SAP SuccessFactors

PUBLIC

Document Version: 2H 2025 – 2026-04-13

Implementing and Using Data Retention Management (Legacy and Non-DRTM)

Content

1 Data Purge

The SAP SuccessFactors HCM suite stores a wide range of information about your employees. Generally speaking, historical data should not be stored any longer than is required. Once the required retention time has passed, data should be purged. A data purge is a means of permanently removing data from storage.

For the purpose of data protection and privacy, you may be required to purge user data from your system after a certain length of time. You may also choose to purge user data simply because it no longer serves any business purpose.

To meet this requirement, SAP SuccessFactors provides the ability to purge different types of data across the HCM suite, on a recurring schedule and based on configurable retention times.

2 List of Legacy and Non-DRTM Purge Requests Types

Lists of legacy and non-DRTM purge request types, without data retention time management (DRTM).

> **Note**
>
> Be aware that the legacy data purge function may not meet your data protection and privacy requirements. It doesn't cover the entire HCM suite and it doesn't permit you to configure retention times for different countries or legal entities.

Data Protection and Privacy Warning [page 7]

Legacy Purge Requests (without DRTM)

Purge Request Type
Purge Inactive User
Purge PM or SM Data
Purge Learning Activity
Purge Development Goal
Purge Career Worksheet
Purge Calibration
Purge Goal
Purge Inactive Job Applications
Purge Inactive Candidate
Purge Compensation/Variable Pay Data
Purge Variable Pay Forecast Data
Purge Time Management Data

Non-DRTM Purge Requests

Purge Request Type
Purge Completed To-Do Items
Purge Non-Sensitive MDF Audit Data
Purge Non-Sensitive MDF Business Data
Purge MDF Attachments

3 Types of Purge Requests

Understanding similarities and difference among legacy, non-DRTM, and DRTM purge requests helps you decide which type meets your data protection and privacy requirements.

Legacy Purge Requests

Data included in legacy purge requests contains personal information that may be legislatively sensitive depending on your location. However, legacy purge requests don't cover the entire HCM suite and don't permit you to configure retention times for different countries/regions or legal entities. All legacy purge requests have corresponding DRTM purge requests whose functions are more comprehensive. We recommend you using DRTM purge requests in cases that you need to purge data included in legacy purge requests.

Non-DRTM Purge Requests

Data included in non-DRTM purge requests doesn't contain personal information. Thus, it doesn't require data retention time management for data protection and privacy. We recommend you using non-DRTM purge requests to free up memory space and improve system performance.

4 Data Protection and Privacy Warning

Be aware that the legacy data purge function may not meet your data protection and privacy requirements. It doesn't cover the entire HCM suite and it doesn't permit you to configure retention times for different countries or legal entities.

> → Remember
>
> We encourage all customers to stop using the legacy purge function and start using data retention time management (DRTM) instead. To get started using this and other data protection and privacy features, refer to the Data Protection and Privacy guide.

The legacy data purge function does **not** meet the following requirements:

- Ability to purge **all** personal data across the HCM suite for a given person or group of people.
- Ability to configure different data retention times for different types of data and for different countries or legal entities.
- Ability to put a legal hold on data for a given person or group of people so that it’s excluded from the purge process until the hold is removed.

If you already use the legacy data purge function and you've verified that it meets your organization's data protection and privacy requirements, you can continue to use it, as long as you're aware of its limitations.

5 Limitations of Legacy Data Purge Function

The legacy *Data Retention Management* tool has the following limitations.

> ⚠ Caution
>
> The legacy purge function may not meet all of your data protection and privacy requirements. It doesn’t cover data across the full HCM suite and doesn’t enable you to configure data retention times.

- If you use legacy purge functions, some attachment files may remain in the database, which could take up the storage space.
- If you use the legacy *Purge Inactive Users* function, some module data may remain in the database. It doesn’t purge data across the full HCM suite.
- If you use the legacy *Purge Inactive Users* function, it isn’t a permanent purge. It only performs a "soft delete" and you still need to manually trigger the *System Identifier Purge* function separately.
- There’s no validation logic in the legacy *System Identifier Purge* function.
- To avoid issues with job scheduler performance for *Purge Inactive Users* requests, limit requests to 10,000 or fewer users at a time.

Related Information

Data Protection and Privacy Warning [page 7]

6 Process for Purging Data with Data Retention Management

Purging data with Data Retention Management is a multistep process.

Here is an overview of the process:

1. Create purge request by defining data to be purged and specifying approvers.
2. Submit purge request to occur immediately or at a future time.
3. Notification is sent to specified approvers.
4. Approval steps vary based on when the purge request is set to occur:
    1. If the purge request was launched immediately, a preview report is generated immediately so that approvers can review it.
    2. If the purge request was scheduled to occur at a future time, approvers first need to approve the request so that a preview report is generated at the scheduled time.
5. Notification is sent to specified approvers when the preview report is ready to review.
6. Approvers review the purge preview report to confirm that the purge is set up correctly and executes successfully.
7. Approvers either approve or decline the purge request.
8. The approved purge request is sent to the job queue:
    1. If the purge request was launched immediately, it’s sent to the job queue as soon as it’s approved and the purge job runs at the next available time.
    2. If the purge request was scheduled to occur at a future time, it's sent to the job queue at the time of recurrence and the purge job runs at the next available time after that.
9. The purge job runs.
10. The purge job completes and the complete final report is generated.
11. Review the complete final report to confirm whether the purge job was successful or not, for each type of data.

7 Recommended Permission Settings for Data Purge Functions

Understand key concepts about role-based permission to design a purge process that restricts data purge capabilities to the appropriate roles.

Data purge is a powerful tool that irreversibly removes data from the system. Use role-based permission carefully to ensure that the purge process has the necessary oversight and to reduce the potential for accidental deletion.

Restrict Users from Using All Purge Functions Simultaneously

The *Data Retention Management* tool includes three types of purge: **DRTM** purge function, **non-DRTM** purge function, and **legacy** purge function. While all have valid uses, we recommend that you don't give the same permission role access to all purge functions.

You can grant permission to create and approve DRTM purge requests and non-DRTM purge requests (legacy purge requests included) separately. If you've configured the DRTM purge function, it's probably necessary for your data protection and privacy requirements. You want to ensure that no one accidentally uses a similarly named legacy purge type instead.

The simplest and surest way to avoid this is to use DRTM only.

However, some customers choose to use the legacy purge as well, for certain specific purge processes. If you have to use both purge functions simultaneously, keep them separate using role-based permission. Create a different permission role for each purge function and assign it to different groups. Then ensure that people in each role know which purge requests they can use. Or, alternatively, use DRTM most of the time, for most purge use cases, and only grant access to the legacy purge function temporarily when the need arises. Then remove access again.

Ensure Oversight

To reduce risk, we recommend a purge process that ensures no one person can complete the full purge process on their own.

You can ensure oversight in two ways:

- Require multiple approvers for each purge request.
- Set up different permission roles for purge request creation and purge request approval.

The simplest way to ensure that oversight is to create one purge role with both permissions to both create and approve purge requests, but require multiple approvers. Or, alternatively, you can separate these actions into different permission roles assigned to different people.

Restrict Access to Purge Information of DRTM Purge Requests

Any user with the permission to access *Data Retention Management* have access to all purge requests submitted in your company's instance. To strengthen data protection and privacy, we recommend restricting access to purge reports of DRTM purge requests based on countries or regions with DRTM enabled.

Assign a Target Population for Purging Inactive Users

Role-based permissions to create or approve purge requests don't require a target population, but purging inactive users does. To completely remove user accounts and basic user information from the system, the user who submits the purge request needs to have *Manage Users* permission **for the target population** that is included in the purge set-up.

The simplest way to set up target permission is to create one purge role that can purge all inactive users and give that role a target population of *Everyone*. Or, alternatively, if required by your business, you can set up more robust data purge controls using multiple permission roles and permission groups, with different target populations.

8 Enabling Data Retention Management

Enable the *Data Retention Management* feature so that you can create and submit purge requests to purge employee data from your system.

Prerequisites

You have the *Company System and Logo Settings* permission.

Procedure

1. Go to *Admin Center* > *Tools* > *Company System and Logo Settings*.
2. Select *Data Retention Management*.
3. In *Minimum # of approvers*, specify the required minimum number of users who must approve a purge request.

   For example, if you type **3**, then anyone who sets up a purge request must specify three or more Approvers before they can save or submit the purge request.
4. Click *Save Company System Setting* to save your changes.

Results

The *Data Retention Management* and *Purge Request Monitor* pages can now be used by people with the appropriate permissions.

The data retention time management (DRTM) function recommended for data protection and privacy is **not** available by default. You need to set it up.

Next Steps

To use legal entity-based data retention with Employee Central, enable that next, while you're on the *Company System and Logo Settings* page. Then proceed with additional set-up steps.

Use role-based permissions to control access to *Data Retention Management* functions.

- Most customers only use one purge function, either DRTM or legacy. If you choose to use both, set up role-based permissions carefully to avoid conflicting purge rules.
- For data retention time management (DRTM), use *Create DRTM Data Purge Request* and *Manage and Approve DRTM Data Purge Request* permissions.

- For the legacy data purge function, use *Create Legacy Data Purge Request* and *Manage and Approve Legacy Data Purge Request* permissions.
- Ensure permission roles who can purge inactive users also have *Manage Users* permission for the appropriate target population.

9 Changing the Minimum Number of Approvers for Purge Requests

Change the minimum number of approvers required for purge requests. By default, the minimum number of approvers is one.

Prerequisites

You have the *Company System and Logo Settings* permission.

Procedure

1. Go to *Admin Center* > *Tools* > *Company System and Logo Settings* .
2. Under *Data Retention Management*, in the *Minimum # of approvers* field, enter an integer value of 1 or more.

   For better oversight of the data purge function, we recommend a value of 2 or more to ensure that no single individual can purge data on their own.
3. Click *Save Company System Setting* to save your changes.

Results

When creating a purge request, you now must add the specified minimum number of approvers to a purge request before you can submit it.

10 Setting Up a Legacy or Non-DRTM Purge Request

Create a legacy or non-DRTM purge request so that you can submit it for approval.

Prerequisites

You have *Create Legacy Data Purge Request* permission.

Context

> ⚠ Caution
>
> Don't use follow these steps if you want to purge data based on a configurable retention time. To use data retention time management (DRTM), please refer to the guide here.

Procedure

1. Go to *Admin Center* > *Data Retention Management*.
2. Click *Create New Purge Request* in the *Manual Data Purge* tab.
3. Select the type of data purge you want to set up in the *Select a purge request type* menu.
4. Define purge rules by selecting the appropriate criteria. The criteria available vary depending on the purge request type you selected.
5. Find and select one approver in the *Add approvers* search box.

   To add others, select *Add another approver*.
6. Click *Save* to save your purge rule.

Results

Your new purge request is saved and ready to submit for approval.

Next Steps

Submit your purge request to the designated approvers.

Related Information

List of Legacy and Non-DRTM Purge Requests Types [page 5]

11 Submitting a Legacy or Non-DRTM Purge Request for Approval

Set up the time you want the purge request to occur and submit it to designated approvers.

Prerequisites

- The purge request has been created and set up completely.
- You must have *Create Legacy Data Purge Request* permission, but you don't need to be the creator of the request.

Context

⚠ Caution

Don't follow these steps if you want to purge data based on a configurable retention time. To use data retention time management (DRTM), refer to the guide here.

Procedure

1. Open the *Edit Purge Request* page in edit mode:
   - If you have just set up a new purge request, you should already be on this page.
   - If you're returning to a previously saved purge request, go to *Admin Center* > *Data Retention Management* and choose the name of your saved request in the *Saved Purge Requests* table.
2. Review your purge request to confirm it's set up correctly.
3. Decide when you want the purge occur.
   - If you want to create a one-time purge request that begins as soon as it's approved, choose *Launch Immediately*, then *Yes* to confirm. In this case, the preview report is generated immediately and the request only needs to be approved once.
   - If you want to create a scheduled purge request that recurs at a specified time, date, and frequency, choose *Schedule*, then use the scheduling dialog to set up the recurrence pattern. In this case, the purge request must be approved twice, once to generate a preview report and once to begin the actual purge process.

> ⚠ Caution
>
> UI issues in the scheduling dialog can cause some unintentional configuration errors. For example, the recurrence pattern is set in 24-hour time, while start and end dates use 12-hour time. Also, purge times are based on our server times, not your local time. Be careful when scheduling your purge request.

Results

- If you selected *Launch Immediately*, the preview report is generated immediately and is available for approvers to review in *Purge Request Monitor* > *Requests Pending Final Approval* when the preview report is ready.
- If you selected *Schedule*, the purge request first appears in *Purge Request Monitor* > *Requests Pending Initial Approval* at the scheduled time.
- In cases where multiple users act on the same purge request, the email notification behavior varies:
  - When a draft purge request is launched immediately, only the user who launched it and the approvers receive email notifications.
  - When a schedule is added to the draft request, the user who created the draft, the user who scheduled it, and the approvers all receive email notifications.

Next Steps

Purge requests can now be reviewed and approved by the specified approvers.

12 Generating Preview Report for a Scheduled Purge Request

Approve the criteria and schedule of a scheduled purge request so that a preview report can be generated.

Prerequisites

- You have either *Manage and Approve DRTM Data Purge Request* or *Manage and Approve Legacy Data Purge Request* permission.
- You're designated as an approver of the purge request.

> Note
>
> As an approver, you should have the permission to purge the target users of the scheduled purge request. Otherwise, users that you don't have the permission to purge are excluded from the purge job. If all users are out of your target population, an empty purge report is generated.

Context

Only scheduled purge requests require a separate step to generate a preview report. Scheduled purge requests show up in *Purge Request Monitor* > *Requests Pending Initial Approval* at the scheduled time.

For immediate purge requests, you can skip this step. The preview report is generated immediately after it's submitted and you only need to approve to start the purge process in *Purge Request Monitor* > *Requests Pending Final Approval*.

> Note
>
> You should only receive an email notification asking you to approve a purge request for which you're identified as an approver. If you haven't received any email, you may not need to complete this step. However, you don't **need** to have received an email in order to do it.

Procedure

1. Go to *Admin Center* > *Purge Request Monitor*.
2. Locate the purge request that needs approval in the *Request Pending Initial Approval* tab.
3. Expand the *Criteria* section to review the purge request setup.

4. Click *View Schedule* to review when the purge request is set to recur.
5. Choose how you want to proceed with scheduled purge requests or decline this request.

Results

- If you agree to generate a preview report, the purge request shows up in the *Request Pending Final Approval* tab when the preview report is ready for review.

  > Note
  >
  > If there are multiple approvers, the preview report is only available when all approvers approve the requests. However, your decision on the approval options only determines your own approval workflow.

- If you decline the request, it goes to the *Purge Progress & Results*.
- If one of the approvers chooses to review preview report for each occurrence, the creator and specified approvers receive an email notification when preview report for each occurrence is ready and the purge request is pending final approval.
- If all approvers choose to approve the whole series, the creator and specified approvers receive an email notification when each occurrence is complete.
- Only future occurrences of a scheduled purge request are executed when the approval is granted after a scheduled time.

Next Steps

Specified approvers must approve the purge request to start the purge process.

13 Reviewing a Purge Preview Report

Review the purge preview report to verify the set-up of a purge request before you approve it.

Prerequisites

- You have either *Manage and Approve DRTM Data Purge Request* or *Manage and Approve Legacy Data Purge Request* permission.
- *Additional access control based on DRTM-enabled countries or regions* and countries/regions selected.

> ⓘ Note
>
> This permission is only required when you have enabled *Additional access control based on DRTM-enabled countries or regions* in *Admin Center* > *Company System and Logo Settings* > *Data Retention Management*.

Procedure

1. Go to *Admin Center* > *Purge Request Monitor*.
2. Locate the purge request you want to review in the *Requests Pending Final Approval* tab.
3. Expand the *Criteria* section to confirm the purge set-up is correct.
4. Download and review the preview report in a ZIP file.

Results

The preview purge report archive may contain multiple CSV files. One of the files lists the selection results—that is, the users that meet the selection criteria. The other files show a preview of purge results and each one corresponds to a different data source. In the preview purge results files, records that will be purged are marked with a process status of "TO BE PURGED".

If a user satisfies the selection criteria but doesn't have the relevant data to be purged, the user is listed in the CSV file for selection results but not listed in the CSV file for the preview purge results. If none of the selected users have relevant data to be purged, no CSV files for preview purge results are generated.

> ⓘ Note
>
> As a Compensation Administrator, you can either purge the complete worksheet or move the existing employees in the worksheet before approving the purge request with the *DRTM Master Data* purge. In addition, the system automatically deletes the purged user data in the Snapshot of Compensation worksheets.

Next Steps

Specified approvers must approve the request to start the purge process.

14 Approving or Declining a Purge Request

As a designated approver, approve or decline a purge request before data can be purged from the system.

Prerequisites

- You have either *Manage and Approve DRTM Data Purge Request* or *Manage and Approve Legacy Data Purge Request* permission.
- You're designated as an approver of the purge request.

> Note
>
> You'll receive an email notification asking you to approve a purge request when the preview report is ready for review. For scheduled purge requests, preview reports are generated at scheduled time and email notifications are sent once the scheduled preview reports are ready for review.

- You've reviewed the purge preview report.

Procedure

1. Use the link in your email notification, or log in and go to *Admin Center* > *Purge Request Monitor*.
2. Locate the purge request that needs approval in the *Requests Pending Final Approval*.
3. Approve or decline the request.

Results

- After a purge request is approved by **all** designated approvers, the purge process can proceed.
- The creator and specified approvers receive an email notification when the purge is complete.
- The creator of the purge request receives email notifications when the purge request is declined.
- Immediate purge requests are submitted to the job scheduler immediately after approval and the purge job begins at the next available time.
- Scheduled purge requests are submitted to the job scheduler at the configured recurrence time and the purge job begins at the next available time.
- Only future occurrences of a scheduled purge request are executed when the approval is granted after a scheduled time.

15 Verifying Final Purge Results

Review a complete final purge report to verify that data was purged successfully.

Prerequisites

You have permission to create or approve purge requests.

Procedure

1. Go to *Admin Center* > *Purge Request Monitor*.
2. Locate the purge request in the *Purge Progress & Results* tab and choose *View Result*.
3. View the number of successful, filtered, and failed records affected by the purge.
4. Download the complete report in a ZIP file.
5. Open the downloaded archive and review its contents.

Results

The complete final purge report archive may contain multiple CSV files. One of the files lists the selection results —that is, the users that meet the selection criteria. The other files show the actual purge results and each one corresponds to a different data source. In these purge results files, records that are successfully purged are marked with a process status of "PURGED".

If a user satisfies the selection criteria but doesn’t have the relevant data to be purged, the user is listed in the CSV file for selection results but not listed in the CSV file for the actual purge results. If none of the selected users have relevant data to be purged, no CSV files for purge results are generated.

16 Checking Job Status and Details for a Purge Request

Use the *Purge Request Monitor* to check the status of a purge job or link to more job details in the Execution Manager.

Prerequisites

- To check status, you need permission to either create or approve purge requests.
- To see job details, you also need permission to access Execution Manager.

Procedure

1. Go to *Admin Center* > *Tools* > *Purge Request Monitor*.
2. Find the purge request you are interested in, using the *Request Name* defined during purge set-up.
3. Check the current status of the purge job in the *Status* column.
    - **Completed** means that the background purge process has completed successfully and that data was either purged or excluded, according to backend purge rules. It does NOT mean that all data for all specified users were necessarily purged. To confirm whether a given user was successfully purged, check the Process Status in the purge report.
      Review the purge report to confirm which data was purged and which data was excluded.
    - **Completed With Error** means that the background purge process has completed and was mostly successful, with some possible exceptions. Exceptions occur when we find bad data that prevents a certain type of data from being purged successfully for some users.
      Use the *View Job Details* action to identify the source of the error or contact Technical Support for help.
    - **Completed with empty report** means that the background purge process has completed successfully but none of the specified user data was eligible for purging, so no data purge occurred. For example, if you try to purge all inactive users in Germany but there are no inactive users in your system who are in Germany and past the required retention time, then the report is empty.
      If correct, no action is needed. If you think this might not be correct, double check the purge criteria and configured retention time. Then submit the request again.
    - **Processing purge** means that the background purge process is still in progress.
      Check again later.
    - **Expired** means that a preview report was generated successfully but the designated approvers didn't respond in time, so no data purge occurred.
      Submit the request again.
    - **Failed** means there was an internal error that caused the background purge process to fail.
      Submit the request again. If the problem persists, contact Technical Support for help.

- **Declined** means that a preview report was generated but one of the designated approvers rejected the request, so no data purge occurred.
  Double check the purge criteria or contact approvers to understand why it was declined. Then adjust the criteria as needed and submit the request again.

4. For technical details about a purge job, to help with troubleshooting, use the *View Job Details* action to open details from the Execution Manger in a pop-up window.

17 Configuring Retention Time for Finished Purge Requests

Set a retention time for all finished purge requests in *Purge Request Monitor* so that they're automatically deleted including purge reports when reaching the defined retention time.

Context

Purge requests in *Purge Request Monitor* > *Purge Progress & Results* with the following status are subject to the retention rule:

- Completed
- Completed with error
- Completed with an empty report
- Declined
- Failed
- Expired

Procedure

1. Go to *Admin Center* > *Company System and Logo Settings*.
2. Go to the *Data Retention Management* section at the bottom of the page.
3. Enter the retention time in days in *Set the retention time in days for finished purge requests in Purge Request Monitor*.
4. Save your changes.

18 Deleting Old Purge Requests

Delete your old purge requests when they're expired, failed, or completed to remove unnecessary clutter from the *Purge Request Monitor*.

Prerequisites

- You have permission to either create or approve purge requests.
- The purge request has a status of EXPIRED, FAILED, or COMPLETED.
- You're the requestor of the purge request.

Context

A large organization with complex purge rules in multiple countries/regions or regions may have a large number of past purge requests. You can delete your old purge requests to remove clutter from the page.

> Note
>
> Purge requests that exceed the retention period are being deleted monthly from the system automatically. The retention time is configured at *Admin Center* > *Company System and Logo Settings*. The associated purge reports are deleted as well. You can't find them in the *Purge Request Monitor*.

> Caution
>
> Deleting a purge request also deletes its associated purge reports. If you want to keep these reports, be sure to download and archive them before deleting the purge request.

Procedure

1. Go to *Admin Center* > *Purge Request Monitor* > *Purge Progress & Results*.
2. Locate the purge request you want to delete.
3. Select *Delete Request* from the actions menu and then *Yes* to confirm.

Results

The purge request is permanently deleted and removed from the *Purge Request Monitor*, along with its associated reports.

19 Deleting Old Purge Reports

Delete your old purge reports when they are no longer needed.

Prerequisites

- You have either *Remove Preview and Complete Reports for DRTM Data Purge Request* or *Remove Preview and Complete Reports for Legacy Data Purge Request* permission.

Context

Purge reports can contain personal information so periodically you may need to remove them from storage, for data protection and privacy.

> Note
>
> Purge requests that exceed the retention period are being deleted monthly from the system automatically. The retention time is configured at *Admin Center* > *Company System and Logo Settings*. The associated purge reports are deleted as well. You can't find them in the *Purge Request Monitor*.

Procedure

1. Go to *Admin Center* > *Tools* > *Purge Request Monitor* > *Purge Progress & Results*.
2. Locate the purge request with reports you want to delete.
3. Use the actions menu to select the report you want to delete and then *Yes* to confirm.
    - Select *Remove Preview Report* to delete the preview that was generated before the purge.
    - Select *Remove Complete Report* to delete the final report that was generated after the purge.

Results

The selected report is permanently deleted from storage and cannot be recovered.

20 Purging MDF Data (Non-DRTM)

If you need to free up memory space, you can permanently remove MDF data that you no longer need. Please note that you should only use legacy and non-DRTM purge requests to purge MDF data if you've confirmed that it meets your organization's data protection and privacy requirements.

Prerequisites

- You understand the limitations of a legacy and non-DRTM purge request, which does **not** use data retention time management (DRTM).
- You're familiar with how the Data Retention Management tool works, and also with the end-to-end-data purge process.
- You have *Create Legacy Data Purge Request* permission.

  > ⚠ Caution
  >
  > The system does not check if the user performing the MDF purges (non-DRTM) has permission at object level or object field level. Therefore, you should only grant this permission to users who are allowed to access all objects and object fields affected by these MDF purges.

Context

Use these purge types to free up memory space, not for data protection and privacy. To thoroughly purge personal data, whether it's stored in MDF or not, use Data Retention Time Management (DRTM) instead.

You want to do one of the following:

- *Purge Non-Sensitive MDF Audit Data*
  This purge request type permanently removes audit data that has been created for MDF objects that have no legislatively sensitive personal data configuration. You can create the purge for both custom and predelivered MDF objects.

  > ⚠ Caution
  >
  > After audit data is purged, you won't be able to generate audit reports for the purged records.

  > ⓘ Note
  >
  > In the context of an MDF audit data purge, "audit data" refers to MDF objects that have MDF Version History switched on to enable audit-logging.

- *Purge Non-Sensitive MDF Business Data*
  This purge request type permanently removes business data for MDF objects that have no legislatively sensitive personal data configuration. The purge can be run for custom and predelivered MDF objects.

- *Purge MDF Attachments*
  This purge request type permanently removes attachments for custom and predelivered MDF objects, both **with and without** legislatively sensitive personal data configuration.

> ⓘ Note
>
> Do not purge attachments from MDF objects with legislatively sensitive personal data unless you've confirmed that they're no longer required by your data retention requirements.

> ⓘ Note
>
> Since attachment fields can sometimes be mandatory, the purge replaces the attachment with a file of smaller size containing a note that the attachment has been purged. This prevents any errors that might have otherwise arisen due to a missing mandatory field entry.

Procedure

1. Go to *Admin Center* > *Data Retention Management* > *Create New Purge Request*.
2. Create a purge request:
   - To purge MDF audit data, select *Purge Non-Sensitive MDF Audit Data*.
   - To purge MDF business data, select *Purge Non-Sensitive MDF Business Data*.
   - To purge MDF attachments, select *Purge MDF Attachments*.
3. Select an MDF object.

   > ⓘ Note
   >
   > You can't purge data for MDF object definitions and MDF picklists, nor DRTM objects.

4. Select at least one field, an operator, and a value. If you select more than one field for an object, you get only those records that meet ALL criteria.
   - For *Purge Non-Sensitive MDF Audit Data*, select *auditTransactionDate* as field.

     > ⚠ Caution
     >
     > - If you select fields other than **`auditTransactionDate`**, this could lead to gaps in the audit history and thus incorrect audit reports.
     > - We don't recommend selecting translatable fields as field criteria, as this could purge more audit records than intended. A translatable field always refers to an object. For example, when the translatable field for object "1234" is purged, the system also purges any other records of object "1234" in that audit log.

   - For *Purge MDF Attachments*, this step is optional. You can restrict the object instances for which you want to purge attachments by selecting one or more object fields with operators and values here.
5. For *Purge MDF Attachments*, select an attachment:
   - To delete only attachments that meet specific criteria, enter size in MB and/or the last upload date as selection criteria.

- To purge **all** attachments of an attachment field, select the attachment field and then enter one of the following:
  - *Size in MB*: >= `0`
  - *Last Upload Date*: <= (select the date on which you create the purge request)

> **Note**
>
> You can select more than one attachment field for an object.

6. To make sure that MDF business data with the status *History Pending* is included in the purge, select *Include Pending History Records*.
7. Proceed with purge set up and approval, as you would for any purge request.

21 Purging Inactive Users with the Legacy Purge Request (Non-DRTM)

Only use the legacy purge request (without DRTM) to purge inactive users if you've confirmed that it meets your organization's data protection and privacy requirements.

Prerequisites

- You understand the limitations of the legacy *Purge Inactive User* purge request. It doesn't remove **all** personal data about a user and it doesn't fully purge all personal data from storage, across the HCM suite.
- You have *Create Legacy Data Purge Request* permission.
- The status of target users has been set to inactive.
- You have *Manage Users* permission for the relevant target population.

> Note
>
> To completely remove user accounts and basic user information from the system, the user who submits the purge request needs to have *Manage Users* permission **for the target population** that is included in the purge set-up.

Context

The legacy purge of inactive users is a multistep process. First, use the *Purge Inactive User* purge request in *Data Retention Management* to effectively remove inactive users from the system. Some system identifiers are retained internally but the users are no longer visible in the system. Then, to completely purge the inactive user accounts, you can use the *System Identifier Purge* option.

> Note
>
> For Employee Central enabled instances, the *Admin Center* > *Company System and Logo Settings* > *Data Retention Management* > *Enable Purge Inactive User request type* option has been removed

Procedure

1. Go to *Admin Center* > *Data Retention Management* > *Manual Data Purge* > *Create New Purge Request* and select *Purge Inactive User*.
2. Select how you want to identify a batch of users to purge:

- If you need to purge a single user, select *Select a single user*.
- If you can use a set of rules to identify users to be purged, select *Select multiple users* and use the fields match users with rules.
- *Upload a user list (by User ID or Assignment ID)*. Use this option to purge data for multiple users, based on your own criteria. Use the downloadable CSV example as a template.

> ⓘ Note
>
> Ensure that the import file only has one column and that the column header matches the unique identifier field you use. By default, the column header is `Assignment ID`. You can use `Assignment ID` or `User Id`.

3. Select conditions under which users should be **excluded** from the purge request, using options in the *Exclude users that meet the following criteria* section.

> ⓘ Note
>
> To delete inactive users from Compensation and Variable Pay worksheets, irrespective of the worksheet status, clear the *User belongs to an incomplete compensation or variable pay form* option from the exclude users section. By default, the system excludes users who belong to incomplete worksheets from purging.

4. Proceed with purge set up and approval, as you would for any purge request.

Next Steps

When the purge job runs, most user data associated with the specified inactive users is purged, except for some internal system identifiers. If necessary, you can use the *System Identifier Purge* function to manually complete the purge process by deleting these identifiers as well.

> ⓘ Note
>
> The *System Identifier Purge* deletes system identifiers that are used both internally and in third-party integrations, so deleting them can have broad impacts. Some customers choose to use the *System Identifier Purge* option because they want to reuse old user IDs for different users. Although this isn't a leading practice, it's possible if required by your business.

Inactive User Purge (Non-DRTM) [page 36]
Use the legacy *Inactive User Purge* to remove inactive users from the system. For Employee Central enabled instances, the *Admin Center* > *Company System and Logo Settings* > *Data Retention Management* > *Enable Purge Inactive User request type* option has been removed.

Permission Required for Purging Inactive Users [page 37]
To purge inactive users with *Data Retention Management*, you need *Manage Users* permission for the target population who is included in the purge.

Related Information

Setting User Status to Inactive

21.1 Inactive User Purge (Non-DRTM)

Use the legacy *Inactive User Purge* to remove inactive users from the system. For Employee Central enabled instances, the *Admin Center* > *Company System and Logo Settings* > *Data Retention Management* > *Enable Purge Inactive User request type* option has been removed.

> ⚠ Caution
>
> This purge request type does **not** support data retention time management (DRTM). It only removes the platform user information and user account, but not other data across the HCM suite that is associated with the inactive users. It does not consider any configured retention time.

> ⓘ Note
>
> Purging Employee Central data deletes the following associated data. For data associated with MDF objects (Time Off, Time Sheet, Alternate CostCenter Assignment Data, Advances, IT Declaration, Deduction, custom GO, Payment Information, Secondary Employment), data is only deleted if the feature is enabled in Provisioning.
>
> - Employee Central data
> - Time Off data
> - Workflow data
> - Global Assignments data
> - Dependents data
> - Alternative Cost Center Assignment data
> - Advances data
> - IT Declarations data
> - Deductions data
> - Time Sheet data
> - Payment Information data
> - Custom GOs with user id as key
> - Secondary Assignment objects for concurrent employment users
>
> If Employee Central data has been replicated to other systems, the replicated data isn't purged from those systems. It's only purged from Employee Central.

Parent topic: Purging Inactive Users with the Legacy Purge Request (Non-DRTM) [page 34]

Related Information

Permission Required for Purging Inactive Users [page 37]

Permission Required for Purging Inactive Users [page 37]

21.2 Permission Required for Purging Inactive Users

To purge inactive users with *Data Retention Management*, you need *Manage Users* permission for the target population who is included in the purge.

To completely remove user accounts and basic user information from the system, the user who submits the purge request needs to have *Manage Users* permission **for the target population** that is included in the purge set-up.

> Example
>
> For example, to run a master data purge of all inactive users in Germany, the user who initiates the purge request needs to be a member of a permission role that: (1) includes the *Manage Users* permission; (2) includes inactive users in Germany within its target population. If the user who initiates the purge does note have *Manage Users* permission for users in Germany, the purge fails and an error appears in the purge report.

The *Manage Users* permission allows the granted user to take many actions on employee data (add, edit, delete, import, export), as well as purge. Only grant this permission to roles who should be able to perform all of these actions.

Parent topic: Purging Inactive Users with the Legacy Purge Request (Non-DRTM) [page 34]

Related Information

Inactive User Purge (Non-DRTM) [page 36]

22 Permanently Deleting Purged Users and User IDs

Use *System Identifier Purge* to delete the system identifiers of inactive users that have already been purged with *DRTM Master Data Purge*, or to delete the system identifiers and leftover module data of inactive users that have been purged with the legacy *Purge Inactive User* function.

Prerequisites

- You have successfully purged inactive users with *DRTM Master Data Purge* or the legacy *Purge Inactive User* purge request.
- You're granted with one of the two permissions in the permission category *Manage Data Purge*:
  - *Create Legacy Data Purge Request*
  - *Create DRTM Data Purge Request*
- You understand the impacts of a permanent purge and how it affects your system.

Context

The *System Identifier Purge* deletes system identifiers that are used both internally and in third-party integrations, so deleting them can have broad impacts. Some customers choose to use the *System Identifier Purge* option because they want to reuse old user IDs for different users. Although this isn't a leading practice, it's possible if required by your business.

Due to the limitations of the legacy *Purge Inactive Users* function, some module data remains in the database. *System Identifier Purge* cleans up those leftover module data along with system identifiers if it's performed following *Purge Inactive Users*.

Procedure

1. Go to *Admin Center* > *Data Retention Management*.
2. Choose the *System Identifier Purge* tab, read the warning message, and confirm that you want to proceed.
3. Choose to purge all inactive users or upload a CSV file identifying the inactive users by their user ID or assignment ID.

   Use the downloadable CSV example as a template.

> ⓘ Note
>
> Ensure that the import file only has one column and that the column header matches the unique identifier field you use. By default, the column header is `Assignment ID`. You can use `Assignment ID` or `User Id`.

4. Choose *Submit* to start the permanent purge process.

Results

System identifiers of specified inactive users are permanently deleted from the system. In cases that *System Identifier Purge* is performed in succession to *Purge Inactive Users*, leftover module data is permanently deleted from the system, in addition to system identifiers.

Any user with one of the create or manage permissions in the permission category *Manage Data Purge* will receive email notifications of the purge results.

23 Using Legacy Data Purge for Recruiting Management Data

You can use legacy data purge to remove Inactive Candidate and Inactive Application data in SAP SuccessFactors Recruiting.

An Inactive Candidate purge request purges inactive candidate data for external candidates. An Inactive Application purge request purges inactive application data for both external and internal candidates.

Internal candidate data is also purged as part of the legacy Inactive User purge.

When a user data purge is triggered, the system purges inactive candidate and inactive application data based on the criteria defined in Recruiting Management.

You can configure the purge rules based on the internal policies for storage of persistent data and records management, based on candidate's country and period of inactive profile.

23.1 Applications and Candidates Purge in Recruiting Management

For data protection and privacy, it is possible to purge candidate profile and applications using DRM 2.0. The applications are purged based on the criteria defined in Recruiting Management.

> → Remember
>
> In Recruiting Management, all the purge jobs anonymize the data without deleting it.

> ⓘ Note
>
> For the fields to be purged, you must mark the field as anonymize="true" in the Candidate Profile XML, Application XML, and Offer Detail XML. Not all fields support anonymization during data purge. In the Offer Detail template, you can only set job application fields as anonymize="true".
>
> For example, you can purge the firstName field as shown:
>
> Sample Code
>
> ```
> <field-definition id="firstName" type="text" required="true" custom="false"
> public="false" readOnly="false" anonymize="true">
> ```

Some of the fields in Candidate and Application do not support anonymization. For more information on the list of fields that do not support anonymization, see the **Related Information** section.

Related Information

XML Fields That Do Not Support Anonymization [page 41]

23.1.1 XML Fields That Do Not Support Anonymization

Review the candidate fields and application fields that do not support anonymization.

Candidate Fields That Do Not Support Anonymization

Field	Field Type
Custom	Date
	Percent
	Boolean
	Number
	Instruction
	Currency
Background data fields	Date
	Int
	Float

Application Fields That Do Not Support Anonymization

Field	Field ID/Field Type
Standard	jobTitle
	applicationDate
	lastModified
	reviewDate
	statusId
	jobsApplied
	interviewResult
Custom	Date
	Percent
	Boolean
	Number

Field	Field ID/Field Type
	Instruction
	Currency

23.1.2 Prerequisites for Purging Applications and Candidate Profiles

Understand the prerequisites for using candidate and application purge with DRM 2.0.

Action	Description
Choose a method to calculate application age.	Go to *Provisioning* > *Company Settings* and enable *DRM 2.0 Application Purge: Use Application Disposition date to start the Application aging for purge (Default is Application last modified date)* option to calculate the age of an application. (The disposition date is the date the application moved into a Disqualified category status). If this option is not enabled, the last modified date of the application is used to calculate the age of the application.
Configure the scheduled anonymization job.	This job actually anonymizes the data, and so must be configured. Go to *Provisioning* > *Managing Job Scheduler* > *Manage Scheduled Jobs*. Click *Create New Job* and select the job type as *RCM Entity Anonymization Job*.
Enabling Data Retention Management	Enabling Data Retention Management [page 12]

23.1.3 Applications Purge in Recruiting Management

Purging application in Recruiting Management for Data Retention Management includes configuring legal obligation period, scheduling anonymization job, and creating a purge request.

Configuring Legal Obligation Period [page 43]
The legal obligation period is the minimum duration applicant data is retained in the system.

Scheduling Anonymization Job for Applications [page 44]
Configuring scheduled anonymization job anonymizes the application data.

[Creating an Application Purge Request [page 45]]
To purge the applications in Recruiting Management, you must create the purge request in Data Retention Management.

[Application Purge Behavior [page 46]]
Applications are purged in the Recruiting Management using DRM 2.0 based on their status as defined in the table.

23.1.3.1 Configuring Legal Obligation Period

The legal obligation period is the minimum duration applicant data is retained in the system.

Context

Legal obligation period is applicable in the following scenarios:

- Internal candidate deleted through inactive user purge routine
- Disqualified applications of the internal candidate deleted through Inactive user purge routine
- Disqualified applications of candidates deleted through RCM Entity Anonymization Job

> ⓘ Note
>
> Applications are marked as *Disqualified*, when they are manually moved into any of the *Disqualification Statuses* configured in the system.

In these situations, the data is retained for the minimum period required for the country. For applications, the legal obligation country is validated against the requisition country. For candidate profiles, the legal obligation is validated against the candidate profile country.

Procedure

1. Go to *Admin Center* > *Configure Minimum Legal Obligation Period*.
2. Create the retention period in days for each country.

   You can configure a legal minimum obligation period for all countries, then different periods for individual countries. Individual country setting overrides the **all country** settings.

   > ⓘ Note
   >
   > Do not configure the retention period as one day. If the legal minimum obligation period is configured this way, the entire date of the customer gets purged.
   >
   > Fill in the *companyExitDate* field to ensure that the legal obligation period calculates correctly when purging internal candidates using Inactive User Purge routine.

> If legal obligation period is missing for the country, the corresponding data of disqualified applications is not purged.
>
> If Employee Central is enabled in the company, best practice is to add the *companyExitDate* standard element to the *hris-sync-mappings* section in the Succession Data Model.

Task overview: Applications Purge in Recruiting Management [page 42]

Related Information

Scheduling Anonymization Job for Applications [page 44]
Creating an Application Purge Request [page 45]
Application Purge Behavior [page 46]

23.1.3.2 Scheduling Anonymization Job for Applications

Configuring scheduled anonymization job anonymizes the application data.

Procedure

1. Go to *Provisioning* > *Managing Job Scheduler* > *Manage Scheduled Jobs* and click *Create New Job*.
2. Select the Job Type as *RCM Entity Anonymization Job*.
3. Enter the job name, owner, and the schedule details for the job.

   > Note
   >
   > It is best practice to configure the job to run daily.
4. Click *Submit Job*.

Task overview: Applications Purge in Recruiting Management [page 42]

Related Information

Configuring Legal Obligation Period [page 43]
Creating an Application Purge Request [page 45]
Application Purge Behavior [page 46]

23.1.3.3 Creating an Application Purge Request

To purge the applications in Recruiting Management, you must create the purge request in Data Retention Management.

Procedure

1. Go to *Admin Center* > *Data Retention Management*.
2. Select the following options for the purge request:

<table>
<tr><th>Purge request option</th><th>Value</th></tr>
<tr><td>Purge request type</td><td>Purge inactive Job applications</td></tr>
<tr><td>Name of the purge request</td><td>Purge inactive Job applications</td></tr>
<tr><td>Define Purge Criteria</td><td>You have two options to define the purge criteria:
1. Job Applications Based on the Retention Period
This request type purges all the job applications after the configured retention time has passed. That's when the job applications become inactive. Use this option to purge all the job applications that became inactive after this request was last run.
Select the country/region for which you want to purge the inactive job applications. Configure inactivity period by defining the number of days of inactivity for each country.
2. Selected Job Applications
This request type anonymizes the sensitivie data on a list of job applications that was missed during the initial anonymization. Upload a CSV file with the list of job application IDs that have been anonymized already. You can upload a maximum of 10,000 records per request.
Use this option when you:
• Set a field in the job application template to <code>anonymize="true"</code> from <code>anonymize="false"</code> after the job applications have been anonymized.
• Change your configuration for Deletion of Correspondence under Manage Recruiting Settings in admin center.
If your CSV file contains job application IDs that weren't anonymized earlier, those records will be rejected as part of the purge request. You can check the job logs from the Purge Request Monitor admin tool.</td></tr>
</table>

Purge request option	Value
Add approvers	Enter the approver name.

3. Click *Launch Immediately* to launch the purge request immediately or click *Save* and schedule it for the later time. If you've created the purge request for *Selected Job Applications*, then you cannot save or schedule the request. You can only launch it immediately.

   To access the list of applications that are picked for purge, go to *Admin Center* > *Purge Request Monitor*. The Admins can approve the purge request, upon which, the applications are purged.

   > Note
   >
   > If the candidate is in purge freeze, the candidate or the permissioned user cannot delete profile or decline DPCS statement. The candidate must be removed from purge freeze for these actions to be completed.

Task overview: Applications Purge in Recruiting Management [page 42]

Related Information

Configuring Legal Obligation Period [page 43]
Scheduling Anonymization Job for Applications [page 44]
Application Purge Behavior [page 46]

23.1.3.4 Application Purge Behavior

Applications are purged in the Recruiting Management using DRM 2.0 based on their status as defined in the table.

When the Status Group is...	And the Status Name is...	Result
Withdrawn Statuses	Deleted on Demand By Candidate Deleted On Demand By Admin Declined DPCS	The Candidate is purged and the application is marked to be picked up by the next run of the RCM Entity Anonymization job. On running the job, Applications that marked for anonymization are anonymized except for **Disqualified Applications**. Applications in disqualified statuses are anonymized based on *Legal Minimum Obligation Period (LMOP)* settings.

When the Status Group is...	And the Status Name is...	Result
	Withdrawn By Candidate	The applications in the Withdrawn status are purged by the *Purge Inactive Job Applications* purge request as per the retention period.
In-Progress Statuses	Any	The applications are not purged.
Forwarded Statuses	Forwarded	The applications are purged as part of the *Purge Inactive Candidate* purge request.
	Invited To Apply	
System Statuses	Default	Applications are not purged.
	Requisition Closed	Applications will be purged only if the *Manage Recruiting Settings* > *DRM and DRTM Purge Settings* > *Consider job applications with the status "Requisition Closed" for purging* option is enabled.
	Hired On Other Requisition	Applications are purged only if the *Manage Recruiting Settings* > *DRM and DRTM Purge Settings* > *Consider job applications with the status "Hired On Other Requisition" for purging* option is enabled.
	Auto Disqualified	The applications in the Auto Disqualified status are purged by the *Purge Inactive Job Applications* purge request as per the retention period.
OnBoard Statuses	Any	The applications in the Onboarded Statuses are purged by the *Purge Inactive Job Applications* purge request as per the retention period.

When the Status Group is...	And the Status Name is...	Result
Disqualification Statuses	Any	The applications in the Disqualified Statuses are purged by the *Purge Inactive Job Applications* purge request as per the retention period. Note For an application to be purged, it must to be in Disqualification status. To move applications in bulk to a Disqualification status, you can use the ODATA batch Upsert on the Job Application entity.

> Note
>
> The behaviour explained in the preceding table is applicable only to purge requests created for job applications to be purged based on the retention period. It isn't applicable to the purge requests created for the *Selected Job Applications* option, which considers only anonymized job applications.

Parent topic: Applications Purge in Recruiting Management [page 42]

Related Information

Configuring Legal Obligation Period [page 43]
Scheduling Anonymization Job for Applications [page 44]
Creating an Application Purge Request [page 45]

23.1.4 Candidate Purge in Recruiting Management

Candidate profiles can be deleted manually or by creating a Purge request in Data retention management.

When the candidate profile is purged, disqualified applications of the candidate are not moved to *Deleted on Demand by Candidate* status. The disqualified applications are purged as per the data retention period defined in the system.

To ensure that the candidate is aware of this, it is recommended that customers mention in their Data Privacy Consent Statement that applications are retained in the system even after the candidate profile has been anonymized. Retaining such unsuccessful or disqualified applications helps to record that the applications were rejected fairly and not due to a bias.

It is also recommended that the Data Privacy Consent Statement should indicate which data is not purged and for how long it is retained.

[Deleting a Candidate Profile Manually in Recruiting Management [page 49]]
Deleting a Candidate Profile manually is purging the candidate and marking the application so that the **RCM Entity Anonymization** job picks it up in the next run.

[Purging the Candidate Profile in Recruiting [page 49]]
To purge the candidate profile in Recruiting, you must create the purge request in Data Retention Management.

[Candidate Purge Behavior [page 51]]
Scenarios where candidate is not purged.

23.1.4.1 Deleting a Candidate Profile Manually in Recruiting Management

Deleting a Candidate Profile manually is purging the candidate and marking the application so that the **RCM Entity Anonymization** job picks it up in the next run.

Context

Candidate profiles can be deleted manually by the following actions:

- Candidate profile Deleted on Demand By Candidate.
- Candidate profile Deleted on Demand By Admin.
- Candidate declined DPCS.

23.1.4.2 Purging the Candidate Profile in Recruiting

To purge the candidate profile in Recruiting, you must create the purge request in Data Retention Management.

Context

Inactive candidates can be purged by creating a purge request in Data Retention Management. Inactive candidates are candidates who haven't logged in to their accounts for the number of days configured as the inactivity period.

For customers who don't want to lose candidate data by way of the purge action, they can contact the candidates via e-mail asking them to activate their accounts by logging in to the system. It is possible to configure the number of days before the purge date, when e-mail alerts are triggered to notify inactive candidates to take action before their profiles are purged.

> **Note**
>
> These e-mail notifications are not triggered for candidates who have not accepted the Data Privacy Consent Statement (DPCS) for the configured retention time.

Procedure

1. Go to *Admin Center* > *Data Retention Management*.
2. Select the following options for the purge request:

Purge request option	Value
Purge request type	Purge Inactive Candidate
Name of the purge request	Purge Inactive Candidate
Define Purge Rule	Select the country for which you want to purge the inactive job applications.
Configure Inactivity period	Define the number of days of inactivity for each country.
Notify candidates before	(Optional) Enter the number of days before the purge date, when e-mail alerts need to be sent to inactive candidates before their profiles are purged. These alerts are triggered only once for each candidate.
Add approvers	Enter the approver name.

3. If you have specified the number of days in the *Notify candidates before* field, perform the following actions:
    a. Go to *Admin Center* > *Recruiting Email Triggers*.
    b. Select the *Imminent Candidate Purge Notification* e-mail trigger and associate it with the appropriate e-mail template.

    > **Note**
    >
    > E-mail alerts aren't triggered if you haven't entered a numeric value in the *Notify candidates before* field, or if the *Imminent Candidate Purge Notification* e-mail trigger isn't configured. Further, e-mail alerts are sent to inactive candidates only for scheduled purge jobs. No e-mail alerts are triggered if purge requests are launched immediately.

4. Click *Launch Immediately* to launch the purge request immediately or click *Save* and schedule it for the later time.

    To access the list of candidates that are picked for purge, go to *Admin Center* > *Purge Request Monitor*. An administrator can approve the purge request, upon which, the candidates are purged.

Results

Once the purge request is launched, all the candidates who have not logged in for the configured retention time (*Inactivity Time Unit*) are purged.

23.1.4.3 Candidate Purge Behavior

Scenarios where candidate is not purged.

- For excluding external candidate profile from being purged in case the candidate has active applications, enable *Do not purge if there are existing applications in the system for that candidate* option from *Admin Center* > *Manage Recruiting Settings* > *DRM and DRTM Purge Settings*. With this option enabled, candidate profile is purged based on the status of the application that exists for the candidate in the following table:

If the Application Status is ...	Candidate profile ...
In-Progress	Is not purged.
Draft, Closed, Withdrawn, Disqualified	Is purged
Requisition Closed	Is purged, if the *Manage Recruiting Settings* > *DRM and DRTM Purge Settings* > *Consider job applications with the status "Requisition Closed" for purging* option is enabled.
Hired On Other Requisition	Is purged, if the *Manage Recruiting Settings* > *DRM and DRTM Purge Settings* > *Consider job applications with the status "Hired On Other Requisition" for purging* option is enabled.

- For excluding internal user from being purged, enable *User has non-anonymized applications* option from *Admin Center* > *Data Retention Management* > *Create New Purge Request* > *Exclude users from the following purge criteria*.

24 Auto Data Purge

An automatic data purge process is used in your SAP SuccessFactors HCM suite instances to optimize cloud storage and improve data storage efficiency of your instances.

Auto Data Purge processes three types of data and supports custom configuration. Weighing the impact of purging data against the storage cost for data retained, you can choose which type of data to be purged and set the retention period based on your business needs.

Purge jobs are scheduled to run monthly. You can find information of the latest purge jobs for each data type in *Data Retention Management* > *Auto Data Purge*.

Default Configuration

In production, test, development, and sales demo instances, all data types aren't selected to be purged by default.

In preview instances, default configurations are different for data types:

- *Documents* are selected by default. You can configure the retention period or choose not to purge this data type.
- *Audit Data Containing Personally Identifiable Information* isn't selected by default.
- *Audit Data Without Personally Identifiable Information* is selected to be purged. You can't make your own configuration of this data type.

Related Information

Configuring Auto Data Purge [page 57]
Impacts of Auto Data Purge [page 53]

25 Impacts of Auto Data Purge

Review the impacts of *Auto Data Purge* before you decide which type of data to be purged.

Mandatory retention periods are set by module teams to guarantee that the system runs smoothly. The actual retention period implemented in the purge process is the longer one between the custom retention period you configured and mandatory retention periods listed in the following table.

Impacts of Documents Purge

Documents are replaced by an empty file when they exceed the set retention periods. The file contains a reminder: "The document that you’re trying to access has been removed from the system." The base date for retention period calculation is the upload date of documents.

> **Note**
>
> If you use a third-party storage vendor (for example: OpenText) to store attachments, these documents aren't affected by *Auto Data Purge*.

Product Name	Attachment	Mandatory Retention Period
Recruiting Management	Resume and cover letter attachments of candidates **Note** You can't find candidate by searching with keywords that were in the resume. Resume Carousel displays the replacement file instead of the original resume.	180 days
Performance Management	Attachments in the Supporting Information pod on the form	180 days
Continuous Performance Management	Continuous Performance Management (CPM) attachments to 1-to-1 meetings (and Performance Reviews if the CPM activities are linked to Goals).	180 days
Calibration	Attachments in the session list page	365 days
Career Development Planning	Learning certificates for custom learning activities	180 days

Product Name	Attachment	Mandatory Retention Period
Metadata Framework	Attachments in object instances whose attachment field is given the value *GENERIC_OBJECT* for the *Module* attribute in *Attachment Field Configuration* **Note** *GENERIC_OBJECT* is the default value for all attachment fields if no specific configuration is made. This default value is applicable for predelivered objects as well.	180 days

Impacts of Audit Data Containing Personally Identifiable Information

Product Name	Impact Description	Mandatory Retention Period
Metadata Framework (MDF)	Entries for person-related and nonperson-related MDF objects in the following **change audit reports** are limited to those valid in the retention period: • *MDF Configuration Data* in configuration data reports • *MDF Change History Data* in business data reports • *Person Search* in personal data reports for person-related MDF objects	365 days
Reporting	Entries in the Table report created using the *Report Execution Audit* and *Report Event Audit* domains are limited to those valid in the retention period.	30 days

Impacts of Audit Data Without Personally Identifiable Information

Product Name	Impact Description	Mandatory Retention Period
Role-Based Permission	The *View change history* content in *Manage Permission Groups* or *Manage Permission Roles* is limited to the retention period.	30 days

Product Name	Impact Description	Mandatory Retention Period
Performance Management	For Performance Management forms that are in progress or completed in the retention period, no audit data is purged and you can use form features as usual. For Performance Management forms that were completed outside of the retention period, we don't recommend that you route those forms back to the Modify stage.	90 days
Goal Management	Audit entries are available in the *Audit History* table only when they're created within the retention period. The purge of audit records may result in the `AssignedFrom` field of an assigned team goal to be irretrievable.	90 days
API	Entries in the OData API Audit Log and SFAPI Audit log pages in *API Center* are limited to those valid in the retention period, or the maximum number of log entities configured in provisioning under *API Settings & Tools*, whichever is lower.	30 days
Onboarding 1.0	Entries in *Onboarding to Employee Central Mapping Audit Log* are limited to those valid in the retention period.	90 days
Calibration	In the Story and the Table reports, the values in the New Value and Old Value columns are limited to the retention period. Such limitation also applies to the notification emails of rating change.	90 days

Product Name	Impact Description	Mandatory Retention Period
Recruiting Management	The following data available from the Recruiting UI is purged after the retention period: • *Correspondence* section on the Application Workbench and Candidate Profile that stores the email content. • The history of changes for a candidate profile, application, and job requisitions. • *Application Status Audit Trail* section on the Application Workbench that stores the audit of the status change. • Search action logs that are captured as part of the candidate search for customers who enabled the OFCCP compliance in *Provisioning*, *Company Settings*, *Enable Candidate Search OFCCP compliance warning and auditing (for US-based job reqs)* • Audit of the status changes for job requisitions.	365 days

Related Information

Auto Data Purge [page 52]
Configuring Auto Data Purge [page 57]
View Change History of Role-Based Permission
Viewing API Audit Logs
How to Change the Attachment Field Configuration
Change Audit Reports for Metadata Framework Objects
Audit Log of Onboarding to Employee Central Mapping Tool

26 Configuring Auto Data Purge

Choose which type of data you want to purge automatically and set the retention period.

Prerequisites

- You have the permission to access *Data Retention Management*.
- You have enabled Metadata Framework.

Procedure

1. Go to *Admin Center* > *Data Retention Management* > *Auto Data Purge*.
2. Select which data you want to purge and set the retention period in days.

   > Note
   >
   > Default configurations are different depending on the type of instance.
3. Save your changes.

Results

Data you select is purged monthly when it exceeds an expected retention period. When the monthly purge job is completed, the purge history is shown under each data type to inform you when the auto purge process is implemented.

> Note
>
> Depending on the timing when you enable the purge, the status message might still show that no purge plan is implemented after the data is selected to be purged. The status message will change when the next monthly purge job is run.

Related Information

Auto Data Purge [page 52]
Impacts of Auto Data Purge [page 53]

Change History

Learn about changes to the documentation for Data Retention Management (Legacy and Non-DRTM) in recent releases.

> ⚠ Caution
>
> Read the Data Protection and Privacy Warning [page 7].
>
> This guide describes legacy, non-DRTM, and auto data purge functions. If you want to purge data covered by legacy purge functions, we recommend that you use the newer data purge solution (DRTM) described in the Data Protection and Privacy guide.

2H 2025

Type of Change	Description	More Information
November 7, 2025		
Updated	We updated the email notification behavior in cases where multiple users act on the same purge request.	Submitting a Legacy or Non-DRTM Purge Request for Approval [page 17]

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