STORMSHIELD

STORMSHIELD DATA SECURITY FOR CLOUD & MOBILITY

RELEASE NOTES

Version 3.3

Document last update: March 15, 2021

Reference: sds-en-sds_for_cloud-release_notes-v3.3sp1

Table of contents

In the documentation, Stormshield Data Security for Cloud & Mobility is referred to in its short form: SDS for C&M, and the Stormshield Data Management Center in the form SDMC.

This document is not exhaustive and more fixes may have been included in this version.

SDS for C&M 3.3 SP1 bug fixes

Support reference: 175779CW

In SharePoint shared spaces, the SDS for C&M LDAP search would fail if some users did not have email addresses. This problem has been fixed: users without email addresses are now displayed in the interface with the "Invalid email " error, and other users can be properly searched in the LDAP directory.

Compatibility

The following platforms are compatible with the SDS for C&M 3.3 client:

Web browsers (server)

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

Operating systems (client)

Microsoft Windows	Windows 10, 1909 and 2004 builds
macOS	Mojave 10.14 and Catalina 10.15

Mobile devices (client)

Supported devices

The SDS for C&M application is supported on the following systems:

Android	Version 10
iOS	Version 13

The tests performed by Stormshield show that SDS for C&M is compatible with the following device models:

iPhone X	13.5.1
iPad 2018	13.5.1
iPad Mini 4	13.5.1
iPhone 8	13.5.1
Samsung Galaxy S9	10.0.0

Google Pixel 3a	10.0.0

The above table only represents the tests actually performed; SDS for C&M can also be deployed and used with other models.

Shared spaces for sharing files

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

Synchronizers for automatic file protection

Google Drive Backup and Sync (Google Drive File Stream is not supported)
Oodrive WebSynchro
SharePoint Online/Office 365
OneDrive Entreprise/for Business in Office 365
SharePoint 2016 (on-premises)
Dropbox and Dropbox Business

Recommendations

We advise you to apply the following recommendations for optimum use of the SDS for C&M 3.3 solution, as they are directly linked to the operating context in which the SDS for C&M solution evolves.

Migrating SDS for C&M 3.2 to SDS for C&M 3.3

Unlike version 3.2, version 3.3 assigns a single password for all devices (workstations and mobile devices) to SDS for C&M accounts. User accounts must be migrated from your SDS for C&M client before this feature can be enabled. Mobile devices cannot be used for migration operations.

With SDS Enterprise

1. During the initial connection to SDS for C&M, the SDS Enterprise connection window appears. Enter your SDS Enterprise login and password.
2. In the migration window, enter the password to your SDS for C&M account, and click on **Next**. The migration process begins.
3. Log in to your SDS for C&M account with the password entered earlier.

Without SDS Enterprise

1. Log in to SDS for C&M with the credentials for your local account.
2. In the migration window, enter a new password to your SDS for C&M account, and click on **Next**.
   The migration process begins.
3. Log in to your SDS for C&M account with the password entered earlier.

Only one device can be migrated for each user account. If you have SDS for C&M accounts on other workstations, you need to delete them manually. To do so, delete the folder of the user in *%localappdata%\Stormshield\Stormshield Data Security\Users* .

SDS for C&M accounts are automatically deleted on mobile devices when the SDS for C&M application is upgraded. Protected files will be kept.

Particular case: users who have an SDS for C&M account but have never used the application from their workstations cannot be migrated. The administrator must delete such users from the SDMC web administration interface. These users will then need to manually delete their account folders in *%localappdata%\Stormshield\Stormshield Data Security\Users*

As soon as the migration operation is complete, and all secondary accounts have been deleted, you can log in with your single password from any of your devices.

Using shared spaces

To modify shared files in online shared spaces, we recommend that users work in their synchronized Microsoft OneDrive for Business or Microsoft SharePoint Online work spaces. As such, in the event of simultaneous access to the same file, the synchronizer will resolve any potential conflicts.

Sharing files in OneDrive for Business

Whenever you share files in a Onedrive for Business synchronized space, you need to select sharing for **Specific persons**. This would allow SDS for C&M to retrieve the list of users who have access to the link, and to automatically suggest this list in the column of authorized users.

OneDrive and the Microsoft Office Suite

For optimum automatic protection of Office files in a OneDrive space, unselect the **Use Office 2016 to sync Office files that I open** option from the **Office** tab in the synchronizer properties.

SDS for C&M application on Android

To avoid issues during the creation/retrieval of your account or connection, set the location to **High accuracy**.

Padlock icon on protected folders

If you are installing Office (from version 2013 onwards) and OneDrive together before you install SDS for C&M, the padlock icon will not be visible on protected folders.

There are two ways to make these icons appear:

- Install Office without OneDrive. For more information, refer to the section "ExcludeApp element" at this page.
- As an administrator, add one or several spaces before the name of the following registry key so that it will be placed above the existing keys in the tree: HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/Explorer/ShellIconOverlayIdentifiers/PhoenixOverlayIconHandler. Restart Explorer in order to apply the change.

Google Drive Backup and Sync

SDS for C&M cannot automatically protect files configured to be continuously backed up by Google. To protect such a file, first make a copy to a folder which is not backed up, then move this copy to your Google Drive. Open your Google Drive synchronizer Preferences to identify the folders that are backed up by Google.

Updating clients

Update clients on a regular basis to take advantage of all upgrades and bug fixes.

Before updating a macOS Client, first close SDS for C&M.

Known issues

The up-to-date list of the known issues related to this version of SDS for C&M is available on the Stormshield Knowledge Base (English only).

SDS for C&M on Windows

SDS for C&M on macOS

SDS for C&M Encryption Portal

SDS for C&M on Android

SDS for C&M on iOS

To connect to the Knowledge Base, use your MyStormshield customer area identifiers.

Explanations on usage

Desktop

If SDS for C&M is used with SDS Enterprise 9.2.5, folders will not be automatically protected. You are strongly advised against installing this version of SDS Enterprise. Version 9.2.5 SP1 fixes this issue.

When automatic file protection is enabled, the "Save as" function cannot be used in the following cases:

- When saving Microsoft Office files in a synchronized space such as OneDrive or SharePoint.
- When saving Libre Office files in any type of synchronized space.

After a certificate renewal, the new certificate is not automatically taken into account when a protected file is edited. The wizard must be run again to manage access to the file and apply the new certificate.

During Protect and Share operations, or Share operations in a Dropbox space, the link may lead to a page that replaces quotes with the character string *"*. This has no impact on the actual name of the file.

SDS for C&M may suddenly shut down during keyboard navigation in the folder view of shared spaces. This is due to a known issue in the Qt framework, for which no fix has been scheduled. For more information, see the QT blog and the QT bug reports.

The use of proxies in NTLM authentication between a SDS for C&M macOS client and the SDMC server is not supported. Only Basic authentication is possible via web proxy or secure web proxy.

In External key management mode, the name of the company does not appear in the protection or sharing wizard.

Different SDS for C&M users cannot log in to the same session on a client workstation.

SDS for C&M currently does not support Microsoft OneNote files.

When a file's protection is removed, Windows privileges applied to the file will be restricted to the session user only.

In order to modify access to a file, it needs to be closed first.

If users' e-mail addresses contain accented characters, their user accounts will not be created properly.

SDS for C&M does not support the *file* protocol for automatic proxy configuration by script file (local file on the machine or available on a shared network).

SDS for C&M does not support resolutions lower than 1024x768.

The characters " # % * : < > ? / \ | [ ] are forbidden in file and folder names.

File and folder names may not begin or end with a period.

When a computer is connected to the Internet through a public WiFi network, it is possible that any redirection between the authentication page on the WiFi network and the authentication page on the shared space may alter the request and display an error on the platform's authentication page. You then need to start the sharing operation again.

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.

Several instances of the same protected Access database (*.accdb* file) cannot be opened simultaneously if the active content has not be enabled.

SDS for C&M does not manage files' external resources (for example a link in a file to an external image).

Files protected by SDS for C&M 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.

SDS for C&M strictly does not support certificate RSA keys smaller than 1024 bits.

When you protect a locked file locally on macOS, the file is protected but the unprotected version of the file is also kept.

If you use SDS for C&M with SDS Enterprise, you cannot log in to SDS for C&M using several accounts within the same Windows session.

Windows desktop only

Windows 10 operating systems cannot be upgraded to a higher version of the system via the upgrade wizard; you must use Windows Update for this upgrade.

Automatic protection cannot be enabled on folders located on a USB drive or on a shared network.

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.

SDS for C&M automatic folder protection cannot apply to folders already protected by Stormshield Data Team.

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.

Temporary decryption folders cannot be locally protected with the Stormshield Data Team module in SDS Enterprise.

If automatic file protection has been enabled in synchronized spaces, the following restriction applies:

The file path from the root of the synchronized folder must not exceed 172 characters. If this is the case, the file will not be protected and will no longer be accessible.

SDS for C&M does not allow the display to be zoomed to 200% (and higher) on Microsoft Windows systems.

SDS for C&M does not take into account the frequency of password or PIN requests, configured in the SDS Enterprise user's account.

If needed, the SDS Enterprise recovery account must be associated with all Stormshield Data Security products.

In Microsoft Windows 10, file icons which open with a "Tile" application, such as images or PDF files, are displayed in white when the files are shared on a shared space.

After SDS for C&M has been uninstalled, its icon may remain in the status bar. Restart your workstation so that it no longer appears.

On Windows Surface tablets with Office 365 installed, silent installations (msiexec /q) may fail on error. In this case, launch a manual installation.

---

macOS desktop only

In some cases, the SDS for C&M pop-up menu does not appear in the Finder. To resolve the issue, enable the SDS for C&M Finder extension in the System Preferences, then restart the workstation.

On macOS Mojave 10.14, the SDS for C&M icon is not always displayed correctly in the Dock.

On macOS Mojave 10.14, after the workstation has been restarted, an explorer will display the executable files on SDS for C&M. To work around this issue, in the Dock settings, unselect **Show recent applications in Dock**. This parameter applies to all applications. For more information, refer to the Stormshield Knowledge Base (authentication required).

Application

If you use SDS for C&M Encryption Portal with a Microsoft Edge browser, files cannot be dragged and dropped in order to be protected or decrypted. This restriction occurs only with Edge. Double-click on the frame at the center of the page to select your file.

With SDS for C&M installed in work profile mode via the MobileIron EMM, it is not possible to use some applications in the personal space. For example, you must manage OneDrive and DropBox applications from the EMM for the authentication file import function to be available.

Android application only

Shared screen mode is not supported.

The characters + / \ ? are prohibited in file names.

The display of SDS for C&M screens may be altered if the font size of Android menus is increased.

---

iOS application only

On iOS13 and iPadOS13 with a Chrome browser, the SDS for C&M Encryption Portal page that allows you to download the decrypted file or select another file to protect does not appear. This issue occurs only with Chrome. To select another document, use the **Previous** button in the browser or open the portal in another compatible browser.

In iOS, once you log in to SDS for C&M, the following error message may appear: *You need an internet connection to continue. Please check your connection settings.*
This error occurs if at least on country has been excluded in SDS for C&M's geographical settings. The application must then check the device's GPS position, which would require access to an online Apple service.

Documentation resources

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

Release Notes

- Stormshield Data Security for Cloud & Mobility - Client Release Notes (PDF)
- Stormshield Data Security for Cloud & Mobility - Server enhancements (HTML)
- Stormshield Data Security for Cloud & Mobility - Encryption Portal enhancements (HTML)

Guides

- Stormshield Data Security for Cloud & Mobility - Administration Guide (PDF)
- Stormshield Data Security for Cloud & Mobility - User Guide for the client (HTML)
- SDS for C&M Encryption Portal - User Guide (PDF)
- Stormshield Data Security for Cloud & Mobility - Architecture and Security (PDF)

Video

- Tutorials Stormshield Data Security for Cloud & Mobility, available on YouTube

Downloading this version

Going to your MyStormshield personal area

You need to go to your MyStormshield personal area in order to download the 3.3 SP1 version of Stormshield Data Security for Cloud & Mobility:

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 for Cloud & Mobility 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 for C&M 3.x

In this section, you will find the new features from previous versions of Stormshield Data Security for Cloud & Mobility 3.x.

3.3	New features	Bug fixes
3.2	New features	Bug fixes
3.1	New features	Bug fixes
3.0	New features	Bug fixes

SDS for C&M 3.3 new features

Desktop

Single SDS for C&M password for all devices

Users now only need a single password to access their SDS for C&M accounts from all of their devices. User accounts must be migrated before this feature can be enabled.

Collaboration with external users

External users who do not have the SDS for C&M client on their computers can now be added during operations to protect, share or modify access. The interface in which users are selected makes it possible to enter their e-mail addresses, and choose whether to grant them permissions to modify content and access to files.
The administrator must enable this feature beforehand in the security policy.

Decrypting files protected by external users

Files that were protected by external users can now be decrypted without the need to go through the SDS for C&M Encryption Portal.

Installing the SDS for C&M client

The installation program of the SDS for C&M client no longer offers the choice between an installation for the current user and an installation for all users. The client is always installed for all users now.

Expiry of the SDS for C&M password

When their passwords expire, users are prompted to change them when they next log in to the SDS for C&M client. A link will redirect them to the dedicated SDS for C&M Encryption Portal page on their default browser.

Error details

When errors occur during *Grant access*, *Restrict access* and *Remove access* operations, the last window shows a summary of the errors, and a **Details** button makes it possible to obtain additional information.

Suggesting co-workers for SharePoint

During *Protect and Share* operations in a SharePoint shared space, users who have access to the shared space appear by default in the list of users authorized to edit the file.

Automatic protection driver

Microsoft has assigned an altitude of 141255 to the Stormshield SDS for C&M automatic protection driver.

Mobile application

Single SDS for C&M password for all devices

Users now only need a single password to access their SDS for C&M accounts from all of their devices. To create an account, a link in the application now redirects users to the SDS for C&M Encryption Portal.

Changing passwords

The button to change a password now redirects the user to the dedicated SDS for C&M Encryption Portal page.

Expiry of the SDS for C&M password

When their passwords expire, users are prompted to change them when they next log in to SDS for C&M. A link will redirect them to the dedicated SDS for C&M Encryption Portal page.

SDS for C&M 3.3 bug fixes

The SDS for C&M client now sends to the server any logs regarding the application of the policy.

When SDS for C&M is opened on macOS via Spotlight, the icon in the menu bar is now correctly displayed.

On the iOS application, icons of Microsoft Word files now correctly show the name of the .doc or .docx extension.

SDS for C&M 3.2 new features

SDS for C&M now includes *Agentless Encryption* technology, which makes it possible to protect and decrypt confidential files directly in a browser. Administrators therefore no longer need to deploy or maintain SDS for C&M clients. SDS for C&M clients also no longer need to be installed on the workstations of external users who receive confidential information. For more information, refer to the SDS for C&M Encryption Portal User Guide.

Collaboration with external users

SDS for C&M makes it possible to share protected files with external users who do not have the SDS for C&M client on their computers or mobile devices. In the **Grant access** menu in the SDS for C&M client, the user enters the recipients' e-mail addresses, then grants them access to the files.

On the recipients' side, they authenticate on SDS for C&M Encryption Portal through their SDS for C&M accounts or by using a code that they received via e-mail if they do not have accounts. They can then upload the protected file to the web page suggested by SDS for C&M Encryption Portal, which decrypts and saves it directly on the workstation.

Learn more

SDS for C&M 3.2 bug fixes

Support references: 165348CW

When a file is protected via SDS for C&M with SDS Enterprise, the error message that appears when the encryption key cannot be found is now clear and makes it easy to debug the issue.

The pop-up menu and its items can now be accessed again via the SDS for C&M taskbar when the connection window appears.

SDS for C&M client 3.1 new features

Managing access to a selection of several files

After your files have been protected, you may modify the list of users allowed to access them. SDS for C&M now allows you to apply the following actions to several files at the same time, in particular the entire contents of folders:

- Add authorized users or grant additional privileges to authorized users.
- Remove authorized users.

This feature is useful, for example, when a coworker leaves the company or when new employees join the company. In a single operation, you will be able to grant or remove access to a user's confidential files.

Learn more

Smart card for authentication on Android and iOS

SDS for C&M is no longer compatible with smart card readers as Gemalto no longer supports Stormshield's built-in library.

The SDMC server's administration interface continues to mention smart cards, but these items will be removed in future versions.

SDS for C&M client 3.1 bug fixes

Support references: 162920CW

The **Merge contextual menus in the file explorer** setting is back in working order. Enabling this setting will group both SDS for C&M and SDS Enterprise pop-up menus under a single header in Windows Explorer.

Support references: 163144CW

In External key management mode, user accounts are now properly created whenever the user whitelist has been declared via the API. Devices will no longer be enrolled as long as their user accounts have not been fully created.

Support references: 163690CW

Whenever files are shared via SDS for C&M, Office 365 shared spaces with URIs that contain the space character (%20) can now be accessed.

SDS for C&M client 3.0 new features

Workstations

Helpdesk and Recovery user

The first user to be registered on the SDMC server will be identified as the Helpdesk and Recovery user and is entitled to a customized account.

Stormshield Data Security Office add-on

A Stormshield Data Security Office add-on makes it possible to protect and share files in a shared space directly from Microsoft Word, Excel or PowerPoint.

Find out more

Deleting users

Users can now be deleted from personal address books, which contain users with whom protected data has been exchanged, and users that have been added manually from an *.sdsi* file.

Automatic folder protection

When a folder is automatically protected, the protection now applies to its entire contents, even documents that have already been protected.

However, files that are already protected and for which you are not allowed to manage access will not be modified.

Connecting from a new device

Whenever a user signs in from a new device, he will receive an email informing him about it. The user can therefore ensure that all connections to his account are legitimate.

Mobile applications

Searching for users

In built-in key management mode in Android, you can now access the list of users registered on the SDMC server from your mobile device. This allows you to easily select users for whom you wish to protect or share documents.

SDS for C&M client 3.0 bug fixes

Support references: 161751CW

If the client workstation has not been restarted for several weeks, SDS for C&M would stop running during protection, sharing or logging operations. This issue, which relates to the locking of the Windows session, has been fixed.

Support references: 161366CW

Issues during the integration of SDS for C&M with single sign-on (SSO) authentication tools have 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.