

**Saviynt – HR System Integration Use Cases**

TABLE OF CONTENTS

[Document Control 3](#_Toc126764662)

[Use Cases 4](#_Toc126764663)

[1. UC.01 Identity Onboarding/refresh of Employees and Contractors from HR Source 4](#_Toc126764664)

[2. UC.02 Onboarding Process for Rehiring Previous Employee/Contractor 6](#_Toc126764665)

[3. UC.03 Process for Voluntary Termination of Identities 8](#_Toc126764666)

[4. UC.04 Temporary Leave of Absence for Identities 10](#_Toc126764667)

[5. UC.05 Identities Joining after Leave of Absence 12](#_Toc126764668)

[6. UC.06 Process for Non-Voluntary (Emergency) Termination of Identities 14](#_Toc126764669)

[7. UC.07 Process for Intercompany Transfer 15](#_Toc126764670)

[8. UC.08 Process for People on Legal Hold 16](#_Toc126764671)

[Appendix 18](#_Toc126764672)

# Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version control** | | | |
| **Version** | **Name** | **Role** | **Date** |
| v1 | Vineet Gupta | Author | 01/31/2023 |
| v2 | Gaurav Khandelwal | Author | 02/08/2023 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Revision history** | | | | |
| **Version** | **Changed Sections** | **Details of Change** | **Date** | **Changed By** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# **Use Cases**

## UC.01 Identity Onboarding/refresh of Employees and Contractors from HR Source

Table 1 – Identity onboarding/refresh of employees and contractors from HR Source – Use Case

|  |  |
| --- | --- |
| **Authoritative DataSource** | HR System |
| **Description** | This is the process to onboard/refresh company’s employees and contractors from HR System applications. At a high level, the HR will receive users’ information from upstream sources e.g. Workday, consolidate and transform attribute values, which will be retrieved by Saviynt to create/update/disable a user’s identity. This process can completely onboard/refresh an identity. |
| **Actors** | Saviynt and HR System |
| **Notifications** | None. |
| **Pre-condition** | 1. Saviynt is setup and ready for onboarding users’ identities and accounts. 2. HR System application has appropriately updated user identity information. |
| **Post-Condition** | None. |
| **Normal Flow** | 1. Process begins. 2. A user’s identity is onboarded in one of the trusted source (Workday)and information is consolidated into HR System. 3. Saviynt connects to the HR System to fetch user information for reconciliation.   If Saviynt can connect to the HR system, the process moves ahead. If Saviynt cannot connect, an error is logged in the log file and a ServiceNow ticket is generated by sending an email to ServiceNow distribution list using a pre-defined template. If the connection is successful, information is fetched from the HR System and new user is created based on matching rule defined using Employee ID, which will be the unique attribute provided by HR sources. For new user’s LAN ID/Enterprise ID will be generated as per business rule – X.   1. If a user’s identity already exists in Saviynt in non-terminated state, then user’s information will be updated in Saviynt database. 2. In Saviynt, user will be created with attributes mentioned in [Section HR System Attributes](#_BR02_–_Email) in Appendix 3. The new user created in Saviynt will be assigned permissions to perform operations as per the pre-defined end user role. 4. Process finishes. |
| **Alternate Flow** | None. |
| **Exception Flow** | * If the process has failed, then based on ServiceNow ticket, error will be investigated and resolved. Afterwards, process will be kicked off on ad-hoc basis. * For Day-0 Load, only Non-Terminated users will be loaded in to Saviynt Security Manager. * For Day-0 Load, lan Id will not be generated in Saviynt, it will be populated as is from the HR Systems. |

## UC.02 Onboarding Process for Rehiring Previous Employee/Contractor

Table 2 – Onboarding process for rehiring previous employee/contractor – Use Case

|  |  |
| --- | --- |
| **Authoritative DataSource** | HR System |
| **Description** | This is the process to onboard rehiring of previous Company employees or contractors from HR Systems application. At a high level, the HR System will receive users’ information from upstream sources e.g. Workday, sources consolidate and transform attribute values, which will be retrieved by Saviynt to create a new user identity or enable terminated user’s identity. Through this process, an identity who was previously a company s employee/contractor will be onboarded. |
| **Actors** | Saviynt and HR Systems |
| **Notifications** | None. |
| **Pre-condition** | 1. Saviynt is setup and ready for onboarding users’ identities and accounts. 2. HR System application has appropriately updated user identity information. |
| **Post-Condition** | None. |
| **Normal Flow** | 1. Process begins. 2. A rehiring user’s identity is onboarded in one of the trusted source (Workday) and information is consolidated into The HR System. 3. Saviynt connects to the HR System to fetch user information for reconciliation.   If Saviynt can connect to the HR System, the process moves ahead. If Saviynt cannot connect, an error is logged in the log file and a ServiceNow ticket is generated by sending an email to ServiceNow distribution list using a pre-defined template.  If the connection is successful, information is fetched from the HR System.   1. If a user’s identity already exists in Saviynt in disabled state based on Employee ID matching criteria, then user’s identity will be enabled in Saviynt. 2. If user’s identity was terminated in Saviynt and user’s target accounts are purged and if such user is hired with the same old employee Id, then the Saviynt user will be activated, and provisioning will be triggered as per the business rules. 3. Process finishes. |
| **Alternate Flow** | Users that are terminated as per UC:06 Process for non-voluntary (Emergency) termination and for whom termination is also reconciled from HR System, then such user if rehired will follow the process mentioned above.  Users that are terminated as per UC:06 Process for non-voluntary (Emergency) termination and for whom termination is not reconciled from the HR Sytem, then such user needs to be enabled from the Saviynt UI by HelpDesk before they are hired back in HR System. |
| **Exception Flow** | If the process has failed, then based on ServiceNow ticket, error will be investigated and resolved. Afterwards, process will be kicked off on ad-hoc basis. |

## UC.03 Process for Voluntary Termination of Identities

Table 3 – Process for voluntary termination of the Companies identities – Use Case

|  |  |
| --- | --- |
| **Authoritative DataSource** | HR System |
| **Description** | This is the process to initiate voluntary termination of company identities. At a high level, a user’s identity can be terminated via user import. The HR System will receive users’ information from upstream sources e.g. Workday sources and synchronize with Saviynt. Once a user’s termination information is retrieved by Saviynt or user’s identity is terminated in Saviynt, user’s identity is terminated in Saviynt and connected application accounts like Active Directory will be disabled. Through this process, an identity is completely terminated in Saviynt and connected applications. |
| **Actors** | Saviynt, HR System and other connected applications |
| **Notifications** | None. |
| **Pre-condition** | 1. Saviynt is setup and ready for terminate users’ identities and accounts. 2. HR System application has appropriately updated user identity information. 3. Other applications are connected with Saviynt to synchronize information. |
| **Post-Condition** | 1. User’s identity is terminated in Saviynt and the HR System and accounts are disabled in connected applications. |
| **Normal Flow** | 1. Process begins. 2. A user’s identity is terminated in one of the trusted source (Workday and information is consolidated into the HR System 3. Saviynt connects to HR Systemv () to synchronize user information for provisioning.   If Saviynt can connect to the HR System, the process moves ahead. If Saviynt cannot connect, an error is logged in the log file and a ServiceNow ticket is generated by sending an email to ServiceNow distribution list using a pre-defined template.  If the connection is successful, termination information is fetched from the HR System and user is disabled in Saviynt.  If HR code (value of filelocationattribute) from the HR System is “X”/”X”/”X”/”X”, the user is identified as a terminated user. Please refer to [Appendix](#_BR02_–_Email) for the full attribute mapping.   1. If a user has other connected application accounts, these accounts will be disabled along with user’s termination. 2. After X days of termination date, user’s account on downstream applications will be purged. 3. The X days of termination will not be applicable for users with legal hold. Once the legal hold is uplifted, the termination will happen from X days of (or after X days of) termination date. Refer [UC.08 Process for people on legal hold](#_UC.08_Process_for) 4. In case of a user, who is on long term LOA (user is inactive and accounts in disabled state) is terminated, the termination date will be updated on users’ profile to carry out deletion after X days. 5. Process finishes. |
| **Alternate Flow** | None. |
| **Exception Flow** | If the process has failed, then based on ServiceNow ticket, error will be investigated and resolved. Afterwards, process will be kicked off on ad-hoc basis. |

## UC.04 Temporary Leave of Absence for Identities

Table 4 – Temporary Leave of Absence of the Companies identities – Use Case

|  |  |
| --- | --- |
| **Authoritative DataSource** | HR System |
| **Description** | This is the process to temporary disable company’s identities due to leave of absence. At a high level, a user’s identity can be disabled temporarily via user import. The HR Systemwill receive users’ information from upstream sources e.g. Workdayources consolidate and transform attribute values. Once a user’s disable information is retrieved by Saviynt or user’s identity is disabled in Saviynt, user’s identity is disabled in Saviynt and connected application accounts like Active Directory will be disabled. Through this process, an identity is temporarily disabled in Saviynt and connected applications. |
| **Actors** | Saviynt, HR System and other applications |
| **Notifications** | None. |
| **Pre-condition** | 1. Saviynt is setup and ready for disable users’ identities and accounts. 2. HR System application has appropriately updated user identity information. 3. Other applications are connected with Saviynt to synchronize information. |
| **Post-Condition** | 1. User’s accounts are disabled temporarily in Saviynt, HR System and other applications. |
| **Normal Flow** | 1. Process begins. 2. A user’s identity is temporarily disabled in one of the trusted source (Workday) and information is consolidated into the HR System. 3. Saviynt connects to the HR System to synchronize user information for provisioning.   If Saviynt can connect to the HR System, the process moves ahead. If Saviynt cannot connect, an error is logged in the log file and a ServiceNow ticket is generated by sending an email to ServiceNow distribution list using a pre-defined template.  If the connection is successful, information is fetched from the HR System and user is disabled in Saviynt temporarily.  If HR code (value of File Locationattribute) from HR System is “X”/”X” and NETWORK\_ACCESS is X the user is identified as a long term LOA user. Please refer to [Appendix](#_BR02_–_Email) for the full attribute mapping.   1. If a user has other connected application accounts, these accounts will be suspended or disabled after user is disabled in Saviynt. 2. In the case, if only HR code (value of File location attribute) from HR System is updated as “X”/”X” irrespective of NETWORK\_ACCESS, then this will be termed as short term LOA. The NETWORK\_ACCESS value will not be ‘X’. 3. In short term LOA, only the File Location value will be synced on Saviynt user’s profile. User and its accounts status will not be affected. 4. In the case a user on short term LOA, goes on long term LOA i.e. the NETWORK\_ACCESS in the HR system is updated to ‘X’, then user will be inactivated in Saviynt followed by disabling its target accounts. 5. Process finishes. |
| **Alternate Flow** | None. |
| **Exception Flow** | If the process has failed, then based on ServiceNow ticket, error will be investigated and resolved. Afterwards, process will be kicked off on ad-hoc basis. |

## UC.05 Identities Joining after Leave of Absence

Table 5 – Identities joining after Leave of Absence – Use Case

|  |  |
| --- | --- |
| **Authoritative DataSource** | HR System |
| **Description** | This is the process to enable the companies’ identities due to leave of absence. At a high level, the HR System will receive users’ information from upstream sources e.g. Workday, , consolidate and transform attribute values, which will be retrieved by Saviynt to enable a user’s identity for leave of absence. Through this process, identity will be enabled. |
| **Actors** | Saviynt, the HR System and other applications |
| **Notifications** | None. |
| **Pre-condition** | 1. Saviynt is setup and ready for terminate users’ identities and accounts. 2. The HR System application has appropriately updated user identity information. 3. Other applications are connected with Saviynt to synchronize information. |
| **Post-Condition** | 1. User’s accounts are enabled in Saviynt, the HR System and other applications. |
| **Normal Flow** | 1. Process begins. 2. A user’s identity is enabled in one of the trusted source (Workday and information is consolidated into the HR System. 3. Saviynt connects to the HR System to synchronize user information for provisioning.   If Saviynt can connect to the HR System, the process moves ahead. If Saviynt cannot connect, an error is logged in the log file and a ServiceNow ticket is generated by sending an email to ServiceNow distribution list using a pre-defined template.  If the connection is successful, information is fetched from the HR System and user is processed appropriately in Saviynt as mentioned below.   1. In case of a user in Saviynt is on short term LOA, and if HR code (value of File Location attribute) from the HR System is coming as “”, this status is reflected on user profile. User and its accounts status will not be affected 2. In case of a user in Saviynt is on long term LOA and if HR code (value of File Locationattribute) from the HR System is coming as “X” then irrespective of its NETWORK\_ACCESS value, user will be activated and its target application will be enabled from suspension.   .   1. Process finishes. |
| **Alternate Flow** | None. |
| **Exception Flow** | If the process has failed, then based on ServiceNow ticket, error will be investigated and resolved. Afterwards, process will be kicked off on ad-hoc basis. |

## UC.06 Process for Non-Voluntary (Emergency) Termination of Identities

Table 6 – Process for non-voluntary (Emergency) termination of identities – Use Case

|  |  |
| --- | --- |
| **Authoritative DataSource** | HR System |
| **Description** | This is the process to terminate compnaies identities due to emergency. At a high level, user will be terminated in HR system and user’s accounts will be disabled in all applications. Saviynt will retrieve user’s information to terminate user’s identity. |
| **Actors** | HelpDesk |
| **Notifications** | 1. The User’s manager will receive a notification after user is terminated. |
| **Pre-condition** | None. |
| **Post-Condition** | 1. User’s identity is terminated in Saviynt and application accounts are disabled. |
| **Normal Flow** | * + - 1. Manager calls HelpDesk to terminate a user due to emergency.       2. HelpDesk will submit a request via update user form for emergency termination.       3. This will inactivate the user in Saviynt, set an emergency term flag on user profile and disables its target accounts.       4. A notification is sent to the user’s manager.       5. This user will not be marked for X days of deletion unless the termination flag comes from the HR System. The day this user is terminated in HR Systems and reconciled to Saviynt; this emergency terminated user will marked for deletion after X days. |
| **Alternate Flow** | None. |
| **Exception Flow** | None. |

## UC.07 Process for Intercompany Transfer

Table 7 – Process for intercompany transfer – Use Case

|  |  |
| --- | --- |
| **Authoritative DataSource** | HR System |
| **Description** | This is a process to allow transfer of employees to different departments within the company while maintaining the same identity and user account. |
| **Actors** | Saviynt, HR System and other applications |
| **Notifications** | 1. The User’s manager will receive a notification after user is transferred. |
| **Pre-condition** | 1. Saviynt is setup and ready for transferred users’ identities and accounts. 2. The HR System application has appropriately updated user identity information. 3. Other applications are connected with Saviynt to synchronize information. |
| **Post-Condition** | User’s accounts are enabled in Saviynt, the HR System and other applications. |
| **Normal Flow** | 1. Process begins. 2. A user’s department code i.e. LEGACY\_ENTITY\_INDICATOR is updated in one of the trusted sources (Workdayand information is consolidated into the HR System. 3. Saviynt connects to The HR System to synchronize user information.   If Saviynt can connect to the HR System, the process moves ahead. If Saviynt cannot connect, an error is logged in the log file and a ServiceNow ticket is generated by sending an email to ServiceNow distribution list using a pre-defined template. If the connection is successful, information is fetched from the HR System and user department code is updated in Saviynt.   1. The legacy entity indicator attribute on Saviynt user’s profile will be updated and email will be sent to users’ manager. 2. The possible values for this attribute coming from The HR System are X,X,X,X,X.Process finishes. |
| **Alternate Flow** | None. |
| **Exception Flow** | None. |

## UC.08 Process for People on Legal Hold

Table 8 – Process for people on legal hold – Use Case

|  |  |
| --- | --- |
| **Authoritative DataSource** | HR System |
| **Description** | This is a process to allow placing legal hold on a users’ identity if it is involved in a litigation. It will allow to preserve users AD accounts beyond the X days from when the identity is terminated in Saviynt. |
| **Actors** | Saviynt, AD |
| **Notifications** | The User’s manager will receive a notification after user is placed on legal hold. |
| **Pre-condition** | 1. Saviynt is setup and ready for placing users’ identities on legal hold. 2. Attribute for designating account on legal hold is identified. |
| **Post-Condition** | User’s account is disabled in Saviynt and AD accounts will not be purged till account is on legal hold. |
| **Normal Flow** | 1. Process begins. 2. Legal Team will submit a request via update user form for applying legal hold on a user. 3. This will update legal hold attribute on users’ profile as ‘Yes’ 4. Saviynt will disable the user identity on termination but does not purge AD accounts on day X of termination 5. If legal hold is uplifted after day X of termination, Saviynt should purge AD account. 6. If legal hold is uplifted within X days of termination, Saviynt will purge AD account on day X. 7. Saviynt will send email to manager when legal hold is set or uplifted. 8. Saviynt connects to The HR System to synchronize user information. |
| **Alternate Flow** | None. |
| **Exception Flow** | None. |

# **Appendix**

1. **HR Code mapping with Saviynt Lifecycle Events**

|  |  |  |
| --- | --- | --- |
| HR Code | HR Code Description | Saviynt Action |
| A | Active | Active User |
| D | Deceased | Disable -> Terminated User |
| L | Leave of Absence | Disable |
| P | Leave With Pay | Disable |
| T | Terminated | Disable -> Terminated User |
| U | Terminated With Pay | Disable -> Terminated User |
| X | Pre Employee | Active User |
| Y | Pre Employee Termination | Disable -> Terminated User |