



PUBLIC

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

# Creating Change Audit Reports

# Content

<b>1</b>	<b>Change Audit.</b>	<b>4</b>
1.1	Change Audit Use Cases.	5
1.2	Trigger-Based Audit.	6
1.3	Other Audit Capabilities.	7
<b>2</b>	<b>Important Notes About Change Audit.</b>	<b>9</b>
<b>3</b>	<b>Retiring Scheduled Job for Provisioning Change Audit.</b>	<b>10</b>
<b>4</b>	<b>Limitations of Change Audit.</b>	<b>11</b>
<b>5</b>	<b>Enabling Change Audit.</b>	<b>12</b>
<b>6</b>	<b>Process for Generating Change Audit Reports.</b>	<b>14</b>
6.1	Creating a Change Audit Report.	15
	Importing a PGP File Encryption Key.	18
	Configuring SFTP Settings for a Recurring Change Audit Report.	19
6.2	Downloading a Change Audit Report.	21
6.3	Interpreting a Change Audit Report.	22
6.4	Viewing or Deleting Recurrence Schedules for Change Audit Reports.	23
<b>7</b>	<b>Using Change Audit for SAP SuccessFactors Compensation</b>	<b>25</b>
7.1	Enabling Permission to Export Compensation Plan Audit Data.	25
7.2	Downloading Compensation Audit Reports.	26
	Exporting Audit Reports for Worksheets.	27
	Exporting Audit Reports For Employees.	28
7.3	Creating Reports with Promotion-Based Information.	28
<b>8</b>	<b>Standard Data Included in All Change Audit Reports.</b>	<b>30</b>
<b>9</b>	<b>Change Audit Reports.</b>	<b>33</b>
9.1	Personal Data Audit Reports.	33
	Employee Central Data in Personal Data Audit Reports.	34
9.2	Configuration Data Audit Reports.	36
	RBP Role Change Report.	38
	RBP Group Change Report.	40
	RBP Static Group Membership Change Report.	42
	RBP User Role Change Report.	43
	Proxy Assignment Change Report.	44
	Feature Settings Audit Report.	47

	Employee Central Feature Settings Audit Report. . . . .	51
	MDF Configuration Data Report. . . . .	54
	Job Scheduler Requests Report. . . . .	55
	Change Audit for Locales and Customizations. . . . .	56
	Manage Support Access Change Report. . . . .	58
	Email Configurations Change Audit Report. . . . .	59
9.3	Business Data Audit Reports. . . . .	59
	User Change Report. . . . .	60
	MDF Change History Data Report. . . . .	61
	Employee Profile Data Change Report. . . . .	66
	Employee Central Object and Element Audit Configuration. . . . .	69
	Dynamic Teams Data Change Report. . . . .	76
	Objectives and Key Results Data Change Report. . . . .	78
9.4	Change History in Data Retention Management. . . . .	83
<b>10</b>	<b>Change History. . . . .</b>	<b>92</b>

# 1 Change Audit

Change auditing capabilities enable you to track changes that have been made to different kinds of data in your system. You can audit changes to personal data, system configuration, or other business data.

If you enable change auditing in your system, we capture information about changes to the system in our audit logs. Then you can generate change audit reports, based on the data in our audit logs, as required by your business. Generated audit reports are available for download for 48 hours and then purged from storage.

Change audit reports tell you which data records were changed during a given period, what the change was, who changed them, and when. Changes are captured in logs whether they're made in the user interface, via API, or with an import file. Reports are available for many types of data, including personal data, configuration data, and other types of data in the HCM suite. Use the self-service audit reporting tool to create the most common reports directly from the Admin Center.

## Changes to Personal Data

Personal data is subject to frequent changes. Use change audit reports to keep track of changes to an employee's personal data and comply with your organization's data protection and privacy policy.

You can create change audit reports to track changes to personal data across the SAP SuccessFactors HCM suite, including:

- Changes made **about** a specific user's personal data (changes made by anyone to John's personal data)
- Changes made **by** a specific user **to** other people's personal data (changes made by John to anyone else's personal data)

### Note

Change audit includes all changes to personal data fields, including insertions, updates, or deletions.

## Changes to Other Data

Your SAP SuccessFactors system contains more than just personal data. It includes other types of data, such as configuration data or transactional business data. Use change audit reports to keep track of changes to your system, build proper internal controls, and ensure data security.

You can create change audit reports on wide range of data types from across the SAP SuccessFactors HCM suite, including:

- Role-based permissions
- Proxy assignments
- Basic and extended user information
- Feature settings

### [Change Audit Use Cases \[page 5\]](#)

Learn about some business scenarios that might require a change audit.

### [Trigger-Based Audit \[page 6\]](#)

Trigger-based auditing introduces new audit capabilities covering data across the HCM suite, with greater self-service reporting.

### [Other Audit Capabilities \[page 7\]](#)

If the [Change Audit Reports](#) page doesn't include the data you need, there may be other ways to conduct an audit. Try using other reporting or auditing capabilities in the HCM suite instead.

## Related Information

[Important Notes About Change Audit \[page 9\]](#)

[Limitations of Change Audit \[page 11\]](#)

[Change Audit \[page 4\]](#)

[Enabling Change Audit \[page 12\]](#)

[Change Audit Reports \[page 33\]](#)

## 1.1 Change Audit Use Cases

Learn about some business scenarios that might require a change audit.

### Compliance

You may be required to produce change audit reports on certain types of data in order to comply with legal or regulatory requirements. For example, you might need to audit changes to personal data due to data protection and privacy requirements. Or you may need audit reports to demonstrate internal business controls on other types of changes, such as to financial data.

For data protection and privacy, we provide self-service change audit reports on personal data across the HCM suite.

For other types of compliance, we provide change audit reports on a wide variety of data, for different audit use cases.

### Data Security

The security of data in your system is governed by extensive role-based permissions. To ensure that permissions are managed properly in your system, you can audit changes to role-based permission and proxy settings.

We provide change audit reports for permission roles, permission groups, user role assignments, and proxy management settings.

## Intrusion Detection

Change audit reports can help you detect unexpected changes to your system and identify the source of the changes. You can use information in the report to determine whether the change was appropriate and if preventative action is required.

We provide a change audit report on Provisioning settings, which enables you to track changes made to your system configuration by people outside your company, such as Technical Support or implementation partners.

## Data Recovery

You can use change audit reports to recover data or configuration settings that were changed accidentally. You can use the reports to determine what data was changed when and see both the old and new value. You can use this information to restore the old value if necessary.

We provide change audit reports that can be used for this purpose, on a wide variety of data across the HCM suite.

**Parent topic:** [Change Audit \[page 4\]](#)

## Related Information

[Trigger-Based Audit \[page 6\]](#)

[Other Audit Capabilities \[page 7\]](#)

## 1.2 Trigger-Based Audit

Trigger-based auditing introduces new audit capabilities covering data across the HCM suite, with greater self-service reporting.

Our audit solutions are now based on database triggers. That means certain operations in your system "trigger" the recording of information about that operation in our audit logs. The captured audit data can be used later to create audit reports.

Our trigger-based change audit capability replaces an older, replication-based change audit (sometimes also known as "write audit"). Now, instead of replicating large amounts of audit data with no business purpose, the new trigger-based audit solution is designed to support specific, known business use cases. It also extends audit capabilities to customer systems using SAP HANA.

Parent topic: [Change Audit \[page 4\]](#)

## Related Information

[Change Audit Use Cases \[page 5\]](#)

[Other Audit Capabilities \[page 7\]](#)

## 1.3 Other Audit Capabilities

If the [Change Audit Reports](#) page doesn't include the data you need, there may be other ways to conduct an audit. Try using other reporting or auditing capabilities in the HCM suite instead.

For example, you can use the standard HCM suite reporting capabilities to generate reports that include change data. Some of our delivered reports may also contain change data that's relevant to your audit purposes.

For effective-dated entities, you can also check the Version History of a data record.

Here are some alternate audit capabilities for different solutions in the HCM suite that you can use instead of the [Change Audit Reports](#) page.

Solution	Description
Calibration	<p>You can use ad hoc reports to audit changes to Calibration Activity. The Calibration Activity ad hoc report records the change history of ratings in a calibration session.</p> <p><a href="#">Ad Hoc Reports for Calibration</a></p> <p><a href="#">Creating a Calibration Report in Report Center</a></p>
Compensation	<p>Compensation audit reports are made available when you enable the <a href="#">General Audit</a> setting. However, they require more set-up and are generated differently than other change audit reports.</p> <p><a href="#">Enabling Permission to Export Compensation Plan Audit Data [page 25]</a></p> <p><a href="#">Downloading Compensation Audit Reports [page 26]</a></p>
Employee Central	<p>You can use ad hoc reports to audit changes to Person and Employment information in Employee Central.</p> <p><a href="#">Ad Hoc Report Types for Employee Central</a></p>
Goal Management	<p>You can use ad hoc reports to audit changes to Goal Management.</p>
Performance Management (except Continuous Performance Management)	<p>You can use Audit Trail to audit changes to Performance Management forms and see who the form is routed to.</p> <p><a href="#">Audit Trail for Performance Management</a></p>

Solution	Description
Platform (API)	<p>You can enable audit log settings for OData API in Admin Center. You can use API audit logs to audit the request/response headers and payloads of API calls.</p> <p><a href="#">Audit Log Settings for OData API</a></p>
Succession & Development (except Mentoring)	<p>You can use ad hoc reports to audit changes to Nomination History in Succession Management, including all nominee status changes.</p> <p><a href="#">Succession Reporting Schemas</a></p> <p>You can view the Audit History (who created or modified a form) in Career Development Planning.</p>
User Management	<p>You can use ad hoc reports to create a <a href="#">Login Data</a> report that includes user login details.</p> <p><a href="#">Exporting Login Data with Ad Hoc Report</a></p>

**Parent topic:** [Change Audit \[page 4\]](#)

## Related Information

[Change Audit Use Cases \[page 5\]](#)

[Trigger-Based Audit \[page 6\]](#)



## 2 Important Notes About Change Audit

Before using the change audit function, here are some things to keep in mind.

- Audit reports are created by scheduled jobs. You'll be notified by email once the report is ready to view.
- Audit reports are automatically purged after 48 hours. Be sure to check the report you are interested in within 48 hours of generation and archive it if necessary. Otherwise, you may have to run it again.
- There is a total storage limit of 10 GB for reports. On the [Access Reports](#) tab, you can see the size of each report and how close you are to reaching the overall storage limit.
- You can use change audit to track changes made via a shared user account, using secondary login in the Provisioning application.  
SAP SuccessFactors allows you to set up shared users that can be accessed by multiple people for certain purposes, such as system maintenance or troubleshooting. For example, the `sfadmin` user is typically shared by multiple Technical Support representatives and accessed using the secondary login feature in Provisioning. We ensure that only one person at a time can log on to a shared user account using secondary login. For data protection and privacy, you can create audit reports that list all personal data that was accessed by a shared user account and the email address of the person that was logged on to the account at the time.
- Field values in change audit reports can't be more than 4000 characters. Longer values are truncated, so some changes may not be visible in the report. Try to limit the value of fields you need to audit to less than 4000 characters.

### Related Information

[Important Notes About Change Audit \[page 9\]](#)

[Limitations of Change Audit \[page 11\]](#)

[Change Audit \[page 4\]](#)

[Enabling Change Audit \[page 12\]](#)

[Change Audit Reports \[page 33\]](#)

### 3 Retiring Scheduled Job for Provisioning Change Audit

You no longer have to set up a scheduled job to log changes to Provisioning settings. Use the [Feature Settings Audit Report](#) instead.

Previously, you had to set up the scheduled job [BizX Audit Report \(RBP & Employee Profile\)](#) and then retrieve generated reports in your SFTP folder.

Now, you can set up a recurring [Feature Settings Audit Report](#) and save the output to your SFTP folder using the self-service change audit reporting tool.

Because it's no longer needed, the scheduled job [BizX Audit Report \(RBP & Employee Profile\)](#) has been retired. It's no longer available for scheduling.

# 4 Limitations of Change Audit

Learn about the current limitations of overall change audit functionality or of specific change audit reports.

Before using change audit, be aware of the following limitations:

- There's a limitation in the [Feature Settings Audit Report](#). Currently, it doesn't include changes to configuration fields, like the Company ID. It only includes on/off checkbox settings.
- Limitations to personal data reports are noted separately, in the [Data Protection and Privacy](#) guide.
- Compensation audit reports can't be set up with a recurrence schedule. You have to generate the report each time.

## Related Information

[Important Notes About Change Audit \[page 9\]](#)

[Limitations of Change Audit \[page 11\]](#)

[Change Audit \[page 4\]](#)

[Enabling Change Audit \[page 12\]](#)

[Change Audit Reports \[page 33\]](#)

# 5 Enabling Change Audit

Enable change audit logging so that authorized users can create audit reports tracking changes to different types of data.

## Prerequisites

You have both *View Read and Change Audit Configuration* and *Edit Read and Change Audit Configuration* permission.

## Context

### Note

This task is only necessary to enable change audit for the following solutions: Compensation (except Rewards and Recognition), Performance & Goals (except Continuous Performance Management), Succession & Development (except Mentoring), Employee Profile, User Management, Proxy Management, and Role-Based Permissions.

For other SAP SuccessFactors solutions, change audit reporting does **not** require this task because change audit is always enabled. These solutions include: Employee Central, Onboarding, Recruiting, Mentoring, Rewards and Recognition, and Continuous Performance Management.

## Procedure

1. Go to ► [Admin Center](#) ► [Manage Audit Configuration](#) ►.
2. On the [Change Audit](#) tab, switch on the [Change Audit](#) option.  
The [Personal Data Audit](#) option is switched on by default.
3. Switch the following options on or off, based on your audit requirements.

Setting	Description
<a href="#">Personal Data Audit</a>	Enable this option for data protection and privacy so that you can create change audit reports on personal data.
<a href="#">Configuration and Business Data Audit</a>	Enable this option for other audit purposes, so that you can create change audit reports for configuration and business data, such as configuration settings or user management.

4. Choose [Save](#).

You get a message telling you that the activation process has started. It usually takes about 24 hours.

5. Confirm that the activation process has completed successfully.

- Come back later to the [Manage Audit Configuration](#) page to verify that the toggle switch is enabled. If so, it means that the process is complete— but it doesn't guarantee the process was successful.
- Wait for an email notification to confirm if the process was successful or not. If it fails for some reason, follow instructions in the email to contact us for help.

## Results

Change audit logging is enabled for the following solutions: Compensation (except Rewards and Recognition), Performance & Goals (except Continuous Performance Management), Succession & Development (except Mentoring), Employee Profile, User Management, Proxy Management, and Role-Based Permissions.

## Next Steps

Give the [Generate Change Audit Reports](#) permission to the appropriate roles.

If you're using Career Site Builder, you may need to take additional steps.

### Note

Create Data Privacy Consent Statements using standard SAP SuccessFactors solutions for Recruiting. The [Career Site Builder](#) > [Settings](#) > [Data Privacy Consent Statements](#) option is available only if your Career Site Builder is **not** integrated with SAP SuccessFactors Recruiting.

# 6 Process for Generating Change Audit Reports

Use change audit reports to track changes in your system.

A wide variety of change audit reports are available, for different audit processes. For example, you can create change audit reports on changes to someone's personal data or a change audit report on changes to feature setting configuration.

Here's an overview of the process:

1. Create the type of change audit report you need.
2. Wait for the report to be generated. You're notified by email when the report is complete.

## Note

Change Audit data generated in the first day is only available after 8 am the next day in UTC. Depending on the time when the Change Audit data is generated, it's only available in 8 to 32 hours.

3. Download and save the report within 48 hours. After 48 hours, completed reports are purged from storage.
4. Interpret audit data in the report to understand the changes made in your system.

### [Creating a Change Audit Report \[page 15\]](#)

Create a change audit report to track changes in your system, such as changes to personal data or configuration settings.

### [Downloading a Change Audit Report \[page 21\]](#)

Download and save your Change Audit report when it is available so that you can investigate changes made in your system.

### [Interpreting a Change Audit Report \[page 22\]](#)

Learn how to read and interpret the data in a change audit report so that you can understand specific changes made to your system.

### [Viewing or Deleting Recurrence Schedules for Change Audit Reports \[page 23\]](#)

View a list of recurrence schedules, delete ones that are no longer needed, and check the status of completed recurring reports.

## 6.1 Creating a Change Audit Report

Create a change audit report to track changes in your system, such as changes to personal data or configuration settings.

### Prerequisites

- You've enabled the change audit function and the activation process has completed successfully.
- You have the [Generate Change Audit Reports](#) permission. Data Privacy Officers should have this permission.
- If you plan to set up a recurring schedule that saves reports to SFTP, be sure that you have the technical details required to set up the connection. If you plan to use file encryption, be sure that you've already imported your PGP public key on the [PGP Key Management](#) page.

### Context

You can use this procedure to audit changes to most types of data, but not Compensation configuration data. Compensation audit reports are generated and exported using a different procedure on the [Compensation Plan Activity Audit](#) page.

#### 📘 Note

Change Audit data generated in the first day is only available after 8 am the next day in UTC. Depending on the time when the Change Audit data is generated, it's only available in 8 to 32 hours.

### Procedure

1. Go to ► [Admin Center](#) ► [Change Audit Reports](#) ►.
2. Select the appropriate tab, based on your audit requirements.
  - Select [Create Personal Data Report](#) to create an audit report on changes to personal data across the HCM suite, for data protection and privacy.
  - Select [Create Configuration Data Report](#) to create an audit report on changes to configuration of your system.
  - Select [Create Business Data Report](#) to create an audit report on other types of changes.
3. Select the type of report you want to create.

A dialog opens where you can configure the report settings.
4. For a personal data report, specify the person you want to report on.

#### 📘 Note

When you choose [Person Search](#), you can create a change audit report for up to 10 users.

- To see changes to personal data about a specified employee, select [Change On Subject User](#) and use the [Person](#) search to specify the employee.
  - To see changes to personal data made by a specified employee, select [Change By User](#) and use the [Person](#) search to choose the employee.
  - To see changes to personal data about an external candidate, use the [External Candidate](#) search to specify the candidate.
  - To see changes to personal data about a new hire who is still in the onboarding process, for Onboarding 1.0 use the [Onboarder](#) search to specify the new hire.
  - To see changes to personal data about a new hire who is still in the onboarding process, for Onboarding use the [Person](#) search to specify the new hire.
  - To see changes to personal data about an external rater in Performance Management, use the [External User](#) search to specify the external rater.
5. For a personal data report, select the modules and functional areas you want to include in the search.

#### Note

To optimize system performance, limit your search to only the required data. The more modules you choose, the longer the report takes to compile.

6. Configure the time range you want to report on, up to a maximum of 31 days.
- The schedule you set here is based on your browser timezone.
7. Configure other settings, as required for the change audit report you're creating.

Report	Configuration Settings
Role-Based Permissions	Select the report type <a href="#">RBP Role Change Report</a> , <a href="#">RBP Group Change Report</a> , <a href="#">RBP User Role Change Report</a> , or <a href="#">RBP Static Group Membership Change Report</a> .
Employee Profile Data Change	Select the report type <a href="#">Background Data Change</a> or <a href="#">Feedback Data Change</a> .
MDF Configuration Data	<ul style="list-style-type: none"> <li>• Change By Person</li> <li>• Configuration Type</li> <li>• Object Type</li> <li>• Search Deleted Object Type (on/off)</li> </ul>
MDF Change History Data	<ul style="list-style-type: none"> <li>• Change By Person</li> <li>• Object Type</li> <li>• External Code</li> <li>• Search Deleted Object Type (on/off)</li> </ul>

8. Use the [Recurrence](#) switch to set up a recurring schedule.
- [No](#) means that there's no recurrence and we try to generate the report as soon as you submit it. [No](#) is the default setting.
  - [Yes](#) means that you want the report to be generated on a recurring schedule that you define.

To define a recurring schedule, fill out the following information.

Field	Description
Schedule Name	The name of the recurring schedule on the <a href="#">View Schedules</a> tab.



Field	Description
Method	<p>The location of the generated report file.</p> <ul style="list-style-type: none"> <li>Select <a href="#">Offline</a> to access the report within the application, on the <a href="#">Access Reports</a> tab.</li> <li>Select <a href="#">Secure File Transfer Protocol (SFTP)</a> to access the report in your SFTP folder.</li> </ul>
SFTP settings	If you select the SFTP access method, set up the required technical details to connect to your SFTP server. Then continue to create your report.
Recurring Pattern	When and how often you want the report to be generated (Daily, Weekly, Monthly, Yearly).
Start	Date and time when the recurrence begins.
End	Date and time when the recurrence ends.

### Note

If you set up a recurring schedule, the dates you select as the time range apply to the **first occurrence** of the report only. With each recurrence, the dates are adjusted accordingly. For example, if you set up an initial time range of April 1 to April 7 with a monthly recurrence starting on April 15, the first occurrence of the report on April 15 includes changes between April 1 and April 7, the second occurrence on May 15 includes changes between May 1 and May 7, and so on.

- Submit the request to generate a report.

## Results

If you didn't set up a recurring schedule, the report generation job is scheduled immediately but it may take some time to prepare. It may take just a few minutes, but, if there's a lot of data, it can take longer. You receive an email notification when the report is complete (or if it has failed).

If you set up a recurring schedule, the first report is generated on the exact date and time configured in the recurrence pattern, following the start date. Each subsequent report is generated on the configured day, at the configured time, but on the dates are adjusted accordingly.

## Next Steps

Wait to receive an email notification and use the link provided, within 48 hours, to go directly to the page where you can view and download the report in CSV format.

### → Remember

Audit reports are automatically purged after 48 hours. Be sure to check the report you are interested in within 48 hours of generation and archive it if necessary. Otherwise, you may have to run it again.

Alternatively, if you don't want to wait for the email, you can always check job status and download completed reports by going to ► [Change Audit Reports](#) ► [Access Reports](#) ►.

**Task overview:** [Process for Generating Change Audit Reports \[page 14\]](#)

## Related Information

[Downloading a Change Audit Report \[page 21\]](#)

[Interpreting a Change Audit Report \[page 22\]](#)

[Viewing or Deleting Recurrence Schedules for Change Audit Reports \[page 23\]](#)

[Downloading Compensation Audit Reports \[page 26\]](#)

[Importing a PGP File Encryption Key \[page 18\]](#)

[Configuring SFTP Settings for a Recurring Change Audit Report \[page 19\]](#)

## 6.1.1 Importing a PGP File Encryption Key

Import a PGP Public Key to encrypt files generated using SFTP Outbound Integrations.

### Prerequisites

You must have generated a PGP key pair so that you can import the PGP public key.

### Context

If you want to send sensitive data, it is always recommended to encrypt the data at message level. Security Center offers message level encryption using PGP (Pretty Good Privacy) encryption methodology.

### Procedure

1. Go to ► [Admin Center](#) ► [Security Center](#) ► [PGP File Encryption Keys](#) ►.
2. To import your PGP Public key for encryption, select [Import a Key](#).  
The [Import Key](#) dialog box opens.
3. Enter a name for your key in the [Name](#) field.

4. Choose [Choose File](#) to select your file.

Some common file formats used for PGP Public keys are: **.pub** and **.asc**.

5. To finish, choose [Import Key](#) to import your file.

#### Note

- The size of the file varies based on the key size that you have set on the tool to generate a PGP key. The size of the generated key is generally between 512 and 4096 bytes.
- You cannot upload PGP keys with same name.

Your imported PGP Key is encrypted and listed in the [Keys](#) table. To delete a key, choose  from [Actions](#).

## Results

You can use these keys in various admin tools that support PGP encryption, such as [Integration Center](#) or [Change Audit Reports](#).

## Related Information

[Information on PGP Message Format](#) 

## 6.1.2 Configuring SFTP Settings for a Recurring Change Audit Report

Configure SFTP settings if you want to access a recurring change audit report in an SFTP folder, instead of in the user interface.

## Prerequisites

- You are in the process of creating a new change audit report and have set the [Recurrence](#) switch to [Yes](#).
- If you plan to use file encryption, you have already imported your PGP public key on the [PGP Key Management](#) page.

## Procedure

1. In the report creation dialog, set [Method](#) to [Secure File Transfer Protocol \(SFTP\)](#).

2. Set up server access.

Provide information about the SFTP server where you want to use.

Option	Description
<a href="#">SuccessFactors hosted SFTP server</a>	Select <a href="#">SuccessFactors hosted SFTP server</a> to use your SAP SuccessFactors SFTP server. Most customers use this option.
<a href="#">Host Address</a> and <a href="#">Port</a>	If you cannot use the SAP SuccessFactors SFTP server, type the host address and port of your SFTP server.
<a href="#">FTP Login</a>	Type the user ID that SAP SuccessFactors uses to authenticate to the SFTP server. The user ID must have access to the server and to the file path where you want to put the file.
<a href="#">FTP Password</a>	Type the password that SAP SuccessFactors uses to authenticate to the SFTP server.

3. Click [Test Connection](#) to test server access.

4. Set up file access.

Provide information about the directory where you want the file to be saved.

Option	Description
<a href="#">File Path</a>	The directory path, from the SFTP user ID home, where the file is stored. <div><div>ⓘ Note</div><div>The path should begin with a forward slash. For example: <code>/audit/rbp</code></div></div>
<a href="#">File Encryption</a>	Select a PGP encryption key imported on the <a href="#">PGP Key Management</a> page. If no keys have been imported, <a href="#">No Encryption</a> is the only option.

5. Click [Test Permission](#) to test server access.

6. When both tests are successful, you can continue setting up your report.

## Next Steps

Finish setting up the change audit report, as required, and then click [Submit](#).

## Related Information

[Importing a PGP File Encryption Key \[page 18\]](#)

## 6.2 Downloading a Change Audit Report

Download and save your Change Audit report when is available so that you can investigate changes made in your system.

### Prerequisites

- You created the report.
- The report was created using the [Change Audit Reports](#) page in Admin Center.

### Context

You can only download audit reports that you created.

Use this procedure to audit most types of changes, except for Compensation configuration data. Compensation audit reports are generated and exported using a different procedure on the [Compensation Plan Activity Audit](#) page.

### Procedure

1. Go to ► [Admin Center](#) ► [Change Audit Reports](#) ►.
2. On the [Access Reports](#) tab, find the report you want to download.
  - If you see a download action icon, the job is complete and the report is ready for download.
  - If you don't see a download action icon and the report was created recently, the job may be incomplete or failed.
  - If you don't see a download action icon and the report is not recent, the old report has been purged and you need to create a new one.

#### Note

Server-side interruptions may cause the report generation to fail. In such cases, the generation job will be rebooted twice at most and you can find failed jobs with the same job ID in [Access Report](#).

3. Click the download action icon to download your report.
4. Save the downloaded zip file locally and extract the CSV file containing your change audit report.

### Next Steps

Open the CSV file as a spreadsheet so that you can read the report.

**Task overview:** [Process for Generating Change Audit Reports \[page 14\]](#)

## Related Information

[Creating a Change Audit Report \[page 15\]](#)

[Interpreting a Change Audit Report \[page 22\]](#)

[Viewing or Deleting Recurrence Schedules for Change Audit Reports \[page 23\]](#)

[Standard Data Included in All Change Audit Reports \[page 30\]](#)

[Downloading Compensation Audit Reports \[page 26\]](#)

## 6.3 Interpreting a Change Audit Report

Learn how to read and interpret the data in a change audit report so that you can understand specific changes made to your system.

### Prerequisites

- You have successfully created and downloaded your Change Audit report in CSV format.
- You can open the generated CSV as a spreadsheet.

### Procedure

1. Open the CSV file containing your Change Audit report as a spreadsheet.
2. Adjust formatting of the spreadsheet to make it more readable.
  - Auto-fit column widths so that you can read column headers
  - Align text at the top and enable text-wrapping so that you can see all the data
  - Use filters or sorting or other formatting to make data easier to find, as needed

#### → Remember

Don't forget to save changes to the file locally so that it's ready the next time you need it.

3. Read general information about the report at the top of the sheet, such as when it was generated and the date range it covers.
4. Find and read information about the changes you are interested in. Each row in the spreadsheet corresponds to a single change.

Each row contains standard data that's included in all change audit reports, as well as some data that is specific to the type of report.

- **Who?** You can see information about the user who made the change and the user who's personal data was changed.
- **Where?** You can see information about the module, functional area, and specific context where the change was made.
- **What?** You can see the old and new values of the field that was changed.
- **When?** You can see the date and time when the change was made. All timestamps are in the UTC timezone.

#### Note

Some values may be blank. Data is only present if it exists in audit logs for that specific change. Not all columns in the report may be relevant for that type of change.

Columns in the report may vary. Most columns are standard and usually present (even if blank) in all change audit reports. But some reports may omit the standard columns altogether, or add new ones, as appropriate for that specific type of report.

When you generate the Change Audit report for a specific user, you can view the change profile history of all candidates in the CSV file.

**Task overview:** [Process for Generating Change Audit Reports \[page 14\]](#)

## Related Information

[Creating a Change Audit Report \[page 15\]](#)

[Downloading a Change Audit Report \[page 21\]](#)

[Viewing or Deleting Recurrence Schedules for Change Audit Reports \[page 23\]](#)

[Standard Data Included in All Change Audit Reports \[page 30\]](#)

[Standard Data Included in All Change Audit Reports \[page 30\]](#)




## 6.4 Viewing or Deleting Recurrence Schedules for Change Audit Reports

View a list of recurrence schedules, delete ones that are no longer needed, and check the status of completed recurring reports.

### Prerequisites

You have the [Generate Change Audit Reports](#) permission.

## Procedure

1. Go to ► [Admin Center](#) ► [Change Audit Reports](#) ►.
2. On the [View Schedules](#) tab, choose one of the following actions.
  - View a list of all recurrence schedules active in your system.
  - Use search to find a recurrence schedule on the list.
  - Use  (delete) to remove a schedule and end the recurring report generation.
  - Use  (detail view) to check the status of all completed recurring reports.
  - Use  (refresh) to refresh the page and check for recently created schedules.

**Task overview:** [Process for Generating Change Audit Reports \[page 14\]](#)

## Related Information

[Creating a Change Audit Report \[page 15\]](#)

[Downloading a Change Audit Report \[page 21\]](#)

[Interpreting a Change Audit Report \[page 22\]](#)



# 7 Using Change Audit for SAP SuccessFactors Compensation

Change audit reports for SAP SuccessFactors Compensation are set up differently and generated on a different page than other change audit reports.

You have to:

1. Give Compensation Administrators permission to export audit data for compensation plan activity.
2. Use Compensation tools to export compensation audit reports.

## [Enabling Permission to Export Compensation Plan Audit Data \[page 25\]](#)

To be able to export compensation plan audit reports, administrators need to enable the *Allow Compensation Administrator to export compensation plan activity audit via UI* permission from *Admin Center*. The permission allows administrators to export data changes made on worksheets, Executive Reviews, and Compensation Profiles from ► *Manage Worksheet* ► *Compensation Plan Activity Audit* ►.

## [Downloading Compensation Audit Reports \[page 26\]](#)

Compensation audit reports help companies to report on historical data changes made on worksheets, Compensation Profiles and Executive Review. You can download these reports on the *Compensation Plan Activity Audit* page.

## [Creating Reports with Promotion-Based Information \[page 28\]](#)

You can create worksheet reports containing promotion-based information for employees. The system exports data from Employee Central for Employee Central-enabled templates, and from job selector fields within compensation for worksheets that aren't Employee Central-enabled.

## 7.1 Enabling Permission to Export Compensation Plan Audit Data

To be able to export compensation plan audit reports, administrators need to enable the *Allow Compensation Administrator to export compensation plan activity audit via UI* permission from *Admin Center*. The permission allows administrators to export data changes made on worksheets, Executive Reviews, and Compensation Profiles from ► *Manage Worksheet* ► *Compensation Plan Activity Audit* ►.

### Context

When running a compensation plan activity audit, the system returns results only for employees in the target group approved by means of Role-Based Permissions (RBPs).

## Procedure

1. Go to ► [Admin Center](#) ► [Compensation Home](#) ►
2. In the *Data for all Plans* section, select *Actions for all plans*.
3. Select *Company Settings*.

The *Manage Company Settings* page appears.

4. In the *Compensation and Variable Pay* section, select *Allow Compensation Administrator to export compensation plan activity audit via UI*.
5. Save your changes.

**Task overview:** [Using Change Audit for SAP SuccessFactors Compensation \[page 25\]](#)

## Related Information

[Downloading Compensation Audit Reports \[page 26\]](#)

[Creating Reports with Promotion-Based Information \[page 28\]](#)

## 7.2 Downloading Compensation Audit Reports

Compensation audit reports help companies to report on historical data changes made on worksheets, Compensation Profiles and Executive Review. You can download these reports on the [Compensation Plan Activity Audit](#) page.

### Prerequisites

Ensure that you've enabled

1. *Allow Compensation Administrator to export compensation plan activity audit via UI* on the *Company Settings* page. Enabling this option will allow you to view *Compensation Plan Activity Audit* on *Manage Worksheet* page. For more information about enabling this permission, refer [Enabling Permission to Export Compensation Plan Audit Data \[page 25\]](#).
2. *Compensation Plan Activity Audit* permission from ► [Admin Center](#) ► [Manage Permission Role](#) ► [\[Permission Role\]](#) ► [Manage Compensation](#) ►. Enabling this permission will allow users or a specific group of users to export audit reports.

## Procedure

1. Go to the [Admin Center](#).
2. In the [Tool Search](#) field, type **Compensation Home**.
3. In the [Plans](#) section, choose a Compensation Plan template.
4. Click [Manage Worksheets](#).
5. In the [Update Worksheets](#) section, click [Compensation Plan Activity Audit](#). This brings up the [Compensation Plan Activity Audit](#) page.

Audit reports can be exported for a worksheet or for an employee based on the customer's requirements.

The audit reports will run as a scheduled job. To track the progress of the job, navigate to the [Job Monitor](#) page. Once the report has been exported, you can download the report from [Home](#) > [Reports](#) > [Scheduled Reports](#).

**Task overview:** [Using Change Audit for SAP SuccessFactors Compensation \[page 25\]](#)

## Related Information

[Enabling Permission to Export Compensation Plan Audit Data \[page 25\]](#)

[Creating Reports with Promotion-Based Information \[page 28\]](#)

## 7.2.1 Exporting Audit Reports for Worksheets

You can export the data changes performed through manual edits, mass update, user data import, updates through Employee Central, calculated or derived fields in the Compensation worksheet, over a particular date range.

## Procedure

1. From the [View activity by](#) dropdown, choose [Template](#).
2. From the [Select Reported Fields](#) dropdown, choose the fields that you'd want to appear on the audit report.
3. Choose [Include Rating Fields in Audit report](#) if you want to add custom rating fields on the audit report.
4. Select a worksheet that you'd want to export.
5. Specify the time period of the export in the [Start Date](#) and [End Date](#) fields.

Note that you can export an audit report only for a maximum period of 30 days.

6. Click [Export Results](#).

## 7.2.2 Exporting Audit Reports For Employees

You can export the audit report only for selected employees in the Compensation worksheet, over a particular date range.

### Procedure

1. From the [View activity by](#) dropdown, choose [Employee](#).
2. From the [Select Reported Fields](#) dropdown, choose the fields that you'd want to appear on the audit report.
3. Choose [Include Rating Fields in Audit report](#) if you want to add custom rating fields on the audit report.
4. Specify the time period of the export in the [Start Date](#) and [End Date](#) fields.

Note that you can export an audit report only for a maximum period of 30 days.

5. To narrow down the search results of employees in the plan template, in the [Advanced Search](#) section, enter a value in any of the following fields: [First Name](#), [Username](#), [Department](#), [Location](#), and so on.
6. Click [Search](#).

A list of users based on your search criteria will appear in the [Search Users](#) section.

7. To list all the users in the plan template, click [Search](#), leaving the fields empty in the [Advanced Search](#) section.
8. In the [Search Users](#) section, choose the employees for whom you'd want to export the audit report.
9. To export the report for all employees listed, click [Select All](#).

The selected users will appear in the [Selected Users](#) section at the right pane.

10. Use the delete icon corresponding to each user in the [Selected Users](#) section to remove the users from reporting on the audit report.
11. Click [Export Results](#).

## 7.3 Creating Reports with Promotion-Based Information

You can create worksheet reports containing promotion-based information for employees. The system exports data from Employee Central for Employee Central-enabled templates, and from job selector fields within compensation for worksheets that aren't Employee Central-enabled.

### Prerequisites

To be allowed to create reports with promotion-based information, you must have the ► [Administrator](#) ► [Manage Compensation](#) ► [Enable Promotion Data Report](#) ► permission.

You manage the Employee Central fields exported into Compensation through the [User > Employee Central – Compensation Integration](#) permission. From the list of Employee Central Job Information fields, set the fields as appropriate:

- [View](#) to allow the system to export the field from Employee Central and enable administrators to view the field.
- [Edit](#) to allow the system to export the field from Employee Central and enable administrators to edit the field as well as to view it.

## Procedure

1. Go to [Admin Center > Compensation Home](#).
2. Select a compensation plan template from the list.
3. Go to [Manage Worksheets](#).
4. Select the [Promotion Report](#).
5. The system displays a message asking you to confirm. If correct, select [Continue](#).
6. A *The Compensation promotion data report has been scheduled, please go to the Report Center to download* message is shown.

### Note

Because the report can take time to generate, it's scheduled. When ready, you go to [My Jobs](#) in the [Report Center](#) to access and download the report.

**Task overview:** [Using Change Audit for SAP SuccessFactors Compensation \[page 25\]](#)

## Related Information

[Enabling Permission to Export Compensation Plan Audit Data \[page 25\]](#)

[Downloading Compensation Audit Reports \[page 26\]](#)

## 8 Standard Data Included in All Change Audit Reports

Learn about the standard data that is typically included in all change audit reports.

### Note

The following tables describe standard data points that **may** be included in all change audit reports. Most reports display this information, when present. But for any given report, if no data is present, some columns may be blank.

### Information about the report

Field	Description
Report Name	The name of the report as it appears in the user interface
Report GUID	An internal ID used by the job scheduler
Report Creator User ID	The person who created the report
Time Range (Start)	The start of the time and date range included in the report, in Coordinated Universal Time (UTC).
Time Range (End)	The end of the time and date range included in the report, in Coordinated Universal Time (UTC).

### Information about who made the change

Field	Description
Changed By User	First name, last name, and username of the person (or user account) who made the change
Proxy: Logged in User	First name, last name, and username of the logged-in proxy user who made the change (via the "Changed By" user's user account)
Secondary User	Provisioner ID and email address of the person who used secondary login in Provisioning to make the change (via the "Changed By" user's user account).

## Information about the change

Field	Description
Subject User	First name, last name, and username of the data subject user, the person whose data was changed
Module	Name of the SAP SuccessFactors solution that the changed data record belongs to
Functional Area	Functional area or major feature that the changed data record belongs to
Functional Sub Area	Subcategory of the functional area that the changed data record belongs to
Context Key-Value pairs	Contextual data tells you more about where the change was made. Contextual data is defined in a set of numbered key-value pairs that differ in each type of change audit report: <code>&lt;Context 1 Key&gt;</code> , <code>&lt;Context 1 Value&gt;</code> , <code>&lt;Context 2 Key&gt;</code> , <code>&lt;Context 2 Value&gt;</code> , and so on.

### Note

Contextual data varies for each type of report type. To understand a given change audit report, you need to understand the meaning of each context key-value pair in that type of report.

### Example

In an RBP Role Change report, you might see a `<Context 1 Key>` of "Role" and a `<Context 1 Value>` of "System Admin". The key "Role" tells you that a change was made to an RBP role and the value "System Admin" tells you the name of the RBP role in your system that was changed.

In a ChangedOn report about someone's personal data, you might see a `<Context 1 Key>` of "Admin Action" and a `<Context 1 Value>` of "Manage Users". The key "Admin Action" tells you that a change was made in Admin Center and the value "Manage Users" tells you it was made via the Manage Users page.

Field	Description
Field Name	<p>Field name of the data record that changed</p> <div> <p><b>❖ Example</b></p> <p>In an RBP Role Change report, a field name "Permission" tells you it's a change to permissions in the role. Or a field name of "Role name" tells you it's a change to the name of the role.</p> <p>In a ChangedOn report about someone's personal data, the field name is the name of the user data record that changed, such as "Last Name" or "Address".</p> </div>
Old Value and New Value	<p>Old and new values of the data record that was changed</p> <div> <p><b>📘 Note</b></p> <p>Field values in change audit reports can't be more than 4000 characters. Longer values are truncated, so some changes may not be visible in the report. Try to limit the value of fields you need to audit to less than 4000 characters.</p> </div>
Operation Performed	<p>Type of operation that made the change.</p> <ul style="list-style-type: none"> <li>• I is for Insert of a new record</li> <li>• U is for Update of a record</li> <li>• D is for Delete of a record</li> </ul>
Timestamp	Time and date of the change, in Coordinated Universal Time (UTC).
Effective Start Date	Effective start date, for effective-dated records
Effective Sequence	The sequence of changes made during a single effective-dated transaction. This field applies mainly to SAP SuccessFactors Employee Central.



# 9 Change Audit Reports

Change audit reports are offline reports containing audit data about changes in your system.

For the most common audit requirements, you can use self-service audit reporting tools in Admin Center to generate and download change audit reports in CSV format.

Change audit reports are grouped into several categories:

- Personal data reports on the [Change Audit Reports](#) page.
- Configuration data reports on the [Change Audit Reports](#) page.
- Business data reports on the [Change Audit Reports](#) page.
- Other audit capabilities available in other parts of the HCM suite, using other tools.

## [Personal Data Audit Reports \[page 33\]](#)

Personal data change audit reports include changes to personal data records **about** or **by** a specific user.

## [Configuration Data Audit Reports \[page 36\]](#)

Configuration data audit reports include changes to the configuration of your system.

## [Business Data Audit Reports \[page 59\]](#)

Business data audit reports include changes to other types of data records in your system, such as transactional data in a business process.

## [Change History in Data Retention Management \[page 83\]](#)

Learn about [Change History in Data Retention Management](#) and how to read it.

## 9.1 Personal Data Audit Reports

Personal data change audit reports include changes to personal data records **about** or **by** a specific user.

Personal data audit reports are available on the [Create Personal Data Report](#) tab when you enable the [Personal Data Audit](#) setting.

Report	Description
<a href="#">Person Search</a> > <a href="#">Change On Subject User</a> >	Use this report to audit changes to personal data <b>about</b> an individual employee or internal candidate.
<a href="#">Person Search</a> > <a href="#">Change By User</a> >	Use this report to audit changes to <b>by</b> an individual employee or internal candidate <b>to</b> other people's personal data.
<a href="#">External Candidate Search</a>	Use this report to audit changes to personal data for someone who has applied for jobs at your company, but who is not an employee.
<a href="#">Onboarder Search</a>	Use this report to audit changes to personal data for someone who is in the process of being onboarded, but who is not yet a full employee.

Report	Description
<a href="#">External User Search</a>	Use this report to audit changes to personal data <b>about</b> an external user in Performance Management and also all changes to personal data made <b>by</b> that user.


#### [Employee Central Data in Personal Data Audit Reports \[page 34\]](#)

Track personal data of employees for downstream integrations, support SAP SuccessFactors HCM suite processes and reporting. Understand and report out your Employee Central configuration changes by using the table below.

## 9.1.1 Employee Central Data in Personal Data Audit Reports

Track personal data of employees for downstream integrations, support SAP SuccessFactors HCM suite processes and reporting. Understand and report out your Employee Central configuration changes by using the table below.

Block or Area	Type	ID	Fields Affected	Audit Report
Personal Information	hris-element	personallInfo	<ul style="list-style-type: none"> <li>First Name</li> <li>Last Name</li> <li>Gender</li> <li>Marital Status</li> </ul>	Create Personal Data Report
		personInfo	<ul style="list-style-type: none"> <li>Country of Birth</li> <li>Date of Birth</li> <li>Person ID</li> </ul>	
		nationalIdCard	<ul style="list-style-type: none"> <li>Country</li> <li>isPrimary</li> <li>Type</li> </ul>	
		nationalIdCard	Format of National ID card	
		homeAddress	Address 1, 2, 3 (not country/region specific)	
		homeAddress	Address 1,2,3, province/state with country/region-specific formatting	
		globalInfo	<ul style="list-style-type: none"> <li>Challenged</li> <li>Ethnic Group</li> <li>Student</li> <li>Veteran Status</li> </ul>	

Block or Area	Type	ID	Fields Affected	Audit Report
		emailInfo	<ul style="list-style-type: none"> <li>Address</li> <li>isPrimary</li> <li>Type</li> </ul>	
		phoneInfo	<ul style="list-style-type: none"> <li>isPrimary</li> <li>Number</li> <li>Type</li> </ul>	
		imlInfo	<ul style="list-style-type: none"> <li>Email</li> <li>isPrimary</li> <li>Username</li> </ul>	
		emergencyContactPrimary	<ul style="list-style-type: none"> <li>Address</li> <li>Email</li> <li>isPrimary</li> <li>Name</li> <li>Phone</li> <li>Relationship</li> </ul>	
		personRelationshipInfo	<ul style="list-style-type: none"> <li>Dependent information</li> <li>Name</li> <li>Relationship</li> </ul>	
		workPermitInfo	<ul style="list-style-type: none"> <li>Document Type</li> <li>Document Title</li> <li>Expiration Date</li> <li>Issue Date</li> </ul>	
		paymentInfo	<ul style="list-style-type: none"> <li>Payment Method</li> </ul>	
			<div>  <b>Note</b>  All other fields of object are controlled by the Payment Information generic object. </div>	
		userAccountInfo	username	
Employment Information	hris-element	jobInfo	<ul style="list-style-type: none"> <li>Employee Class</li> <li>Job Code</li> <li>Job Title</li> <li>Position</li> <li>Pay Grade</li> <li>Regular/Full Time</li> </ul>	Create Personal Data Report

Block or Area	Type	ID	Fields Affected	Audit Report
		jobInfo	<ul style="list-style-type: none"> <li>EEO</li> <li>FLSA</li> <li>Any country/region specific job-related fields</li> </ul>	
		employmentInfo	<ul style="list-style-type: none"> <li>First day worked</li> <li>Hire date</li> <li>OK to Rehire</li> <li>Original Hire Date</li> </ul>	
		jobRelationsInfo	<ul style="list-style-type: none"> <li>Name</li> <li>Relationship Type</li> </ul>	
		complInfo	<ul style="list-style-type: none"> <li>Pay Frequency</li> <li>Compa-ratio</li> </ul>	
		payComponentRecurring	<ul style="list-style-type: none"> <li>Amount</li> <li>Currency</li> <li>Frequency</li> <li>Pay component</li> </ul>	
		payComponentNonRecurring	<ul style="list-style-type: none"> <li>Amount</li> <li>Currency</li> <li>Frequency</li> <li>Pay component</li> </ul>	
		pensionPayoutsInfo	<ul style="list-style-type: none"> <li>Start Date</li> <li>End Date</li> <li>Pension Provider</li> </ul>	
		globalAssignmentInfo	<ul style="list-style-type: none"> <li>Assignment type</li> <li>Start date</li> <li>Planned end date</li> </ul>	
		Concurrent Employment	Country	
		Contingent Worker	isContingentWorker	

## 9.2 Configuration Data Audit Reports

Configuration data audit reports include changes to the configuration of your system.

Configuration data audit reports are available on the [Create Configuration Data Report](#) tab when you enable the [General Audit](#) setting.

Report	Description
► <a href="#">Role Based Permission</a> ► <a href="#">RBP</a> <a href="#">Role Change Report</a> ►	Use this report to audit changes to RBP permission roles.
► <a href="#">Role Based Permission</a> ► <a href="#">RBP</a> <a href="#">Group Change Report</a> ►	Use this report to audit changes to RBP permission groups.
► <a href="#">Role Based Permission</a> ► <a href="#">RBP</a> <a href="#">Static Group Membership Change Report</a> ►	Use this report to audit changes to the membership of RBP static permission groups.
► <a href="#">Role Based Permission</a> ► <a href="#">RBP</a> <a href="#">User Role Change Report</a> ►	Use this report to audit changes to RBP role assignments.
<a href="#">Proxy Assignment Change</a>	Use this report to audit changes to proxy management configuration.
<a href="#">Feature Settings Audit Report</a>	Use this report to audit changes to feature settings.
<a href="#">MDF Configuration Data</a>	Use this report to audit changes to Metadata Framework (MDF) configuration, including the MDF data model, Legislatively Sensitive Personal Data configuration, and other MDF configuration data.
<a href="#">Job Scheduler Requests</a>	Use this report to audit changes made to scheduled job requests created in <b>Job Scheduler</b> , such as creation of a new job.
<a href="#">Manage Support Access</a>	Use this report to audit changes made to support access in the <a href="#">Manage Support Access</a> admin tool.

#### [RBP Role Change Report \[page 38\]](#)

Learn about the [RBP Role Change Report](#) and how to read it.

#### [RBP Group Change Report \[page 40\]](#)

Learn about the [RBP Group Change Report](#) and how to read it.

#### [RBP Static Group Membership Change Report \[page 42\]](#)

Learn about the [RBP Static Group Membership Change Report](#) and how to read it.

#### [RBP User Role Change Report \[page 43\]](#)

Learn about the [RBP User Role Change Report](#) and how to read it.

#### [Proxy Assignment Change Report \[page 44\]](#)

Learn about the [Proxy Assignment Change](#) report and how to read it.

#### [Feature Settings Audit Report \[page 47\]](#)

Learn about the [Feature Settings Audit Report](#) and how to read it.

#### [Employee Central Feature Settings Audit Report \[page 51\]](#)

The table identifies all areas of Employee Central where MDF objects and Foundation Objects can be changed.

#### [MDF Configuration Data Report \[page 54\]](#)

Learn about the [MDF Configuration Data](#) and how to read it.

#### [Job Scheduler Requests Report \[page 55\]](#)

Learn about the [Job Scheduler Requests](#) report and how to read it.

[Change Audit for Locales and Customizations \[page 56\]](#)

You can track changes users've made to locales and customizations by looking at change audit reports that are generated on demand or on a recurring basis.

[Manage Support Access Change Report \[page 58\]](#)

Learn about the [Manage Support Access](#) report and how to read it.

[Email Configurations Change Audit Report \[page 59\]](#)

Learn how to read the change audit report for email notification configurations.

## 9.2.1 RBP Role Change Report

Learn about the [RBP Role Change Report](#) and how to read it.

The [RBP Role Change Report](#) describes changes made to RBP permission roles.

### How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Context 1 Key	"Role" indicates that the corresponding context value is an RBP role.
Context 1 Value	The current name of the RBP role that was changed
Field Name	<ul style="list-style-type: none"><li>"Permission" indicates a change to permissions in the role.</li><li>"Group" indicates a change to granting rules for the role. These include changes to granted permission groups, changes to target permission groups, and changes to the role's active/inactive status.</li><li>"Role name" indicates a change to the name of the role.</li></ul>
Old Value	<ul style="list-style-type: none"><li>For "Permission" changes, it shows permissions that were removed from the role.</li><li>For "Group" changes, it shows granted or target permission groups that were removed from the role, or the old status of the role.</li><li>For "Role name" changes, it shows the old name of the role.</li></ul>

#### Note

You can ignore any reference to internal rules by number, such as "Rule 401".

Field	Description
New Value	<p>For "Permission" changes, it shows permissions that were added to the role. For "Group" changes, it shows permission groups that were added to the role. (You can ignore any reference to internal rules, such as "Rule 401".)</p> <ul style="list-style-type: none"> <li>For "Permission" changes, it shows permissions that were added to the role.</li> <li>For "Group" changes, it shows granted or target permission groups that were added to the role, or the new status of the role.</li> <li>For "Role name" changes, it shows the old name of the role.</li> </ul> <div> <p><b>Note</b></p> <p>You can ignore any reference to internal rules by number, such as "Rule 401".</p> </div>

## Examples

### ❖ Example

You change permissions in the RBP role "System Admin". You grant two new permissions allowing users in this role to use the configuration check tool.

The [RBP Role Change Report](#) includes the following information:

Context 1 Key	Context 1 Value	Field Name	Old Value	New Value
Role	System Admin	Permission		Access Check Tool, Allow Configuration Export

### ❖ Example

You change permissions in the RBP role "System Admin". You remove two permissions from the role in order to remove access from configuration check tool.

The [RBP Role Change Report](#) includes the following information:

Context 1 Key	Context 1 Value	Field Name	Old Value	New Value
Role	System Admin	Permission	Access Check Tool, Allow Configuration Export	

### ❖ Example

You change groups associated with the RBP role "System Admin". First, you grant this role to the permission group "Employee Central Admin". Then you add a new target population group "All Employees".

The [RBP Role Change Report](#) includes the following information:

Context 1 Key	Context 1 Value	Field Name	Old Value	New Value
Role	System Admin	Group		Rule 401: Granted: Employee Central Admin Target: All Employees

#### ❖ Example

You change the status of the RBP role "System Admin" from "inactive" to "active".

The [RBP Role Change Report](#) includes the following information:

Context 1 Key	Context 1 Value	Field Name	Old Value	New Value
Role	System Admin	Group	inactive	active

#### ❖ Example

You change the name of an RBP role from "Admin" to "System Admin".

The [RBP Role Change Report](#) includes the following information:

Context 1 Key	Context 1 Value	Field Name	Old Value	New Value
Role	System Admin	Role name	Admin	System Admin

## 9.2.2 RBP Group Change Report

Learn about the [RBP Group Change Report](#) and how to read it.

The [RBP Group Change Report](#) describes changes made to dynamic permission groups in RBP.

### ⚠ Restriction

This report only reflects changes on the definitions of dynamic groups. It doesn't include any information about the changes of impacted users in these groups.

## How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.



Field	Description
Context 1 Key	"Group" indicates that the corresponding context value is an RBP group.
Context 1 Value	The current name of the RBP group that was changed
Field Name	<ul style="list-style-type: none"> <li>"People Pool" indicates a change to the inclusion or exclusion criteria used to define the group.</li> <li>"Group name" indicates a change to the name of the group.</li> </ul>
Old Value	<ul style="list-style-type: none"> <li>For "People Pool" changes, it shows the old values of the inclusion or exclusion criteria that were changed.</li> <li>For "Group name" changes, it shows the old name of the group.</li> </ul>
New Value	<p>For "People Pool" changes, it shows inclusion criteria or exclusion criteria that were added to the group.</p> <ul style="list-style-type: none"> <li>For "People Pool" changes, it shows the new values of the inclusion or exclusion criteria that were changed.</li> <li>For "Group name" changes, it shows the new name of the group.</li> </ul>

## Examples

### ❖ Example

You change inclusion criteria defining the RBP group "Admin". You add the user "ghill" to the group.

The [RBP Group Change Report](#) includes the following information:

Context 1 Key	Context 1 Value	Field Name	Old Value	New Value
Group	Admin	People pool		People Pool(include) (user = Geoff Hill)

### ❖ Example

You change inclusion criteria defining the RBP group "Admin". You add users with a country of "United States" or "Canada" to the group.

The [RBP Group Change Report](#) includes the following information:

Context 1 Key	Context 1 Value	Field Name	Old Value	New Value
Group	Admin	People pool		People Pool(include) (std_country = United States OR Canada)

### ❖ Example

You change the name of an RBP group from "Admin" to "North America Admin".

The [RBP Group Change Report](#) includes the following information:

Context 1 Key	Context 1 Value	Field Name	Old Value	New Value
Group	North America Admin	Group name	Admin	North America Admin

## 9.2.3 RBP Static Group Membership Change Report

Learn about the [RBP Static Group Membership Change Report](#) and how to read it.

The [RBP Static Group Membership Change Report](#) describes changes made to RBP static permission groups.

### How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Context 1 Key	"User" indicates that the corresponding context value is a user account.
Context 1 Value	The username for the user account whose group membership was changed.
Context 2 Key	"User name" indicates that the corresponding context value is the name of a user.
Context 2 Value	The first and last name of the user whose group membership was changed.
Field Name	"Group" indicates a change to granted permission groups.
Old Value	If the operation is "D", this field shows the permission group that the user was removed from.
New Value	If the operation is "I", this field shows the permission group that the user was added to.
Operation Performed	<ul style="list-style-type: none"><li>"I" indicates that the user was added to the permission group.</li><li>"D" indicates that the user was removed from the permission group.</li></ul>

### Examples

#### ❖ Example

You add Geoff Hill to and remove Carla Grant from the Payroll Admin static permission group.

Context 1 Key	Context 1 Value	Context 2 Key	Context 2 Value	Field Name	Old Value	New Value	Operation Performed
User	ghill	User name	Geoff Hill	Group		Payroll Admin	I
User	cgrant	User name	Carla Grant	Group	Payroll Admin		D

## 9.2.4 RBP User Role Change Report

Learn about the [RBP User Role Change Report](#) and how to read it.

The [RBP User Role Change Report](#) describes changes made to RBP role assignments.

### How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Changed By User	First name, last name, and username of the person (or user account) who made the change.
Context 1 Key	"User" indicates that the corresponding context value is a user account.
Context 1 Value	The username for the user account whose role was changed
Context 2 Key	"User name" indicates that the corresponding context value is the name of a user.
Context 2 Value	The first and last name of the user whose role was changed
Field Name	"Role" indicates a change to the RBP roles that are granted to the specified user.
Old Value	The name of RBP roles were removed from the user.
New Value	The name of RBP roles that were granted to the user

### Examples

A user's RBP roles can change as a result of three changes in the system: a change to RBP roles, a change to RBP groups, or a change to user information.

#### ❖ Example

You recently added the user "ghill" to the RBP group "Admin". As a result, that user is now assigned to all RBP roles that are granted to that group. In your system, the RBP group "Admin" is granted to two roles that are new to this user, "Payroll Admin" and "System Admin".

The *RBP User Role Change Report* includes the following information:

Context 1 Key	Context 1 Value	Context 2 Key	Context 2 Value	Field Name	Old Value	New Value
User	ghill	User name	Geoff Hill	Role		Payroll Admin
User	ghill	User name	Geoff Hill	Role		System Admin

#### ❖ Example

You recently granted the RBP role "System Admin" to members of the RBP group "Employee Central Admin". As a result, all users previously included in the "Employee Central Admin" group are now assigned to the "System Admin" role. The user "bsander" is one such user.

The *RBP User Role Change Report* includes the following information:

Context 1 Key	Context 1 Value	Context 2 Key	Context 2 Value	Field Name	Old Value	New Value
User	bsander	User name	Bernd Sander	Role		System Admin

#### ❖ Example

The user "bsander" recently became a manager. As a result, he's now a member of the "Managers" group and, thus, assigned to the "Manager" role.

The *RBP User Role Change Report* includes the following information:

Context 1 Key	Context 1 Value	Context 2 Key	Context 2 Value	Field Name	Old Value	New Value
User	bsander	User name	Bernd Sander	Role		Manager

## 9.2.5 Proxy Assignment Change Report

Learn about the *Proxy Assignment Change* report and how to read it.

The *Proxy Assignment Change* report describes changes made to proxy assignments.

### How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Changed By User	As in all change audit reports, these fields show first name, last name, and username of the user account that was used to change Proxy Management settings.
Proxy:Logged in User	As in all change audit reports, these fields show first name, last name, and username of the person who logged in as a proxy and changed Proxy Management settings via another person's user account.
Subject User	In the Proxy Report, the Subject User is the same as the "Proxy Rights For" user in Context 1 Value column.
Context 1 Key	"Proxy Rights For" indicates that the corresponding context value is the name of the proxy (the person who proxy rights were given to).
Context 1 Value	The first and last name of the person who proxy rights were given to.
Context 2 Key	"Proxy Rights To" indicates that the corresponding context value is the person whose account the proxy user was given access to.
Context 2 Value	The first and last name of the person whose account the proxy user was given access to.
Field Name	The name of the field that was changed, such as module permission, start date, and end date.
Old Value	For module permissions, this is a list of pages or features that the proxy user had access to before the change.  For start and end dates, this is the date and time before the change.
New Value	For module permissions, this is a list of pages or features that the proxy user has access to after the change.  For start and end dates, this is the date and time after the change.

## Examples

### ❖ Example

You log in as the admin user "sfadmin" and change proxy assignments. You give Lisa Chupak (username "lchupak") permission to act as a proxy for Carla Grant (username "cgrant"). You also specify the pages and features that Lisa can access as a proxy for Carla.

The *Proxy Assignment Change* report includes the following information:

Changed By User (User-name)	Subject User (User-name)	Context 1 Key	Context 1 Value	Context 2 Key	Context 2 Value	Field Name	Old Value	New Value
sfadmin	Ichupak	Proxy Rights For	Lisa Chupak	Proxy Rights To	Carla Grant	Module Permission		Admin Tools, Home Page Tab, Live Profile, organization chart

### ❖ Example

You log in as the admin user "sfadmin" and change proxy assignments. You remove proxy permissions for some pages or features from Lisa Chupak (username "Ichupak") so that she can no longer access these pages as a proxy for Carla Grant (username "cgrant"). You remove Lisa's proxy access to the "Live Profile" and "Organization Chart" features.

The *Proxy Assignment Change* report includes the following information:

Changed By User (User-name)	Subject User (User-name)	Context 1 Key	Context 1 Value	Context 2 Key	Context 2 Value	Field Name	Old Value	New Value
sfadmin	Ichupak	Proxy Rights For	Lisa Chupak	Proxy Rights To	Carla Grant	Module Permission	Admin Tools, Home Page Tab, Live Profile, Organization chart	Admin Tools, Home Page Tab

### ❖ Example

You log in as the admin user "sfadmin" and use *Proxy Now* to act as a proxy on behalf of another admin user "ghill". While logged in as a proxy for "ghill", you change proxy assignments for Lisa Chupak (username "Ichupak").

The *Proxy Assignment Change* report includes the following information:

Changed By User (User-name)	Proxy:Log ged in User (User-name)	Subject User (User-name)	Context 1 Key	Context 1 Value	Context 2 Key	Context 2 Value	Field Name	Old Value	New Value
ghill	sfadmin	Ichupak	Proxy Rights For	Lisa Chu-pak	Proxy Rights To	Carla Grant	Module Permis-sion	Admin Tools, Home Page Tab	Admin Tools, Home Page Tab, Live Pro-file,Organi-zation chart

## 9.2.6 Feature Settings Audit Report

Learn about the *Feature Settings Audit Report* and how to read it.

The *Feature Settings Audit Report* describes changes made to feature settings in your system, including many settings in both Provisioning and Admin Center.

### ⚠ Restriction

Currently, this report only includes on/off checkbox settings and doesn't include feature configuration fields, such as URLs for system integration.

## How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Changed By User	First name, last name, and username of the person (or user account) who enabled the feature <b>for the first time</b> in Admin Center.

Field	Description
Secondary User	<p>Provisioner ID and email address of the person who enabled the feature <b>for the first time</b> using the Provisioning application.</p> <ul style="list-style-type: none"> <li>• If only Secondary User is present in the report, the change was made directly in Provisioning.</li> <li>• If both Secondary User and Changed By User are present in the report, the change was made by a someone who used the secondary login feature in Provisioning to access an admin user account and make a change in Admin Center.</li> <li>• If Secondary User is blank in the report, the change was made by an admin user in Admin Center.</li> </ul>
Context 1 Key	"Company Id" indicates that the corresponding context value is a Company ID.
Context 1 Value	The Company ID of the instance that was changed.
Context 2 Key	"Feature Id" indicates that the corresponding context value is a Feature ID.
Context 2 Value	The Feature ID of the feature setting that was changed.
Context 3 Key	"Feature Name" indicates that the corresponding context value is the technical name of a feature setting.
Context 3 Value	The technical name of the feature setting that was changed.
Context 4 Key	"Product" doesn't indicate the name of a product. Instead, it indicates that the corresponding context value is the common name of a feature setting. In most cases, it's nearly identical to the technical name.
Context 4 Value	The common name of the feature setting that was changed.
Context 5 Key	"Modified By" indicates that the corresponding context value is the <b>last</b> user who enabled or disabled a feature.
Context 5 Value	The username of the <b>last</b> person who enabled or disabled a feature, either in Admin Center or Provisioning.
Field Name / Old Value / New Value	These columns aren't <b>used</b> in this report. Currently, this report only includes on/off checkbox settings and not feature configuration fields.
Operation Performed	<p>Indicates the value of the checkbox for the feature setting.</p> <ul style="list-style-type: none"> <li>• I is for Insert and indicates that the setting was selected and the feature is enabled.</li> <li>• D is for Delete and indicates that the setting was deselected and the feature is disabled.</li> </ul>

## Examples

### ❖ Example

You manually log into your company instance "BestRun" as the admin user "sfadmin" and **enable** the "Personal Data Audit" setting in Admin Center.

The *Feature Settings Audit Report* report includes the following information.



Chan ged By User (User- name)	Con- text 1 Key	Con- text 1 Value	Con- text 2 Key	Con- text 2 Value	Con- text 3 Key	Con- text 3 Value	Con- text 4 Key	Con- text 4 Value	Con- text 5 Key	Con- text 5 Value	Field Name	Old Value	New Value	Oper- ation Per- forme d
sfad- min	Com- pany Id	Be- stRun	Fea- ture Id	914	Fea- ture Name	ENA- BLE_P ER- SON_ DATA_ AUDIT	Prod- uct	Ena- ble Per- son Data Audit	Modi- fied By	sfad- min				I

### ❖ Example

Another user logs into the same company instance "BestRun" with another account "abcdef" and disables the "Personal Data Audit" setting in Admin Center.

The *Feature Settings Audit Report* includes the following information.

Chan ged By User (User- name)	Con- text 1 Key	Con- text 1 Value	Con- text 2 Key	Con- text 2 Value	Con- text 3 Key	Con- text 3 Value	Con- text 4 Key	Con- text 4 Value	Con- text 5 Key	Con- text 5 Value	Field Name	Old Value	New Value	Oper- ation Per- forme d
sfad- min	Com- pany Id	Be- stRun	Fea- ture Id	914	Fea- ture Name	ENA- BLE_P ER- SON_ DATA_ AUDIT	Prod- uct	Ena- ble Per- son Data Audit	Modi- fied By	sfad- min				I
sfad- min	Com- pany Id	Be- stRun	Be- stRun	914	Fea- ture Name	ENA- BLE_P ER- SON_ DATA_ AUDIT	Prod- uct	Ena- ble Per- son Data Audit	Modi- fied By	abc- def				D

### ❖ Example

Your implementation consultant (jsmith@techconsultants.com) uses the Provisioning application to **disable** the Employee Directory feature for your company instance "BestRun".

The *Feature Settings Audit Report* includes the following information.

Chan- ged By User (Use- rname)	Sec- on- dary User Pro- vi- sion- er ID	Sec- on- dary User Email	Con- text 1 Key	Con- text 1 Value	Con- text 2 Key	Con- text 2 Value	Con- text 3 Key	Con- text 3 Value	Con- text 4 Key	Con- text 4 Value	Con- text 5 Key	Con- text 5 Value	Field Name	Old Value	New Value	Op- era- tion Per- form- ed
	EMP1 2345	jsmit h@te chco nsul- tants .com	Com- pany Id	Be- stRu n	Fea- ture Id	63	Fea- ture Name	EM- PLOY EE_D IRE- CTO RY	Prod- uct	Em- plove e Di- rec- tory	Modif ied By	EMP1 2345				D

## ❖ Example

Your implementation consultant (jsmith@techconsultants.com) uses the secondary login feature in Provisioning to access the admin user account "sfadmin" for the company instance "BestRun" and **enable** the "Personal Data Audit" setting in Admin Center.

The [Feature Settings Audit Report](#) includes the following information.

Chan- ged By User (Use- rname)	Sec- on- dary User Pro- vi- sion- er ID	Sec- on- dary User Email	Con- text 1 Key	Con- text 1 Value	Con- text 2 Key	Con- text 2 Value	Con- text 3 Key	Con- text 3 Value	Con- text 4 Key	Con- text 4 Value	Con- text 5 Key	Con- text 5 Value	Field Name	Old Value	New Value	Op- era- tion Per- form- ed
sfad- min	EMP1 2345	jsmit h@te chco nsul- tants .com	Com- pany Id	Be- stRu n	Fea- ture Id	914	Fea- ture Name	ENA- BLE_ PER- SON _DAT A_AU DIT	Prod- uct	Ena- ble Per- son Data Audit	Modif ied By	sfad- min				I

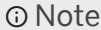
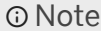
## 9.2.7 Employee Central Feature Settings Audit Report

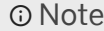
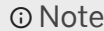
The table identifies all areas of Employee Central where MDF objects and Foundation Objects can be changed.

### Limitations

- Change by does not include RBP Permission Group or RBP Permission Role details.

Block or Area	Type	ID	How Updated	Fields Affected	Current Audit Method	Audit Report
Foundation -Organization Information	MDF Object	BusinessUnit	Manage Data		MDF Configuration Change Audit Reports	MDF Configuration Data report
		CostCenter	Manage Data			
		Department	Manage Data			
		Division	Manage Data			
		LegalEntity	Manage Data			
		LegalEntityLocal	Manage Data			
	hris-element	corporateAddress	Manage Organization, Pay, and Job Structures		None	None
		corporateAddress	Manage Organization, Pay, and Job Structures			
		locationGroup	Manage Organization, Pay, and Job Structures	Grouping locations together for reporting purposes		
		geozone	Corporate Data Model	US_EAST, US_WEST, US_MIDWEST, grouping locations together for the purpose of compensation		
		location	Manage Organization, Pay, and Job Structures			
Foundation - Pay Information	hris-element	payRange	Manage Organization, Pay, and Job Structures		None	None
		payGrade	Manage Organization, Pay, and Job Structures			

Block or Area	Type	ID	How Updated	Fields Affected	Current Audit Method	Audit Report
		payComponent	Manage Organization, Pay, and Job Structures			
		payComponentGroup	Manage Organization, Pay, and Job Structures			
	MDF Object	PayGroup	Manage Data		MDF Configuration Change Audit Reports	MDF Configuration Data report
		PayCalendar	Manage Data			
		JobClassification	Manage Data			
		JobClassificationLocal	Manage Data			
		JobFunction	Manage Data			
Foundation - Frequency	hris-element	Frequency	Manage Organization, Pay, and Job Structures		None	Ad Hoc Reporting> Foundation Object >Filter by Last Modified Date
<div>  <b>Note</b>  This report does not provide field level before and after results. </div>						
Foundation - Dynamic Role	hris-element	dynamicRole	Manage Organization, Pay, and Job Structures		None	Ad Hoc Reporting> Foundation Object >Filter by Last Modified Date
		dynamicRoleAssignment	Manage Organization, Pay, and Job Structures			
<div>  <b>Note</b>  This report does not provide field level before and after results. </div>						

Block or Area	Type	ID	How Updated	Fields Affected	Current Audit Method	Audit Report
Foundation - Workflow	hris-element	wfConfig	Manage Organization, Pay, and Job Structures		None	Ad Hoc Reporting> Foundation Object >Filter by Last Modified Date
		wfStepApprover	Manage Organization, Pay, and Job Structures			
		wfConfigContributor	Manage Organization, Pay, and Job Structures			
		wfConfigCC	Manage Organization, Pay, and Job Structures			
<div><div></div><div><b>Note</b> This report doe not provide field level before and after results.</div></div>						
Foundation - Events	hris-element	eventReason	Manage Organization, Pay, and Job Structures	<ul style="list-style-type: none"><li>Hire</li><li>Leave of Absence</li><li>Promotion</li><li>Rehire</li><li>Termination</li><li>Transfer</li></ul>	None	Ad Hoc Reporting> Foundation Object >Filter by Last Modified Date
<div><div></div><div><b>Note</b> This report doe not provide field level before and after results.</div></div>						
Generic Objects	generic objects	Company Structure Overview	Manage Data		MDF Configuration Change Audit Reports	MDF Change History Report
		Country	Manage Data			
		Dismissal Protection	Manage Data			
		Employee Central Help Text	Manage Data			
		Pay Scale	Manage Data			
		Payment Information	Manage Data			
		Position	Manage Data			
MDF	Picklists	Picklists	Picklist Center		MDF Change History Report	MDF Change History Report

## 9.2.8 MDF Configuration Data Report

Learn about the [MDF Configuration Data](#) and how to read it.

The [MDF Configuration Data](#) report describes changes made to MDF configuration data, such as changes to the object definition.

### How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Context 1 Key	Indicates the field names of external name and external code of root object.
Context 1 Value	Values of external name and external code of root object.
Context 2 Key	Indicates the field names of external name and external code of first-level child object concatenated with child object type. This field isn't used, if it is applicable.
Context 2 Value	Values of external name and external code of first-level child object. The values aren't used, if it isn't applicable.
Context 3 Key	Indicates the field names of external name and external code of second-level child object concatenated with child object type. This field isn't used, if it isn't applicable.
Context 3 Value	Values of external name and external code of second-level child object. The values aren't used, if it isn't applicable.
Context 4 Key	Indicates the field names of external name and external code of third level child object concatenated with child object type. This field isn't used, if it isn't applicable.
Context 4 Value	Values of external name and external code of third level child object. This field isn't used, if it isn't applicable.
Field Name	The name of the field that was changed. If it's a field of a child object, field name is concatenated with the association name between the child object and its parent object.
Old Value	Old value of the field before the change.
New Value	New value of the field after the change.

### Examples

#### ❖ Example

For example, the [MDF Configuration Data](#) report might include the following information.

Changed By User (User-name)	Context 1 Key	Context 1 Value	Context 2 Key	Context 2 Value	Context 3 Key	Context 3 Value	Field Name	Old Value	New Value	Operation Performed
sfadmin	Name(Code)	cust_Object(cust_Object)	GOField-Definition.Name(GO-FieldDefinition.Code)	sfFields.sffField1(cust_string)	Condition.Name(Condition.Code)	(cust_string)	Condition.FieldId		cust_String	I

## 9.2.9 Job Scheduler Requests Report

Learn about the [Job Scheduler Requests](#) report and how to read it.

The [Job Scheduler Requests](#) report describes changes made to scheduled job requests created in [Job Scheduler](#), such as creation of a new job.

### How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Changed By User (Username)	User name of the person who made the change. The value can be: <ul style="list-style-type: none"> <li>A provisioner ID</li> <li>A user ID</li> <li>Empty (if it's a system-initiated change)</li> </ul>
Context Key 1	"JOB_REQUEST" indicates that the corresponding context is a job request.
Context Value 1	The job request ID that was changed.
Field Name	The name of the field that was changed.
Old Value	Old value of the field before the change.
New Value	New value of the field after the change.

## Examples

### ❖ Example

The system admin submits a scheduled job request.

The [Job Scheduler Requests](#) report includes the following information:

Changed By User (User- name)	Context 1 Key	Context 1 Value	Field Name	Old Value	New Value	Operation Performed	Timestamp
admin	JOB_RE- QUEST	1352	STATUS	NEW	SUBMITTED	U	2019-08-06T 22:54:34Z

### ❖ Example

The system admin creates a new job request.

The [Job Scheduler Requests](#) report includes the following information:

Changed By User (User- name)	Context 1 Key	Context 1 Value	Field Name	Old Value	New Value	Operation Performed	Timestamp
admin	JOB_RE- QUEST	4235	REQUEST_ID		5235	I	2019-08-06T 08:05:24Z

## 9.2.10 Change Audit for Locales and Customizations

You can track changes users've made to locales and customizations by looking at change audit reports that are generated on demand or on a recurring basis.

### Change Audit Report - Creation

You create the change audit report for locales and customizations using the admin tool [Change Audit Reports](#), under the "Create Configuration Data Report" tab. For detailed instructions on how to obtain a change audit report, see "Creating a Change Audit Report" and "Downloading a Change Audit Report" in Related Information.

### Change Audit Report - Interpretation

A change audit report contains data common in every report as well as data specific to a particular feature or module. To understand the general structure of a report and standard data contained, see "Interpreting a Change Audit Report" and "Standard Data Included in All Change Audit Reports" in Related Information.



The following table lists the columns that are relevant to changes made on the [Manage Languages](#) page. Knowing the purpose of each column helps you find out what changes have been made to your locales and customizations.

#### Key Columns in Audit Change Report for Locales and Customizations

Column	Description
Module	For the Locales and Customizations audit change report, it's always "Platform".
Functional Area	For the Locales and Customizations audit change report, it's always "Localization".
Context 1 Key and Value	Context 1 Key is the data affected by a change, which could be any of the following: <ul style="list-style-type: none"> <li>Custom translation: The custom translation of a locale was being operated on.</li> <li>Locale flag: The flag representing a locale was affected.</li> <li>Labels: Individual labels were affected.</li> <li>Locale: A specific locale was affected.</li> <li>Limit configuration: Limits on number of keys and file size of a custom translation file were affected.</li> </ul>
Context 2 Key and Value	Context 2 Key is the change source, which could be any of the following: <ul style="list-style-type: none"> <li>Admin Center: The change was made directly in Admin Center.</li> <li>Provisioning: The change was made directly in Provisioning.</li> <li>Secondary Logon in Provisioning: The change was made through secondary login in Provisioning.</li> </ul>
Context 3 Key and Value	Context 3 Key is the locale affected, which could be any locale enabled in your system.
Field Name	Field name identifies an object that was operated on, such as custom translation, label, language, flag image, and limit configuration.
Old Value and New Value	Each object (field) that was being operated on can have an old value and a new value. For some operation, there might be just one value. For example, when a custom translation was deleted, the old value may be zh_CN but the new value is null.
Operation	Type of operation that results in the change, including: <p>I: Indicates an insert operation, such as when a custom translation was added.</p> <p>U: Indicates an update operation, such as when a language was changed from enabled to disabled.</p> <p>D: Indicates a delete operation, such as when a custom translation was deleted.</p>

## Related Information

[Creating a Change Audit Report \[page 15\]](#)

[Downloading a Change Audit Report \[page 21\]](#)

[Interpreting a Change Audit Report \[page 22\]](#)

[Standard Data Included in All Change Audit Reports \[page 30\]](#)

### 9.2.11 Manage Support Access Change Report

Learn about the [Manage Support Access](#) report and how to read it.

The [Manage Support Access](#) report describes changes made to support access in the [Manage Support Access](#) admin tool.

#### How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that's specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Context 1 Key	User Id
Context Value 1	The user ID of a support account.
Context 2 Key	User Name
Context 2 Value	The user name of a support account.
Field Name	The name of the field that was changed in <a href="#">Manage Support Access</a> .
Old Value	Old value of the field before the change.
New Value	New value of the field after the change.
Operation Performed	Indicates that the a support access is added or updated.  I is for Insert and indicates that a new support account was created.  U is for update and indicates that a support account was up-dated.
Timestamp	The time and date of the change.

## 9.2.12 Email Configurations Change Audit Report

Learn how to read the change audit report for email notification configurations.

Key Columns in Audit Change Report for Manage Email Notifications

Field Name	Description
IS_SINGLE_SENDER	Whether the single sender is enabled
SINGLE_SENDER_NAME	The name of the single sender name
SINGLE_SENDER_EMAIL	The email address of the single sender
IS_SINGLE_RECIPIENT	Whether the single recipient is enabled
SINGLE_RECIPIENT_NAME	The name of the single recipient
SINGLE_RECIPIENT_EMAIL	The email address of the single recipient
EMAIL_HEADER_FOR_ORIGINAL_RECIPIENT	The header name for TO recipients
EMAIL_HEADER_FOR_ORIGINAL_CC	The header name for CC/BCC recipients
FORWARD_EMAILS	Whether <a href="#">Forward Options</a> is enabled: <ul style="list-style-type: none"><li>• <a href="#">All</a>: forward all emails</li><li>• <a href="#">Customized</a>: Only forward emails addressed to specified domains</li></ul>
FORWARD_DOMAINS	When the forward option is customized, only forward emails addressed to domains listed in this field.
DOMAIN_NAME	Domains being added or updated to be used for the single sender

## 9.3 Business Data Audit Reports

Business data audit reports include changes to other types of data records in your system, such as transactional data in a business process.

Business data audit reports are available on the [Create Business Data Report](#) tab when you enable the [General Audit](#) setting.

Report	Description
<a href="#">User Change</a>	Use this report to audit changes to user accounts and user information.
<a href="#">MDF Change History Data</a>	Use this report to audit changes to Metadata Framework (MDF) data, for non-personal data.
<a href="#">Employee Profile Data Change</a>	Use this report to audit changes to background information on the employee profile.

[User Change Report \[page 60\]](#)

Learn about the [User Change](#) report and how to read it.

[MDF Change History Data Report \[page 61\]](#)

Learn about the [MDF Change History Data](#) and how to read it.

#### [Employee Profile Data Change Report \[page 66\]](#)

Learn about the [Employee Profile Data Change](#) report and how to read it.

#### [Employee Central Object and Element Audit Configuration \[page 69\]](#)

Track personal data of employees for downstream integrations, support SAP SuccessFactors HCM suite processes and reporting. Understand and report out your Employee Central configuration changes by using the table below. The table identifies all areas of Employee Central where object and/or element configuration can be changed and how. For example, by adding a field, changing a field name, or making a field required. Run reports of your configuration changes including who made the changes and provide scheduled and/or ad hoc reports to required teams.

#### [Dynamic Teams Data Change Report \[page 76\]](#)

Learn about the [Dynamic Teams Data Change](#) report and how to read it.

#### [Objectives and Key Results Data Change Report \[page 78\]](#)

Learn about the [Objectives and Key Results Data Change](#) report and how to read it.

## 9.3.1 User Change Report

Learn about the [User Change](#) report and how to read it.

The [User Change](#) report describes changes made to user accounts and user information in your system.

### How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Subject User	In the User Change report, the Subject User is the person whose user information was changed.
Context 1 Key	"Admin Action" indicates that the corresponding context value is an admin tool.
Context 1 Value	The name of the admin tool used to make the change
Field Name	The name of the user information field that was changed
Old Value	Old value of the user information field before the change.
New Value	New value of the user information field after the change.

## Examples

### ❖ Example

You manually log into the system as the admin user "sfadmin" and make changes to user information for Jimmy Klein (username "jklein"). You change his first name from "James" to "Jimmy".

The [User Change](#) report includes the following information:

Changed By User (User-name)	Proxy: Logged in User (User-name)	Subject User (First Name)	Subject User (Last Name)	Subject User (User-name)	Context 1 Key	Context 1 Value	Field Name	Old Value	New Value
sfadmin		Jimmy	Klein	jklein	Admin Action	Manage Users	First Name	James	Jimmy

### ❖ Example

You log in as the admin user "sfadmin" and use [Proxy Now](#) to act as a proxy on behalf of another admin user "twalker". While logged in as a proxy for "twalker", you change user information for Raymond Akoshile (username "rakoshile"). You change his first name from "Ray" to "Raymond".

The [User Change](#) report includes the following information:

Changed By User (User-name)	Proxy: Logged in User (User-name)	Subject User (First Name)	Subject User (Last Name)	Subject User (User-name)	Context 1 Key	Context 1 Value	Field Name	Old Value	New Value
twalker	sfadmin	Raymond	Akoshile	rakoshile	Admin Action	Manage Users	First Name	Ray	Raymond

## 9.3.2 MDF Change History Data Report

Learn about the [MDF Change History Data](#) and how to read it.

The [MDF Change History Data](#) report describes data in the change history of MDF data. MDF data is any data record that is stored in an MDF object.

### How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Context 1 Key	Indicates the field names of external name and external code of root object.
Context 1 Value	Values of external name and external code of root object.
Context 2 Key	Indicates the field names of external name and external code of current child object concatenated with child object type. This field isn't used, if current object is the root object.
Context 2 Value	Values of external name and external code of current child object. The values aren't used, if current object is root object.
Field Name	The name of the field that was changed. If it is a field of a child object, field name is concatenated with the association name between the child object and its parent object.
Old Value	Old value of the field before the change.
New Value	New value of the field after the change.

## Examples

### ❖ Example

For example, the [MDF Change History Data](#) report might include the following information.

Changed By User (User-name)	Context 1 Key	Context 1 Value	Context 2 Key	Context 2 Value	Field Name	Old Value	New Value	Operation Performed
sfadmin	Name(Code )	Parent Object(ParentObject)	ChildObject.Name(ChildObject.Code)	Child Object(ChildObject))	Children.Age		7	I

### 9.3.2.1 Generating Business Configuration UI Audit Logs (Business Data Reports) in Admin Center

As an Admin, you can use self-service audit reporting tools in [Admin Center](#) to generate and download change audit reports in CSV format.

## Prerequisites

1. You have set up Change Audit in your system. For more information, refer to [Setting Up Change Audit](#).

2. You have the role-based [Generate Change Audit Reports](#) permission.
3. If you plan to set up a recurrence schedule that saves reports to SFTP, be sure that you have the technical details required to set up the connection. If you plan to use file encryption, be sure that you have already imported your PGP public key on the PGP Key Management page. For more information, refer to [Importing PGP File Encryption Keys](#)

## Context

Change audit reports are offline reports containing audit data about changes in your system. The [MDF Change History Data](#) report describes data in the change history of MDF data. MDF data is any data record that is stored in an MDF object.

## Procedure

1. Go to the [Admin Center](#).
  2. In the [Tools Search](#) field, enter [Change Audit Reports](#).
  3. Select [Create Business Data Report](#) tab.
- A dialog opens where you can configure the report settings.
4. Click on [MDF change History Data](#) and enter the following details:

Parameter	Description
Change by Person	Indicates the First name, last name, and username of the person (or user account) who made the change. You can enter either <a href="#">Change by Person</a> or <a href="#">External Code</a> .
Object Type	<p>Select the object type from the below list for which you can download the audit logs:</p> <ul style="list-style-type: none"><li>• Background Element</li><li>• EP View Template Config</li><li>• Employee Profile Standard</li><li>• Employee Profile User Info</li><li>• Field Display Format</li><li>• Format Group</li><li>• Number Format</li><li>• Section</li><li>• Tab Element</li><li>• CustomFilterConfig</li><li>• DGFiltersConfig</li></ul> <p>The Object Type can be:</p> <ul style="list-style-type: none"><li>• HRIS Element</li><li>• Localized HRIS Element</li><li>• Dynamic Group Filters</li></ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>Employee Profile User Info</li> <li>HRIS Action</li> <li>Custom Filter</li> </ul>
External Code	Enter the external code such as JobInfo, ComplInfo, and so on.
Time Range	Configure the time range you want to report on, up to a maximum of seven days.

→ Remember

Change audit reports cover a maximum time range of seven days. If you want to audit changes over a longer period of times, create multiple reports. For example, if you want to audit changes made over the course of a month, run four separate reports of seven days each.

5. Use the [Recurrence](#) switch to set up a recurrence schedule.
- [No](#) means that there is no recurrence and we try to generate the report as soon as you submit it. [No](#) is the default setting.
  - [Yes](#) means that you want the report to be generated on a recurring schedule that you define.

To define a recurrence schedule, fill out the following information.

Field	Description
Schedule Name	The name of the recurrence schedule on the <a href="#">View Schedules</a> tab.
Method	<p>The location of the generated report file.</p> <ul style="list-style-type: none"> <li>Select <a href="#">Offline</a> to access the report within the application, on the <a href="#">Access Reports</a> tab.</li> <li>Select <a href="#">Secure File Transfer Protocol (SFTP)</a> to access the report in your SFTP folder.</li> </ul>
SFTP settings	<p>If you select the SFTP access method, set up the required technical details to connect to your SFTP server. Then continue to create your report.</p> <p>For more information, refer to <b>Setting Up SFTP Settings for a Recurring Change Audit Report</b> in the Related links section.</p>
Recurring Pattern	When and how often you want the report to be generated (Daily, Weekly, Monthly, Yearly).
Start	Date and time when the recurrence begins.
End	Date and time when the recurrence ends.



## Note

If you set up a recurrence schedule, the exact dates you select as the time range apply to the **first occurrence** of the report only. With each recurrence, the dates are adjusted accordingly. For example, if you set up an initial time range of April 1 to April 7 with a monthly recurrence starting on April 15, the first occurrence of the report on April 15 includes changes between April 1 and April 7, the second occurrence on May 15 includes changes between May 1 and May 7, and so on.

## Tip

As a best practice, set up report generation to recur at least three days after the end of the time range you want to audit. Some types of audit data can take up to 72 hours to be made ready for reporting.

6. Submit the report.

## Results

If you did not set up a recurrence schedule, the report generation job is scheduled immediately but it may take some time to prepare. It may take just a few minutes, but, if there is a lot of data, it can take longer. You receive an email notification when the report is complete (or if it has failed).

If you set up a recurrence schedule, the first report is generated on the exact date and time configured in the recurrence pattern, following the start date. Each subsequent report is generated on the configured day, at the configured time, but on the dates are adjusted accordingly.

## Next Steps

You can download and save your Change Audit report when it is available so that you can investigate changes made in your system. On the [Access Reports](#) tab, find the report you want to download. For more information on downloading and reading a Change Audit report, refer to the Related Links section.

## Note

The operations supported in [Admin Center](#) are Update, Delete, and Insert.

## Example

For example, the MDF Change History Data report might include the following information.

Report Name	Change Audit Report															
Report GUID	3e70c748-e3b0-406d-bf1e-b83836302bb9															
Report Creator User ID	adminb1															
Data Operator	adminf pwd															
Modules																
Functional Areas																
Time Range (Start)	2019-06-03T09:57:00Z															
Time Range (End)	2019-06-06T09:57:00Z															
Changed By User (First Name)	Changed By User (Last Name)	Changed By User (Username)	Module	Functional Area	Functional Sub Area	Context 1 Key	Context 1 Value	Context 2 Key	Context 2 Value	Field Name	Old Value	New Value	Operation Performed	Timestamp	Effective Start Date	Effective Sequence
sadmin	SF	admin	Foundation	PLT_AUDITLOGGING_MDF_CHANGE_HIST	Localized HRIS Element	Name(Code)	Time and Schedule Information(JobInfo, USA)	ECLocalElementFieldConfigName(ECLocalElementFieldConfig.Code)	TestCustString(USA)(custom-string94)	Label US English	TestCustString	TestCustStringUSA	U	2019-06-04T04:25:21Z	2019-06-04T04:25:21Z	0
adminf	SF	adminb1	Foundation	PLT_AUDITLOGGING_MDF_CHANGE_HIST	Localized HRIS Element	Name(Code)	Time and Schedule Information(JobInfo, USA)	ECLocalElementFieldConfigName(ECLocalElementFieldConfig.Code)	TestCustString(USA)(custom-string94)	Localized HRIS Fields.Maximum Length		250	U	2019-06-04T04:25:21Z	2019-06-04T04:25:21Z	0

## Related Information

[Setting Up SFTP Settings for a Recurring Change Audit Report](#)

[Downloading a Change Audit Report](#)

[Reading an MDF Change History Data Report](#)

### 9.3.3 Employee Profile Data Change Report

Learn about the [Employee Profile Data Change](#) report and how to read it.

The [Employee Profile Data Change](#) report includes two report types: [Background Data Change](#) and [Feedback Data Change](#). The two reports describe changes made to background information or feedback information on the Employee Profile respectively.

#### How to Read the Report


In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Context fields	Context key-value pairs aren't used in this report, so they're all blank.
Field Name	The name of the background/feedback element and background/feedback data field that was changed, separated by a slash. For example, in a <a href="#">Background Data Change</a> report, <b>Previous Employment/Start Date</b> indicates that the <b>Start Date</b> data field was changed in the <b>Previous Employment</b> background element.
Old Value	Old value of the data field before the change.
New Value	New value of the data field after the change.
Operation Performed	Type of operation that made the change, as with all reports.

#### Note

You can use the Operation Performed to determine if the change was made in the user interface or with an Extended User Information import file. An Update operation indicates a change via the user interface. A Delete operation followed by an Insert operation indicates a change via import.

Field	Description
Timestamp	Time and date of the change.

 **Note**  
 If you see many changes by the same Changed By user with exactly the same timestamp, it indicates that changes were likely made with an Extended User Information import file.

## Examples

### Example

You manually log in as the admin user "sfadmin" and change background information for the user "jbaker" using the Extended User Information import file. During the same time range, the user "sbattle" changes her Willingness to Relocate flag from "no" to "yes" and the user "ghill" attaches a document "certification\_1.doc" to his employee profile.

The [Background Data Change](#) report includes the following information. The timestamp and operations performed tell you that the changes to Previous Employment/Start Date were made via import. The Update operation and Changed By User tell you that user "sbattle" updated her profile herself. The Insert operation and Changed By User tell you that the user "ghill" attached a new document to his profile himself.

Changed By User (User-name)	Subject User (User-name)	Module	Functional Area	Field Name	Old Value	New Value	Operation Performed	Timestamp
sfadmin	jbaker	Employee Profile	Background	Previous Employment/Start Date	11/26/2019		D	2019-04-16 T05:30:05Z
sfadmin	jbaker	Employee Profile	Background	Previous Employment/Start Date		11/26/2018	I	2019-04-16 T05:30:05Z
sfadmin	jbaker	Employee Profile	Background	Previous Employment/End Date	1/5/2019 0:00		D	2019-04-16 T05:30:05Z
sfadmin	jbaker	Employee Profile	Background	Previous Employment/End Date		1/5/2016 0:00	I	2019-04-16 T05:30:05Z

Changed By User (User-name)	Subject User (User-name)	Module	Functional Area	Field Name	Old Value	New Value	Operation Performed	Timestamp
sfadmin	jbaker	Employee Profile	Background	Previous Employment/ Company Name	ACE		D	2019-04-16 T05:30:05Z
sfadmin	jbaker	Employee Profile	Background	Previous Employment/ Company Name		BestRun	I	2019-04-16 T05:30:05Z
sbattle	sbattle	Employee Profile	Background	Geographic Mobility/ Willing to Relocate?	no	yes	U	2019-04-15 T011:3015Z
ghill	ghill	Employee Profile	Background	Documents/ Document Name		certification_1	I	2019-04-17 T08:30:09Z

### ❖ Example

You manually log in as the admin user "sfadmin" and change feedback information for the user "jbaker" using the Extended User Information import file.

The [Feedback Data Change](#) report includes the following information. The timestamp and operations performed tell you that the changes to Performance Rating/Start Date were made via import. The admin also imported the rating label and rating for "jbaker".

Changed By User (User-name)	Subject User (User-name)	Module	Functional Area	Field Name	Old Value	New Value	Operation Performed	Timestamp
sfadmin	jbaker	Employee Profile	Feedback	Performance Rating/Start Date	11/26/2019		D	2019-04-16 T05:30:05Z
sfadmin	jbaker	Employee Profile	Feedback	Performance Rating/Start Date		11/26/2018	I	2019-04-16 T05:30:05Z
sfadmin	jbaker	Employee Profile	Feedback	Performance Rating/End Date	1/5/2019 0:00		D	2019-04-16 T05:30:05Z

Changed By User (User-name)	Subject User (User-name)	Module	Functional Area	Field Name	Old Value	New Value	Operation Performed	Timestamp
sfadmin	jbaker	Employee Profile	Feedback	Performance Rating/End Date		1/5/2016 0:00	I	2019-04-16 T05:30:05Z
sfadmin	jbaker	Employee Profile	Feedback	Performance Rating/Rating Label		Good	I	2019-04-16 T05:30:05Z
sfadmin	jbaker	Employee Profile	Feedback	Performance Rating/Rating		2	I	2019-04-16 T05:30:05Z

### 9.3.4 Employee Central Object and Element Audit Configuration


Track personal data of employees for downstream integrations, support SAP SuccessFactors HCM suite processes and reporting. Understand and report out your Employee Central configuration changes by using the table below. The table identifies all areas of Employee Central where object and/or element configuration can be changed and how. For example, by adding a field, changing a field name, or making a field required. Run reports of your configuration changes including who made the changes and provide scheduled and/or ad hoc reports to required teams.

#### Limitations

- It is currently not possible to audit business rules at field level. The audit is only possible at the header level.

Block or Area	Type	ID	How Updated	Fields Affected	Current Audit Method	Audit Report
Personal Information	hris-element	personalInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>First Name</li> <li>Last Name</li> <li>Gender</li> <li>Marital Status</li> </ul>	BCUI Audit report	Create Business Data Report

Block or Area	Type	ID	How Updated	Fields Affected	Current Audit Method	Audit Report
		personInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Country of Birth</li> <li>Date of Birth</li> <li>Person ID</li> </ul>	BCUI Audit report	Create Business Data Report
		nationalIdCard	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Country</li> <li>isPrimary</li> <li>Type</li> </ul>	BCUI Audit report	Create Business Data Report
		nationalIdCard	Country/Region-Specific Succession Data Model/BCUI	Format of National ID card	BCUI Audit report	Create Business Data Report
		homeAddress	Succession Data Model/BCUI	Address 1, 2, 3 (not country/region specific)	BCUI Audit report	Create Business Data Report
		homeAddress	Country/Region-Specific Succession Data Model/BCUI	Address 1,2,3, province/state with country/region-specific formatting	BCUI Audit report	Create Business Data Report
		globalInfo	Country/Region-Specific Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Challenged</li> <li>Ethnic Group</li> <li>Student</li> <li>Veteran Status</li> </ul>	BCUI Audit report	Create Business Data Report
		emailInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Address</li> <li>isPrimary</li> <li>Type</li> </ul>	BCUI Audit report	Create Business Data Report
		phoneInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>isPrimary</li> <li>Number</li> <li>Type</li> </ul>	BCUI Audit report	Create Business Data Report
		imInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Email</li> <li>isPrimary</li> <li>Username</li> </ul>	BCUI Audit report	Create Business Data Report

Block or Area	Type	ID	How Updated	Fields Affected	Current Audit Method	Audit Report
		emergencyContactPrimary	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Address</li> <li>Email</li> <li>isPrimary</li> <li>Name</li> <li>Phone</li> <li>Relationship</li> </ul>	BCUI Audit report	Create Business Data Report
		personRelationshipInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Dependent information</li> <li>Name</li> <li>Relationship</li> </ul>	BCUI Audit report	Create Business Data Report
		workPermitInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Document Type</li> <li>Document Title</li> <li>Expiration Date</li> <li>Issue Date</li> </ul>	BCUI Audit report	Create Business Data Report
		paymentInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Payment Method</li> </ul>	BCUI Audit report	Create Business Data Report
		<div>  <b>Note</b>            All other fields of object are controlled by the Payment Information generic object.         </div>				
Employment Information	hris-element	userAccountInfo	Succession Data Model/BCUI	username	BCUI Audit report	Create Business Data Report
		jobInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Employee Class</li> <li>Job Code</li> <li>Job Title</li> <li>Position</li> <li>Pay Grade</li> <li>Regular/ Full Time</li> </ul>	BCUI Audit report	Create Business Data Report

Block or Area	Type	ID	How Updated	Fields Affected	Current Audit Method	Audit Report
		jobInfo	Country/ Region-Specific Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>EEO</li> <li>FLSA</li> <li>Any country/region specific job-related fields</li> </ul>		
		employmentInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>First day worked</li> <li>Hire date</li> <li>OK to Re-hire</li> <li>Original Hire Date</li> </ul>		
		jobRelationsInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Name</li> <li>Relationship Type</li> </ul>		
		compInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Pay Frequency</li> <li>Comparison</li> </ul>		
		payComponentRecurring	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Amount</li> <li>Currency</li> <li>Frequency</li> <li>Pay component</li> </ul>		
		payComponentNonRecurring	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Amount</li> <li>Currency</li> <li>Frequency</li> <li>Pay component</li> </ul>		
		pensionPayoutInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Start Date</li> <li>End Date</li> <li>Pension Provider</li> </ul>		
		globalAssignmentInfo	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>Assignment type</li> <li>Start date</li> <li>Planned end date</li> </ul>		



Block or Area	Type	ID	How Updated	Fields Affected	Current Audit Method	Audit Report
		Concurrent Employment	Succession Data Model/BCUI	Country		
		Contingent Worker	Succession Data Model/BCUI	isContingent-Worker		
Take Action	hris-action	terminateAction	Succession Data Model/BCUI	Termination Action text display	BCUI Audit report	Create Business Data Report
Filters	dg-filters	permission-group-filter	Succession Data Model/BCUI	<ul style="list-style-type: none"> <li>jobInfo fields</li> <li>employmentInfo fields</li> </ul>	BCUI Audit report	Create Business Data Report
Foundation -Organization Information	MDF Object	BusinessUnit	Configure Object Definition		MDF Configuration Change Audit Reports	MDF Configuration Data report
		CostCenter	Configure Object Definition			
		Department	Configure Object Definition			
		Division	Configure Object Definition			
		LegalEntity	Configure Object Definition			
		LegalEntityLocal	Configure Object Definition			
	hris-element	corporateAddress	Corporate Data Model		None	None
		corporateAddress	Country/Region-Specific Corporate Data Model			
		locationGroup	Corporate Data Model	Grouping locations together for reporting purposes		
		geozone	Corporate Data Model	US_EAST, US_WEST, US_MIDWEST, grouping locations together for the purpose of compensation		

Block or Area	Type	ID	How Updated	Fields Affected	Current Audit Method	Audit Report
		location	Corporate Data Model			
Foundation - Pay Information	hris-element	payRange	Corporate Data Model		None	None
		payGrade	Corporate Data Model			
		payComponent	Corporate Data Model			
		payComponentGroup	Corporate Data Model			
	MDF Object	PayGroup	Configure Object Definition		MDF Configuration Change Audit Reports	MDF Configuration Data report
		PayCalendar	Configure Object Definition			
		JobClassification	Configure Object Definition			
		JobClassificationLocal	Configure Object Definition			
		JobFunction	Configure Object Definition			
Foundation - Frequency	hris-element	Frequency	Corporate Data Model		None	None
Foundation - Dynamic Role	hris-element	dynamicRole	Corporate Data Model		None	None
		dynamicRoleAssignment	Corporate Data Model			
Foundation - Workflow	hris-element	wfConfig	Corporate Data Model		None	None
		wfStepApprover	Corporate Data Model			
		wfConfigContributor	Corporate Data Model			
		wfConfigCC	Corporate Data Model			

Block or Area	Type	ID	How Updated	Fields Affected	Current Audit Method	Audit Report
Foundation - Events	hris-element	eventReason	Corporate Data Model	<ul style="list-style-type: none"> <li>Hire</li> <li>Leave of Absence</li> <li>Promotion</li> <li>Rehire</li> <li>Termination</li> <li>Transfer</li> </ul>	None	None
HRIS Sync Mappings	hris-sync-mappings	Mapping between HRIS Elements	Succession Data Model/BCUI		None	None
Generic Objects	generic objects	Advances	Configure Object Definition		MDF Configuration Change Audit Reports	MDF Configuration Data Report
		Deductions	Configure Object Definition			
		Alternative Cost Distribution	Configure Object Definition			
		Apprentice Management	Configure Object Definition			
		Company Structure Overview	Configure Object Definition			
		Country	Configure Object Definition			
		Dependents Management	Configure Object Definition			
		Dismissal Protection	Configure Object Definition			
		Employee Central Help Text	Configure Object Definition			
		Document Generation	Configure Object Definition			
		Fiscal Year	Configure Object Definition			
		IT Declaration	Configure Object Definition			
		Location-Based Payments	Configure Object Definition			
		Pay Scale	Configure Object Definition			
		Payment Information	Configure Object Definition			

Block or Area	Type	ID	How Updated	Fields Affected	Current Audit Method	Audit Report
		Position	Configure Object Definition			
		Work Seniority	Configure Object Definition			
MDF	Business Rules	Business Rules	Configure Business Rules		MDF Configuration Change Audit Reports	
<div> <i>Note</i> <p>Only captures the header of rule, does not capture field level rule changes.</p> </div>						
MDF	Picklists	Picklists	Picklist Center		MDF Configuration Change Audit Reports	MDF Configuration Data Report

## 9.3.5 Dynamic Teams Data Change Report

Learn about the [Dynamic Teams Data Change](#) report and how to read it.

The [Dynamic Teams Data Change](#) report describes changes made to data about dynamic teams.

### How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Context 1 Key	"ID" indicates that the corresponding context value is a team ID. This is an internal identifier that's not shown in the UI.
Context 1 Value	The team ID of the dynamic team that was changed

Field	Description
Context 2 Key	"NAME" indicates that the corresponding context value is a team name, as it appears on the screen.
Context 2 Value	The team name of the dynamic team that was changed
Field Name	<p>The name of the field that was changed:</p> <ul style="list-style-type: none"> <li>NAME is the name of a dynamic team.</li> <li>DESCRIPTION is the description of a dynamic team.</li> <li>AVATAR is the attachment file ID. This is an internal identifier that's not shown in the UI.</li> <li>AVATAR_DOWNLOAD_URL is the URL where the image file is stored. You can use this URL to download the file.</li> <li>STATUS is the status of the team. "0" means active, "1" means inactive, and "2" means deleted.</li> <li>LAST_CHANGED_BY is the username of the person who made the change and is the same as the "Changed By User (Username)" column.</li> <li>LAST_CHANGED_AT is the time and date of the change and is usually similar to the "Timestamp" column.</li> </ul>
Old Value	Old value of the data field before the change.
New Value	New value of the data field after the change.

## Examples

### ❖ Example

You log in as the admin user "sfadmin" and make changes to a dynamic team. You change the team name from "Employee Engagement" to "Employee Engagement Team". You add a team description and avatar image.

The [Dynamic Teams Data Change](#) report includes the following information:

Changed By User (User-name)	Module	Functional Area	Context 2 Key	Context 2 Value	Field Name	Old Value	New Value	Operation Per-formed	Time-stamp
sfadmin	Dynamic Teams	Dynamic Teams	NAME	Employee Engagement Team	LAST_CHANGED_BY		sfadmin	U	2023-08-21T19:43:27Z
sfadmin	Dynamic Teams	Dynamic Teams	NAME	Employee Engagement Team	LAST_CHANGED_AT	2023-08-21T19:42:43.658979600Z		U	2023-08-21T19:43:27Z

Changed By User (User-name)	Module	Functional Area	Context 2 Key	Context 2 Value	Field Name	Old Value	New Value	Operation Per-formed	Time-stamp
sfadmin	Dynamic Teams	Dynamic Teams	NAME	Employee Engagement Team	NAME	Employee Engagement	Employee Engagement Team	U	2023-08-21T19:43:27Z
sfadmin	Dynamic Teams	Dynamic Teams	NAME	Employee Engagement Team	DESCRIPTION		A team dedicated to driving employee engagement	U	2023-08-21T19:43:27Z
sfadmin	Dynamic Teams	Dynamic Teams	NAME	Employee Engagement Team	AVATAR		8676	U	2023-08-21T19:43:27Z
sfadmin	Dynamic Teams	Dynamic Teams	NAME	Employee Engagement Team	AVATAR_DOWNLOAD_URL		/sf/attach-ment?id=8676  (URL may also include other information.)	U	2023-08-21T19:43:27Z

## 9.3.6 Objectives and Key Results Data Change Report

Learn about the [Objectives and Key Results Data Change](#) report and how to read it.

The [Objectives and Key Results Data Change](#) report describes changes made to the objectives and key results (OKRs) of dynamic teams.

### How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Functional Sub Area	<p>Indicates the entity that was changed:</p> <ul style="list-style-type: none"> <li>• Objective</li> <li>• Key Result</li> <li>• Contributor</li> <li>• Objective-Goal Link</li> <li>• Key Result Comment</li> </ul>
Context fields	Context key-value pairs aren't used in this report, so they're all blank.

Field	Description
Field Name	<p>The name of the data field that was changed.</p> <p>For changes to <b>all</b> entities:</p> <ul style="list-style-type: none"> <li>LAST_MODIFIED_BY is the username of the person who made the change and is the same as the "Changed By User (Username)" column.</li> <li>LAST_MODIFIED_DATE_TIME is the time and date of the change and is usually similar to the "Timestamp" column.</li> </ul> <p>For changes to an <b>objective</b>:</p> <ul style="list-style-type: none"> <li>OBJECTIVE_NAME is the name of an objective.</li> <li>OVERALL_SCORE is the calculated overall score of the objective, based on all key results.</li> <li>END_DATE is the end date of an objective.</li> <li>STATUS_ID is the status of an objective. The ID is an internal identifier that's not shown in the UI.</li> </ul> <p>For changes to a <b>key result</b>:</p> <ul style="list-style-type: none"> <li>KEY_RESULT_NAME is the name of a key result.</li> <li>UNIT is the unit of measurement for a key result.</li> <li>TARGET_VALUE is the target value of a key result.</li> <li>ACTUAL_VALUE is the current value of a key result.</li> <li>DEFINITION_OF_SUCCESS is the percentage of the target value that's considered a success.</li> <li>DUE_DATE is the due date of a key result.</li> <li>OBJECTIVE_ID is the objective that a key result is associated with. The ID is an internal identifier that's not shown in the UI.</li> </ul> <p>For changes to <b>contributors</b>:</p> <ul style="list-style-type: none"> <li>KEY_RESULT_ID is the key result for which contributors were either added or removed. The ID is an internal identifier that's not shown in the UI.</li> </ul> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>You can't see the names of contributors in the business data audit report. For that, use the personal data audit report for a specified user.</p> </div> <p>For changes to the <b>objective-goal link</b>:</p> <ul style="list-style-type: none"> <li>OBJECTIVE_ID is the objective in Dynamic Teams that's linked to a goal in Goal Management. The ID is an internal identifier that's not shown in the UI.</li> <li>GOAL_ID is the ID of the goal in Goal Management that the objective is linked to.</li> <li>GOAL_PLAN_ID is the ID of the goal plan in Goal Management that the linked goal belongs to.</li> </ul> <p>For changes to <b>key result comments</b>:</p>



Field	Description
	<ul style="list-style-type: none"> <li>KEY_RESULT_ID is the key result for which comments were either added, updated, or deleted. The ID is an internal identifier that's not shown in the UI.</li> <li>COMMENT is the text of the comment.</li> </ul>
Old Value	Old value of the data field before the change.
New Value	New value of the data field after the change.

## Examples

### ❖ Example

You log in as the admin user "sfadmin" and make changes to an OKR. You change the objective name from "Employee Engagement" to "Increase Employee Engagement". You add a new key result "Engagement Survey" with a due date, unit of measurement, definition of success, target value, and current value. As a result of progress on the new key result, the overall score of the objective is recalculated and updated automatically.

The [Objectives and Key Results Data Change](#) report includes the following information:

Changed By User (User-name)	Module	Functional Area	Functional Sub Area	Field Name	Old Value	New Value	Operation Performed	Timestamp
sfadmin	Objectives and Key Results	Objectives and Key Results	Objective	LAST_MODIFIED_DATE_TIME	2023-08-21 T19:44:49.3 77340200Z	2023-08-21 T19:45:23.2 25345520Z	U	2023-08-21 T19:45:23Z
sfadmin	Objectives and Key Results	Objectives and Key Results	Objective	OBJECTIVE_NAME	Employee Engagement	Increase Employee Engagement	U	2023-08-21 T19:45:23Z
sfadmin	Objectives and Key Results	Objectives and Key Results	Objective	STATUS_ID	D7E60200 4C0B51371 80035FA2D 807656	D8E60200 4C0B51371 80035FA2D 807656	U	2023-08-21 T19:45:23Z
sfadmin	Objectives and Key Results	Objectives and Key Results	KeyResult	LAST_MODIFIED_DATE_TIME	2023-08-21 T19:44:49.3 16537Z	2023-08-21 T19:45:53.6 34417285Z	U	2023-08-21 T19:45:53Z
sfadmin	Objectives and Key Results	Objectives and Key Results	KeyResult	OBJECTIVE_ID		e4d1950a8 9f694de01 8a19a2a86f 042a	I	2023-08-21 T19:47:33Z
sfadmin	Objectives and Key Results	Objectives and Key Results	KeyResult	DUE_DATE		9/1/2023	I	2023-08-21 T19:47:33Z

Changed By User (User-name)	Module	Functional Area	Functional Sub Area	Field Name	Old Value	New Value	Operation Performed	Timestamp
sfadmin	Objectives and Key Results	Objectives and Key Results	KeyResult	UNIT		surveys		2023-08-21 T19:47:33Z
sfadmin	Objectives and Key Results	Objectives and Key Results	KeyResult	DEFINITION_OF_SUCCESS		70		2023-08-21 T19:47:33Z
sfadmin	Objectives and Key Results	Objectives and Key Results	KeyResult	TARGET_VALUE		100	I	2023-08-21 T19:47:33Z
sfadmin	Objectives and Key Results	Objectives and Key Results	KeyResult	ACTUAL_VALUE		50	I	2023-08-21 T19:47:33Z
sfadmin	Objectives and Key Results	Objectives and Key Results	KeyResult	KEY_RESULT_NAME		Engagement Survey	I	2023-08-21 T19:47:33Z
sfadmin	Objectives and Key Results	Objectives and Key Results	KeyResult	LAST_MODIFIED_DATE_TIME		2023-08-21 T19:47:33.613305674Z	I	2023-08-21 T19:47:33Z
sfadmin	Objectives and Key Results	Objectives and Key Results	KeyResult	LAST_MODIFIED_BY		sfadmin	I	2023-08-21 T19:47:33Z
sfadmin	Objectives and Key Results	Objectives and Key Results	Objective	LAST_MODIFIED_DATE_TIME	2023-08-21 T19:46:44.972256100Z	2023-08-21 T19:47:33.630899997Z	U	2023-08-21 T19:47:33Z
sfadmin	Objectives and Key Results	Objectives and Key Results	Objective	OVERALL_SCORE	0	50	U	2023-08-21 T19:47:33Z
sfadmin	Objectives and Key Results	Objectives and Key Results	KeyResult	LAST_MODIFIED_DATE_TIME	2023-08-21 T19:47:33.613305600Z	2023-08-21 T19:47:34.118598888Z	U	2023-08-21 T19:47:34Z
sfadmin	Objectives and Key Results	Objectives and Key Results	Objective	LAST_MODIFIED_DATE_TIME	2023-08-21 T19:47:33.630899900Z	2023-08-21 T19:47:48.898248463Z	U	2023-08-21 T19:47:48Z
sfadmin	Objectives and Key Results	Objectives and Key Results	Objective	STATUS_ID	D7E602004C0B5137180035FA2D807656	D9E602004C0B5137180035FA2D807656	U	2023-08-21 T19:47:48Z

## 9.4 Change History in Data Retention Management

Learn about [Change History in Data Retention Management](#) and how to read it.

Change history in Data Retention Management includes the following changes:

- Approving or declining a purge request

### Note

If you choose [Approve the whole series](#) in the initial approval stage, your approval isn't included in the change audit reports. This type of approval will be included in the change audit reports in a future release.

- Deleting purge requests
- Deleting preview or complete purge reports
- Purging inactive users by [DRTM Master Data Purge](#) or [Purge Inactive User](#)

### Note

When choosing [Changes on subject user](#) as the activity, you need to enter a user ID manually because the subject user has been purged and can't be searched.

## How to Read the Report

In addition to standard change audit data, some columns in this report contain audit data that is specific to this type of change. To understand audit data in this report, you have to understand the meaning of each context key, context value, field name, and field value.

Field	Description
Context 1 key/value	Request name
Context 2 key/value	When the subject user is defined by a uploaded list or other criteria, this field shows the criteria of the purge request. When only one user is selected in the setup of the purge request, this field shows the assignment ID of the purged user.
Context 3 key/value	When the subject user is defined by a uploaded list or other criteria, this field is left empty. When only one user is selected in the setup of the purge request, this field shows the user ID of the purged inactive user.
Context 4 key/value	The field is only available when the change audit record is for a specific purged inactive user and it shows the creator of the purge request.
Context 5 key/value	The field is only available when the change audit record is for a specific purged inactive user and it shows the approvers of the purge request.

## Examples

### ❖ Example

You manually log in as the admin user "sfadmin". You approved a purge request named "DRTM Master Data Purge [938]". Later, you deleted the preview report and the complete report. These actions are captured in the report like the following:

Changed By User (First Name)	Changed By User (Last Name)	Changed By User (User-name)	Module	Functional Area	Functional Sub Area	Context 1 Key	Context 1 Value	Context 2 Key	Context 2 Value	Field Name	Old Value	New Value	Time-stamp
admin	sf	sfad-min	Administration	Data Retention Management	DRTM MasterDataObject Type	Request Name	DRTM Master Data Purge [938]	Criteria	{ "exclusionFilters": [ "UserBasedCompEntryReportGeneratorFilter" ], "idFilters": null, "purgeObjectList": null, "rule": { "active": false, "countries": [], "dataValid": false, "immediatePurge": false, "inactive": false, "legalEntities": [], "uploadFileName": null, "uploaded": null, "userId	Purge Request Status		Approved	2021-09-14T06:00:13Z

Chang ed By User (First Name)	Chang ed By User (Last Name)	Chang ed By User (User- name)	Mod- ule	Func- tional Area	Func- tional Sub Area	Con- text 1 Key	Con- text 1 Value	Con- text 2 Key	Con- text 2 Value	Field Name	Old Value	New Value	Time- stamp
									":mas terDa- taPur- ge- SUPT2 165" }, "ver- sion": " 2.0" }				

Chang ed By User (First Name)	Chang ed By User (Last Name)	Chang ed By User (User- name)	Mod- ule	Func- tional Area	Func- tional Sub Area	Con- text 1 Key	Con- text 1 Value	Con- text 2 Key	Con- text 2 Value	Field Name	Old Value	New Value	Time- stamp
admin	sf	sfad- min	Ad- minis- tration	Data Reten- tion Man- age- ment	DRTM Mas- terDa- taOb- ject- Type	Re- quest Name	DRTM Master Data Purge [938]	Crite- ria	{ "ex- clu- sionFil- ters": [ "User Base- dCom- pEn- tryRe- port- Gener- atorFil- ter" ], "idFil- ters":n ull, "pur- geO- bject- List":n ull, "rule": { "ac- tive":fa lse, "coun- tries": [], "da- ta- Valid":f alse, "im- medi- ate- Purge" :false, "inac- tive":fa lse, "le- galEn- tities": [], "up- loadFi- le- Name" :null, "uploa- dId":nu ll, "userId	Pre- view Report Status	De- leted	2021-0 9-13T1 0:49:2 1Z	

Chang ed By User (First Name)	Chang ed By User (Last Name)	Chang ed By User (User- name)	Mod- ule	Func- tional Area	Func- tional Sub Area	Con- text 1 Key	Con- text 1 Value	Con- text 2 Key	Con- text 2 Value	Field Name	Old Value	New Value	Time- stamp
									": "mas terDa- taPur- ge- SUPT2 165" }, "ver- sion": " 2.0" }				



Chang ed By User (First Name)	Chang ed By User (Last Name)	Chang ed By User (User- name)	Mod- ule	Func- tional Area	Func- tional Sub Area	Con- text 1 Key	Con- text 1 Value	Con- text 2 Key	Con- text 2 Value	Field Name	Old Value	New Value	Time- stamp
admin	sf	sfad- min	Ad- minis- tration	Data Reten- tion Man- age- ment	DRTM Mas- terDa- taOb- ject- Type	Re- quest Name	DRTM Master Data Purge [938]	Crite- ria	{ "ex- clu- sionFil- ters": [ "User Base- dCom- pEn- tryRe- port- Gener- atorFil- ter" ], "idFil- ters":n ull, "pur- geO- bject- List":n ull, "rule": { "ac- tive":fa lse, "coun- tries": [], "da- ta- Valid":f alse, "im- medi- ate- Purge" :false, "inac- tive":fa lse, "le- galEn- tities": [], "up- loadFi- le- Name" :null, "uploa- dId":nu ll, "userId	Com- plete Report Status	De- leted	2021-0 9-13T1 0:49:2 6Z	

Chang ed By User (First Name)	Chang ed By User (Last Name)	Chang ed By User (User- name)	Mod- ule	Func- tional Area	Func- tional Sub Area	Con- text 1 Key	Con- text 1 Value	Con- text 2 Key	Con- text 2 Value	Field Name	Old Value	New Value	Time- stamp
									": "mas terDa- taPur- ge- SUPT2 165" }, "ver- sion": " 2.0" }				

## ❖ Example

2 inactive users are purged by *DRTM Master Data Purge* and *Purge Inactive User* created by user "sfadmin" and approved by 2 other users. These actions are captured in the report like the following:

Ch an ge d By Us er (Fir st Na me )	Ch an ge d By Us er (La st Na me )	Ch an ge d By Us er (Us er- na me )	Su bje ct Us er (Fir st Na me )	Su bje ct Us er (La st Na me )	Su bje ct Us er (Us er- na me )	Mo dul e	Func tional Area	Func tional Sub Area	Co ntext 1 Key	Co ntext 1 Value	Co ntext 2 Key	Co ntext 2 Value	Co ntext 3 Key	Co ntext 3 Value	Co ntext 4 Key	Co ntext 4 Value	Co ntext 5 Key	Co ntext 5 Value	Fiel d Name	Old Value	New Value	Time stamp
ad- mi n	sf	sfa dm in	Pur ged	Us er	PU RG ED _R EC OR D_ a6 Of8 08 7-1 46 9-4 ce3 -93 fb- 3cd 4fa d3 ac2 8	Ad- mi nis- tra- tio n	Dat- a Re- ten tio n	Us- erO bje ctT ype	Re- que st Na me	Pur- ge In- ac- tive Us er [89 5]	As- sig- nm ple ID	ex- am ple ID	Us- er ID	ex- am ple Us erI D	Cre- ato r	sfa dm in	Ap- pro ver List 1, ap- pro ver 2	Sta- tus	In- ac- tive	Pur- ged	20 21- 09- 10T 07: 19: 18Z	

Ch an ge d By Us er (Fir st Na me )	Ch an ge d By Us er (La st Na me )	Ch an ge d By Us er (Us er- na me )	Su bje ct Us er (Fir st Na me )	Su bje ct Us er (La st Na me )	Su bje ct Us er (Us er- na me )	Mo dul e	Fu nct ion al Are a	Co nt e xt 1 Are a	Co nt e xt 1 Ke y	Co nt e xt 2 Ke y	Co nt e xt 2 Val ue	Co nt e xt 3 Ke y	Co nt e xt 3 Val ue	Co nt e xt 4 Ke y	Co nt e xt 4 Val ue	Co nt e xt 5 Ke y	Co nt e xt 5 Val ue	Fiel d Na me	Old Val ue	Ne w Val ue	Ti me sta mp
ad- mi n	sf	sfa dm in	Pur ged	Us er	PU RG ED _R EC OR D_ a6 Of8 08 7-1 46 9-4 ce3 -93 fb- 3cd 4fa d3 ac2 8	Ad- mi nis- tra- tio n	Dat a Re- ten tio n Ma nag em ent	DR TM Re- Ma ste rDa taO bje ctT ype	Re- que st Na me	DR TM Ma ste r Dat a Pur ge [90 8]	As- sig nm ID sig nm en- tID	Us er ID ple erl D	ex- am ple Us erl D	Cre ato r in	sfa dm in	Ap- pro ver List 1, ap- pro ver 2	ap- pro ver 1, ap- pro ver 2	Sta tus	In- ac- tive	Pur ged	20 21- 09- 10T 08: 49: 17Z

# 10 Change History

Learn about changes to the documentation for Change Audit in recent releases.

## 1H 2025

Type of Change	Description	More Info
New	We added information about change audit reports of Manage Support Access.	<a href="#">Manage Support Access Change Report [page 58]</a> <a href="#">Configuration Data Audit Reports [page 36]</a>

## 2H 2024



Type of Change	Description	More Info
New	We added information about change audit reports of locales and customizations, and email notification configurations.	<a href="#">Change Audit for Locales and Customizations [page 56]</a> <a href="#">Email Configurations Change Audit Report [page 59]</a>

# 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.

© 2025 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.