SAP SuccessFactors

PUBLIC

Document Version: 2H 2020 – 2020-10-16

Data Retention Management (Legacy and Non-DRTM)

THE BEST RUN SAP

Content

What's New in Data Retention Management (Legacy and Non-DRTM)

A summary of recent changes to this guide.

> ⚠ Caution
>
> Read the Data Protection and Privacy Warning [page 11].
>
> 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 2020

What's New	Description	More Info
Auto Data Purge in Preview Instances Includes Attachments and More Audit Data	Audit data purged automatically in preview instances now includes attachments and audit data from more modules.	Impact of Auto Data Purge in Preview Instances [page 55]
Auto Data Purge in Preview Instances Supports Retention Period Configuration and Purging Process Monitoring	You can choose which data to be purged in your preview instance and set retention periods. You can check purge schedules under each data type.	Configuring Auto Data Purge in Preview Instances [page 58]

1H 2020

What's New	Description	More Info
April 10, 2020		
Purging candidate profiles	Minor edits to content	Purging the Candidate Profile in Recruiting [page 52]
April 3, 2020		
Legacy and non-DRTM purge requests	Add information about different types of purge requests helps you decide which type meets your data protection and privacy requirements.	Types of Purge Requests [page 10]

What's New	Description	More Info
Option to Purge System Identifiers of All Inactive Users in *User Permanent Purge*	You can now use the *Purge all inactive users* option in the *User Permanent Purge* to delete system identifiers of inactive users that are already purged using *Data Retention Management*.	Permanently Deleting Purged Users and User IDs [page 41]
New purge request types to purge MDF data (non-DRTM)	You can now use three new purge request types to purge MDF audit data, MDF business data, and MDF attachments (non-DRTM).	Purging MDF Data (Non-DRTM) [page 34]
Imminent Candidate Purge Notification	Advance e-mail notifications can be triggered in Recruiting to notify inactive candidates to take action before their profiles are purged.	Purging the Candidate Profile in Recruiting [page 52]
Audit Data Purge in Preview Instances	To optimize cloud storage and improve data storage efficiency, audit data in preview instances is purged when it exceeds its retention time.	Impact of Auto Data Purge in Preview Instances [page 55]

Q4 2019

What's New	Description	More Info
Assignment ID	You can now use either User ID or Assignment ID to identify users when you upload a list of people to include in an Inactive User Purge request.	Purging Inactive Users with the Legacy Purge Request (Non-DRTM) [page 37]
Permanent purge	Add information about how to use the *User Permenant Purge* option.	Permanently Deleting Purged Users and User IDs [page 41]
Controlling access to data purge functions	Add information about how to use role-based permission to control access to data purge functions, including both the newer DRTM function and the older legacy function.	Recommended Permission Settings for Data Purge Functions [page 14]
Purging completed to-do items	Add *Purge Completed To-Do Items* to the list of legacy purge requests types.	List of Legacy and Non-DRTM Purge Requests Types [page 9]
Simplified organization	Simplified content structure and removed duplicate information to make this guide easier to read.	N/A

Q3 2019

What's New	Description	More Info
Legacy Purge for Recruiting	Added information about the legacy purge types Inactive Candidate and Inactive Application for SAP SuccessFactors Recruiting.	Using Legacy Data Purge for Recruiting Management Data [page 43]

Q2 2019

What's New	Description	More Info
Deleting purge reports	You can now delete preview reports and complete reports from the Purge Request Monitor page when they're no longer needed. Purge reports can contain personal information so you may need to periodically remove them from storage, for data protection and privacy.	Deleting Old Purge Reports [page 33]

Q1 2019

What's New	Description	More Info
No changes	We didn't update the guide in this period.	N/A

Q4 2018

What's New	Description	More Info
Added a legacy purge request to delete Variable Pay forecast results	You can now purge the completed forecast bonus results of a Variable Pay plan template using the *Purge Variable Pay Forecast Data* option.	List of Legacy and Non-DRTM Purge Requests Types [page 9]

What's New	Description	More Info
Added a note about purging inactive users from Compensation worksheets	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	Purging Inactive Users with the Legacy Purge Request (Non-DRTM) [page 37]

1 Data Purge

The SAP SuccessFactors HXM 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 HXM 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).

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

Data Protection and Privacy Warning [page 11]

Legacy Purge Requests (without DRTM)

Purge Request Type
Purge Inactive User
Purge PM or SM Data
Purge Learning Activity
Purge Development Objective
Purge Career Worksheet
Purge Calibration
Purge Objective
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 HXM 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 HXM 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 HXM 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 data purge function may not meet all of your data protection and privacy requirements. It does not cover data across the full HXM Suite and does not enable you to configure data retention times.
- If you use the legacy *Purge Inactive Users* function, some module data may remain in the database. It does not purge data across the full HXM Suite.
- If you use the legacy *Purge Inactive Users* function, it is not a permanent purge. It only performs a "soft delete" and you still need to manually trigger the *User Permanent Purge* function separately.
- There is no validation logic in the legacy *User Permanent 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 11]

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 initiates 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 9]

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 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. 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* > *Tools* > *Data Retention Management* and click 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 should occur.
   - If you want to create a one-time purge request that begins as soon as it's approved, click *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, click *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

- Specified approvers are notified by email.
- If you selected *Launch Immediately*, the preview report is generated immediately and is available for approvers to review.
- If you selected *Schedule*, the purge request must be approved twice. Approve it once to generate a preview report, at the next scheduled recurrence time after it's approved the first time. Approve it a second time to begin the actual purge process, at the next scheduled recurrence time after it's approved the second time.

Next Steps

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

12 Generating the 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 are designated as an approver of the purge request.

Context

Only scheduled purge requests require a separate approval to generate a preview report. After reviewing the preview report, you have to approve again to start the purge process.

For immediate purge requests, you do not need to complete this step. The preview report is generated immediately after it is submitted and you only need to approve once to start the purge process.

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

Procedure

1. Go to *Admin Center* > *Tools* > *Purge Request Monitor*.
2. Click the *Scheduled Requests Awaiting Approval* tab and locate the purge request that needs approval.
3. Expand the *Criteria* section to review the purge request set-up.
4. Click *View Schedule* to review when the purge request is set to recur.
5. Click *Approve* to generate a preview report.

Results

After the purge request is approved, a purge preview report is generated at the scheduled time.

> **i** Note
>
> Approving a purge request on the *Scheduled Requests Awaiting Approval* tab does **not** run the actual purge job. It only generates a preview report. When the preview report is available, it is visible on the *Requests Awaiting Approval* tab.

Next Steps

Specified approvers must approve the purge request.

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.

> **i 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* > *Tools* > *Purge Request Monitor*.
2. Click the *Requests Awaiting Approval* tab and locate the purge request you want to review.
3. Expand the *Criteria* section to confirm the purge set-up is correct.
4. Click *Download Preview Report* to download the preview report in a ZIP file.
5. Open the downloaded archive and review its contents.

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.

> **i 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

Approve or decline a purge request. As designated approver, your approval is required 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 are designated as an approver of the purge request.
- You have reviewed the purge preview report.

Context

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

Procedure

1. Use the link in your email notification or log in and go to *Admin Center* > *Tools* > *Purge Request Monitor*.
2. Click the *Requests Awaiting Approval* tab and locate the purge request that needs approval.
3. Either approve or deny the request.
    - Click *Approve* to approve the request so that the purge process can proceed.
    - Click *Decline* to decline the request and stop the purge process.

Results

After a purge request is approved by **all** designated approvers, the purge process can proceed.

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.

15 Verifying Final Purge Results

Review a complete final purge report after the purge job has completed to verify that data was purged successfully.

Prerequisites

- You have permission to create or approve purge requests.

Procedure

1. Go to *Admin Center* > *Tools* > *Purge Request Monitor*.
2. Click the *Approved Requests* tab.
3. Click *View History* for the relevant purge request.
4. In the *View History* dialog, you can view the number of successful, filtered, and failed records affected by the purge.
5. Click *Download Complete Report* to download the complete report in a ZIP file.
6. 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 Cloud 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 Cloud 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 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.

> ⚠ 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* > *Approved Requests*.
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.

18 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.

Procedure

1. Go to *Admin Center* > *Tools* > *Purge Request Monitor* > *Approved Requests*.
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.

19 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.

  > ℹ 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.

  > **i 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.

  > **i 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.

   > **i 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)

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

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

20 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 HXM Suite.
- You have *Create Legacy Data Purge Request* permission.
- You have *Manage Users* permission for the relevant target population.

> **i** Note
>
> To completely remove user accounts and basic user information from the system, the user who initiates 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 *User Permanent Purge* option.

Procedure

1. Go to *Admin Center* > *Data Retention Management* > *Create New Purge Request*.
2. Create a *Purge Inactive User* and define the users whose data you want to purge, as you would for any purge request.
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.

> **i** 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 *User Permanent Purge* function to manually complete the purge process by deleting these identifiers as well.

> **i Note**
>
> The *User Permanent 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 *User Permanent Purge* option because they want to reuse old user IDs for different users. Although this is **not** a leading practice, it's possible if required by your business.

Inactive User Purge (Non-DRTM) [page 38]
Use the legacy *Inactive User Purge* to remove inactive users from the system.

Permission Required for Purging Inactive Users [page 39]
To purge inactive users with *Data Retention Management*, you need *Manage Users* permission for the target population who is included in the purge.

20.1 Inactive User Purge (Non-DRTM)

Use the legacy *Inactive User Purge* to remove inactive users from the system.

> **⚠ 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 HXM Suite that is associated with the inactive users. It does not consider any configured retention time.

> **i 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 37]

Related Information

Permission Required for Purging Inactive Users [page 39]
Permission Required for Purging Inactive Users [page 39]

20.2 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 initiates 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 37]

Related Information

Inactive User Purge (Non-DRTM) [page 38]

21 Permanently Deleting Purged Users and User IDs

Use *System Identifier Purge* to completely purge the inactive users, including system identifiers such as User ID.

Prerequisites

- You have successfully purged inactive users with the *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.

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.

   > **i 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

The specified user accounts are permanently deleted from storage, including internal system identifiers such as User ID.

22 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.

22.1 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.

> i 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 44]

22.1.1 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 Type	Field
Standard	dateOfAvail
	minAnnualSal
	currency
Custom	Date
	Percent
	Boolean
	Number
	Instruction
	Currency
Background data fields	Date
	Int
	Float

Application fields that do not support anonymization

Field Type	Field
Standard	jobTitle
	averageRating
	applicationDate
	lastModified
	reviewDate
	source
	statusId
	referralSource
	jobsApplied

Field Type	Field
	availability
	minAnnualSal
	bkgrndChkAttachment
	formerEmployee
	startDate
Custom field types	Date
	Percent
	Boolean
	Number
	Instruction
	Currency

22.1.2 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.

Action	Description
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 for Recruiting Management [page 46]

22.1.2.1 Enabling Data Retention Management for Recruiting 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.

Next Steps

Grant the relevant permissions for *Data Retention Management* to the appropriate roles in your company:

- Go to *Admin Center* > *Manage Permission Roles* > *[select role]* > *Permissions* > *Administrator Permissions* > *Manage Data Purge*.
- DRM has two permission options. Select one or both the options.
  Create Legacy Data Purge Request option allows a user to configure country-specific purge rules in Admin Center.
  Manage and Approve Legacy Data Purge Request option allows a user to approve purge requests submitted to an administrator.
- To completely and permanently remove inactive users from the system, using either purge function, also grant *Manage Users* permission to the appropriate roles and target populations.

22.1.3 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 47]
The legal obligation period is the minimum duration applicant data is retained in the system.

Scheduling Anonymization Job for Applications [page 48]
Configuring scheduled anonymization job anonymizes the application data.

Creating an Application Purge Request [page 49]
To purge the applications in Recruiting Management, you must create the purge request in Data Retention Management.

Application Purge Behavior [page 49]
Applications are purged in the Recruiting Management using DRM 2.0 based on their status as defined in the table.

22.1.3.1 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.

22.1.3.2 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*.

22.1.3.3 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:

Purge request option	Value
Purge request type	Purge inactive Job applications
Name of the purge request	Purge inactive Job applications
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.
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.

   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.

> **i 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.

22.1.3.4 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	The Candidate is purged and the application is marked to be picked up by the
	Deleted On Demand By Admin	

When the Status Group is...	And the Status Name is...	Result
	Declined DPCS	next run of the RCM Entity Anonymization job.
	Withdrawn By Candidate	The applications in the Withdrawn status are purged by the DRTM Inactive Application Purge 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 DRTM Inactive Candidate Purge.
	Invited To Apply	
System Statuses	Default	Applications are not purged.
	Requisition Closed	Applications will be purged only if the *Manage Recruiting 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* > *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 DRTM Inactive Application Purge as per the retention period.
OnBoard Statuses	Any	The applications in the Onboarded Statuses are purged by the DRTM Inactive Application Purge 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 DRTM Inactive Application Purge as per the retention period. **i 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.

22.1.4 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 52]
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 52]
To purge the candidate profile in Recruiting, you must create the purge request in Data Retention Management.

Candidate Purge Behavior [page 53]
Scenarios where candidate is not purged.

22.1.4.1 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.

22.1.4.2 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.

> **i** 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.

   > **i** 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.

22.1.4.3 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 2.0 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* > *Consider job applications with the status "Requisition Closed" for purging* > option is enabled.
Hired On Other Requisition	Is purged, if the *Manage Recruiting 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* >.

23 Impact of Auto Data Purge in Preview Instances

Learn about the impact of auto data purge in preview instances.

Background

To optimize cloud storage and improve data storage efficiency, audit data and attachment in preview instances are purged automatically when they exceed their retention periods. A retention period is implemented as the minimum requirement for each kind to guarantee no impact on your business workflow. You can decide which data you want to keep and for how long.

> **i** Note
>
> Data in your production instances isn't affected.

> **i** Note
>
> You may find data available in your instance for a longer period than the retention period listed. It is because we implement a longer retention period in the 1H 2020 release and schedule the purge in phases. You can find implementation schedule for each data type in *Data Retention Management* > *Auto Data Purge*.

Impact of Non-Person Related Audit Data Purge

Product Name	Impact Description	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
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

Product Name	Impact Description	Retention Period
Goal Management	Audit entries are available in the *Audit History* table only when they're created within the retention period.	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

Impact of Person Related Audit Data Purge

Product Name	Impact Description	Retention Period
Metadata Framework (MDF)	Entries for person-related and non-person 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* reports created using the *Report Execution Audit* and *Report Event Audit* domains are limited to those valid in the retention period.	30 days

Impact of Attachment Purge

Attachment files are replaced by a file named *removed* 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.".

Product Name	Attachment	Retention Period
Recruiting	Resume and cover letter attachments of candidates **i 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
Calibration	Attachments in the session list page	365 days
Career Development Planning	Learning certificates for custom learning activities	180 days
Metadata Framework	Attachments in object instances whose attachment field is given the value *GENERIC_OBJECT* for the *Module* attribute in *Attachment Field Configuration* **i Note** *GENERIC_OBJECT* is the default value for all attachment fields if no specific configuration is made. This is applicable for predelivered objects as well.	180 days

Related Information

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

24 Configuring Auto Data Purge in Preview Instances

Choose which data you want to purge automatically in your preview instances and set the retention period. Data is purged periodically.

Prerequisites

- You are in a preview instance.
- You have the permission to access *Data Retention Management*.
- You have enabledMetadata Framework.

Context

To optimize cloud storage and improve data storage efficiency, audit data and attachment in preview instances are purged automatically when they exceed their retention periods. A retention period is implemented as the minimum requirement for each kind to guarantee no impact on your business workflow. You can decide which data you want to keep and for how long.

> **i** Note
>
> Data in your production instances isn't affected.

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.

   > **i** Note
   >
   > - *Non-Person Related Audit Data* in all preview instances are to be purged. You can't make your own configuration of this data type.
   > - *Person Related Audit Data* isn't selected by default. You can select it and enter a retention period based on your need.
   > - *Attachment* is selected by default. You can configure the retention period or choose not to purge this data type.
3. Save your changes.

Results

Data you select is purged periodically when it exceeds the retention period you set. Purge plan is shown under each data type to inform you when the auto purge process is implemented.

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 a 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.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

www.sap.com/contactsap

THE BEST RUN SAP