GUIDE

SDS ENCRYPTION PORTAL

ADMINISTRATION USER GUIDE

Document last updated: April 02, 2025

Reference: sds-en-sdse-encryption_portal_guide

Table of contents

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

1. Getting started

Welcome to the SDS Encryption Portal *Administration user guide*.

This guide is intended for SDS Encryption Portal administrators.

SDS Encryption Portal allows users in your organization to protect (encrypt) and download (decrypt) confidential documents using a web browser. They can exchange these documents within their organization or with external partners, thus guaranteeing the protection of sensitive data. SDS Encryption Portal can be accessed from workstations or mobile devices.

To use the portal, you must ask Stormshield to create a tenant for your organization.

Your tenant members can then protect documents not only for themselves, but also for anyone else, whether a Stormshield tenant member or not.

NOTE
A user who does not have a tenant, and therefore no encryption keys, can only use SDS Encryption Portal to decrypt documents that have been encrypted for him/her. In this case, SDS Encryption Portal is free.

The portal security administrator holds the helpdesk and recovery roles. He/she can also delegate these roles to other users.

1.1 Usage modes

SDS Encryption Portal offers two modes:

- **"External PKI" mode.** This mode lets you use users' existing encryption keys if your organization has a PKI solution. In this mode, user authentication to the portal works exclusively with the Microsoft Entra ID identity management solution.
  This mode is currently available as a Beta version. Contact your Stormshield sales representative if you would like to implement this solution.

  This mode is compatible with the Stormshield Data Security solution.

- **"Internal PKI" mode.** If your organization does not have a PKI solution for generating encryption keys for your users, this mode enables keys to be generated automatically when users use the portal for the first time. The keys remain stored in the portal database and cannot be retrieved. In this mode, users log in to the portal using their email address and a specific password.

  This mode is not compatible with the Stormshield Data Security solution.

For more information on these modes, see Selecting SDS Encryption Portal usage mode.

You choose how to use it when Stormshield creates the tenant for your organization. Once the tenant has been created, it is not possible to change the usage mode.

1.2 Requirements for using SDS Encryption Portal

- Stormshield must first create a tenant for your organization, by configuring the “External PKI” or “Internal PKI” mode.
- You need a web browser, an Internet connection and an e-mail address. The browser must support TLS 1.2 or higher.
- Traffic to *https://sds.stormshieldcs.eu* must be allowed.
- JavaScript must be allowed to run for the server *https://sds.stormshieldcs.eu* or the domain *stormshieldcs.eu*.
- The size of the documents to be protected must not exceed 20 MB. To view or protect larger documents, users need the Stormshield Data Security solution.
- You will be receiving e-mails from the address *noreply@stormshieldcs.eu*. Allow this address in your mail account so that these e-mails will not be considered spam.

2. Selecting SDS Encryption Portal usage mode

Please read the following sections to understand the difference between the two SDS Encryption Portal usage modes.

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

2.1 Understanding "external PKI" mode

This mode is recommended for organizations that use a PKI solution to generate their encryption keys. SDS Encryption Portal can then use existing user keys.

2.1.1 Features

"External PKI" mode has the following features:

- Users log in to the portal via the Microsoft Entra ID solution,
- You use the encryption keys generated by your PKI and already in use in the organization. Users import them into the portal to encrypt and decrypt documents for themselves or for other users of the same tenant.
- Tenant users can share encrypted documents with external users, i.e. those outside their tenant, using keys generated on the fly.
- Interoperability with the Stormshield Data Security solution is ensured by the use of the same encryption keys: documents encrypted via the portal, in *.sdsx* format, can be decrypted via the Stormshield Data Security agent, and vice versa,

2.1.2 Requirements

- You must have the Microsoft Entra ID identity management solution,
- You must have a PKI solution within your organization.

2.1.3 Operation

Once the tenant has been created, users log on to SDS Encryption Portal via Microsoft Entra ID, using their usual login and password. When they log in for the first time, we recommend that they import their private key/certificate pair into the portal in *.p12* format, so that they can use their existing keys. The private key is securely stored in the "IndexedDB" section of the Web browser, and the certificate is published in the tenant database.

Once the keys have been imported, they are used for encryption and decryption operations carried out on the portal by users of the same tenant. The same files can be encrypted or decrypted either from SDS Encryption Portal or from Stormshield Data Security.

Users can also encrypt for external recipients, i.e. those belonging to a tenant other than their own or to no tenant at all, thanks to a system of on-the-fly generation of specific public keys.

To use SDS Encryption Portal in "External PKI" mode, see to the following sections:

- Logging in to SDS Encryption Portal
- Importing encryption keys
- Protecting a file
- Reading protected files

2.2 Understanding “Internal PKI” mode

This mode is recommended for organizations that do not use encryption keys provided by a PKI solution.

2.2.1 Features

"Internal PKI" mode has the following features:

- Users log in to the portal with their email address and a specific password,
- First-time key generation and use are transparent to users,
- The keys enable them to encrypt and decrypt documents for themselves or for other users of the same tenant,
- As the encryption keys are stored by the portal, users can use it from any device, browser or network,
- Tenant users can share encrypted documents with external users, i.e. those outside their tenant, using keys generated on the fly. These keys are also stored by the portal.

2.2.2 Operation

Each user member of a tenant must have an account on the portal. For more information, see Create user accounts.

The first time each user logs on to the portal, their private and public encryption keys are automatically generated and stored in the portal database.

The keys are then used for encryption and decryption operations performed on the portal by users.

Users can also encrypt for external recipients, i.e. those belonging to a tenant other than their own or to no tenant at all, thanks to a system of on-the-fly generation of specific public keys.

To use in SDS Encryption Portal “Internal PKI” mode, see the following sections:

- Creating the security administrator account
- Create user accounts
- Logging in to SDS Encryption Portal
- Protecting a file
- Reading protected files

3. Creating a tenant for your organization

SDS Encryption Portal is a cloud service hosted by Stormshield.

Stormshield creates a tenant for each of the organizations using the portal in order to reserve a secure space for users of the same organization. This tenant is configured according to the needs of security administrators and users.

Contact Stormshield to create a tenant for your organization.

The following information is required when creating your tenant:

Identification of the organization	• Name • Business type • Size • Address • Additional address (optional) • Country • State/Province/Region (optional) • Zip code • City
Usage mode	Choose the portal usage mode you wish to set up: "Internal PKI" mode or "External PKI" mode. For more information on usage modes, see Selecting SDS Encryption Portal usage mode. This choice cannot be changed afterwards. If in doubt, consult Stormshield.
Contact information	If you choose “External PKI” mode, you must provide Stormshield with contact information when creating the tenant. Your Stormshield sales representative will give you the details of the information to be provided.
Sharing documents with external users	You must also tell Stormshield whether you want your users to be able to share encrypted documents with external users, i.e. those belonging to another tenant or who do not have a tenant.

4. Creating the security administrator account

WARNING
This section applies to the “Internal PKI” usage mode only.
In “External PKI” mode, the recovery system is provided by your PKI solution and the helpdesk (lost password) is provided by your identity management solution.

In SDS Encryption Portal, the first user account created becomes a helpdesk and recovery account, and its owner is the security administrator. This account is essential for proper solution operation and security and cannot be deleted.

The roles of the security administrator are the following:

- **Helpdesk:** assigns a new password to users who have forgotten their passwords or if password confidentiality has been compromised,
- **Recovery**: Provides one user with access to all the protected documents of another user, in case the latter leaves the organization without decrypting their data, for example.

To create the first user account, see Creating an individual user account.

For more information, see the Helpdesk and recovery section of the *Architecture and Security* guide.

The security administrator can also delegate these roles to other users. For further information, see Managing users.

NOTE
If the security administrator is also a user of the portal, they must create an account with an email address different from the administrator account to use it.

5. Create user accounts

WARNING
This section applies to the “Internal PKI” usage mode only.

There are two ways to create user accounts on the portal. You can use the Stormshield Data Management Center public API (SDMC) to create your own user accounts. Or each user can create their own account by going to the portal.

5.1 Creating accounts via the public API

The SDMC public API allows you to create a list of predefined users:

- Use the route https://sds.stormshieldcs.eu/doc/api/#operation/createUsers to enter the email address of the users. Each user will then receive an email asking them to activate their account on the portal. If the email is not in their inbox, they should check their junk mail. The confirmation link expires after 48 hours.

5.2 Creating an individual account

Inform your users of the following procedure:

1. Go to SDS Encryption Portal and click on **Create account**.
2. Enter your first and last names and work e-mail address, then accept the conditions of use and click on **Next**.
3. In the **Password** window, enter and confirm your password, which must meet the given criteria, then click on **Next**.
4. You will receive an e-mail at the e-mail address that you have specified. Check your mailbox to confirm your email address and activate your SDS Encryption Portal account. If you do not see such an e-mail in your inbox, check your spam folder. The confirmation link expires within 48 hours, but you can always request a new one from your administrator if necessary.
5. Once you have created your account, log in to SDS Encryption Portal. You must log in at least once so that other users can share protected files with you.

6. Logging in to SDS Encryption Portal

Depending on the user's situation, the login procedure differs.

6.1 User login in "External PKI" mode

If you have chosen "External PKI" mode, your users log on to the portal via the Microsoft Entra ID solution, with their usual credentials. Inform your users of the following procedure:

1. Go to the SDS Encryption Portal.
2. Enter your email address and click on **Next**.
3. Click on **Sign in with Google**.
   The Microsoft login window opens.
4. If necessary, re-enter your email address, then enter your password and click on **Sign in**.

You can now Reading protected files or Protecting a file.

6.2 User login in "Internal PKI" mode

If you have chosen the "Internal PKI" mode, your users log in with their email address and password specific to SDS Encryption Portal. Inform your users of the following procedure:

1. Go to the SDS Encryption Portal.
2. Enter your email address and click on **Next**.
3. Enter your password and click on **Sign in**.

You can now Reading protected files or Protecting a file.

6.3 External user keys

When SDS Encryption Portal users protect a document for external recipients who do not have an account on the portal, they must follow the procedure below to view the document:

1. Go to the SDS Encryption Portal.
2. Enter your e-mail address and click on **Next** to obtain your one-time access code.
3. Check your e-mails. You should have received an e-mail from Stormshield (*noreply@stormshieldcs.eu*) containing the code. If you do not see such an e-mail in your inbox, check your spam folder. Click on **Enter code**.
4. Enter the code in the relevant field, then click on **Sign in**.
   The file selection page appears.
   The code can only be used once, and is valid for two hours. If your code has expired, request a new code by repeating the procedure from step 2. Ensure that you enter the latest code received, because the latest code generated renders all previous codes invalid.
5. Once you are logged into SDS Encryption Portal, you can Reading protected files.

External users who do not have an account on SDS Encryption Portal cannot protect a document.

7. Importing encryption keys

WARNING
This section applies to the “External PKI” usage mode only.

If you use a PKI solution, SDS Encryption Portal allows you to use the keys generated by your solution for encryption and decryption operations on the portal, between users of the same tenant.

When users first log on to SDS Encryption Portal, they can import their private key/certificate pair in *.p12* format.

If your organization also uses the Stormshield Data Security solution, using the same keys for SDS Encryption Portal and for Stormshield Data Security ensures interoperability between the two solutions. The same files can be encrypted or decrypted either from SDS Encryption Portal or from Stormshield Data Security.

To import the keys into the portal, instruct your users as follows:

1. Go to SDS Encryption Portal and log in.
2. Click on  in the upper right corner, and select **Import a .p12 file**.
   The *.p12* file must contain:
   - a single private key and certificate,
   - The attribute E corresponding to the user's e-mail address.
3. Import the file and enter its password.
   The private key is securely stored in the “IndexedDB” section of the Web browser, and the certificate is published in the tenant database.

The following principles must be observed:

- If a user does not import their encryption keys the first time they log on to the portal, keys are generated on the fly and stored by the portal. In this case, interoperability with the Stormshield Data Security solution is not possible. If you ultimately want the user to use their own encryption keys, please contact your Stormshield sales representative.
- If a user wants to log on to the portal from another browser or device, they will need to import their encryption keys again.
- If the private key or certificate is changed, the user can re-import their keys by following the same procedure. The new *.p12* file replaces the previous one.
- Once a user has imported their encryption keys into the portal via a browser, if a different user uses the same browser to logo on to the portal, the private key stored by the browser is automatically deleted. The new user can then import their encryption keys.

8. Protecting a file

When a user protects access to a document containing confidential information, only they and authorized persons can view it.

To grant access to other people, the cases vary:

Recipients belong to the same tenant as the user	The email addresses of the recipients used for sharing are contained in the tenant database. They are automatically suggested when selecting recipients.
Recipients belong to a tenant other than the user's	The user enters their email addresses manually.
Recipients do not have an account on SDS Encryption Portal	The user enters their email addresses manually. Recipients access the protected document using a temporary code. For more information, see External user login.

To protect a document, instruct your users as follows:

1. Log in to SDS Encryption Portal. For further information, see Logging in to SDS Encryption Portal.
   The file selection page appears.
2. Click on the frame at the center of the page to select the file on your disk that you wish to protect.
   - or -
   Drag and drop the file you wish to protect to the frame at the center of the page.
3. If you wish to allow other users to read this file, enter their e-mail addresses in the **Emails** field. You can enter up to 30 addresses;
4. Click on **Protect**.
   The protected file is saved as an *.sdsx* file in your default download folder, and only you and the people you allow can read the file by logging in with your e-mail addresses.
5. If your browser prevents you from saving the file, click on **Save the file**.

> **WARNING**
> The unprotected version of the file can still be found at its initial location. You are advised to delete it so that you have only the protected version on your disk. Remember to empty the recycle bin greater more security.

6. Make the protected file available to authorized recipients, for example by sharing them in a shared space or sending them by e-mail. They will be able to view it via SDS Encryption Portal, or via Stormshield Data Security if your portal usage mode allows it. For more information, see Reading protected files.
7. If you wish to protect another confidential file, click on **New file** and repeat the process from step 2.

9. Reading protected files

1. Log in to SDS Encryption Portal. For further information, see Logging in to SDS Encryption Portal.
   The file selection page appears.
2. Click on the frame at the center of the page to select the protected file on your disk. This file must be in *.sdsx*.
   - or -
   Drag and drop the protected file to the frame at the center of the page.
   If you have the rights to this document, it is decrypted and saved in your default download folder.
3. If your browser prevents you from saving the file, click on **Save the file**.
4. If you wish to view another protected document, click on **New document** and repeat step 2.

10. Managing passwords

WARNING
This section applies to the “Internal PKI” usage mode only.

If you use SDS Encryption Portal in “Internal PKI” mode, users have an account protected by a password specific to the portal. If users forget their password, they can request a password reset from their administrator.

Users can also change their password as often as they like, by providing both the old and the new password.

Inform your users of the following procedures.

10.1 Resetting passwords

If you have forgotten your password, to reset it:

1. Contact your administrator who will issue you a temporary password.
2. Log in to SDS Encryption Portal using this password. For further information, see Logging in to SDS Encryption Portal.
   The **Expired password** page appears.
3. In the **Old password** field, enter the temporary password.
4. In the **Password** and **Confirm password** fields, enter a new password that meets the security criteria listed.
5. Click on **Change.**
   Your new password is saved and you are automatically logged in to SDS Encryption Portal with it.

As an administrator, for information on how to generate a temporary password for a user, see Managing users.

10.2 Changing passwords

If you are concerned that your password is no longer secure enough and would like to change it:

1. Log in to SDS Encryption Portal. For further information, see Logging in to SDS Encryption Portal.
2. Click on the  icon at the top on the right, and select **Change password**.
3. Fill in the fields **Old password**, **Password**, and **Confirm password**. Comply with the criteria given for the new password.
4. Click on **Change**.
   Your password has been changed.

11. Managing users

WARNING
This section applies to the “Internal PKI” usage mode only.

If you are a security administrator, you can use SDS Encryption Portal to perform the following administration tasks:

- Assigning administration permissions to other users: helpdesk, recovery, user deletion,
- Granting access to all the protected files of one user to another user (Recovery) and assigning a new password to a user (Helpdesk),
- Deleting users.

11.1 Assigning administration permissions

1. Log in to SDS Encryption Portal as a security administrator. For further information, see Logging in to SDS Encryption Portal.
2. Click on the icon at the top on the right, and select **Manage users**.
3. In the **Users** menu, click on the user to whom you wish to assign permissions.
4. In the **Security administration permissions** area, enable or disable the various permissions as needed:
   - **Give a user's access to another user (Recovery role).** this role makes it possible to grant access to all the protected files of one user to another user, for example if the former user has left the company.
   - **Change users' passwords (Helpdesk role)**. this role makes it possible assign a new password to a user who has forgotten the password associated with his SDS Encryption Portal account.
   - **Delete user**
5. Click on **Apply**.

An icon appears on the user's page indicating that they hold the *Recovery* and/or *Helpdesk* role (s).

After logging back on to SDS Encryption Portal, the user can now perform the operations that his role allows.

However, this user is not allowed to assign these roles to other users.

11.2 Give a user access to another user's data

EXAMPLE
If Paul resigns from the company, this operation would allow his colleague Alice to access all of Paul's protected files after he has left. Alice will keep her own access privileges while holding those belonging to Paul.

1. Log in to SDS Encryption Portal with a user account that has the *Recovery* role. For further information, see Logging in to SDS Encryption Portal.
2. Click on the icon at the top on the right, and select **Manage users**.

3. In the **Users** menu, click on the user whose account you wish to recover (Paul in our example).
   The information regarding this user appears.
4. Click on **Give access**.
5. Enter the full or partial name of the user to whom you wish to grant access (Alice in our example). The list of matches appears.
6. Select your user, then click on **Give access**.

After logging back in to SDS Encryption Portal, Alice can now access all Paul's protected documents by inheriting his rights.

11.3 Assigning a new password to a user

1. Log in to SDS Encryption Portal with with a user account that has the *Helpdesk* role. For further information, see Logging in to SDS Encryption Portal.
2. Click on the  icon at the top on the right, and select **Manage users**.
3. In the **Users** menu, click on the user whose password you wish to change.
   The user's page appears.
4. Click on **Change password.**
5. Enter the new temporary password and confirm it, then click on **Change password**.
6. Securely send the temporary password to the user. They will need to change it.

11.4 Deleting users

Before deleting a user, be sure to give access to their protected documents to another user, if necessary, by following the recovery procedure above.

1. Log in to SDS Encryption Portal with a user account that has user deletion privileges. For further information, see Logging in to SDS Encryption Portal.
2. Click on the  icon at the top on the right, and select **Manage users**.
3. In the **Users** menu, click on the icon  of the user to delete, and select **Delete permanently**.
4. Confirm the deletion.

12. Further reading

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

13. 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.

documentation@stormshield.eu