



STORMSHIELD



GUIDE

**STORMSHIELD DATA SECURITY
ENTERPRISE**

STORMSHIELD DATA MAIL NOTES EDITION

E-mail security solution

Version 10.1

Document last update: March 29, 2022

Reference: sds-en-sd_mail_notes-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 5
 - 1.2 Securing your messages 6
 - 1.2.1 Public key cryptography 6
 - 1.2.2 Encryption 6
 - 1.2.3 Certificates 6
 - 1.2.4 Digital signatures 6
 - 1.2.5 Trust 7
 - 1.2.6 Trusted address book 7
 - 1.2.7 Revocation control 7
 - 1.3 Local protection of your keys 7
- 2. Installing Stormshield Data Mail Notes Edition 9
 - 2.1 Required configuration 9
 - 2.2 Installing Stormshield Data Mail Notes Edition 9
 - 2.3 Exchanging certificates 9
- 3. Getting started with Stormshield Data Mail Notes Edition 10
 - 3.1 Stormshield Data Security menu 10
 - 3.2 Connecting to Stormshield Data Security 10
 - 3.3 Pre-selected security settings 12
 - 3.3.1 Pre-selection by recipient 13
 - 3.3.2 Management rules 14
 - 3.4 Prohibited destinations 15
 - 3.5 Defining display parameter on connection request 16
- 4. Sending a secure message 17
 - 4.1 Entering security options 17
 - 4.2 Certificate not found or invalid 18
 - 4.3 You are not connected to Stormshield Data Security or your session is locked 19
- 5. Reading a secure message 20
 - 5.1 Opening a secure message 20
 - 5.2 Deleting security from a message 21
 - 5.2.1 Manually deleting security from a message 21
 - 5.2.2 Automatically deleting security from a message 21
 - 5.3 Consulting the security report 22
- 6. Advanced functions 23
 - 6.1 Managing your algorithms 23
 - 6.1.1 Signature 23
 - 6.1.2 Strong encryption and weak encryption 25
 - 6.2 Notes edition settings 26
 - 6.2.1 Entering security options 27
 - 6.2.2 Security report 27
 - 6.2.3 Storage of secure messages 27



6.3 Delegating decryption 28

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



Preface

Stormshield Data Mail Notes 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 Notes Edition.

1.1 General

1.1.1 Overview

Stormshield Data Mail Notes 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 Notes 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 Notes Edition, the message with double security measures will not be readable by its recipient.

1.1.2 Supported messaging software

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

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

In "integrated" mode, Stormshield Data Mail 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 is available as an add-in for the following messaging software:

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

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 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.

i 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*.

1.2.4 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.

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 Notes 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 Stormshield Data Mail Notes Edition

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.

! CAUTION

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

2.2 Installing Stormshield Data Mail Notes Edition

Stormshield Data Mail Notes 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 Notes Edition, the first opening of your messaging software can take several dozens of seconds.

i IMPORTANT

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

2.3 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:

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

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



3. Getting started with Stormshield Data Mail Notes Edition

Stormshield Data Security launches automatically when your system starts up.

To be able to sign and encrypt messages, and send and decrypt secure mail, you need to install Stormshield Data Mail Notes Edition and connect to Stormshield Data Security.

To connect to Stormshield Data Security, you need to have an "account". The account creation and management procedure is described in the *Installation and Implementation guide*.

This chapter only applies to password-protected accounts. If you use some physical authentication device (smartcard, USB key), refer to the *Installation and Implementation guide*.

3.1 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.

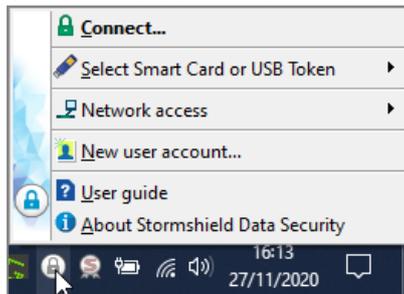


The Stormshield Data Security menu items displayed depends on the different parameters set up during configuration, such as actions for connecting/disconnecting, locking/unlocking, etc.

3.2 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:

Stormshield Data Security - Connection

Stormshield Data Security

Type of account

Identifier:
alice smith

Enter your secret code:
●●●●●●●●

Validate Cancel

- 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:

Stormshield Data Security - Connection

Stormshield Data Security

Type of account

Card No:
CGA BOB - A175FA0667FDAB41

Enter your secret code:
.....

Validate Cancel

- 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).

3.3 Pre-selected security settings

You can configure the default security settings in one of the following ways:

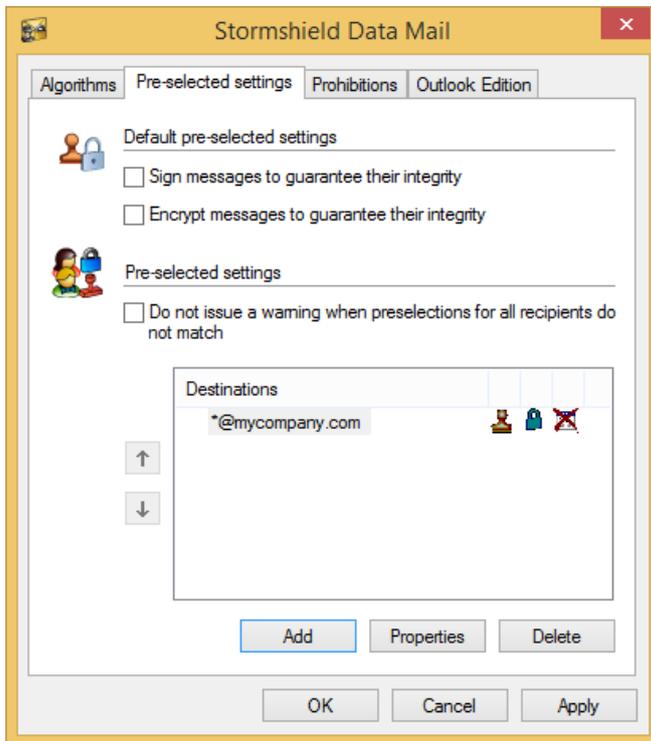
- globally for all of the messages you send
- according to the recipients of the message

To do this:

1. Open the Stormshield Data Security menu.
2. Choose Properties.
3. Select the Configuration tab.



4. Click on the Stormshield Data Mail Notes Edition icon.
5. Select the Pre-selected settings tab:



3.3.1 Pre-selection by recipient

You can configure Stormshield Data Mail so that a message's security settings are pre-selected depending on its recipient. You can also request that these options are applied automatically, without requiring your confirmation.

For example, you can:

- automatically sign and encrypt messages addressed to your headquarters
- automatically sign messages addressed to some of your suppliers
- neither sign nor encrypt messages that are addressed to your private correspondents, while at the same time giving you the possibility to edit these two options

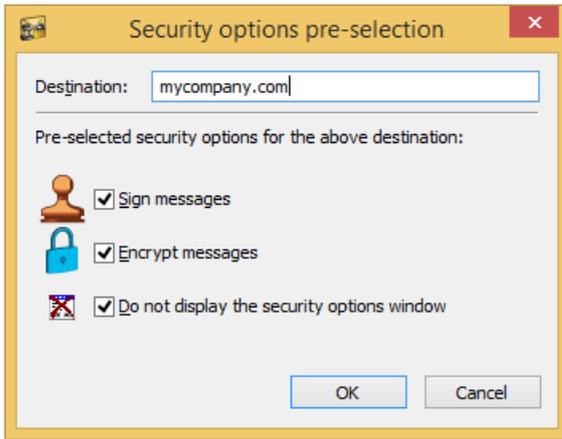
Use the Destination option to pre-select your security options. A destination is an e-mail address filter: a pre-selection is applied if a recipient's e-mail address satisfies the filter for the relevant destination. You can use the "*" character to represent an entire sequence of characters and "?" to represent just one character.

For example, if mail addresses at your company's headquarters all end with "@hq.company.com", you can define the destination "*@hq.company.com" and apply signature and encryption options to it.

A destination can thus, for example, be a domain name instead of being a complete e-mail address.

To define a pre-selection:

1. Go to the Pre-selected settings tab.
2. Click Add from the list of pre-selections. The following screen is displayed.



3. Enter the destination (e-mail address suffix) in the Destination field.
4. Select the security options that you want to apply to this destination:
 - Sign messages
 - Encrypt messages

You can select one or both of these options.

5. Select the option Do not display the security options window if you want these security options to be automatically applied to messages addressed to this destination, without requiring your confirmation.

Deselect this option if, alternatively, you want to be able to edit security options before messages are sent.

6. Click OK to confirm.

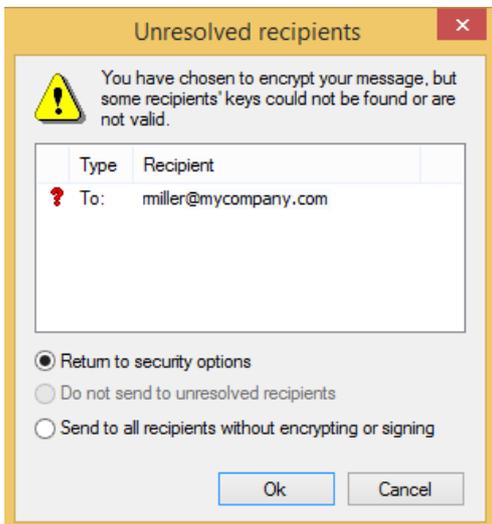
The first destination on the list is applied to a recipient. To change a destination's position in the list, use the arrows on the right of the list.

3.3.2 Management rules

An option (sign or encrypt) is pre-selected (selected) if it is requested for at least one recipient.

The security options window is displayed if it is requested for at least one recipient.

If the application encounters a processing error when operating in pre-selections mode (for example if you have requested encryption when you do not have the certificates of all recipients), Stormshield Data Mail Notes Edition displays the following window.





You must choose one of the following options:

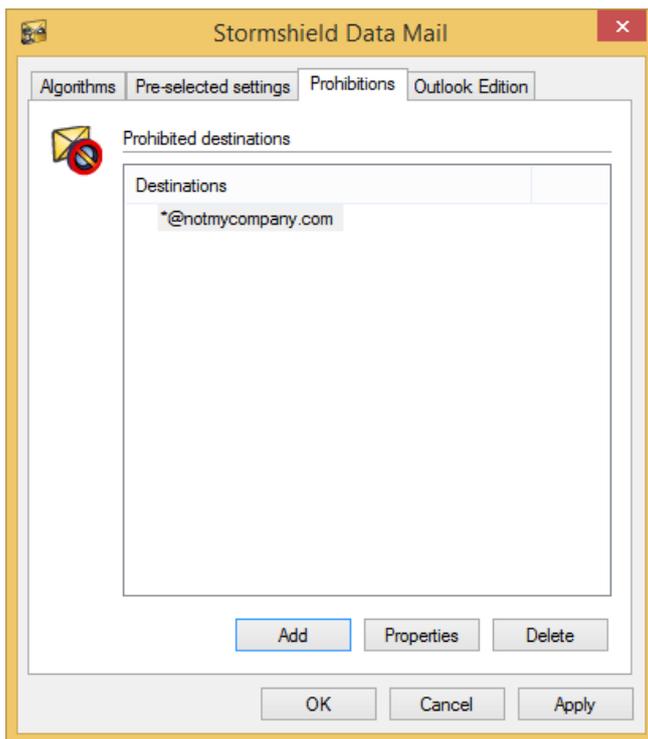
- Return to the security options
- Do not send to unresolved recipients: the mail will only be sent to recipients with valid certificates
- Send to all recipients without encrypting: the message will be sent in plaintext to all recipients

3.4 Prohibited destinations

You can prevent messages being sent to certain destinations or e-mail addresses (refer to [Section 3.3.2, "Pre-selection by recipient"](#)).

To do this:

1. Open the Stormshield Data Security menu.
2. Choose Properties.
3. Select the Configuration tab.
4. Double-click on the Stormshield Data Mail Notes Edition icon.
5. Select the Prohibitions tab.



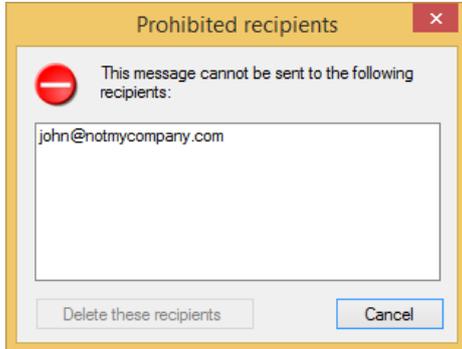
6. Click Add.
7. Enter the e-mail address in the Destination field of the following screen.

You can use the "*" character to represent an entire sequence of characters and "?" to represent just one character.

**i NOTE**

Prohibition rules take precedence over preselection rules. This means if a recipient is included in a preselection and in a prohibition rule, the mail will be prohibited.

If you address a message to a prohibited destination, Stormshield Data Mail Notes Edition displays the following error window:



Click Delete these recipients to send the message to authorized recipients only.

3.5 Defining display parameter on connection request

You can define separately display behaviors' parameters of connection request when sending an unencrypted message in Disconnected user and Locked user mode. These parameters can be defined into *sbox.ini* file [section [Mail]] :

- Disconnected user mode: DisplayComlogWindow
- 0: Displays connection window only if user selects the Sign or Encrypt buttons when composing message.
- 1: Automatic display of Stormshield Data Security connection window (by default).
- Locked user mode: DisplayComlogWindowUserLocked
- 0: Displays connection window, only if user selects the Sign or Encrypt buttons when composing message.
- 1: Automatic display of Stormshield Data Security connection window (by default).



4. Sending a secure message

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

4.1 Entering 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 the section Section 3.2, "Connecting to Stormshield Data Security".

To send a message:

1. Open and write it as you usually would using your e-mail software.

! CAUTION

If you save your message before sending it (i.e. save it as a "draft"), your message is not secured: it is only secured when you send it.

2. To enter the security options for your message, click the Delivery options button on the Lotus Notes button bar.

The following window is displayed.

3. In the Basic tab, select the security options you want to apply to your message using the check boxes Sign and/or Encrypt, and click OK.

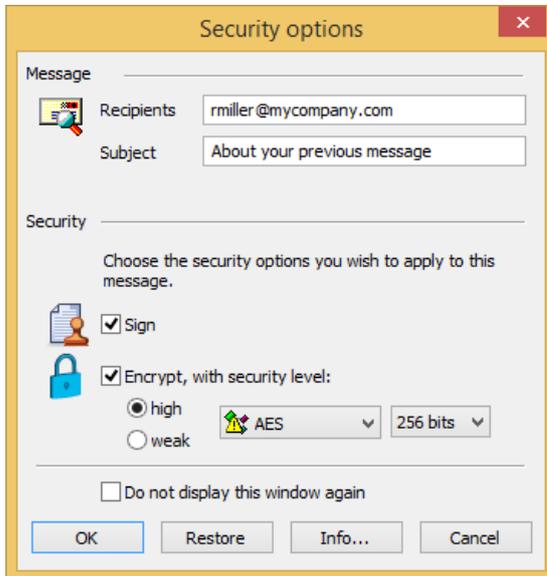
By default, Stormshield Data Mail Notes Edition replaces the Lotus Notes security, but keeps the interface of Lotus Notes to manage security options. It is possible to configure Stormshield Data Security to use both Lotus Notes and Stormshield Data Mail Notes Edition. To do so, refer to the information in the *Administration guide*.

By selecting one of the options, the window Security Options will be pre-filled, based on your choice.



If you specified in your configuration that the Stormshield Data Security window Security Options should not be displayed, the Lotus Notes window Delivery Options (above) will be displayed, in order to select the security options to apply to the message.

4. When you send your message, Stormshield Data Mail Notes Edition displays the following window:



Edit the security options to apply to the message, if required.

- a. If you are encrypting the message, by default Stormshield Data Mail Notes Edition suggests you use a strong algorithm. If some of your correspondents use a messaging system which does not support strong encryption, select the Weak radio button to make sure your correspondent will be able to decrypt it.

i NOTE

Your message is now less secure.

- b. You can also select any of the other algorithms provided by Stormshield Data Mail Notes Edition by selecting them from the drop-down list.

To edit the strong and weak algorithm settings, refer to Section 6.1.2, “Strong encryption and weak encryption”.

- c. You may decide to no longer display this window by selecting the option Do not display this window again .
5. To confirm your selection and send the message, click OK.

Your transmitted 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 chapter [Reading a secure message](#)).

4.2 Certificate not found or invalid

If you are encrypting your message, Stormshield Data Mail Notes 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 any certificates are not found or are invalid, Stormshield Data Security lists the affected recipients.

1. Select the action you want to take:
 - Return to the security options
 - Do not send to unresolved recipients: the mail will only be sent to recipients with valid certificates
 - Send to all recipients without encrypting: the message will be sent in plaintext to all recipients
2. Then click OK or Cancel the message.

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

If you send a message when you are not connected to Stormshield Data Security or your session is locked, the following window is displayed:



If you click Connect (or Unlock), Stormshield Data Mail Notes Edition displays the connection (or unlock) window, and asks you to select the security options to apply to the message.

If you select Cancel, the transfer is canceled. To send it later, you must go to your e-mail system and re-send it.

If you click Send unsecured the selected message is sent without any security.



5. Reading a secure message

This chapter indicates how you can view and read secured messages with Stormshield Data Mail Notes Edition. It also explains how you can remove the security from a message.

5.1 Opening a secure message

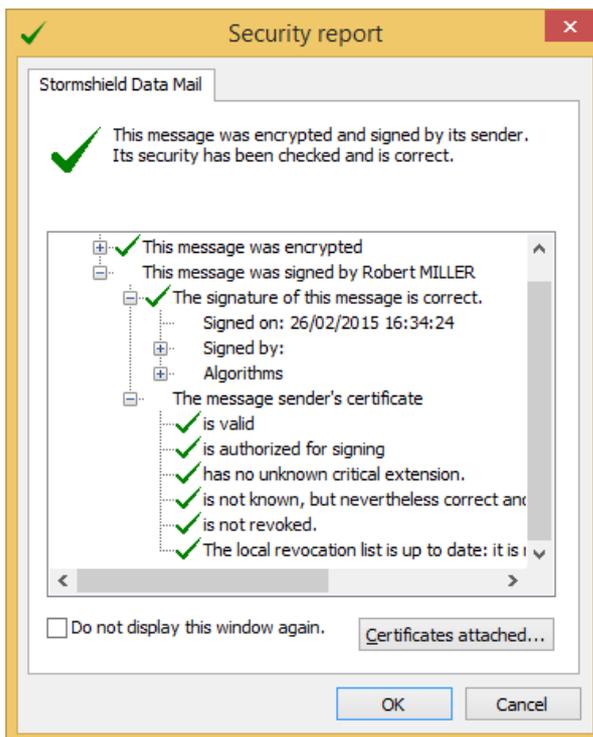
You receive and read messages as you normally would using your messaging software: Stormshield Data Mail Notes Edition begins "decrypting" all secure messages when you open them.

If you are not connected to Stormshield Data Security or if your Stormshield Data Security session is locked, a dialog box opens.

If you click on Connect (or Unlock) Stormshield Data Mail Notes Edition displays the connection window, and then decrypts the message.

Stormshield Data Mail Notes Edition then displays the message's "security report".

Click on  to open the branch:



This report details all the algorithms used during encryption and signing.

For signatures, it also includes:

- the identity of the sender who has signed the message
- the result of the cryptographic verification of the signature (verified with the public key contained in the certificate of the sender): signature correct or incorrect
- the results of checks carried out on the sender's certificate; Stormshield Data Mail Notes 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)
- an indication of the level of trust assigned to the sender's certificate



By default, Stormshield Data Mail Notes Edition displays the security report when a secure message is opened. If you do not want the report to be displayed each time you open a message, select the option Do not display this window again. The window will no longer be displayed if all checks are correct; however, if even one of the checks is incorrect, the window will be displayed when opening the message in order to warn you about detected problems.

You can configure this feature (see [Section 6.2.2, "Security report"](#)).

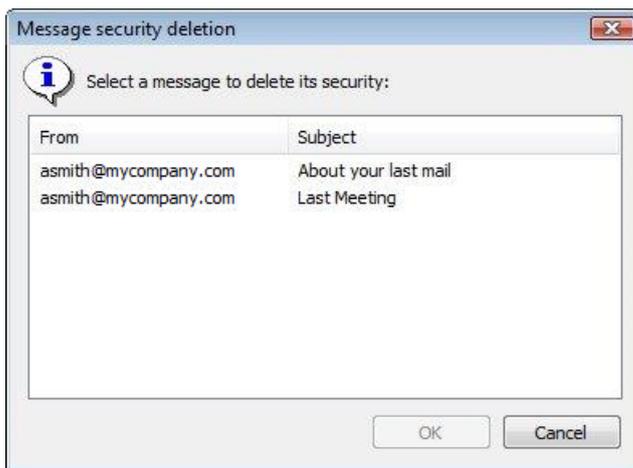
5.2 Deleting security from a message

By default, secure messages that you receive are stored as secure messages in the Stormshield Data Mail Notes Edition messages database.

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.

5.2.1 Manually deleting security from a message

To delete security from a message, select the message and choose Action > Delete security. If several messages are open at the same time, select the message from which you want to delete security:



CAUTION

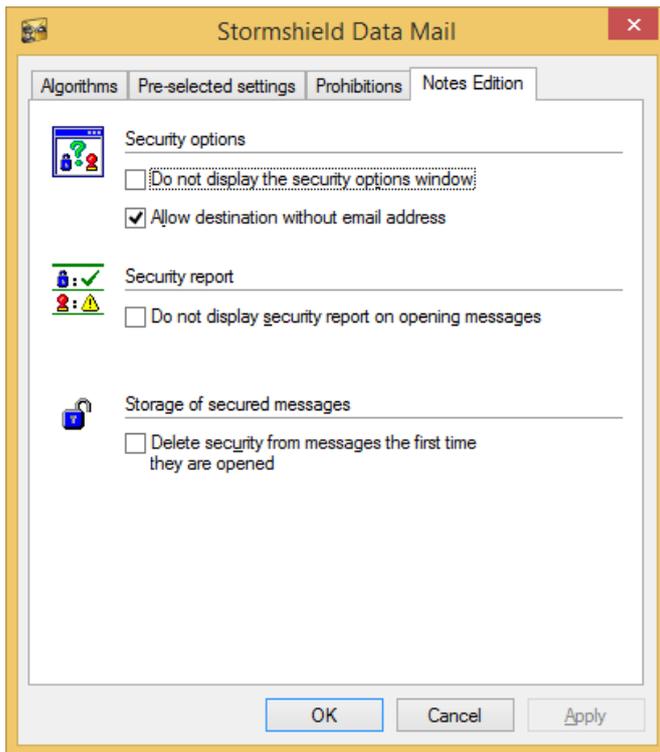
If you confirm the deletion of its security, the message will be stored as plaintext in the Notes messages database, without any security.

5.2.2 Automatically deleting security from a message

Stormshield Data Mail Notes Edition can automatically delete the security from messages you receive. The message's security will be deleted as soon as you open it.

To do this:

1. Open the Stormshield Data Security menu.
2. Choose Properties
3. Click on the Configuration tab.
4. Double-click on the Stormshield Data Mail Notes Edition icon.
5. Select the Notes Edition tab.



6. Check the Delete security from messages the first time they are opened option.

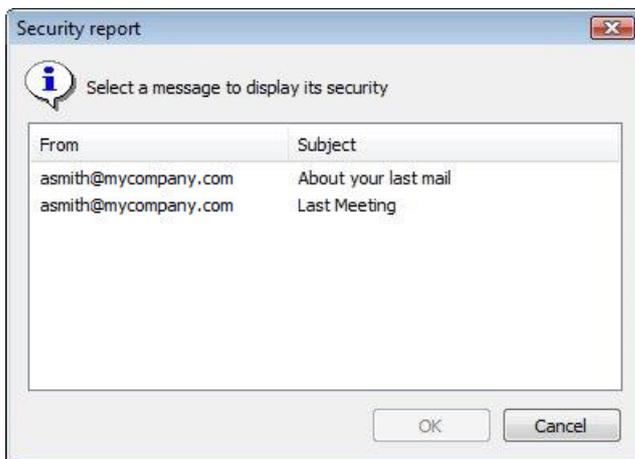
! CAUTION

All information relating to the security of the message (algorithms, signature verification report,...) will only be available the first time you open the message. This information will then be lost.

5.3 Consulting the security report

Once your message has been opened, you can consult the message's security report by selecting Actions > Display security report.

If several messages are open at the same time, select the message for which you want to display the report.





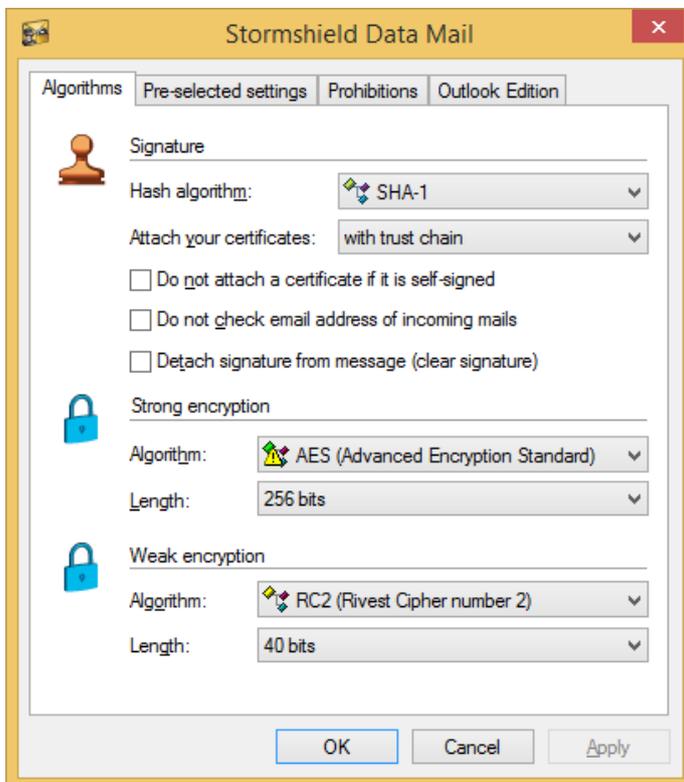
6. Advanced functions

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

6.1 Managing your algorithms

To modify your algorithms used in Stormshield Data Mail Notes Edition:

1. Open the Stormshield Data Security menu.
2. Choose Properties.
3. Select the Configuration tab.
4. Double-click on the Stormshield Data Mail Notes Edition icon.
5. Select the Algorithms tab.



6.1.1 Signature

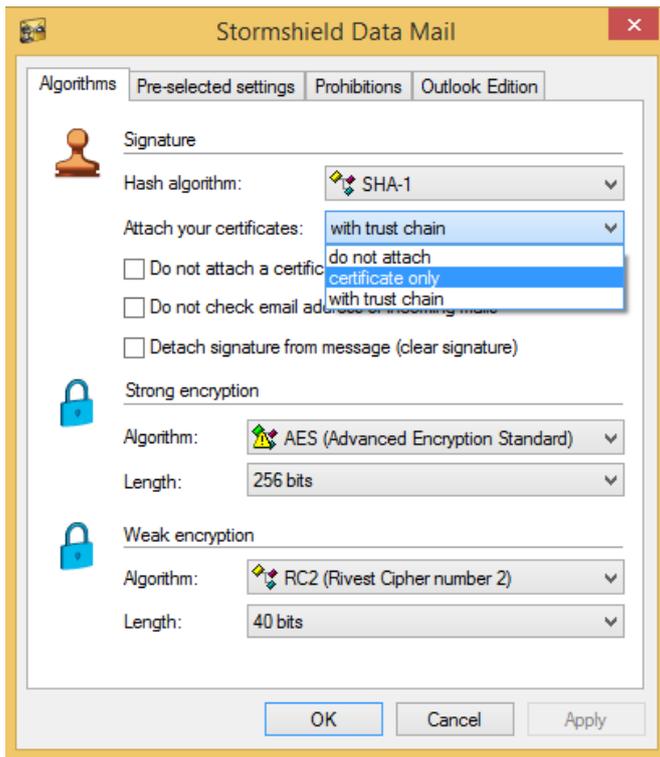
The following sections describe the options available on the Algorithms tab.

Hash algorithm

This drop-down menu allows you to choose the hash algorithm used when signing a message. The options are: SHA-1 (recommended) and MD5.

Attach your certificates

This drop-down menu allows you to choose the way you want to communicate your certificates to your correspondents:



Do not attach: You must then send the certificate in another way than a signed message.

Certificate alone: The certificate is sent without the trust chain. You must have the parent in your trusted address book to validate the chain. You will not have the option to import the certificates in order to have the complete chain (with the root certificate as a trusted source) when the next messages are sent.

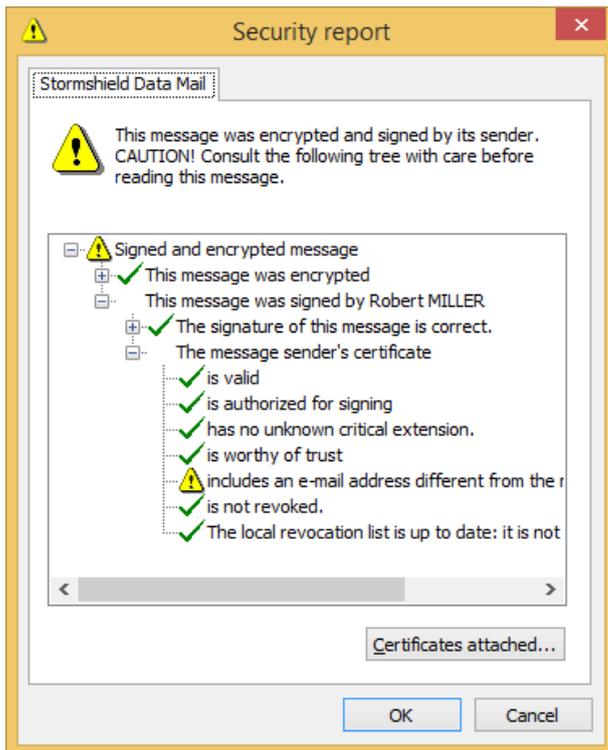
Certificate with trust chain: This is the recommended method. The certificate is sent with the trust chain. The recipient must have the root certificate in the trusted address book to validate the certificate.

Do not attach a certificate if it is self signed

Select this check box if you are waiting for your certificates from the authority. This avoids propagation of useless certificates, for example if the recipient imports the certificate without taking into account that it is temporary.

Do not check e-mail address of incoming mail

Select this check box to delete the error message “the certificate has a different e-mail address than the sender”.

**i NOTE**

Selecting this option is risky, as users generally trust the information indicated by their e-mail system. In this case, they would assume that the sender is the one indicated, which could raise security issues.

Detach signature from message (clear signature)

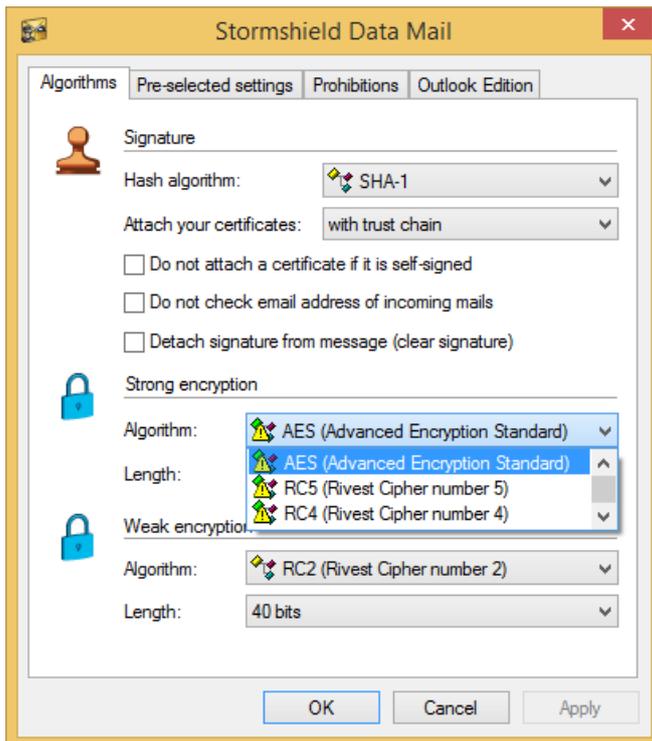
Select this check box if you want to send your signature in clear (plaintext).

Enabling a signature in plaintext ensures that a recipient can read the message even if they do not have an e-mail system that takes into account S/MIME format, or if their e-mail system refuses to display messages with signatures that cannot be validated (for example if the certificates and CRLs are not available).

However, a signature in plaintext is more exposed to modifications during transfer of the message. Normally servers do not modify messages, but it is possible that tags are added, blank lines are added or removed, etc.

6.1.2 Strong encryption and weak encryption

In the Strong encryption and Weak encryption sections, you can preselect the encryption algorithms and their key length which are later suggested by Stormshield Data Mail Notes Edition when entering the security options.



When encrypting a message, it is the strong encryption algorithm (and its appropriate key length) which is used, by default.

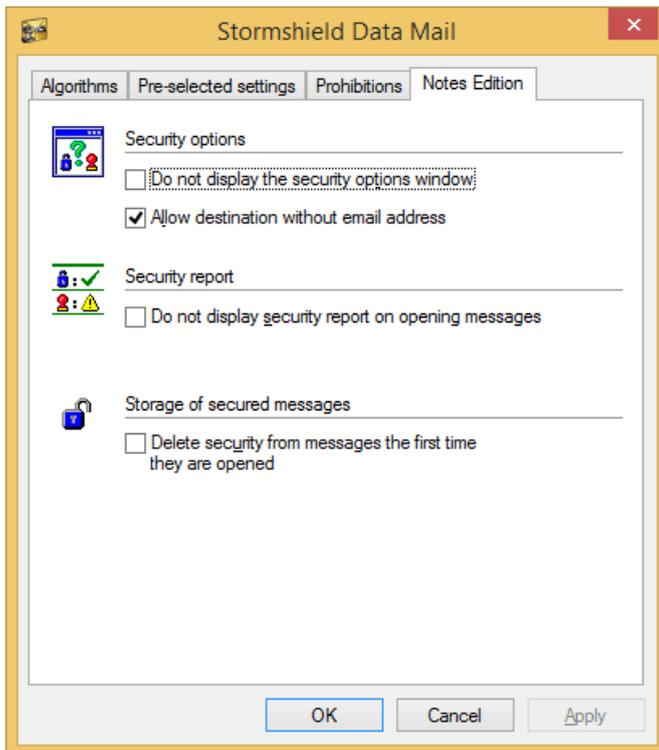
i NOTE

When the result of the evaluation of the security rules leads to automatic encryption of a message, the encryption uses the strong encryption algorithm selected above.

Typically, the strong encryption is AES-256, and the weak encryption is triple DES-128. The strong encryption can be used with Stormshield Data Mail Notes Edition and newer e-mail systems, while the weak encryption is used when communicating with older e-mail systems.

6.2 Notes edition settings

1. Open the Stormshield Data Security menu.
2. Choose Properties.
3. Click on the Configuration tab.
4. Double-click on the Stormshield Data Mail Notes Edition icon.
5. Select the Notes Edition tab:



6.2.1 Entering security options

Do not display the security options window

If you select this option, the security options which you have selected while editing your message (and possibly enforced according to its destinations) will be applied without requiring your confirmation.

If you deselect this option, you must confirm these options before each message can be transmitted, unless the security is already configured by pre-selected options, and you have requested that no confirmation windows be displayed.

Allow destination without e-mail address

This option allows you to send messages to recipients who do not have a standard e-mail address like "name@domain.com".

Use this option if you have defined correspondents that do not have an internet address. However, this is less common.

6.2.2 Security report

Do not display the security report window on opening messages

If you deselect this option, the security report window will be displayed each time you open a secure message.

If you select this option, the security report window will only be opened if some security checks are not correct. But it will be displayed if even one control is incorrect.

6.2.3 Storage of secure messages

Delete security from messages the first time they are opened

If you deselect this option, your messages will remain secured in your Notes folders.



If you select this option, security will be deleted from a message when you open it for the first time. In this case, all information relating to the security of the message (algorithms, signature verification report,..) will only be available the first time you open the message. This information will then be lost.

6.3 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*.



STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2022. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.