhere on your network. No need to install Diplomat EBS on every server.

Diplomat eBusiness Solution's intuitive user interface requires no special skills. Rather than entering detailed parameters into each PGP command, you enter parameters into a Diplomat EBS transaction. When you want to execute the transaction, the only parameter needed is the Transaction ID.

Replace PGP commands in three steps...

1. Set encryption parameters using checkboxes and fill-in-the-blank fields. Control all aspects of an encryption job, such as encryption or signature key, ASCII armoring or conversion to canonical text.

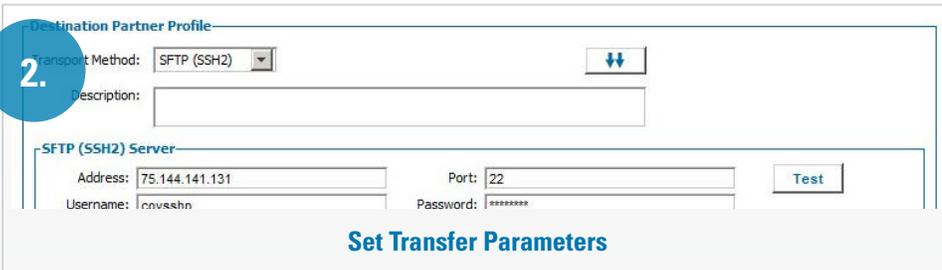


1. File Handling

- Encrypt
- Sign
- Add ASCII Armoring
- Source File Format: ASCII
- Use OpenPGP Command Line Console

OpenPGP Encryption Key: Trading Partner
Additional OpenPGP Encryption Keys (AEKs): <None Selected>
OpenPGP Signature Key: Coviant Key Pair
 Compress
 Convert to Canonical Text
Destination File Format: Binary

Set Encryption Parameters



2. Destination Partner Profile

Transport Method: SFTP (SSH2)

Description:

SFTP (SSH2) Server

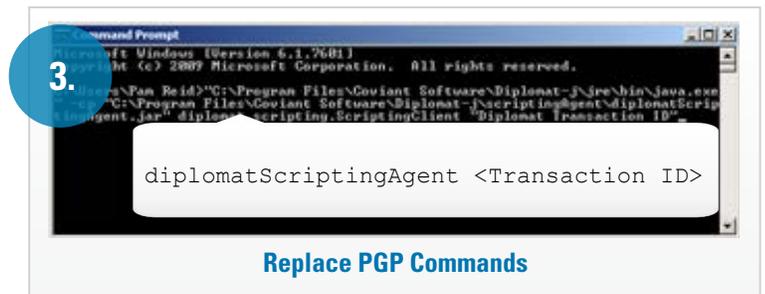
Address: 75.144.141.131 Port: 22 Test

Username: cnvsshin Password: *****

Set Transfer Parameters

2. Set transfer parameters, such as type of FTP server, address, port and login credentials. You can choose any combination of local network, FTP, FTPS, SFTP, HTTP/S, email or SMB for transport.

3. Replace PGP commands using Diplomat commands with a single Transaction ID parameter in your batch scripts. A Diplomat command can encrypt, decrypt and transfers files. Plus, it performs other tasks, such as file archiving, audit trail entries, log entries, email notifications and initiation of other jobs.



3. Command Prompt

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files\Coviant Software\Diplomat>java.exe
"C:\Program Files\Coviant Software\Diplomat\scripting\agent\diplomatScriptingAgent.jar" diplomatScriptingClient "Diplomat Transaction ID"
```

diplomatScriptingAgent <Transaction ID>

Replace PGP Commands

FEWER PROBLEMS / RAPID RESOLUTION

Successful file encryption jobs rely on your internal network, internet connection and other resources being available. A small problem can cause jobs to fail. But these failures are usually preventable. When an error occurs, like a dropped FTP session or a brief network outage, Diplomat eBusiness Solution automatically attempts to recover and complete the job. Most transient problems are addressed and file encryption jobs succeed without manual intervention.

Unlike most PGP command line jobs, Diplomat eBusiness Solution continues processing files when a decryption or other error prevents a file from being processed successfully. If your trading partner uses the wrong OpenPGP encryption key for a file, the other files in the job are processed and you are notified of the one failed file.

When attempting to encrypt and transfer files, unexpected problems often crop up. A file was encrypted with the wrong key. FTP account login credentials are outdated. Files are not ready for pickup. You may have processing deadlines or SLAs to meet. Diplomat EBS helps ensure these technical problems don't become business problems. Diplomat EBS sends notifications that include the detailed information required to address a problem immediately – without searching through log files.

Diplomat eBusiness Solution offers troubleshooting tools to ensure fast problem diagnosis and resolution. Diplomat eBusiness writes set-up and run-time events to a log file. The built-in log viewer makes it easy to locate and view only the log entries you need to diagnose a problem. And, you can turn on advanced troubleshooting to capture more data, such as temporary files, to pinpoint the source of a problem.

REDUCED BUSINESS RISK

REGULATORY COMPLIANCE

Most organizations are required to maintain confidentiality of a variety of data under regulations such as HIPAA, Sarbanes-Oxley and PCI DSS. You must be able to demonstrate that any data transferred outside the company's firewall was secure. The built-in Diplomat audit database puts comprehensive audit data at your fingertips by capturing over 100 data elements for every file encryption job.

User activity tracking is critical to compliance. Diplomat eBusiness Solution makes it easy to know when set-up data has been changed. Diplomat EBS's log file captures comprehensive user activity, such as User ID and IP address, for each update to the Diplomat database. And, each screen displays a timestamp, user ID and user IP address that reflects the last time any data on the screen was modified.

SECURITY BREACH CONTAINMENT

When you or a trading partner has a security breach, immediate control is critical. You need to stop any file transfers that might be compromised, but unaffected transfers need to continue. With Diplomat EBS, you can easily stop specific transfers from executing. When the security issue is resolved, re-enabling each file encryption job is only one click away.

APPLICATION RECOVERY

Diplomat eBusiness is designed for both expected and unexpected disruptions in your production environment. When you need to upgrade your production environment, you can create a single-file backup of Diplomat EBS's internal database and restore it on any other system running Diplomat eBusiness Solution. If your production system goes down unexpectedly, you can have a hot standby Diplomat eBusiness Solution ready to run without a disruption in service.

DATA RECOVERY

As part of a file encryption job, you can archive copies of data files to a central location and, if desired, an additional location. You always have a copy on hand for your own records or to resend to a partner. Archiving to two locations lets you keep one copy accessible to the IT group and another copy for a business group, such as payroll or production.

Archival copies of sensitive files need to be protected. When sending files to a trading partner, you can encrypt files with your own private key pair in addition to your partner's public key in one step. When you use your own key pair as an additional encryption key, you can safely archive encrypted files and decrypt when you need them.

GROWTH PATH

Diplomat eBusiness Solution is packaged as a full version with unlimited OpenPGP keys or a partner version for organizations with a single trading partner. You can add more OpenPGP keys to the partner version as your needs expand. And, Diplomat EBS can be easily upgraded to Diplomat MFT solutions with expanded features.



5-Star Rating
SC Magazine Encryption-in-Motion Test

To learn more call 781.210.3310.

Start Free Trial »

Try Diplomat MFT Standard Edition free for 15 days to see how it works in your environment.

Request Demo »

Schedule a live demo on how to control and monitor your file transfer jobs.

Try Diplomat Online »

Try Diplomat Sandbox to set up file transfer jobs without downloading and installing trial software.

TECHNICAL SPECIFICATIONS

COMPONENT & PLATFORM SUPPORT

Diplomat MFT Service

- Windows 7, 8 and 10 (64-bit)
- Windows Server 2008 R2, 2012 R2 and 2016 (64-bit)
- Red Hat Linux (64-bit; x86)

Diplomat MFT Web Launch

- Any system supporting Java Runtime Environment (JRE) 1.8 or higher

Diplomat MFT Scripting Agent

- Any system supporting Java Runtime Environment (JRE) 1.8 or higher

Diplomat MFT Client

- Windows 7, 8 and 10 (64-bit)
- Windows Server 2008 R2, 2012 R2 and 2016 (64-bit)

FILE TRANSFER SUPPORT

FTP

- FTP (RFC 959)
- FTPS (RFC 2228 with Secure FTP Using TLS)
- SFTP (RFC 4253)

Email

- SMTP (RFC 2821)
- POP3 (RFC 1939)
- IMAP (RFC 3501)

HTTP/S

- HTTP/S (RFC 2616)

SMB

- SMB 1.0, 2.0 and 3.0

OPENPGP ENCRYPTION

Symmetric Algorithms

- AES (up to 256-bit keys)
- Blowfish (up to 448-bit keys)
- CAST5
- DES (56-bit keys)¹
- IDEA (128-bit keys)¹
- Safer (128-bit keys)¹
- Triple DES (up to 168-bit keys)
- Twofish (up to 256-bit keys)¹

Asymmetric Algorithms

- DSA (1024-bit key only)
- El Gamal (up to 4096-bit keys)
- RSA (up to 4096-bit keys)

Hash Algorithms

- MD2¹, MD5
- RIPEMD-160
- SHA-512, SHA-384, SHA-256, SHA-224, SHA-1

Interoperability (RFC2440/4880)

- McAfee E-business Server v8.0 or later
- PGP Command Line v9.0 or later
- Any other RFC 2440 or RFC 4880 OpenPGP-compliant product

¹ Only supports decrypting existing messages encrypted with algorithm or encrypting to existing keys specifying algorithm as preferred cipher.

ABOUT COVARIANT SOFTWARE

Coviant Software has been a trusted provider of OpenPGP encryption, decryption, signing, verification and other OpenPGP features for 10 years. Coviant Software delivers Managed File Transfer solutions to improve the productivity of file transfer administrators. Diplomat Managed File Transfer software uses Intelligent File Transfer™ design with embedded secure file transfer logic, so file transfer experts can quickly design and deploy file transfer jobs with fewer errors and failed transfers.

© 2008-2018 Coviant Software. All rights reserved. Coviant and Diplomat are registered trademarks of Coviant Software Corporation. All other company and product names are trademarks or registered trademarks of their respective owners.



www.coviantsoftware.com