



STORMSHIELD



**STORMSHIELD DATA SECURITY
ENTERPRISE**

RELEASE NOTES

Version 11

Document last updated: November 2, 2023

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



Table of contents

New firewall behavior	3
Stormshield Data Security Enterprise 11.0 features and enhancements	4
Stormshield Data Security Enterprise 11.0 fixes	7
Compatibility	8
Known issues	9
Explanations on usage	10
Documentation resources	14
Downloading this version	15
Going to your MyStormshield personal area	15
Checking the integrity of the binary files	15
Contact	16

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 firewall behavior

Changes introduced in version 11.0

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

The cmdlet or .NET APIs that enable log in, log out, locking or unlocking on the SDS Enterprise account, which are available via the Connector component, are now disabled when users log in to their SDS Enterprise accounts in SSO mode.

The SDS Enterprise agent in version 11.0 is available only on Microsoft Windows 64-bit workstations.



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 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

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 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. Users' encryption and signature keys are saved in the Microsoft certificate manager or on TPM chips.



[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 co-workers

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
Version release notes	<ul style="list-style-type: none">• New firewall behavior,• New features and enhancements,• Bug fixes,• Compatibility,• Explanations on usage.
Administration Guide	<ul style="list-style-type: none">• Installing and uninstalling the solution,• Configuration and administration via SDMC,• Configuration of File, Team, Share, Mail and Virtual Disk features.
Advanced configuration guide	<ul style="list-style-type: none">• Configuration and administration via a security policy's configuration file in <i>json</i> format,• Configuration via the <i>SBox.ini</i> file and the advanced parameters of the registry base,• Configuration of File, Team, Share, Mail and Virtual Disk features.
Advanced user guide	<ul style="list-style-type: none">• Advanced use of the File, Team, Share, Mail, Shredder, Sign and Virtual Disk features, intended for solution administrators.



Document	Contains
User guide	<ul style="list-style-type: none">• Daily use of the File, Team, Share, Mail, Shredder, Sign and Virtual Disk features, intended for solution end users.
Stormshield Data Connector	<ul style="list-style-type: none">• Configuration and use of Stormshield Data Connector.
Architecture and security guide	<ul style="list-style-type: none">• 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

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

Support reference: 208745CW

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

Support reference: 199751CW



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

Oodrive WebSynchro
SharePoint Online/Office 365
OneDrive Enterprise/for Business in Office 365
SharePoint 2016 (on-premises)
Dropbox and Dropbox Business



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

In SDMC, public key infrastructures (PKIs) cannot be managed, unlike in 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.

Accounts can only be created on a TPM chip with RSA keys that do not exceed 2048 bits. This limitation also applies to SSO accounts with keys that are stored on a TPM chip.

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.). All protocols are properly managed.

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

Stormshield Data File

SDS Enterprise currently does not support Microsoft OneNote files.

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.

In the event a protected file in the process of being edited cannot be backed up (e.g. if the file has been deleted or renamed in the meantime, or the file is located on a shared network and the connection has been shut down), the user will need to modify the backup location or rename his file.

Files protected by SDS Enterprise and stored on a shared network, while in the process of being modified by an authorized user, can still be simultaneously modified by another authorized user.

The SDSX format strictly does not support certificate RSA keys smaller than 2048 bits.

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

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 file protection is enabled on a folder, and you are using "Save as" on allowed applications, you must shut down the application that is attempting to save, so that the file can be seen 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.

To ensure that files moved to a Dropbox synchronized space are automatically protected, use the drag and drop or copy and paste functions. If you use the **Move to Dropbox** pop-up menu on a file, it will not be protected.

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 does not appear on a protected folder, check the registry base, under "Ordinateur\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers", that the following keys have been placed 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.

Stormshield Data Mail

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 correction timeout may prevent access to the disk or changes made to the disk may not be saved.

Stormshield Data Team

Stormshield Data Team is not compatible with the backup tool Veeam. 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.

Stormshield Data Team cannot support synchronized directories such as SharePoint, Dropbox, Office 365, etc. and thus cannot encrypt them. We recommend that you exclude these directories from the folders analyzed by Stormshield Data Team by using the **Folder exclusion** advanced parameter found in the configuration of the Team feature in the SDMC administration console.



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
- Stormshield Data Security Enterprise - Architecture and security guide
- Stormshield Data Authority Manager - User Guide
- Stormshield Data Connector - User Guide



Downloading this version

Going to your MyStormshield personal area

You need to go to your [MyStormshield](#) personal area in order to download the 11.0 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**.



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 2023. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.