STORMSHIELD

STORMSHIELD DATA SECURITY ENTERPRISE

RELEASE NOTES

Version 11

Document last updated: October 30, 2026

Reference: sds-en-sdse-release_notes-v11.5.3

Table of contents

New behavior 3
New features and enhancements in SDS Enterprise 11.5.3 4
Compatibility 5
Known issues 6
Explanations on usage 7
Documentation resources 12
Downloading this version 13
Previous versions of SDS Enterprise v11 14
Contact 39

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

This document is not exhaustive and minor changes may have been included in this version.

New behavior

Changes introduced in version 11.4

When installing SDS Enterprise 11.4, the event logs are now enabled by default. They can be accessed via the Windows Event Viewer on user workstations.

You can disable all or part of the logs via a GPO. For more information, see Viewing event logs in the *Administration guide*.

Users must now accept the change of security policy signatory before logging into their SDS Enterprise account. For more information, see Modifying the signatory of a security policy in the *Administration guide*.

Changes introduced in version 11.3

As of January 2025, Stormshield will no longer offer functional upgrades to the Stormshield Data Team feature. The feature will switch to maintenance mode from this date.

Change introduced in version 11.1.1

Starting with SDS Enterprise version 11.1.1, the agent is now installed by default with a security policy, which applies if you do not use your own security policy.

Changes introduced in version 11.0

The directory in which temporary files are stored during Stormshield Data Sign co-signing and counter-signing operations is now always *%temp%*. You can no longer customize it using the TmpFolder parameter in the *SBox.ini* file.

The Stormshield Data Authority Manager administration tool has been replaced by the Stormshield Data Management Center web administration interface. Policies defined in SDMC Data Authority Manager cannot be configured in Stormshield. To obtain help on the reproduction of security policies in SDMC and the migration of encryption keys and signature of users from version 10 to version 11 of SDS Enterprise, contact your commercial team Stormshield.

In the Properties of the SDS Enterprise agent, the icons of the following features are no longer available: **File**, **Shredder**, **Virtual Disk** and **Mail**, as well as the **Automatic update** icon. These features are now fully configurable via the SDMC administration console.

Stormshield Data Mail for Lotus Notes has been removed from SDS Enterprise.

The .NET cmdlets or APIs for logging in/out and locking/unlocking the SDS Enterprise account, available via the Connector component, are now disabled in cases where users log in to their SDS Enterprise account in SSO mode.

SDS Enterprise agent version 11.0 is only available for Microsoft Windows 64-bit workstations.

New features and enhancements in SDS Enterprise 11.5.3

System

Some improvements have been made to SDS Enterprise in order to increase its robustness and thereby reduce the risk of vulnerabilities.

Compatibility

Refer to the Product life cycle guide to find out more on compatibility with Microsoft Windows versions.

Web browsers (server)

Microsoft Edge	Latest stable version
Google Chrome	Latest stable version
Mozilla Firefox	Latest stable version

Synchronizers for automatic file protection

SharePoint Online/Office 365
OneDrive Entreprise/for Business in Office 365

Known issues

The up-to-date list of the known issues related to this version of SMC is available on the Stormshield Knowledge base. To connect to the Knowledge base, use your MyStormshield customer area identifiers.

Explanations on usage

Stormshield Data Management Center

SDMC does not support public key infrastructure (PKI) management, unlike Stormshield Data Authority Manager version 10.

Smart cards/tokens

For the SDS Enterprise middleware to function properly, the smart card minidrivers of the cryptographic medium in question must be installed on the workstation.

The smart card reader for a cryptographic medium cannot be changed during the course of a Windows session. If you have started using a smart card in a certain reader, you must restart your Windows session in order to use this card in another reader.

Virtual card accounts can only be created with RSA keys of up to 2048 bits. This limitation also applies to SSO accounts whose keys are stored on a virtual card.

Microsoft Virtual Smart Cards and certain types of smart cards associated to their middleware do not support the RSA-OAEP-SHA-256 encryption algorithm. This incompatibility prevents *.sdsx* files from being decrypted. For more information, refer to the Stormshield knowledge base.

Kernel

After the SDS Enterprise agent has been installed or after changes have been made to the security policy, the workstation must be restarted for the policy to be correctly applied.

Malfunctions may occur when connecting two cryptographic devices (token and/or card) at the same time on a workstation. This restriction does not apply when the SmartCard support Stormshield middleware is used.

When the Windows setting for the size of the elements is set to more than 100%, the SDS band in the connection window and in the "About" window does not display on the entire width of the window.

When importing PGP keys, if the window **Password required** is resized, the buttons **Cancel** and **OK** do not correctly display.

When peers are selected from the LDAP directory for an encryption operation, for peers that have several certificates, SDS Enterprise will always suggest the most recent certificate, even if it has been revoked. The encryption operation will therefore fail. We recommend deleting revoked certificates from your LDAP directory.

When a *.usi* account from the SDAM is installed on a user's workstation, the values of the parameters prescribed by the *.json* policy configuration file prevail when the kernel starts up, and when the user logs in.

The type of SSO account used to log in to the SDS Enterprise account depends on the operation of the smart card or USB token account type. The agent card extension must therefore be installed for it to run.

When an SDS Enterprise account is blocked, the only way for a password account to be unblocked is via the account's backup password.

Specific revocation list download protocols cannot be disabled (HTTP, FILE, etc.).

The date on which the revocation list was last downloaded is no longer shown in the revocation controller. However, an entry in the Windows event log is generated.

The recovery account certificate must have Data Encipherment and Key Encipherment features.

Stormshield Data File

User access management - the "Edit access" menu cannot be used when selecting both files and folders.

SDS Enterprise currently does not support Microsoft OneNote documents.

When a file is protected in *.sdsx* format, or protection is removed from an .sdsx file, Windows permissions applied to the file are restricted to the session user only and to the permissions inherited from the parent folder.

If it is not possible to save a protected document currently being edited (the document has been renamed or deleted in the meantime, or the document is on a network share and the connection is interrupted), the user must change the save location or rename the document.

The SDSX format does not support RSA keys for certificates strictly below 2048 bits.

Temporary decryption folders cannot be protected locally with the Data Team module.

Stormshield Data Share

Automatic folder protection is not supported on the contents of a newly added disk volume. You must restart the workstation so that the volume is recognized by Stormshield Data Share.

Automatic folder protection cannot apply to folders already protected by Team.

By default, Microsoft applications are not allowed to "Save as" in synchronized shared spaces, to prevent sharing files in plaintext.

When automatic document protection is enabled for a folder and you use the "Save as" function on the applications concerned, you need to close the application from which you saved the file for the file to be visible in the automatically protected folder.

The file path from the root of the synchronized folder must not exceed 185 characters, including extensions (e.g., .pptx, .sdsx). Otherwise, the file will not be protected and will no longer be accessible.

When an automatic protection rule is applied to the content of a folder, or when protection is removed from the content of a folder after an automatic protection rule has been disabled, the Windows permissions applied to the files contained in the folder are restricted to the session user and to the permissions inherited from the parent folder.

Share is not supported on network shares, file servers or external drives.

If the "padlock" icon is not visible on a protected folder, check in the registry, in "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers", that the following keys are positioned above the existing keys in the tree:

- EncrypterOverlayIcon
- SDSShareOverlayIcon

If this is not the case, add spaces before their names and restart Explorer in order to apply the change.

The protection of a folder cannot be modified if you have already protected or modified access to one of its sub-folders or parent folders.

User access management - the "Edit access" menu cannot be used:

- when both files and folders are selected.
- on a simultaneous selection of several protected folders or on an unprotected folder.

Sharing protection rules

For a shared protection rule on a folder to apply to a user, he or she must be logged into their SDS Enterprise account, be one of the recipients of the rule and be browsing the folder concerned.

An automatic protection rule defined locally on a collaborative space folder by one user and not shared is overwritten if another user defines a shared rule on the same folder, including the first user.

If two users define a different shared protection rule on the same folder, the most recent rule is taken into account.

When a user deletes a folder bearing a shared protection rule by placing it in the recycle bin, the rule remains active until the recycle bin is emptied.

It is not possible to transform a shared protection rule into a non-shared rule, and vice versa.

Stormshield Data Mail

Microsoft Outlook's message recall feature is not compatible with Stormshield Data Mail encryption.

Encrypted messages cannot be sent to recipients over Microsoft Exchange in offline mode in Microsoft Outlook. A connection is required for SMTP address resolution.

Users may sometimes not be able to open .sdsx files attached to encrypted messages It is therefore recommended to download attachments before opening them.

PGP messages received as attachments (.msg) cannot be opened by dragging and dropping them in an Outlook folder.

When the Outlook reading pane is disabled, simply double-clicking on a large encrypted message will not open it. You must double-click twice on the message.

The encryption band does not display when writing a new encrypted email via the **Start** menu if Outlook is not running. The email will thus be correctly encrypted.

The Mail add-in is not compatible with Kaspersky Outlook Anti-Virus Addin. If the certificates of the recipient are not available, some e-mails can be sent as they are not encrypted.

We do not recommend removing the smart card to lock a SDS Enterprise card account whereas an e-mail is being saved as the backup will not work.

In Windows Explorer, *.msg* files signed or encrypted with Outlook cannot be opened. In this case, apply the workaround described in the Stormshield Knowledge base (authentication required).

Stormshield Data Virtual Disk

You are advised against using a Virtual Disk volume on remote spaces. A loss of connection could prevent disk access or lead to the loss of changes made to the disk, or even irreparably corrupt the data on the disk.

Stormshield Data Team

Stormshield Data Team is not compatible with the Veeam backup tool. The tool prevents folders protected with a Team rule from being encrypted.

In Microsoft Windows 10 and 11, when the user encrypts a folder, the SDS Enterprise padlock icon does not always appear on encrypted files. However files are correctly encrypted.

The Shadow Copy volume backup system, enabling version management in Windows Explorer among other things, is not supported by Stormshield Data Team.

Synchronized directories such as SharePoint, Dropbox, Office 365, Google Drive on premise, etc. are not supported by Stormshield Data Team and therefore cannot be secured by the module. We recommend excluding these directories from the folders analyzed by Stormshield Data Team using the advanced **Folder exclusion** setting available in Team functionality configuration in the SDMC administration console.

The user must be logged in to their SDS Enterprise account or must unlock it when they want to copy and paste a file into a folder secured by Stormshield Data Team if a file with the same name already exists in the folder. If the user performs the operation without being logged in, the contents of the file are emptied.

The user must be logged in to their SDS Enterprise account or must unlock it if they want to modify a *zipped* folder contained in a folder secured by Stormshield Data Team. If they edit a *.zip* folder without being logged in, the files inside are deleted.

Stormshield Data Shredder

It is not possible to permanently delete synchronized OneDrive folders using the Shredder feature. However, the files contained in these folders can be deleted with Shredder.

SDS Encryption Portal

In "external PKI" mode and on mobile phones only, when users of the encryption portal log in via the Microsoft Entra ID solution, if two-factor authentication is not set up, they must authenticate once and then click on **Log in with Microsoft** again.

Documentation resources

The following technical documentation resources are available on the Stormshield technical documentation website. We recommend that you rely on these resources to get the best results from all features in this version.

Guides

- Stormshield Data Security Enterprise - Administration guide
- Stormshield Data Security Enterprise - Advanced configuration guide
- Stormshield Data Security Enterprise - Advanced user guide
- Stormshield Data Security Enterprise - User guide
- SDS Encryption Portal - Administration user guide
- Stormshield Data Security Enterprise - Architecture and security guide
- Stormshield Data Connector - User Guide
- Migration guide

Downloading this version

Going to your MyStormshield personal area

You need to go to your MyStormshield personal area in order to download the 11.5.3 version of Stormshield Data Security Enterprise:

1. Log in to MyStormshield with your personal identifiers.
2. In the left panel, select **Downloads**.
3. In the right panel, select the relevant product and version.

Checking the integrity of the binary files

To check the integrity of Stormshield Data Security Enterprise binary files:

1. Enter one of the following commands and replace `filename` by the name of the file you want to check:
   - Linux operating system: `sha256sum filename`
   - Windows operating system: `CertUtil -hashfile filename SHA256`
2. Compare with hashes provided on MyStormshield personal area, section **Downloads**.

Previous versions of SDS Enterprise v11

In this section, you will find the new features and fixes from previous versions of Stormshield Data Security Enterprise 11.x.

11.5.1		Bug fixes
11.5	New features	
11.4.5	New features	Bug fixes
11.4.4		Bug fixes
11.4.3		Bug fixes
11.4.2		Bug fixes
11.4.1	New features	
11.4	New features	Bug fixes
11.3	New features	Bug fixes
11.2.1		Bug fixes
11.2	New features	Bug fixes
11.1.1		Bug fixes
11.1	New features	Bug fixes
11.0	New features	Bug fixes

Version 11.5.2 not published

Version 11.5.2 is not available to the public.

SDS Enterprise 11.5.1 fixes

Updated from SDS Enterprise 10 to SDS Enterprise 11

When updating from SDS Enterprise version 10 to version 11, the folder *C:\ProgramData\Arkoon\Security BOX\DefaultUsr* is now created automatically if it does not already exist. Consequently, the workstation remains functional after the update, even if this folder was deleted.

Certificate Renewal

Support reference STORM-62983

Users who changed their email address when renewing their certificate no longer receive an error message when they change coworkers access to an encrypted file.

Middleware for USB card or token accounts

Support reference STORM-62680

If the user changes the type of smart card or USB token used by SDS Enterprise from the **Card extension configurator** or from the **Choose card or USB key type** menu accessible from the SDS Enterprise icon in the Windows taskbar, they no longer encounter a block when restarting the SDS Enterprise Agent.

Stormshield Data Team

Support reference STORM-64235

Files uploaded to a folder secured by Stormshield Data Team are now properly processed and secured when Microsoft Defender XDR is enabled on the workstation.

Support reference STORM-65009

The SkipApp registry key is used to exclude Windows processes that regularly access Stormshield Data Team-encrypted folders and are considered secure. In some cases, this key could be ignored and this led to incompatibility between Stormshield Data Team and other security software installed on workstations. This issue has been fixed.

Exporting a SDS Enterprise user account

Support reference STORM-69249

It is again possible to export a SDS Enterprise Password account and import it to another workstation. The export no longer worked correctly since version 11.4.0.

However, please note that:

- a user account exported from a version 11 cannot be imported by a version 10 of SDS Enterprise.
- a self-certified user account exported from version 11.5 cannot be imported by a previous version 11 due to changes made to enhance security.

SDS Enterprise 11.5 new features and enhancements

SDS Enterprise administration

New default policy
In SDMC, you can now use the new « *Diffusion Restreinte* Policy », suitable for sensitive information tagged as *Diffusion restreinte* (DR).

Find out more

New features and enhancements in SDS Enterprise 11.4.5

Automatic creation of card or USB token accounts

You can now use two certificate authorities for encryption keys and two for signature keys by adding the following settings to the *accountPolicy.creation.automatic* section of your policy's JSON file:

- *secondaryEncryptionKeyAuthorityId*
- *secondarySignatureKeyAuthorityId*

During automatic account creation, SDS Enterprise always selects the most recent certificate (i.e., the one with the most recent validity start date), regardless of the issuing authority.

For more information, see the *Account* section of the Advanced Configuration Guide.

SDS Enterprise 11.4.5 fixes

Stormshield Data Shredder

Support reference STORM-66291

Environment variables and SDS Enterprise keywords used in file paths for the Shredder feature are now interpreted correctly. For more information about the format, see the *Configure Stormshield Data Shredder* section of the Administration Guide.

SDS Enterprise 11.4.4 fixes

Stormshield Data File

Support reference STORM-63859

If you use the feature that automatically converts *.sbox* files to the *.sdsx* format, SDS Enterprise will now search for valid equivalent certificates in the trusted address book and then in the LDAP directory during cross-encryption if collaborators' encryption certificates contain errors (expired, revoked, or RSA key size incompatible with the security policy). If it does not find valid certificates, the coworkers are excluded from the coworker list of the *.sdsx* file.

Support reference STORM-66291

The parameters in the Windows registry base that allow configuring the target directory that SD File must use to store decrypted *.sbox* files when it is called by other applications (Microsoft Outlook for example) are operational again. The values of these parameters were not properly applied in version 11.4.3.

The parameters in question are as follows:

- `ExeToCheck`
- `ExeTargetDirectory`
- `AllowOverwriteFile`
- `ExeActivate`

For more information about these parameters, refer to the *Administration guide* of SDS Enterprise version 10.1. As written in the *Migration guide*, they have been moved from the *sbox.ini* file to the registry base in version 11 but they still work the same way.

SDS Enterprise 11.4.3 fix

Agents SDS Enterprise

Support reference STORM-56695

When updating to version 11.4.2, the agent drivers did not update correctly due to a signature issue. This problem has been fixed with version 11.4.3.

Version 11.4.2 is no longer available. Version 11.4.3 includes the fixes of version 11.4.2.

SDS Enterprise 11.4.2 fixes

Stormshield Data Team

Support references STORM-58628 and STORM-59406

When the latest version of Microsoft Defender XDR M365 E5 was installed on the workstation, moving a file protected by Stormshield Data Team from a file server to an unprotected local folder of the computer caused a blue screen. This issue has been fixed.

Support reference STORM-48

Corrected an anomaly preventing Stormshield Data Team from encrypting files smaller than or equal to 4 KB.

Stormshield Data Connector

Support reference STORM-59113

Corrected an incompatibility between the SDS Enterprise agent and PowerShell 5 latest version. Installing Stormshield Data Connector component on workstations made PowerShell unusable.

For more information, refer to the Stormshield knowledge base.

New features and enhancements in SDS Enterprise 11.4.1

Stormshield Data Management Center (SDMC)

A new **Policies** > **Accounts** > **Connection** tab allows you to configure the behavior of the SDS Enterprise agent when:

- The screen saver activates,
- The Windows session is locked,
- The smart card or USB token is removed.

You can also configure these settings in the security policies file in *.json* format.

Find out more

SDS Enterprise agent

Virtual Disk

The Virtual Disk shortcut is now available on the **Properties** > **Configuration** tab of the SDS Enterprise agent. This shortcut provides access to the user's volumes.

Connection settings

In the SDS Enterprise agent properties, the **Screen saver** tab no longer exists in the **Connection** menu. The options for configuring the agent's behavior when the screen saver activates and Windows session is locked can now be set in SDMC.

SDS Enterprise 11.4 new features and enhancements

SDS Enterprise administration

Stopping *SBox.ini* configuration file support

To simplify SDS Enterprise deployment and administration, the settings found in the *SBox.ini* configuration file have been moved and this file is no longer required.

The configuration settings can now be found either in the security policy *.json* file or in the Windows registry. Some other parameters have been replaced with fixed values in the code or deleted.

Helpful hints:

- a migration tool is available on request,
- A migration guide is available on the Technical documentation site.

Find out more

Stormshield Data Management Center (SDMC)

Converting *.sbox* encrypted files to *.sdsx* format

To help you convert your encrypted files from the old *.sbox* format to the new, more secure *.sdsx* format, you can now configure automatic conversion of these files when the user opens them in the security policy. The operation is transparent for the user, and the *.sdsx* format means, among other things, that files do not need to be re-encrypted after use. You'll find these new options in the SDMC **Policies** > **Features** > **File** menu and in the *.json* configuration file settings.

Find out more

User keyring management

In the new **Keyring** tab of the **Policies** > **Accounts** menu, you can choose whether or not to display the tabs for managing user keyring encryption, signature, decryption and recovery keys.

Find out more

Agent SDS Enterprise

Custom SDS Enterprise icon on protected synchronized shared space folders

You can now add a registry key to customize the icon of synchronized workspace folders protected by the Stormshield Data Share feature, making them easy to identify. It allows you to replace the default Windows folder icon with a SDS Enterprise icon.

Find out more

SDS Enterprise 11.4 fixes

SDS Enterprise agent

Support reference STORM-52916

SDS Enterprise in SSO mode now starts correctly, even if a personal store certificate is incorrectly formatted.

Choice of recipients

Support reference STORM-51540

The recipient selection window now retrieves the correct status of the revocation list when a coworker is added to an encrypted file.

Stormshield Data Team

Support reference STORM-50534

Corrected an anomaly preventing a coworker from being added while their certificate is valid.

When the user moves files to a folder secured by Stormshield Data Team:

- If the certificate of a coworker with whom the folder is shared has an error (e.g. revoked, parent chain revoked or unavailable), then encryption is systematically performed **except** for the coworker in question.
- If the certificate of a coworker with whom the file is shared has a warning (e.g., expired, CRL expired or unavailable), then encryption will always take place, **including** for the coworker in question.

  Previously, in these same cases, the user could cancel the encryption action.

Stormshield Data Shredder

Support reference STORM-51107

SDS Enterprise now asks the user for confirmation before shredding the first file of a multiple file selection.

Stormshield Data Virtual Disk

Support reference STORM-11289

Corrected an anomaly preventing the disassembly of secured volumes.

SDS Enterprise 11.3 new features and enhancements

SDS Enterprise security policy

Automatic encryption and signing with Microsoft Purview

If your company uses the sensitivity label system offered by Microsoft Purview Information Protection, you can now declare these labels in the settings of the Mail feature of a security policy and associate them with an automatic agent action. When the user applies a label to a message, the agent checks that the label is present in the policy and triggers the corresponding security action: encrypt only the message, sign only the message, or a combination of both.

Find out more

Shared protection rules management

In the settings of the Share feature of a security policy, you can now require or prohibit the creation of shared rules when a user creates an automatic folder protection rule directly from their workstation. By default, the user has the choice to share or not share a rule when creating it.

Find out more

Automatic Windows encryption of temporary file decryption directory

In the File feature settings of a security policy, you can now enable automatic Windows encryption of the SDS Enterprise directory, called *Decrypted*, which allows *.sdsx* files to be temporarily stored when they are being modified by the user.

Find out more

SDS Encryption Portal

The SDS Encryption Portal portal, which lets you read and protect confidential documents in a web browser, now offers the option of using your own PKI solution, by selecting the "External PKI" mode when creating your organization's tenant. In this way, you use the user encryption keys already in use within the organization. In this mode, user authentication to the portal works exclusively with the Microsoft Entra ID identity management solution.

This mode also enables SDS Encryption Portal interoperability with SDS Enterprise. Documents encrypted via the web portal, in *.sdsx* format, can now be decrypted via the SDS Enterprise agent and vice versa.

The "External PKI" mode is currently available in Beta version. Contact your Stormshield sales representative if you would like to implement this solution.

For more information about SDS Encryption Portal, see the ***Administration and User Guide*** and Portal ***News***.

SDS Enterprise 11.3 fixes

Stormshield Data Team

Support reference STORM-6995

It is now possible to encrypt *.pdf* files in a Stormshield Data Team-secured folder when they are saved via the Microsoft Edge browser.

Searching for peers

Support reference STORM-12166

Fixed a display issue when searching for peers prior to an encryption operation.

SDS Enterprise 11.2.1 fixes

Stormshield Data Team

A *.zip* archive created in Windows Explorer from a sub-folder in a Stormshield Data Team-secured folder is now correctly encrypted.

Files placed in a folder secured by Stormshield Data Team and located on a network share are now correctly encrypted.

Support reference STORM-48

When McAfee antivirus is present, files smaller than 2 KB are now correctly encrypted by Stormshield Data Team.

Support reference STORM-50

The '~00' characters are no longer displayed in the names of certain files encrypted by Stormshield Data Team.

Stormshield Data Shredder

Support reference STORM-10612

You can now permanently delete the contents of the Windows recycle bin with Stormshield Data Shredder.

Coworker search

Support reference STORM-8943

In the **Select recipients** window, it is now possible to perform an LDAP search on email addresses and on the common name of coworkers at the same time.

Single Sign-On accounts (SSO)

Support reference STORM-8068

It is now possible to create an SSO user account if the Windows store contains expired certificates.

SDS Enterprise 11.2 new features and enhancements

WARNING BEFORE UPDATING THE AGENT
From SDS Enterprise version 11.1.1 onwards, the agent is now installed by default with a security policy.
As a consequence, if you already use a customized security policy in your environment, it will be replaced by the default policy when the agent is updated. It will be then necessary to deploy again your policy after the update.
You will not need to deploy again your customized policy during future updates of the agent from version 11.1.1 to a higher version.

SDS Enterprise agent

Sharing protection rules with the Stormshield Data Share feature

When you use the Stormshield Data Share feature to automatically protect folders synchronized with your collaborative workspaces, you can now share protection rules with your coworkers. Once the rule has been created for a folder, it automatically applies to all coworkers listed in the rule, and their files are protected when they are placed in the folder.

This feature is available in the agent interface via a checkbox in the coworker selection window, as well as via PowerShell commands usable with Stormshield Data Connector.

Find out more

Changing coworker access to a file or folder

The new **Edit access** menu allows users present in a protection rule to give or remove access to coworkers. The menu can be used on a folder, a file or several files at once.

Find out more

SDS Enterprise 11.2 fixes

Stormshield Data File

Support reference: STORM-3352

An error that could block the simultaneous encryption of two files has been corrected.

Stormshield Data Virtual Disk

Support reference: STORM-171

The speed of virtual disk creation has been increased.

Stormshield Data Team

Support reference: STORM-44

A processing error that could prevent the decryption of files with the Stormshield Data Team feature has been corrected.

Coworker search

Support reference: STORM-108

The search time in the LDAP directory via the add coworker window when encrypting files, folders or virtual disks has been improved.

SDS Enterprise 11.1.1 fix

WARNING BEFORE UPDATING THE AGENT
From SDS Enterprise version 11.1.1 onwards, the agent is now installed by default with a security policy.
As a consequence, if you already use a customized security policy in your environment, it will be replaced by the default policy when the agent is updated. It will be then necessary to deploy again your policy after the update.
You will not need to deploy again your customized policy during future updates of the agent from version 11.1.1 to a higher version.

Stormshield Data Virtual Disk

Support reference: STORM-154

A memory crash which would prevent the SDS Enterprise agent version 10 from updating to version 11 has been fixed.

SDS Enterprise 11.1 new features and enhancements

Stormshield Data Management Center (SDMC)

Managing keys for using the SDMC API

A new tab **API keys** is available in SDMC. It allows administrators with the **Manage API keys** permission to create API keys, valid for one year by default. API keys allows them to use the SDMC public API, particularly to access administration logs. Administrators can also permanently delete these keys.

Find out more

Accessing the administration logs via the SDMC API

It is now possible to access administrators connection logs through the SDMC API. Among other things, these logs indicate the connection mode used by the administrators (password or SAML).

You can still access the administration logs which were already available in the version 1 of SDMC through the API.

Security policy signature

The PS256 algorithm used by default at the time of signature of the policies. The previous RS256 signature algorithm remains functional with the signature utility and the SDS Enterprise agent.

Find out more

Managing users' keys and certificates in Password accounts

In the **Accounts > Creation** menu of a security policy, in the **Password account creation** section, the checkboxes for selecting the source of user keys and certificates have been replaced by a drop-down list.

Excluding folders from encryption with the Team feature

In the Team settings of a security policy, you can now specify a list of folders on which a user will not be able to create a Team security rule to automatically secure the folder. The list is recursive and automatically includes sub-folders.

Find out more

New secure deletion mode with the Shredder feature

In the Shredder advanced settings of a security policy, you can now configure the secure file deletion mode. This feature would write a series of characters in bytes in several rounds, replacing the file contents. SDMC now makes it possible to select the values of the successive rounds which replace the contents to be deleted.

Find out more

Importing security policies in SDMC

You can now import a *.json* format security policy in SDMC which has been previously exported from SDMC. However, LDAP directories and authorities certificates indicated in the policy are not imported.

Find out more

Advanced configuration of security policies

The following changes have been made to the JSON parameters of security policies:

- In the *accountPolicy - creation - automatic* section, the *encryptionKeyAuthorityId* and *signatureKeyAuthorityId* parameters are now optional.
- In the *accountPolicy - parameters- cryptography* section, the new optional parameter *keyEncryptionMethod* allows selecting the algorithm to use for encrypting the keys.
- In the *diskPolicy* section, the new parameter *encryptionAlgorithm* is used to select the algorithm to be used when encrypting secured virtual volumes.

SDS Enterprise agent

Updating a signatory policy

Users are now informed after the security policy signatory has been updated used with the SDS Enterprise agent.

Find out more

Encryption of volumes with the Virtual Disk functionality

The AES-XTS encryption algorithm can now be used to encrypt the secured virtual volumes generated with the SDS Enterprise agent.

Find out more

SDS Enterprise 11.1 fixes

Stormshield Data Mail

Support reference: STORM-56

An error resulting from an invalid policy or an expired signature certificate was displayed when opening each Outlook message. The problem was corrected by applying less restrictive permissions.

Support reference: STORM-57

A single click on **Send** is now enough to send a message when several LDAP servers are declared, and one of them is not functional.

SDS Enterprise agent

Support reference: STORM-15

The SDS Enterprise agent now operates properly when installed jointly with the Sentinel One software.

Stormshield Data Security Enterprise 11.0 features and enhancements

Stormshield Data Management Center (SDMC)

SDS Enterprise administration

SDS Enterprise can now be managed in the 11.3 web administration interface, which includes the following features:

- Centralized definition of LDAP directories so that they can be used when policies are created,
- Centralized definition of authority certificates, as well as data recovery certificates so that they can be used when policies are created,
- Configuration of security policies for SDS Enterprise agents, and then generating them in *.json* format. Through these policies, you can configure the use of SDS Enterprise features.
- Downloads of the latest version of the SDS Enterprise agent and the security policy signature tool. Signatures make it possible to guarantee the authenticity and integrity of policies,
- Access management for administrators of a corporate account: you can invite or delete administrators or modify their permissions.

You can also manually configure security policies directly in *.json* configuration files. These files enable the same level of configuration as Stormshield Data Authority Manager.

For more information on configuring policies and deploying agents in a pool, refer to the *Administration Guide* and the SDS Enterprise *Advanced configuration guide*.

SaaS mode

SDMC is in SaaS mode; new features and fixes are continuously provided, regardless of the SDS Enterprise agent version. Following the commercial release of SDS Enterprise version 11, a page listing the latest enhancements to 11.3 will be available on the Stormshield Technical Documentation website and continuously updated.

Authenticating administrators with SAML

You can now choose between two connection modes to access SDMC: the standard mode with an e-mail address and password, and SAML mode, which makes it possible to delegate the authentication of administrators to an identity provider.

Find out more

SDS Enterprise agent

Sign-On (SSO) connection

Through Windows SSO mode, SDS Enterprise users can now connect directly to the agent via their Windows sessions. User encryption and signing keys are stored in the Microsoft Certificate Manager.

Find out more

Automatic folder and sub-folder protection locally or in a synchronized space

The Stormshield Data Share feature allows users to enable automatic protection on a local folder or shared space. It also allows administrators to configure automatic protection of all or some synchronized shared spaces for all users. OneDrive, DropBox, SharePoint and Oodrive are supported.

The Stormshield Data Connector component, which drives the features of the SDS Enterprise solution through a PowerShell module or .NET APIs, now makes it possible to enable and disable the automatic protection of synchronized spaces via Stormshield Data Share.

Find out more

Updating security policies

When a security policy update is available on a distribution point, SDS Enterprise agents now apply it automatically when the user's workstation starts.

Find out more

Selecting coworkers

When using File, Team, Share and Virtual Disk, users can now select groups of users with whom they work. These groups can be selected from the local trusted address book or from an LDAP directory (Active Directory).

Improved agent pop-up menus

Menus that enable the use of the File, Team and Share features have been reorganized to facilitate their use.

SDS Enterprise Documentation

SDS Enterprise technical documentation has been restructured as follows:

Document	Contains
Release Notes	• New firewall behavior, • New features and enhancements, • Bug fixes, • Compatibility, • Explanations on usage.
Administration Guide	• Installing and uninstalling the solution, • Configuration and administration via SDMC, • Configuration of File, Team, Share, Mail and Virtual Disk features.
Advanced configuration guide	• Configuration and administration via a security policy's configuration file in *.json* format. • Configuration via the *SBox.ini* file and the advanced parameters of the registry base, • Configuration of File, Team, Share, Mail and Virtual Disk features.
Advanced user guide	• Advanced use of the File, Team, Share, Mail, Shredder, Sign and Virtual Disk features, intended for solution administrators.

Document	Contains
User guide	• Daily use of the File, Team, Share, Mail, Shredder, Sign and Virtual Disk features, intended for solution end users.
Stormshield Data Connector	• Configuration and use of Stormshield Data Connector.
Architecture and security guide	• Technical information regarding the confidentiality, integrity and availability of our users' data.

Information contained in former Stormshield Data File, Team, Mail, Shredder, Sign and Virtual Disk guides have been spread out among the administration guide, advanced configuration guide and advanced user guide.

Stormshield Data Security Enterprise 11.0 fixes

Stormshield Data Mail

Support reference: 208745CW

A message's security can now be disabled even when the message does not contain the sender's SMTP address.

Support reference: 199751CW

When sending secure messages, the issue with an error indicating that the message was too large in some cases has been fixed.

Contact

To contact our Stormshield Technical Assistance Center (TAC):

- https://mystormshield.eu/
  All requests to technical support must be submitted through the incident manager in the private-access area https://mystormshield.eu, under Technical support > Manage cases.
- +33 (0) 9 69 329 129
  In order for us to provide high-quality service, you are advised to use this communication method only to follow up on incidents that have been created earlier on https://mystormshield.eu.



STORMSHIELD

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

Copyright © Stormshield 2026. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.