



STORMSHIELD



GUIDE

**STORMSHIELD DATA SECURITY
ENTERPRISE**

ADMINISTRATION GUIDE

Version 11.0

Document last updated: February 26, 2024

Reference: [sds-en-sdse-administration_guide-v11.0](#)



Table of contents

| | |
|--|----|
| 1. Getting started | 7 |
| 1.1 What does SDS Enterprise do? | 7 |
| 1.2 How does SDS Enterprise work? | 7 |
| 1.3 How to deploy SDS Enterprise to your pool? | 8 |
| 1.4 Understanding the concept of a trusted address book | 9 |
| 1.5 Architecture diagram of SDS Enterprise | 9 |
| 2. Use environment | 10 |
| 2.1 Recommendations on security watch | 10 |
| 2.2 Recommendations on keys and certificates | 10 |
| 2.3 Recommendations on algorithms | 10 |
| 2.4 Recommendations on user accounts | 10 |
| 2.5 Recommendations on workstations | 10 |
| 2.6 Recommendations on administrators | 11 |
| 3. Logging in to SDMC | 12 |
| 3.1 Creating the corporate account | 12 |
| 3.2 Creating the first administration account | 12 |
| 3.3 Logging in to SDMC via an identity provider | 13 |
| 3.3.1 Providing the well-known location | 13 |
| 3.3.2 Configuring the identity provider | 13 |
| 3.3.3 Encrypting communications with the SDMC certificate | 14 |
| 3.3.4 Troubleshooting | 15 |
| 3.4 Changing the connection mode | 15 |
| 4. Managing the license | 16 |
| 4.1 Getting the SDS Enterprise license | 16 |
| 4.2 Importing the license in SDMC | 16 |
| 4.3 Looking up license information | 16 |
| 5. Managing administrators in SDMC | 17 |
| 5.1 Inviting a new administrator | 17 |
| 5.2 Accepting an invitation to manage SDS Enterprise | 17 |
| 5.3 Managing the list of administrators | 18 |
| 5.4 Modifying an administrator's permissions | 18 |
| 5.5 Deleting administrators | 18 |
| 6. Managing authority certificates and recovery certificates in SDMC | 19 |
| 6.1 Understanding the use of user keys and certificates | 19 |
| 6.2 Importing certificates in SDMC | 20 |
| 6.3 Renaming, deleting or downloading certificates | 20 |
| 7. Managing LDAP directories in SDMC | 21 |
| 7.1 Adding an LDAP directory | 21 |
| 7.2 Editing, duplicating or deleting LDAP directories | 21 |
| 8. Managing security policies in SDMC | 22 |
| 8.1 Creating a policy | 22 |
| 8.1.1 Creating a new policy | 22 |
| 8.1.2 Creating a policy from an existing policy | 22 |



- 8.2 Configuring user accounts 22
 - 8.2.1 Configuring generic account settings 23
 - 8.2.2 Setting account creation parameters 24
 - 8.2.3 Enabling data recovery 24
- 8.3 Configuring features 25
 - 8.3.1 Configuring Stormshield Data File 25
 - 8.3.2 Configuring Stormshield Data Team 27
 - 8.3.3 Configuring Stormshield Data Disk 28
 - 8.3.4 Configuring Stormshield Data Mail 29
 - 8.3.5 Configuring Stormshield Data Sign 31
 - 8.3.6 Configuring Stormshield Data Shredder 32
 - 8.3.7 Configuring Stormshield Data Share 33
- 8.4 Configuring corporate directories 33
 - 8.4.1 Adding LDAP directories from the library 34
 - 8.4.2 Configuring automatic directory updates 34
 - 8.4.3 Adding WKD servers to encrypt messages in PGP format 35
- 8.5 Adding certification authorities and configuring certificate revocation control 35
 - 8.5.1 Understanding revocation control 35
 - 8.5.2 Understanding revocation lists 36
 - 8.5.3 Adding the certification authority's certificates 36
 - 8.5.4 Configuring revocation control in a policy 36
- 8.6 Configuring policy distribution points 37
- 9. Installing SDS Enterprise agents on user workstations 38
 - 9.1 Finding out the system requirements for SDS Enterprise 38
 - 9.2 Downloading security policies 38
 - 9.3 Signing security policies 39
 - 9.3.1 Requirements 39
 - 9.3.2 Signing the policy 39
 - 9.4 Downloading SDS Enterprise agents' installation packages form SDMC 39
 - 9.5 Deploying the SDS Enterprise agent installation package on user workstations 40
 - 9.5.1 Choosing the installation package deployment mode 40
 - 9.5.2 Deploying the signed security policy file and the peer certificate 41
 - 9.5.3 Configuring preselected features 41
 - 9.6 Updating the policy on SDS Enterprise agents 42
- 10. Creating and managing SDS Enterprise accounts on user workstations 43
 - 10.1 Configuring the middleware required for Card or USB token accounts 43
 - 10.1.1 Specifying a list of middleware in the security policy 43
 - 10.1.2 Installing the smart card extension 44
 - 10.1.3 Configuring the smart card extension 45
 - 10.1.4 Viewing private objects 47
 - 10.2 Creating smart card or USB token accounts 48
 - 10.2.1 Creating accounts automatically 49
 - 10.2.2 Creating accounts manually 49
 - 10.2.3 Using keys from the smart card or USB token 49
 - 10.3 Creating password accounts manually 50
 - 10.3.1 Generating keys 50
 - 10.3.2 Importing keys 52
 - 10.4 Creating a Single Sign-On (SSO) account 53
 - 10.4.1 Requirement 53
 - 10.4.2 Configuring SSO accounts in SDMC 53
 - 10.4.3 Configuring SSO accounts in the security policy's .json file 54



| | |
|--|----|
| 10.4.4 Using the SSO account | 54 |
| 10.5 Renewing keys and certificates | 55 |
| 10.5.1 Password accounts | 55 |
| 10.5.2 Card or USB token accounts | 56 |
| 10.5.3 Single Sign-On accounts (SSO) | 57 |
| 10.6 Unblocking user accounts | 58 |
| 10.6.1 Using the backup password | 58 |
| 10.6.2 Using the user account backup | 58 |
| 10.7 Exporting an SDS Enterprise account | 58 |
| 10.8 Exporting a security key | 59 |
| 10.9 Decrypting a user's data with an old key or a delegation key | 60 |
| 10.9.1 Setting up delegated decryption | 61 |
| 10.9.2 Decrypting OpenPGP messages | 62 |
| 10.10 Decrypting a user's data with a recovery certificate | 63 |
| 10.10.1 Looking up recovery certificates | 63 |
| 10.10.2 Using a recovery certificate to decrypt data | 64 |
| 11. Managing the trusted address book from the SDS Enterprise agent | 65 |
| 11.1 Looking up the trusted address book and managing certificates from the SDS Enterprise agent | 65 |
| 11.1.1 Opening your trusted address book | 65 |
| 11.1.2 Displaying certificates | 66 |
| 11.1.3 Importing certificates | 67 |
| 11.1.4 Exporting certificates or the trusted address book | 69 |
| 11.1.5 Creating a certificates group | 71 |
| 11.1.6 Modifying a certificate group | 72 |
| 11.1.7 Exporting a certificates group | 73 |
| 11.1.8 Deleting a certificate group | 73 |
| 11.2 Exchanging certificates via Stormshield Data Mail | 73 |
| 11.3 Working offline | 74 |
| 12. Looking up certification authorities from the SDS Enterprise agent | 75 |
| 12.1 Downloading a CRL | 75 |
| 12.2 Deleting an authority | 75 |
| 13. Configuring and using the agent's advanced features | 77 |
| 13.1 Stormshield Data Virtual Disk | 77 |
| 13.1.1 Recovering a volume | 77 |
| 13.1.2 Unmounting a volume by force | 77 |
| 13.1.3 Duplicating a volume | 78 |
| 13.1.4 Using the volume within a Windows multi-session context | 78 |
| 13.1.5 Stormshield Data Virtual Disk limitations | 78 |
| 13.2 Stormshield Data File | 78 |
| 13.3 Stormshield Data Mail | 78 |
| 13.3.1 Information about the RTF format | 78 |
| 13.3.2 Using cross-encryption | 79 |
| 13.3.3 Configuring the LDAP directory for certificates that contain several e-mail addresses | 79 |
| 13.3.4 Ensuring the consistency of e-mail addresses | 79 |
| 13.4 Stormshield Data Team | 80 |
| 13.4.1 DFS environment restriction | 80 |
| 13.4.2 Managing the user's temporary folder (%TEMP%) | 80 |
| 13.4.3 Managing the system's temporary folder | 80 |
| 13.4.4 Moving folders available offline | 80 |



- 13.4.5 Keeping performance optimal on the workstation 80
- 13.4.6 Moving an intra-volume folder 80
- 13.4.7 Prohibiting access to encrypted files if the certificate is revoked 81
- 13.4.8 Changing the dates of the last access 81
- 13.4.9 Using the cache in a network 81
- 14. Troubleshooting 83
 - 14.1 Viewing event logs 83
 - 14.1.1 Enabling event logs 83
 - 14.1.2 Understanding the message types 84
 - 14.1.3 Understanding details of logged information 84
 - 14.2 Troubleshooting issues 84
 - 14.2.1 Understanding how tracing works 84
 - 14.2.2 Use the tracing system 85
- 15. Uninstalling SDS Enterprise from user workstations 86
- 16. Further reading 87
- Appendix A. List of SDS Enterprise logs 88
 - A.1 Administration 88
 - Stormshield Data Security Suite installation 88
 - Directory administration 89
 - Management of the revocation list 90
 - A.2 Virtual Disk 90
 - Volume management 90
 - A.3 File 91
 - Encryption/Decryption 91
 - Encryption/Decryption 92
 - A.4 Kernel 92
 - Start/Stop 92
 - LDAPS authentication 92
 - Select cryptographic device 93
 - A.5 Keystore 93
 - Login/Logout 93
 - Account management 93
 - Key management 95
 - Keyring management 95
 - A.6 Mail 96
 - Outgoing/Incoming 96
 - Cross-encryption 96
 - Disabling security 96
 - Administration 97
 - A.7 Shredder 97
 - A.8 Sign 97
 - Signature 97
 - A.9 Team 98
 - Rule management 98
 - Team rule update 99
 - Encryption/decryption 100
 - Backup/Restoration 100
 - Driver 101
 - A.10 Share 101



Appendix B. Third-party libraries102

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



1. Getting started

This guide contains the information needed for managing SDS Enterprise and installing SDS Enterprise agents in your environment.

1.1 What does SDS Enterprise do?

SDS Enterprise guarantees the protection and confidentiality of data stored on local, shared or cloud-based folders, by relying on the transparent end-to-end encryption built into communication and collaboration tools. With it, access to protected data can also be restricted to defined groups and user profiles.

SDS Enterprise includes the SDMC administration console, from which you can define security policies and an agent installed on users' workstations. This agent makes it possible to apply policies and provides the following features:

- Real-time transparent file encryption, for transfer by e-mail or secure backup,
- Encryption of files stored on spaces synchronized with online hosting services OneDrive, DropBox, SharePoint and Oodrive,
- Encryption and signature of e-mails, making it possible to protect the data that they contain, and guarantee the authenticity of their sender's identity and the integrity of their contents,
- Sharing of encrypted files with co-workers over my company's network,
- Secure and irreversible erasure of data,
- Electronic signature of files and folders, making it possible to guarantee the authenticity of their sender's identity and the integrity of their contents,
- Encryption of virtual disks, making it possible to store protected files. These virtual disks can be shared among co-workers;

The solution also includes the Stormshield Data Connector component, allowing to control the features of the SDS Enterprise solution through a PowerShell module or .NET APIs.

The SDMC administration console is hosted by Stormshield's Cloud services. In SDMC, you can:

- Create and configure the security policies applied by the SDS Enterprise agents installed on users' workstations,
- Declare the certification authorities on which user certificates depend,
- Declare corporate LDAP directories to manage certificate exchanges,
- Download SDS Enterprise agents' installation packages.

To use the SDMC console, start by creating a corporate account, then one or several administrator accounts as described in the section [Logging in to SDMC](#).

You can also configure a security policy directly in a *json* file and include it in the SDS Enterprise installation package. For more information on how to configuration this file, refer to the *Advanced configuration guide*.

1.2 How does SDS Enterprise work?

Requirement

You must have your own infrastructure to generate encryption and signature keys for the users



in the company. You can then distribute them to users in whatever method you choose, for example via smart cards.

SDS Enterprise uses public key cryptography technology.

Each user has at least a pair of keys: a private key and a public key. The private key is carefully kept by its owner. The public key, by contrast, is freely distributed.

A different key pair is required for each purpose:

- A pair of encryption keys is required for encrypting and sharing confidential files or e-mails,
- A pair of signature keys is required to sign documents or e-mails,

To secure your users' private keys, you can store them on cryptographic media that support the PKCS#11 standard. As part of user single sign-on, you must store the keys in the Windows Certificate Store.

To encrypt files or send encrypted messages to peers, users must know their peers' public encryption key.

Public keys are distributed as certificates. A certificate is an electronic document that associates a public key with its owner. SDS Enterprise supports the X.509 V3 certificate format. These certificates are stored in users' trusted address book, as explained in the [Understanding the notion of users' trusted address book](#) section.

RSA keys of users and certification authorities must be a minimum size of 4096 bits, with a public exponent strictly greater than 65536. The certificates and CRLs must be signed with the SHA-512 algorithm.

! IMPORTANT

When renewing encryption keys, make sure to keep the users' old keys securely in their SDS Enterprise account. This will still allow the user to decrypt data encrypted with an old key. For more information, see [Decrypting user data with an old key or a delegation key](#) and [Decrypting user data with a recovery key](#).

For more information on managing certificates, refer to the sections [Managing authority certificates and recovery certificates in SDMC](#) and [Setting account creation parameters](#).

1.3 How to deploy SDS Enterprise to your pool?

You can deploy SDS Enterprise to user workstations with remote distribution solutions such as [Microsoft Endpoint Configuration Manager](#). You must deploy on the workstations:

- the SDS Enterprise agent installation package in the *.msi* format. You can download it from the SDMC console in French and English.
- deploying the signed security policy file and the peer certificate. The policy is created and configured in the SDMC console. You must download it from the console and have it signed by the administrator who has the role of security policy signatory. The signature utility is also available in SDMC.

Each time the SDS Enterprise agent restarts, it checks if a new update is available on the server that acts as the policy distribution point. If this is the case, it will apply it automatically.

For further information on agent deployment, refer to the [Installing SDS Enterprise agents on user workstations](#) section.



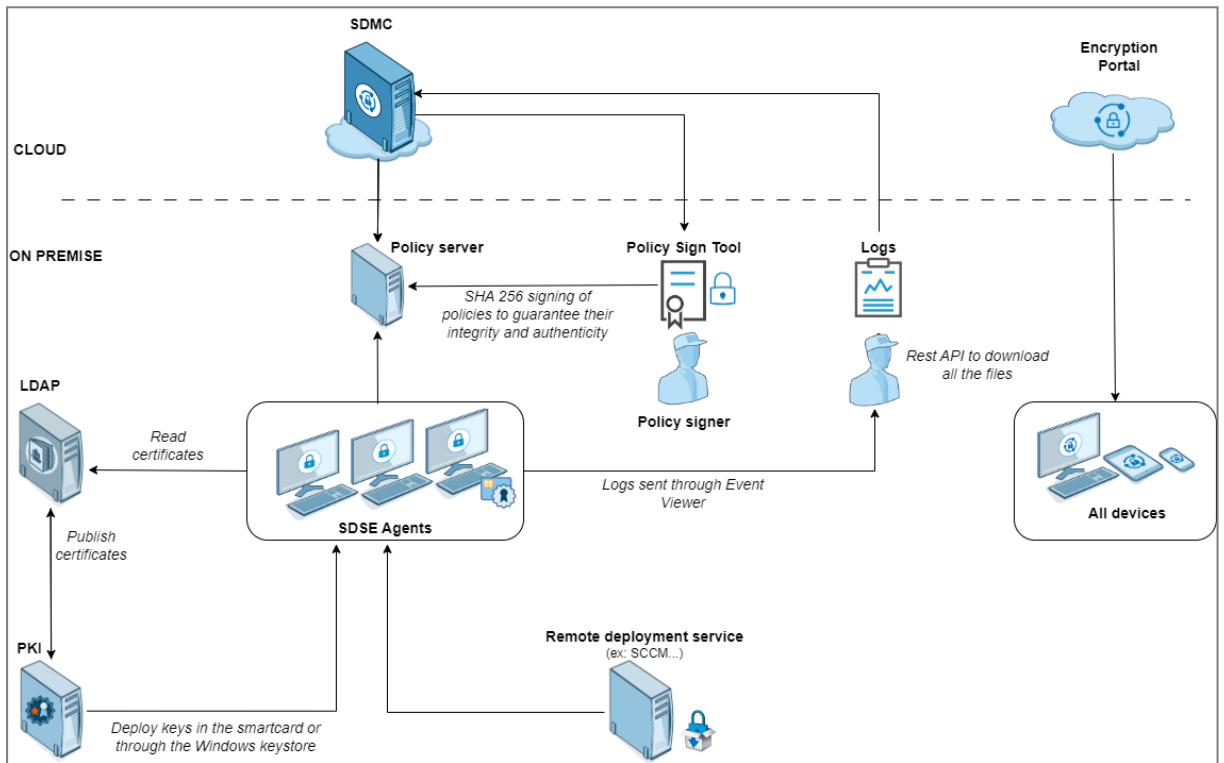
1.4 Understanding the concept of a trusted address book

SDS Enterprise makes it possible to manage a trusted address book on users' workstations: you can add the certificates (public keys) of the users and authorities that you trust in the address book.

Users can be automatically added to the trusted address book via an LDAP directory.

For more information, refer to the sections [Managing LDAP directories in SDMC](#) and [Configuring corporate directories](#).

1.5 Architecture diagram of SDS Enterprise





2. Use environment

To use SDS Enterprise under the conditions of the Common Criteria evaluation and of the french qualification at standard level, it is essential to observe the following guidelines.

2.1 Recommendations on security watch

1. Regularly check security alerts provided on <https://advisories.stormshield.eu/>.
2. Always apply the software update if it contains a security breach correction. These updates are available on your customer area [MyStormshield](#).

2.2 Recommendations on keys and certificates

1. RSA keys of users and certification authorities must be a minimum size of 4096 bits, with a public exponent strictly greater than 65536.
2. The certificates and CRLs must be signed with the SHA-512 algorithm.

2.3 Recommendations on algorithms

SDS Enterprise Supports AES 256 encryption algorithm and SHA 512 signature algorithm.
For a use beyond the year 2030, the minimum size of an RSA key is 3072 bits.

2.4 Recommendations on user accounts

1. The user accounts must be protected by the AES 256 encryption algorithm and SHA-256 cryptographic hash standard.
2. Passwords should be subject to a security policy preventing weak passwords.
3. Appropriate organizational measures must ensure the authenticity of policies from which the user accounts are created.
4. In case of using a hardware key ring (smart card or hardware token), this device protects the confidentiality and integrity of keys and certificates that it contains.

2.5 Recommendations on workstations

1. The workstation on which SDS Enterprise is installed must be healthy. There must be an information system security policy whose requirements are met on the workstations. This policy shall verify the installed software is regularly updated and the system is protected against viruses and spyware or malware (firewall properly configured, antivirus updates, etc.).
2. The security policy should also consider that the workstations not equipped with SDS Enterprise do not have access to shared confidential files on a server, so that a user can not cause a denial of service by altering or removing inadvertently or maliciously, files protected by the product.



3. Access to administrative functions of the workstation system is restricted only to system administrators.
4. The operating system must manage the event logs generated by the product in accordance with the security policy of the company. It must for example restrict read access to these logs to only those explicitly permitted.
5. The user must ensure that a potential attacker can not see or access the workstation when the SDS Enterprise session is open.

2.6 Recommendations on administrators

1. SDS Enterprise administrators are considered as trusted. They are responsible for defining the SDS Enterprise security policy by respecting the state of the art, and they may create user accounts in the Stormshield Data Management Center application.
2. The system administrator responsible is also considered as trusted. He/She is responsible for the installation and maintenance of the application and workstation (operating system, protection software, *PKCS#11* interface library with a smart card, desktop and engineering software. He/She applies the security policy defined by the SDS Enterprise administrators.
3. The product user must respect the company's security policy.



3. Logging in to SDMC

Before using an SDMC administration console, you must first create your corporate account.

When creating your account, you can choose from two connection modes: password or SAML.

If you are using passwords, you must create the first administration account in order to log in to SDMC. Other administrators can then be created directly in SDMC. To create other administration accounts, refer to the section [Managing administrators in SDMC](#).

For more information on the SAML connection mode, refer to the section [Logging in to SDMC via an identity provider](#).

When you create your corporate account, you will have a 30-day trial period. After this period, you must import a permanent license. For more information on the license, see the section [Managing the license](#).

3.1 Creating the corporate account

The corporate account contains all the information relating to your company: It is created at the beginning, when your company is registered on the SDMC solution.

The corporate account is dedicated to a single company and is never shared with other companies.

1. Click on <https://sds.stormshieldcs.eu/admin/#/register-my-company>.
2. Fill in the information about your company and your contact information.
3. Select **I agree with the General Conditions of Use**.
4. Click on **Create** to save your corporate account.
5. Click on the link sent to you by e-mail to confirm the creation of the account and domain.
6. Stormshield must then confirm the activation of the account. You will receive a confirmation e-mail.
 - If you have chosen SAML connection mode, you can log in to SDMC with your corporate credentials. Prior to this step, you must have configured the connection mode via an identity provider. Refer to the section [Logging in to SDMC via an identity provider](#). You can always access the page allowing you to log in to your SDMC administration console at <https://sds.stormshieldcs.eu/admin>. If you encounter a connection error, refer to the section [Troubleshooting](#).
 - If you have chosen the Password connection mode, you can proceed to the next step.

3.2 Creating the first administration account

If you have chosen the Password connection mode, you must create an administration account.

1. After Stormshield has confirmed the activation of your corporate account, you will receive an e-mail asking you to create an administration account within the specified time limit. Click on the **Create the administrator account** link in the e-mail.
2. Fill in the required fields. The e-mail address is already entered.
3. Click on **Create** to save your administration account.
4. Log in to SDMC. You can always access the page allowing you to log in to your SDMC administration console at <https://sds.stormshieldcs.eu/admin>.



3.3 Logging in to SDMC via an identity provider

With the SAML protocol, SDMC can rely on an identity provider (IdP) to authenticate administrators.

To set up this connection mode:

- Provide SDMC with a well-known location indicating the IdP to contact,
- Configure the IdP of your choice so that it provides SDMC with the information required for authentication. The IdP must be accessible over the Internet and you must have a certificate for it.

3.3.1 Providing the well-known location

The well-known location is a configuration folder containing the *sdmc-configuration* configuration file. Provided by a server, it must be accessible via HTTPS from all networks. The well-known host server must approve the SDMC certificate before communication between the two is possible.

The *sdmc-configuration* file is in .JSON format. It must contain the following information on the IdP to contact:

- *idpCertificate*: URL of the certificate assigned to the IdP,
- *idpUrl*: URL of the IdP to contact.

The file must be accessible at the following URL so that SDMC can reach it:

`https://sdmc.[domain-company]/.well-known/sdmc-configuration`

Where:

- *https* is mandatory,
- *sdmc.* is a sub-domain needed by the client to expose the well-known file,
- *[domain-company]* is replaced by the domain of the corporate account present in the e-mail address of the administrator attempting to connect,
- *.well-known* is the folder containing all the well-known files,
- *sdmc-configuration* is the file for SDMC. It allows retrieving SAML connection information such as the IdP URL.

For performance reasons, *idpUrl* and *idpCertificate* information is cached for 24 hours from the first connection. Changes to the *sdmc-configuration* file may therefore not be immediately sent to SDMC. This may take up to 24 hours.



EXAMPLE

For the domain name *example.com*, the well-known location must be accessible at the URL `https://sdmc.example.com/.well-known/sdmc-configuration` and must be in the following form:

```
{
  "idpCertificate": "https://example.com/assets/certificate.pem",
  "idpUrl": "https://example.com/saml/login"
}
```

3.3.2 Configuring the identity provider



The following parameters must be configured on the IdP so that it sends the expected information format to SDMC when an administrator attempts to log in:

| Parameter | Type | Value | Status |
|-------------|--------|--|-----------|
| "email" | String | Email address, in the form: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress | Mandatory |
| "firstName" | String | First name, in the form: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | Optional |
| "lastName" | String | Surname, in the form: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname | Optional |

You must also add the following URLs to the IdP application configuration:

- **Entity ID:** <https://sds.stormshieldcs.eu/api/internal/5/admins/saml/metadata.xml>
- **Assertion Consumer Service URL:**
<https://sds.stormshieldcs.eu/api/internal/5/admins/saml/acs>

3.3.3 Encrypting communications with the SDMC certificate

Some IdPs offer SAML 2.0 communication encryption. To implement it, add the following public key, extracted from the SDMC certificate, to the IdP configuration associated with communication encryption:

```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAGEAu5nGaYFmaHGk6fu6+H5b
qo/JBUvbuZQlhWE7Ybocns4YIEKVSi6B9QtxasLN4BhZuh6autZmhLqQtZtxV8S4
4BkU44KXNeKPGGhD1izp2mJ8iE6Z3lhUCYRxrRebZQ2Fmu8Z/rKpUDMxwhjOskkQ
LVHWf1UIT8heRQuUNqN3nqF7049Fe3rQQvI07NOokmPnwO5EpptopOCRj0b2FSGx
KdTk/RNm/QKBuirF/7w8JremeG6W+HIC6810cN/Lf88aHoL9Nkm0A9eknJyzcKy3
wH0TTBF3N4n521psttg22hOZjQXMqSjKXUPHEMBq6br9Tixg53Q8rJhthS+Ahosb
qsxRkAOUIaEPmOR8Kx6AlJ6gdGJe0PAqiZTOiYKEFx1yU6kEbpuU7KkKJwsmOZVg
VQMFIVOQiv/1wRLx49ybvizqyNgFuZx4+4pGQt3ETkdQhK10s0x07/UUMYEKu59C
YSAyJNVYVjujC2QqaP8YXcJNndEbSPH58PxFDZ8SmBa9uSzxco2o+Zg2972dxUXW
fIZpWifdkDw6ktor9LhaqDYUw6KLMhH8phRzg49Kt7JaJUtbC9x0YgaXJ23ZfaP9
ndOaWK4loycCS4yyA6Uqupqp5oJV/pyPEAIzrYAVHHBtyxcv2uCXWF1mBZeN6RDZ
Y6tY9gfqqoatDT32PfH4Xs0CAwEAAQ==
-----END PUBLIC KEY-----
```



3.3.4 Troubleshooting

The authentication of an SDMC administrator failed and an error code appears. Ask the administrator for a code. The error may be one of the following:

| | |
|------|--|
| 4001 | The well-known location is not available. |
| 4002 | The identity provider is not sending the right information. Check the configuration. |
| 4003 | The certificate's URL address cannot be accessed. Internal error. Forward the error code to Stormshield. |
| 4004 | The well-known location was not correctly configured. Check the configuration. |
| 4006 | Internal error. Contact Stormshield and forward the error code. |

3.4 Changing the connection mode

If you wish to change the connection mode (SAML or password), we advise you to get in touch with Stormshield. Stormshield will make the necessary changes for you.



4. Managing the license

The SDMC administration console is provided by default with a trial license that allows it to be used for 30 day period following its initial startup.

After 30 days, you must obtain your license from your [MyStormshield](#) client area and import it in SDMC.

4.1 Getting the SDS Enterprise license

1. Make sure you have the Stormshield PDF delivery document and log in to your [MyStormshield](#) client area.
2. From the menu on the left, choose **SDS - General > Register an SDS instance**, and accept the terms of use.
3. Enter the following information:
 - **Associated company:** Name of the company under which you are registered at Stormshield.
 - **License key:** Character string located in the Serial number column of the delivery document (for example `FOBBABBJ-At07vu9Y`).
 - **Reseller:** name of your SDS Enterprise reseller.
4. Click on **Save**.
5. On your personal area dashboard, from the **List of products** table, click on your serial number.
6. Click on **Download all licenses** and unzip the downloaded file.

4.2 Importing the license in SDMC

1. In SDMC, select the **License** menu on the left.
2. Click on **Import** and select the file you have just unzipped (for example `FOBBABBJ-At07vu9Y.licence`).

The SDMC console will not import a license if it has expired.

4.3 Looking up license information

The following information is available in the **License** menu:

- The license key to use for agents on workstations,
- License validity dates.



5. Managing administrators in SDMC

If you have chosen the Password connection mode when the corporate account was created, during the initial connection to SDMC, you [created an administrator account](#). This administrator is allowed to perform all configuration operations on the console, and may also invite other administrators to carry out these operations.

If you have chosen the SAML connection mode, the list of administrators will be filled in automatically every time a new administrator connects. No manual operations are possible.

5.1 Inviting a new administrator

The first administrator created is allowed to share administration tasks with other users. To do so, this administrator must send them an invitation so that they can create their administration accounts. By default, these invited administrators are granted only privileges to create and edit security policies. For more information, refer to the section [Modifying an administrator's permissions](#).

1. Select the **Administrators** menu on the left.
2. Click on **Invite**.
3. In the **E-mail address** field, enter the e-mail address of the person you wish to invite. The address must be part of the same domain as the corporate account's domain.
4. Click on **Invite**. The new administrator will receive an e-mail telling him to create his administrator account via a link. This link is valid for 72 hours.
5. Select the **Administrators** menu on the left. The administrator that you have just invited will now appear on the list. Only his e-mail address is entered as his invitation remains pending until he creates his administrator account

5.2 Accepting an invitation to manage SDS Enterprise

After you receive an e-mail inviting you to manage SDS Enterprise, you must create your administration account within 72 hours.

1. Open the e-mail that you received from SDS Enterprise.
2. Click on **Create my account**.
3. Fill in the form with information about your account, then click on **Save**.
4. You can now log in to the [SDMC](#) to manage SDS Enterprise according to your privileges. For more information on permissions, refer to the section [Modifying an administrator's permissions](#).

If the 72 hours have lapsed or if the administrator no longer wishes to invite you, an error message will appear when you attempt to access the form. For more information, contact the administrator.



5.3 Managing the list of administrators

- Select the **Administrators** menu on the left. The list of administrators appears. The status of the administrator is shown in the **Creation** column:
 - **Validation pending:** The administrator has received the invitation but has not yet created the account. You can send the e-mail again by clicking on the administrator's row and on **Resend invitation**.
 - **Invitation expired:** The administrator did not create his account within 72 hours and the invitation has expired. You can send the e-mail again by clicking on the administrator's row and on **Resend invitation**.
 - **Date:** The administrator has created the account and can log in to SDMC.


5.4 Modifying an administrator's permissions

To modify an administrator's permissions, you will need the **Global administrator** permission.

1. Select the **Administrators** menu on the left. The list of administrators appears.
2. Click on the administrator whose permissions you would like to modify. The page showing the administrator's properties appears.
3. In the **Permissions** tab, enable or disable the various permissions as needed:
 - **Global administrator** makes it possible to invite other administrators, delete administrators or modify their permissions. Administrators cannot modify this permission on their own.
 - **Managing tokens** makes it possible to generate tokens for access to the API in order to provide them to third-party applications. It also allows you to view and delete the list of tokens.

5.5 Deleting administrators

You can delete administrators if you no longer wish to allow them to manage SDS Enterprise. Connected administrators cannot delete themselves.

1. Select the **Administrators** menu on the left.
2. In the list of administrators, click on the  icon on row of the administrator you want to delete.
3. Click on **Delete permanently**, then confirm.



6. Managing authority certificates and recovery certificates in SDMC

Using SDS Enterprise requires the use of encryption and signature keys. In addition, the keys must be certified by trusted certification authorities.

i Requirements

You must have your own infrastructure to generate encryption and signature keys for the users in the company. You can then distribute them to users in whatever method you choose, for example via smart cards.

SDMC makes it possible to declare the certification authorities that issued certificates containing your users' identities and public keys. These authorities are therefore considered trustworthy.

To do so, you must import the certificates from all authorities in the certificate library, then use them in your security policies.

SDMC also makes it possible to import recovery certificates, which are necessary when users lose their encryption keys. For more information, see the section [Enabling data recovery](#).

Certificates are distributed to users via LDAP directories and added automatically to their trusted address book. For more information, refer to the section [Managing LDAP directories in SDMC](#).

6.1 Understanding the use of user keys and certificates

The following certificate formats are supported:

- *.cer*
- *.cert*
- *.crt*
- *.der*
- *.pem*

If several certificates are available for the same user (in the trusted address book or in an LDAP directory), SDS Enterprise automatically selects the valid certificate with the most recent validity start date.

If the e-mail address of a user changes (e.g., change in marital or employment status), this user's certificate must be renewed (with a publication in the LDAP directory, if necessary) so that their e-mail address is the same as the one on their certificate(s). If this is not the case, other users will no longer be able to send secured messages, or encrypt files or folder for any user whose e-mail address has changed.

Keys generated by your infrastructure must comply with the following PKCS#11 attributes:

- Private key:
 - CKA_DECRYPT
 - CKA_SIGN
 - CKA_SIGN_RECOVER
 - CKA_UNWRAP



- Public key:
 - CKA_ENCRYPT
 - CKA_VERIFY
 - CKA_VERIFY_RECOVER
 - CKA_WRAP


6.2 Importing certificates in SDMC

1. Select the **Certificate library** menu on the left.
2. Click on **Import** at the top on the right.
3. Select the file and certificate type and import it.

The list of certificates shows their names, type, the security policies in which they are used and their expiry date.

After you have imported the certificates of the certification authorities that you consider trustworthy, and recovery certificates, you can use them in your security policies. See section [Creating a policy](#).

6.3 Renaming, deleting or downloading certificates

- In the **Certificate library** menu on the left, click on a certificate's  icon to choose one of three actions.



7. Managing LDAP directories in SDMC

In the SDMC LDAP library, the LDAP directories in your organization that contain your users' certificates can be declared.

Certificates in X509 format contain, in addition to other information, data concerning the holder and the holder's public key. The public key is used for the encryption of confidential data, which can then be sent securely.

LDAP directories make it possible to automatically add users to the trusted address book. For more information on the trusted address book, refer to the section [Managing the trusted address book from the SDS Enterprise agent](#).

Next, you will indicate the LDAP directories to use in your security policies, so that encryption and signature operations can be performed on users' workstations. For more information on how to use directories in your policies, refer to [Configuring corporate directories](#).


7.1 Adding an LDAP directory

1. Select the **LDAP library** menu on the left.
2. Click on **Add** at the top on the right.
3. Fill in all the fields and then add the directory. We recommend indicating an account with read-only access to the directory as logins are saved in plaintext in security policies.

The list of directories shows their names, the security policies in which they are used and the date on which changes were last made.

After you have added the LDAP directories, you can use them in your security policies, For more information, refer to the section [Configuring corporate directories](#).

7.2 Editing, duplicating or deleting LDAP directories

- In the **LDAP library** menu on the left, click on a directory's  icon to choose one of three actions.



8. Managing security policies in SDMC

SDMC makes it possible to create and configure security policies that you can later include in the agent installation packages on users' workstations.

Define the following elements in the policies:

- Encryption, signature and user account management parameters, including account creation and connection settings, data recovery management,
- Feature settings,
- Directory settings,
- Certificate revocation settings,
- Distribution points for policy updates.

You can also configure a policy directly in a `.JSON` file. For more information, refer to the SDS Enterprise *Advanced configuration guide*.

After you have configured a security policy, you can **download** it to **include** it in your agent installation package.


8.1 Creating a policy

You can create new policies or duplicate existing policies.

8.1.1 Creating a new policy

1. Select the **Policies** menu on the left.
2. Click on **Create** at the top on the right.
3. Enter a name for the policy.
4. Select a policy template.
5. Click on **Create** to confirm. The new policy will appear in the list of policies.
6. Click on the row of a policy to configure it. Refer to the following sections for details on parameters.

8.1.2 Creating a policy from an existing policy

1. In the list of policies, click on the  icon of a policy that you want to duplicate.
2. Select the **Duplicate** menu.
3. Enter a name for the policy.
4. Click on **Duplicate**. The duplicated policy appears in the list.
5. Click on the row of a policy to configure it. Refer to the following sections for details on parameters.

8.2 Configuring user accounts

There are three types of user accounts to choose from: Password, smart card or Single Sign-on (SSO).



With password and smart card accounts, corporate users must log in to their SDS Enterprise accounts.

In Single Sign-on mode, users' connection to SDS Enterprise is transparent and automatic when they log in to their Windows session.

In the **Accounts** menu of the security policy, you can choose generic user account settings, account creation settings, and settings for the recovery of encrypted data.

For further information on creating user accounts, refer to [Creating and managing SDS Enterprise accounts on user workstations](#) and [Creating a Single Sign-On \(SSO\) account](#).

8.2.1 Configuring generic account settings

In **Policies > Accounts > Settings**, configure the generic user account settings:

| | |
|--|--|
| Account type | Select an SDS Enterprise account for the following user categories: Smart card, Password, Password and smart card, or Single Sign-on (SSO). For more information on how to use SSO mode, refer to the section Creating a Single Sign-On (SSO) account . |
| Encryption and signature | |
| Encryption algorithm | Algorithm used to encrypt the data. SDS Enterprise offers only the AES algorithm. |
| Signature algorithm | Algorithm used to sign data. Choose SHA-256 or SHA-512. |
| Card or USB token accounts | |
| Middleware | Middleware allows SDS Enterprise to communicate with all types of smart cards and USB tokens. Select the middleware to use on user workstations from the list of middleware supported by SDS Enterprise. Only one middleware solution can be selected for each policy. The Stormshield Data Security middleware is selected and installed by default. In the security policy's <i>.json</i> configuration file, you can manually specify several middleware options to use (<i>cardMiddlewares</i> parameter). For more information, refer to the <i>SDS Enterprise Advanced configuration guide</i> . The middleware must be installed beforehand on user workstations. For more information, see section Configuring the middleware required for Card or USB token accounts . |
| Advanced settings | Here, enable filtering by drive (card or token) when several types of drives are plugged into the same workstation at the same time. This option allows SDS Enterprise to know which drive is used to connect to an SDS Enterprise account. |
| Password accounts | |
| On automatic Windows session lock | These settings make it possible to define the behavior of the SDS Enterprise agent when the Windows session is locked. <ul style="list-style-type: none"> • No actions • Lock SDS session: Locking your session prevents access to your keys. This means that the user can no longer access encrypted data, but can continue to use files that are already open. You can choose to unlock SDS when the Windows session resumes. • Log out of SDS session: Logging out amounts to closing the SDS Enterprise account. As a result, SDS Enterprise features cannot be used. |



8.2.2 Setting account creation parameters

In **Policies > Accounts > Creation**, configure the parameters for the creation of user accounts. User accounts can then be created manually or automatically from SDS Enterprise agents. For further information on creating accounts, refer to [Creating and managing SDS Enterprise accounts on user workstations](#).

| | |
|---|--|
| General Settings | Allow or prohibit the creation of smart card, USB token or password accounts on the SDS Enterprise agent. Smart card and USB token accounts can either be created manually or automatically. Password accounts can only be created manually. These settings are not available when you select an SSO account. |
| Key management | Specify whether you are creating an account with a single key (encryption or signature) or an account with two keys (encryption key and signature key). For the automatic creation of accounts on the agent, select the certification authority(ies) that issue(s) the keys to use to create the account. The authorities found in the list are the ones that were already declared in the certificate library. For more information, refer to the section Managing authority certificates and recovery certificates in SDMC . |
| Password account creation | |
| Password strength | Select the password strength criteria for password accounts. These settings are not available when you select an SSO account. |
| Manual creation of password accounts | For the manual creation of password accounts: Select the source of user certificates (public keys): you can either import certificates in the form of .p12 files, or generate .p12 certificates locally. If you select Generate .p12 certificates locally , SDS Enterprise will generate self-certified certificates when the account is created. Next: <ul style="list-style-type: none"> • Select the size of the keys that SDS Enterprise will generate when it creates the account. • Set the validity period of the certificates in years When creating an account or When renewing a key. |

8.2.3 Enabling data recovery

Recovery accounts make it possible to secure the use of SDS Enterprise. If, for example, a user leaves the company without decrypting all their data, the recovery account will allow them to recover all the data.

Recovery accounts are created by administrators of the public key infrastructure (PKI) that the organization uses.

SDMC makes it possible to list the certificates (public keys) of recovery accounts. This list is specific to each security policy.

Recovery certificates are shared on user workstations via the security policy, so all that users encrypt will also be encrypted with the recovery certificate. Such data can then be decrypted with the recovery account's private key.

**! IMPORTANT**

Recovery accounts must be protected with a sufficiently strong password and kept in a safe location.

Recovery certificates must be added beforehand in the [Certificate library](#) menu.

In **Policies > Accounts > Data recovery**, indicate the recovery certificates that you wish to use for this policy:

1. Click on **Add from library**.
2. Select one or more certificates.
3. Click on **Add**.

On the SDS Enterprise agent side, recovery certificates can be looked up in the user's key ring. For more information, refer to the section [Decrypting a user's data with a recovery certificate](#).

8.3 Configuring features

The **Features** menu in the security policy makes it possible to configure the major features in SDS Enterprise. The license determines which features are available on agents.

8.3.1 Configuring Stormshield Data File

File encryption in Stormshield Data File makes it possible to guarantee the confidentiality of the data that your users process every day. With this feature, encryption and decryption tasks on user-defined event triggers can also be automated.

For more information, refer to *Securing files* in the *SDS Enterprise advanced user guide*.

Configuring file encryption

- Go to **Policies > Features > File**, and enable the settings of your choice.

| | |
|----------------------------------|---|
| Properties | The default encryption format is <i>.sdsx</i> . In this format, the user can edit an encrypted file transparently without the need to decrypt and subsequently re-encrypt it, as was the case with the previous <i>sbox</i> format. |
| Encryption and decryption | Select the items for which you want to allow encryption and decryption. |
| Multiple encryption | <ul style="list-style-type: none"> • If the user frequently needs to encrypt a large volume of files, unselect Confirm encryption for each file. • You can choose whether to encrypt hidden files. |
| Special encryption | <ul style="list-style-type: none"> • When you enable file encryption for a recipient, you will use the recipient's public key for encryption and they will use their private key for decryption. • Self-decrypting files can be shared with recipients who do not have either Stormshield Data File or Security BOX SmartFILE. • SmartFILES can be shared with recipients who only have Security BOX SmartFILE. For more information, see <i>Creating a Security BOX SmartFILE compatible file</i> in the <i>SDS Enterprise Advanced User Guide</i>. |



| | |
|---|--|
| Encryption of read-only files | There are several options available for the encryption of read-only files. |
| Manual encryption and decryption of lists | See the section below on how to use lists. |

For more information on the advanced use of the File feature on the SDS Enterprise agent, refer to the section [Stormshield Data File](#).

Using lists

Encryption and decryption lists can be used to automate file encryption and decryption for error-free ease of use. A file list can also be created to prevent selected files from being encrypted.

Using encryption and decryption lists

Files enrolled in encryption or decryption lists are automatically processed at a predetermined time or when a predetermined event takes place. For example, you can choose to automatically encrypt files when the session is locked, when the user logs out from SDS Enterprise, or at set intervals (e.g., every 15 minutes) as a background task.

- Indicate the paths of the files or folders to be encrypted or decrypted. The list can be exported and imported in .JSON format.



EXAMPLE OF A .JSON FILE

```
{
  "askForConfirmation":false,
  "path":"C:\\Users\\john\\Documents\\Files", "recursive":true
},
{
  "askForConfirmation":false,
  "path":"C:\\Users\\john\\Documents\\Images", "recursive":false
}
```

Encryption and decryption lists can also be used to manually launch a batch encryption or decryption of all of the list items or of selected ones only.

Recursion of automatic file list encryption or decryption defines the sub-folder inclusion behavior. It is set by the **Include sub-folders** option and can either be on or off. Recursion is applied as follows:

- as a mode, it applies to all items and can be enabled and repeated in various screens.
- as a property of a folder, it defines whether only the indicated folder will be encrypted or decrypted automatically or its sub-folders as well.
- as a property of a file, it defines whether only the indicated file will be encrypted or decrypted automatically or whether files with the same name, but located in other folders, will also be encrypted or decrypted.
- as a property of a file set defined by an expression using wildcard characters [* and ?], it defines whether only the file set will be encrypted or decrypted, or whether files of the same name located in other folders, will also be encrypted or decrypted.

Using exclusion lists

For security reasons, you may need to prevent the encryption of certain files so that they will not be encrypted by mistake. You can create an exclusion list, which will contain the list of files that must not be encrypted.



- Indicate the paths of the files or folders to exclude from encryption. The list can be exported and imported in .JSON format.

The recursion principles explained in [Using encryption and decryption lists](#) apply to exclusion lists.

To prevent the encryption of the system folder [C:\WINDOWS\ by default] and the Stormshield Data File installation folder [C:\Program Files\Arkoon\Security BOX by default], we recommend adding these folders to the exclusion list.

Do take note of the following rules as well:

1. If a file/folder belongs to both the encryption and exclusion lists, the exclusion list overrides the encryption list.
2. When several exclusion rules apply to a file, the most restrictive one applies. If one requires confirmation and the other excludes it unconditionally, the file is excluded without any confirmation request.
3. Exclusion rules are enforced between the verification of hidden files and that of read-only files. In other words, if the rules are as follows:
 - a. the hidden files must not be encrypted,
 - b. a confirmation request for read-only files is required.

If both rules apply to a file, it will not be encrypted without a confirmation request.

8.3.2 Configuring Stormshield Data Team

Stormshield Data Team makes it possible to automatically encrypt files wherever they are, in real time and transparently. Encryption is defined by security rules on folders, whether shared or not, and these rules specify which collaborators are authorized to read and edit files stored in the folders.

For more information, refer to *Automatically securing folder content* in the *SDS Enterprise advanced user guide*.

To configure automatic folder encryption:

- Go to **Policies > Features > Team**, and enable the settings of your choice.

| | |
|---------------------------|---|
| Properties | Select the possible actions when changes occur with the collaborators selected in the security rules, or when there is an issue with the user certificate revocation list. In the first option, access to files can be denied to users who have been deleted from a rule. The two options that follow make it possible to retain such users' access to files. |
| Showing co-workers | When a folder is protected by a rule: <ul style="list-style-type: none"> • Either all users can show the rule, regardless of whether they are co-workers in the rule, • Or only co-workers in the rule can show the rule, |



| | |
|---|--|
| Authorizations | <p>These four options correspond to the menus available in the SDS Enterprise pop-up menu when the user right-clicks on a folder.</p> <ul style="list-style-type: none"> • If the option Allow encryption according to the rules defined is enabled, the user will see the Secure according to defined rules pop-up menu, which will allow the encryption of a folder by sharing it with other users. • If the Allow save and restore option is enabled, the user will be able to see the Advanced > Save and Advanced > Restore pop-up menus. • If the option Allow encryption is enabled, the user will see the Secure the folder pop-up menu, which will allow the encryption of a folder without sharing it with other users. • If the Allow deletion option is enabled, the user will be able to see the Advanced > Delete pop-up menu. <p>For detailed information on these menus, refer to <i>Automatically securing folder content</i> in the <i>SDS Enterprise Advanced user guide</i>.</p> |
| Access to encrypted files | <p>Set the rules granting access to files encrypted in a folder. This applies to situations when the user certificate is revoked or has an issue, or when the certificate revocation list can no longer be accessed.</p> |
| Date changes when files are encrypted or decrypted | <p>Select these options if you want the dates on which the file was created, modified or last accessed to be changed every time a file is encrypted or decrypted.</p> |
| Advanced settings | <p>Advanced settings make it possible to change some of the default behavior settings in Stormshield Data Team:</p> <ul style="list-style-type: none"> • By default, the report window remains displayed after encryption. • By default, the encryption progress window is not shown. • By default, encrypted files can be opened in non-secure folders. Do be careful, however. Depending on the application used, if you open an encrypted file in a non-secure folder, a temporary plaintext file may be created in this folder. When you save and close the file, the temporary plaintext replaces the original encrypted file. Moreover, even if you do not save the file, the deleted temporary plaintext file remains on your PC and can be recovered using specialized tools, which is a security risk. • By default, encrypted files and folders are decrypted when they are copied or moved to a non-secure folder. Regardless of the option selected here, the Save agent's pop-up menu always makes it possible to copy encrypted files and secure folders while preserving encryption. For more information on this menu, refer to <i>Saving an encrypted file</i> in the <i>Advanced user guide SDS Enterprise</i>. |

For more information on the advanced use of the Team feature on the SDS Enterprise agent, refer to the section [Stormshield Data Team](#).

8.3.3 Configuring Stormshield Data Disk

With Stormshield Data Disk, virtual encrypted volumes can be created, on which users can securely store confidential data. The disk owner can choose whether to allow co-workers to access their encrypted disk.

For more information, refer to *Creating secure virtual volumes* in the *SDS Enterprise Advanced user guide*.

To configure the creation of encrypted virtual volumes:

- Go to **Policies > Features > Disk**, and enable the settings of your choice.



| | |
|---|---|
| Mount volumes as non removable disks | Depending on your infrastructure, choose whether to mount volumes as virtual or removable disks. |
| Maximum size allowed | Specify in MB the maximum size that the volume can occupy. Enter a size larger than 1MB. |
| File system | Choose the type of file system: NTFS, FAT32 or FAT. |
| Volume name | Indicate the name of the volume that appears in users' Windows Explorer. |
| Automatic volume creation | <ul style="list-style-type: none"> • Select Create a volume automatically if you want a volume to be created the first time the user logs in to SDS Enterprise. You can choose to display a report after the volume is created. • Enter the full path to the file associated with the virtual volume, and in which the user's confidential data will be stored. The file must have a <code>.vbox</code> extension. Windows environment variables can be used in the path to the file (e.g., <code>%PATH%</code>), as well as Windows CSIDL values, and the SDS Enterprise passwords below between <code><></code>: <ul style="list-style-type: none"> <code><UserId></code>: The user's SDS Enterprise identifier, <code><RootPath1></code>: Main folder of user accounts, specified in the policy, <code><RootPath2></code>: Backup folder of user accounts, specified in the policy. <code><COMMON_APPDATA></code>: Folder containing application data for all users, C:\Program Data. <code><COMMON_DOCUMENTS></code>: Folder containing the common files for all users, C:\Users\Public\Documents. <code><DESKTOP></code>: Folder containing files on the desktop, C:\Users\username\Desktop. <code><LOCAL_APPDATA></code>: Folder containing the data of local applications, C:\Users\username\AppData\Local. <code><MYDOCUMENTS></code>: Folder containing the user's files, C:\Users\username\Documents. <code><PROFILE></code>: Folder of the user's profile, C:\Users\username. <code><USERNAME></code>: Windows username. • Specify the size of the volume created automatically. By default, the volume size will be 10% of the disk space available on the user workstation. • Enable or disable automatic mounting of the volume when the user logs in to SDS Enterprise. • Select the Drive letter associated with the volume (Z: by default). |

For more information on the advanced use of the Disk feature on the SDS Enterprise agent, refer to the section [Stormshield Data Virtual Disk](#).

8.3.4 Configuring Stormshield Data Mail

Stormshield Data Mail makes it possible to encrypt and sign e-mails to guarantee their confidentiality and integrity, and confirm the identity of the sender. Stormshield Data Mail runs with the help of an extension built into users' Outlook mail client.

For more information, refer to *Securing e-mails* in the *SDS Enterprise Advanced* user guide.

Securing e-mails: a few concepts

Stormshield Data Mail uses public key cryptography technology.



Each peer has one or several pairs of keys: a private key and a public key. The **public key** is closely guarded by its owner. The **public key** (certificate), by contrast, is freely distributed.

Stormshield Data Mail can use one of the following:

- A single key pair for encryption and signing,
- Two different key pairs, one for encryption, the other for signing.

For more information on key pairs, refer to [Setting account creation parameters](#).

Security level

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

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.

Encryption

The sender encrypts messages with the recipient's public key; the recipient uses their own private key to decrypt 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.

i NOTE

Senders will be able to encrypt an e-mail only if they have a encryption key in their key ring. As a SDS Enterprise account only has one signature key, it cannot be used to encrypt e-mails.

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 signer.

Signers sign messages with their private keys. Recipients verify the signature by using the signer's public key. Since the signer is in sole possession of the private key used to sign the message, the recipient is sure that it has been sent by the signer and that the message has not been modified during its transfer.

i NOTE

Senders will be able to sign an e-mail only if they have a signature key in their key ring. An SDS Enterprise account that only holds an encryption key cannot therefore be used to sign e-mails.

There are two types of signatures: opaque and detached (i.e., plaintext) signatures. Stormshield Data Mail allows e-mails to be sent and received with both types of signature.

Detached signatures allow recipients to read the e-mail even if their messaging software does not support S/MIME format or refuses to display e-mails with signatures that cannot be confirmed. This occurs, for example, when certificates and revocation lists are not available.

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.

When a signed e-mail arrives and is opened in the reading pane or in a new window, SDS Enterprise checks among other things that the sender's e-mail address and the address



specified in the associated certificate match. If they do not match, a warning is displayed in the security lower band of the e-mail received.

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

Trusted address book

Stormshield Data Mail includes a trusted address book that you can use to insert the certificates of correspondents and authorities that you trust.

If you wish to encrypt a message for one or several recipients for whom you do not have valid certificates in your trusted address book, the LDAP directory can be queried automatically. To do so, you must declare an LDAP directory beforehand and enable automatic updates from the LDAP directory. For more information, see the section [Configuring corporate directories](#).

Encrypting and signing e-mails

To configure how e-mails are encrypted and signed:

- Go to **Policies > Features > Mail**, and enable the settings of your choice.

| | |
|-------------------------|--|
| Properties | Select the type of opaque or detached signature to use when sending and receiving e-mails. Refer to the section Digital signatures for further information. If you choose to enable signature and encryption by default on all messages, the user will still be able to disable them on individual messages. |
| PGP encryption | If you choose to allow message encryption and decryption in PGP format, you must specify one or several WKDs (Web Key Directories) to query. Refer to the following line in this table. |
| WKD server | In the Directories menu of the policy, you can indicate the WKD servers to query for PGP encryption. These public key directories allow Stormshield Data Mail to retrieve the public PGP keys belonging to the recipients of encrypted e-mails. For more information, see the section Configuring corporate directories . |
| Directory update | When sending encrypted messages: To update the trusted address book when sending encrypted messages, you must have declared an LDAP directory beforehand. For more information, see the section Configuring corporate directories . When receiving a signed message: Users can send their encryption certificates (their public keys) to their co-workers by sending them a signed e-mail. You can choose whether to allow recipients to manually import the certificate into their trusted address books to update them, and whether to allow the address book to be automatically updated. If you allow these operations only for known authorities, this means that the user's encryption certificate will be imported only if it was issued by an authority with a certificate already in the recipient's trusted address book. |

For more information on the advanced use of the Mail feature on the SDS Enterprise agent, refer to the section [Stormshield Data Mail](#).

8.3.5 Configuring Stormshield Data Sign


Stormshield Data Sign makes it possible to electronically sign documents and guarantee the authenticity of signers' identities and the integrity of what these files contain.

For more information, refer to *Signing files* in the *SDS Enterprise Advanced user guide*.

To configure file signing:

- Go to **Policies > Features > Sign**, and enable the settings of your choice.



| | |
|---|--|
| Properties | <p>Select the file extension that will be used to identify the new file after it is signed. The original file name will be kept; only the file extension is different.</p> <p>The possible extensions are Stormshield Data sign (.p7f) or S/MIME (.p7m).</p> <p>You are advised to select the .p7f file extension to avoid conflict with any other tools that use .p7m files.</p> <p>When you select the .p7f file extension:</p> <ul style="list-style-type: none"> The icon shown below will be displayed over the right top bottom of the original file icon in the explorer.  The file cannot be read by any person using a different electronic signature tool. <p>Use the .p7m format to validate and send files to peers who do not use Stormshield Data Sign, but other RFC 2630-compliant software.</p> |
| Types of signature | <p>Select the types of signature you wish to allow.</p> <p>For more information, refer to Signing files in the SDS Enterprise Advanced user guide.</p> |
| Active content management | <p>Allow or prohibit the signing of files that contain macros or dynamic fields. This is important because the layout or contents of such files can be subsequently modified after they are signed, therefore casting doubt on their integrity.</p> |
| Signature process | <p>Choose whether to force the user to always display the document before signing.</p> |
| Active content detection in PDF files | <p>Choose whether to inform the user when macros are detected in the contents of a PDF file.</p> |
| Active content detection in Microsoft Word files | <p>Choose whether to inform the user when macros or dynamic fields are detected in the contents of a Microsoft Word file.</p> |

8.3.6 Configuring Stormshield Data Shredder

Stormshield Data Shredder guarantees the permanent, irreversible erasure of data that you wish to delete. With it, third parties will not be able to recover, without your knowledge, information that you thought had been deleted.

For more information, refer to the section *Permanently deleting files* in the *SDS Enterprise Advanced user guide*.

To configure the permanent deletion of files:

- Go to **Policies > Features > Shredder**, and enable the settings of your choice.

| | |
|----------------------|--|
| Shredding | <p>Enable or disable the shredding of files and/or folders.</p> |
| Drag and drop | <p>Enable or disable the possibility of dragging and dropping files and folders on the Stormshield Data Shredder icon on the Windows desktop.</p> |
| Miscellaneous | <ul style="list-style-type: none"> Allow or prohibit the interruption of a shredding operation. If interruptions are allowed, the user can click on Stop. Allow or prohibit the use of Stormshield Data Shredder to securely empty the bin. If the option is enabled, the Securely empty the bin pop-up menu will appear on the Shredder icon. |



| | |
|---|--|
| Confirmation request | <p>If the shredding request applies to several files, select the type of confirmation that you wish:</p> <ul style="list-style-type: none"> • Confirm only once for all files: The confirmation of shredding is global. • Confirm for each file: The shredding confirmation applies to Individual files. During the operation, the user can still unselect the checkbox Request confirmation for each file to stop confirmation requests for the following files. |
| Access to Stormshield Data Shredder in Windows | Choose whether to add a Stormshield Data Shredder shortcut to the Windows desktop. The shortcut makes it possible to erase files by dragging and dropping them on the desktop icon. |
| Advanced settings | There are several options available for the encryption of read-only files. |

8.3.7 Configuring Stormshield Data Share

Stormshield Data Share allows users to automatically encrypt files saved in shared spaces synchronized with online hosting services DropBox, OneDrive, OneDrive for Business, SharePoint and Oodrive. This feature depends on Stormshield Data File and cannot run without it.

For more information, refer to the section *Protecting files in synchronized shared spaces* in the *SDS Enterprise Advanced user guide*.

To enable automatic protection:

1. In **Policies > Features > Share**, select the type(s) of synchronized spaces for which you would like to enable automatic protection.
2. In the **Advanced** menu, choose whether to protect all shared space content or a selection of folders. For the second option, select **Protect only the folders below** and add the name or relative path of one or several folders [e.g., *Data\Project* to protect only the sub-folder *Project*].

As Stormshield Data Team does not secure folders in shared spaces, you are advised to configure Team so that its menus do not appear when you right-click on a synchronized folder.

To exclude synchronized folders from the Team perimeter:

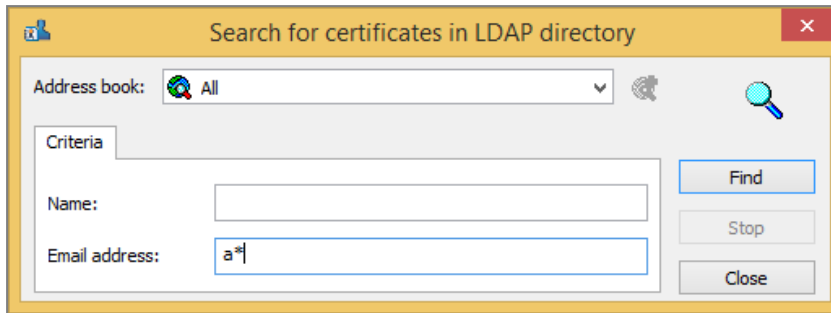
- Configure the `excludedFolders` parameter in the security policy's `.json` file. For more information, see section *Stormshield Data Team* in the *Advanced configuration guide*.

8.4 Configuring corporate directories

In a security policy, you can indicate the LDAP directories to use to provide user certificates and configure the certificate search criteria in the directory.

Directories must be added beforehand in the [Certificate library](#) menu.

Directories selected in a security policy make it possible to automatically add users to local trusted address book. From their trusted address books, users can also manually search for certificates originating from LDAP directories selected in the policy:



The configuration of the trusted address book and associated LDAP directories can be looked up in read-only mode from the SDS Enterprise agent.

For more information, refer to the section [Managing the trusted address book from the SDS Enterprise agent](#).

SDMC also makes it possible to indicate the addresses of the WKD servers used to encrypt PGP messages.

8.4.1 Adding LDAP directories from the library

To add an LDAP directory:

1. In **Policy > Directories > LDAP**, allow the use of the generic character "*" as a suffix if necessary, and the inclusion of the search filter "usercertificate; binary".
2. Click on **Add from library** in **LDAP/LDAPS directories**.
3. Select one or more directories.
4. Change the order of directories if necessary by clicking and dragging.

8.4.2 Configuring automatic directory updates

Every time the corporate LDAP directory is updated, SDMC makes it possible to automatically update the local trusted address book to reflect changes.

The options in the **Trusted directory update** section in the **Policy > Directories > LDAP** menu enable the modular configuration of automatic updates.

| | |
|---|---|
| Activation and execution | <ul style="list-style-type: none"> • Update the directory automatically: if this option is disabled, the options in the sections Activation and execution and Certificates update from an LDAP directory are grayed out. • Update frequency: indicate a value between 0 and 24. • Start the directory update when the user connects to the SDS account: enable this option to update the directory every time the user logs in, regardless of the update frequency defined above. |
| Certificates update from an LDAP directory | Enable these options to update the statuses of certificates in the local directory. |
| Deletion of certificates expired/revoked/removed from the LDAP | If you do not wish to delete from the local directory certificates that have expired or been revoked or removed from the LDAP directory, you can select the issuing certification authorities to filter the certificates that you wish to delete. |



8.4.3 Adding WKD servers to encrypt messages in PGP format

To enable users to send and receive e-mails encrypted in PGP format with the Stormshield Data Mail feature, you must:

- Enable PGP message encryption/decryption in **Features** > **Mail** in the policy.
- Add the addresses of one or several WKDs (Web Key Directories) to query in **Directories** > **PGP**. These public key directories allow Stormshield Data Mail to retrieve the public PGP keys belonging to the recipients of encrypted e-mails.

To add WKD servers:

- In the **PGP** tab in the **Directories** menu, indicate the URLs of the WKD servers by following one of the formats below, and by adapting them to the domain (or sub-domain) names of the servers:
 - **https://openpgpkey.optional-sub-domains.domain.toplevel/.well-known/openpgpkey/<d>/hu/<k>?get_parameters=optional**
 - **https://optional-sub-domains.domain.domain.toplevel/.well-known/openpgpkey/hu/<k>?get_parameters=optional**
Sections in bold in the URLs must be maintained as they are.

SDS Enterprise communicates with WKD servers in HTTPS. All computers on which Stormshield Data Mail has been installed must therefore have the certificate from the authority that issued the SSL certificate of the WKD server.

8.5 Adding certification authorities and configuring certificate revocation control

SDMC makes it possible to add certificates from your certification authorities to your security policies, so that the SDS Enterprise agent can monitor users' certificate trust chain.

It also allows you to set up revocation control, which is the only way to indicate that a user's certificate must no longer be used. For example, if the owner of the certificate no longer belongs to a group, if the user's key may have been compromised, or if the user has obtained another certificate.

Revocation control can be performed either thanks to a Certificate Revocation List (CRL) or thanks to the OCSP protocol. In this case, the OCSP responder's URL address must be specified in the certificate.

Such data is generated by the administrator of the public key infrastructure (PKI) that the organization uses.

SDMC makes it possible to list the CRL distribution points for every certification authority that issues certificates to your users. This list is specific to each security policy.

SDS Enterprise agents download CRLs from the indicated distribution points so that the validity of users' certificates can be verified.

8.5.1 Understanding revocation control

Three aspects of a certificate are verified:



- The certificate itself: format, validity dates, signature, extension, etc.;
- The trust chain: It must be possible to establish a complete chain, up to the certificate from a trusted authority. Each certificate must meet the same level of security as the original certificate being checked. When a certificate in a chain cannot be validated, another chain is verified, until a valid chain is found.
- Revocation control. This check ensures that each certificate in the chain is not on a CRL supplied by the certification authority (or a third party that has the delegation to create CRLs). Since CRLs are also signed by a certificate, the control also checks the certificates applied at the level of the CRLs.

8.5.2 Understanding revocation lists

The CRL verification mechanism is described in the standards governing certificates and CRLs (X.509 standard, RFC 3280 and RFC 5280).

There are two ways in which SDS Enterprise agents can obtain the CRLs to be downloaded locally for certificate verifications:

- From the CRL distribution list set in the authorities' certificate settings,
- From the custom CRL distribution lists indicated for each authority, in the security policy in SDMC.

You can set the number of days CRLs will remain valid.

8.5.3 Adding the certification authority's certificates

When you add certification authority certificates in SDMC, they can be looked up in the **Authority** tab in the trusted address book on user workstations. These certificates allow the SDS Enterprise agent to guarantee that user certificates are issued by trusted authorities and to verify the validity of the certificates.

To add a certificate:

1. In **Policy > Authorities**, click on **Add from library** to the left of the panel.
2. Select one or more certificates out of the ones that were added earlier in the **Certificate library** menu.

The settings of certification authority certificates contain CRL distribution lists. If you wish to indicate the custom CRL distribution lists for each authority, refer to the following section.

8.5.4 Configuring revocation control in a policy

To customize the CRL distribution points for each certification authority, go to **Policy > Authorities**. You can indicate as many distribution points as you need. To download CRLs, the SDS Enterprise agent looks up these distribution points in addition to the one indicated in the certificate of each authority.

1. Indicate a CRL validity period. This is the duration after which the SDS Enterprise agent downloads CRLs again locally to ensure that they always have updated data.
2. Select a certification authority from the left side of the panel.



3. To the right of the panel, indicate one or several CRL distribution points for each selected authority. The distribution point can be accessed via the following protocols:
 - http:// or https://
 - LDAP:// or LDAPS://
 - file:///
4. Change the order of distribution points if necessary by clicking and dragging.

From their SDS Enterprise accounts, users can look up the list of certification authorities and CRL distribution points. For more information, refer to the section [Looking up certification authorities from the SDS Enterprise agent](#).

8.6 Configuring policy distribution points

In the **Policies > Distribution** menu, indicate one or several distribution points for each security policy. These points contain the update files of policies.

When the workstation starts up, the Stormshield Data Security Enterprise agent will check the list of distribution points in the order you have set. It will apply the first valid policy that it detects; this policy must be accessible, signed and more recent than the current policy.

To configure distribution points:

1. In the **Full path to the policy file** field, enter the full path to the *.jwt* policy file of your choice. The path must begin with one of the following prefixes:

| Prefix | Examples |
|----------|---|
| http:// | http://mycompany.example.com/folder/policy.jwt |
| https:// | https://mycompany.example.com/folder/policy.jwt |
| file: | file://myserver/sharing/folder/policy.jwt file:///c:/folder/policy.jwt |

2. Click on + to add the path to the list. The button is disabled if the path already exists or if the prefix is wrong.
3. Repeat the operation for every distribution point to declare.
4. Drag and drop items to change the sequence of distribution points whenever necessary. SDS Enterprise agents will analyze the distribution points in the order of their appearance in the list.

Once you have declared the distribution points, you must provide the policy update files so that they will be deployed on the SDS Enterprise agents. For further information, refer to the section [Updating the policy on SDS Enterprise agents](#).



9. Installing SDS Enterprise agents on user workstations

SDS Enterprise agents make it possible to apply the security policies defined in SDMC and use the product's features on users' workstations.

Follow the steps below to install SDS Enterprise agent on workstations:

1. Download the policies,
2. Sign the policies with the utility provided by Stormshield,
3. Download the SDS Enterprise agent installation package,
4. Deploy the SDS Enterprise agents on user workstations,
5. Deploy the signed security policy file and the peer certificate on user workstations.

9.1 Finding out the system requirements for SDS Enterprise

SDS Enterprise is a solution for workstations running 64-bit Microsoft Windows.

To find out which Microsoft Windows versions are compatible, refer to the *Product life cycle section*.

If you choose to deploy the agent installation package in silent mode, the prior installation of the VSTO Runtime 4.0 Office 2010 package is required for the Stormshield Data Mail feature. The VSTO package is available from your [MyStormshield](#) client area (**Downloads > Stormshield Data Security > Enterprise > Tools** menu).

i NOTE

Domain users cannot install the agent while authenticated in Windows with a user account if User Account Control (UAC) is enabled because privilege escalation does not function.

! IMPORTANT


The SDS Enterprise agent is not compatible with the **Fast User Switching** feature.

9.2 Downloading security policies

When your security policy is ready to be deployed on SDS Enterprise agents, you must download it from SDMC to sign it then include it in the agent installation package .

For more information on signing policies and customizing packages, refer to [Signing security policies](#) and [Deploying the SDS Enterprise agent installation package on user workstations](#).

To download a policy (.JSON format):

1. Select the **Policies** menu on the left,
2. In the list of policies, click on the  icon of a policy that you want to download.
3. Click on **Download**.



9.3 Signing security policies

Before integrating a security policy into an installation package, you must sign the policy to guarantee its authenticity and integrity.

Stormshield provides a utility that allows you to sign your policies.

The signature is based on the JWT standard. The algorithm used is HS256.

The signature utility makes it possible to sign several policies at the same time if needed.

9.3.1 Requirements

To sign a security policy, you need:

- A *.p12* file containing a private signature key. We recommend that you protect the file with a strong password.
- To download the utility *SDSPolicySignCLI.exe* from the **Downloads** menu in SDMC.
- To download the policy in *.JSON* format if you have already configured it in SDMC. To download the policy, refer to [Downloading security policies](#).

9.3.2 Signing the policy

1. Run the *SDSPolicySignCLI.exe* tool in command line. To display the list of commands, type `-help`:

| | |
|-------------------------------|--|
| <code>-k or --key</code> | Mandatory parameter. Indicates the relative or absolute path to the folder of the <i>.p12</i> file that allows the signature. |
| <code>-p or --password</code> | Password that protects the <i>.p12</i> file. If the file is protected with a password and you do not enter the parameter manually, you will be automatically asked to enter the password (recommended method). |
| <code>-f or --file</code> | Mandatory parameter. Indicates the relative or absolute path to the folder of the <i>.json</i> file of the policy to be signed. You can indicate several files by separating them with commas or spaces. |
| <code>--help</code> | Shows help. |
| <code>--version</code> | Shows the version of the utility. |

2. When the file is being signed, a sub-folder with the name of the policy will be created at the same location as the policy file. This folder contains the signed *policy.jwt* file. Retrieve this file to include it in the agent installation package, as shown in the following section.



EXAMPLE

```
C:\Myfolder\SDSPolicySignCLI.exe --key C:\Keys\MyPrivateKey.p12 --file  
C:\Policies\Policy1.json C:\Policies\Policy2.json
```

Replace the names of folders and files with those on your own workstation. In this example, the policies are signed in the files *C:\Policies\Policy1\policy.jwt* and *C:\Policies\Policy2\policy.jwt* respectively.

9.4 Downloading SDS Enterprise agents' installation packages form SDMC

You can choose to download an *.msi* or *.exe* package from SDMC:



1. Select the **Downloads** menu on the left.
2. Select the `.msi` or `.exe` package from the upper section in the language of your choice:

`.msi` Package allowing the product to be installed in silent mode. See [Deploying the SDS Enterprise agent installation package on user workstations](#).

`.exe` Standalone package allowing the solution and its requirements to be installed in interactive mode. See [Deploying the SDS Enterprise agent installation package on user workstations](#).

3. Download the package and refer to the following section for details on how to deploy it.

The links on the download page redirect you to the [MyStormshield](#) client area. By default, the latest available version of the agent will be downloaded. If you wish to download an earlier version, go to your [MyStormshield](#) client area.

9.5 Deploying the SDS Enterprise agent installation package on user workstations

To deploy the SDS Enterprise agent installation package on user workstations, you can choose either an interactive or silent installation. You can also choose the features to be deployed.

After the agents are deployed, you must deploy the signed security policy file and the peer certificate on user workstations in the folders indicated below, so that the SDS Enterprise agents will apply your security policy.

You must hold administrator privileges on the computer in order to deploy the SDS Enterprise agent.

i NOTE

Before installing the Stormshield Data Mail feature, ensure that your appliance pool uses a Windows version compatible with SDS Enterprise. For more information on compatibility, refer to the section *Product life cycle*.

9.5.1 Choosing the installation package deployment mode

There are two ways to deploy packages:

- **Interactive mode:** standalone mode using the `.exe` package. Click on the custom `.exe` package to launch the installation. Once you have entered the license key and accepted the license contract, you can install all the product features allowed by the license key.
- **Silent mode:** the installation requires no user interaction. This mode uses the `.msi` package. Refer to the [requirements](#) before installing the package. An administrator can then install the `.msi` package with the usual Windows Installer commands. If the package is not installed with administrator privileges, the installation will fail (error 1925).

To deploy the `.msi` package in silent mode, you can use the Windows Installer `msiexec` package editing tool or [Microsoft Endpoint Configuration Manager](#).

To use the `msiexec` tool, the procedure is as follows:



1. Open a command line window as an administrator,
2. Enter the following command:


```
msiexec /qn /i "<path>Stormshield Data Security 11.0"
LICENCENUM=<licensenum>
```

<licensenum> consists of 16 characters without spaces.
3. All the features allowed with the license will then be installed. The `REMOVE` property (refer to section [Configuring preselected features](#)) allows you to restrict the features installed. Once the installation is complete, SDS Enterprise will automatically run every time you start Windows.

There are several variants to the command:

- `/qn`: installation without any window,
- `/qn+`: installation with a final confirmation window,
- `/qb`: installation with a window that shows a progress bar and estimated remaining time,
- `/qb+`: installation with a window that shows a progress bar and estimated remaining time, and a final confirmation window.

i NOTE

The `/norestart` command is not supported. To prevent the computer from restarting, create a `.mst` with the relevant options.

9.5.2 Deploying the signed security policy file and the peer certificate

After having deployed the SDS Enterprise agent on user workstations via the `.exe` or `.msi` package, you must deploy the following files on the workstations so that the agents will apply your security policy:

- The signed policy file named `policy.jwt`,
- The certificate (public key) with which the signature of the policy can be verified. It must be named `admin_policy.cer`.

To deploy these files in their intended folders:

1. Save the signed policy file named `policy.jwt` in the folder named `%programdata%\Stormshield\Stormshield Data Security`, or replace it if it already exists.
2. Save the certificate named `admin_policy.cer` in the sub-folder named `Program Files 64\Arkoon\Security BOX` in the SDS Enterprise installation folder, or replace it if it already exists.

9.5.3 Configuring preselected features

The `REMOVE` property can be used to restrict the number of features that the user is allowed to install, even when the license key allows other features.

For example, you can create several installation profiles with only one license key and one installation package.

Below is the list of possible values:

| Code | Removed feature |
|----------|-----------------------|
| SBoxFile | Stormshield Data File |



| Code | Removed feature |
|----------------------|--|
| SBoxShare | Stormshield Data Share (the Share feature is a Stormshield Data File sub-feature, which will be automatically deleted if Stormshield Data File is deleted) |
| SBoxDisk | Stormshield Data Virtual Disk |
| SBoxShredder | Stormshield Data Shredder |
| SBoxMailOutlookAddIn | Stormshield Data Mail |
| SBoxTeam | Stormshield Data Team |
| SBoxExtCarte | Stormshield Data Card Extension |
| SBoxSign | Stormshield Data Sign |
| SBoxConnector | Stormshield Data Connector |

When setting the value of the `REMOVE` property, the features that you want to prevent the user from installing must be separated by a comma without any spaces.

For example, to install the `.msi` package by deleting Stormshield Data File and Stormshield Data Virtual Disk as features:

1. Open a command line window as an administrator,
2. Enter the following command:

```
msiexec /i "<path>\ Stormshield Data Security 11.0"  
LICENCENUM=<SBOXLICENCENUM> REMOVE=SBoxFile,SBoxDisk
```

9.6 Updating the policy on SDS Enterprise agents

After a policy is initially deployed on agents, you can automatically update it on your pool by placing it on a server that acts as a distribution point.

The distribution points must first be declared in the policies. For more information, refer to the section [Configuring policy distribution points](#).

1. Download the `.json` file of the policy that you have updated. For more information, refer to the section [Downloading security policies](#).
2. Sign the file. For more information, refer to the section [Signing security policies](#).
3. Copy the file to the distribution points that you have declared for this policy.

The next time the agent starts, it will check whether a new update is available, and if so, the agent will automatically apply it.

If no distribution points have been declared, the policy can also be manually updated by replacing the policy file locally.



10. Creating and managing SDS Enterprise accounts on user workstations

When agents are deployed on user workstations, users need SDS Enterprise accounts in order to use the product's features.

Depending on the account types defined in the policy, accounts are created either manually or automatically:

- Password accounts: manual
- Smart card and USB token accounts: manual or automatic
- Single Sign-on (SSO) accounts: automatic with transparent authentication

Regardless of the account type, you must allow account creation beforehand in the security policy. For more information, see the section [Configuring user accounts](#).

Creating your account may involve creating your main key(s), which will be used for securing your files, volumes and messages, and self-certifying the key so that you can use it immediately.

Once users have SDS Enterprise accounts, the product is ready for use. For find out how to use SDS Enterprise, refer to the SDS Enterprise *Advanced user guide*

10.1 Configuring the middleware required for Card or USB token accounts

To communicate with a smart card or USB token, SDS Enterprise requires the presence of middleware on user workstations.

SDS Enterprise makes it possible to use any smart card or USB token as long as its vendor provides a compatible PKCS#11 cryptographic module (standard interface).

SDS Enterprise provides the Stormshield Data Security middleware by default, but you can use others by specifying them in the security policy.

In this case, you must manually install the middleware on the users' workstations.

For smart cards and tokens by vendors that have published mini drivers with Microsoft, the Stormshield Data Security middleware provided by default can be used so that plug-and-play can be supported.

In addition, to operate the Card or USB token account type for your users, you must first install the card extension on the workstations, as described in the sections below.

The Card Extension Configurator allows you to view the middleware used by SDS Enterprise to communicate with the card or USB token. The middleware used is registered in the registry database. If required, the extension also allows you to select another middleware that you specified in the security policy.

The installation of the extension is also required for the operation of Single Sign-on (SSO) accounts. The Stormshield Data Security middleware is used for this type of account. For more information on how to use SSO accounts, refer to the section [Creating a Single Sign-On \(SSO\) account](#).

10.1.1 Specifying a list of middleware in the security policy

The security policy lists the middleware that can be used by SDS Enterprise on user workstations to communicate with USB cards or tokens.



If you configure the security policy via SDMC, see [Configuring generic account settings](#). By default, the Stormshield Data Security middleware is selected. Only one middleware solution can be selected via SDMC.

In the security policy's *.json* configuration file, you can manually specify several middleware options to use (*cardMiddlewares* parameter). For more information, refer to the *SDS Enterprise Advanced configuration guide*.

When the security policy is deployed and taken into account by the user workstations, the middleware to be used is registered in the registry. If more than one middleware is specified in the policy, SDS Enterprise takes into account, in order of appearance, the first middleware in the list that is functional on the workstation. This means that it must be available and run without errors.

The configuration information of the middleware used is written in the following registry keys:

- **HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Kernel\Components\Pkix**
 - *Pkcs11CardDll*: path to the middleware DLL,
 - *Pkcs11CardLabel*: middleware name.
- **HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Properties\NewUserWizardGP1 and NewUserWizardGP2**
 - *eCKA_[ATTRIBUTE]*: parameters that monitor the use of various PKCS#11 attributes during communication with smart cards/USB tokens.

Each time you start SDS Enterprise, the registry tells you which middleware to use. We do not recommend that you change these values manually.

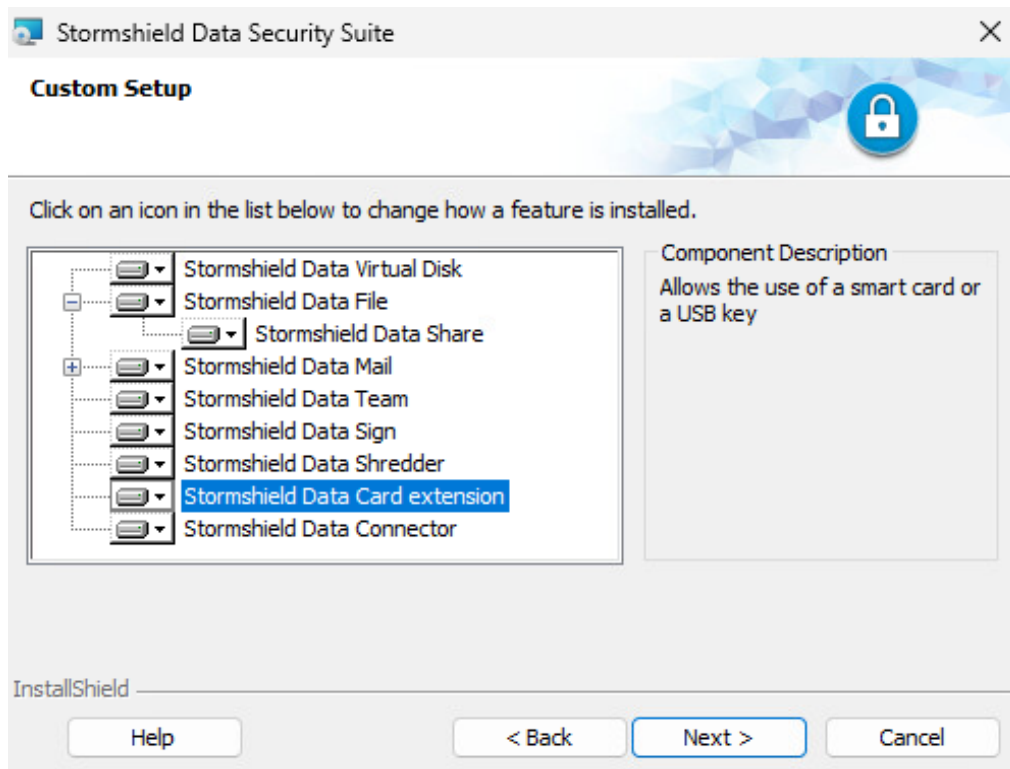
You can select another middleware to use at any time from a user's workstation. The values in the registry are then updated automatically. For further information, refer to the section [Configuring log management](#).

10.1.2 Installing the smart card extension

The SDS Enterprise extension for smart cards and USB tokens or Single Sign-On accounts can be installed on workstations at the same time as the other features. For further information, refer to [Deploying the SDS Enterprise agent installation package on user workstations](#).

For subsequent installations, follow the steps below:

1. Open the **Start** menu in the user workstation taskbar.
2. Open the **Control panel** and select **Add/Delete programs**.
3. From the list of programs, select SDS Enterprise.
4. Click on **Change**. You will be in **Maintenance** mode.
5. Select **Modify** then go through the screens that follow.



6. Select **Stormshield Data Card extension**.
7. Complete the installation procedure.

10.1.3 Configuring the smart card extension

To open the Map Extension Configurator:

- Click on the **Start > Stormshield Data Security Suite > Card extension configurator** menu.

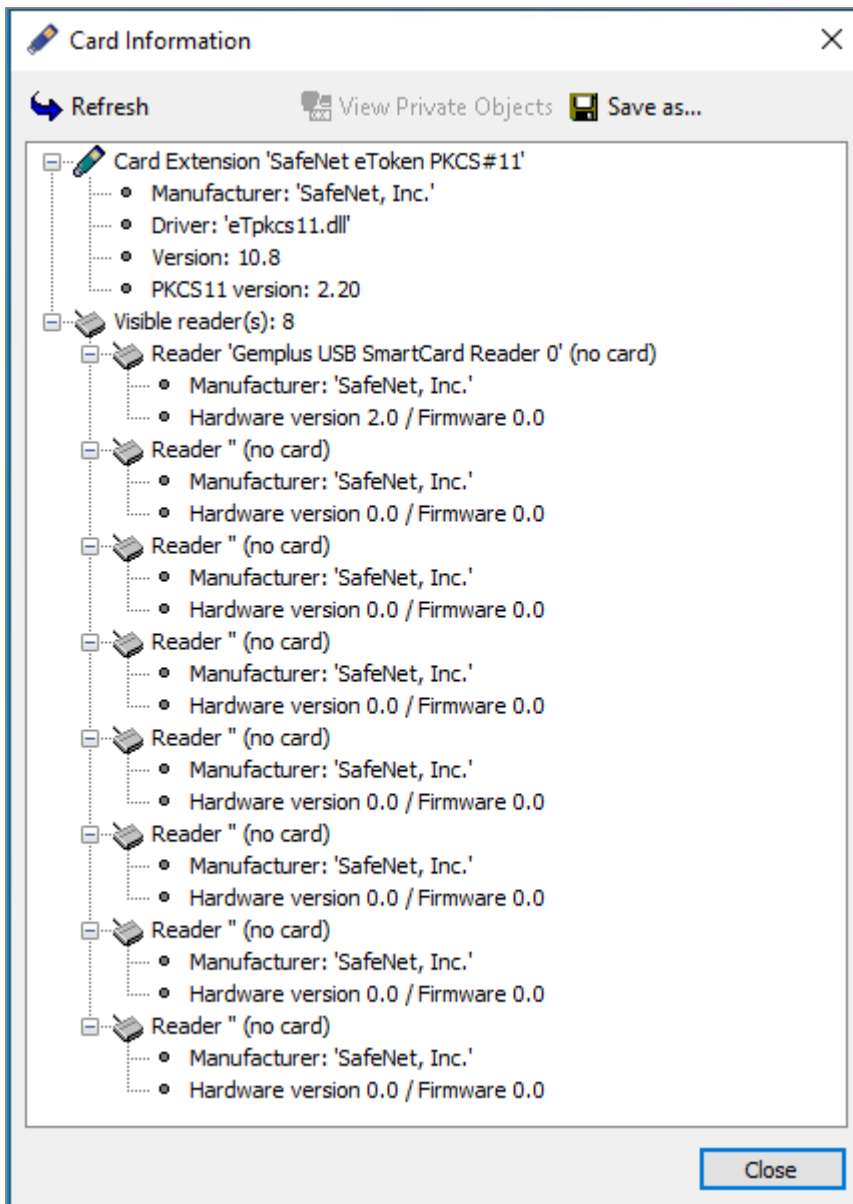
The **Card or USB stick type** menu displays the middleware used by SDS Enterprise on the workstation, as defined by the security policy.

You can select another middleware. The drop-down list shows all those specified in the security policy, in the order they appear in the policy. In this case, the middleware configuration is changed in the registry and a restart of SDS Enterprise is required.

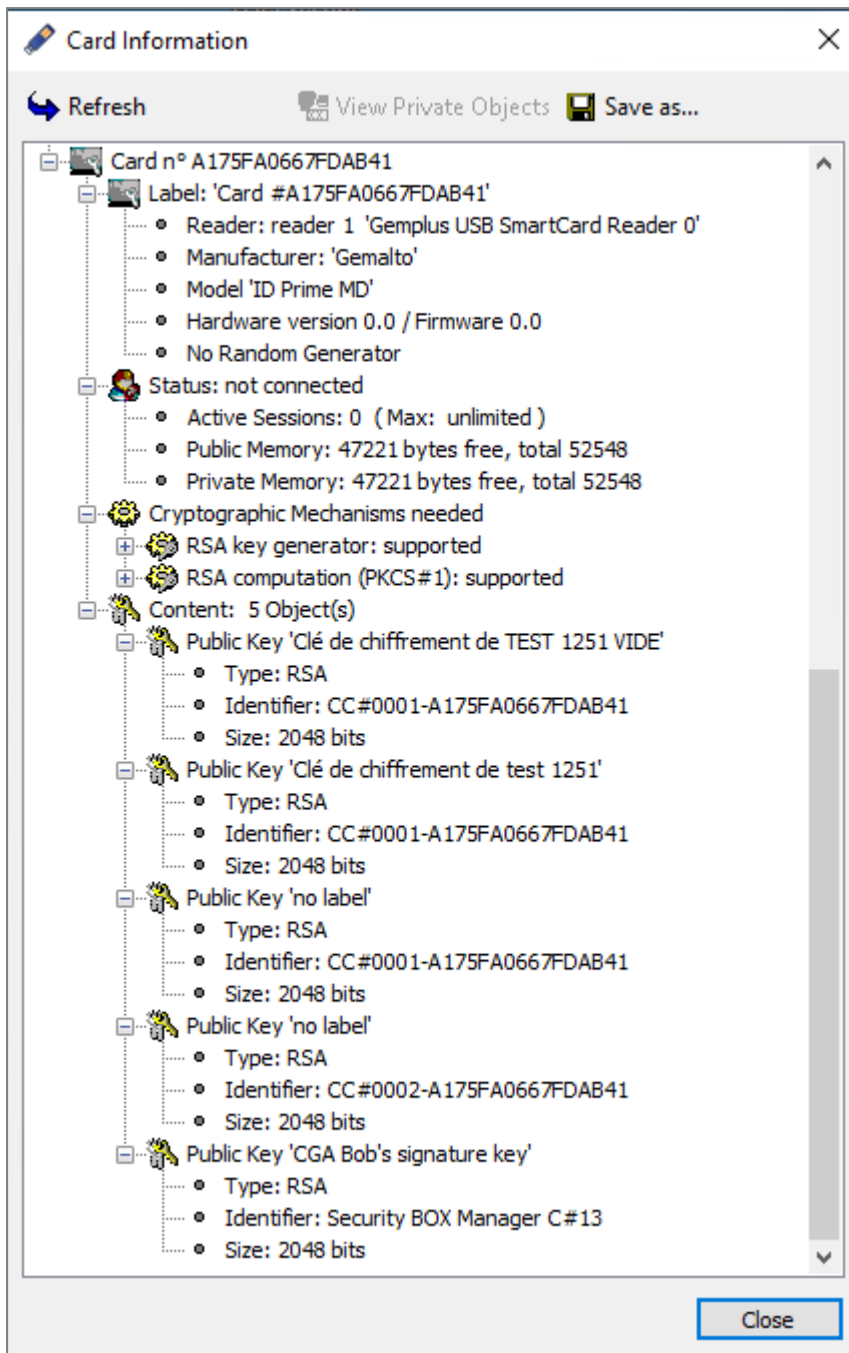
If the newly selected middleware is not available, an error is displayed.

- Click **Information** to investigate card or token access issues. The menu is used to test the *PKCS#11* interface module: the number of readers visible is indicated. If the *PKCS#11* DLL cannot be reached, an error message will indicate it. In this case, simply verify the name and path of the DLL and verify whether the required items for this DLL are present (especially other DLLs).


The following screen capture shows that the card extension exists and is configured for Gemalto smart cards. However, there are no actual USB tokens.



The following screen capture shows that a USB token is inserted and presents the USB token's characteristics as well as public objects such as public keys and certificates.



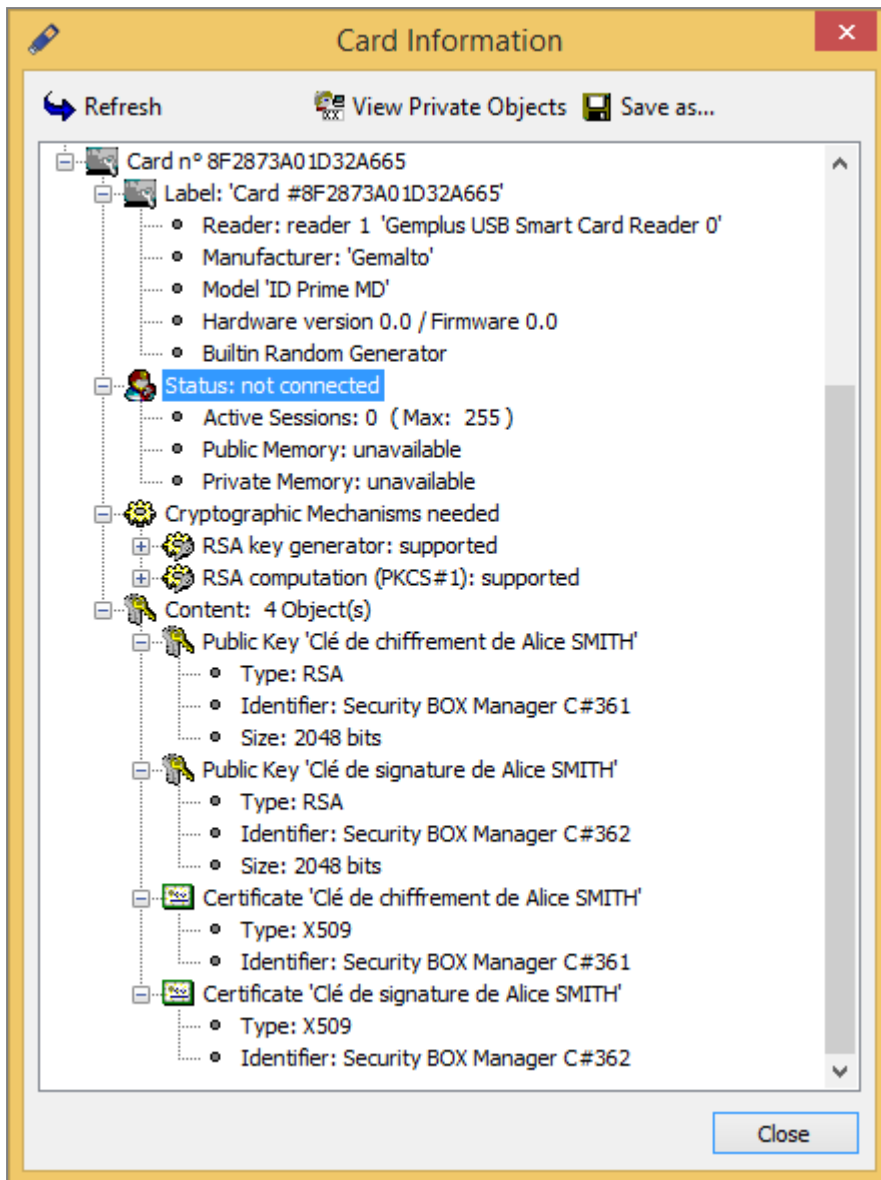
You can also select another middleware from the SDS Enterprise menu:

- By right-clicking on the SDS Enterprise  icon in the Windows taskbar, then by selecting the menu **Select smart card or USB token**. The menu is only visible when no user is logged in. Unlike the Map Extension Configurator, this menu only displays the middleware installed on the workstation and functional.

10.1.4 Viewing private objects

You can view private objects (essentially private keys) in the **Card extension configurator**:

1. Click on **Information**.
2. Select the line **Status: not connected** in the information window.



3. Click on **View private objects**. This button will not be available if the previous line is not selected.

4. Enter the PIN.

The **Save as** button makes it possible to save the content of the window in a text file.

10.2 Creating smart card or USB token accounts

To create a smart card or USB token account, enable automatic account creation in SDMC so that the account creation process is transparent for the user when they insert their USB token or smart card for the first time. You can also manually create an account from the agent on the workstation.

In either case, the Stormshield Data Card Extension feature must be installed on users' workstations, with the other features from the SDS Enterprise agent. For more information, refer to the sections [Deploying the SDS Enterprise agent installation package on user workstations](#) and [Configuring the middleware required for Card or USB token accounts](#).

With a smart card or a USB token:



- Your private keys and certificates are stored on the smart card,
- The smart card will perform the calculations (signature and decryption) that generate your private keys.


When an account associated with a smart card is created, the smart card must already contain the associated private keys and certificates.

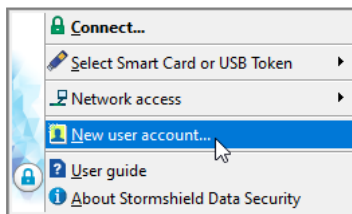
10.2.1 Creating accounts automatically

To make it easier to deploy smart card or USB token accounts and to minimize user intervention, SDS Enterprise can automatically create the user's account when the card or token is inserted for the first time. To do so, you must first install and configure the required middleware and enable the feature in SDMC. To select the appropriate middleware and enable automatic account creation, refer to the sections [Configuring generic account settings](#) and [Setting account creation parameters](#).

The user then simply inserts their smart card or USB token. SDS Enterprise automatically detects that there is no existing account associated and proposes to create one. To continue, the user only needs to enter the PIN for the smart card or USB token, and the SDS Enterprise account is then created.

10.2.2 Creating accounts manually

1. On the user workstation, insert the USB card or token.
2. Right-click the SDS Enterprise icon  in the system tray.
3. Select **New user**.



4. Select **Account with physical or virtual smart card**.
5. Click on **Create your account**.
6. Select the smart card or USB token you wish to use.
7. Enter the PIN code of the USB card or token. SDS Enterprise connects to the USB card or token and displays its contents (keys and certificates).
8. Validate the following screens. If the card or the USB token contains several usable keys, choose the desired key.
9. Check the account summary.
10. Click on **Finish**.

The SDS Enterprise account created using a smart card or USB token has the serial number of the card or token as an identifier.

10.2.3 Using keys from the smart card or USB token

In addition to the user's current keys, other encryption keys may be saved on the smart card or USB token.



SDS Enterprise automatically uses these encryption keys to decrypt documents (messages/files) when the current key cannot do it.

These keys can come from several sources:

- The user's old encryption keys. Obsolete keys may be saved on the card (with their associated certificates) to allow the user to decrypt files that were encrypted with old keys. This is particularly useful for archived files,
- External keys. For example, keys for former employees that can be used to retrieve information (files/messages).

Depending on the SDS Enterprise features, the keys on the card are not identified in the same way. For some features, the keys are identified by their CKA_ID PKCS#11 attribute (so they must always keep the same CKA_ID value), but for other features, identification is done using information from the certificate (issuer and serial number).

We recommend that keys stored on the cards always have the same CKA_ID PKCS#11 attribute and that all of the associated certificates are also present.

10.3 Creating password accounts manually

There are two ways to create an SDS Enterprise password account:

- By generating a key or two keys via SDS Enterprise,
- By importing a key that was saved earlier in a file (PKCS#12 format, P12 or PFX extensions).


If you are creating an account with two keys (encryption and signature), depending on the security and certification policies defined in SDMC, you can use either method to create each key.

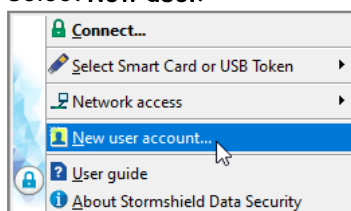
10.3.1 Generating keys

Generated keys will be used to secure files and e-mails, for example. These keys are self-certified, so that SDS Enterprise can use them immediately. However, they will not be automatically trusted by peers but can be certified later by a certification authority.

You can create two separate keys to encrypt and sign. In this case, you will need to repeat the procedure below. It describes how to create an encryption key.

To generate a key:

1. On the user workstation, right-click on the SDS Enterprise  icon in the Windows system tray.
2. Select **New user**.



3. Select **Account with password**.
4. Click on **Create your account**.
5. Enter a login and password. You will be asked to enter them to connect to SDS Enterprise.
6. Click on **Next**.



7. Select **Generate your encryption key** and select the key type.
8. Click on **Next**.
9. In the next window, generate a key from random numbers by moving the mouse or typing on the keyboard.
Once the random number has been captured, click on **Next**.
10. Enter the details that make up the user's identity, as you want them to appear on the self-certified certificate.
11. Click on **Next**.
12. Set a backup password, which you will be asked to provide if you forget the main password or if users are locked out of their accounts when they consecutively enter the wrong code too many times . For more information, please refer to the section [Unblocking user accounts](#).
Click on **Next**.
13. Check the account summary.
14. Click on **Finish**.

SDS Enterprise will generate the keys and create the account.

The account includes a personal self-certified certificate. Since the certificate was created by the user, it may not be trusted by some peers, who only trust certificates created by known authorities. We recommend using certified keys issued from a PKI (*Public Key Infrastructure*).



10.3.2 Importing keys

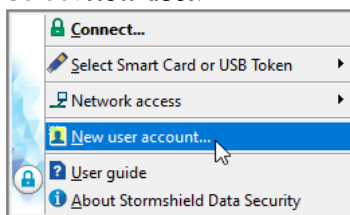
This section explains how to create an account by retrieving keys and certificates saved in a *PKCS#12* format (extensions *P12* or *PFX*).

This feature makes it possible to use a previously generated key and its associated certificate, or a key generated centrally by a PKI. This feature also makes it possible to save private keys that can be used for recovery operations.

The actions described below apply to both the encryption key and the signature key.

1. On the user workstation, right-click on the SDS Enterprise  icon in the Windows system tray.

2. Select **New user**.



3. Select **Account with password**.

4. Click on **Create your account**.

5. Enter a login and password. You will be asked to enter them to connect to SDS Enterprise.

6. Click on **Next**.

7. Select **Import your personal key** and:

- select the file in the *PKCS#12* format with the *P12* or *PFX* extension,
- enter the password that protects the key stored in this file.

Stormshield - Account creation - Personal key

STORMSHIELD Data Security

Generate your personal key

Key type: RSA 2048 bits

Import your personal key

File: C:\tmp\SMITH Alice.p12

Password:

< Back Next > Cancel

8. Click on **Next**.

If the file contains several keys or certificates, select the key to be imported and the certificate associated with this key.

9. Click on **Next**.



10. Set a backup password, which you will be asked to provide if you forget the main password or if users are locked out of their accounts when they consecutively enter the wrong code too many times (three times by default). For more information, please refer to the section [Unblocking user accounts](#).
Click on **Next**.
11. Check the account summary.
12. Click on **Finish**.
SDS Enterprise will import the key and create the account.

10.4 Creating a Single Sign-On (SSO) account

SDS Enterprise allows users to log in to SDS Enterprise automatically and seamlessly using the SSO mode that links the SDS Enterprise account to their Windows user account. SDS Enterprise uses the encryption and signature keys stored in the Windows Certificate Store.

In the security policy, the use of SSO accounts can be configured. User accounts will then be automatically created on their workstations.

10.4.1 Requirement

- The Stormshield Data Card Extension feature must be installed on users' workstations, with the other features from the SDS Enterprise agent. For more information, refer to the sections [Deploying the SDS Enterprise agent installation package on user workstations](#) and [Configuring the middleware required for Card or USB token accounts](#).
- Users' encryption and signature certificates must be stored beforehand in the **Personal** store in the **Microsoft certificate manager** on workstations. These certificates must have been issued by the certification authorities that were declared in the security policy, when SSO accounts were configured, as indicated in the next two following sections.
Ensure that users have a private key that matches each certificate stored on the TPM chip or in the Microsoft certificate manager.

10.4.2 Configuring SSO accounts in SDMC

To configure SSO accounts and ensure that users' SDS Enterprise accounts are associated with their Windows user accounts, configure the following options in SDMC:

1. Go to the **Accounts** menu of the relevant security policy.
2. In the **Parameters** tab, select **Single Sign-on (SSO)**. For further information, refer to the section [Configuring generic account settings](#).
3. In the **Creation** tab, under **Key management**, select the use of accounts with single keys or key pairs. For further information, refer to the section [Setting account creation parameters](#).
4. In both cases, select the certification authorities that issued the encryption and signature keys.
5. Once the security policy is ready, deploy it on users' workstations as indicated in [Installing SDS Enterprise agents on user workstations](#) or [Updating the policy on SDS Enterprise agents](#).

Next, refer to the section [Using the SSO account](#).



10.4.3 Configuring SSO accounts in the security policy's *.json* file

To manually configure SSO accounts directly in a security policy's *.json* file, the following fields must be filled in:

1. Indicate SSO as the type for the "AccountMode" parameter:

```
"accountPolicy": {
  "parameters": {
    "accountMode": "SSO"
  }
}
```

2. Indicate the number of keys in the "accountKeyMode" parameter ("dualKey", "singleKeyEncryption" or "singleKeySignature"):

```
"accountPolicy": {
  "creation": {
    "accountKeyMode": "dualKey"
  }
}
```

3. In the parameters "encryptionKeyAuthorityId" and "signatureKeyAuthorityId", indicate the ID of the certificate from the authority that issued the keys to be used to create the accounts:

```
"accountPolicy": {
  "creation": {
    "automatic": {
      "encryptionKeyAuthorityId": "0123456789ab-cdef-0123-4567-89abcdef",
      "signatureKeyAuthorityId": "0123456789ab-cdef-0123-4567-89abcdef"
    }
  }
}
```

4. In the "certificateData" parameter, indicate the data of the certificates mentioned in step 3 in "base 64" format:

```
"certificateData": [
  {
    "id": "0123456789ab-cdef-0123-4567-89abcdef",
    "data": "LS0tLS1CRUdJTtBDR [...] GSUNBVEU+LS0tLQ0K"
  }
]
```

5. Once the security policy is ready, deploy it on users' workstations as indicated in [Installing SDS Enterprise agents on user workstations](#) or [Updating the policy on SDS Enterprise agents](#).

To configure the security policy in *.json* format, refer to the *SDS Enterprise Advanced configuration guide*.

Next, refer to the section [Using the SSO account](#).

10.4.4 Using the SSO account

Once the policy has been deployed on workstations, users' SDS Enterprise SSO accounts will automatically be created the next time they log in to their Windows accounts. They can then






use SDS Enterprise without going through its connection window.

To specify a location for SDS Enterprise account files on the user's workstation, use the parameters "RootPath1" and "RootPath2" in the *SBox.ini* configuration file. Files are saved in a sub-folder named after the current user of the Windows session. This sub-folder itself is located in an "SSO" sub-folder in the path specified by the "RootPath1" and "RootPath2" parameters.

To configure the *Sbox.ini* file, refer to the *SDS Enterprise Advanced configuration guide*.

Users are automatically logged in to and out of the SDS Enterprise account every time the user's Windows session is opened and closed. The same occurs when the account is locked and unlocked.

SSO accounts have the following particular characteristics:

- Connection and locking menus remain visible by clicking on the SDS Enterprise  icon in the Windows task bar, but are grayed out.
- However, users can choose in the properties of their SDS Enterprise accounts > **Connection settings** > **Screensaver** tab to lock the SDS Enterprise session when the Windows screensaver begins or when the Windows session is locked, and to not unlock when session resumes. In this case, users can use the **Unlock** menu by clicking on the SDS Enterprise  icon in the task bar.
- In the user's key ring, which can be accessed from the SDS Enterprise  icon in the Windows task bar, the **Operations** button is not shown in the **Encryption** and **Signature** tab.


10.5 Renewing keys and certificates

When encryption or signature keys or certificates are lost, compromised or expired, please follow these procedures to renew them depending on your users' account type.

10.5.1 Password accounts

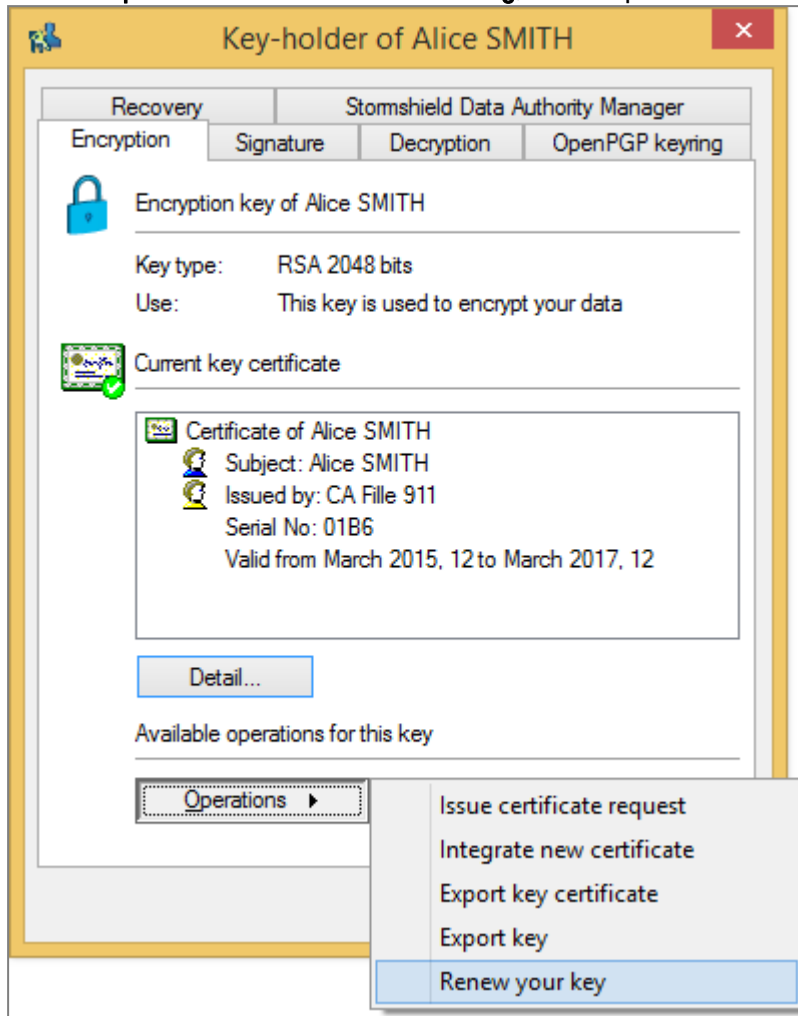
You can renew the keys of a user of a Password account to change their encryption or signature keys.

To renew keys from a user's workstation:

1. Right-click on the SDS Enterprise  icon in the system tray.
2. Select **Properties**.
3. Select the **Configuration** tab.
4. Double-click on the **Key ring** icon.
 - If the user has two keys, choose the **Encryption key** or **Signing key** tab.
 - If the user has only one key, choose the **Personal key** tab.



5. Click on **Operations** and choose **Renew key**, then skip the introduction screen.



6. Specify how to create the encryption key:
 - To create a new key, select the option **Generate your key** and select the type and length of the key. Refer to the section [Creating a Password Account Manually](#) for further instructions.
 - To import an existing key, choose **Import your key**. Refer to the section [Creating a Password Account Manually](#) for further instructions.

7. Click on **Finish**.

SDS Enterprise generates or imports the personal key and moves the old key as a decryption key so that the user can decrypt his old documents. It is visible in the user's Keyring **Decryption** tab. Signature keys are not kept.

For more information, refer to the section [Decrypting a user's data with an old key or a delegation key](#).

10.5.2 Card or USB token accounts

To renew certificates or keys on smart cards and USB tokens, take note of the information below.



Renewing certificates

When renewing certificates on the smart card or USB token, the new certificates are effective the next time the user connects to SDS Enterprise.

When a new certificate is added, the certificate object that is created must have the same CKA_ID PKCS#11 attribute as the old one.

The old certificate should not be deleted unless SDS Enterprise has correctly recognized the new one. You can check whether the new certificate is recognized in the SDS Enterprise agent's key ring.

Renewing keys

When renewing keys (with the associated certificate), the new keys are used when the old keys become obsolete or, more specifically, when their certificate becomes obsolete.

For an account with several keys (one for encryption and one for signing), the new keys are selected based on the use of the associated certificates.

You can check whether the new keys are recognized in the SDS Enterprise agent's keyring.

Make sure that you keep the old encryption key, even after the new key has been taken into account by SDS Enterprise. The old key automatically becomes a decryption key and always decrypts the user's old documents. It is visible in the user's Keyring **Decryption** tab.

It is not necessary to keep the old signature key.

For more information, refer to the section [Decrypting a user's data with an old key or a delegation key](#).

10.5.3 Single Sign-On accounts (SSO)

In SSO mode, encryption and signature keys as well as certificates can be stored in the user's Windows Certificate Store. In this case, please observe the following information.

Renewing keys

If you need to renew a user's keys in the Windows Certificate Store, the new keys overwrite the old keys. In order for the user to continue decrypting his old documents, follow these steps:

1. Get their private key, which is used to decrypt their data and stored in your key generation infrastructure or other.
2. In the user's SDS Enterprise keyring, which can be accessed from their account properties, view the **Decryption** tab.
3. Click the **Operations** button and then **Import a key**.
4. Import the old private key. This allows the user to decrypt documents encrypted with their previous encryption key.

For more information, refer to the section [Decrypting a user's data with an old key or a delegation key](#).

If the signature key is renewed, you do not need to do anything in the SDS Enterprise user's account.

Renewing certificates

If you need to renew a user's certificate (without changing the key), you must renew it via the Windows Certificate Manager so that it remains associated with the same encryption or signature key:



- In the user's personal store, right-click on the certificate to be renewed and select the menu **All tasks > Advanced operations > Renew this certificate with the same key.**

The next time SDS Enterprise starts, the new certificate is automatically taken into account in the user's keyring.

10.6 Unblocking user accounts

If users forget their passwords or if their accounts have been blocked because they entered the wrong password too many times, their accounts can be unblocked.

10.6.1 Using the backup password

1. In the connection window, select **Unlock** to start the unlocking tool and click on **Next**.
2. Select **I know the backup password**.
3. Enter the backup password that was set when the account was created, then click on **Next**.



IMPORTANT

If you block the backup password, you will no longer be able to unblock the account.

4. Enter a new user password according to the criteria displayed and confirm it.
5. Click on **Finish**.

The account is now operational again with the new password.

10.6.2 Using the user account backup

With each successful connection, SDS Enterprise makes a backup `[.bak]` of the keystore `[.usr]`, folder `[.usd]` and revocation database `[.brcl]` files that make up the user account.

If the user account is blocked or corrupted, you can restore the account from its last backup.

To do so, in the folder containing the user account (configured in the [security policy](#)):

1. Rename the `.usr`, `.usd`, and `.brcl` files;
2. Make a backup copy of the files `.usr.bak`, `.usd.bak`, and `.brcl.bak`;
3. Delete the `.bak` extension from the files `.usr.bak`, `.usd.bak`, and `.brcl.bak`.


The user account is then reset to how it was at the time of the last successful connection.

10.7 Exporting an SDS Enterprise account

You can export a user account in a Windows Installer file which will contain all the information and files from the account.

Once the account is exported, you can either store this file to save it, or install it on another computer where SDS Enterprise is installed to install the user account.

To export the account:

1. On the user workstation, right-click on the SDS Enterprise icon in the  Windows system tray.
2. Select **Properties**.



3. Select the **Wizards** tab.
4. Click on **Account export**.
5. Skip the introductory screen.
6. Click on the **Browse** icon to select the folder to which the account will be exported, and enter the name of the file to be created.
7. Click on **Next**.
8. Check that the summary corresponds to the account you want to export, and click Finish. SDS Enterprise creates a *.usi* file in the location you indicated, and provides a final summary.

10.8 Exporting a security key

You can create a file to export a security key (public key and private key), with its certificate and any trust chain.

For an account with two keys, you can export each key individually.


By saving this file, you can:

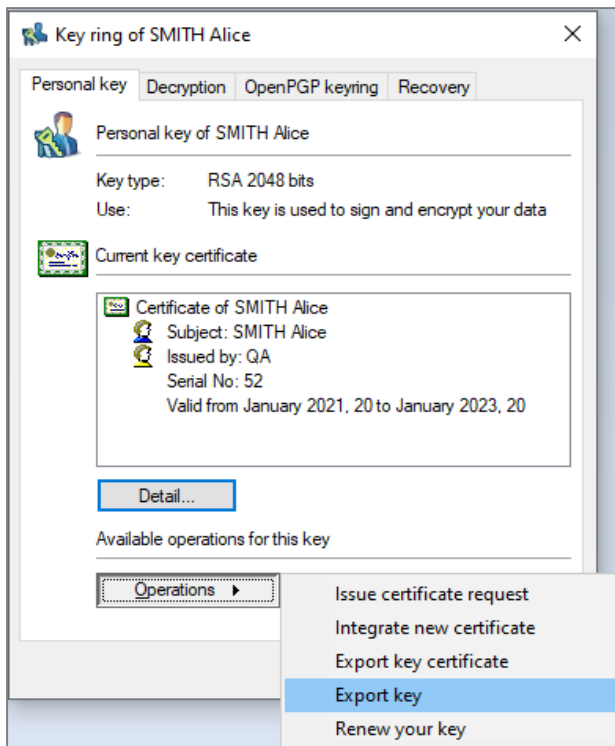
- Create a new account using the current key,
- Use this key in any application that can import security keys.

This will be useful for delegated decryption keys (see [Decrypting a user's data with an old key or a delegation key](#)). This is also useful if you want to decrypt files or information previously encrypted with this key.

The file containing your key is generated in *PKCS#12* format (extension *.p12* or *.pfx*). If the user has two keys, each key will be exported in a separate file.

To export a key:

1. On the user workstation, right-click on the SDS Enterprise  icon in the Windows system tray.
2. Select **Properties**.
3. Select the **Configuration** tab.
4. Double-click on the **Key ring** icon.
 - If the user has two keys, choose the **Encryption key** or **Signing key** tab.
 - If the user has only one key, choose the **Personal key** tab.
5. Click on **Operations** and choose **Export key**, then skip the introduction screen.



6. Select one of the following two options. You can tick both options.
 - The **Provide certificate trust chain** to associate the key with the certificate of the authority (ies) that certified the key. Only the certificates found in the trusted address book will be listed. No LDAP search will be performed.
 - The **Provide former key certificates** option if the user renewed one or several certificates but wishes to decrypt documents which were encrypted with the previous certificates. You can select both options.
7. Enter the name of the file to be created, and proceed to the next screen. The **Save as** button enables you to browse folders in order to set the target file. However, the keys are not yet exported.
8. Enter a password to protect the file: this will allow you to encrypt the key in the generated file.

i NOTE

The password must be at least eight characters long and contain either a number or an interpunction. If this is not the case, the export is denied.

9. Proceed to the next screen, check the summary, and click on **Finish**. The key has been exported into the indicated file.

10.9 Decrypting a user's data with an old key or a delegation key

With the help of decryption keys, SDS Enterprise makes it possible to decrypt files and messages transparently when they are encrypted by a key other than the user's current key. SDS Enterprise allows two types of decryption keys:




- Former private keys. When users renew their encryption keys (or personal keys), their former keys are automatically moved to a location where all their former decryption keys are kept,
- Delegation keys. These are encryption keys that coworkers can share with other users, to allow them to decrypt documents or messages that were encrypted for their use.

10.9.1 Setting up delegated decryption

Delegated decryption consists of allowing User A to decrypt messages or files encrypted for User B in the latter's absence. To do so, User A must be given User B's encryption key.

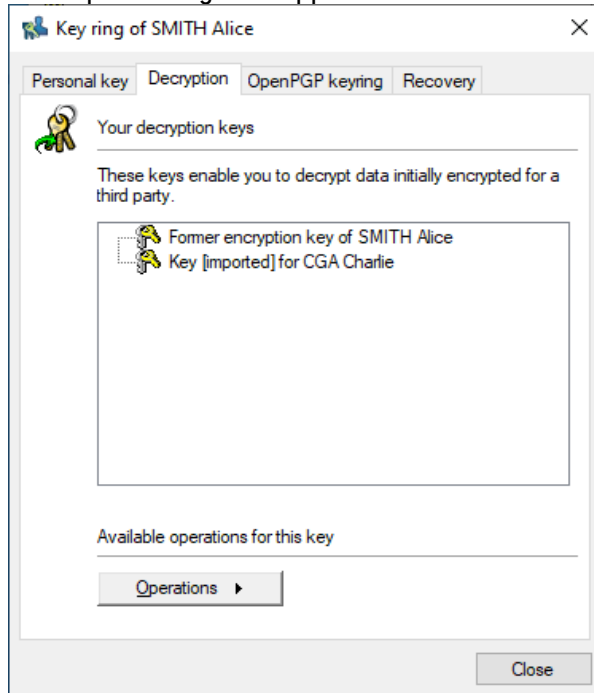
With this encryption key, User A can only decrypt messages. To ensure that User A can sign on behalf of User B, we recommend using separate keys for encryption and signature.

To set up delegation, User B must export their encryption key from their SDS Enterprise account, which User A must then import into their own SDS Enterprise account by following the steps below:

1. User B logs in to their SDS Enterprise account by clicking on the  icon in the task bar .
2. They then double-click on the **Key ring** icon.
3. In the **Encryption** tab, User B selects the **Operations** > **Export key** menu.
4. User B then sends the exported file to User A.
5. User A logs in to their SDS Enterprise account.
6. They then double-click on the **Key ring** icon.
7. In the **Decryption** tab, they select the **Operations** > **Import key** menu.
8. They then indicate the name of the file containing the key to be imported and the password. SDS Enterprise displays a list of certificates present in the file, that is the certificate associated with the key contained in the file and its trust chain.
9. To view a certificate from the list, the user can click on it.
10. User A selects the certificates in the trust chain if they wish to import them into their trusted address book, then proceeds to the next screen.
11. They then choose the type of key to import (delegation or former key), then continue to the next screen.



- They click on **Finish** once they checked the result of the operation. The imported key then appears in the list:



- The user can right-click on a key in the list to rename it, display its properties or delete it when delegation is no longer necessary, for example.

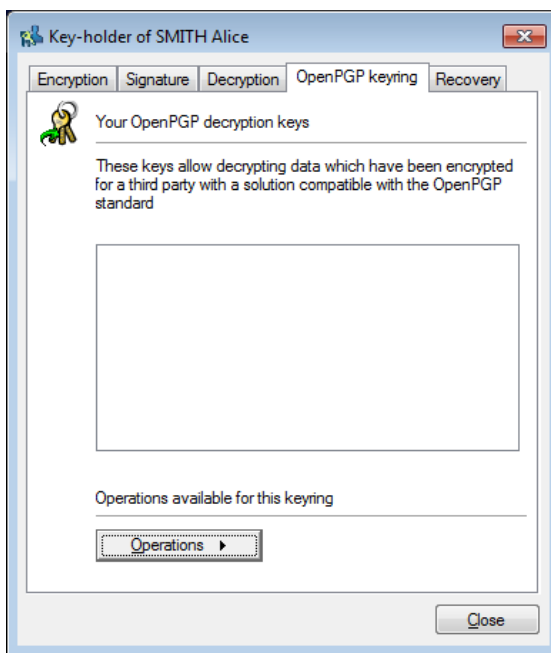
i NOTE

Keys imported this way cannot be exported by the person who received the key. In other words, the delegated people cannot forward the delegation.


10.9.2 Decrypting OpenPGP messages

SDS Enterprise also manages decryption keys for messages in OpenPGP format. These keys are used by the Stormshield Data Mail feature to read messages secured by PGP and GnuPG applications, or any other application compatible the OpenPGP format.

When the Stormshield Data Mail is installed on the machine, the **OpenPGP keyring** tab in the properties of the user account will make it possible to manage these keys.



To import an OpenPGP keyring:

1. On the user workstation, right-click on the SDS Enterprise icon in the  Windows system tray.
2. Select **Properties**.
3. Select the **Configuration** tab.
4. Double-click on the **Key ring** 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.

10.10 Decrypting a user's data with a recovery certificate

The recovery certificate secures the use of a strong encryption solution. If a user loses access to their account and has not saved the encryption key, a recovery certificate ensures that the user can still decrypt the data. For example, if coworkers leave the company without decrypting all their data, this data can be recovered in plaintext.


WARNING

The recovery certificate may come from another SDS Enterprise account from which the public encryption certificate will have been exported. Due to the fact that this recovery key is highly sensitive and because of the use of this key, it is essential that this recovery account be protected.

10.10.1 Looking up recovery certificates

To look up the recovery certificates used for any encryption operation on the SDS Enterprise agent:



1. From the Windows task bar on the user workstation, right-click on the SDS Enterprise icon .
2. Select **Properties**.
3. Select the **Configuration** tab.
4. Double-click on the **Key ring** icon.
5. Select the **Recovery** tab. The certificates shown in the list are from the security policy. For more information, see the section [Enabling data recovery](#).

10.10.2 Using a recovery certificate to decrypt data

Recovery certificates from an SDS Enterprise account or other external source can be used.

- If the recovery certificate was generated from an SDS Enterprise account, use this account to decrypt data.
- If the recovery certificate came from another source, export the private key and its certificate from this source in *PKCS#12* (.P12) format.
Next, create an SDS Enterprise account using this .P12 file and its associated password, then use this SDS Enterprise account to decrypt data. For more information on creating accounts, refer to the section [Importing keys](#).
You can create an account with only the decryption function.

You can use the recovery certificate to decrypt all information encrypted by the original owner of the certificate, or encrypted for the original user by a co-worker using the same certificate. However, you cannot decrypt information received from an external source (for example received e-mails) as they were not encrypted with the recovery certificate.



11. Managing the trusted address book from the SDS Enterprise agent

The trusted address book allows you to save and use certificates from your users (and authorities). This address book is protected and only the user can edit it. It is considered “trusted” because all the certificates on it are considered valid by SDS Enterprise.


SDS Enterprise allows you to import user certificates from an LDAP directory into the trusted address book. To declare an LDAP directory in a security policy, refer to the section [Configuring corporate directories](#).

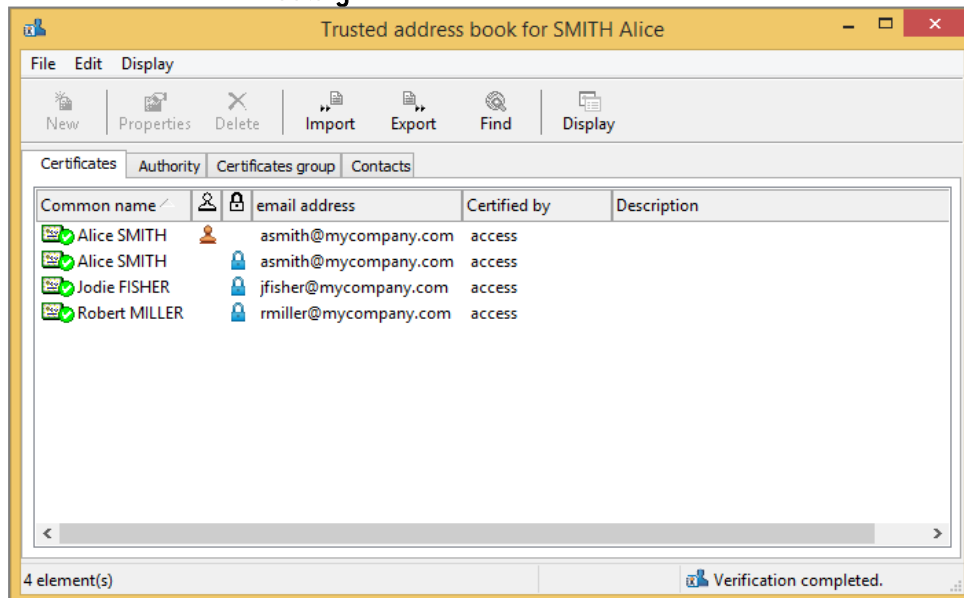
11.1 Looking up the trusted address book and managing certificates from the SDS Enterprise agent

The SDS Enterprise agent's **Directory** menu makes it possible to look up the contents of the user's trusted address book, or import or export certificates. The configuration of LDAP directories associated with the trusted address book can also be looked up.

11.1.1 Opening your trusted address book

To open your trusted address book from a user's workstation:

1. Right-click on the SDS Enterprise icon  in the Windows system tray.
2. Select **Properties**.
3. Select the **Configuration** tab.
4. Double-click on the **Directory** icon.



The *Certificates* tab displays users' personal certificates, i.e., certificates that are not issued by a certification authority.

The *Authority* tab displays authority certificates, i.e., certificates that have the X.509 extension indicating that they are authority certificates (see Note below on X.509 v1 certificates).



The *Certificate group* tab displays certificates that group several certificates at once, i.e., encryption for a group of persons with a single certificate.

The *Contacts* tab allows you to create shortcuts towards certificates located in an LDAP directory.

The validity of a certificate is shown by the icon on the left. All icons are shown in the following table.

| | valid | expired, or not yet valid | invalid |
|-----------------------|-------|---------------------------|---------|
| user certificate | | | |
| authority certificate | | | |

For non-authority certificates, two columns show whether the certificate has been authorized for signing and/or encryption:

- the certificate is authorized for encryption
- the certificate is authorized for signing

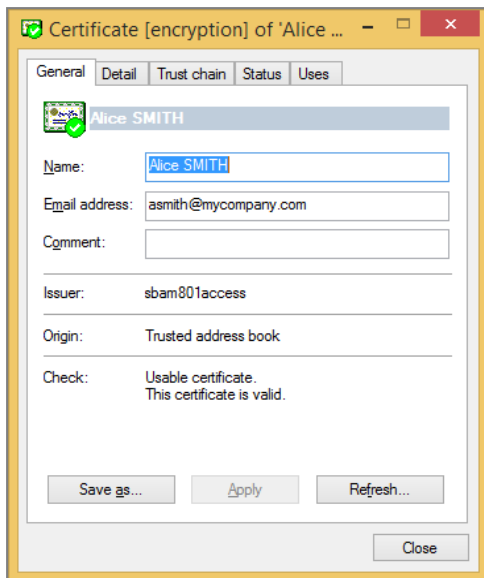
To change the display of certificates, click on the Display button or select the Display>Presentation menu.

NOTE

- an X.509 v3 certificate is an authority certificate if it has a specific extension ("BasicConstraint"). This extension can include the full length of the certification chain belonging to this certificate.
- some authorities use root X.509 v1 certificates (Verisign for example), a version that does not support the above extension. SDS Enterprise treats all self-certified X.509 v1 certificates as authority certificates. These certificates can be used by various SDS Enterprise features for encrypting and signing. There is no way to find out how they are used and the fact that they are explicitly authority certificates. You are however advised against using such certificates.
- SDS Enterprise does not use X.509 v2 certificates.

11.1.2 Displaying certificates

To display a certificate, double-click on it or select it from the list and click on the **Properties** button.



The **General** tab displays a summary of the certificate's contents:

- The name and e-mail address of the holder,
- Comments that you can update as required (they are not part of the certificate),
- The name of the certification authority,
- The origin of the certificate (trusted address book, LDAP, e-mail),
- The state after a verification check. If needed, a message indicates the error or warning.

From this window, you can also export the certificate, using the Save as button.

The **Detail** tab displays the contents of the certificate.

For information on the various fields displayed, see the X.509 v3 standards, or the RFC 3280.

If an error or warning appears, the same explanation message will appear in this window immediately after the first line.

The Trust Chain tab rebuilds and displays the certification chain, and shows the results of checks carried out on the chain.

i NOTE

Only the trusted address book will be queried if you search for certificates involved in this trust chain. No LDAP searches are performed for this chain.

You can click on certificates in the chain to see their contents.

11.1.3 Importing certificates

You can import the following into your trusted address book:

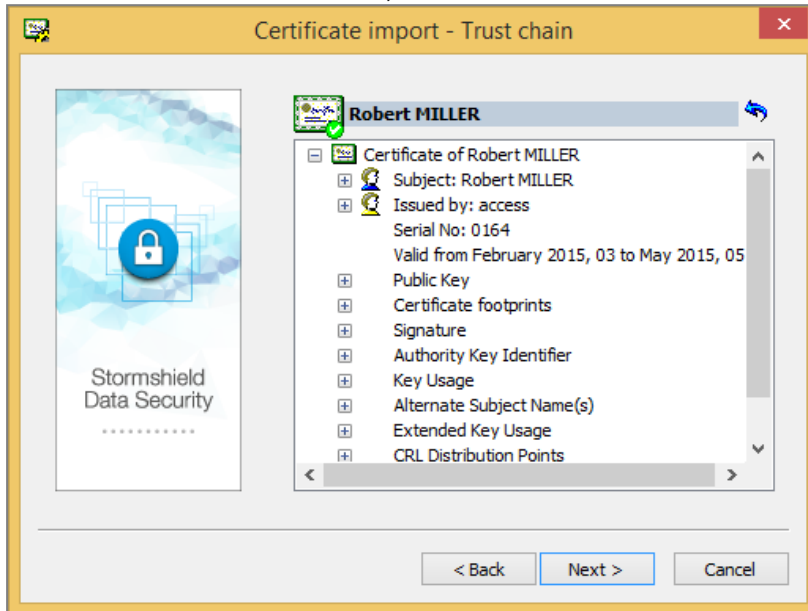
- Certificates only, saved as binary files (.cer extension) or a base 64 file (.crt extension),
- Lists of certificates saved in PKCS#7 format (.p7b or .p7c extension),
- A full backup of your address book (.p7z extension),
- Certificates from an LDAP directory.

Importing certificates from the workstation

To import certificates, you can either use the wizard or drag and drop them.



1. Click on **Import** in the trusted address book main window, or drag and drop a certificate or list of certificates from the Desktop or the Windows Explorer.
2. Enter the name of the file that contains the certificate(s) you want to import, and proceed to the next screen. SDS Enterprise displays all the certificates held in the file.
3. To view a certificate from the list, click on it:



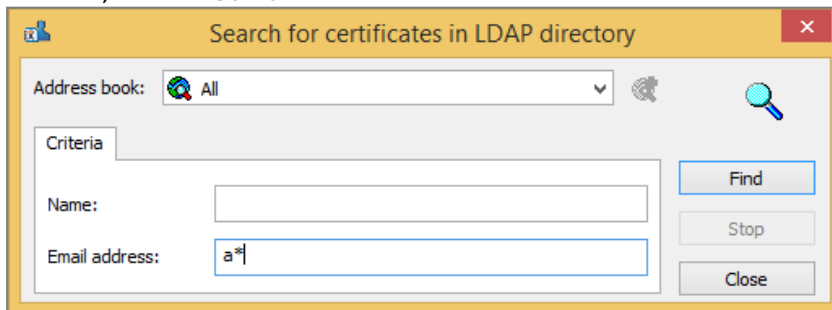
Files are checked when they are imported. The check results in a green, yellow or red mark in the certificate icon. Regardless of the status, the result does not block the import; it is possible to import invalid certificates.

4. To return to the list of certificates, click on
5. To check whether a certificate belongs to a user, contact the user and check the hash shown.
6. To import one or more certificates from the list, select them and click on **Next**; check the summary, and click on **Finish**.

Importing a certificate from an LDAP directory

SDS Enterprise allows you to import a peer's certificate into the trusted address book from an LDAP directory:

1. To do so, click on **Search** in the main window of the trusted address book.



2. Enter the address of the LDAP server to be searched and the search parameters: name and/or e-mail address. You can include generic characters such as "*" or "?" in your search parameters if the directory you are searching accepts them.



3. Click on Search now to launch the search. The results are displayed. SDS Enterprise only displays certificates found in the directory, that are valid (according to the validity period) and which can be used for encryption or electronic signatures.
4. To display the details of a certificate, select it and click on Preview.
5. To import one or more certificates into the trusted address book, select the certificate(s) and click on **Import**.

The LDAP directory(ies) available in this window were declared beforehand in the security policy in SDMC. For more information, see the section [Configuring corporate directories](#).

11.1.4 Exporting certificates or the trusted address book

If a user has certificates in their trusted address book that some peers do not have, the user share these certificates by exporting them.

You can export certificates using the wizard, or by dragging and dropping them.

If you want to export certificates groups, see section [Exporting a certificates group](#).

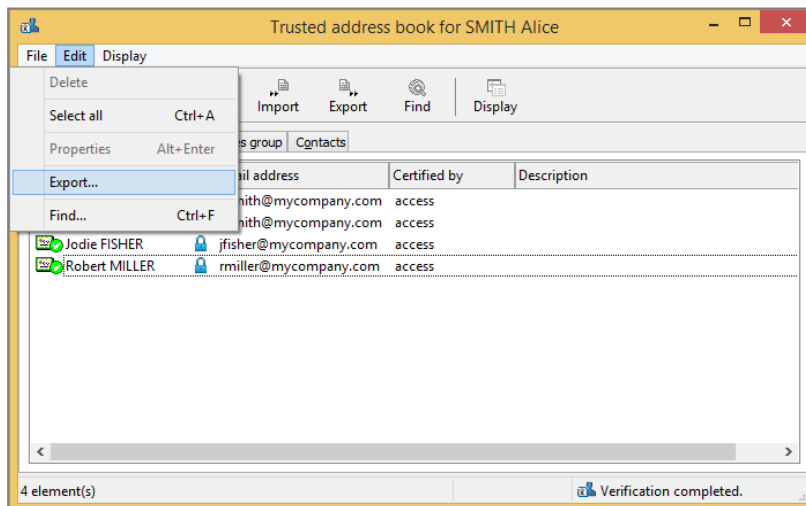
You can also export an entire trusted address book in a SDS Enterprise file with the extension `.p7z`.

The export will include all certificates, any custom settings, certificate groups and contacts' certificates.

Exporting via the wizard

To export one or several certificates from a trusted address book:

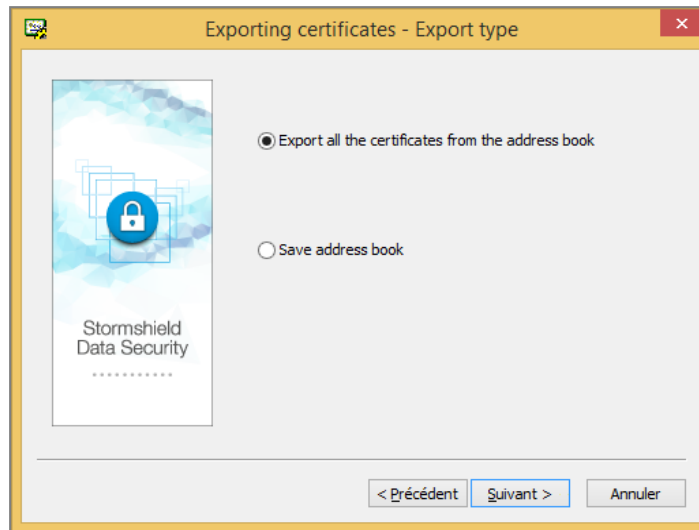
1. Select them in the address book.
2. Click on **Export** or select the **Edit > Export** menu.



Continue to the next screen.



3. Choose the export type.



According to the elements you have selected in the address book, the text of the first option changes:

- **Export all the certificates from the address book:** this option is available when no certificate is selected in the address book. In this case all the certificates will be exported in a *.p7b* or *.p7c* file.
- **Export the selected certificates:** this option is available if several certificates or groups are selected in the address book. In this case only the selected certificates will be exported in a *.p7b* or *.p7c* file.
- **Export the selected certificate:** this option is available when only one certificate is selected in the address book. In this case the selected certificate will be exported in a *.cer* or *.crt* file.

The **Save address book** option allows in any case to save all the certificates of the address book with their customized information if any.

4. If you have selected the first option of the **Export type** window and only in this case, the **Options** window opens. Additional elements can be added to the export file:

- **Include parent-child relationship:** allows exporting the certificate's trust chain. In this case, any authority certificates that are shared are not duplicated.
- **Include groups and contacts:** allows including groups and contacts certificates in the export file. If you want to export groups, see section [Exporting a certificates group](#).

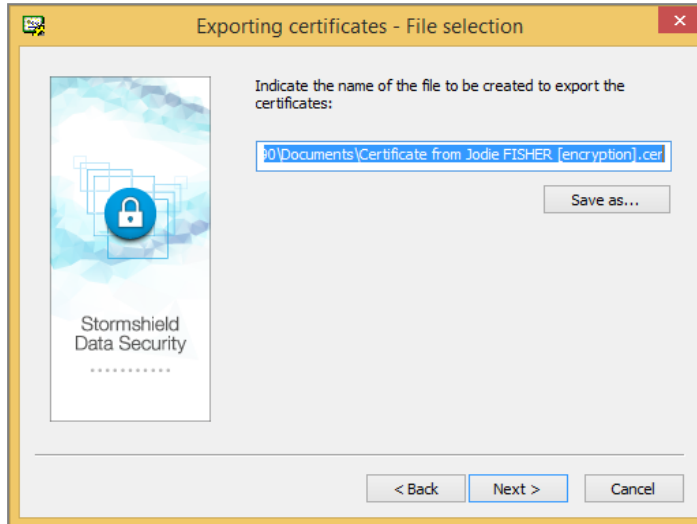
This check box is checked by default when groups are selected in the address book. It is also unavailable to avoid unchecking it and generating an empty export file.

i NOTE

If this option is checked whereas no group is selected in the address book, all the groups will be exported.



5. Enter a name and location for the export file. The assistant provides a default name, according to the selected export type. You can also directly type the information in the edit box or click the **Save as** button.

**i NOTE**

The file extension is automatically changed if the extension chosen is not the right extension for the selected export type.

6. Check the information on the summary page before starting the export.
7. The selected certificates have been exported in the indicated file. You can send the resulting file by e-mail, USB token, shared file, etc., or use it to restore the content of your address book (.p7z extension required).

Exporting via drag and drop

You can also export certificates using the drag and drop feature in your trusted address book.

1. Select the certificate(s) you want to export.
2. Keeping your left mouse button down, drag the certificates to your desktop, or to a folder in Windows Explorer, or to an application that can receive such a file.

If only one certificate is exported, the file will be named <CommonName>.cer. It is not possible to select another name or another format. The name does not distinguish between signature certificates or encryption certificates.

If several certificates are exported with drag and drop, the resulting file will be named *Certificate_List.p7b*. It is not possible to select another name or another format.

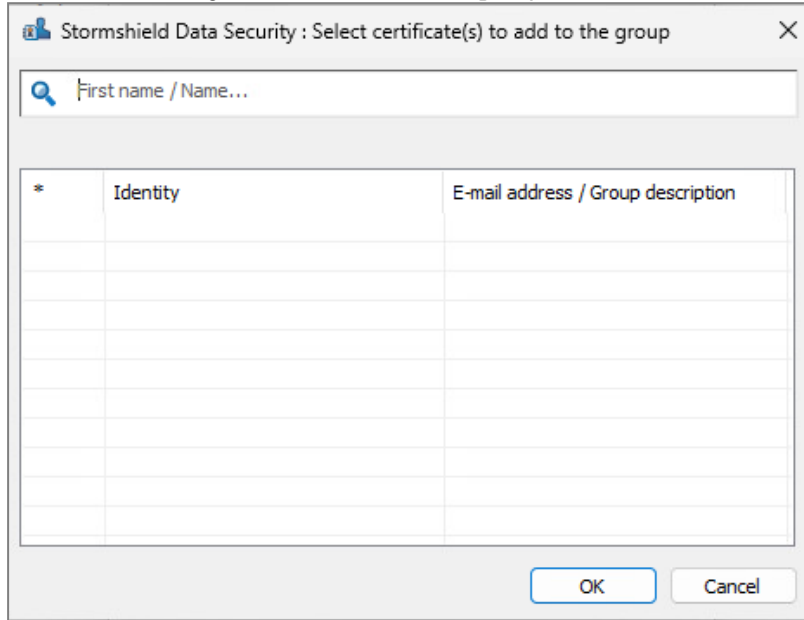
11.1.5 Creating a certificates group

Creating a group of certificates simplifies the encryption for fixed groups of recipients. Instead of selecting each recipient, you can select a predefined group. If you use a group to encrypt a document, the document will be encrypted for every member of the group that has a valid certificate.

SDS Enterprise accepts only groups saved in the trusted address book. You cannot use or import groups from an LDAP directory.



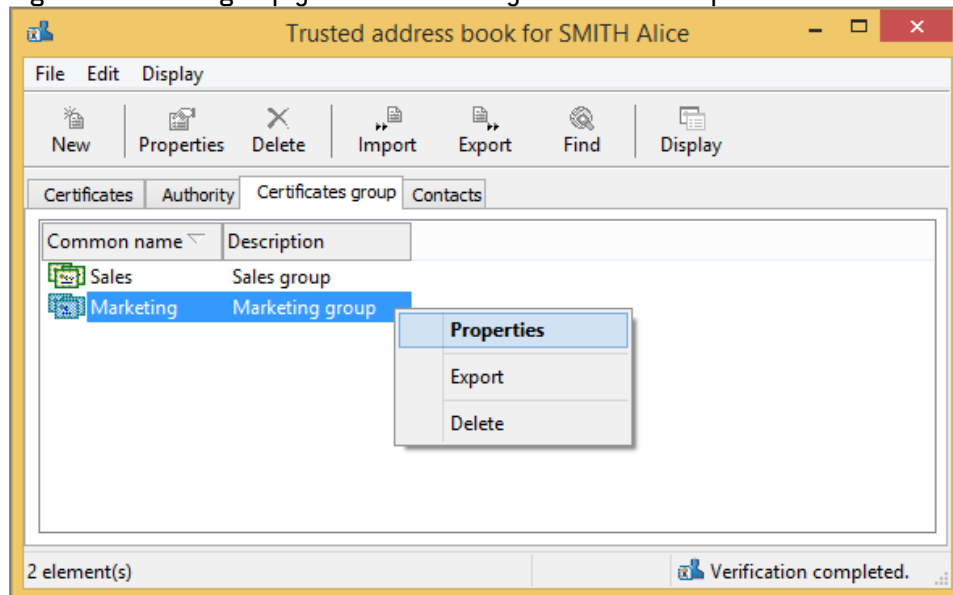
1. To create a group of certificates, choose the **Certificate group** tab in your trusted address book.
2. Right-click in the window and choose **New**.
3. Enter the information on the group and click on **Add** to add certificates.
4. Select the users you wish to add to the group.



5. Click **OK** when you are done.
6. Click **OK** to close the window.

11.1.6 Modifying a certificate group

1. Choose **Certificate group** in your trusted address book.
2. Right-click on the group you wish to modify and choose Properties.

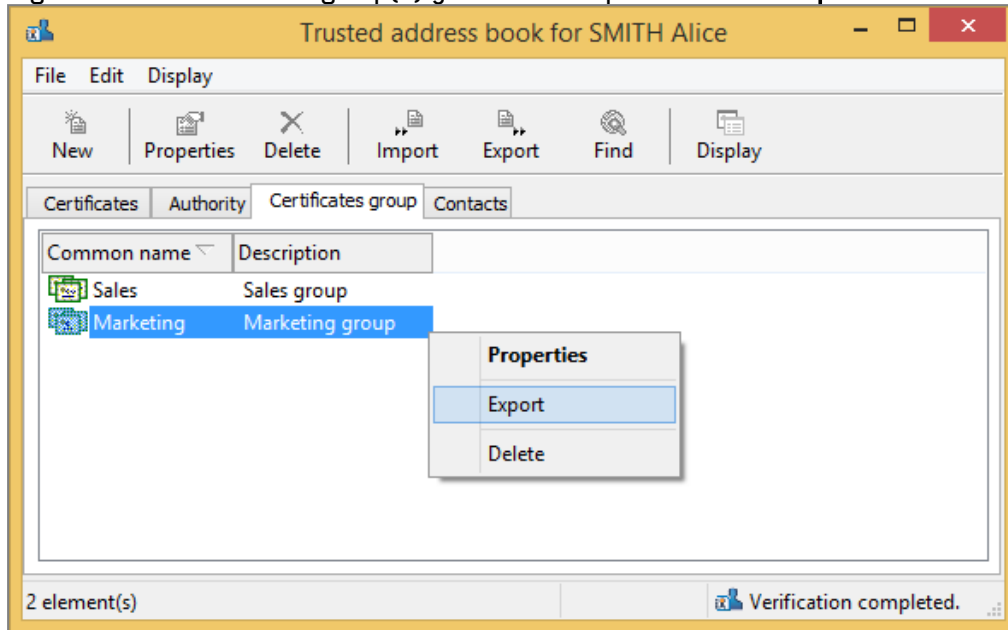


3. Add or remove certificates.
You can also modify the group name and description.
4. Click OK to confirm your changes.



11.1.7 Exporting a certificates group

1. Right-click the certificates group(s) you want to export and select **Export**.



Several groups can be selected for export. In this case, all the certificates in the groups will be exported. If the same certificate appears in more than one group, it will only be exported once.

2. The following steps are the same for exporting certificates. Refer to the section [Exporting certificates or the trusted address book](#).

11.1.8 Deleting a certificate group

1. Select the group from the list of groups in the trusted address book.
2. Right-click on the group you wish to remove and click on **Delete**.

Use the usual Windows keys to select several groups (Shift + Ctrl).

To delete all groups, right-click without selecting any group in particular and click on **Select all**, then click on **Delete**.

11.2 Exchanging certificates via Stormshield Data Mail

In practice, certificates are seldom exchanged between users. LDAP directories are generally used to share certificates between peers. Manual exchanges are used only when sharing certificates with colleagues outside a company, or for test purposes.

Certificate exchange procedures differ depending on whether you use Stormshield Data Mail. If you do not have Stormshield Data Mail, you will need to use the certificate export/import procedures described in [Looking up the trusted address book and managing certificates from the SDS Enterprise agent](#), and then send your certificate file by any appropriate means of communication.

By signing a message, Stormshield Data Mail facilitates certificate exchanges by automatically attaching signature and encryption certificates (and their entire trust chain) to secure messages.

**i NOTE**

Self-signed certificates are not attached to signed messages.

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

1. In Microsoft Outlook, if peers have shared their certificates by signing a message with SDS Enterprise, in the lower Stormshield Data Security banner, click on **Import certificates**.
2. Certificates are then imported and your trusted address book is up to date. The link will no longer appear in the lower banner.

If an error occurs, refer to the security report. For more information, refer to *Securing e-mails* in the *SDS Enterprise Advanced user guide*.

11.3 Working offline

SDS Enterprise verifies the physical connection to the local corporate network.

When the user is connected to the network (online), every time the user searches the LDAP directory for a certificate, certificates found as a result of the search are saved in a local temporary file (cache).

When the user is disconnected from the network (offline), SDS Enterprise detects that the network is missing and searches for certificates in this local cache.

This mechanism makes it possible to encrypt files and e-mails sent to your coworkers even when the user is disconnected from the corporate network, as long as each coworker's certificate has been previously used at least once.

Certificate revocation lists are also downloaded online and cached locally in a file that the user can consult even offline.

SDS Enterprise makes it possible to force offline mode if necessary, for example if there are local network problems. To do so:


1. Right-click on the SDS Enterprise icon in the task bar.
2. Select **Network access > Work offline**.
3. Unselect **Network access > Reconnect automatically**.
4. When you re-enable **Reconnect automatically**, SDS Enterprise automatically detects the network connection and switches back to online mode.

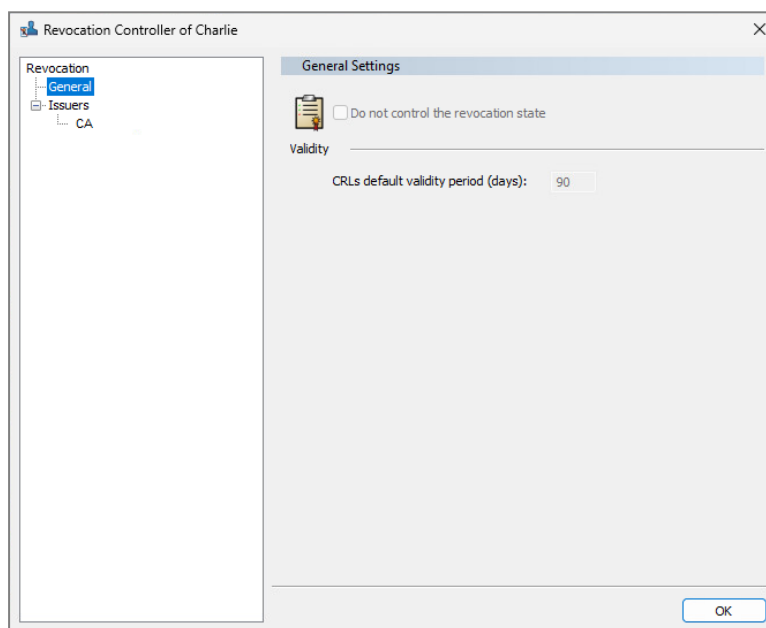


12. Looking up certification authorities from the SDS Enterprise agent

From the SDS Enterprise agent, the revocation controller makes it possible to look up the certification authorities that issue user certificates, as well as the certificate revocation list (CRL) distribution points for each authority.

To display the revocation controller on user workstations:

1. Right-click on the SDS Enterprise icon  in the Windows system tray.
2. Select **Properties**.
3. In the **Configuration** tab, double-click on the **Revocation** icon.



The revocation controller is in read-only mode. To configure user certificate revocation, specify the certification authorities in the security policies, as well as any associated CRL distribution points. For more information, refer to the section [Adding certification authorities and configuring certificate revocation control](#).

12.1 Downloading a CRL

- To download a CRL from the revocation controller, right-click on the name of the authority under **Issuers**, and select **Download**.

NOTE

Manual downloads are generally used for users that only rarely have access to the company's network. In this case, they need to download the CRLs when they can.

12.2 Deleting an authority

You can delete authorities from the issuer list.



- Select the authority from the list of **Issuers** and click on **Delete**.

This does not affect the performance of the product and is used only to clean up the list of authorities.



13. Configuring and using the agent's advanced features

This chapter contains all the technical information (tips, limitations, and warnings) about the agent's features.

13.1 Stormshield Data Virtual Disk

13.1.1 Recovering a volume

Recovering a volume with a container file

The physical medium for a secure volume is a container file (.vbox extension) that contains:

- The cryptographic components required for mounting the volume: the volume's symmetric encryption key is protected with the public key for each authorized user and with each recovery key,
- The content belonging to the volume: files stored in the volume and file system.

The cryptographic components are always saved in a backup file: .vboxsave extension when the volume is created and again with each modification to the user list.

Recovering a Stormshield Data Virtual Disk volume is identical to changing the owner, as described in the product user manual. Basically, the user requesting a change in ownership is not the initial owner but the user whose encryption certificate has been defined as the recovery certificate.

Therefore, recovery consists of defining a new user as the owner of the volume. The new owner can then perform all the chosen operations.

Recovering a volume without a container file

However, for a simple ownership change, a recovery can be launched without a container file, only with the VBOXSAVE volume.

This procedure is particularly useful for remote recovery operations. The user with the container file does not need to send the entire container file so that the recovery can be launched, and only needs to send the .vboxsave file.

For this, users who want a recovery must send the .vboxsave file to the administrator in charge of recovery. The administrator proceeds in the same way as for changing the owner, then send back the .vboxsave file to the user who made the request. They only have to update the .vboxsave file and continue the ownership change procedure as if they had updated the .vboxsave file themselves.

13.1.2 Unmounting a volume by force

We advise against unmounting a Stormshield Data Virtual Disk volume "by force" or when there are open files in it. If such an operation is necessary, we strongly recommend checking the volume, by using the Windows tool for checking the disk, the next time it is mounted before using it.



13.1.3 Duplicating a volume

If a secure volume is duplicated by copying the `.vbox` container file, both copies cannot be mounted simultaneously on a single workstation.

Generally, you are advised against duplicating volumes by copying the `.vbox` container file. This method should be used only for backups.

13.1.4 Using the volume within a Windows multi-session context

For a better integration within Microsoft Windows, a Stormshield Data Virtual Disk volume behaves in the same way than a standard storage volume.

An encrypted volume mounted in a Windows session is thus accessible from other Windows sessions opened on the workstation.

To avoid that, the user must select the SDS Enterprise account lockout when the Windows session locks.

Locking the account unmounts encrypted volumes mounted in the session. However unmounting by force a volume may damage the files opened on this volume. The user must save modifications before locking the session.

On a Windows server, a remote user cannot see the Stormshield Data Virtual Disk volumes mounted by other remote users connected to the same server. We recommend however selecting automatic locking because disk volumes are actually just hidden. Data on the disks may then be accessed.

13.1.5 Stormshield Data Virtual Disk limitations

- The maximum size of a Stormshield Data Virtual Disk volume is 2048 GB (2 TB).
- Volumes larger than 2 GB cannot be formatted in FAT16 (FAT16 limitation).
- Volumes smaller than 2.5 MB cannot be formatted in NTFS (NTFS limitation).
- The icon for a Stormshield Data Virtual Disk volume may be incorrect in Explorer (either a normal disk icon or a document icon).

13.2 Stormshield Data File

If permissions (in NTFS terms) are set for a file, they will be lost after Stormshield Data File encrypts or decrypts the file.

If Windows permissions must be implemented on confidential files secured by Stormshield Data File, these permissions must then be set for the directories containing the files, not on the files themselves.

13.3 Stormshield Data Mail

13.3.1 Information about the RTF format

Stormshield Data Mail does not support RTF format because it does not guarantee reliable interoperability with the security mechanism in SDS Enterprise. Using the RTF format may cause information loss.



HTML is therefore the recommended format for writing secure messages, as it enables interoperability.

13.3.2 Using cross-encryption

Cross-encryption makes it possible to update the protection level of secured messages (S/MIME format messages or plain text messages including an attachment encrypted with Stormshield Data File). 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.

To access the user's private keys during cross-encryption, you must be connected to SDS Enterprise.

You are therefore advised to disable automatic logout and session locking in your screen saver options when there are many messages to be cross-encrypted. The processing time is proportional to the number of messages to be processed.

A secured message will not be cross-encrypted if the user's current encryption key is the key that originally encrypted the message.

A message which has already been cross-encrypted by the current key will not be cross-encrypted again, as long as the user's current key is not updated.

13.3.3 Configuring the LDAP directory for certificates that contain several e-mail addresses

If recipients with several e-mail addresses in their certificates are not in the SDS Enterprise trusted address book but are in your LDAP directory(ies), a dialog box warning that "the certificate has not been found in your trusted address book" may appear when an encrypted e-mail is sent to this recipient.

In this case, you can configure the LDAP directory to retrieve the certificate when sending the encrypted e-mail.

To do so, check that the user attribute « proxyAddresses » in the LDAP directory contains all the user secondary e-mail addresses.

In the attribute, each secondary e-mail address must be preceded by « smtp: », whereas the main address is preceded by « SMTP: ».

This attribute can be updated via enterprise mail servers such as Exchange.

13.3.4 Ensuring the consistency of e-mail addresses

When sending e-mails, the system will search for the best available certificate for each recipient. If the certificate comes from the LDAP directory, the consistency of the recipient's e-mail address will be verified with the address specified in this certificate. If they are not the same, the certificate is rejected and the e-mail may not be sent.

If you use internal aliases for users' addresses, this mechanism may not be appropriate.

- To disable the consistency check on a user's workstation, set the value of **DWORD CheckLDAPCertificateEmailAddress** to 0 in the HKLM\SOFTWARE\Arkoon\Security BOX Enterprise\Mail registry key.

**i NOTE**

The e-mail address consistency check is implemented for security reasons. We therefore recommend that you do not disable it unless specifically required.

13.4 Stormshield Data Team

13.4.1 DFS environment restriction

- A DFS root cannot be encrypted.
- SDS Enterprise accounts must not be stored on a DFS share.

13.4.2 Managing the user's temporary folder (%TEMP%)

Do not list multiple collaborators on rules that involve the temporary folder for the Windows profile. Applications use this folder to store user-specific temporary files.

Failure to comply with this rule may cause blockages.

13.4.3 Managing the system's temporary folder

System processes (services, for example) use this folder to store temporary files, and it is shared with the other users on the system.

This folder may be, for example, **C:\windows\temp**. The exact location depends on the installation of the operating system.

This folder must not be encrypted with Stormshield Data Team.

13.4.4 Moving folders available offline

Using the *cachemov.exe* tool, the system folder `<%WINDIR%>CSC`, which contains the files that are available offline, can be moved.

In order to support this particular environment, the configuration on workstations must be modified through the registry base. For more information, see section *Moving folders available offline* in the *Advanced configuration guide*.

13.4.5 Keeping performance optimal on the workstation

When Stormshield Data Team is used, users' workstations may slow down. To keep the usual levels of performance, you can change the configuration on workstations via the registry base. For further information, refer to the section *Keeping performance optimal on the workstation* in the *Advanced configuration guide*.

13.4.6 Moving an intra-volume folder

Intra-volume folders are not allowed to be moved when the source and destination directories do not have the same level of security.



If the action is executed in Windows Explorer, the moving operation will be replaced with `Copy + Delete the source`. In this case, the destination folder's security level will be applied to the "moved" folder.

13.4.7 Prohibiting access to encrypted files if the certificate is revoked

Stormshield Data Team prevents users from accessing encrypted files if their encryption key certificates are revoked, even when these users appear in the list of users.

In this case:

- Any operations on files secured by Stormshield Data Team (opening, creating, renaming, moving and deleting) will be denied.

These operations will fail even if the file is encrypted with an old encryption key.

- No operations can be performed on Team rules. The user interfaces are grayed out and only allow rule parameters to be read.

Stormshield Data Team uses the revocation controller configuration defined at the user level. Therefore:

- Do not allow the user to disable revocation control,
- Do not forget to correctly configure the downloading rule for the revocation lists.

13.4.8 Changing the dates of the last access

Some solutions, such as archive solutions, rely on the dates on which files were last accessed to run their processes. However, when Stormshield Data Team is installed on a workstation, the last access date is changed when a folder is browsed.

You can control the restoration of the last access dates on files, and then delete changes to last access dates when files were opened with Stormshield Data Team. To do so, change the configuration on workstations via the registry base. For further information, refer to the section *Changing the dates of the last access* in the *Advanced configuration guide*.

13.4.9 Using the cache in a network

When the cache is used in a network, changes may be made to files, folders and rules beyond the control of the user's local file system. If a change is made by a user on the network, other workstations using the share may temporarily have incorrect cache entries and therefore invalid statuses in Windows Explorer. As a result, the new statuses will not take effect immediately.

You can take the following measures to reduce these inconsistencies:

- Secure a folder from the moment it is created while it is still empty,
- Notify users so that they will avoid using the share at critical moments,
- Do not destroy a folder and then recreate it with the same name but different characteristics. If you must perform this operation, leave enough time between both operations for caches to be updated (15 minutes or restart the user's workstation to immediately apply changes),
- For major operations, perform them on a file tree (securing/desecuring) at times when no or few users are connected (e.g. during lunch break or at the end of the day).



As there is no particular issue with adding or deleting coworkers from an existing rule, no special precautions need to be taken.



14. Troubleshooting

If you encounter issues, you can look up event logs in the Windows Event Viewer and also use the tracing system to form a diagnosis with the SDS Enterprise Technical Assistance Center.

14.1 Viewing event logs

All events relating to SDS Enterprise can be accessed via Windows event viewer on user workstations.

During a new installation of SDS Enterprise, event logs are disabled by default. To enable them, modify the registry parameters relating to the various event categories so that specific types of events can be reported.

If you encounter issues while using SDS Enterprise, refer to [Troubleshooting issues](#).

To view the list of event logs available in SDS Enterprise, refer to [List of SDS Enterprise logs](#).

14.1.1 Enabling event logs

Event logs can be enabled via the local group policy editor (*gpedit.msc*). The logs can be accessed via Windows Event Viewer.

Microsoft Windows GPO uses *.admx* files for the configuration parameters and *.adml* language files, where all the texts related to these parameters are referenced.

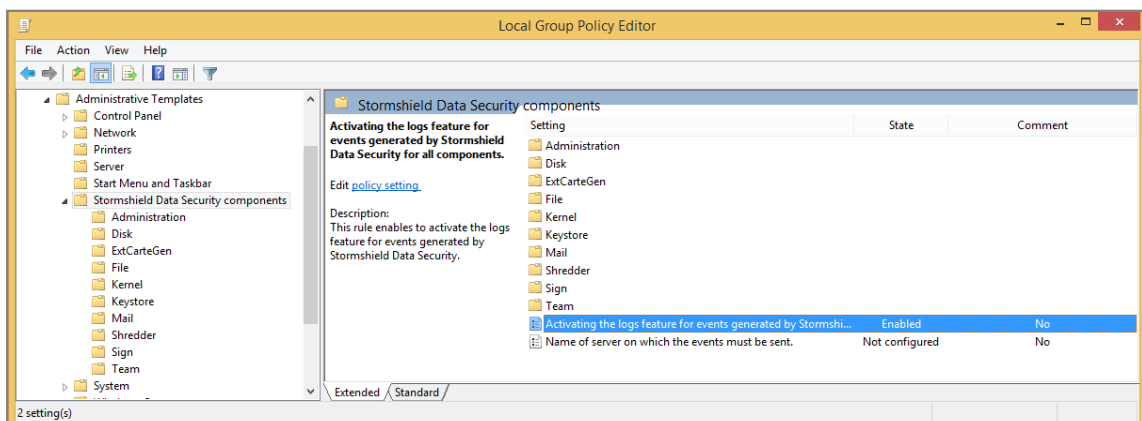
The installation of SDS Enterprise places:

- the *Sbsuite.admx* file in the *%SystemRoot%\PolicyDefinitions* folder
- the *Sbsuite.adml* language file in the *%SystemRoot%\PolicyDefinitions\en-US* folder.

These files are automatically uploaded when launching *gpedit* and it is not necessary to upload them.

1. Run the local group policy editor: **Start > Execute >** then enter *gpedit.msc*.
2. Click on **Administrative Templates > Stormshield Data Security components**. The **Activating the logs feature for events generated by Stormshield Data Security for all modules** entry makes it possible to start generating events once it has been activated. The other entries allow you to configure event generation with greater precision.

Any changes made to the group policy will change the corresponding values in the registry database. These values apply to all users individually. They can be found under the key HKEY_CURRENT_USER in the registry base. However, a group policy (specified remotely by Active Directory) takes priority over changes made locally.



**i NOTE**

The feature **Activating the events logs for Stormshield Data Security Administration components** is a general parameter: if deactivated, no event will be generated, whatever the parameter for the modules. Moreover, a “non configured” module is active if the general parameter is activated.

For example, if you want to activate the events for the Virtual Disk module only:

1. Activate the events logs feature for all modules.
2. Activate the events logs feature for the Virtual Disk module.
3. Disable event logging for all other SDS Enterprise modules.

14.1.2 Understanding the message types

The error messages generated by SDS Enterprise may be one of three types:

- **Information messages:** a simple informational message that does not involve security or require corrective action,
- **Warnings:** an indication to alert the administrator to a potential issue,
- **Errors:** a serious issue that prevents the product from functioning.

14.1.3 Understanding details of logged information

Logs make it possible to display the following information:

- **Message type:** information, warning or error,
- **Date:** date on which the message was generated;
- **Time:** time at which the message was generated;
- **Source:** source from which the event was generated;
- **Category:** short description of the event source;
- **Event:** number corresponding to the type of generated message;
- **User:** SDS Enterprise user name.
- **Computer:** computer name (NetBIOS).

14.2 Troubleshooting issues

If any issue occurs when using the software, SDS Enterprise offers a tracing system. It provides the SDS Enterprise Technical Assistance Center with useful information for the analysis of issues. The workstation and Windows session do not need to be restarted to enable tracing.

14.2.1 Understanding how tracing works

To enable tracing on SDS Enterprise, double-click on a file with the extension *.sbdia*g provided by the SDS Enterprise Technical Assistance Center, or select the **Stormshield Tracing** menu from the Windows **Start** menu.

During tracing, the following elements will be saved in a *.zip* archive found in the the folder **C:/ProgramData/Arkoon/Security BOX/Traces:**



- Generated SDS Enterprise traces (*Trace.etl* file).
- SDS Enterprise events (*audits.evtx* file): it is possible to configure the generation of this file in the interface or in the *.sbdia* file. Events logs must be enabled. To enable them, refer to [Viewing event logs](#).
- A digest of the workstation (*sbdia.xml* file): contains information about the system and the installation of SDS Enterprise and the Microsoft Office suite,
- A PSR trace (Problem Steps Recorder): this tool is provided with Windows operating systems from Windows 7 and allows recording actions performed when reproducing a problem on the workstation. It is possible to configure the generation of this file in the interface or in the *.sbdia* file.

14.2.2 Use the tracing system

From an *.sbdia* file

1. Double-click on the *.sbdia* file provided by the SDS Enterprise Technical Assistance Center to start the tracing interface in pre-configured mode.
2. Click on **Start tracing**.
3. Wait for the **Tracing in progress** message.
4. Reproduce the sequence of actions to be traced.
5. When the sequence is done, click on **Stop tracing**.
6. In the next window, add comments for the SDS Enterprise Technical Assistance Center if needed. Provide additional information about the method of reproduction, time markers, file names, etc.
7. Wait until the folder containing the tracing session opens. Send the zip file *Trace<timestamp>.zip* to the SDS Enterprise Technical Assistance Center.

In pre-configured mode, parameters cannot be modified.

From the tracing interface

If you do not have an *.sbdia* file or if you want to customize the tracing session, select **Stormshield Tracing** in the Windows **Start** menu:

1. To start the session, first open the settings window by clicking on the gear icon and select options.
2. You are advised to select both options in the upper settings panel. Events logs must be enabled to extract SDS Enterprise events. To enable them, refer to [Viewing event logs](#).

i NOTE

The PSR (Problem Steps Recorder) tool can record screen captures during tracing session.

3. Select only the Kernel module and the module affected by the tracing.
4. After you have clicked on **OK** in the dialogue box, a file with the extension *.sbdia* will automatically be created, and the tracing session can then proceed as described in the previous section.



15. Uninstalling SDS Enterprise from user workstations

1. Open the **Control Panel**.
2. Select **Programs and features**.
3. From the list of programs, select SDS Enterprise.
4. Click on **Uninstall**.
5. Follow the on-screen instructions.

You can also use the Setup command of the installation pack which gives you the choice to install, uninstall and modify the list of components installed on your PC.



16. Further reading

Additional information and answers to questions you may have are available in the [Stormshield knowledge base](#) (authentication required).



Appendix A. List of SDS Enterprise logs

You can refer to the list of event logs by feature in the following sections.

To enable logging in the Windows Event Viewer and understand logged information, refer to [Viewing event logs](#).

A.1 Administration

Stormshield Data Security Suite installation

| Number | Type | Description |
|--------|-------------|---|
| 300 | Information | Stormshield Data Security installation was successful. The configuration parameters are: <ul style="list-style-type: none">• Version: %2 [%3]• Patch version: %4• Installation folder: %5• Company: %6 |
| 301 | Information | Stormshield Data Security modification was successful. The configuration parameters are: <ul style="list-style-type: none">• Version: %2 [%3]• Patch version: %4• Installation folder: %5 |
| 302 | Information | Stormshield Data Security uninstall was successful. The configuration parameters are: <ul style="list-style-type: none">• Version: %2 [%3]• Patch version: %4• Installation folder: %5 |
| 303 | Information | Stormshield Data Security patch installation was successful. The configuration parameters are: - <ul style="list-style-type: none">• Version: %2 [%3]• Patch version: %4• Installation folder: %5• Company: %6 |
| 304 | Information | Stormshield Data Security patch modification was successful. The configuration parameters are: - <ul style="list-style-type: none">• Version: %2 [%3]• Patch version: %4• Installation folder: %5 |



| Number | Type | Description |
|--------|-------------|--|
| 305 | Information | Stormshield Data Security patch uninstall was successful. The configuration parameters are: - <ul style="list-style-type: none"> • Version: %2 [%3] • Patch version: %4 • Installation folder: %5 |
| 306 | Error | Stormshield Data Security setup closed unexpectedly. |
| 307 | Error | Stormshield Data Security setup closed before it ends up correctly. |
| 308 | Error | According to the group policy, events are sent to the '%2' server, but connecting to this address fails with the error code %3: "%4". Please ask your administrator. |
| 309 | Error | The policy is not available: %2. |
| 1925 | Error | You do not have sufficient privileges to run this installation for all users on this computer. Open a session as an administrator, then try to run this installation again. |

Directory administration

| Number | Type | Description |
|--------|-------------|--|
| 700 | Information | The automatic update of the directory was successful. |
| 701 | Error | The automatic update of the directory failed. |
| 702 | Information | The manual update of the directory was successful. |
| 703 | Error | The update of the directory failed. |
| 704 | Information | The update of the directory at logon was successful. |
| 705 | Error | The update of the directory at logon failed. |
| 706 | Information | The update of the directory after unlock was successful. |
| 707 | Error | The update of the directory after unlock failed. |
| 708 | Information | The export of certificate(s) %4 of the directory with format '%3' was successful in file '%2'. |
| 709 | Error | The export of certificate(s) %4 of the directory with format '%3' in file '%2' failed. |
| 710 | Information | The import of certificate(s) %2 in the directory was successful. |
| 711 | Error | The import of certificate(s) %2 in the directory failed. |
| 712 | Information | COMPATIBILITY_MODE option: Value: %2 Acces %3 |
| 713 | Information | ALLOW_MANUAL_UPDATE option: Value: %2 Acces %3 |
| 714 | Information | DISABLE_CHECK_ON_DISPLAY option: Value: %2 Acces %3 |
| 715 | Information | ACTIVATE option: Value: %2 Acces %3 |
| 716 | Information | ALLOW_DOWNLOAD_CRL option: Value: %2 Acces %3 |



| Number | Type | Description |
|--------|-------------|---|
| 717 | Information | REPLACE_FROM_LDAP option: Value: %2 Acces %3 |
| 718 | Information | START_ON_CONNECTION option: Value: %2 Acces %3 |
| 719 | Information | REPLACE_FROM_LDAP_OUTOFDATE_CERT option: Value: %2 Acces %3 |
| 720 | Information | REPLACE_FROM_LDAP_REVOKEDCERT option: Value: %2 Acces %3 |
| 721 | Information | DELETE_IF_OUTOFDATE option: Value: %2 Acces %3 |
| 722 | Information | DELETE_IF_REVOKE option: Value: %2 Acces %3 |
| 723 | Information | DELETE_IF_NOT_ON_LDAP option: Value: %2 Acces %3 |
| 724 | Information | SB_EVT_ADMINISTRATION_INFO_REPLACE_ON_VALID_CERT option: Value: %2 Acces %3 |
| 725 | Information | TIMER option: Value: %2 Acces %3 |
| 726 | Information | COMMON_NAME_REPLACE option: Value: %2 Acces %3 |
| 727 | Information | COMMON_NAME_OUT_OF_DATE option: Value: %2 Acces %3 |
| 728 | Information | COMMON_NAME_REVOKE option: Value: %2 Acces %3 |
| 729 | Information | COMMON_NAME_NOT_ON_LDAP option: Value: %2 Acces %3 |
| 730 | Warning | The LDAP update of the certificate which email is '%2' could not be applied because the revocation list is not available. |

Management of the revocation list

| Number | Type | Description |
|--------|-------------|---|
| 1100 | Information | The update of the revocation list %2 was successful. |
| 1101 | Error | The update of the revocation list %2 failed. |
| 1102 | Information | The update of the revocation list %2 from the cache was successful. |
| 1103 | Error | The automatic update of the revocation list %2 from the cache failed. |

A.2 Virtual Disk

Volume management

| Number | Type | Description |
|--------|-------------|--|
| 8300 | Information | The automatic volume '%2' was successfully mounted on '%3' in '%4' mode. |
| 8301 | Error | The automatic volume '%2' failed to mount on '%3' in '%4' mode. |
| 8302 | Information | The volume '%2' was successfully mounted on '%3' in '%4' mode. |
| 8303 | Error | The volume '%2' failed to mount on '%3' in '%4' mode. |
| 8304 | Information | The automatic volume '%2' mounted on '%3' was successfully unmounted. |



| Number | Type | Description |
|--------|-------------|--|
| 8305 | Error | The automatic volume '%2' mounted on '%3' failed to unmount. |
| 8306 | Information | The volume '%2' mounted on '%3' was successfully unmounted. |
| 8307 | Error | The volume '%2' mounted on '%3' failed to unmount. |
| 8308 | Information | The volume '%2' mounted on '%3' was successfully locked. |
| 8309 | Error | The volume '%2' mounted on '%3' failed to unlock. |
| 8310 | Information | The volume '%2' mounted on '%3' was successfully unlocked. |
| 8311 | Error | The volume '%2' mounted on '%3' failed to unlock. |
| 8312 | Information | The volume '%2' was successfully created. |
| 8313 | Error | The creation of volume '%2' failed. |
| 8314 | Information | The volume '%2' was successfully added to the list of automatic volumes. It will be mounted on '%3'. |
| 8315 | Error | The volume '%2' failed to be added to the list of automatic volumes. |
| 8316 | Information | The volume '%2' mounted on '%3' was successfully deleted from the list of automatic volumes. |
| 8317 | Error | The volume '%2' (mounted on '%3') failed to be deleted from the list of automatic volumes. |

A.3 File

Encryption/Decryption

| Number | File type | Type Description |
|--------|-------------|--|
| 18300 | Information | The user successfully encrypted the file '%2' in auto-decryptable mode. |
| 18301 | Error | The encryption of the file '%2' in auto-decryptable mode failed. |
| 18302 | Information | The user successfully encrypted the folder '%2' in auto-decryptable mode. |
| 18303 | Error | The encryption of the folder '%2' in auto-decryptable mode failed. |
| 18304 | Information | The user successfully encrypted the file '%2' via SecurityBOX SmartFile. |
| 18305 | Error | The encryption of file '%2' via SecurityBOX SmartFile failed. |
| 18306 | Information | The user successfully encrypted the folder '%2' via SecurityBOX SmartFile. |
| 18307 | Error | The encryption of the folder '%2' via SecurityBOX SmartFile failed. |
| 18308 | Information | The user successfully encrypted the file '%2' for the following peers: %3. |
| 18309 | Error | The encryption of the file '%2' failed for the following peers: %3. |
| 18310 | Information | The user successfully encrypted the folder '%2' for the following peers: %3. |
| 18311 | Error | The encryption of the folder '%2' failed for the following peers: %3. |



| Number | File type | Type Description |
|--------|-------------|---|
| 18312 | Information | These coworkers were successfully added to the file '%2': %r%3. |
| 18313 | Error | These coworkers could not be added to the file '%2': %r%3. |
| 18314 | Information | These coworkers were successfully removed from the file '%2': %r%3. |
| 18315 | Error | These coworkers could not be removed from the file '%2': %r%3. |
| 18316 | Error | An error occurred with the certificate of '%2'. |

Encryption/Decryption

| Number | File type | Type Description |
|--------|-------------|--|
| 18700 | Information | The user successfully encrypted the file '%2'. |
| 18701 | Error | The encryption of the file '%2' failed. |
| 18702 | Information | The user successfully decrypted the file '%2'. |
| 18703 | Error | The decryption of the file '%2' failed. |
| 18704 | Error | The path '%2' has not been decrypted because it is protected by Share. |
| 18705 | Error | The folder '%2' was not decrypted because it contains a Share protected subfolder. |

A.4 Kernel

Start/Stop

| Number | Type | Description |
|--------|-------------|--|
| 25300 | Information | The kernel was successfully started. |
| 25301 | Error | The kernel failed to start. |
| 25302 | Information | The kernel was successfully shut down. |
| 25303 | Error | The kernel failed to shut down. |

LDAPS authentication

| Number | Type | Description |
|--------|-------------|---|
| 25700 | Warning | SSL security warning: invalid server certificate. Issued to: %2% Issued by: %3 Valid from %4 to %5. Contact your administrator. |
| 25701 | Error | SSL security error: invalid server certificate. Issued to: %2% Issued by: %3 Valid from %4 to %5. Contact your administrator. |
| 25702 | Error | All authentication methods submitted to the LDAP server %2 have failed. |
| 25703 | Information | The user is authenticated by the LDAP server %2 with the method: %3. |



Select cryptographic device

| Number | Type | Description |
|--------|-------------|--|
| 26100 | Information | The user selected the '%2' middleware. |

A.5 Keystore

Login/Logout

| Number | Type | Description |
|--------|-------------|--|
| 31300 | Information | The user logged in to their Stormshield Data Security keyring. |
| 31301 | Error | Login to Stormshield Data Security keyring failed. |
| 31302 | Information | The user logged out of their Stormshield Data Security keyring. |
| 31303 | Error | The user could not log out of their Stormshield Data Security keyring. |
| 31304 | Information | The Stormshield Data Security user session was locked. |
| 31305 | Error | The Stormshield Data Security user session failed to lock. |
| 31306 | Information | The Stormshield Data Security user session successfully unlocked. |
| 31307 | Error | The Stormshield Data Security user session failed to unlock. |
| 31308 | Warning | A user is already logged in to Stormshield Data Security in another Windows session. |
| 31309 | Warning | Incorrect secret code entered. |
| 31310 | Warning | The identifier '%2' does not match any Stormshield Data Security account. |
| 31311 | Warning | The Stormshield Data Security session could not be unlocked because the wrong smart card was in the drive. |
| 31312 | Error | The Stormshield Data Security account or smart card was blocked. |
| 31313 | Information | The smart card was removed from the drive. |
| 31314 | Error | The smart card is blocked. |
| 31315 | Error | Unable to notify a component. |
| 31316 | Error | Unable to load a component: '%2'. |

Account management

| Number | Type | Description |
|--------|-------------|---|
| 31700 | Information | The account was successfully created. |
| 31701 | Warning | The installation of the Stormshield Data Security account encountered a non-blocking error. |



| Number | Type | Description |
|--------|-------------|---|
| 31702 | Error | Could not install the Stormshield Data Security account. |
| 31703 | Information | The Stormshield Data Security account was successfully uninstalled. |
| 31704 | Error | Could not uninstall the Stormshield Data Security account. |
| 31705 | Information | The security policy was updated. |
| 31706 | Error | The security policy update failed with the following error: %2. |
| 31707 | Information | The Stormshield Data Security account was successfully exported. |
| 31708 | Error | Could not export the Stormshield Data Security account. |
| 31709 | Information | The account's secret code was successfully changed. |
| 31710 | Error | Could not change the account's secret code. |
| 31711 | Error | The number of errors while changing the secret code exceeded the authorized limit. |
| 31712 | Error | Could not create a new Stormshield Data Security account because the smart card is blocked. |
| 31713 | Warning | Incorrect secret code entered. |
| 31714 | Error | The contents of the smart card do not allow automatic account creation. |
| 31715 | Error | Could not create a new Stormshield Data Security account because the template is blocked. |
| 31716 | Error | Could not create a new Stormshield Data Security account because the template cannot be accessed. |
| 31717 | Information | A new security policy signatory was set. |
| 31718 | Warning | The security policy update was not applied because the user has rejected the new signer. |
| 31719 | Information | Security policy downloaded from '%2'. |
| 31720 | Warning | Error in the security policy downloaded from '%2'. |
| 31721 | Information | The security policy update was not applied because the account is up to date. |
| 31722 | Error | The security policy update was not applied because the file signature is incorrect. |
| 31723 | Error | The security policy update was not applied for the following reason: '%2'. |
| 31724 | Warning | The security policy update was not applied despite the warning: %2. |
| 31725 | Error | The 'MasterPolicies' parameter prohibits the duplication of the file '%2'. |
| 31726 | Error | %2 smart card account automatically created: %3. |



Key management

| Number | Type | Description |
|--------|-------------|---|
| 32100 | Information | The encryption key was successfully exported. |
| 32101 | Error | Failed to export the encryption key. |
| 32102 | Information | The encryption key was successfully renewed. |
| 32103 | Error | Failed to renew the encryption key. |
| 32104 | Information | The signature key was successfully exported. |
| 32105 | Error | Failed to export the signature key. |
| 32106 | Information | The signature key was successfully renewed. |
| 32107 | Error | Failed to renew the signature key. |
| 32108 | Information | The key was successfully exported. |
| 32109 | Error | Failed to export the key. |
| 32110 | Information | The key was successfully renewed. |
| 32111 | Error | Failed to renew the key. |
| 32112 | Information | The encryption key certificate was successfully exported. |
| 32113 | Error | Failed to export the encryption key certificate. |
| 32114 | Information | The signature key certificate was successfully exported. |
| 32115 | Error | Failed to export the signature key certificate. |
| 32116 | Information | The key certificate was successfully exported. |
| 32117 | Error | Failed to export the key certificate. |
| 32118 | Information | A certificate for the %2 was not imported into the user account because it has expired. |
| 32119 | Information | A certificate for the %2 was not imported into the user account because it has insufficient privileges. |

Keyring management

| Number | Type | Description |
|--------|-------------|---|
| 32500 | Information | The decryption key was successfully imported. |
| 32501 | Error | Failed to import the decryption key. |
| 32502 | Information | The recovery key was successfully imported. |
| 32503 | Error | Failed to import the recovery key. |



A.6 Mail

Outgoing/Incoming

| Number | Type | Description |
|--------|-------------|--|
| 39312 | Information | The certificate of the user '%2' has not been found in the trusted address book. |
| 39313 | Information | The certificate of the user '%2' has been revoked. |
| 39314 | Information | The certificate of the user '%2' is no longer valid. |
| 39315 | Information | The trust chain of the user '%2' has been revoked. |
| 39316 | Information | The trust chain of the user '%2' is no longer valid. |
| 39317 | Information | The certificate revocation list is not available for the user '%2'. |
| 39318 | Warning | The user received an encrypted e-mail but does not have any decryption key. |
| 39319 | Warning | The user received an e-mail with an invalid signature. The e-mail has been signed with the certificate '%2'. |
| 39320 | Information | Sending a signed e-mail was successful [Recipient(s): %2]. |
| 39321 | Information | Sending an encrypted e-mail was successful [Recipient(s): %2]. |
| 39322 | Information | Sending a signed and encrypted e-mail was successful [Recipient(s): %2]. |

Cross-encryption

| Number | Type | Description |
|--------|-------------|---|
| 39700 | Information | The user run transcipherment on the folder '%2' |
| 39701 | Warning | Issues occurred with transcipherment. |

Disabling security

| Number | Type | Description |
|--------|-------------|---|
| 40100 | Information | The security of e-mails in the folder '%2' has been disabled. |
| 40101 | Information | The security of some e-mails has been disabled (number: %2). |
| 40102 | Warning | Issues occurred when disabling the security of some e-mails. |



Administration

| Number | Type | Description |
|--------|-------------|--|
| 40500 | Information | The Stormshield Data Mail module has been successfully loaded in Outlook '%2'. |
| 40501 | Information | The Stormshield Data Mail module has been disabled in Outlook '%2'. |
| 40502 | Information | The following exception has been raised in the Stormshield Data Mail module: '%2'. |
| 40503 | Warning | The following registry key, which is necessary for the Stormshield Data Mail Outlook Edition add-in to work properly, has been modified: '%2'. |

A.7 Shredder

| Number | Type | Description |
|--------|-------------|---|
| 46300 | Information | Shredding was successfully initiated. |
| 46301 | Error | Failed to start shredding. |
| 46302 | Information | Shredding was successful. |
| 46303 | Error | Shredding failed. |
| 46304 | Information | The file '%2' was successfully deleted. |
| 46305 | Error | Could not delete the file '%2'. |
| 46306 | Information | The folder '%2' was successfully deleted. |
| 46307 | Error | Could not delete the folder '%2'. |
| 46308 | Information | Bin was securely emptied. |
| 46309 | Error | Failed to empty bin securely. |
| 46310 | Information | The list of files was securely cleaned. |
| 46311 | Error | Failed to clean the list of files securely. |

A.8 Sign

Signature

| Number | Type | Description |
|--------|-------------|---|
| 47300 | Information | The file '%2' was successfully signed. |
| 47301 | Error | Could not sign the file '%2'. |
| 47302 | Information | The file '%2' was successfully co-signed. |
| 47303 | Error | Could not co-sign the file '%2'. |



| Number | Type | Description |
|--------|-------------|--|
| 47304 | Information | The file '%2' was successfully counter-signed. |
| 47305 | Error | Could not counter-sign the file '%2'. |
| 47306 | Information | The file '%2' was successfully over-signed. |
| 47307 | Error | Could not over-sign the file r '%2'. |
| 47308 | Error | File '%2' is corrupted. |

A.9 Team

Rule management

| Number | Type | Description |
|--------|-------------|--|
| 49300 | Information | A security rule has been set for the folder '%2'. |
| 49301 | Error | Configuration of folder '%2' as a secure folder failed. |
| 49302 | Information | The folder '%2' is back to clear mode (not secure). |
| 49303 | Error | Configuration of folder '%2' as a non-secure folder has failed. |
| 49304 | Information | The following co-workers have been successfully added to folder '%2' rule:%r%3. |
| 49305 | Error | Could not add the following co-workers to folder '%2' rule:%r%3. |
| 49306 | Information | The following co-workers have been successfully removed from folder '%2' rule:%r%3. |
| 49307 | Error | Could not remove the following co-workers from folder '%2' rule: %r%3. |
| 49308 | Information | The following owners have been successfully added to folder '%2' rule: %r%3. |
| 49309 | Error | Could not add the following owners to folder '%2' rule: %r%3. |
| 49310 | Information | The following owners have been successfully removed from folder '%2' rule: %r%3. |
| 49311 | Error | Could not remove the following owners from folder '%2' rule: %r%3. |
| 49312 | Information | Folder '%2' has been successfully configured as a secure folder (profile). |
| 49313 | Error | Configuration of folder '%2' as a secure folder failed (profile). |
| 49314 | Information | Folder '%2' has been successfully configured as a non-secure folder (profile). |
| 49315 | Error | Configuration of folder '%2' as a non-secure folder failed (profile). |
| 49316 | Information | The folder '%2' rule has been successfully updated (profile). |
| 49317 | Error | Could not update the folder '%2' rule (profile). |
| 49318 | Information | The following co-workers were successfully added to folder '%2' rule (profile):%r%3. |



| Number | Type | Description |
|--------|-------------|---|
| 49319 | Error | Could not add the following co-workers to folder '%2' rule (profile):%r%3. |
| 49320 | Information | The following co-workers have been successfully removed from folder '%2' rule (profile):%r%3. |
| 49321 | Error | Could not remove the following co-workers from folder '%2' rule (profile): %r%3. |
| 49322 | Warning | Could not update the rules file (.ust) of the folder '%2': inconsistent header. |
| 49323 | Warning | The user is not one of the users allowed for the rule on '%2'. |
| 49324 | Warning | The user is accessing the rule properties on '%2' even though the certificate is revoked. |
| 49325 | Information | The security rule of folder '%2' has been saved in the user account. |
| 49326 | Warning | Could not find the certificate '%2'. |
| 49327 | Information | The certificate '%2' is invalid and has been ignored. |
| 49328 | Information | The certificate '%2' is invalid; the user interrupted the encryption operation. |
| 49329 | Warning | The certificate '%2' could not be fully verified and has been used. |
| 49330 | Information | The certificate '%2' could not be fully verified and has been ignored. |
| 49331 | Warning | The certificate '%2' is invalid and revoked, and has been deleted from the rule. |
| 49332 | Information | The safety rule on folder '% 2' has been restored from the user account. |
| 49333 | Warning | Attack suspected: the security rule of folder '%2' has been replaced. |
| 49334 | Information | The security rule of folder '%2' has disappeared. |
| 49335 | Warning | A false coworker has been detected and ignored in the security rule of folder '%2'. |
| 49336 | Information | The safety rule on folder '% 2' has been restored from the local rule. |
| 49342 | Warning | Could not verify the parent-child relationship or revocation list. |

Team rule update

| Number | Type | Description |
|--------|---------|---|
| 49337 | Warning | Could not find the new certificate of co-worker '%2', who is no longer part of the rule. |
| 49338 | Warning | The rule known on folder '%2' is not up to date. The automatic update could not be applied. |
| 49339 | Warning | Folder '%2', to which the rule applies, could not be found or is no longer secure. |
| 49340 | Error | Could not find the encryption key of co-worker '%2'. |
| 49341 | Warning | Could not find co-worker '%2' in the rule. |



Encryption/decryption

| Number | Type | Description |
|--------|-------------|---|
| 49700 | Information | File '%2' was successfully moved from a secure folder to a non-secure folder. |
| 49701 | Error | Failed to move file '%2' from a secure folder to a non-secure folder. |
| 49702 | Information | Folder '%2' was successfully moved from a secure folder to a non-secure folder. |
| 49703 | Error | Failed to move folder '%2' from a secure folder to a non-secure folder. |
| 49704 | Information | File '%2' was successfully secured with defined rules. |
| 49705 | Error | Failed to secure file '%2' with defined rules. |
| 49706 | Information | Folder '%2' was successfully secured with defined rules. |
| 49707 | Error | Failed to secure folder '%2' with defined rules. |
| 49708 | Information | Security on file '%2' was successfully removed. |
| 49709 | Error | Failed to remove security from file '%2'. |
| 49710 | Information | Security was successfully removed from folder '%2'. |
| 49711 | Error | Failed to remove security from folder '%2'. |
| 49712 | Information | Securing operation cancelled. |
| 49713 | Information | Removal of security cancelled. |
| 49714 | Error | Could not ensure compliance of folder '%2': you do not have the Windows permissions. |
| 49715 | Warning | Could not ensure compliance of hidden folder '%2': you do not have the Windows permissions. |

Backup/Restoration

| Number | Type | Description |
|--------|-------------|-------------------------------------|
| 50100 | Information | File '%2' successfully backed up. |
| 50101 | Error | Could not back up file '%2'. |
| 50102 | Information | Folder '%2' successfully backed up. |
| 50103 | Error | Could not back up folder '%2'. |
| 50104 | Information | File '%2' successfully restored. |
| 50105 | Error | Could not restore file '%2'. |
| 50106 | Information | Folder '%2' successfully restored. |
| 50107 | Error | Could not restore folder '%2'. |
| 50108 | Information | Save cancelled. |



| Number | Type | Description |
|--------|-------------|--|
| 50109 | Information | Restoration cancelled. |
| 50110 | Error | Could not save in folder '%2': you do not have the Windows permissions. |
| 50111 | Error | Could not restore in folder '%2': you do not have the Windows permissions. |

Driver

| Number | Type | Description |
|--------|---------|---|
| 50500 | Warning | File '%2' cannot be opened using '%3'. |
| 50501 | Error | A timeout occurred while trying to open the file '%2' using '%3'. |
| 50502 | Error | Team service request failed: '%2' using '%3'. |

A.10 Share

| Number | File type | Type Description |
|--------|-------------|--|
| 14300 | Information | The Share configuration file '%2' is invalid. |
| 14301 | Information | The Share configuration file '%2' is missing. |
| 14302 | Information | Unable to communicate with the Share driver. |
| 14303 | Information | The user successfully encrypted the file '%2' using an automatic protection rule. |
| 14304 | Error | Failed to encrypt file '%2' using an automatic protection rule. |
| 14305 | Information | The user has successfully encrypted the file '%2' using an automatic protection rule for the following correspondents: %r%3. |
| 14306 | Error | Failed to encrypt file '%2' using an automatic protection rule for the following correspondents: %r%3. |
| 14307 | Information | Automatic protection rule has been applied. |
| 14308 | Error | Automatic protection rule cannot be applied. |
| 14309 | Information | The user successfully encrypted the folder '%2' using an automatic protection rule. |
| 14310 | Error | Encryption of folder '%2' using an automatic protection rule failed. |
| 14311 | Information | Automatic protection rule has been activated. |
| 14312 | Error | Automatic protection rule cannot be enabled. |
| 14313 | Information | Automatic protection rule has been disabled. |
| 14314 | Error | Automatic protection rule cannot be disabled. |
| 14315 | Information | Automatic protection has been modified. |
| 14316 | Error | The automatic protection rule cannot be changed. |



Appendix B. Third-party libraries

SDS Enterprise uses the following libraries:

- JsonCpp
- OpenSSL
- OssiASN1
- ZLib
- Efs
- Reber
- Didisoft



STORMSHIELD

documentation@stormshield.eu

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

Copyright © Stormshield 2024. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.