Saviynt Identity Cloud Administration Guide

Copyright

saviynt.com

CONTENTS

You can accept the risks which are causing the SOD violations identified through detective SOD analysis using the **SOD Violations** workbench. Before accepting the risk of SOD violations, you can view the summary or detailed information of associated functions with the list of conflicting entitlements. After the risk is accepted, the current status of the SOD violation will be removed from **Open** or **In process** status and moved to **Risk Accepted** status in the **SOD Violation** workbench.

To accept risks of SOD violations, perform the following steps:

1. Log in to Saviynt Identity Cloud and navigate to **SOD > SOD Violations**. Alternatively, enter **SOD Violations** in the search box and select the required menu item. For more information, see Using the Unified Navigation.

   You can accept the risk of the SOD violations which are in the following status:

   - **Open**: SOD violations which requires immediate attention and remediate actions.
   - **In Process**: SOD violations which are assigned and the remediation is in process.

2. Click the appropriate status type. The SOD violations appear based on the status.

3. Click the relevant risk name in-line with the functions in the Risk Code column.

   The value in the Risk Code column drill-downs to functions. You can view the summary or detailed information of associated functions with the list of conflicting entitlements.

The detailed view displays additional columns which covers first used, last used and total used details of entitlements. Displays the function details in the following columns.

Column	Description
Assigned Roles	Displays the assigned role. The column appears for both **Summary** and **Detailed** view.
Associated Role	Displays the associated role. The column appears for both **Summary** and **Detailed** view.
Entitlement	Displays the associated entitlement. The column appears for both **Summary** and **Detailed** view.
System Name	Displays the relevant system name. The column appears for both **Summary** and **Detailed** view.

Column	Description
Endpoint	Displays the relevant endpoint name. The column appears for both **Summary** and **Detailed** view.
Account	Displays the account name. The column appears for both **Summary** and **Detailed** view.
Entitlement Type	Displays the appropriate entitlement type. The column appears for both **Summary** and **Detailed** view.
Object	Displays the appropriate object name. The column appears only for **Detailed** view.
Field	Displays the appropriate field name. The column appears only for **Detailed** view.

Column	Description
Value	Displays the appropriate value. The column appears only for **Detailed** view.
First Used	Displays the appropriate entitlement first used date. The column appears only for **Detailed** view.
Last Used	Displays the appropriate entitlement last used date. The column appears only for **Detailed** view.
Total Used	Displays the total number of entitlement usage. The column appears only for **Detailed** view.

4. Click the Actions arrow and select **Remediate** option.
5. Before accepting risk, you can view the impact of the function. Click **VIEW IMPACT** in line with the function name to view the impact details.The Show Impact Detail pop-up window appears. It displays the following:

- **User Impact Summary**- Displays the account name of the user who is getting impacted.
- **Summary**- Displays the total number of SOD violations which is getting remediated and users impacted in numerical format

6. Click **Accept Risk** to accept the risk of the SOD violation. The Select Mitigating Control pop-up window appears.
7. Select the appropriate mitigating control in the Select Mitigation Control pop-up window and click **Next**.
8. Enter comments, review the duration of the mitigating control and click **Next**.

Note

- The risk is now accepted. The SOD violation will be removed from Open or In Process status and moved to Risk Accepted status in the SOD Violation workbench.
- Depending upon the type of function, Summary/Detailed button are displayed in the details page of the function that are accessed from the SOD Violations page.
- If the Function Type is **SAP**, the details of the function page are displayed either in the Summary view or in the detailed view. Using the toggle bar as highlighted in the screenshot below, you can change the views accordingly.

The following screenshot illustrates both the summary view and the detailed view of SAP functions.

If the Function Type is **non-SAP**, the details of the Function page are displayed only in the Summary view.

The following screenshot illustrates the summary view of non-SAP functions.

The following actions have been added under the **Actions** drop down of the **Risk accepted** tab using which you can modify mitigating controls and extend their end dates in bulk.

- Extension of bulk end date
- Bulk change MC

Extending Mitigating Control End Dates in Bulk

You can use the **Bulk Enddate Extension** action to extend the end date of mitigating controls in bulk. To extend the end dates of mitigating controls in bulk, follow these steps:

1. Log in to Saviynt Identity Cloud.

2. Navigate to **SOD > SOD Violations**. Alternatively, enter **SOD Violations** in the search box and select the required menu item. For more information, see Using the Unified Navigation

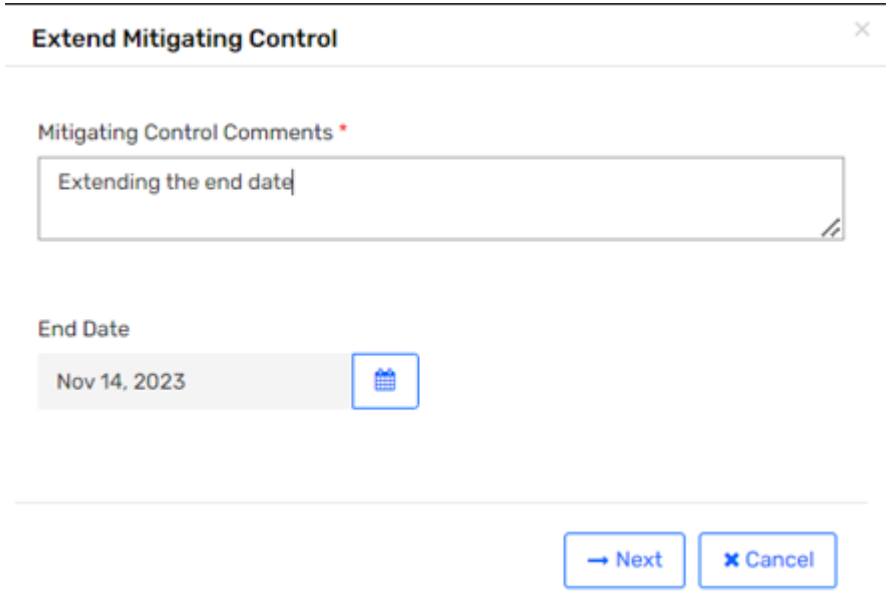
3. On the **Risk Accepted** tab, click **Actions** > **Bulk Enddate Extension**.

> **Note**
>
> Ensure that there is at least one risk listed on the **Risk Accepted** tab has at least one risk.

4. In the **RISK CODE** column, select the risk(s) for which you want to extend the end date.

> **Note**
>
> Make sure to select risks associated with the same mitigating control.

5. Navigate to the **Actions** drop down and select **Bulk Enddate Extension**. The **Extend Mitigating Control** window appears.



6. In the **Mitigating Control Comments** window, specify the reason for extending the end date of the mitigating control. In the **End Date** field, select the required new end date.

7. Click **Next**.

   The **MITIGATING CONTROL** column will now display the updated end date for the risk for which the end date has been extended.

Bulk Modification of Mitigating Controls

You can use the **Bulk Change MC** action to associate new mitigating controls to multiple risks.

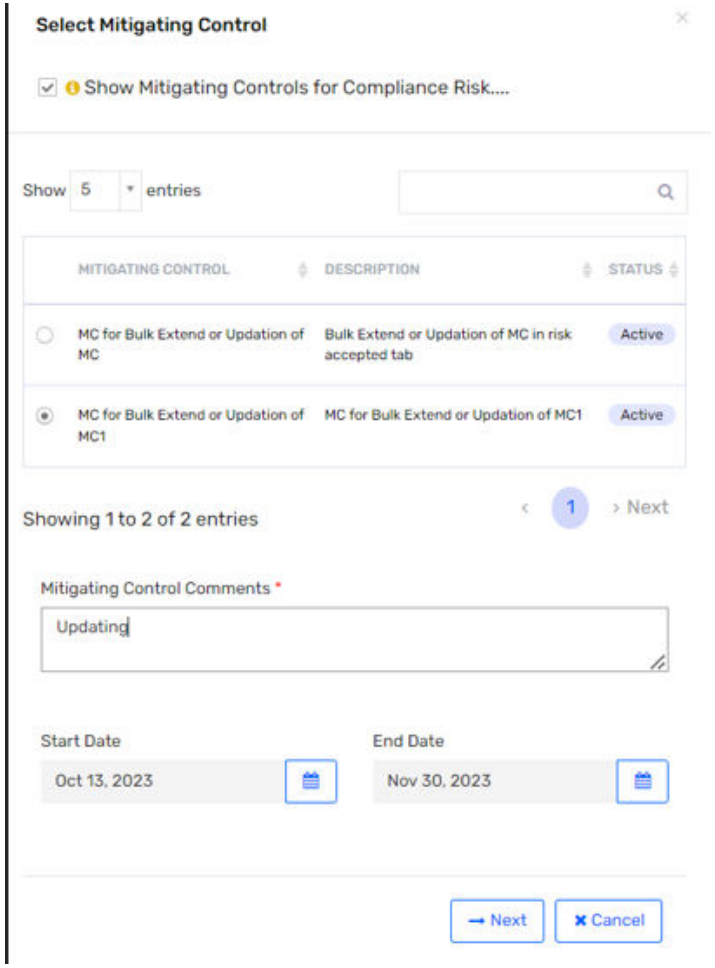
To make bulk mitigating control changes, follow these steps:

1. Log in to Saviynt Identity Cloud.
2. Navigate to **SOD > SOD Violations**. Alternatively, enter **SOD Violations** in the search box and select the required menu item. For more information, see Using the Unified Navigation
3. Navigate to the **Risk Accepted** tab and click **Actions** > **Bulk Enddate Extension**.

   Note

   Ensure that there is at least one risk listed on the **Risk Accepted** tab.

4. In the **RISK CODE** column, select the risk(s) for which you want to change the existing mitigating control.
5. Navigate to the **Actions** drop-down menu and select **Bulk Change MC**. The Select Mitigating Control window appears.



6. Choose the appropriate mitigating control, and in the **Mitigating Control Comments** section, provide your comments and select the new start and end date relevant to the mitigating control.

7. Click **Next**.

   The **MITIGATING CONTROL** column will now display the updated mitigating control, along with the new start and end date