GUIDE

# STORMSHIELD DATA SECURITY ENTERPRISE

# STORMSHIELD DATA MAIL OUTLOOK EDITION

## E-mail security solution

Version 10.1

Document last update: March 29, 2022

Reference: sds-en-sd_mail_outlook-user_guide-v10

# Table of contents

Preface ... 4

1. Introduction ... 5
1.1 General ... 5
1.1.1 Overview ... 5
1.1.2 Supported messaging software ... 5
1.1.3 What is secured ... 6
1.2 Securing your messages ... 6
1.2.1 Public key cryptography ... 6
1.2.2 Encryption ... 6
1.2.3 Digital signatures ... 6
1.2.4 Certificates ... 7
1.2.5 Trust ... 7
1.2.6 Trusted address book ... 8
1.2.7 Revocation control ... 8
1.3 Local protection of your keys ... 8

2. Installing and getting started with Stormshield Data Mail Outlook Edition ... 9
2.1 Required configuration ... 9
2.2 Installing Stormshield Data Mail Outlook Edition ... 9
2.3 Stormshield Data Security menu ... 10
2.4 Connecting to Stormshield Data Security ... 10
2.5 Exchanging certificates ... 12

3. Sending a secure message ... 14
3.1 Adding security options ... 14
3.2 Certificate not found, in error or invalid ... 15
3.3 Several certificates are available ... 16
3.4 Attached certificates ... 16
3.5 Certificates including several e-mail addresses ... 16
3.6 You are not connected to Stormshield Data Security or your session is locked ... 16

4. Reading a secure message ... 17
4.1 Opening a secure message ... 17
4.2 Consulting the security report ... 17
4.3 Answering or forwarding an encrypted message ... 18
4.4 Attached secure messages ... 18
4.5 Messages secured in OpenPGP ... 18
4.5.1 Importing an OpenPGP keyring ... 18
4.5.2 Reading a message secured in OpenPGP ... 18
4.5.3 Reading a message secured in partitioned PGP ... 19

5. Advanced functions ... 20
5.1 Interacting with Stormshield Data Connector ... 20
5.2 Managing signature algorithms ... 20
5.2.1 Signature ... 20
5.2.2 Encryption ... 20
5.3 Detached signature ... 20
5.4 Encryption learning ... 20
5.5 Delegating decryption ... 21

5.6 Transcipherment ..... 21
5.6.1 Principles of transcipherment ..... 21
5.6.2 Transcipherment and co-workers management ..... 22
5.6.3 Using transcipherment ..... 22
5.6.4 Transcipherment limitations ..... 24
5.7 Disabling security ..... 24
5.7.1 Security removal principles ..... 24
5.7.2 Disabling security ..... 24
5.7.3 Limitations when disabling security ..... 25

In the documentation, Stormshield Data Security Enterprise is referred to in its short form: SDS.

# Preface

Stormshield Data Mail Outlook Edition is fully integrated with Stormshield Data Security (public key solutions). This allows you to use an existing account with previously installed keys and certificates in order to access all the Stormshield Data Security components installed on your workstation.

For more information, refer to the *Installation and Implementation guide*.

There are two versions of Stormshield Data Mail:

- Stormshield Data Mail Notes Edition,
- Stormshield Data Mail Outlook Edition, for Microsoft Outlook 2019 and 365 Professional.

# 1. Introduction

This chapter presents the security measures included in Stormshield Data Mail Outlook Edition.

## 1.1 General

### 1.1.1 Overview

Stormshield Data Mail Outlook Edition is a security software product. It adds the following security features to Intranet/Internet messages (e-mail) that you send and receive daily:

- confidentiality: the transmitted message may only be read by the people to whom it is addressed
- integrity: the message cannot be modified during transfer without detection
- sender authentication: the recipient of the message is sure of the identity of the sender

Confidentiality is ensured by encryption of the message.

The integrity of the message and the authentication of the sender are ensured using a digital signature.

Stormshield Data Mail Outlook Edition uses the S/MIME V3 standard: you can exchange secure messages with any correspondent whose messaging software supports the S/MIME V2 or V3 standard.

**CAUTION**
If you attempt to secure a message with the native security functions of your mailer and then with Stormshield Data Mail Outlook Edition, the message with double security measures will not be readable by its recipient.

### 1.1.2 Supported messaging software

Stormshield Data Mail Outlook Edition does not replace your traditional messaging software: it simply adds functionality, ensuring the security of your messages.

Stormshield Data Mail Outlook Edition uses the following technique to secure your messages:

In "integrated" mode, Stormshield Data Mail Outlook Edition is an extension that is integrated into your messaging software. It secures (encrypts and/or signs) and decrypts your messages, not outside of your messaging software as a proxy would do, but directly in the database of your e-mail system.

Messages that you send and receive are thus securely held in your message database.

Stormshield Data Mail Outlook Edition is available as an add-in for the following messaging software:

- Microsoft Outlook 2019 and 365 Professional
- Lotus Notes 8.x and 9.x

Stormshield Data Mail Outlook Edition is compatible with the following e-mail servers:

- Microsoft Exchange Server 2010 SP1/SP2/SP3
- Microsoft Exchange Server 2013 SP1
- Microsoft Exchange Server 2019
- Microsoft Exchange Server 2019

### 1.1.3 What is secured

The S/MIME V3 standard allows the body of a message to be secured, that is, its text and attachments.

However, for S/MIME standards, the header of the message (rfc822 header) is not secured. This header contains the name of the sender, the list of recipients, the transmission date, and especially the subject of the message.

Therefore, even if the message is secured, its subject could have been read and modified over the network. Be careful when you write or read an information in the subject line of a secured message.

## 1.2 Securing your messages

### 1.2.1 Public key cryptography

Stormshield Data Mail uses a cryptography technology called public key.

Each correspondent has a pair of keys: a private key and a public key. The public key is closely guarded by its owner. The public key, by contrast, is freely distributed.

This pair of keys is used for encryption and digital signatures, as explained below.

Stormshield Data Mail can use one of the following:

- a pair of unique keys for encryption and signing
- two different key pairs, one for encryption, the other for signing

### 1.2.2 Encryption

Encryption is a mathematical technique which allows legible messages (plaintext) to be transformed into messages which only designated recipients can decode and read (encrypted).

The sender encrypts messages with the public key of the recipient. The recipient then uses his private key to decipher the message. Since the recipient is the sole owner of the required private key, the sender is assured that the message cannot be read by third parties.

### 1.2.3 Digital signatures

A digital signature is a mathematical "seal" that is imprinted on the message: it guarantees the integrity of the message and the identity of its signatory.

The signatory signs a message with their private key; the recipient verifies the signature with the signatory's public key. Since the signatory is in sole possession of the private key used to sign the message, the recipient is sure that it has been sent by the signatory and that the message has not been modified during its transfer.

> **NOTE**
> Senders will be able to sign an e-mail only if they have a signature key in their key ring. A Stormshield Data Security account which only has en encryption key cannot be used to sign e-mails then.

There are two types of signature: opaque and detached signatures. Stormshield Data Mail Outlook Edition allows sending and receiving e-mails with both types of signature.

Detached signature allows recipients to read the e-mail even if their messaging software does not support S/MIME format or denies opening e-mails with signatures which cannot be checked (if certificates and revocation lists are not available for example).

However a detached signature may be modified when the e-mail is sent. Usually servers do not modify e-mails, but tags can be added and white lines can be added or removed. The signature of the e-mail would then be incorrect.

To know how to enable detached signature, refer to Detached signature.

When a signed e-mail arrives and is opened in the reading pane or in a new window, Stormshield Data Security checks among other things that the sender's e-mail address and the address specified in the associated certificate (in attachment of the e-mail) match. If they do not match, a warning is displayed in the security lower band of the e-mail received.

**NOTE**
If the certificate contains two e-mail addresses separated by a semicolon, the signature of the e-mail is considered as valid, regardless of which address is used by the sender (among the addresses specified in the certificate).

**NOTE**
Only one error is showed in the security report. If several errors or warnings occurred, only the most critical is showed.

### 1.2.4 Certificates

In order to send encrypted messages to correspondents, you need to know the public key of your correspondents. Moreover, in order to check the digitally signed messages, your correspondent needs to know your public key.

Public keys are distributed as certificates. A certificate is an electronic document that links a public key to its owner. Stormshield Data Security manages certificates with the X.509 V3 format.

**IMPORTANT**
In case of encryption key or certificate renewal, the previous encryption certificate and associated key must be kept in the Stormshield Data Security user account in order to be able to decrypt previously-encrypted messages.

For more information on exporting and importing certificates, see the *Installation and Implementation guide*.

### 1.2.5 Trust

A certificate links a public key to an identity. You can only use the certificate if you trust this link.

If, for example, you want to send an encrypted message to Alice, you must be sure that the certificate actually belongs to Alice. If not, there is a risk that the message has not been encrypted with Alice's real key, but with the key of an impostor who can then decipher your message.

Two techniques enable the trust of a certificate to be established:

- inherited trust is based on the principle that if you trust a certification authority, you implicitly trust the certificates that it distributes.

- explicit trust means that you need to verify the origin of the certificate yourself. One way to do this is to check a parallel source of information (telephone, publication, mail, website, etc.).

### 1.2.6 Trusted address book

The management of trusted address books and certificates is described in the *Installation guide*.

Stormshield Data Mail Outlook Edition includes a trusted address book: you can use it to insert the certificates of trusted correspondents and authorities.

If you want to encrypt an email for one or more recipients who are not listed in your trusted address book and you have specified an LDAP directory, this one is automatically queried.

In this case, if the parameter `SilentImportTrustedLdapCert` of the *SBOX.ini* configuration file is set to 1, then the certificates got from the LDAP directory are automatically imported in the trusted address book as long as there is no status error (not revoked or expired).

For more information about this parameter, refer to the [Mail] section in the *Administration guide.*

### 1.2.7 Revocation control

Revocation control checks that a certificate is valid before it is used, i.e. that it has not been revoked. Revocation lists (CRLs) are provided by certification authorities.

Stormshield Data Security automatically downloads revocation lists from the distribution points declared in the certificates or configured in the product revocation controller. You can configure download criteria for each certificate sender (or authority). Revocation lists received are stored locally in a secure database.

For more information on revocation lists, refer to *Installation and Implementation guide*.

## 1.3 Local protection of your keys

Access to your keys is protected. To be able to use your keys you must connect to Stormshield Data Security, a process which involves self-authentication, i.e. proving that you are actually the owner of the keys.

Stormshield Data Security provides two authentication methods:

- by password: you enter an identifier and a password
- by smartcard or cryptographic USB token: you enter the secret code of the card (the PIN, or Personal Identification Number)

Stormshield Data Security provides support for different types of smartcard or USB tokens.

The management of user accounts and logins is described in the *Installation and Implementation guide*.

# 2. Installing and getting started with Stormshield Data Mail Outlook Edition

This chapter presents the required configuration and the installation of the application. It also explains how to getting started with it.

After the installation, Stormshield Data Security automatically starts when turning the workstation on.

To be able to sign and encrypt messages, to read and check secure messages, you must connect to Stormshield Data Security.

To connect to Stormshield Data Security, you must have an “account”. Refer to the *Installation and Implementation guide* and to the *Administration guide* of Stormshield Data Security to create and manage user accounts.

This chapter only describes accounts protected by password. If your account is protected by smartcard or any hardware device, refer to the *Installation and Implementation guide* which describes the common features of the Stormshield Data Security.

## 2.1 Required configuration

For the required configuration, refer to the section **Compatibility** of the Stormshield Data Security 10.1 Release Notes.

200 MB of disk space are needed for the installation of all the Stormshield Data Security components.

The hardware configuration required for the .NET Framework 4.5.2 is:

- Processor: 1 GHz minimum,
- RAM: 512 MB,
- Available disk space for a 32-bit system: 850 MB,
- Available disk space for a 64-bit system: 2 GB.

**NOTE**
Stormshield Data Security is not compatible with the **Fast User Switching** feature.

## 2.2 Installing Stormshield Data Mail Outlook Edition

Stormshield Data Mail Outlook Edition is a component of Stormshield Data Security Enterprise.

You should have a license key, given to you depending on the acquired user's rights when the product was ordered. This license key is requested during setup.

The installation procedure is described in the *Installation and Implementation guide*.

**WARNING**
After installing Stormshield Data Mail Outlook Edition, the first opening of your messaging software can take several dozens of seconds.

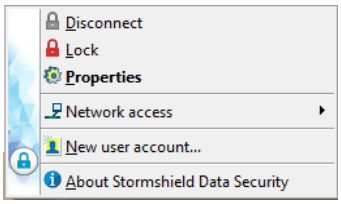
**IMPORTANT**
It is not possible to add other S/MIME addins such as Microsoft MAPI S/MIME AME processor.

## 2.3 Stormshield Data Security menu

All functions relating to your Stormshield Data Security connection can be carried out by right-clicking on the Stormshield Data Security icon on the right of your Windows system tray.

This icon is grayed out when you are not connected, red when the Stormshield Data Security session is locked or green when you are connected.

Right-click this icon to open the Stormshield Data Security menu.

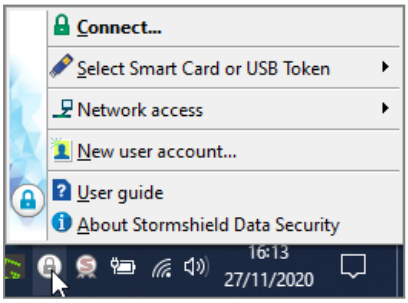



The Stormshield Data Security menu items displayed depends on the different parameters set up during configuration, such as actions for connecting/disconnecting, locking/unlocking, etc.

## 2.4 Connecting to Stormshield Data Security

When you connect to Stormshield Data Security, your identity is verified and your configuration settings are retrieved.

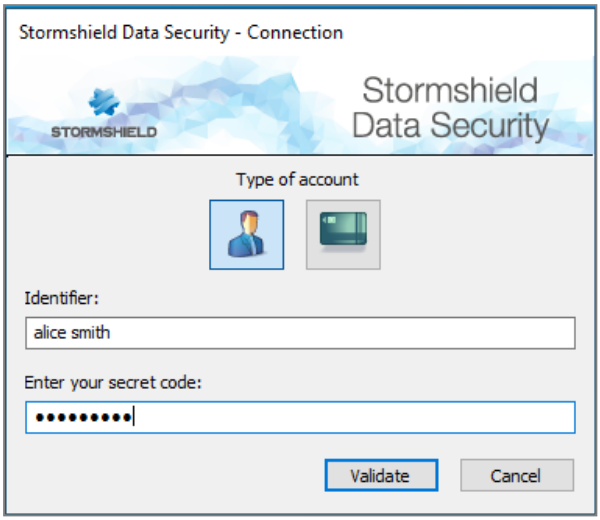
1. To connect to Stormshield Data Security, open the Stormshield Data Security menu (right click on the icon in the Windows system tray) and choose **Connect**:



2. Select the **Account type** with which you want to connect.

For a password account:

a. Enter your login and password:

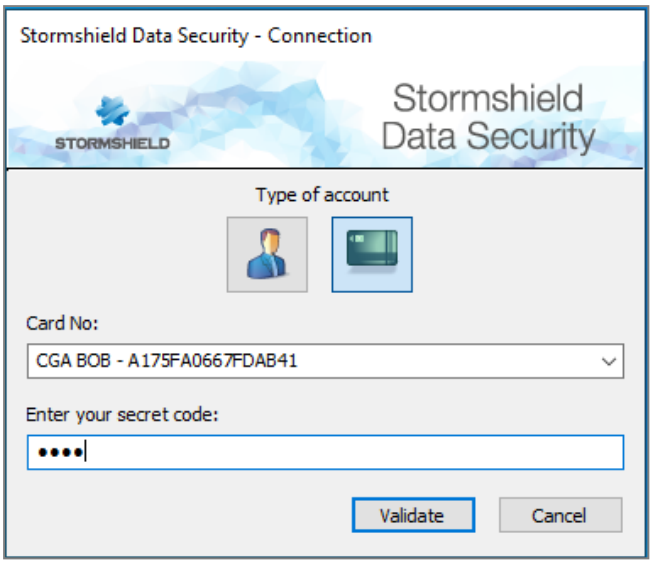



b. Click on **OK**.

c. If the login does not match any existing account, the password field and OK button remain disabled. Create an account in this case. Refer to **Creating an account** in the *Installation Guide*.

For a smart card account:

a. Select the card or token and enter your PIN:




b. Click on **OK**.

c. If the login does not match any existing account, <NO SDS ACCOUNT> will be added before it. Create an account in this case. Refer to **Creating an account** in the *Installation Guide*.

By default, Stormshield Data Security suggests the login of the last connected user.

**CAUTION**
If you enter your password incorrectly too many times (default is three tries), your account will be blocked.

The person icon to the left of the user identifier field is only displayed once Stormshield Data Security finds the account corresponding to the identifier.

Once your connection has been validated, the Stormshield Data Security icon in the system tray turns green: .

You have just opened a Stormshield Data Security session. As long as you remain connected, you may access installed software components from the Stormshield Data Security from your desktop (such as Stormshield Data File, Stormshield Data Virtual Disk, StormshieldData Shredder, Stormshield Data Mail).

## 2.5 Exchanging certificates

In order to send an encrypted message, the sender must know the public key of the recipient which is contained in the recipient's certificate.

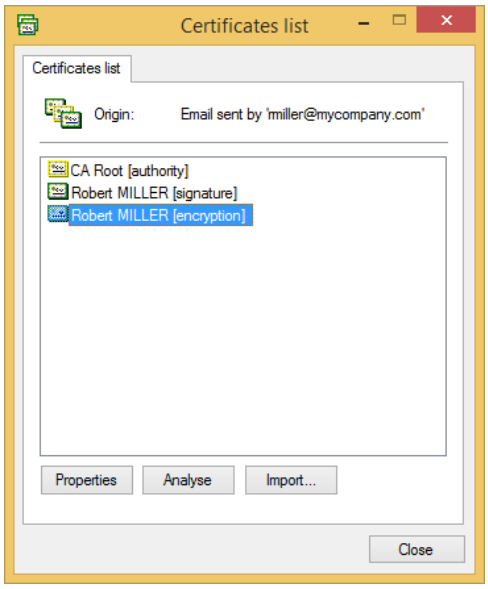
Several methods can be used to obtain recipient certificates:

- use an LDAP directory
- exchange certificates by sending a message
- consult and manage your trusted address book

These methods are described in the *Installation and Implementation guide*.

To exchange certificates by sending a message, follow the procedure below:

1. If your correspondent sent their certificate by signing an e-mail, click the Security report link in the lower band when opening a secure e-mail.
2. In the upper right part of the security report window, click the Attached certificates link to start integrating certificates in your address book.
3. Double-click a certificate to consult the properties.
4. Select one or more certificates to import.




Click Import.

5. Click Next and check the summary. Click Finish.

# 3. Sending a secure message

This chapter explains how to send a secure message using Stormshield Data Mail Outlook Edition.

## 3.1 Adding security options

This section assumes that you are already connected to Stormshield Data Security before sending your message. If this is not the case, refer to You are not connected to Stormshield Data Security or your session is locked.

**IMPORTANT**
Stormshield Data Mail Outlook Edition does not support RTF format because it does not guarantee reliable interoperability with the security mechanism in Stormshield Data Security. Using the RTF format could cause information loss.

HTML is therefore the recommended format for writing secure messages, because there are no interoperability issues with it.

To send a message:

1. Write it as you usually would using your e-mail software.

**NOTE**
If you save your message before sending it (i.e. saving it as a draft), your message is not secured; it is only secured when you send it.

2. You can choose to sign and/or encrypt the message. To do so, in the **Security** zone of the *Message* tab, click on the  icon to sign the message and/or the  icon to encrypt the message.
3. The Stormshield Data Security lower banner appears in the message window and displays the security options you selected.

Click on the **Modify...** link to:

- select the format in which secured messages will be sent – S/MIME or PGP. This option is only available if PGP was configured in SDS. For more information, refer to the *SDS Administration guide*.
- look up and change the available signature algorithms if necessary. For more information about algorithms, refer to Section 5.1, "Managing signature and encryption algorithms".
- enable detached signatures. For more information, refer to Digital signatures.
- enable encryption learning. For more information, refer to the section Encryption learning.
- hide the window asking for confirmation before sending a message in PGP format.

4. Click on **Send**.

Your sent message is stored in your folder (**Sent items** by default), secured with the security options you have selected. If you have selected encryption, the message is automatically encrypted with your own public key. It will be decrypted when you open it. See section Opening a secure message.

**NOTE**
Editing a secured message directly in the outbox is not supported.

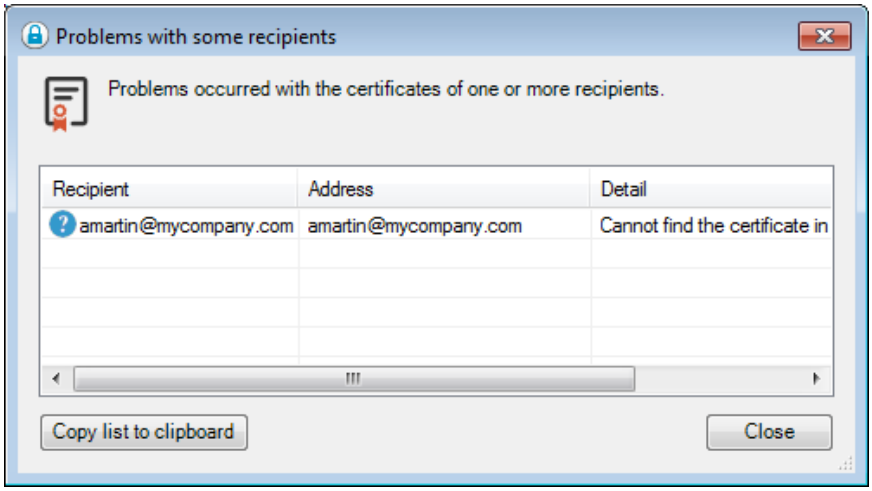
## 3.2 Certificate not found, in error or invalid

If you are encrypting your message, Stormshield Data Mail Outlook Edition searches your trusted address book and, if necessary, the LDAP directories for the certificate of each recipient. It also verifies that the certificate is valid, is authorized for encryption, and presents no unsupported critical extensions (if it does, the certificate is rejected). If one of the recipients is an Outlook contact group or an Exchange distribution group, Stormshield Data Mail Outlook Edition searches all the certificates of the recipients in the group (and in the subgroup if necessary).

**CAUTION**

It is not possible to search the recipients' certificates when sending an e-mail to a dynamic distribution group. Contrary to standard distribution groups which include a defined list of members, the members list of dynamic distribution groups is worked out each time an e-mail is sent to the group.

If any certificates are not found when sending the e-mail, Stormshield Data Mail Outlook Edition displays the affected recipients with the sign.




You have to resolve the certificate(s) issue(s) to be able to send the e-mail. If they are not in your address book, you have to import them. If the recipients are part of a contact group, you can remove the affected recipients.

Stormshield Data Mail Outlook Edition displays the certificates which show a problem (auto-certified certificate, revocation list out of date, etc.) with the warning sign. If, when sending the e-mail, all the certificates display with this warning sign, you can however continue sending the message by clicking Continue or resolve the issues after cancelling sending the message.

If, when sending the e-mail, at least one certificate is in error (out of date, revocated, etc.),

Stormshield Data Mail Outlook Edition displays the affected recipients with the sign. You have to resolve the issues to be able to send the message.

At any time, it is possible to copy the certificates list to clipboard by clicking Copy list to clipboard. It allows you to keep the list in order to resolve the issues later.

**IMPORTANT**
If a co-worker's e-mail address changes (wedding, contractor becoming an employee of the company), it is mandatory to renew the user's certificate (and publish it again on the LDAP address book if needed) so as to the co-worker's e-mail address be identical to the address on their certificate(s). If it is not done, the co-worker will not be able to send secured messages again.

## 3.3 Several certificates are available

If several certificates are available for the same recipient (in your address book or in your LDAP directory(ies)), Stormshield Data Mail Outlook Edition automatically selects the valid certificate which validity start date is the most recent.

## 3.4 Attached certificates

By signing an e-mail, Stormshield Data Mail Outlook Edition makes the exchange of certificates with recipients easier by automatically attaching certificates (signature and/or encryption certificates) and all their trust chain to your secure e-mail. For more information, refer to Section 2.5, "Exchanging certificates".

**NOTE**
Auto-signed certificates are not attached to signed messages.

## 3.5 Certificates including several e-mail addresses

Stormshield Data Mail Outlook Edition supports e-mails encryption for recipients owing several e-mail addresses in their certificates.

If certificates are located in your Stormshield Data Security trusted address book, no configuration modification is needed.

If certificates are not in your trusted address book but are in your LDAP directory(ies), a configuration modification of your LDAP directory(ies) is required.

Please note that you cannot send an encrypted e-mail to a recipient's secondary address defined in the SDAM if this address is not specified in the certificate.

For more information about the modification to do in the LDAP directory, refer to the section *LDAP settings: certificates with several e-mail addresses* in the *Stormshield Data Security Administration guide*.

## 3.6 You are not connected to Stormshield Data Security or your session is locked

If you select a security option (sign and/or encrypt) when you are not connected to Stormshield Data Security or your session is locked, a window displays and prompts you to connect or to unlock your session.

If you click Cancel, the e-mail will not be secure. If you no longer want to secure e-mails, explicitly disable security by clicking the icon and/or the icon .

# 4. Reading a secure message

This chapter explains how to read a secure message using Stormshield Data Mail Outlook Edition.

## 4.1 Opening a secure message

You receive and read messages as you normally would using your messaging software: Stormshield Data Mail Outlook Edition begins "decrypting" all secure messages when you open them. If the message is signed (with or without encryption), Stormshield Data Mail Outlook Edition checks the signature and indicates issues if any.

If you are not connected to Stormshield Data Security, a window displays and prompts you to connect to be able to read the message or verify the signature.

**NOTE**
An encrypted and/or signed *.msg* file cannot be opened from Windows Explorer. For more information, refer to the article in the Stormshield Knowledge Base.

**CAUTION**
You cannot modify a received secured message with the Outlook menu **Actions > Edit Message** because this action could disable the security of the message.

## 4.2 Consulting the security report

When opening a secure message, you can view the security report by clicking the link in the Stormshield Data Security lower band.

**NOTE**
An icon next to the Security report link may indicate an error or a warning detailed in the report if any. If there is an error, the security band is red.

The security report details the algorithms used to encrypt and sign the message.

If the message is signed, the security report also displays:

- the identity of the sender who has signed the message
- an indication of the level of trust assigned to the sender's certificate in the upper band of the report window which indicates:
- the result of the cryptographic verification of the signature: signature correct or incorrect.
- the results of checks carried out on the sender's certificate; Stormshield Data Mail Outlook Edition checks that the certificate is valid, is authorized to sign, and does not present any unsupported critical extensions (if it does, the certificate is rejected).

**NOTE**
Stormshield Data Mail Outlook Edition does not support checking the signature of messages in PGP format (not S/MIME). A message indicating the signature could not be checked will be displayed in the Stormshield Data Security lower band.

## 4.3 Answering or forwarding an encrypted message

When you answer one or more recipients of an encrypted message, the encryption option is automatically selected in the answer message.

This is also the case when forwarding encrypted messages.

## 4.4 Attached secure messages

To be able to read a secure message which is attached to another message (secure or not), you need to drag and drop it to one of the folders of your reception box.

**NOTE**
When receiving e-mails including attachments, Outlook displays the size of the attachments. When the e-mails are encrypted, Outlook always displays “0 bytes”.

## 4.5 Messages secured in OpenPGP

Messages secured by a mail client that supports the OpenPGP protocol (PGP/MIME format) can be decrypted by Stormshield Data Mail Outlook Edition. Decryption keys must be imported into your keyring beforehand in OpenPGP format.

Please refer to the section *OpenPGP decryption keys* in the *Stormshield Data Security Installation and Implementation guide*.

### 4.5.1 Importing an OpenPGP keyring

1. Open the **Stormshield Data Security** menu.
2. Select **Properties**.
3. Click on the *Configuration* tab.
4. Select the **Keyring** icon.
5. Select the *OpenPGP keyring* tab.
6. Click on **Operations** then on **Import a keyring**.
7. Select a file in OpenPGP format (*.gpg*, *.pgp*or *.asc*). The file may contain several keys.
8. Enter the password that protects the file.

To delete or replace the keyring, select the menus **Delete the keyring** or **Replace the keyring** in the **Operations** menu.

Replacing a keyring overwrites the existing keyring.

### 4.5.2 Reading a message secured in OpenPGP

You receive and read messages as you normally would using your messaging software: Stormshield Data Mail Outlook Edition begins "decrypting" all secure messages when you open them.

If you are not connected to Stormshield Data Security, a window appears and prompts you to connect to be able to read the message.

**NOTE**
Stormshield Data Mail Outlook Edition does not support the verification of the signature of messages signed in PGP format. A message indicating that the signature could not be verified will appear in the security banner for such messages.

### 4.5.3 Reading a message secured in partitioned PGP

The Partitioned PGP format is the predecessor of the PGP/MIME format. Both formats rely on the same security mechanisms so the keyring format is the same.

Messages secured in Partitioned PGP are read in the same way as messages in PGP/MIME format.

# 5. Advanced functions

This chapter covers advanced functions of the Stormshield Data Mail Outlook Edition, and is recommended for expert users.

## 5.1 Interacting with Stormshield Data Connector

If the Stormshield Data Connector module has been installed on the machine, you can send encrypted and/or signed messages from a PowerShell script or a .NET program.

Please refer to the Stormshield Data Connector User guide for further information.

## 5.2 Managing signature algorithms

It is possible to modify the default Stormshield Data Mail Outlook Edition signature algorithms when writing a new message. Click the Modify link at the right of the Stormshield Data Security lower band in the message editing window.

### 5.2.1 Signature

In the **Hash algorithm** drop-down list, select the algorithm to sign the message: SHA-1 (selected by default) or SHA-256.

If you have the Stormshield Data Authority Manager administration tool, you can change the default algorithm.

### 5.2.2 Encryption

In the **Algorithm/Length** drop-down list, select the algorithm to encrypt the message: AES 256 (selected by default) or Triple DES 192.

If you have the Stormshield Data Authority Manager administration tool, you can change the default algorithm.

An encrypted message can be decrypted with any messaging software with Stormshield Data Mail Outlook Edition, regardless of the algorithm used. However, if the recipient does not have Stormshield Data Mail Outlook Edition, it is possible that some old messaging software do not decrypt the AES 256 algorithm.

## 5.3 Detached signature

To enable detached signature, click the **Modify** link at the right of the Stormshield Data Security lower band in the message editing window.

For more information about detached signature, refer to Digital signatures.

If you have the Stormshield Data Authority Manager administration tool, you can enable this option by default.

## 5.4 Encryption learning

Encryption learning is a mechanism able to detect the user's habits about e-mail encryption.

When learning is enabled and the user writes an e-mail to someone specific, Stormshield Data Security works out how often a secured e-mail is sent to this recipient.

Since logging is enabled (with 90 days as a maximum), if at least three encrypted e-mails have been sent to this recipient, the next new e-mails to this recipient will be automatically encrypted.

The user can manually disable encryption if needed. In this case, automatic encryption is temporarily disabled for the e-mail being edited. The user will then need to manually enable encryption again if needed.

- To enable learning, click the **Modify** link at the right of the Stormshield Data Security lower band in the message editing window.

Learning can be reset in security options.

## 5.5 Delegating decryption

Delegating decryption involves allowing somebody else (your secretary, for example) to decrypt your messages in your absence. To do this, you need to entrust your personal key (if you only have one key for signing and encryption) or your encryption key (if you have two different keys for signing and encryption) to the delegated person.

Note that with the key provided, the delegated person will only be able to decrypt your messages: they cannot sign in your name. This assumes that the key is a decryption key (not a signature key) or that the key was imported as a decryption key and the PKCS#12 file is not available to the person with the delegation.

To delegate decryption, you must export the key used for encryption from your security account, in order to import it to the machine and in the security account of the person to whom you will be entrusting the key.

To export your security key, refer to the *Installation and Implementation guide*.

## 5.6 Transcipherment

### 5.6.1 Principles of transcipherment

Transcipherment makes it possible to update the protection level of secured messages (S/MIME format messages or plain text messages including an attachment encrypted with the Stormshield Data Mail Outlook Edition component). It consists of re-encrypting with your new key any message encrypted with a former encryption key and by using the default encryption algorithm defined in the user account.

The former encryption key may be out of date for the following reasons:

- The encryption key has been renewed.
- The user account has been updated and the encryption key became unusable (change from a password account to a smart card account, key revocation, key coming from another encryption system).
- The encryption key was sent by a third party (for example when privileges are transferred during a transition to a new position).

To transcipher a secured message, the former encryption key is needed in order to decrypt the message first. The key must be in the keycase as a decryption key.

Once the message is transciphered, only the new key is able to decrypt it.

Messages and attachments are transciphered to their original formats: if they are in .sbox, they will remain in .sbox after transcipherment.

**NOTE**
A delegation key cannot be used for transcipherment because it only allows secured messages to be read.

### 5.6.2 Transcipherment and co-workers management

In these two cases, the transcipherment process works as follows:

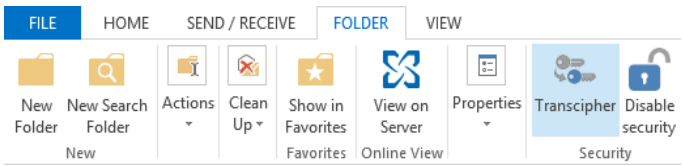
- When a S/MIME secured message received by several co-workers is transciphered, it is then secured only for the current user. Co-workers are not impacted, only the local personal copy of the message is transciphered.
- When a plain text message with a .SBOX secured attachment is transciphered, only the security level of the attachment is updated. If the attachment is forwarded to co-workers declared in the .SBOX original file and their certificates are still valid, they will still be able to access the attachment.

Recovery accounts associated to user accounts are always included to transciphered messages.

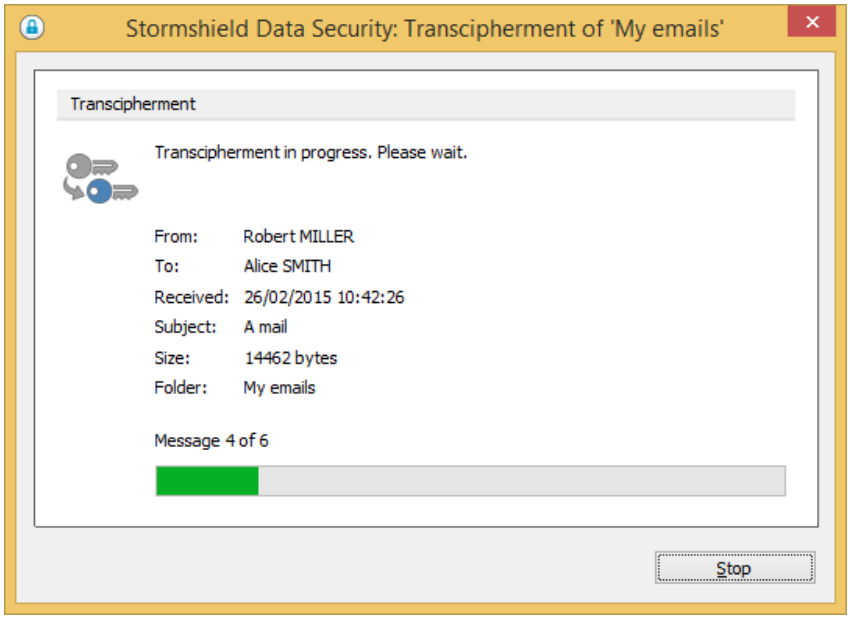
### 5.6.3 Using transcipherment

Transcipherment applies to a folder and its subfolders.

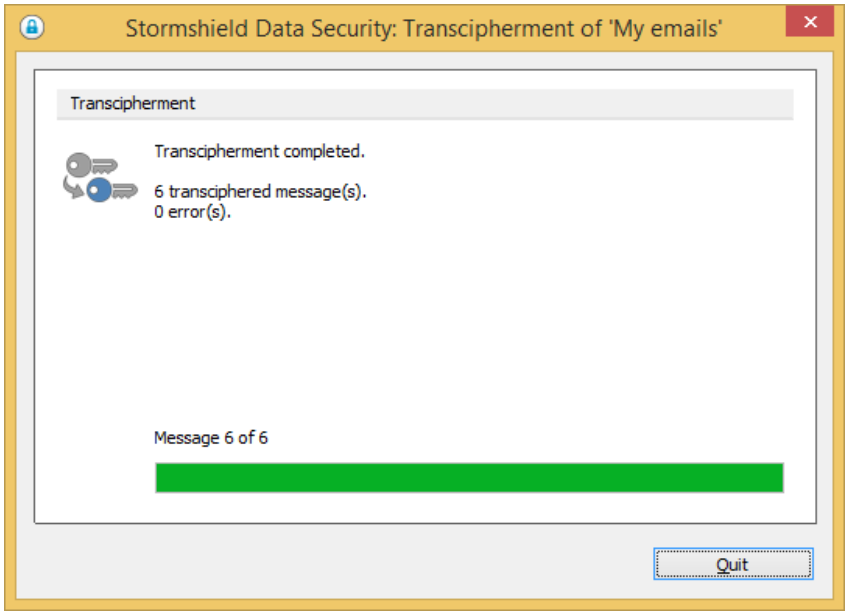
1. Select the folder you need to transcipher.
2. Right-click on the folder to display the contextual menu and select Transcipher or click on Transcipher from the Folder tab on the main ribbon.




3. In the transcipherment window, click Transcipher. During processing, information enables to follow the progress of the operation.




4. When finished, a report displays the number of transciphered messages and the numbers of errors. Click View report in case of error.




The report gives details about the error type for each message:

- The user does not have a valid encryption key.
- The user only owns a delegation key.
- The processing of the message engendered an error.
- The Stormshield Data Mail Outlook Edition component is not installed (in the case the message contains a .SBOX secured attachment).

The report file's name is SBoxTranscipherMentReport-<user>-<timestamp>.txt. It is kept in the temporary folder of the user.

**IMPORTANT**
You need to be connected to your Stormshield Data Security account during transcipherment to access private keys.

The progress window prevents any interaction with Microsoft Outlook during the process. If transcipherment is interrupted for any reason, you need to start it again manually.

### 5.6.4 Transcipherment limitations

Some configurations of encrypted messages are not supported by the transcipherment process:

- A .SBOX attachment included in a S/MIME secured message is not transciphered.
- A secured message sent as a .MSG attachment in a plain text message is not transciphered.

Transcipherment is not possible on messages encrypted with the OpenPGP protocol.

## 5.7 Disabling security

### 5.7.1 Security removal principles

By default, secure messages that you receive are stored as secure messages in the database of the e-mail client.

It is possible that you may not want to store messages in a secure format, for example if you want to put the message into a public folder.

When disabling security, encrypted and/or signed e-mails will be stored in plain- text mode, without encryption or signature.

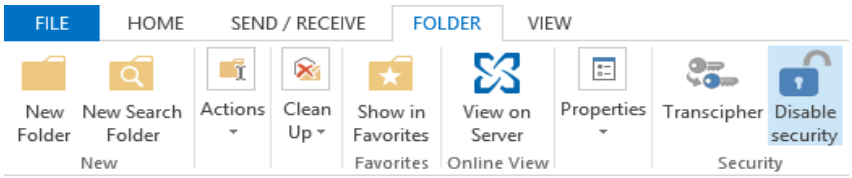
**CAUTION**
A delegation key cannot be used to remove security.

### 5.7.2 Disabling security

The security can be disabled on a folder and all its sub-folders or on a selection of e-mails.

To disable security on a folder:

1. Select the folder.
2. Right-click the folder to display the contextual menu and select **Disable security** or click **Disable security** on the *Folder* tab from the main ribbon.




3. In the security disabling window, click **Disable security**. Information about the operation is displayed during the process.
4. At the end of the process, a report shows the number of unsecured messages and the number of errors. If errors occurred, click **View report**.

To disable security on a selection of e-mails:

1. Select one or more e-mails.
2. Right-click the selection to display the contextual menu and select **Disable security** or click **Disable security** on the *Home* tab from the main ribbon.
3. The following steps are the same than in the procedure above.

The report gives details about the errors for each e-mail impacted:

- The user does not have a valid encryption key.
- The user only has a delegation key.
- An error occurred during the processing of the message.

The report file is named *SBoxDeleteSecurityReport- <timestamp>.txt* and is stored in the temporary folder of the user. The file remains in this folder.

E-mails on which errors occur are usually encrypted e-mails which use an unknown key (for example, an old key which has not been imported as a decryption key in your account).

> **IMPORTANT**
> Users need to be connected to their Stormshield Data Security account when disabling the security on e-mails so that private keys can be accessed.

The progress window prevents any interaction with Microsoft Outlook during the process. If the security disabling process is even though interrupted, the user must manually restart the process.

### 5.7.3 Limitations when disabling security

The security cannot be disabled on some e-mail configurations:

- The security of a secured e-mail sent as an attachment *.msg* of a plain-text e-mail or a secured e-mail cannot be disabled.
- The security of an e-mail encrypted and signed or only signed with the OpenPGP format cannot be disabled.

documentation@stormshield.eu