SAP SuccessFactors

PUBLIC

Document Version: 1H 2025 – 2025-04-04

Implementing Advanced Encryption

THE BEST RUN SAP

Content

1 Advanced Encryption

For increased protection of data at rest in your organization, SAP SuccessFactors HCM suite, advanced encryption add-on extends SAP's default encryption practice by offering customer-managed encryption keys.

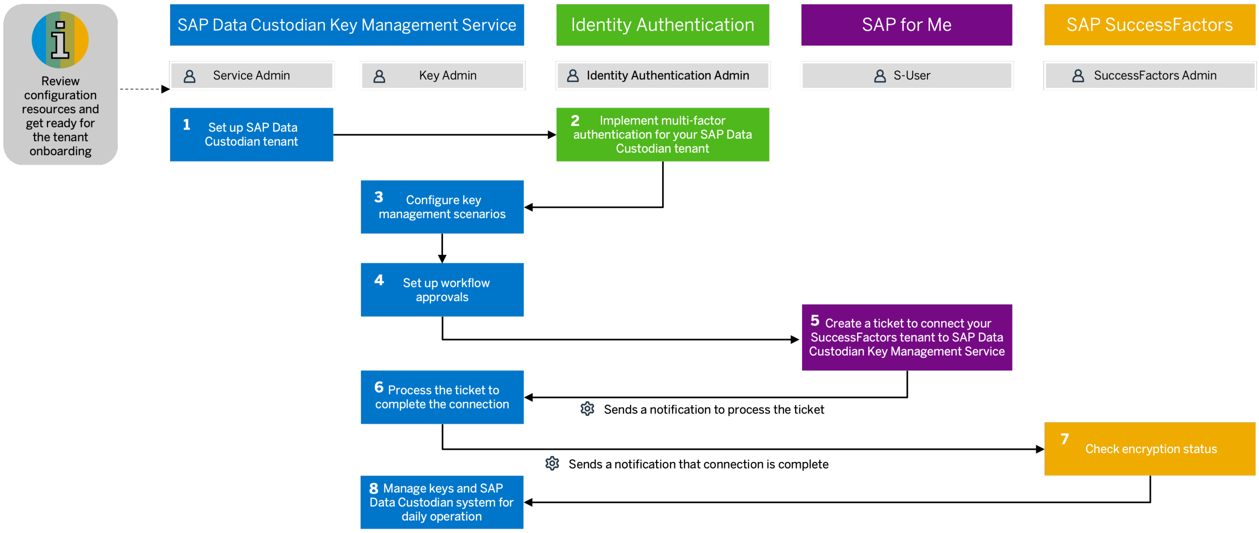
Data encryption at rest is enabled by default at SAP, so your stored data is already encrypted. For an additional level of data protection, you can choose our add-on, Advanced Encryption, which brings you several benefits, including:

- **Individualized keys per tenant**
  You have encryption keys specific to your tenant.
- **Customer-controlled encryption keys**
  You have full control of your encryption keys to manage the key lifecycle and control the database access for your organization's security needs and compliance requirements.

> ⓘ Note
>
> Advanced Encryption can be enabled in certain Production data centers. For more information, see 3381145.

Process Overview

This diagram explains how you set up and manage Advanced Encryption.



Review configuration resources and get ready for the tenant onboarding
SAP Data Custodian Key Management Service
Identity Authentication
SAP for Me
SAP SuccessFactors
Service Admin
Key Admin
Identity Authentication Admin
S-User
SuccessFactors Admin
1 Set up SAP Data Custodian tenant
2 Implement multi-factor authentication for your SAP Data Custodian tenant
3 Configure key management scenarios
4 Set up workflow approvals
5 Create a ticket to connect your SuccessFactors tenant to SAP Data Custodian Key Management Service
6 Process the ticket to complete the connection
Sends a notification to process the ticket
7 Check encryption status
Sends a notification that connection is complete
8 Manage keys and SAP Data Custodian system for daily operation

- https://help.sap.com/docs/sap-data-custodian/help-guide/getting-started-key-management-service?locale=en-US#configuration-resources [https://help.sap.com/docs/sap-data-custodian/help-guide/getting-started-key-management-service?locale=en-US#configuration-resources]

- https://help.sap.com/docs/IDENTITY_AUTHENTICATION/6d6d63354d1242d185ab4830fc04feb1/0d41cd49f6504f3eaf29b58d616b040f.html?locale=en-US [https://help.sap.com/docs/IDENTITY_AUTHENTICATION/6d6d63354d1242d185ab4830fc04feb1/0d41cd49f6504f3eaf29b58d616b040f.html?locale=en-US]
- https://help.sap.com/docs/sap-data-custodian/help-guide/users-key-management-service?locale=en-US [https://help.sap.com/docs/sap-data-custodian/help-guide/users-key-management-service?locale=en-US]
- Setting Up Advanced Encryption [page 7]
- https://help.sap.com/docs/SAP_DATA_CUSTODIAN/538dde61cf134c89bda1c31100a6c0e1/6f28f83e189e411ea2b8857a69defd8f.html?locale=en-US [https://help.sap.com/docs/SAP_DATA_CUSTODIAN/538dde61cf134c89bda1c31100a6c0e1/6f28f83e189e411ea2b8857a69defd8f.html?locale=en-US]
- Connecting Your Tenant to SAP Data Custodian Key Management Service [page 9]
- Managing Advanced Encryption [page 11]
- Monitoring Encryption Status [page 12]
- Connecting Your Tenant to SAP Data Custodian Key Management Service [page 9]

Data Encryption at Rest [page 4]
SAP SuccessFactors HCM suite, advanced encryption add-on is the encryption of your data at rest. Data at rest represents any data that is persistent in the storage for your organization.

SAP Data Custodian Key Management Service [page 5]
SAP SuccessFactors HCM suite, advanced encryption add-on integrates with SAP Data Custodian to provide you with key management service.

1.1 Data Encryption at Rest

SAP SuccessFactors HCM suite, advanced encryption add-on is the encryption of your data at rest. Data at rest represents any data that is persistent in the storage for your organization.

By encrypting data at rest, your organization can reduce the risk of unauthorized access and address compliance. It helps your organization comply with data privacy regulations and protect the privacy of users.

Parent topic: Advanced Encryption [page 3]

Related Information

SAP Data Custodian Key Management Service [page 5]

1.2 SAP Data Custodian Key Management Service

SAP SuccessFactors HCM suite, advanced encryption add-on integrates with SAP Data Custodian to provide you with key management service.

SAP Data Custodian is a Software as a Service (SaaS) solution that protects sensitive data stored in public, private, hybrid, and multicloud environments. One of SAP Data Custodian's main services is the Key Management Service, which provides simplified cryptographic key provisioning, control, and monitoring services to protect your sensitive data.

With Advanced Encryption enabled, you can do the following for your encrypted tenant using SAP Data Custodian Key Management Service.

- Manage the encryption key lifecycle and storage, including key creation, storage, access, rotation, and expiration.
- Define users' access to the encryption tools in the SAP Data Custodian system.
- Access audit logs in the SAP Data Custodian system.

Parent topic: Advanced Encryption [page 3]

Related Information

Data Encryption at Rest [page 4]
Getting Started with SAP Data Custodian

2 Current Scope of Advanced Encryption

Learn which types of data and which SAP SuccessFactors applications are included in the scope of SAP SuccessFactors HCM suite, advanced encryption add-on.

Data Included in Current Scope

All master data stored in the core transactional database in SAP SuccessFactors Platform for the following applications:

- SAP SuccessFactors Platform, including Reporting
- SAP SuccessFactors Employee Central
- SAP SuccessFactors Time Tracking
- SAP SuccessFactors Onboarding
- SAP SuccessFactors Recruiting, excluding Recruiting Posting and Recruiting Marketing
- SAP SuccessFactors Performance & Goals
- SAP SuccessFactors Succession & Development
- SAP SuccessFactors Opportunity Marketplace
- SAP SuccessFactors Compensation

3 Setting Up Advanced Encryption

Learn about how to configure SAP SuccessFactors HCM suite, advanced encryption add-on before using it the first time.

Perform the steps listed below in the following sequence:

Step	Description	More Information
1. Review the important concepts about SAP Data Custodian Key Management Service.	Familiarize yourself with the important concepts required for setting up the SAP Data Custodian Key Management Service.	Concepts
2. Set up your SAP Data Custodian tenant.	After your SAP Data Custodian tenant is ready and the sign-on option is configured, assign user roles in the SAP Data Custodian system. ⓘ Note Your Service Administrators and Key Administrators must be different persons.	User Roles and Permissions
3. Enable multi-factor authentication for the SAP Data Custodian tenant.	To protect the SAP Data Custodian tenant, we recommend that you implement multi-factor authentication for SAP Data Custodian through Identity Authentication service.	Multi-Factor Authentication

Step	Description	More Information
4. Configure key management scenarios.	SAP SuccessFactors HCM suite supports the following types of key management scenarios: • SAP Provided Keystore scenarios allow you to create and manage encryption keys within your Key Management Service tenant using a keystore. • Bring Your Own Key (BYOK) scenarios allow you to securely import cryptographic keys from your own managed keystore or key vault into Key Management Service. • Hold Your Own Key (HYOK) scenarios allow you to generate and manage cryptographic keys from your own keystore. SAP Data Custodian connects to your HYOK keystore and enables you to use permitted keys as primary keys to encrypt data for SAP SuccessFactors HCM suite. Refer to the links in the More Information column for supported services in each type of scenarios and detailed instructions. → Recommendation Set the key properties for the master key as RSA: 4096 or higher.	SAP Provided Keystore Scenarios Bring Your Own Key (BYOK) Scenarios Hold Your Own Key (HYOK) Scenarios
5. Set up workflow approvals.	To safeguard against unwanted operations changes, we recommend that you set up workflow approvals in key groups.	Task Management
6. Enable SAP Data Custodian Key Management Service for your tenant.	Connect your SAP SuccessFactors tenant to the encryption key you've created in the SAP Data Custodian system so that you can use SAP Data Custodian Key Management Service.	Connecting Your Tenant to SAP Data Custodian Key Management Service [page 9]

3.1 Connecting Your Tenant to SAP Data Custodian Key Management Service

As part of the process of enabling SAP SuccessFactors HCM suite, advanced encryption add-on, connect your SAP SuccessFactors tenant to an encryption key in the SAP Data Custodian system so that you can use SAP Data Custodian Key Management Service.

Prerequisites

- You have a valid S-user to sign in to SAP for Me and create support tickets.
  If you don't have an S-user ID, contact your super administrator. For assistance identifying your super administrator, contact the Customer Interaction Center.
- You have an active key administrator role in SAP Data Custodian.
- You've created a key group in the *SAP SuccessFactors HXM Suite* application context for connection.
- You've created a master key for the new key group.
- You've created a master Application Technical User for the new key group.

Context

After the connection is completed, you can manage your encryption keys and connect service tickets from SAP for Me to your tenant within the *SAP Data Custodian* > *SAP SuccessFactors HXM Suite* application context. These tickets facilitate the integration between SAP Data Custodian and the SAP SuccessFactors system.

> → Remember
>
> Each SAP Data Custodian key group can only be connected to one SAP SuccessFactors tenant. After a group is connected to a tenant, it cannot be disconnected. You can only delete the connected group in the SAP Data Custodian system.

Procedure

1. Sign in to SAP for Me.
2. Create a request ticket for the service *(SF) Service: Switch over to customer-controlled encryption keys*.

   Specify the following information in the ticket:
   - The SAP SuccessFactors tenant ID, also known as company ID
   - The SAP Data Custodian tenant ID
   - Email address of the key administrator

   The key administrator is notified by an email to process the service request in the SAP Data Custodian system.

3. Go to the *SAP Data Custodian* > *Key Management Service* > *SAP SuccessFactors HXM Suite* > *Groups* page.
4. Select a key group for connection.
5. On the *Connect Service* tab, choose the *Connect* option for your ticket.

   The ticket status appears as *Connecting*.

   > ⓘ Note
   >
   > You'll receive an email notification when the connection starts. Please expect up to 24 hours of system downtime during which you won't be able to access your SAP SuccessFactors instance.

Results

After a couple of days, the ticket status in the SAP Data Custodian system changes to *Completed* and the ticket status in SAP for Me changes to *Service provided*.

The key administrator receives an email notification about the successful connection. Advanced Encryption is enabled for your tenant.

Related Information

Data, Processes and Communication Flow in SAP Support Portal

4 Managing Advanced Encryption

After SAP SuccessFactors HCM suite, advanced encryption add-on is enabled for your system, you can check encryption status and details in the *Admin Center* and manage encryption keys, audit logs, and user roles in the SAP Data Custodian system.

Advanced Encryption in the SAP SuccessFactors Admin Center

The *Advanced Encryption* page displays encryption status of your company system, the corresponding SAP Data Custodian tenant ID, and information about the encryption key in use, for example, key ID and key version.

Key Management Service in SAP Data Custodian

SAP Data Custodian Key Management Service allows you to manage the SAP Data Custodian system and perform key operations, including:

- Manage user roles
- View service usage information
- Manage workflows and review workflow approval requests
- View audit log events from your Key Management Service activities
- Manage keys based on supported keys scenarios
- Enable key export so that you can backup, download, or restore keys

You perform key operations on the UI or via API calls. For more information about the administration tasks and API reference, see related information.

> ⚠ Caution
>
> Please be aware that if you delete or lose the encryption key, it is not possible for SAP SuccessFactors to restore your access to the encrypted tenant.

Related Information

Key Management Service Administration Guide

SAP Business Accelerator Hub: Central Key Management Service (KMS)

Monitoring Encryption Status [page 12]

4.1 Monitoring Encryption Status

Use the *Advanced Encryption* tool to check whether SAP SuccessFactors HCM suite, advanced encryption add-on is enabled for your system and get information about the encryption key in use.

Prerequisites

You have the *Administrator Permissions* > *Manage Security* > *Access Advanced Encryption* permission.

Context

The *Advanced Encryption* tool displays encryption information only specific to your SAP SuccessFactors tenant:

- Encryption status: on or off
- SAP Data Custodian Key Management Service tenant ID, with a navigation link to the tenant
- Encryption key in use: key ID, key version, and master application technical user

> Example
>
> After you rotate a key to create a key version in the SAP Data Custodian system, confirm in the SAP SuccessFactors system if the new version is now used to encrypt data at rest for your system.

Procedure

1. Go to *Admin Center* > *Advanced Encryption*.
2. View encryption details.

   > Note
   >
   > If Advanced Encryption isn't enabled for your system, no encryption details are displayed on the page.

Next Steps

Now that you know the encryption details, you can view the audit log of users' operations on this encryption key in the SAP Data Custodian system:

Go to the *SAP Data Custodian* > *Tenant Management* > *Key Management Service* > *User Logs* tab and enter the key ID for your system into the field *Instance ID* to get the audit log related to the key.

Related Information

Audit Page

5 Change History

Learn about changes to the documentation for Advanced Encryption in recent releases.

2H 2024

Type of Change	Description	More Info
Feb 14, 2025		
Changed	We added information about the Production data centers where you can enable Advanced Encryption.	Advanced Encryption [page 3]
Changed	We added a caution note.	Managing Advanced Encryption [page 11]

1H 2024

Type of Change	Description	More Info
New	Advanced Encryption is now generally available.	Advanced Encryption [page 3]
Changed	We updated the supported keystores in Advanced Encryption.	Setting Up Advanced Encryption [page 7]
New	We added API reference about how to perform key operations.	Managing Advanced Encryption [page 11]

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP