Saviynt

Saviynt Identity Cloud Database Schema Guide

Copyright

saviynt.com

CONTENTS

About this Guide

This guide describes the keys and important database tables used to populate Identity Repository in Saviynt Identity Cloud. It describes the primary and foreign keys in the database tables and their relationships with other key tables. Additionally, it also provides descriptions of columns for important tables covered in this document.

Audience

This guide is intended for:

- Identity Administrators
- Identity and Cloud Architects
- Application Developers
- Application Owners
- Saviynt Operations Staff

Text Conventions

The following text conventions have been used in this document:

Convention	Meaning
bold	Indicates graphical user interface elements that are associated with an action.
italic	Indicates guide titles and placeholder text for which you specify values.
`inline code`	Indicates code elements, executable commands, cmd prompt input or output details, and URLs.
courier new	Indicates parameter values and directory or file paths.

Related Documents

In addition to the information provided in this guide, refer to Saviynt Documentation for related information.

Access to Saviynt Support

Saviynt customers can contact Saviynt Support at https://saviyntsupport.saviynt.com/.

Database Schema Reference

Identity Repository is the foundation on which Saviynt Identity Cloud offers the next-generation identity governance and administration capabilities. This topic provides details of the basic identity repository related objects such as users, accounts, entitlements or entitlement values, roles, security systems, endpoints, and external connections.

User represents a unique identity managed by Saviynt Identity Cloud. Each identity has only one entry in the system. Each user can be uniquely identified using a property such as username. This user can access Saviynt Identity Cloud to view access, manage access and perform administrative tasks based on the role granted within the system.

Accounts are reconciled from the target applications which are managed by Saviynt Identity Cloud. Based on the correlation rule, accounts could be associated with users. Saviynt Identity Cloud manages those accounts that are not associated with the user as Orphan, Service, System, etc. depending on its type. Typically, users have one account per application/system, but depending on the type of account (service, administration, secondary) there could be more accounts associated.

Entitlements refer to any type of access reconciled from the managed application, such as a group, role, permissions, responsibilities, etc. Entitlements are associated with accounts, which in turn, depending on their type, could be associated with users in order to provide a comprehensive view of access. Saviynt Identity Cloud supports a hierarchical entitlement model and multiple levels of access which can be reconciled and managed.

Role is a logical object in Saviynt Identity Cloud which is a collection of entitlements assigned to users. Roles are created based on your requirements and use cases. Saviynt Identity Cloud provides the capability to create, manage, and govern roles of multiple types–for example, Enterprise, Application, or Firefighter.

Security System is a logical group of endpoints used to establish a connection, drive workflows, and policies for the target application managed by Saviynt Identity Cloud. It leverages the connection to bring account, access and usage information (where applicable) into Saviynt Identity Cloud.

Endpoints are representations (instances) of the third-party application in Saviynt Identity Cloud. For example, a Unix server, database instance or production/test instances of an application. Accounts and entitlements (access) are imported to Saviynt Identity Cloud from endpoints.

Requests streamline business by enabling authorized users or business managers to request a new account or access in one or more infrastructures at a time via a fairly simple and intuitive user interface.

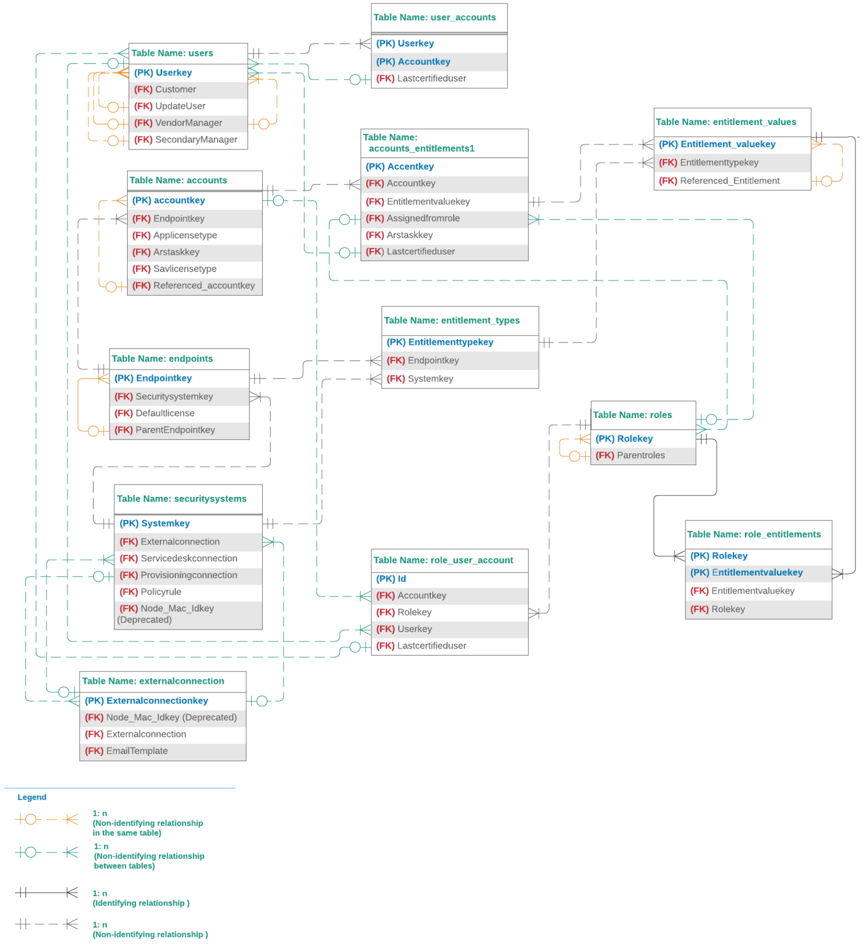
Jobs provide an ability to the administrators to manage and execute different jobs to complete the tasks for respective requests in Saviynt Identity Cloud and the target application.

SOD allows organizations to define unusual combinations of entitlements, which are not recommended to grant to a single user to prevent fraud.

External Connection refers to the configuration setup of Saviynt Identity Cloud connecting to the target application. Examples include AD, LDAP, Oracle EBS, Azure, AWS, Box, etc. For establishing a new connection to a target application, you need to have the third-party application details such as Hostname, IP Address, Username, Password, and values for configuration parameters.

Tables and Relationships in Identity Repository

The following Entity-Relationship (ER) diagram shows the key tables and their relationships in the Identity Repository Schema model.



Fields and Descriptions of Key Tables

Identity Repository is the base and foundation on top of which advanced identity governance and administration features are built-in Saviynt Identity Cloud. This topic provides information about the key tables in the Saviynt Identity Cloud repository used for performing various types of join database SQL queries and obtaining the identity details from the database tables. The tables are categorized to help you execute queries and obtain data related to Identity Repository or features.

Note

This topic describes only the important platform features used for executing join queries among the key tables in Saviynt Identity Cloud. This is only a representation of the Schema.

The following key tables are used for creating Identity Repository:

- Users Table (users)
- Customer Table (customer)
- Customer Entitlement Values Table (customer_entitlementvalues)
- Organization Owners Table (organization_owners)
- SAV Roles Table (savrole_permission)

- SAV Roles Table (savroles)
- User SAV Roles Table (user_savroles)
- Accounts Table (accounts)
- User Accounts Table (user_accounts)
- Account Entitlements Table (account_entitlements1)
- Entitlement Values Table (entitlement_values)
- Entitlement Types Table (entitlement_types)
- Endpoints Table (endpoints)
- Security Systems Table (securitysystems)
- External Connection Table (externalconnattvalue)
- Roles Table (roles)
- Role User Account Table (role_user_account)
- Role Entitlements Table (role_entitlements)
- Access Approver Table (access_approvers)
- SOD Risks Table (sodrisks)
- SOD Risk Entitlement Table (sodrisk_entitlement)
- Entitlement Map Table (entitlementmap)

- ARS Tasks Table (arstasks)
- ARS Requests Table (ars_requests)
- Request Access Table (request_access)
- qrtz_triggers Table
- qrtz_job_details Table
- qrtz_fired_triggers Table
- Duplicate Identity Management and Merge Table (identitymatchandmergedetails)
- RoleAccessMismatches
- aetrustconsolidated Table
- cac_access Table
- cac_role Table
- ruatrustconsolidated Table
- Paa_uk_evk table
- Paa_uk_rk table

Note

PK represents the Primary Key and FK represents the Foreign Key in these schema tables.

Users Table (users)

The users table stores all the details pertaining to users in Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
USERKEY(PK)	id (PK)	bigint(20)	Stores the primary key of the users table that helps you to identify a specific user from the table. You can use this key to map the user with other tables. For instance, to obtain account details of a single user, use userkey from the users table with userkey from the

Column Name	Column Name (For Querying)	Column Type	Description
			user_account table and use the join query using accountkey from the user_account table with accountkey (PK) from the accounts table.
USERNAME	username	varchar(255)	Stores the username of the users. This value is always unique for each user. It cannot be null.
PASSWORD	password	varchar(255)	Stores the user’s password.
ACCOUNTEXPIRED	accountExpired	bit(1)	Specifies whether the account has expired or not.

Column Name	Column Name (For Querying)	Column Type	Description
			• '0' indicates that the account has not expired. • '1' indicates that the account has expired.
ACCOUNTLOCKED	accountLocked	bit(1)	Specifies whether the account is locked or not. • '0' indicates that the account is not locked. • '1' indicates that the account is locked.
CITY	city	varchar(255)	Specifies the name of the city to which the user belongs.
COMMENTS	comments	varchar(255)	Stores the comments added

Column Name	Column Name (For Querying)	Column Type	Description
			for the user.
COMPANYNAME	companyname	varchar(255)	Specifies the company to which the user belongs.
STATUSKEY	statuskey	bigint(20)	Specifies whether the user is active or inactive. • '0' indicates that the user is inactive. • '1' indicates that the user is active.
COSTCENTER	costcenter	varchar(255)	Specifies the value of the cost centre assigned to the user.

Column Name	Column Name (For Querying)	Column Type	Description
COUNTRY	country	varchar(255)	Specifies the country to which the user belongs.
CREATEDBY	createdBy	varchar(255)	Specifies the username who created the user in Saviynt Identity Cloud.
CREATEDATE	createdate	datetime	Specifies the date on which the user was created.
CUSTOMPROPERTY1-50	customproperty1-50	varchar(255)	Defines custom property values in Saviynt Identity Cloud based on the application type and values configured in third-party applications for various custom-properties.

Column Name	Column Name (For Querying)	Column Type	Description
			For the Users table, you can define up to 50 custom properties.
DEPARTMENTNUMBER	departmentNumber	varchar(255)	Specifies the Department Number to which the user belongs.
DEPARTMENTNAME	departmentname	varchar(255)	Specifies the Department Name to which the user belongs.
DISPLAYNAME	displayname	varchar(255)	Specifies the Display Name as provided in the application. In Saviynt Identity Cloud, you can view and update the Display Name.

Column Name	Column Name (For Querying)	Column Type	Description
DONOTDISTURBDELEGATE	doNotDisturbDelegate	varchar(255)	Specifies whether the Do not Disturb Delegate option that allows you to select a delegate user to assign the approval tasks is enabled.
ECP	ecp	longtext	“E” stands for encryption. Specifies that the data is stored in an encrypted format when added from REST APIs but can be decrypted while retrieving it in the connection. You can use this attribute for storing less sensitive information. When this attribute is added to a connector, it is automatically

Column Name	Column Name (For Querying)	Column Type	Description
			decrypted before it is passed to the target application. In Analytics, it is displayed in the encrypted format.
EMAIL	email	varchar(255)	Specifies the user’s email id.
EMPLOYEETYPE	employeeType	varchar(255)	Specifies the Employee type, whether the type is an Employee or Contractor.
EMPLOYEECLASS	employeeclass	varchar(255)	Specifies the employee class of the user. This detail is obtained when the user is imported from the third-party application.

Column Name	Column Name (For Querying)	Column Type	Description
EMPLOYEEID	employeeid	varchar(255)	Specifies the Employee ID assigned to the employee by the employer.
ENDDATE	enddate	datetime	Specifies the end date when the employee is active in the system until that date. When the date exceeds the date specified in the end date, the employee is deactivated.
ENTITY	entity	varchar(255)	Stores the entity of the user, which is another user attribute supported by Saviynt Identity Cloud. If an entity name is specified in the third-party application, that

Column Name	Column Name (For Querying)	Column Type	Description
			entity information is available in Saviynt Identity Cloud after the user is imported.
FIRSTNAME	firstname	varchar(255)	Specifies the first name details of the employee.
HCP	hcp	tinytext	“H” stands for hashing. Specifies that after the data is added in Saviynt Identity Cloud, it is automatically hashed when it is stored in the database and cannot be decrypted. You can use HCP attributes for storing very sensitive information like SSN. As the data is hashed, the only

Column Name	Column Name (For Querying)	Column Type	Description
			option to validate it is by using the validateUserData API.
JOBCODE	jobCode	varchar(255)	Specifies the job code assigned to the employee.
JOBDESCRIPTION	jobDescription	varchar(255)	Specifies the job description of the employee.
JOB_ID	jobID	bigint(20)	Specifies the Job ID of the employee.
JOB_FUNCTION	job_function	varchar(255)	Specifies the job function of the user. This information is obtained when the user is imported to Saviynt Identity Cloud from the third-

Column Name	Column Name (For Querying)	Column Type	Description
			party application.
JOBCODEDESC	jobcodedesc	varchar(255)	Specifies the description of the job code of the employee.
LASTNAME	lastname	varchar(255)	Specifies the last name of the user (employee).
LASTSYNCDATE	lastsyncdate	datetime	Specifies the date when user was most recently synchronized to Saviynt Identity Cloud from the third-party application.
LEAVESTATUS	leaveStatus	varchar(255)	Specifies whether the user is on leave.

Column Name	Column Name (For Querying)	Column Type	Description
LOCATION	location	varchar(255)	Specifies the location details of the user.
LOCATIONDESC	locationdesc	varchar(255)	Specifies the detailed description of the user’s location.
LOCATIONNUMBER	locationnumber	varchar(255)	Stores the location number associated with the location (if any) in the third-party application.
MANAGER	manager	bigint(20)	Stores the user key of the manager.
MIDDLENAME	middlename	varchar(255)	Specifies the middle name of the user.

Column Name	Column Name (For Querying)	Column Type	Description
ORGUNITID	orgunitid	varchar(255)	Stores the Organization Unit Id of the user.
OWNER	owner	varchar(255)	Specifies the owner of the user to whom all the approval workflows should be assigned.
PASSWORDEXPIRED	passwordExpired	bit(1)	Specifies whether to ask a question to the user when the password expires. • '0' indicates that questions will not be asked. • '1' indicates that questions will be asked.
PHONENUMBER	phonenumber	varchar(255)	Stores the primary contact

Column Name	Column Name (For Querying)	Column Type	Description
			number of the respective user.
PREFEREDFIRSTNAME	preferedFirstName	varchar(255)	Specifies the preferred first name of the user.
REGION	region	varchar(255)	Specifies the region to which the user belongs.
REGIONCODE	regioncode	varchar(255)	Stores the region code to which the user belongs.
SAVUPDATEDATE	savUpdateDate	datetime	Specifies the date when the user was last updated in Saviynt Identity Cloud.
SECONDARYMANAGER (FK)	secondaryManager (FK)	bigint(20)	Specifies the details of the

Column Name	Column Name (For Querying)	Column Type	Description
			user's secondary manager. The secondary manager is useful in two-level workflows that require approval from the user's primary and secondary manager.
SECONDARYPHONE	secondaryPhone	varchar(255)	Specifies the secondary contact number of the user.
SECONDARYEMAIL	secondaryEmail	varchar(255)	Specifies the secondary email of the user.
SECURITYANSWERS	encryptedSecurityAnswers	varchar(255)	Stores the question and answers defined by the user for using the forgot password functionality.

Column Name	Column Name (For Querying)	Column Type	Description
SITEID	siteid	varchar(255)	Stores the Site ID of the user.
STARTDATE	startdate	datetime	Specifies the start date, which is ideally the date when the user is created in the system. The start date might relate to an employee’s first date in an organization.
STATE	state	varchar(255)	Specifies the state to which the user belongs.
STREET	street	varchar(255)	Specifies the street address of the user.
TERMDATE	termDate	datetime	Specifies the date when the user will be terminated from

Column Name	Column Name (For Querying)	Column Type	Description
			employment in Saviynt Identity Cloud.
TITLE	title	varchar(255)	Specifies the title of the user.
UPDATEDATE	updatedate	datetime	Specifies the date when the user was last updated in the target system. This is updated with the import process.
USERSOURCE	userSource	varchar(255)	Stores the Connection ID used in the connection through which the user is imported to Saviynt Identity Cloud. Usersource represents the numerical value of the sources from which user data is

Column Name	Column Name (For Querying)	Column Type	Description
			imported to Saviynt Identity Cloud. It is the main source from which Saviynt Identity Cloud obtains the user information.
FAILEDTRIES	failedTries	bigint(20)	Stores the count for the number of failed login attempts.
HANARULEKEY	hanaRuleKey	longtext	Stores the key to trigger the hanarule based on the condition and action configured in the User Update rule.
OWNERONTERMINATE	owneronTerminate	bigint(20)	Stores the user to whom the

Column Name	Column Name (For Querying)	Column Type	Description
			ownership is transferred if the original user is disabled or terminated. Based on the feature ownership of the terminated user, the respective feature ownerships are transferred to the new owner. For example, the Attestation tasks for the previous owner are assigned to the user whose name is given in OwnerOnTerminate.
RULEACTION	ruleAction	varchar(255)	Specifies the result of the action of technical rules on users.

Column Name	Column Name (For Querying)	Column Type	Description
USERSOURCEKEY	userSourceKey	bigint(20)	Specifies the key of the Usersource. Usersource represents the numerical value of the sources from which user data is imported to Saviynt Identity Cloud. Usersource is the main source from which Saviynt Identity Cloud gets information about the user.
ENABLED	enabled	bit(1)	Specifies whether the user is enabled and active or inactive. • '0' indicates the user is inactive and cannot log in

Column Name	Column Name (For Querying)	Column Type	Description
			- '1' indicates the user is enabled and active
CUSTOMER (FK)	customer (FK)	bigint(20)	Stores the customer.
SYSTEMUSERNAME	systemUserName	varchar(255)	Specifies the system username. This is unique and used only for a specific client.
TASKCREATEDFORTERMINATE	taskCreatedforTerminate	bigint(20)	Specifies if the task is created for terminating the user.
UPDATEUSER (FK)	updateuser (FK)	bigint(20)	Specifies the details about the SAV user who has updated the user details. For example, if the admin has updated the user, the admin name appears

Column Name	Column Name (For Querying)	Column Type	Description
			in this column.
VENDORMANAGER (FK)	vendorManager (FK)	bigint(20)	Specifies the vendor manager.
RISKSCORE	riskscore	bigint(20)	Specifies the user's risk score. This field is managed by Saviynt Identity Cloud. Not to be used.
LASTPASSWORDUPDATEDATE	lastPasswordUpdateDate	datetime	Specifies the Date and time when the user’s password was last changed.
LOCALAUTHENABLED	localAuthEnabled	bit(1)	Specifies if the user is allowed to bypass SSO or external LDAP authentication and use Saviynt authentication.

Column Name	Column Name (For Querying)	Column Type	Description
			Values '1' – the user can perform a local authentication even when SSO or external LDAP authentication is enabled. '0' – the user cannot perform a local authentication when SSO or external LDAP authentication is enabled.
PIIERASURESTATUS	piiErasureStatus	bignit(20)	• Stores the timestamp, status and the details of the user for whom the erasure is performed within Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
			• 0 indicates that the user has requested to delete their PII from Saviynt. This value is expected to be set from the authoritative source. • 1 indicates that the erasure is on hold. • 2 indicates that the PII for the user is erased. • 3 indicates that the user is ready for PII Erasure. This value is either set from the authoritative source or from the Update User API manually to mark a user as being ready for erasure. • 4 indicates error in erasure.

Customer Table (customer)

The customer table stores all the details pertaining to the organizations in Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
COMMENTS	comments	varchar(255)	Indicates the comments mentioned for the organization account.
CREATEDATE	createdate	datetime	Indicates the creation date for the organization.
CREATEUSER	createuser	bigint(20)	Indicates the user who created the organization account.
CUSTOMERKEY (PK)	id (PK)	bigint(20)	Indicates the customer key which uniquely identifies an organization.

Column Name	Column Name (For Querying)	Column Type	Description
CUSTOMERNAME	customername	varchar(255)	Indicates the name of the organization.
CUSTOMERTYPE	customertype	bigint(20)	Indicates the type of organization.
CUSTOMPROPERTY1…20	customproperty1...20	varchar(255)	Based on the application type and values configured in third-party applications for various custom-properties, you can define the custom property values in Saviynt Identity Cloud. For the customer table, you can define up to 20 custom properties.

Column Name	Column Name (For Querying)	Column Type	Description
DESCRIPTION	description	varchar(255)	Indicates the description specified for the organization.
LOCATION	LOCATION	varchar(255)	Indicates the geographic location details of the organization.
LOGO	logo	mediumblob	Indicates the link to organization logo.
LOGONAME	logoname	varchar(255)	Indicates the link to the organization logo name.
PARENTCUSTOMER	parentCustomer	bigint(20)	Indicates the parent organization.

Column Name	Column Name (For Querying)	Column Type	Description
PHONENUMBER	phonenumber	varchar(255)	Indicates the phone number of the organization.
PRIMARYVENDORCONTACT	primaryvendorcontact	bigint(20)	Indicates the primary vendor contact for the organization.
RISK	risk	bigint(20)	Indicates the risk associated with this organization.
SCORE	score	bigint(20)	Indicates the organization's risk score. This field is managed by Saviynt Identity Cloud.
STATUS	status	bigint(20)	Indicates the current status of the organization.

Column Name	Column Name (For Querying)	Column Type	Description
			The following values are available: • '0' - Inactive • '1' - Active
UPDATEDATE	updatedate	datetime	Indicates the date on which the organization details were last updated.
UPDATEUSER	updateuser	bigint(20)	Indicates the name of the user who modified the organization details.
VENDORMANAGER	vendormanager	bigint(20)	Indicates the vendor manager.

Customer Entitlement Values Table (customer_entitlementvalues)

This table stores all the details pertaining to the entitlement values related to the organizations in Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
CUSTOMERKEY (PK)	customer (PK)	bigint(20)	Indicates the customer key which uniquely identifies an organization.
ENTITLEMENT_VALUES (PK)	entitlement_values (PK)	bigint(20)	Indicates the entitlement values associated with the organization.
UPDATEDATE	updatedate	datetime	Indicates the date on which the entitlement details were last updated.
UPDATEUSER	updateuser	bigint(20)	Indicates the name of the user who modified the entitlement

Column Name	Column Name (For Querying)	Column Type	Description
			details.

Organization Owners Table (organization_owners)

This table stores all the details pertaining to the organization owners in Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
USERKEY (PK)	userkey (PK)	bigint(20)	Indicates the key representing the user.
CUSTOMERKEY (PK)	customerkey (PK)	bigint(20)	Indicates the key which uniquely identifies an organization.
RANK (PK)	rank (PK)	int(11)	Indicates the rank of the organization owner.

Column Name	Column Name (For Querying)	Column Type	Description
UPDATEDATE	updatedate	datetime	Indicates the date on which the organization owner details were last updated.
UPDATEUSER	updateuser	varchar(255)	Indicates the name of the user who modified the organization owner details.

SAV Roles Table (savrole_permission)

This table stores all details for the analytics and connector permissions on the SAV roles in Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
ACCESSKEY	accesskey	bigint(20)	Specifies unique identifier for corresponding access (ANALYTICSES or ExternalConnection).

Column Name	Column Name (For Querying)	Column Type	Description
SAVROLEKEY	savrolekey	bigint(20)	Indicates the SAV role key.
ACCESSTYPE	accesstype	varchar(255)	Indicates the type of access: • Analytics (ANALYTICSES) • Connection (ExternalConnection)
UPDATEDATE	updatedate	datetime	Indicates the date on which the SAV role details were last updated.
UPDATEUSER	updateuser	bigint(20)	Indicates the name of the user who modified the SAV role details.

SAV Roles Table (savroles)

This table stores all the details pertaining to the SAV roles in Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
CUSTOMPROPERTY1…20	customproperty1…20	longtext	Based on the application type and values configured in third-party applications for various custom-properties, you can define the custom property values in Saviynt Identity Cloud. For the savroles table, you can define up to 20 custom properties.
HOMEPAGE	homepage	bigint(20)	The Saviynt Identity Cloud Home page displayed for a user with an assigned SAV

Column Name	Column Name (For Querying)	Column Type	Description
			role.
READONLY	readOnly	bit(1)	Indicates whether the user who is assigned with an SAV role can perform read-only operations only or not. The following values are available: • **On** - When the read-only feature is ON, the assigned user of an SAV role can perform the read-only operation on all tabs for which access is granted. • **Off** - When the read-only feature is OFF, the

Column Name	Column Name (For Querying)	Column Type	Description
			assigned users of an SAV role can perform read and write operations on all tabs for which access is granted.
ROLEDESCRIPTION	roledescription	varchar(255)	The description of the SAV role.
ROLEKEY (PK)	id (PK)	bigint(20)	Indicates the SAV role key.
ROLENAME	authority	varchar(255)	Indicates the SAV role name.
STATUSKEY	statuskey	bigint(20)	Indicates whether the SAV role is active or inactive. The following values are

Column Name	Column Name (For Querying)	Column Type	Description
			available: • '0' - indicates if the SAV role is Inactive • '1' - indicates if the SAV role is Active
UPDATEDATE	updatedate	datetime	Indicates the date on which the SAV role details were last updated.
UPDATEUSER	updateuser	bigint(20)	Indicates the name of the user who modified the SAV role details.

User SAV Roles Table (user_savroles)

This table stores all the details pertaining to the users assigned to the SAV roles in Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
USERKEY (PK)	userkey (PK)	bigint(20)	Indicates the key representing the user.
ROLEKEY (PK)	rolekey (PK)	bigint(20)	Indicates the SAV role key.
UPDATEDATE	updatedate	datetime	Indicates the date on which the user's SAV role details were last updated.
UPDATEUSER	updateuser	varchar(255)	Indicates the name of the user who modified a user's SAV role details.

The following diagram shows the relationships between users, customer, customer_entitlementvalues, organization_owners, savroles, and user_savroles tables.

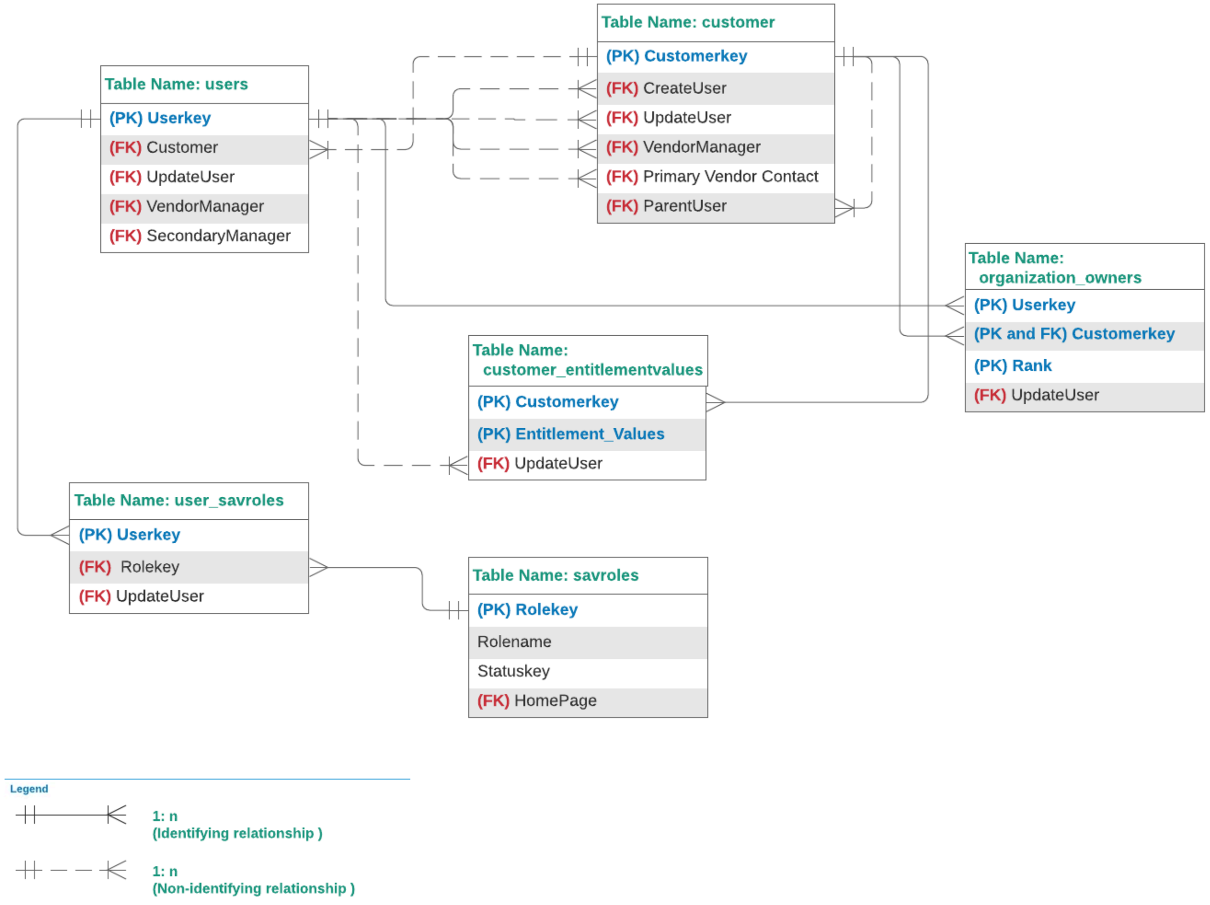


Table Name: users
(PK) Userkey
(FK) Customer
(FK) UpdateUser
(FK) VendorManager
(FK) SecondaryManager
Table Name: customer
(PK) Customerkey
(FK) CreateUser
(FK) UpdateUser
(FK) VendorManager
(FK) Primary Vendor Contact
(FK) ParentUser
Table Name: organization_owners
(PK) Userkey
(PK and FK) Customerkey
(PK) Rank
(FK) UpdateUser
Table Name: customer_entitlementvalues
(PK) Customerkey
(PK) Entitlement_Values
(FK) UpdateUser
Table Name: user_savroles
(PK) Userkey
(FK) Rolekey
(FK) UpdateUser
Table Name: savroles
(PK) Rolekey
Rolename
Statuskey
(FK) HomePage
Legend
1: n
(Identifying relationship)
1: n
(Non-identifying relationship)

Accounts Table (accounts)

The accounts table stores all the details pertaining to user accounts in Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
ACCOUNTKEY (PK)	id (PK)	bigint(20)	This is the primary key to the accounts table. It helps you to identify a specific account from the table. Using this key, you can map the accountkey with the other tables. For example, to fetch account details for a single user, you can use the accountkey in accounts table with accountkey in user_account table. Then you can use the join query using accountkey in

Column Name	Column Name (For Querying)	Column Type	Description
			user_account with accountkey (PK) in accounts table to fetch multiple accounts for a user.
ACCOUNTID	accountID	varchar(255)	Indicates the account ID of the user.
ACCOUNTCLASS	accountclass	varchar(255)	Indicates the account class of the user.
ACCOUNTTYPE	accounttype	varchar(255)	Indicates the account type of the user. Account type can be the standard or external user.
APPLICENSETYPE (FK)	applicensetype (FK)	bigint(20)	Indicates the application license type for the account.

Column Name	Column Name (For Querying)	Column Type	Description
			The application license type indicates the actual licenses setup in Saviynt Identity Cloud.
ARSTASKKEY (FK)	arsTask (FK)	bigint(20)	After the ARS request is approved, a task-key is generated for the respective account. The task key is stored in arstaskkey column.
COMMENTS	comments	varchar(255)	Indicates the comments mentioned for the account.
CREATED_ON	createdon	datetime	Indicates the date on which the account was created.

Column Name	Column Name (For Querying)	Column Type	Description
CREATOR	creator	varchar(255)	Indicates the username of the user who created the account.
CUSTOMPROPERTY1-10	customproperty1-10	varchar(255)	Based on the application type and values configured in third-party applications for various custom-properties, you can define the custom property values in Saviynt Identity Cloud.
CUSTOMPROPERTY11-56	customproperty11-56	varchar(255)	Based on the application type and values configured in third-party applications for various custom-properties, you can define the custom property values in Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
CUSTOMPROPERTY57-60	customproperty57-60	mediumtext	Based on the application type and values configured in third-party applications for various custom-properties, you can define the custom property values in Saviynt Identity Cloud.
DESCRIPTION	description	longtext	Indicates the description specified for the account.
DISPLAYNAME	displayName	varchar(255)	Indicates the name of the user for the respective account.
ENDPOINTKEY	endpointkey	bigint(20)	Indicates the endpoint key mapping to the endpoint where the account has been

Column Name	Column Name (For Querying)	Column Type	Description
			created.
INCORRECTLOGONS	incorrectlogons	bigint(20)	Indicates the count for the number of incorrect logins in Saviynt Identity Cloud.
JOBID	jobid	bigint(20)	Indicates the Job ID associated with the respective account.
LASTLOGONDATE	lastlogondate	datetime	Indicates the last login date of the user to access the account.
LASTPASSWORDCHANGE	lastpasswordchange	datetime	Indicates the date when the password was last changed for the respective user.

Column Name	Column Name (For Querying)	Column Type	Description
			For all change password tasks provisioned using automated provisioning, this field is updated with the timestamp of the successful completion of the task. The Change Password action may be for Self or Others or Service Accounts. It is applicable for the actions: Forgot or Reset or Change password and there must be a valid endpoint synced to Saviynt Identity Cloud. This date is also updated when accounts are imported from target applications

Column Name	Column Name (For Querying)	Column Type	Description
NAME	name	varchar(255)	Indicates the account name.
ORPHAN	orphan	bit(1)	Indicates whether the account is an Orphan account or not. An Orphan account is an account without any username associated with it.
PASSWORDCHANGESTATUS	passwordchangestatus	varchar(255)	Indicates the status of password change action. Provides details for whether the password has been successfully changed or not.
PASSWORDLOCKDATE	passwordlockdate	datetime	Indicates the date when the password was locked on account of entering incorrect

Column Name	Column Name (For Querying)	Column Type	Description
			password details.
PRIVILEGED	privileged	varchar(255)	Indicates if the account is privileged or not.
REFERENCED_ACCOUNTNAME	referenced_accountName	varchar(255)	This column is used in case of a parent-child endpoint relationship. Primary used to synchronize the accounts between parent and child endpoints.
SAVLICENSETYPE	savlicensetype	bigint(20)	The SAV License type helps you to intelligently identify the number of licenses from the App License Type that can be optimally be used and

Column Name	Column Name (For Querying)	Column Type	Description
			procured.
STATUS	status	varchar(255)	Indicates the status of the account using the following options: • '1' - Indicates that the account is active • '2' - Indicates that the account is inactive • '3' - Decommission active • '4' - Decommission inactive • Manually Suspended - Indicates that the account is suspended manually • Manually Provisioned - Indicates that the account

Column Name	Column Name (For Querying)	Column Type	Description
			is provisioned manually.
SYSTEMID	systemid	bigint(20)	This column is used to store the ID of the security system to which the account belongs.
TOTALUSAGE	totalusage	varchar(255)	Indicates the total usage done for the respective account.
UPDATEUSER	updateUser	varchar(255)	Indicates the last updated user to which the account is synchronized.
UPDATEDATE	updatedate	datetime	Indicates the date on which the account was updated.

Column Name	Column Name (For Querying)	Column Type	Description
USERGROUP	usergroup	varchar(255)	Indicates usergroup to which the user and respective accounts are assigned.
USERLOCK	userlock	bigint(20)	Indicates whether the user’s account is locked or not. An account is locked when an incorrect password is entered for more than the configured number of failed login attempts. Following are the available values: • '1' - account locked • '0' - account unlocked

Column Name	Column Name (For Querying)	Column Type	Description
VALIDFROM	validfrom	datetime	Indicates the start date from when the account is valid.
VALIDTHROUGH	validthrough	datetime	Indicates the end date to which the account is valid.
SAVIYNT_CONNECT_JOBID	saviyntConnectJobId	bigint(20)	This column is used to store the Job Id for importing of accounts from third-party applications to Saviynt Identity Cloud.
SAVIYNT_CONNECT_UPDATEDATE	saviyntConnectUpdateDate	datetime	This column is used to store the date on which the jobs are run to import the accounts from third-party applications to Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
REFERENCED_ACCOUNTKEY	referenced_accountkey	bigint(20)	Indicates the referenced account key
ACCOUNTCONFIG	accountConfig	longtext	This column contains the account configuration

User Accounts Table (user_accounts)

The user_accounts table stores the data that is used to identify the user(s) who have access to different accounts, and the number of accounts that are accessible by a specific user.

Column Name	Column Name (For Querying)	Column Type	Description
USERKEY (PK)	userkey (PK)	bigint(20)	This is the primary key of the user_accounts table. It helps you to identify a specific user from the table. Using this key, you can map the user with the

Column Name	Column Name (For Querying)	Column Type	Description
			other tables. For example, to fetch account details for a single user, you can use the userkey in users table with userkey in user_account table. Then you can use the join query using accountkey in user_account with accountkey (PK) in accounts table to fetch multiple accounts for a user.
ACCOUNTKEY (PK)	accountkey (PK)	bigint(20)	This is the primary key of the accounts table. It helps you to identify a specific account from the table. Using this key, you can map the accountkey with the other tables.

Column Name	Column Name (For Querying)	Column Type	Description
			For example, to fetch account details for a single user, you can use the accountkey in accounts table with accountkey in user_account table. Then you can use the join query using accountkey in user_account with accountkey (PK) in accounts table to fetch multiple accounts for a user.
UPDATEDATE	updatedate	datetime	When the account gets assigned to the user, the update date is stored in this column.
UPDATEUSER	updateuser	varchar(255)	Indicates the details of the SAV user who has updated

Column Name	Column Name (For Querying)	Column Type	Description
			the user details. For example, if the administrator has updated the user then the administrator name appears in the updateuser column.
LASTCERTIFIEDCAMPAIGNDATE	lastCertifiedCampaignDate	datetime	Indicates the date of the last certified campaign.
LASTCERTIFIEDCAMPAIGNNAME	lastCertifiedCampaignName	varchar(255)	Indicates the name of the last certified campaign.
LASTCERTIFIEDUSER	lastCertifiedUser	bigint(20)	Indicates the user of the last certified campaign.

Account Entitlements Table (account_entitlements1)

This table provides mapping details of access to different accounts and associated entitlements. The ACCOUNTKEY and ENTITLEMENT_VALUEKEY columns help to map accounts and entitlements.

Column Name	Column Name (For Querying)	Column Type	Description
ACCENTKEY (PK)	id (PK)	bigint(20)	This is the unique primary key that helps you to identify specific account and entitlement association.
SAVACCESS	access	varchar(255)	Indicates the SAV role access details.
ACCOUNTKEY (FK)	accountkey (FK)	bigint(20)	Indicates the account associated with the entitlement.
ARSTASKKEY (FK)	arsTask (FK)	bigint(20)	Indicates the ARS task key

Column Name	Column Name (For Querying)	Column Type	Description
			which assigns the entitlement (entitlement value key) to the account.
ASSIGNEDFROMCOMPROLE (FK)	assignedFromCompRole (FK)	bit(1)	Indicates whether entitlement is assigned from a composite role or not. The following are the available values: • '0' - Not Assigned • '1' - Assigned
ASSIGNEDFROMROLE (FK)	assignedFromRole (FK)	bigint(20)	Indicates whether entitlement is assigned from role or not. The following are the available

Column Name	Column Name (For Querying)	Column Type	Description
			values: • '0' - Not Assigned • '1' - Assigned
ASSIGNEDFROMRULE (FK)	assignedFromRule (FK)	varchar(255)	Indicates whether entitlement is assigned from the rule or not. The following are the available values: • '0' - Not Assigned • '1' - Assigned
ASSIGNEDFROMCHILD (FK)	assignedfromchild (FK)	bit(1)	Indicates whether entitlement is assigned from child role or not.

Column Name	Column Name (For Querying)	Column Type	Description
			The following are the available values: • '0' - Not Assigned • '1' - Assigned
ENDDATE	enddate	datetime	Indicates the end date of the entitlement available for the account.
ENTITLEMENT_VALUEKEY (FK)	entitlement_valuekey (FK)	bigint(20)	Indicates the entitlement name of the entitlement available for the account.
JOB_ID	jobId	bigint(20)	Indicates the job identification number.

Column Name	Column Name (For Querying)	Column Type	Description
JRMRULES	jrmRules	varchar(255)	Indicates the previously used JRM rule.
LASTUSEDENDDATE	lastusedenddate	datetime	Indicates the last used end date of the entitlement available for the account.
STARTDATE	startdate	datetime	Indicates the start date of the entitlement available for the account.
UPDATEDATE	updatedate	datetime	Indicates the last modified date of the entitlement available for the account.
UPDATEUSER	updateuser	bigint(20)	Indicates the name of the user who modified the entitlement

Column Name	Column Name (For Querying)	Column Type	Description
			available for the account..
LASTCERTIFIEDCAMPAIGNNAME	lastCertifiedCampaignName	varchar(255)	Indicates the last certified campaign name.
SAVIYNT_CONNECT_JOBID	saviyntConnectJobId	bigint(20)	Indicates the SAVIYNT_CONNECT job identification number.
SAVIYNT_CONNECT_UPDATE_DATE	saviyntConnectUpdateDate	datetime	Indicates the SAVIYNT_CONNECT updated date of the entitlement available for the account.
ASSIGNEDFROMROLES	assignedFromRoles	varchar(255)	Stores the rolekey of the roles associated with the corresponding entitlement. If

Column Name	Column Name (For Querying)	Column Type	Description
	ⓘ Info The data type of the `ASSIGNEDFROMROLES` column in the account_entitlements1 table is now displayed as text, as the size has been increased from varchar (1024) to varchar (3000).		more than one role is associated with an entitlement, multiple rolekey are stored separated by commas.
LASTCERTIFIEDCAMPAIGNDATE	lastCertifiedCampaignDate	datetime	Indicates the date for the last certified campaign of the entitlement available for the account.
LASTCERTIFIEDUSER	lastCertifiedUser	bigint(20)	Indicates the user for the last certified campaign of

Column Name	Column Name (For Querying)	Column Type	Description
			the entitlement available for the account.
UUID	uuid	varchar(255)	Indicates unique UID of the entitlement available for the account..

Entitlement Values Table (entitlement_values)

This table provides information about the entitlements associated with different entitlement types.

Column Name	Column Name (For Querying)	Column Type	Description
ENTITLEMENT_VALUEKEY (PK)	id (PK)	bigint(20)	This is the unique primary key in the row which helps to identify specific entitlement and entitlement type association.

Column Name	Column Name (For Querying)	Column Type	Description
SAVACCESS	access	varchar(255)	Indicates the SAV role access details.
CONFIDENTIALITY	confidentiality	bigint(20)	This column determines the level of confidentiality that the entitlement carries. The available values for this column are: Very Low, Low, Medium, High, or Critical.
CUSTOMPROPERTY1 to 5	CUSTOMPROPERTY1 to 5	longtext	Based on the application type and values configured in third-party applications for various custom properties, you can define the custom property
CUSTOMPROPERTY6 to 40	CUSTOMPROPERTY6 to 40	varchar(255)	

Column Name	Column Name (For Querying)	Column Type	Description
			values in Saviynt Identity Cloud. For the **entitlement_values** table, you can define up to 40 custom properties.
DESCRIPTION	description	longtext	Indicates the description of the entitlement.
DISPLAYNAME	displayname	• varchar(255) • varchar(1024)	Indicates the display name of the entitlement.

Column Name	Column Name (For Querying)	Column Type	Description
		ⓘ Info Saviynt Identity Cloud supports storing up to 1024 characters of the displayname attribute imported from target applications.	
ENT_OBJHASH	ent_objHash	bigint(20)	Indicates the entitlement object hash value.
ENTCLASS	entclass	varchar(255)	Indicates the entitlement class type.
ENTITLEMENTID	entitlementID	varchar(255)	Indicates entitlement identification.

Column Name	Column Name (For Querying)	Column Type	Description
ENTITLEMENTID_LONG	entitlementID_long	longtext	Indicates entitlement identification if the length of entitlementID is greater than 255 characters.
ENTITLEMENT_GLOSSARY	entitlement_glossary	longtext	Indicates the glossary of the entitlement.
ENTITLEMENT_VALUE	entitlement_value	varchar(255)	Indicates the name of entitlement.
ENTITLEMENTTYPEKEY (FK)	entitlementtypekey(FK)	bigint(20)	Helps to identify the specific entitlement type associated with an endpoint.
JOB_ID	jobID	bigint(20)	Indicates the job identification number.

Column Name	Column Name (For Querying)	Column Type	Description
LASTSCANDATE	lastScanDate	datetime	Indicates the last scan date.
SAVLEVEL	level	bigint(20)	Indicates the SAV role levels.
MODULE	module	varchar(255)	Indicates the module name.
ORPHAN	orphan	bit(1)	Indicates whether this entitlement is orphan or not.
PRIVILEGED	priviliged	bigint(20)	Indicates entitlement privileges.
PROGRAM	program	varchar(255)	Indicates the program to which the entitlement is associated to.

Column Name	Column Name (For Querying)	Column Type	Description
RISK	risk	bigint(20)	Indicates any risk associated with this entitlement.
ROLETYPE	roletype	bigint(20)	Indicates the role type.
SCHEMANAME	schemaname	varchar(255)	Indicates the schema name.
SODDETAILDATA	soddetaildata	longblob	Indicates the Separationof Duties (SOD) detailed data.
SOD	sodflag	bit(1)	Indicates the Separationof Duties (SOD) for the role.
SOX_CRITICAL	soxcritical	bigint(20)	Indicates the SOX criticality. SOX criticality defines the

Column Name	Column Name (For Querying)	Column Type	Description
			level of roles or policies critically compliant with Sarbanes-Oxley IT regulations. The available values for this column are: Very Low, Low, Medium, High, or Critical.
STATUS	status	bigint(20)	Indicates the current status of entitlement. The following are the available values: • '1' - Active • '2' - Inactive

Column Name	Column Name (For Querying)	Column Type	Description
SYS_CRITICAL	syscritical	bigint(20)	Indicates the system criticality.
UPDATEDATE	updatedate	datetime	Indicates the last modified date of the entitlement.
UPDATEUSER	updateuser	bigint(20)	Indicates the name of the user who modified the entitlement details.
SAVIYNT_CONNECT_JOBID	saviyntConnectJobId	bigint(20)	Indicates the SAVIYNT_CONNECT job identification number.
SAVIYNT_CONNECT_UPDATE_DATE	saviyntConnectUpdateDate	datetime	Indicates the SAVIYNT_CONNECT updated date.

Column Name	Column Name (For Querying)	Column Type	Description
ACCTENTMAPPINGINFOCOLUMNFROMENT	acctEntMappingInfoColumnFromEnt	• varchar(255) • longtext ⓘ Info You can store a large volume of entitlements to accounts mapping and entitlement owner mapping data imported from target applications through the REST connector. For more information, see Fields and Descriptions of Key Tables.	Indicates the account entitlement mapping information column from entitlement.
ENTITLEMENTMAPPINGJSO	entitlementMappingJson	longtext	Indicates the entitlement

Column Name	Column Name (For Querying)	Column Type	Description
N			mapping JSON details.
REFERENCED_ENTITLEMENT	referenced_entitlement	bigint(20)	Indicates the relationship between two entitlements in case of parent-child endpoint scenario.
PRIORITY	priority	bigint(20)	Indicates the priority of the entitlement.

Entitlement Types Table (entitlement_types)

This table provides information about the entitlement types associated with the different endpoints in Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
ENTITLEMENTTYPEKEY	id (PK)	bigint(20)	This is the unique primary key

Column Name	Column Name (For Querying)	Column Type	Description
(PK)			in the row that helps to identify specific entitlement types and endpoint associations.
ARS_REQ_ENT_SQLQUEREY	ars_req_ent_sqlquerey	varchar(255)	Indicates the required entitlement SQL query filter from ARS.
ARS_SELECT_ENT_SQLQUEREY	ars_select_ent_sqlquerey	varchar(255)	Indicates the selected ARS entitlement SQL query filter from ARS.
CERTIFIABLE	certifiable	bit(1)	Indicates if the entitlement type is certifiable. When you select the Certifiable option, the system displays all accounts related to

Column Name	Column Name (For Querying)	Column Type	Description
			the endpoint in Attestation and Campaign modules.
CREATETASKACTION	createTaskAction	longtext	The Create Task Action creates a remove task when an entitlement is removed from ARS.
CUSTOMPROPERTY1 to 40	customproperty1 to 40	varchar(255)	Based on the application type and values configured in third-party applications for various custom-properties, you can define the custom property values in Saviynt Identity Cloud. For the entitlement_types table, you can define up to 40

Column Name	Column Name (For Querying)	Column Type	Description
			custom properties.
ENDPOINTKEY (FK)	endpointkey (FK)	bigint(20)	Indicates the endpoint.
ENTITLEMENTDESCRIPTIO N	entitlementdescription	varchar(255)	Indicates the entitlement description.
ENTITLEMENTNAME	entitlementname	varchar(255)	Indicates the entitlement name.
HIEARCHYREQUIRED	hiearchyrequired	int(11)	Indicates if the hierarchy is required. Hierarchy is mainly used for mapped entitlements (parent and child entitlements) and when you want to display the

Column Name	Column Name (For Querying)	Column Type	Description
			child entitlements in the ARS Request Form.
MODULE	module	varchar(255)	Indicates the module name.
RECON	recon	bit(1)	Indicates the reconciliation of data from the target application.
REQUESTFORM	requestform	int(11)	Indicates the ARS Request Form identifier.
REQUIREDINREQUEST	requiredinrequest	bit(1)	Indicates whether the entitlement type is mandatory or not. The following are the available

Column Name	Column Name (For Querying)	Column Type	Description
			values: • '0' - Not Mandatory • '1' - Mandatory
SHOWONCHILD	showonchild	bit(1)	Indicates the name of the entitlement displayed on the child hierarchy level.
SYSTEMKEY (FK)	systemkey (FK)	bigint(20)	Indicates the security system key.
AVAILABLEQUERYSERVICEACCOUNT	availableQueryServiceAccount	varchar(255)	Indicates available query for the service account.
DISPLAYNAME	displayName	varchar(255)	Indicates display name for the

Column Name	Column Name (For Querying)	Column Type	Description
			entitlement type.
ENABLEPROVISIONINGPRIORITY	enableProvisioningPriority	bit(1)	Indicates if provisioning priority is enabled.
ORDERINDEX	orderindex	bigint(20)	Indicates the order index for the entitlement type.
SELECTQUERYSERVICEACCOUNT	selectedQueryServiceAccount	varchar(255)	Indicates the select query for the service account.
WORKFLOW	workflow	varchar(255)	Indicates workflow to be used for the governance of the entitlement type.
UPDATEDATE	updatedate	datetime	Indicates the last modified

Column Name	Column Name (For Querying)	Column Type	Description
			date of the entitlement.

Endpoints Table (endpoints)

This table provides information about the configurations related to endpoints. Endpoints are instances of a target system managed by Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
ENDPOINTKEY (PK)*	id (PK)*	bigint(20)	This is the unique primary key in the row that represents the endpoint.
ACCESSQUERY	accessquery	varchar(255)	Indicates the attributes used to raise access queries to endpoints.

Column Name	Column Name (For Querying)	Column Type	Description
DISABLEACCOUNTREQUEST	disableaccountrequest	varchar(255)	This column provides an option to disable new account requests if the account already exists. Following are the available values: • '1' - enabled • '0' - disabled
	ACCOUNTNAME	bit(1)	Stores the name of the account associated with the endpoint.
ACCOUNTTYPEFORSERVICEACCOUNT	accountTypeForServiceAccount	varchar(255)	Indicates the account type required for service.

Column Name	Column Name (For Querying)	Column Type	Description
ACCOUNTTYPENODEPROVISION	accountTypeNoDeprovision	varchar(255)	Indicates the account type for which de-provisioning tasks should not be created.
ACCOUNTTYPENOPASSWORDCHANGE	accountTypeNoPasswordChange	varchar(255)	Indicates the account type for which the password must not be changed.
CREATEENTTASKFORREMOVEACC	createEntTaskforRemoveAcc	bit(1)	This column provides the enable or disable option to create a dependent entitlement task to remove the access for an endpoint.
DEFAULTLICENSE (FK)#	defaultLicense (FK)#	bigint(20)	Indicates the default license type used to access the endpoint.

Column Name	Column Name (For Querying)	Column Type	Description
DESCRIPTION	description	varchar(255)	Indicates a short description of the configured endpoint.
DISPLAYNAME	displayName	varchar(255)	Indicates a name that is displayed as a system name on the endpoints list table.
ENDPOINTNAME	endpointname	bigint(20)	Indicates the endpoint name that is displayed on the endpoints list table.
ENTSWITHNEWACCOUNT	entsWithNewAccount	longtext	Indicates the entitlement values associated with the new account on an endpoint.
SECURITYSYSTEMKEY (FK)	securitysystemkey (FK)	bigint(20)	Indicates the unique key representing the security

Column Name	Column Name (For Querying)	Column Type	Description
			system.
PARENTENDPOINTKEY (FK)	parentEndpointkey (FK)	bigint(20)	Indicates the unique key representing the parent endpoint to which the endpoint has been mapped.
ACCOUNTNAMERULE	accountNameRule	longtext	This column specifies the rule to create new accounts when the user submits a request for new account creation.
CONNECTION_CONFIG	connectionconfig	longtext	Indicates the configuration for the application.
OWNERKEY	ownerkey	bigint(20)	This column represents the unique key representing

Column Name	Column Name (For Querying)	Column Type	Description
			endpoint owner and is used to alert the security team if an endpoint owner is disabled.
OWNERTYPE	ownerType	bigint(20)	Indicates the type of owner. Following are the possible values: • User Group • User
PARENTACCOUNTPATTERN	parentAccountPattern	varchar(255)	Indicates the name pattern to be associated with parent endpoint.
REQUESTOWNER	requestowner	bigint(20)	Indicates the request owner.

Column Name	Column Name (For Querying)	Column Type	Description
REQUESTOWNERTYPE	requestownertype	bigint(20)	Indicates the type of owner. Following are the possible values: • User Group • User
STATUS	status	bigint(20)	Indicates the endpoint status. Following are the possible values: • '1' - endpoint enabled • '0' - endpoint disabled
USERACCOUNTCORRELATIONRULE	userAccountCorrelationRule	longtext	This column defines the rule to map any user attribute to an

Column Name	Column Name (For Querying)	Column Type	Description
			account attribute.
CUSTOMPROPERTY1 -30	customproperty1 -30	varchar(255)	Based on the application type and values configured in third-party applications for various custom-properties, you can define the custom property values in Saviynt Identity Cloud. For the endpoints table, you can define up to 45 custom properties.
CUSTOMPROPERTY31 -45	customproperty31 -45	tinytext	Based on the application type and values configured in third-party applications for various custom-properties, you can

Column Name	Column Name (For Querying)	Column Type	Description
			define the custom property values in Saviynt Identity Cloud. For the endpoints table, you can define up to 45 custom properties.
CUSTOMPROPERTY1 -29LABEL	customproperty1 -30LABEL	varchar(255)	Based on the application type and values configured in third-party applications for various custom-properties, you can define the label for the custom property values in Saviynt Identity Cloud. For the endpoints table, you can define up to label for 56 custom properties.

Column Name	Column Name (For Querying)	Column Type	Description
CUSTOMPROPERTY31 -56LABEL	customproperty31 -56LABEL	tinytext	Based on the application type and values configured in third-party applications for various custom-properties, you can define the label for the custom property values in Saviynt Identity Cloud. For the endpoints table, you can define up to label for 56 custom properties.
ACCOUNTNAMEVALIDATOR REGEX	accountNameValidatorRegex	longtext	Indicates regex used to validate the account name.
APPLICATIONLOGO	applicationLogo	varchar(255)	Indicates the link to the application logo.

Column Name	Column Name (For Querying)	Column Type	Description
APPLICATIONURL	applicationUrl	varchar(255)	Indicates the application URL.
CREATEDATE	createDate	datetime	Indicates the creation date for the endpoint.
CREATEDBY	createdBy	bigint(20)	Indicates the user who created the endpoint.
CREATEDFROM	createdFrom	varchar(255)	Indicates the source from where the endpoint was created.
DISABLEACCOUNTREQUEST	disableaccountrequest	varchar(255)	Indicates disable account request JSON.
DISABLEACCOUNTREQUES	disableaccountrequestService	varchar(255)	Indicates the JOSN for

Column Name	Column Name (For Querying)	Column Type	Description
TSERVICEACCOUNT	Account		disabling th new service account request if a service account already exists.
ENABLECOPYACCESS	enableCopyAccess	bit(1)	Indicates if copy access is enabled.
ENDPOINTCONFIG	endpointConfig	longtext	Indicates the endpoint configuration.
JRMDATAPOPULATED	jrmDataPopulated	bit(1)	Indicates if JRM data is populated.
LASTIMPORT	lastImport	longtext	Indicates the last import information.

Column Name	Column Name (For Querying)	Column Type	Description
PRIMARYACCOUNTTYPE	primaryAccountType	varchar(255)	Indicates the primary account type to be used for the endpoint.
ROLETYPEASJSON	roleTypeAsJson	longtext	Indicates the role type JSON.
SERVICEACCOUNTACCESSQUERY	serviceAccountAccessQuery	varchar(255)	Indicates the service account access query.
SERVICEACCOUNTNAMERULE	serviceAccountNameRule	longtext	Indicates the service account query.
UPDATEDATE	updateDate	datetime	Indicates the last date when the endpoint details have been updated in Saviynt Identity Cloud.

Column Name	Column Name (For Querying)	Column Type	Description
UPDATEDBY	updatedBy	bigint(20)	Indicates the user who updated the endpoint.

Tip

Sample Use Case: You want to view a single reconciliation report showing the status of reconciliation for all the endpoints.

Solution: Query the **ecmimportjob** table to list all the data import jobs with the status. This table stores the Saviynt Identity Cloud database schema and can provide the complete log data in the XML format.

Security Systems Table (securitysystems)

This table provides information about the configurations related to security systems.

Security systems are used to establish a secure connection between Saviynt Identity Cloud and the target system it manages.

Column Name	Column Name (For Querying)	Column Type	Description
SYSTEMKEY (PK)	id (PK)	bigint(20)	This is the unique primary key in the row used to identify a specific security system.
ACCESSADDWORKFLOW	accessAddWorkflow	varchar(255)	Indicates the workflow to add a user in the security system.
ACCESSREMOVEWORKFLOW	accessRemoveWorkflow	varchar(255)	Indicates the workflow to remove a user from the security system
DASHBOARDIMPORTCONFIG	dashboardImportConfig	longtext	Indicates the dashboard import configuration.
DISPLAYNAME	displayName	varchar(255)	Indicates the name that is displayed as a system name on the security system list

Column Name	Column Name (For Querying)	Column Type	Description
			table.
HOSTNAME	hostname	varchar(255)	Indicates the hostname of the security system.
INSTANTPROVISION	instantprovision		Indicates if instant provisioning is enabled.
LOGTABLE	logtable	varchar(255)	Indicates the log table name, if the user uploads system logs after creating the security system.
MANAGEENTITY	manageEntity	bit(1)	This column indicates the Saviynt Identity Cloud Data Space model when objects are not maintained in

Column Name	Column Name (For Querying)	Column Type	Description
			Saviynt Database but in another repository. In other words, manage entity indicates if the data is to be saved in Saviynt DB or in external DB. The following options are available: • 'Yes' - If selected as Yes, it will use Saviynt as the native DB. • 'No' - Select No, if you do not want to use the Saviynt as the native DB and you want to use some other external identity repository as the DB. In that case,

Column Name	Column Name (For Querying)	Column Type	Description
			Saviynt acts as a wrapper on top of any other DB and works as a real-time call.
ONECLICKIMPORTCONFIG	oneClickImportConfig	longtext	Indicates the configuration for one-click import.
OWNER	owner	bigint(20)	Indicates the security system owner, and is used to alert the security team if an end-point owner is disabled.
PERSISTENTDATA	persistentData	bit(1)	Indicates if data need to be persistent.
EXTERNALCONNECTION (FK)	externalConnection (FK)	bigint(20)	Indicates the external connection associated with the

Column Name	Column Name (For Querying)	Column Type	Description
			configured security system.
NODE_MAC_ID (FK) (Deprecated)	nodeMac (FK) (Deprecated)	bigint(20)	Indicates the MAC ID or hardware ID of the security system.
POLICYRULE (FK)	policyRule (FK)	bigint(20)	Indicates the rules associated with the configuration of the security system.
PORT	port	varchar(255)	Indicates the port used for establishing a connection.
PROPOSEDACCOUNTOWNERSWORKFLOW	proposedAccountOwnersworkflow	varchar(255)	Indicates the account owner workflow of a user to manage the security system.

Column Name	Column Name (For Querying)	Column Type	Description
PROVISIONINGCONNECTION (FK)	provisioningConnection (FK)	bigint(20)	Indicates the connector type used for provisioning.
SERVICEDESKCONNECTION (FK)	serviceDeskConnection (FK)	bigint(20)	Indicates the key to service desk connection.
STATUS	status	bigint(20)	Indicates the security system status. Following are the available values: • '1' - security system enabled • '0' - security system disabled

Column Name	Column Name (For Querying)	Column Type	Description
SYSTEMNAME	systemname	varchar(255)	Indicates the security system name.
AUTOMATEDPROVISIONING	automatedProvisioning	bit(1)	This column describes if automated provisioning of security system is enabled or not. Following are the available values: • '1' - automated provisioning enabled • '0' - automated provisioning disabled
CONNECTIONPARAMETERS	connectionparameters	longtext	Indicates the parameters used to establish a connection with

Column Name	Column Name (For Querying)	Column Type	Description
			the security system.
DEFAULTSYSTEM	defaultSystem	bit(1)	Indicates the default security system used.
RECONAPPLICATION	reconApplication	bit(1)	This column specifies the application reconciliation associated with the security system. Following are the available values: • '1' - Recon application enabled • '0' - Recon application disabled

Column Name	Column Name (For Querying)	Column Type	Description
USEOPENCONNECTOR	useopenconnector	bit(1)	This column specifies if an open connector can be used. Following are the available values: • '1' - use of open connector enabled • '0' - use of open connector disabled
ADDSERVICEACCOUNTWORKFLOW	addServiceAccountWorkflow	varchar(255)	Indicates the service account workflow.
CREATEDATE	createDate	datetime	Indicates the date the security system is created. This is created internally for Saviynt Identity Cloud usage.

Column Name	Column Name (For Querying)	Column Type	Description
CREATEDBY	createdBy	bigint(20)	Indicates the user who created the security system.
CREATEDFROM	createdFrom	varchar(255)	Indicates if the process security system is created from like manual/upload.
FFIDREQUESTACCESSWORKFLOW	firefighteridRequestAccessWorkflow	varchar(255)	Indicates the workflow for the Firefighter access request.
FIREFIGHTERIDWORKFLOW	firefighteridWorkflow	varchar(255)	Indicates the workflow for the Firefighter.
PROVISIONINGCOMMENTS	provisioningcomments	varchar(255)	Indicates the provisioning comments.

Column Name	Column Name (For Querying)	Column Type	Description
PROVISIONINGTRIES	provisioningTries	bigint(20)	Indicates the number of tries to be made for provisioning, in case of any error.
PROVLIMITJSON	provLimitJSON	longtext	This column contains the JSON for the provisioning limit.
REMOVESERVICEACCOUNTWORKFLOW	removeServiceAccountWorkflow	varchar(255)	Indicates the workflow for the remove service account.
UPDATEDATE	updateDate	datetime	Indicates the last modified date of the security system.
UPDATEDBY	updatedBy	bigint(20)	Indicates the user updating the security system.

External Connection Table (externalconnattvalue)

This table provides information about the configurations related to connector establishment.

External connection refers to the configuration setup of Saviynt Identity Cloud when it connects to target applications in the external public network.

Column Name	Column Name (For Querying)	Column Type	Description
EXTERNALCONNECTIONKEY (PK)	id (PK)	bigint(20)	This is the unique primary key representing an external connection.
CONNECTIONDESCRIPTION	connectiondescription	varchar(255)	Indicates a short description of the configured connection.
CONNECTIONNAME	connectionname	varchar(255)	Indicates the external connection name.
CREATEDBY	createdBy	varchar(255)	Indicates the user who created

Column Name	Column Name (For Querying)	Column Type	Description
			the external connection.
CREATEDON	createdOn	datetime	Indicates the date and time at which the connector was created.
EMAILTEMPLATE (FK)	emailTemplate (FK)	varchar(255)	Describes the e-mail template associated with the external connection created.
EXTERNALCONNECTIONTYPE (FK)	externalconnectiontype (FK)	bigint(20)	Indicates the type of external connection created.
NODE_MAC_ID (FK) (Deprecated)	nodeMac (FK) (Deprecated)	bigint(20)	Indicates the MAC ID or hardware ID of the external connection created.

Column Name	Column Name (For Querying)	Column Type	Description
STATUS	status	bigint(20)	Indicates the external connection status, defines whether connection status is enabled or not. Following are the available values: • '1' - external connection enabled • '0' - external connection disabled
STATUSFORENABLEDISABLE	statusForEnableDisable	bigint(20)	Indicates whether the connection is successfully established or not. Following are the available values:

Column Name	Column Name (For Querying)	Column Type	Description
			• '1' - the external connection was successfully established • '0' - the external connection was unsuccessful
UPDATEDBY	updatedBy	varchar(255)	Indicates the user who updated the external connection.
UPDATEDON	updatedOn	datetime	Indicates the date when details were updated for an existing connector.
TEMPLATENAME	templateName	varchar(255)	Indicates the template name used to create the external connection.

Column Name	Column Name (For Querying)	Column Type	Description
TEMPLATE_MANDATORYDATA	templateMandatoryData	longtext	Indicates the JSON used to define the attribute in the template.

ECM Import Job (ecmimportjob)

The ecmimportjob table provides information related to the **Job History Details** page on the **Job Control Panel** page.

Column Name	Column Type	Description
JOBID	bigint	Stores the job id once it is scheduled.
COMENTS	longtext	Stores the details of all the columns in concatenated form.
EXTERNALCONNECTION	mediumtext	Stores the name of the external connection used for importing data into Saviynt.
IP ADDRESS	varchar(255)	Stores the IP address from where the job was executed.

Column Name	Column Type	Description
JOBENDDATE	datetime	Stores the end date and time by when the job execution is complete.
JOBSTARTDATE	datetime	Stores the start date and time by when the job execution started.
JOBGROUP	varchar(255)	Specifies the category to which the job belongs.
JOBNAME	varchar(255)	Stores the name of the job.
SAVRESPONSE	varchar(255)	Stores the status of the job once its execution is complete. Following are its statuses: • Success

Column Name	Column Type	Description
		- Failure
SYSTEMNAME	varchar(255)	Stores the name of the security system.
TRIGGERNAME	varchar(255)	Stores the name of the job trigger.

Import Log Table (importlog)

This table provides information on the job log details page of the Job Control Panel.

Column Name	Column Type	Description
IMPORTLOGID	bigint	Stores each record entry in an incremental format.
FILENAME	varchar(255)	Stores the name of the job.
JOBID	bigint	Indicates the job ID associated with the job.
LOGDATAASXML	longtext	Stores the log details of the job in the

Column Name	Column Type	Description
		XML format.
PARENTJOBID	bigint	Stores the parent job ID where multiple jobs are part of a single job. For example, TriggerChainJob.

Roles Table (roles)

This table provides information related to roles and role configuration in Saviynt Identity Cloud.

Roles are assigned to users to define their access rights such as basic access, job-based requirements, auxiliary, or dynamic access.

Column Name	Column Name (For Querying)	Column Type	Description
ROLEKEY (PK)	id (PK)	bigint(20)	This is the unique primary key representing the role.
CONFIDENTIALITY	confidentiality	bigint(20)	This column determines the level of confidentiality that the role carries. The role owner

Column Name	Column Name (For Querying)	Column Type	Description
			can approve or reject requests based on the value in this column. The available values for this column are: Very Low, Low, Medium, High, or Critical.
CUSTOMPROPERTY 1-5	customproperty1 1-5	longtext	Based on the application type and values configured in third-party applications for various custom-properties, you can define the custom property values for different roles in Saviynt Identity Cloud. You can define up to 60

Column Name	Column Name (For Querying)	Column Type	Description
			custom properties for a role. The custom properties differentiate roles from one another.
CUSTOMPROPERTY 6-60	customproperty1 6-60	varchar(255)	Based on the application type and values configured in third-party applications for various custom-properties, you can define the custom property values for different roles in Saviynt Identity Cloud. You can define up to 60 custom properties for a role. The custom properties differentiate roles from one another.

Column Name	Column Name (For Querying)	Column Type	Description
DEFAULTTIMEFRAMEHRS	defaultTimeFrameHrs	bigint(20)	Indicates time frame in hours for the role
DESCRIPTION	DESCRIPTION		Indicates the description of a role.
DISPLAYNAME	displayname	varchar(255)	Indicates the display name of the role. The display name is used when filtering or searching roles using the **Advanced Search** option.
ENDPOINTKEY	endpointkey	bigint(20)	Indicates the endpoint name to which a role is associated.

Column Name	Column Name (For Querying)	Column Type	Description
FLAGEXPORTEDTOOIA	flagexportedtoOIA	bit(1)	Indicates the flag indicating if the role is exported to OIA.
GLOSSARY	glossary	varchar(255)	Indicates the glossary of the role.
SAVLEVEL	level	bigint(20)	Indicates the SAV role levels. An SAV role is defined by Saviynt Identity Cloud. It is available by default.
MAXTIMEFRAMEHRS	maxTimeFrameHrs	bigint(20)	Indicates the maximum time frame in hours that a role lasts.
MININGINSTANCE	mininginstance	varchar(255)	Indicates the role mining instance.

Column Name	Column Name (For Querying)	Column Type	Description
			Role mining provides information about users assigned to similar roles across various business applications.
PARENTROLES (FK)	parentroles (FK)	bigint(20)	Indicates the parent role to which the role is assigned.
PRIVILEGED	privileged	bigint(20)	Indicates if the role is a privileged role. Privileges determine the additional attributes that are associated with an entitlement type based on which the access is granted to the associated role.

Column Name	Column Name (For Querying)	Column Type	Description
REQUESTABLE	requestable	bit(1)	Indicates if the role is requestable. The values are Yes or No.
RISK	risk	bigint(20)	Indicates the risk level associated with the role. This value populates the criticality or risk involved in assigning this role to user based on the SOD configuration.
ROLE_NAME	role_name	varchar(255)	Indicates the name of the role.
ROLETYPE	roletype	bigint(20)	Indicates the type of role that is created.

Column Name	Column Name (For Querying)	Column Type	Description
			The values are firefighter, enabler, enterprise, transactional, or application.
SHOWDYNAMICATTRS	showDynamicAttrs	bit(1)	Indicates whether to show or hide the dynamic attributes associated with the role.
SOD	sodflag	bit(1)	Indicates the Separationof Duties (SOD) for the role.
SOX_CRITICAL	soxcritical	bigint(20)	Indicates the SOX criticality for the role. SOX criticality defines the level of roles or policies critically compliant with Sarbanes-Oxley IT

Column Name	Column Name (For Querying)	Column Type	Description
			regulations. The following values are available for this column: Very Low, Low, Medium, High, or Critical.
STATUS	status	bigint(20)	Indicates the status of the role. • Active - Indicates that the role is active for the assignee. • Inactive - Indicates that the role is inactive for the assignee.

Column Name	Column Name (For Querying)	Column Type	Description
SYS_CRITICAL	syscritical	bigint(20)	Indicates the criticality level of roles or policies within the system. The following values are available for this column: Very Low, Low, Medium, High, or Critical.
SYSTEMID	systemid	bigint(20)	Stores the ID of the security system to which the role belongs.
UPDATEDATE	updatedate	datetime	Indicates the last modified date of the role.
UPDATEUSER	updateuser	bigint(20)	Indicates the name of the user

Column Name	Column Name (For Querying)	Column Type	Description
			who modified the role details.

Role User Account Table (role_user_account)

This table provides information about the roles assigned to user accounts.

Column Name	Column Name (For Querying)	Column Type	Description
Id (PK)	Id (PK)	bigint(20)	The unique primary key representing the role assigned to the user account.
ACCOUNTKEY(FK)	accountkey(FK)	bigint(20)	The key representing the user account.
COMMENTS	comments	varchar(255)	Specifies the comments added when the role is assigned to

Column Name	Column Name (For Querying)	Column Type	Description
			the user account.
ENDDATE	enddate	datetime	Specifies the end date when the role assigned to the user account expires.
LASTCERTIFIEDCAMPAIGNDATE	lastCertifiedCampaignDate	datetime	Specifies the date of the last certified campaign.
LASTCERTIFIEDCAMPAIGNNAME	lastCertifiedCampaignName	varchar(255)	Specifies the campaign name which certified the role assigned to the user account.
LASTCERTIFIEDUSER	lastCertifiedUser	bigint(20)	Specifies the last certified user of the campaign.

Column Name	Column Name (For Querying)	Column Type	Description
ROLEKEY (FK)	rolekey (FK)	bigint(20)	Specifies the key representing the role.
SOURCE	source	varchar(255)	Specifies the source of the role assigned to the user account.
STARTDATE	startdate	datetime	Specifies the start date from when the role assigned to the user account is valid.
UPDATEDATE	updatedate	datetime	Specifies the date of assigning the role to the user account.
UPDATEUSER	updateuser	varchar(255)	Specifies the name of the user who modified the role assignment for the user

Column Name	Column Name (For Querying)	Column Type	Description
			account.
USERKEY (FK)	userkey (FK)	bigint(20)	Specifies the key representing the user.

Role Entitlements Table (role_entitlements)

This table provides information about the role entitlement configuration.
In Saviynt Identity Cloud, roles are created and assigned entitlements as required. Roles can constitute a collection of entitlements. It is possible to create a role with or without entitlements. After the roles are created, they are assigned to the users.

Column Name	Column Name (For Querying)	Column Type	Description
ROLEKEY (PK)	rolekey (PK)	bigint(20)	Specifies the unique key representing the role. It is used to certify individual roles from the list of roles associated with role owners.

Column Name	Column Name (For Querying)	Column Type	Description
ENTITLEMENT_VALUEKEY (PK)	entitlement_valuekey (PK)	bigint(20)	Specifies the unique key representing the value of the entitlement. It is used in entitlement queries to refine the query to filter the user accounts while creating an attestation.
UPDATEDATE	updatedate	datetime	Specifies the date the role entitlement record was updated.
UPDATEUSER	updateuser	varchar(255)	Indicates the name of the user who modified the role entitlement record.

User Group Users Table (usergroup_users)

This table provides information about the users of user groups.

Column Name	Column Name (For Querying)	Column Type	Description
USERKEY (PK)	userkey (PK)	bigint(20)	This is the primary key of the **usergroup_users** table that helps you identify a specific user from the table. You can use it to map the user with other tables. For example, to obtain account details of a single user, use the userkey from the **users** table with the userkey from the **user_account** table and use the join query using accountkey in the user_account with accountkey (PK) in accounts table.

Column Name	Column Name (For Querying)	Column Type	Description
USER_GROUPKEY (PK)	user_groupkey (PK)	bigint(20)	This is another primary key of the **usergroup_users** table that helps you identify a specific usergroup from the table. You can use it to map the usergroup with other tables.
UPDATEDATE	updatedate	datetime	Specifies the last modified date of the user group.
UPDATEUSER	updateuser	varchar(255)	Specifies the name of the user who modified the usergroup details.

User Group Entitlements Table (usergroup_entitlements)

This table provides information about user group entitlements.

Column Name	Column Name (For Querying)	Column Type	Description
ENTITLEMENT_VALUEKEY (PK)	entitlement_valuekey (PK)	bigint(20)	Specifies the unique key representing the entitlement value. It is used in entitlement queries to refine the query to filter the user accounts while creating an attestation.
USER_GROUPKEY (PK)	user_groupkey (PK)	bigint(20)	This is another primary key of the usergroup_entitlements ta ble that helps you identify a specific usergroup entitlement from the table. You can use it to map the usergroup with other tables.
UPDATEDATE	updatedate	datetime	Specifies the last modified date of the user group entitlements.

Column Name	Column Name (For Querying)	Column Type	Description
UPDATEUSER	updateuser	bigint(20)	Specifies the name of the user who modified the user group entitlements details.

User Group Owners Table (usergroup_owners)

This table provides information about the user group owners.

Column Name	Column Name (For Querying)	Column Type	Description
USERKEY (PK)	userkey (PK)	bigint(20)	This is the primary key of the **usergroup_owners** table. It helps you identify a specific user from the table. You can use it to map the user with other tables. For example, to obtain the account details of a single

Column Name	Column Name (For Querying)	Column Type	Description
			user, use userkey from the **users** table with userkey from the **user_account** table and then use the join query using accountkey from the **user_account** table with accountkey (PK) from the **accounts** table.
USERGROUPKEY (PK)	usergroupkey (PK)	bigint(20)	This is another primary key of the **usergroup_owners** table that helps you identify a specific usergroup owner from the table. You can use it to map the usergroup with other tables.
RANK (PK)	rank (PK)	int(11)	Specifies the rank of the user

Column Name	Column Name (For Querying)	Column Type	Description
			group.
UPDATEDATE	updatedate	datetime	Specifies the last modified date of the user group owners.
UPDATEUSER	updateuser	varchar(255)	Specifies the name of the user who modified the user group owner details.

User Groups Table (user_groups)

This table provides information about the user groups.

Column Name	Column Name (For Querying)	Column Type	Description
USERGROUPKEY	id	bigint(20)	This is a primary key of the **user_groups** table that

Column Name	Column Name (For Querying)	Column Type	Description
			helps you identify a specific user group from the table. You can use it to map the user groups with other tables.
GROUPID	groupID	bigint(20)	Specifies the group ID of the user group.
UPDATEDATE	updatedate	datetime	Specifies the last modified date of the user groups.
UPDATEUSER	updateuser	bigint(20)	Specifies the name of the user who modified the user group details.
USER_GROUPDESCRIPTION	user_groupdescription	varchar(255)	Specifies the description of the user group.

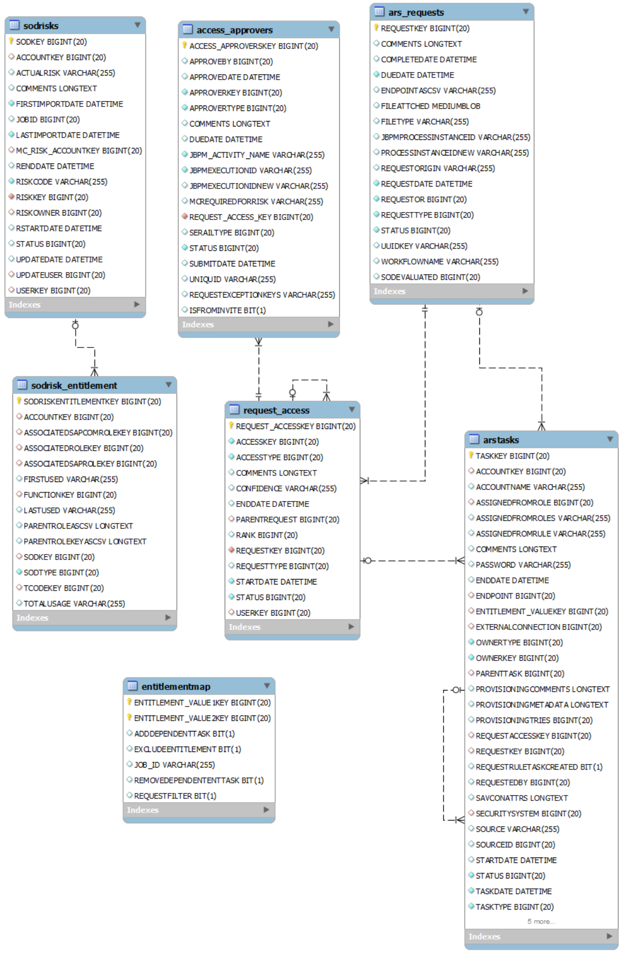
Column Name	Column Name (For Querying)	Column Type	Description
USER_GROUPNAME	user_groupname	varchar(255)	Specifies the name of the user group.

Request Table

This table provides information related to requests and approvals and how they are mapped.

The requests are raised by users for themselves or for other users to obtain authorized access to perform tasks. The requests are then assigned to approvers to validate them based on the configured workflows.

The following diagram shows the relationship among the participants of request and approval system whose details are stores in different tables (requestor, approver, ars_requests, request_access, access_approver, and arstask):


sodrisks
SODKEY BIGINT(20)
ACCOUNTKEY BIGINT(20)
ACTUALRISK VARCHAR(255)
COMMENTS LONGTEXT
FIRSTIMPORTDATE DATETIME
JOBID BIGINT(20)
LASTIMPORTDATE DATETIME
MC_RISK_ACCOUNTKEY BIGINT(20)
RENDDATE DATETIME
RISKCODE VARCHAR(255)
RISKKEY BIGINT(20)
RISKOWNER BIGINT(20)
RSTARTDATE DATETIME
STATUS BIGINT(20)
UPDATEDATE DATETIME
UPDATEUSER BIGINT(20)
USERKEY BIGINT(20)
Indexes
access_approvers
ACCESS_APPROVERSKEY BIGINT(20)
APPROVEBY BIGINT(20)
APPROVEDATE DATETIME
APPROVERKEY BIGINT(20)
APPROVERTYPE BIGINT(20)
COMMENTS LONGTEXT
DUEDATE DATETIME
JBPM_ACTIVITY_NAME VARCHAR(255)
JBPMEXECUTIONID VARCHAR(255)
JBPMEXECUTIONIDNEW VARCHAR(255)
MCREQUIREDFORRISK VARCHAR(255)
REQUEST_ACCESS_KEY BIGINT(20)
SERAILTYPE BIGINT(20)
STATUS BIGINT(20)
SUBMITDATE DATETIME
UNIQUID VARCHAR(255)
REQUESTEXCEPTIONKEYS VARCHAR(255)
ISFROMINVITE BIT(1)
Indexes
ars_requests
REQUESTKEY BIGINT(20)
COMMENTS LONGTEXT
COMPLETEDATE DATETIME
DUEDATE DATETIME
ENDPOINTASCSV VARCHAR(255)
FILEATTCHED MEDIUMBLOB
FILETYPE VARCHAR(255)
JBPMPROCESSINSTANCEID VARCHAR(255)
PROCESSINSTANCEIDNEW VARCHAR(255)
REQUESTORIGIN VARCHAR(255)
REQUESTDATE DATETIME
REQUESTOR BIGINT(20)
REQUESTTYPE BIGINT(20)
STATUS BIGINT(20)
UUIDKEY VARCHAR(255)
WORKFLOWNAME VARCHAR(255)
SODEVALUATED BIGINT(20)
Indexes
sodrisk_entitlement
SODRISKENTITLEMENTKEY BIGINT(20)
ACCOUNTKEY BIGINT(20)
ASSOCIATEDSAPCOMROLEKEY BIGINT(20)
ASSOCIATEDROLEKEY BIGINT(20)
ASSOCIATEDSAPROLEKEY BIGINT(20)
FIRSTUSED VARCHAR(255)
FUNCTIONKEY BIGINT(20)
LASTUSED VARCHAR(255)
PARENTROLEASCSV LONGTEXT
PARENTROLEKEYASCSV LONGTEXT
SODKEY BIGINT(20)
SODTYPE BIGINT(20)
TCODEKEY BIGINT(20)
TOTALUSAGE VARCHAR(255)
Indexes
request_access
REQUEST_ACCESSKEY BIGINT(20)
ACCESSKEY BIGINT(20)
ACCESSTYPE BIGINT(20)
COMMENTS LONGTEXT
CONFIDENCE VARCHAR(255)
ENDDATE DATETIME
PARENTREQUEST BIGINT(20)
RANK BIGINT(20)
REQUESTKEY BIGINT(20)
REQUESTTYPE BIGINT(20)
STARTDATE DATETIME
STATUS BIGINT(20)
USERKEY BIGINT(20)
Indexes
arstasks
TASKKEY BIGINT(20)
ACCOUNTKEY BIGINT(20)
ACCOUNTNAME VARCHAR(255)
ASSIGNEDFROMROLE BIGINT(20)
ASSIGNEDFROMROLES VARCHAR(255)
ASSIGNEDFROMRULE VARCHAR(255)
COMMENTS LONGTEXT
PASSWORD VARCHAR(255)
ENDDATE DATETIME
ENDPOINT BIGINT(20)
ENTITLEMENT_VALUEKEY BIGINT(20)
EXTERNALCONNECTION BIGINT(20)
OWNERTYPE BIGINT(20)
OWNERKEY BIGINT(20)
PARENTTASK BIGINT(20)
PROVISIONINGCOMMENTS LONGTEXT
PROVISIONINGMETADATA LONGTEXT
PROVISIONINGTRIES BIGINT(20)
REQUESTACCESSKEY BIGINT(20)
REQUESTKEY BIGINT(20)
REQUESTRULETASKCREATED BIT(1)
REQUESTEDBY BIGINT(20)
SAVCONATTRS LONGTEXT
SECURITYSYSTEM BIGINT(20)
SOURCE VARCHAR(255)
SOURCEID BIGINT(20)
STARTDATE DATETIME
STATUS BIGINT(20)
TASKDATE DATETIME
TASKTYPE BIGINT(20)
5 more...
Indexes
entitlementmap
ENTITLEMENT_VALUE1KEY BIGINT(20)
ENTITLEMENT_VALUE2KEY BIGINT(20)
ADDDEPENDENTTASK BIT(1)
EXCLUDEENTITLEMENT BIT(1)
JOB_ID VARCHAR(255)
REMOVEDEPENDENTENTTASK BIT(1)
REQUESTFILTER BIT(1)
Indexes

ARS Requests Table (ars_requests)

This table provides information about the requests.

Column Name	Column Name (For Querying)	Column Type	Description
REQUESTKEY	id	bigint(20)	This is the unique identifier for each request raised through ARS.
COMMENTS	comments	longtext	Specifies the comments entered by the user while making a request.
COMPLETEDATE	completeDate	datetime	Specifies the date when the request is completed meaning the access is granted and the request is closed.
DUEDATE	duedate	datetime	Specifies the date of when the

Column Name	Column Name (For Querying)	Column Type	Description
			granted access expires.

ENDPOINTASCSV	endpointascsv	varchar(255)
		varchar(2000)
			Specifies comma-separated values of the endpoint names involved in the request.
			ⓘ Info
			The column size is extended to varchar(2000).

JBPMPROCESSINSTANCEID	processinstanceid	varchar(255)	Provides a concatenated expression including the current workflow activity name and the request-id from the user interface. For example, if

Column Name	Column Name (For Querying)	Column Type	Description
			the current workflow activity associated with this request is ManagerApproval and request-id is 1050, this field displays ManagerApproval.1050.
REQUESTORIGIN	requestOrigin	varchar(255)	Specifies the source of the request such user interface, file upload, web service, SOD, or an existing request.
REQUESTDATE	requestdate	datetime	Specifies the date of submitting the request.
REQUESTOR	requestor	bigint(20)	Stores the user key of the requestor.

Column Name	Column Name (For Querying)	Column Type	Description
REQUESTTYPE	requesttype	bigint(20)	Stores the numeric equivalent of the request type. For example, request type 1 means that it is an “Add Access” request, request type 3 means that it is a “New Account” request.
STATUS	status	bigint(20)	Stores the numeric equivalent of the status of the request. For example, Status 1 means that the request is created and not yet approved, 3 means request is completed.
UUIDKEY	uuid	varchar(255)	Stores a unique alphanumeric identifier such as Length.

Column Name	Column Name (For Querying)	Column Type	Description
WORKFLOWNAME	workflowname	varchar(255)	Stores the name of the workflow used for processing the request.
SODEVALUATED	sodEvaluated	bigint(20)	Stores the numeric equivalent of the status of the SOD evaluation.

Request Access Table (request_access)

This table provides information about the approved entitlements via requests.

Column Name	Column Name (For Querying)	Column Type	Description
REQUEST_ACCESSKEY	id	bigint(20)	Specifies unique identifiers for each access associated with the request.

Column Name	Column Name (For Querying)	Column Type	Description
ACCESSKEY	accesskey	bigint(20)	Stores the entitlement value key of the entitlement associated with the request.
ACCESSTYPE	accesstype	bigint(20)	Stores the numeric equivalent of the type of access involved as part of the request.
COMMENTS	comments	longtext	Stores the comments entered by the approver while approving or rejecting the request.
ENDDATE	enddate	datetime	Specifies the end date to remove the access for the user.

Column Name	Column Name (For Querying)	Column Type	Description
PARENTREQUEST	parentrequest	bigint(20)	Specifies the parent request number in the request (child request).
RANK	rank	bigint(20)	Specifies the access rank.
REQUESTKEY	requestkey	bigint(20)	Stores the corresponding request key from the ars_requests table.
REQUESTTYPE	requesttype	bigint(20)	Specifies the numeric equivalent of the type of request.
STARTDATE	startdate	datetime	Specifies the date when the authorized user is granted the requested access.

Column Name	Column Name (For Querying)	Column Type	Description
STATUS	status	bigint(20)	Specifies the status of the request. It store only the numeric equivalent of the status.
USERKEY	userkey	bigint(20)	Specifies the user key of the beneficiary user.

Access Approver Table (access_approvers)

This table provides information about the approved requests along with approver details.

Column Name	Column Name (For Querying)	Column Type	Description
ACCESS_APPROVERSKEY	id	bigint(20)	This is the primary key of the Access_approvers table that uniquely identifies each approval or rejection activity

Column Name	Column Name (For Querying)	Column Type	Description
			by the approver.
APPROVEBY	approveby	bigint(20)	Specifies the user key of the user who approved the request.
APPROVEDATE	approvedate	datetime	Specifies the date when the request is approved or rejected by the approver.
APPROVERKEY	approverKey	bigint(20)	Stores the user key of the user to whom the request was assigned for approval.
APPROVERTYPE	approverType	bigint(20)	Specifies the type of approver.

Column Name	Column Name (For Querying)	Column Type	Description
			• '1' - indicates the approver is a user. • '2' - indicates the approver is a user group.
COMMENTS	comments	longtext	Stores the comments submitted during approval or rejection of the request.
DUEDATE	duedate	datetime	Stores the due date for approval of the request.
JBPM_ACTIVITY_NAME	jbpmActivityName	varchar(255)	Stores the activity name of the workflow associated with the approval or rejection of the access

Column Name	Column Name (For Querying)	Column Type	Description
JBPMEXECUTIONID	jbpmexecutionid	varchar(255)	Stores a combined value of the JBPM workflow name and the request-id.
REQUEST_ACCESS_KEY	request_access	bigint(20)	Stores the request access key from the request_access table.

REQUESTEXCEPTIONKEYS	requestexceptionkeys	varchar(255)
		varchar(1024)
			Stores the request exception keys.
			ⓘ Info
			The column size is exteneded to varchar(1024).

STATUS	status	bigint(20)	Specifies the status of the

Column Name	Column Name (For Querying)	Column Type	Description
			request.
SUBMITDATE	submitdate	datetime	Specifies the date of submitting the request.
UNIQUID	uniquid	varchar(255)	Specifies the unique identifier for each access record.
ISFROMINVITE	isFromInvite	bit(1)	This is a Boolean field that determines whether the request is generated from an invite activity.

ARS Tasks Table (arstasks)

This table provides information about task details.

Column Name	Column Name (For Querying)	Column Type	Description
TASKKEY	id	bigint(20)	Specifies the unique task identifier. It is displayed as Task Id in the user interface.
ACCOUNTKEY	accountKey	bigint(20)	Stores the account key for the account associated with the task.
ACCOUNTNAME	accountName	varchar(255	Stores the name of the account associated with the task.
ASSIGNEDFROMROLE	assignedFromRole	bigint(20)	Stores the corresponding rolekey if the access associated with the task is assigned from a single role.

Column Name	Column Name (For Querying)	Column Type	Description
ASSIGNEDFROMROLES	assignedFromRoles Info The data type of the `ASSIGNEDFROMROLES` column in the account_entitlements1 table is now displayed as text, as the size has been increased from varchar (1024) to varchar (3000).	varchar(255)	Stores the corresponding rolekey if the access associated with the task is assigned from multiple roles.
ASSIGNEDFROMRULE	assignedFromRule	varchar(255)	Stores the corresponding rulekey if the access associated with the task is assigned from a rule.

Column Name	Column Name (For Querying)	Column Type	Description
COMMENTS	comments	longtext	Stores the comments entered during task execution. Comments that are entered when an action is selected from the Actions drop-down list from Pending or Completed Task screens are also stored.
PASSWORD	encryptedPassword	varchar(255)	Stores the encrypted password associated with the task.
ENDPOINT	Cendpoint	bigint(20)	Stores the endpoint key of the endpoint for which the task is targeted.

Column Name	Column Name (For Querying)	Column Type	Description
ENTITLEMENT_VALUEKEY	entitlement_valueKey	bigint(20)	Stores the entitlement value key of the entitlement associated with the task.
EXTERNALCONNECTION	externalConnection	bigint(20)	Specifies the connection used to perform the task.
OWNERTYPE	ownerType	bigint(20)	Stores the numeric equivalent for the type of the owner. • '1' - indicates the owner type is a specific user. • '2' - indicates the owner type is a user group.
OWNERKEY	ownerkey	bigint(20)	Stores either the user key or the user group key based on

Column Name	Column Name (For Querying)	Column Type	Description
			the owner type.
PARENTTASK	parenttask	bigint(20)	Stores the task id of the parent task.
PROVISIONINGCOMMENTS	provisioningComments	longtext	Stores the comments added while provisioning the task. Use this field to determine what has gone wrong if a task fails.
PROVISIONINGMETADATA	provisioningMetadata	longtext	Stores the metadata associated while provisioning the task to the target application.
PROVISIONINGTRIES	provisioningTries	bigint(20)	Specifies the number of tries

Column Name	Column Name (For Querying)	Column Type	Description
			performed to provision the task.
REQUESTACCESSKEY	requestAccessKey	bigint(20)	Stores the corresponding request access key from the request_Access table.
REQUESTKEY	requestKey	bigint(20)	Stores the corresponding request access key from the ars_requests table.
REQUESTRULETASKCREATED	requestRuleTaskCreated	bit(1)	Specifies whether the task is created as a result of request rule execution.
REQUESTEDBY	requestedBy	bigint(20)	Stores the user key of the requestor.

Column Name	Column Name (For Querying)	Column Type	Description
SECURITYSYSTEM	securitysystem	bigint(20)	Stores the security system key of the security system associated with this task.
SOURCE	source	varchar(255)	Stores the source that has generated the task. Tasks are generated from multiple sources.
STARTDATE	startDate	datetime	Specifies the time when the task was created.
STATUS	status	bigint(20)	Stores the numeric equivalent of the status of the task.
TASKDATE	taskdate	datetime	Specifies the date and time of executing the task.

Column Name	Column Name (For Querying)	Column Type	Description
TASKTYPE	tasktype	bigint(20)	Stores the numeric equivalent of the type of task.
UPADTEUSER	upadteuser	bigint(20)	Stores the userkey of the user who has most recently updated or modified the task.
UPDATEACCOUNTTASKCREATED	updateAccountTaskCreated	bit(1)	Specifies if the task is an Update Account Task.
UPDATEDATE	updateDate	datetime	Specifies the most recent date of updating the task.
USERKEY	users	bigint(20)	Stores the user key of the beneficiary user whose account or profile will be modified after the task is

Column Name	Column Name (For Querying)	Column Type	Description
			executed.

SOD Table (Separationof duties)

This table provides information related to the Separationof duties defined in Saviynt Identity Cloud.

SOD Risks Table (sodrisks)

This table provides information about SOD risks.

Column Name	Column Name (For Querying)	Column Type	Description
SODKEY	id	bigint(20)	Stores the unique SOD key to identify an organization.
ACCOUNTKEY	accountkey	bigint(20)	Stores the unique user accountkey to identify the account that violates the risk.

Column Name	Column Name (For Querying)	Column Type	Description
ACTUALRISK	actualRisk	varchar(255)	Specifies whether the SOD risk is a potential risk or an actual risk based on the usage log of access retrieved from the target application.
COMMENTS	comments	longtext	Stores the comments added while specifying the SOD risk.
FIRSTIMPORTDATE	firstImportDate	datetime	Specifies the date when the SOD risk is added to the user account.
JOBID	jobId	bigint(20)	Stores the Job ID of the RiskSODEvaluation job for which this SOD risk was generated.

Column Name	Column Name (For Querying)	Column Type	Description
LASTIMPORTDATE	lastImportDate	datetime	Specifies the most recent date when the SOD risk is added to the user account.
MC_RISK_ACCOUNTKEY	mc_risk_account	bigint(20)	Stores the foreign key association between the SOD risk and the mc_risk_account table.
RENDDATE	renddate	datetime	Specifies the last date of mitigating control applied to the SOD risk.
RISKCODE	riskcode	varchar(255)	Specifies the risk name of the SOD risk.
RISKKEY	riskkey	bigint(20)	Stores the risk key of the SOD

Column Name	Column Name (For Querying)	Column Type	Description
			risk.
RISKOWNER	riskowner	bigint(20)	Stores the userkey of the SOD risk owner.
RSTARTDATE	rstartdate	datetime	Specifies the start date of mitigating control applied to the SOD risk.
STATUS	status	bigint(20)	Specifies the current status of the SOD risk. • 1 - New • 2 - In Progress • 3 - Risk • 4 - closed

Column Name	Column Name (For Querying)	Column Type	Description
			• 5 - Accepted/Remediated
UPDATEDATE	updatedate	bigint(20)	Specifies the most recent date of updating the SOD risk.
UPDATEUSER	updateuser	bigint(20)	Stores the userkey of the user who recently updated the SOD risk.
USERKEY	userkey	bigint(20)	Stores the userkey of the user whose account violates the SOD risk.

SOD Risk Entitlement Table (sodrisk_entitlement)

This table provides information about entitlements related to SOD risks.

Column Name	Column Name (For Querying)	Column Type	Description
SODRISKENTITLEMENTKEY	id	bigint(20)	Stores a unique SOD key to identify the SOD risk entitlement.
ACCOUNTKEY	accountkey	bigint(20)	Stores a unique user account key to identify the account that violates the risk.
ASSOCIATEDSAPROLEKEY	associatedsaprolekey	bigint(20)	Stores the entitlement_valuekey of parent entitlement which is directly assigned to user account.
FUNCTIONKEY	functionkey	bigint(20)	Stores the function associated with risk that is added with a violating entitlement.

Column Name	Column Name (For Querying)	Column Type	Description
PARENTROLEASCSV	parentroleascsv	longtext	Stores the entitlement value of the parent entitlement that is directly assigned to the user account.
PARENTROLEKEYASCSV	parentrolekeyascsv	longtext	Stores the entitlement_valuekey of the parent entitlement that is directly assigned to the user account.
SODKEY	sodkey	bigint(20)	Stores the foreign key association between the SOD risk and the sodrisk_entitlement table.
SODTYPE	sodtype	bigint(20)	Specifies the type of the SOD.

Column Name	Column Name (For Querying)	Column Type	Description
			The options are: • '1' - indicates role. • '2' - indicates entitlement.
TCODEKEY	tcodekey	bigint(20)	Stores the entitlement_valuekey of the child entitlement assigned to the user account that causes the violation.

Entitlement Map Table (entitlementmap)

This table contains the details of the child and parent entitlements associated with the access.

Column Name	Column Name (For Querying)	Column Type	Description
ENTITLEMENT_VALUE1KEY	entitlement_value1key	bigint(20)	Stores the unique key in the

Column Name	Column Name (For Querying)	Column Type	Description
			row which helps to identify specific entitlement and entitlement type association.
ENTITLEMENT_VALUE2KEY	entitlement_value2key	bigint(20)	Stores the unique key in the row which helps to identify specific entitlement and entitlement type association.
ADDDEPENDENTTASK	addDependentTask	bit(1)	Specifies the
EXCLUDEENTITLEMENT	excludeEntitlement	bit(1)	Specifies the entitlement that is excluded while requesting access.
JOB_ID	jobId	varchar(255)	Stores the unique job id associated with the access.

Column Name	Column Name (For Querying)	Column Type	Description
REMOVEDEPENDENTENTTASK	removeDependentEntTask	bit(1)	Specifies the dependent entitlement task to remove the access.

Identity Match and Merge Table (identitymatchandmergedetails)

Info

The Identity Match and Merge feature is applicable from Release v2021.0 onwards.

This table contains the details of fields used in Identity Match and Merge.

Column Name	Column Name (For Querying)	Column Type	Description
MATCHKEY	id	bigint(20)	This is the primary key of this table. This contains a unique id of every match pair combination.

Column Name	Column Name (For Querying)	Column Type	Description
ATTRIBUTESMATCHED	attributesMatched	text	Contains those attributes among the ones defined in fine-matching criteria based on which the match is derived. Sample data: “firstname, lastname".
COMMENTS	comments	text	Stores the details of the actions taken on every match.
CREATEDON	createdOn	datetime	Stores the date on when the match was detected first.
PRIMARYUSERKEY	primaryUserKey	bigint(20)	Stores the userkey of the primary user

Column Name	Column Name (For Querying)	Column Type	Description
DUPLICATEUSERKEY	duplicateUserKey	bigint(20)	Stores the userkey of the duplicate user
JOBID	jobId	bigint(20)	Stores the job id of the Identity Match and Merge job.
LASTMODIFIEDON	lastModifiedOn	datetime	Stores the date on when the record was last modified. If these records were merged or rejected, then the date on when those actions were performed is stored here.
MATCHDETAILS	matchDetails	text	
MATCHPERCENT	matchPercent	bigint(20)	Stores the similarity score of the primary and the duplicate

Column Name	Column Name (For Querying)	Column Type	Description
			user based on the threshold defined in the fine matching criteria.
MERGEDBY	mergedBy	bigint(20)	Stores the userkey of the user who has merged the records.
MERGEDON	mergedOn	datetime	Stores the date on when the matched record was merged.
SOURCE	source	varchar(255)	Not applicable for now
STATUS	status	bigint(20)	Stores the current status of the match. The possible values: 0,1,2,3,4. If the STATUS_INACTIVE = 0,

Column Name	Column Name (For Querying)	Column Type	Description
			then the match is no longer valid, and the combination is inactive. If the STATUS_ACTIVE = 1 , then the match has been detected in any of the identity matching process. A manual review is still pending on this record. If the STATUS_MERGED = 2, then the duplicate and the primary combinations have been merged. If the STATUS_REJECTED = 3, then the match will not be redetected as a duplicates even in the future runs. If the STATUS_IGNORED = 4, then the match was ignored

Column Name	Column Name (For Querying)	Column Type	Description
			and can be redetected as a duplicate in the future runs.

merged_attribute_details	mergedAttributeDetails	longtext	Whenever we pick up attributes of a duplicate user to be merged into the primary user, the details are stored here in the JSON format. Sample data is shown below:
			JSON
			`{`
			`  "city": {`
			`    "fromPrimary":`
			`"Bangalore",`
			`    "fromDuplicate":`
			` "Mumbai"  },`
			`  "state": {`

Column Name	Column Name (For Querying)	Column Type	Description

			`"fromPrimary":`
			`"Karnataka",`
			`"fromDuplicate":`
			`"Maharashtra"  }`
			`}`

RoleAccessMismatches

This table contains the details of fields used in RoleAccessMismatches.

Column Name	Column Type	Description
RAMKEY	bignit(20)	Stores the role access mismatches key
MISMATCH_TYPE	varchar(255)	Stores the types of mismatches
MISMATCH_SOURCEKEY	bigint(20)	Stores the key of mismatch sources.
REASON	varchar(255)	Stores the source of mismatch
ROLEKEY	bigint(20)	Stores the primary key of all roles that helps you to identify a specific role from the table.

Column Name	Column Type	Description
USERKEY	bigint(20)	Stores the primary key of all users that helps you to identify a specific user from the table.
ACCOUNTKEY	bigint(20)	Stores the primary key of all account that helps you to identify a specific account from the table.
ENTITLEMENT_VALUEKEY	bigint(20)	Indicates the entitlement name of the entitlement available for the account.
JOBID	bigint(20)	Indicates the job identification number.
RUA_ENDDATE	datetime	Stores the end date of users account to a role.
AE_ENDDATE	datetime	Stores the end date of accounts associated to entitlements.
ACCOUNTSTATUS	varchar(255)	Stores the account status.
REQUESTFORM	int(11)	Indicates the ARS Request Form identifier.
USERSTATUS	bigint(20)	Indicates the user's status.
CHILDROLEKEY	bigint(20)	Indicates the child role key.

Duplicate Identity Management and Merge Table (identitymatchandmergedetails)

This table contains the details of fields used in Duplicate Identity Management.

Column Name	Column Name (For Querying)	Column Type	Description
MATCHKEY	id	bigint(20)	This is the primary key of this table. This contains a unique id of every match pair combination.
ATTRIBUTESMATCHED	attributesMatched	text	Contains those attributes among the ones defined in fine-matching criteria based on which the match is derived. Sample data: “firstname, lastname".
COMMENTS	comments	text	Stores the details of the

Column Name	Column Name (For Querying)	Column Type	Description
			actions taken on every match.
CREATEDON	createdOn	datetime	Stores the date on when the match was detected first.
PRIMARYUSERKEY	primaryUserKey	bigint(20)	Stores the userkey of the primary user
DUPLICATEUSERKEY	duplicateUserKey	bigint(20)	Stores the userkey of the duplicate user
JOBID	jobId	bigint(20)	Stores the job id of the Duplicate Identity Detection Job. If the match is detected during user import or creation or update from Saviynt Identity Cloud Identity Repository, then

Column Name	Column Name (For Querying)	Column Type	Description
			the internal job id is stored.
LASTMODIFIEDON	lastModifiedOn	datetime	Stores the date on when the record was last modified. If these records were merged or rejected, then the date on when those actions were performed is stored here.
MATCHDETAILS	matchDetails	text	
MATCHPERCENT	matchPercent	bigint(20)	Stores the similarity score of the primary and the duplicate user based on the threshold defined in the fine matching criteria.

Column Name	Column Name (For Querying)	Column Type	Description
MERGEDBY	mergedBy	bigint(20)	Stores the userkey of the user who has merged the records.
MERGEDON	mergedOn	datetime	Stores the date on when the matched record was merged.
SOURCE	source	varchar(255)	Not applicable for now
STATUS	status	bigint(20)	Stores the current status of the match. The possible values: 0,1,2,3,4. If the STATUS_INACTIVE = 0, then the match is no longer valid, and the combination is inactive. If the STATUS_ACTIVE = 1 , then the match has been

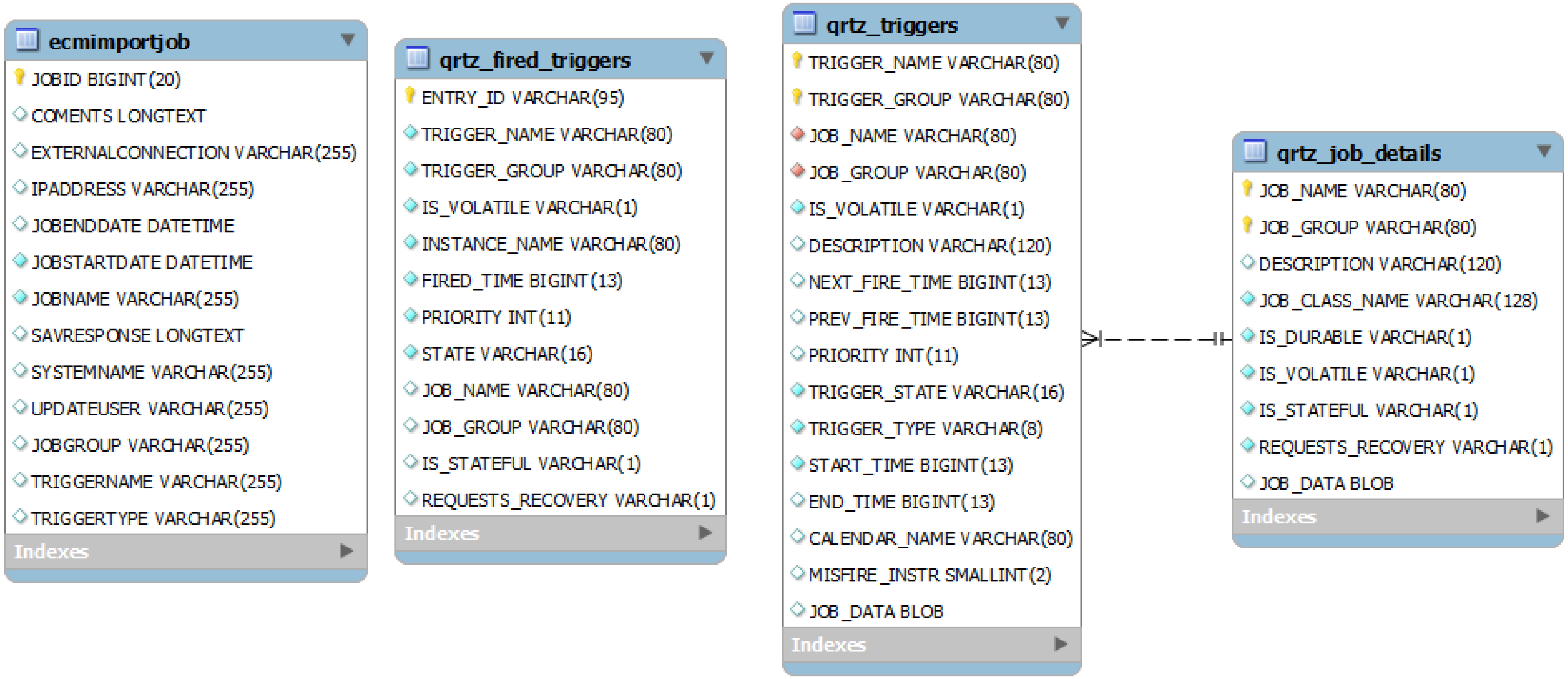
Column Name	Column Name (For Querying)	Column Type	Description
			detected in any of the identity matching process. A manual review is still pending on this record. If the STATUS_MERGED = 2, then the duplicate and the primary combinations have been merged. If the STATUS_REJECTED = 3, then the match will not be redetected as a duplicates even in the future runs. If the STATUS_IGNORED = 4, then the match was ignored and can be redetected as a duplicate in the future runs.
merged_attribute_details	mergedAttributeDetails	longtext	Whenever we pick up

Column Name	Column Name (For Querying)	Column Type	Description
			attributes of a duplicate user to be merged into the primary user, the details are stored here in the JSON format. Sample data is shown below: JSON

```
{
  "city": {
    "fromPrimary":
"Bangalore",
    "fromDuplicate":
 "Mumbai"  },
  "state": {
    "fromPrimary":
"Karnataka",
    "fromDuplicate":
 "Maharashtra"  }
}
```

Jobs Table

This table provides information about the jobs provided by Saviynt Identity Cloud.



ecmimportjob
JOBID BIGINT(20)
COMENTS LONGTEXT
EXTERNALCONNECTION VARCHAR(255)
IPADDRESS VARCHAR(255)
JOBENDDATE DATETIME
JOBSTARTDATE DATETIME
JOBNAME VARCHAR(255)
SAVRESPONSE LONGTEXT
SYSTEMNAME VARCHAR(255)
UPDATEUSER VARCHAR(255)
JOBGROUP VARCHAR(255)
TRIGGERNAME VARCHAR(255)
TRIGGERTYPE VARCHAR(255)

qrtz_fired_triggers
ENTRY_ID VARCHAR(95)
TRIGGER_NAME VARCHAR(80)
TRIGGER_GROUP VARCHAR(80)
IS_VOLATILE VARCHAR(1)
INSTANCE_NAME VARCHAR(80)
FIRED_TIME BIGINT(13)
PRIORITY INT(11)
STATE VARCHAR(16)
JOB_NAME VARCHAR(80)
JOB_GROUP VARCHAR(80)
IS_STATEFUL VARCHAR(1)
REQUESTS_RECOVERY VARCHAR(1)

qrtz_triggers
TRIGGER_NAME VARCHAR(80)
TRIGGER_GROUP VARCHAR(80)
JOB_NAME VARCHAR(80)
JOB_GROUP VARCHAR(80)
IS_VOLATILE VARCHAR(1)
DESCRIPTION VARCHAR(120)
NEXT_FIRE_TIME BIGINT(13)
PREV_FIRE_TIME BIGINT(13)
PRIORITY INT(11)
TRIGGER_STATE VARCHAR(16)
TRIGGER_TYPE VARCHAR(8)
START_TIME BIGINT(13)
END_TIME BIGINT(13)
CALENDAR_NAME VARCHAR(80)
MISFIRE_INSTR SMALLINT(2)
JOB_DATA BLOB

qrtz_job_details
JOB_NAME VARCHAR(80)
JOB_GROUP VARCHAR(80)
DESCRIPTION VARCHAR(120)
JOB_CLASS_NAME VARCHAR(128)
IS_DURABLE VARCHAR(1)
IS_VOLATILE VARCHAR(1)
IS_STATEFUL VARCHAR(1)
REQUESTS_RECOVERY VARCHAR(1)
JOB_DATA BLOB

ECM Import Job Table (ecmimportjob)

This table contains details about imported accounts or access (entitlements).

Column Name	Column Name (For Querying)	Column Type	Description
JOBID	id	bigint(20)	Stores the unique id for the job.
COMMENTS	comments	longtext	Stores the comments entered for the job.
EXTERNALCONNECTION	externalconnection	varchar(255)	Specifies the name of the connection used for the job.
IPADDRESS	ipaddress	varchar(255)	Specifies the IP address of the system that initiates the job.
JOBENDDATE	jobEndDate	datetime	Specifies the date when

Column Name	Column Name (For Querying)	Column Type	Description
			the job stops to run.
JOBSTARTDATE	jobStartDate	datetime	Specifies the date when the job starts to run.
JOBNAME	jobname	varchar(255)	Specifies the name of the job.
SAVRESPONSE	response	longtext	Stores the Saviynt Identity Cloud's response for the job.
SYSTEMNAME	systemName	varchar(255)	Specifies the system name for the job.
UPDATEUSER	updateUser	varchar(255)	Specifies the id of the user who initiated the job.

Column Name	Column Name (For Querying)	Column Type	Description
JOBGROUP	jobgroup	varchar(255)	Specifies the name of the group that the job belongs to.
TRIGGERNAME	triggerName	varchar(255)	Specifies the name of the job trigger.
TRIGGERTYPE	triggerType	varchar(255)	Specifies the type of the job trigger.

qrtz_triggers Table

This table stores information about the configured triggers.

Column Name	Column Type	Description
TRIGGER_GROUP	varchar(80)	Specifies the job trigger group name.

Column Name	Column Type	Description
JOB_NAME	varchar(80)	Specifies the name of the job.
JOB_GROUP	varchar(80)	Specifies the name of the group that the job belongs to.
IS_VOLATILE	varchar(1)	Specifies if the job is volatile. A volatile job can perform different tasks such as import application data, import access and accounts. A volatile job is not persisted between program shutdowns.
DESCRIPTION	varchar(120)	Specifies the description of the job.
NEXT_FIRE_TIME	bigint(13)	Specifies the time to trigger the job again.

Column Name	Column Type	Description
PREV_FIRE_TIME	bigint(13)	Specifies the most recent time when the job was triggered.
PRIORITY	int(11)	Specifies the priority of the job.
TRIGGER_STATE	varchar(16)	Stores the trigger state of the job.
TRIGGER_TYPE	varchar(8)	Stores the trigger type of the job.
START_TIME	bigint(13)	Specifies the start time when the job runs.
END_TIME	bigint(13)	Specifies the time when the job stops running.
CALENDAR_NAME	varchar(80)	Stores the name of the calendar used for

Column Name	Column Type	Description
		the job.
MISFIRE_INSTR	smallint(2)	Stores the misfired instruction issued for the job.
JOB_DATA	blob	Stores the metadata related to the job.

qrtz_job_details Table

This table stores detailed information for every configured job.

Column Name	Column Type	Description
JOB_NAME	varchar(80)	Stores unique name to identify the job.
JOB_GROUP	varchar(80)	Specifies the name of the group that the job belongs to.

Column Name	Column Type	Description
DESCRIPTION	varchar(120)	Specifies the description of the job.
JOB_CLASS_NAME	varchar(128)	Stores the class name of the job.
IS_DURABLE	varchar(1)	Specifies if the job is durable. A non-durable job is automatically deleted from the scheduler when no active triggers are associated with it.
IS_VOLATILE	varchar(1)	Specifies if the job is volatile. A volatile job can perform different tasks such as import application data, import access, and accounts. A volatile job is not persisted between program shutdowns.

Column Name	Column Type	Description
IS_STATEFUL	varchar(1)	Specifies if the job is stateful. A stateful job guarantees that only one job runs at one time.
REQUESTS_RECOVERY	varchar(1)	Specifies if the scheduler re-executes a job when it encounters a 'recovery' or a 'fail-over' situation.
JOB_DATA	blob	Stores the metadata related to the job in a text field.

qrtz_fired_triggers Table

This table stores the status information about the triggers that have been issued and the relevant execution information about the corresponding job.

Column Name	Column Type	Description
ENTRY_ID	varchar(95)	Stores the unique identifier for the trigger.
TRIGGER_NAME	varchar(80)	Specifies the name of the job trigger.
TRIGGER_GROUP	varchar(80)	Specifies the name of the group that the trigger belongs to.
IS_VOLATILE	varchar(1)	Specifies if the job is volatile. A volatile job can perform different tasks such as import application data, import access and accounts. A volatile job is not persisted between program shutdowns.
INSTANCE_NAME	varchar(80)	Specifies the instance name of the job.

Column Name	Column Type	Description
FIRED_TIME	bigint(13)	Specifies the time when the job was issued.
PRIORITY	int(11)	Specifies the priority of the job.
STATE	varchar(16)	Specifies the state of the job.
JOB_NAME	varchar(80)	Specifies the name of the job.
JOB_GROUP	varchar(80)	Specifies the name of the group that the job belongs to.
IS_STATEFUL	varchar(1)	Specifies if the job is stateful. A stateful job guarantees that only one job runs at one time.

Column Name	Column Type	Description
REQUESTS_RECOVERY	varchar(1)	Specifies if the scheduler re-executes a job when it encounters a 'recovery' or a 'fail-over' situation.

Campaign Tables

Table	Description	Associated Tables
Cert_Role_Entitlements_Status	This table is mainly used in the Role Owner campaign and it holds the certification_role, and certification_entitlement_value tables key values along with the certification key, certified to log the actions taken by the end user.	Cert_Role_Entitlements
Certification	This is a directly associated table that has one to many relationships. Many	Cert_Service_Account_Status

Table	Description	Associated Tables
	certifications may be associated to a campaign. This table holds all certification attributes like certification name, certifier, start date, end date, etc.	Certification_Customer_Status Certification_Account_Entitlements_privilege_Status Certification_User_Status Certification_User_Account_Status Certification_Account_Entitlement1_Status Certification_Certifier Certification_Role_User_Account_Status Cert_Ent_Values_Status Cert_Role_Entitlements_Status Cert_Roles_Status

Table	Description	Associated Tables
		Certification_Entitlement2_Status
Campaign	This is the main parent table of the campaign module. It holds all the attributes related to the campaign such as campaign name, campaign type, start date, end date, etc.	Certification
Cert_Service_Account_Status	This table is used in the Service Account campaign and it holds the certification_account table key along with the certification key, certified to log the actions taken by the end user.	Certification_Account
Certification_Account_Entitlement1_Status	This table is mainly used in the User Manager, Service Account, and Application Owner campaigns and it holds	Certification_Account Certification_Entitlement_Value

Table	Description	Associated Tables
	the Certification_entitlement_value, and Certification_account tables key values along with the certification key, certified to log the actions taken by the end user.	
Certification_Account_Entitlements_privilege	This table is mainly used for all type of campaigns and it holds the certification_account, and certification_entitlement_value tables key values along with the attribute name and attribute values.	Certification_Account Certification_Entitlement_Value
certification_account_entitlements_privilege_Status	This table is used in the Entitlement Owner campaign and it holds the Certification_account_entitlements_Privilege table key along with the certification key, certified to log the actions taken by the end user.	Certification_Account_Entitlements_privilege

Table	Description	Associated Tables
Certification_Customer_Status	This table is used in the Organization Owner campaign and it holds the certification_customer table key along with the certification key, certified to log the actions taken by the end user.	Certification_Customer
Cert_Ent_Values_Status	This table is mainly used in the Entitlement Owner campaign and it holds the certification_entitlement_value key along with the certification key, certified to log the actions taken by the end user.	Certification_Entitlement_Value
Certification_Entitlement_Value	This table holds the entitlement value object snapshot from the parent Entitlement Value table. It holds all the Entitlement Value attributes.	Certification_Entitlement2_Status

Table	Description	Associated Tables
Cert_Roles_Status	This table is mainly used in the Role Owner campaign and it holds the certification_role key along with the ceritification key, certified to log the actions taken by the end user.	Certification_Role
Cert_Role_User_Account	This table is mainly used for all type of campaigns to hold Certification_role, Users, Accounts, and Roles tables key values.	Certification_Role
Cert_Role_Entitlements	This table holds the role entitlements object snapshot from the parent Role_entitlements table. It holds all the Role_entitlements attributes. This table also maintains the role and entitlement relationship.	Certification_Role

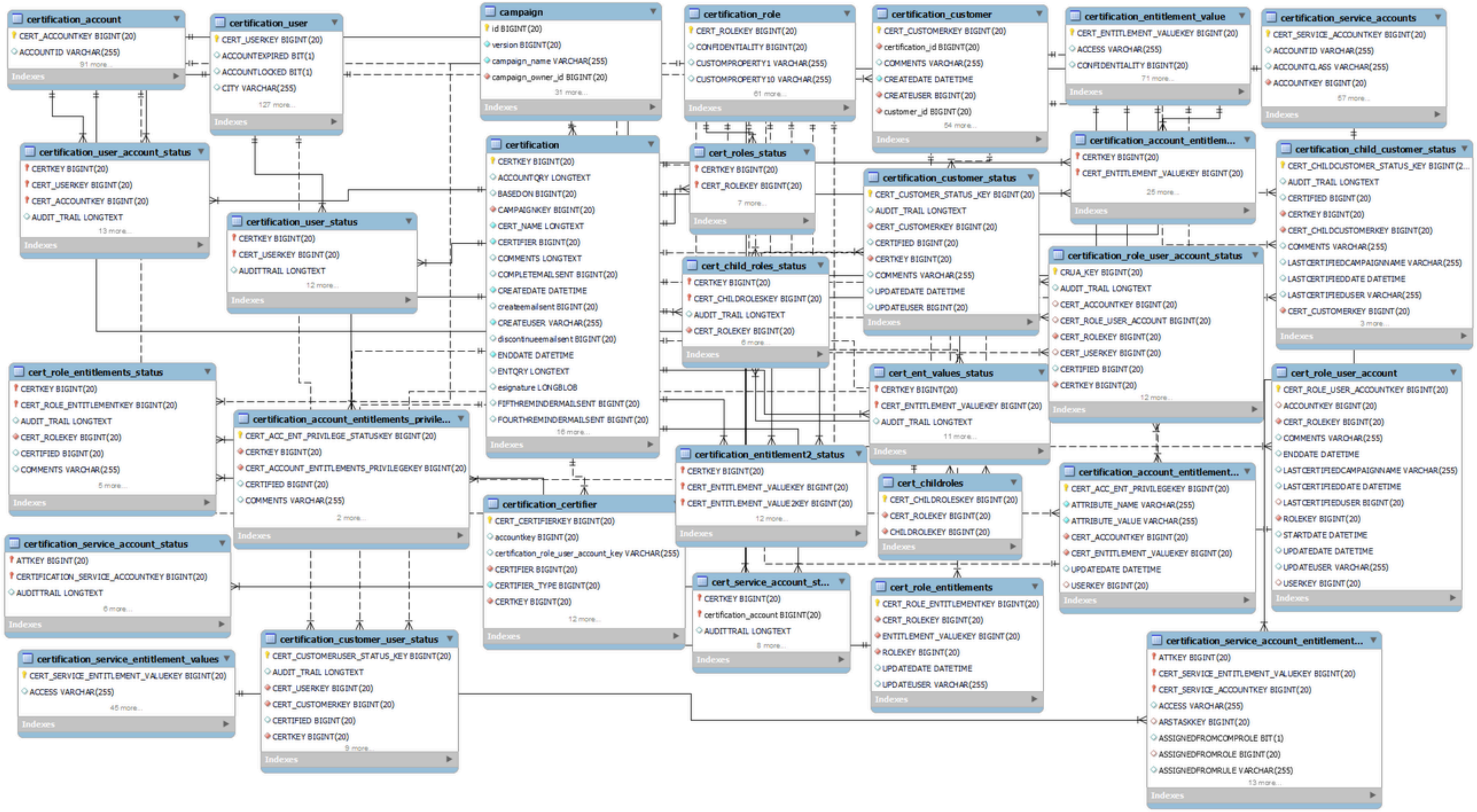
Table	Description	Associated Tables
Certification_User_Status	This table is mainly used in the User Manager campaign and it holds the certification_user table key value along with the certification key, certified to log the actions taken by the end user.	Certification_User
Certification_User_Account_Status	This table is mainly used in the User Manager, Service Account, and Application Owner campaigns and it holds the certification_user, and Certification_account tables key values along with the certification key, certified to log the actions taken by the end user.	Certification_User Certification_Account Certification_Role Cert_Role_User_Account
Certification_Certifier	This table is used when any certification item is consulted with another certifier. It holds the certifier key, cert key, cert type etc.	N/A

Table	Description	Associated Tables
Certification_Customer	This table is mainly used for all type of campaigns and it holds the customer table snapshot with all the customer domain object attributes along with the certification key.	N/A
Certification_User	This table holds the user object snapshot from the parent User table. It holds all the User attributes.	N/A
Certification_Account	This table holds the account object snapshot from the parent Account table. It holds all the Account attributes.	N/A
Certification_Entitlement2_Status	This table holds the child entitlement value with its parent entitlement valuekey along with the certkey, certified, and	N/A

Table	Description	Associated Tables
	status columns to log the actions taken by the end user.	
Certification_Role	This table holds the role object snapshot from the parent Role table. It holds all the role attributes.	N/A
Certification_Role_User_Account_Status	This table is mainly used for all* type of campaigns to holds the Certification_role, Certification_user, Certification_account, Certification_Role_user_account tables key values along with the certification key, certified to log the actions taken by the end user.	Certification_User Certification_Account Certification_Role Cert_Role_User_Account
certification_child_customer_status	This table holds the relationship between parent customer column data and child	Certification, Certification_customer

Table	Description	Associated Tables
	customer data column for particular a certification.	
certification_customer_user_status	This table holds the relationship of customer column data and user column data for a particular certification.	Certification, Certification_user, Certification_customer
campaign_template	This table holds the campaign related information in the form of template to launch a campaign any number of time effortlessly.	NA
campaign_template_history	This table holds the history of changes made in a template.	campaign_template
cert_child_roles_status	This table holds the relationship of roles column data and child roles column data	Certification, Certification_ChildRoles, Certification_role

Table	Description	Associated Tables
	of particular certification.	
cert_childroles	This table holds the relationship between parent role column data and child role column data.	Certification_role(Parent), Certification_role(Child)


certification_account
CERT_ACCOUNTKEY BIGINT(20)
ACCOUNTID VARCHAR(255)
91 more...
Indexes
certification_user
CERT_USERKEY BIGINT(20)
ACCOUNTEXPIRED BIT(1)
ACCOUNTLOCKED BIT(1)
CITY VARCHAR(255)
127 more...
Indexes
campaign
id BIGINT(20)
version BIGINT(20)
campaign_name VARCHAR(255)
campaign_owner_id BIGINT(20)
31 more...
Indexes
certification_role
CERT_ROLEKEY BIGINT(20)
CONFIDENTIALITY BIGINT(20)
CUSTOMPROPERTY1 VARCHAR(255)
CUSTOMPROPERTY10 VARCHAR(255)
61 more...
Indexes
certification_customer
CERT_CUSTOMERKEY BIGINT(20)
certification_id BIGINT(20)
COMMENTS VARCHAR(255)
CREATEDATE DATETIME
CREATEUSER BIGINT(20)
customer_id BIGINT(20)
54 more...
Indexes
certification_entitlement_value
CERT_ENTITLEMENT_VALUEKEY BIGINT(20)
ACCESS VARCHAR(255)
CONFIDENTIALITY BIGINT(20)
71 more...
Indexes
certification_service_accounts
CERT_SERVICE_ACCOUNTKEY BIGINT(20)
ACCOUNTID VARCHAR(255)
ACCOUNTCLASS VARCHAR(255)
ACCOUNTKEY BIGINT(20)
57 more...
Indexes
certification_user_account_status
CERTKEY BIGINT(20)
CERT_USERKEY BIGINT(20)
CERT_ACCOUNTKEY BIGINT(20)
AUDIT_TRAIL LONGTEXT
13 more...
Indexes
certification_user_status
CERTKEY BIGINT(20)
CERT_USERKEY BIGINT(20)
AUDITTRAIL LONGTEXT
12 more...
Indexes
certification
CERTKEY BIGINT(20)
ACCOUNTQRY LONGTEXT
BASEDON BIGINT(20)
CAMPAIGNKEY BIGINT(20)
CERT_NAME LONGTEXT
CERTIFIER BIGINT(20)
COMMENTS LONGTEXT
COMPLETEMAILSENT BIGINT(20)
CREATEDATE DATETIME
createemailsent BIGINT(20)
CREATEUSER VARCHAR(255)
discontinueemailsent BIGINT(20)
ENDDATE DATETIME
ENTQRY LONGTEXT
esignature LONGBLOB
FIFTHREMINDERMAILSENT BIGINT(20)
FOURTHREMINDERMAILSENT BIGINT(20)
16 more...
Indexes
cert_roles_status
CERTKEY BIGINT(20)
CERT_ROLEKEY BIGINT(20)
7 more...
Indexes
certification_customer_status
CERT_CUSTOMER_STATUS_KEY BIGINT(20)
AUDIT_TRAIL LONGTEXT
CERT_CUSTOMERKEY BIGINT(20)
CERTIFIED BIGINT(20)
CERTKEY BIGINT(20)
COMMENTS VARCHAR(255)
UPDATEDATE DATETIME
UPDATEUSER BIGINT(20)
Indexes
certification_account_entitlem...
CERTKEY BIGINT(20)
CERT_ENTITLEMENT_VALUEKEY BIGINT(20)
25 more...
Indexes
certification_child_customer_status
CERT_CHILDCUSTOMER_STATUS_KEY BIGINT(2...
AUDIT_TRAIL LONGTEXT
CERTIFIED BIGINT(20)
CERTKEY BIGINT(20)
CERT_CHILDCUSTOMERKEY BIGINT(20)
COMMENTS VARCHAR(255)
LASTCERTIFIEDCAMPAIGNNAME VARCHAR(255)
LASTCERTIFIEDDATE DATETIME
LASTCERTIFIEDUSER VARCHAR(255)
CERT_CUSTOMERKEY BIGINT(20)
3 more...
Indexes
cert_child_roles_status
CERTKEY BIGINT(20)
CERT_CHILDROLESKEY BIGINT(20)
AUDIT_TRAIL LONGTEXT
CERT_ROLEKEY BIGINT(20)
6 more...
Indexes
certification_role_user_account_status
CRUA_KEY BIGINT(20)
AUDIT_TRAIL LONGTEXT
CERT_ACCOUNTKEY BIGINT(20)
CERT_ROLE_USER_ACCOUNT BIGINT(20)
CERT_ROLEKEY BIGINT(20)
CERT_USERKEY BIGINT(20)
CERTIFIED BIGINT(20)
CERTKEY BIGINT(20)
12 more...
Indexes
cert_role_entitlements_status
CERTKEY BIGINT(20)
CERT_ROLE_ENTITLEMENTKEY BIGINT(20)
AUDIT_TRAIL LONGTEXT
CERT_ROLEKEY BIGINT(20)
CERTIFIED BIGINT(20)
COMMENTS VARCHAR(255)
5 more...
Indexes
certification_account_entitlements_privile...
CERT_ACC_ENT_PRIVILEGE_STATUSKEY BIGINT(20)
CERTKEY BIGINT(20)
CERT_ACCOUNT_ENTITLEMENTS_PRIVILEGEKEY BIGINT(20)
CERTIFIED BIGINT(20)
COMMENTS VARCHAR(255)
2 more...
Indexes
cert_ent_values_status
CERTKEY BIGINT(20)
CERT_ENTITLEMENT_VALUEKEY BIGINT(20)
AUDIT_TRAIL LONGTEXT
11 more...
Indexes
cert_role_user_account
CERT_ROLE_USER_ACCOUNTKEY BIGINT(20)
ACCOUNTKEY BIGINT(20)
CERT_ROLEKEY BIGINT(20)
COMMENTS VARCHAR(255)
ENDDATE DATETIME
LASTCERTIFIEDCAMPAIGNNAME VARCHAR(255)
LASTCERTIFIEDDATE DATETIME
LASTCERTIFIEDUSER BIGINT(20)
ROLEKEY BIGINT(20)
STARTDATE DATETIME
UPDATEDATE DATETIME
UPDATEUSER VARCHAR(255)
USERKEY BIGINT(20)
Indexes
certification_entitlement2_status
CERTKEY BIGINT(20)
CERT_ENTITLEMENT_VALUEKEY BIGINT(20)
CERT_ENTITLEMENT_VALUE2KEY BIGINT(20)
12 more...
Indexes
cert_childroles
CERT_CHILDROLESKEY BIGINT(20)
CERT_ROLEKEY BIGINT(20)
CHILDROLEKEY BIGINT(20)
Indexes
certification_account_entitlement...
CERT_ACC_ENT_PRIVILEGEKEY BIGINT(20)
ATTRIBUTE_NAME VARCHAR(255)
ATTRIBUTE_VALUE VARCHAR(255)
CERT_ACCOUNTKEY BIGINT(20)
CERT_ENTITLEMENT_VALUEKEY BIGINT(20)
UPDATEDATE DATETIME
USERKEY BIGINT(20)
Indexes
certification_certifier
CERT_CERTIFIERKEY BIGINT(20)
accountkey BIGINT(20)
certification_role_user_account_key VARCHAR(255)
CERTIFIER BIGINT(20)
CERTIFIER_TYPE BIGINT(20)
CERTKEY BIGINT(20)
12 more...
Indexes
certification_service_account_status
ATTKEY BIGINT(20)
CERTIFICATION_SERVICE_ACCOUNTKEY BIGINT(20)
AUDITTRAIL LONGTEXT
6 more...
Indexes
cert_service_account_st...
CERTKEY BIGINT(20)
certification_account BIGINT(20)
AUDITTRAIL LONGTEXT
8 more...
Indexes
cert_role_entitlements
CERT_ROLE_ENTITLEMENTKEY BIGINT(20)
CERT_ROLEKEY BIGINT(20)
ENTITLEMENT_VALUEKEY BIGINT(20)
ROLEKEY BIGINT(20)
UPDATEDATE DATETIME
UPDATEUSER VARCHAR(255)
Indexes
certification_service_entitlement_values
CERT_SERVICE_ENTITLEMENT_VALUEKEY BIGINT(20)
ACCESS VARCHAR(255)
45 more...
Indexes
certification_customer_user_status
CERT_CUSTOMERUSER_STATUS_KEY BIGINT(20)
AUDIT_TRAIL LONGTEXT
CERT_USERKEY BIGINT(20)
CERT_CUSTOMERKEY BIGINT(20)
CERTIFIED BIGINT(20)
CERTKEY BIGINT(20)
9 more...
Indexes
certification_service_account_entitlement...
ATTKEY BIGINT(20)
CERT_SERVICE_ENTITLEMENT_VALUEKEY BIGINT(20)
CERT_SERVICE_ACCOUNTKEY BIGINT(20)
ACCESS VARCHAR(255)
ARSTASKKEY BIGINT(20)
ASSIGNEDFROMCOMPROLE BIT(1)
ASSIGNEDFROMROLE BIGINT(20)
ASSIGNEDFROMRULE VARCHAR(255)
13 more...
Indexes

Data Mapping

ARS Request Type Mappings

Column Name	Mapping Value
Add Access	1
Remove Access / Account	2
NEW ACCOUNT	3
ROLE REQUEST	4
CREATE ROLE	5
MODIFY ROLE	6

Column Name	Mapping Value
CREATE_BADGE	7
REPLACE_BADGE	8
UPDATE_BADGE	9
REMOVE_BADGE	10
FFROLE REQUEST	11
UPDATE ACCOUNT	12
PROPOSED ACCOUNT OWNERS	15
MODIFY_ORGANIZATION	16

Column Name	Mapping Value
PROPOSED ENTITLEMENT OWNERS	17
CREATE USER	18
UPDATE USER	19
CREATE RULE	20
UPDATE RULE	21
DISABLE RULE	22
FIREFIGHTER ID	23
FIREFIGHTERID ACCESS	24

Column Name	Mapping Value
T2P	25
ENABLE RULE	26
EXTEND ACCESS	28

Ars_Requests Request Status Mappings

Column Name	Mapping Value
DRAFT	0
NEW	1
IN PROCESS	2

Column Name	Mapping Value
COMPLETED	3
EXPIRED	4
DISCONTINUED	6
ARCHIVED	7
STATUS_INPROGRESS (This status is introduced for Release v23.2 and later releases)	8
STATUS_NEEDS_MORE_INFO (This status is introduced for Release v23.2 and later releases)	9
STATUS_FAILED	10

Column Name	Mapping Value
(This status is introduced for Release v23.2 and later releases)	
STATUS_TEMP_REQUEST_DISCONTINUE (This status is introduced for Release v23.2 and later releases)	11
STATUS_READY_FOR_RETRY (This status is introduced for Release v23.2 and later releases)	12
STATUS_RETRY_IN_PROGRESS (This status is introduced for Release v23.2 and later releases)	13

Ars_Requests SOD Evaluated Status Mappings

Column Name	Mapping Value
Both internal and external SODs are not evaluated	0

Column Name	Mapping Value
Internal SOD is not evaluated and evaluation for external SOD has failed	1
Internal SOD is not evaluated __External SOD Evaluation done but no SOD found	2
Internal SOD is not evaluated __External SOD Evaluation done and SOD found	3
INTERNALSOD_EVALUATIONFAILED__EXTERNALSOD_NOTEVALUATED	4
INTERNALSOD_EVALUATIONFAILED__EXTERNALSOD_EVALUATIONFAILED	5
INTERNALSOD_EVALUATIONFAILED__EXTERNALSOD_EVA	6

Column Name	Mapping Value
LUATIONDONE_NOSODFOUND	
INTERNALSOD_EVALUATIONFAILED__EXTERNALSOD_EVALUATIONDONE_SODFOUND	7
INTERNALSOD_EVALUATIONDONE_NOSODFOUND__EXTERNALSOD_NOTEVALUATED	8
INTERNALSOD_EVALUATIONDONE_NOSODFOUND__EXTERNALSOD_EVALUATIONFAILED	9
INTERNALSOD_EVALUATIONDONE_NOSODFOUND__EXTERNALSOD_EVALUATIONDONE_NOSODFOUND	10
INTERNALSOD_EVALUATIONDONE_NOSODFOUND__EXTERNALSOD_EVALUATIONDONE_SODFOUND	11

Column Name	Mapping Value
INTERNALSOD_EVALUATIONDONE_SODFOUND__EXTERNALSOD_NOTEVALUATED	12
INTERNALSOD_EVALUATIONDONE_SODFOUND__EXTERNALSOD_EVALUATIONFAILED	13
INTERNALSOD_EVALUATIONDONE_SODFOUND__EXTERNALSOD_EVALUATIONDONE_NOSODFOUND	14
INTERNALSOD_EVALUATIONDONE_SODFOUND__EXTERNALSOD_EVALUATIONDONE_SODFOUND	15

Roletype Attribute Column Mappings

Column Name	Mapping Value
None	0

Column Name	Mapping Value
ENABLER Role	1
TRANSACTIONAL Role	2
FIREFIGHTER Role	3
ENTERPRISE Role	4
APPLICATION Role	5
ENTITLEMENT BASED ROLE	6

Request_access Access Type Column Mappings

Column Name	Mapping Value
ROLE	1
ENTITLEMENT	2
ACCOUNT	3
ORGANIZATION	4
USER	5
RULE	6
ROLE BASED ENTITLEMENT	7

Column Name	Mapping Value
Emergency ID	8
Emergency ACCESS	9
Transport	10

Request_Access Request Type Mappings

Column Name	Mapping Value
Add Access	1
Update Account	12
REMOVE access	2

Column Name	Mapping Value
UPDATE ROLE	3
REMOVE ROLE	4
PROPOSED ACCOUNT OWNERS	15
MODIFY_ORGANIZATION	16
PROPOSED Entitlement OWNERS	17
CREATE USER	18
UPDATE USER	19
CREATE RULE	20

Column Name	Mapping Value
UPDATE RULE	21
DISABLE RULE	22
MODIFY PRIVILEGE	23
Emergency Access ID	24
Emergency Access Role	25
Transport Import	26
ENABLE RULE	27
EXTEND ACCESS	28

Column Name	Mapping Value
ENABLE ACCOUNT	29
DISABLE ACCOUNT	30
LOCK ACCOUNT	31
UNLOCK ACCOUNT	32
CREATE ORGANIZATION	33
BULK USER UPLOAD	34

Request_Access Status

Column Name	Mapping Value
DEFAULT	1
Request is APPROVED	2
Request is approved and task created	3
Request is rejected	4
Request is completed	5
Request is discontinued	6
Task duration is expired	7

Column Name	Mapping Value
Task created after the revoking end date Info Available from Release v5.5 SP4 onwards.	8

Access_Approver Request Status

Column Name	Mapping Value
STATUS_ASSIGNED_BUT_NO_SHOW	-1
STATUS_NEW	1
STATUS_APPROVE	2

Column Name	Mapping Value
STATUS_REJECTED	3
STATUS_ESCLATE	4
STATUS_EXPIRE	5
STATUS_DISCONTINUE	6
STATUS_REASSIGNED	7

ArsTasks Task Type Mappings

The ARS tasks are created when specific request type approvals are completed. The following table describes the mapping between the request and the tasks.

Source Value	Mapping Value	Description
ADD	1	Task created when the user requests for new access and the request approval is completed.
REMOVE ACCESS	2	Task created when the user requests for removing access and the request approval is completed.
NEWACCOUNT	3	Task created when the user requests for a new account and the request approval is completed.
ROLE REQUEST	4	Task created when the user requests for a new role and the request approval is completed.
CHANGEPASSWORD	5	Tasks created when the user requests for

Source Value	Mapping Value	Description
		changing the account password, changing the account password for others, and changing the service account password and the request approval is completed.
ENABLE ACCOUNT	6	Tasks created when the user request for enabling the account and the request approval is completed.
PROPOSED ACCOUNT OWNERS	7	
DELETE ACCOUNT	8	Tasks created when the user request for deleting an account and the request approval is completed.
UPDATE USER	9	Tasks created when the user request for updating the user information and the

Source Value	Mapping Value	Description
		request approval is completed.
UPDATE ACCOUNT	12	Tasks created when the user request for updating the account information and the request approval is completed.
PROPOSED Entitlement OWNERS	13	
DISABLE ACCOUNT	14	Tasks created when the user request for disabling the account and the request approval is completed.
MODIFY PRIVILEGE	23	Tasks created when the user request for modifying the existing privileges and the request approval is completed.

Source Value	Mapping Value	Description
CREATE ENTITLEMENT	24	Tasks created when the user request for creating entitlement and the request approval is completed.
UPDATE ENTITLEMENT ACCESS ADD	25	
UPDATE ENTITLEMENT ACCESS ADD	26	
UPDATE ENTITLEMENT	27	Tasks created when the user request for updating the entitlement and the request approval is completed.
DELETE ENTITLEMENT	28	Tasks created when the user request for deleting an entitlement and the request approval is completed.

Source Value	Mapping Value	Description
FIREFIGHTER ID GRANT ACCESS	29	
FIREFIGHTER ID REVOKE ACCESS	30	Tasks created when the user request for revoking the firefighter access and the request approval is completed.
UPDATE ACCESS END DATE	31	Tasks created when the user request for updating the access end date and the request approval is completed.
LOCK ACCOUNT	32	Tasks created when the user request for locking the account and the request approval is completed.
UNLOCK ACCOUNT	33	Tasks created when the user request for unlocking the account and the request approval is completed.

Source Value	Mapping Value	Description
FIREFIGHTER INSTANCE GRANT ACCESS	34	
FIREFIGHTER INSTANCE REVOKE ACCESS	35	
FIREFIGHTER ACCESS ALERT	36	
CREATE ORGANIZATION	37	Tasks created when the user request for creating the organization and the request approval is completed.
UPDATE ORGANIZATION	38	Tasks created when the user requests for updating the organization and the request approval is completed.

Arstasks Status Mapping

Column Name	Mapping Value	Description
NEW	1	The tasks created for the requests whose approvals are completed.
IN PROGRESS	2	
COMPLETE	3	The tasks are successfully provisioned.
DISCONTINUED	4	The tasks are discontinued
PENDING CREATE	5	
PENDING PROVISIONING	6	
PROVISIONING FAILED	7	

Column Name	Mapping Value	Description
ERROR	8	An error has occurred from the target system while provisioning the tasks.
NO_ACTION_REQUIRED	9	The tasks require no action to complete the provision.

Arstasks Source Types

Source Value	Description
REQUEST	Tasks created as a result of approved requests.
REMOVE ACCOUNT	Tasks created based on remove account requests submitted from Access Request interface.
CERTIFICATION	Tasks created after taking certain actions during certification processes.

Source Value	Description
ZERODAY	Tasks created as a result of configured birthright provisioning rules.
PROVRULE	Tasks created based on configured technical, user update, or entitlement request rules.
SOD	Tasks created for removing conflicting access as a result of remediation of SOD violations.
ONECLICKDISABLE	Tasks created as a result of terminating users using the One-click disable option.
ANALYTICS	Tasks created based on actions taken from the merged interface of Analytics.
ANALYTICS_V1	Tasks created based on actions taken from V1 Analytics.

Source Value	Description
ANALYTICS_V2	Tasks created based on actions taken from V2 or Elasticsearch-based Analytics.
ROLES	Tasks created during assigning or deprovisioning roles from users.
FFID_GRANT	Tasks created for the addition of Emergency Access IDs.
FFID_REVOKE	Tasks created for the removal of Emergency Access IDs.
PRECEDENCE	
DEESCALATION	
UPDATE_ROLE	Tasks created during role updation. When entitlements are

Source Value	Description
	added or removed, tasks are created for existing users to adjust the access accordingly.
changeOwnPasswordFromUI	Tasks created to synchronize user passwords with user accounts when the users change their passwords from Profile menu > Change Password option.
forgotPassword	Tasks created to synchronize a user's password with the user's accounts when the user changes their own password from the Forgot Password option.
adminFunctionResetPassword	Tasks created to synchronize a user's password with the user's accounts when the user password is reset by the administrator.
changePasswordResetPassword	Tasks created when account passwords are changed or reset from the Change Password tile.

aetrustconsolidated Table

The **aetrustconsolidated table** stores trust information for access and entitlements available in the system.

Column Name	Column Type	Description
OBJECTKEY	bigint	Indicates the key representing the object in the account_entitlements1 table
TRUSTSCORE	int	Specifies the trust score, a value between 1 and 100, calculated based on trust signals
TRUSTJUSTIFICATION	varchar(2000)	Stores the justification for the trust score, explaining the rationale for its calculation
JOBID	bigint	Specifies the job ID associated with generating the trust score
DATE	datetime	Stores the date and time when the trust modeling job last ran and updated trust score details

cac_access Table

The **cac_access table** stores information used for computing access confidence.

Column Name	Column Type	Description
ID	bigint	Indicates the ID representing the object key in the aeconsolidated table
JRMRULES	varchar(255)	Specifies the recommendation confidence score, associated recommendations, and reasons
JOBID	bigint	Indicates the job ID associated with generating the recommendation confidence score

cac_role Table

The **cac_role table** stores information required for computing access confidence for roles.

Column Name	Column Type	Description
ID	bigint	Indicates the ID representing the object key in the ruatrustconsolidated table
JRMRULES	varchar(255)	Specifies the recommendation confidence score, associated recommendations, and reasons

Column Name	Column Type	Description
JOBID	bigint	Indicates the job ID associated with generating the recommendation confidence score for roles

ruatrustconsolidated Table

The **ruatrustconsolidated table** stores trust information for role-user associations.

Column Name	Column Type	Description
OBJECTKEY	bigint	Indicates the key representing the object in the role_user_account table
TRUSTSCORE	int	Specifies the trust score, a value between 1 and 100, calculated based on trust signals
TRUSTJUSTIFICATION	varchar(2000)	Stores the justification for the trust score, explaining the rationale for its calculation
JOBID	bigint	Specifies the job ID associated with generating the trust score for role-user associations

Column Name	Column Type	Description
DATE	datetime	Stores the date and time when the trust modeling job last ran and updated trust score details

Paa_uk_evk table

The following tables will be refreshed when the recommendation job is run.The paa_uk_evk table stores the outlier scores for Account Entitlements from the AE1 table.

Column Name	Column Type	Description
USERKEY	bigint	Stores the key of the users table that helps you to identify a specific user from the table. You can use this key to map the user to other tables. For instance, to obtain account details of a single user, use userkey from the users table with userkey from the user_account table, and use the join query using accountkey from the user_account table with accountkey

Column Name	Column Type	Description
		(PK) from the accounts table.
ENTITLEMENT_VALUEKEY	bigint	Indicates the entitlement name of the entitlement available for the account.
ENTITLEMENTTYPEKEY	bigint	Helps to identify the specific entitlement type associated with an endpoint.
ACCENTKEY	bigint	This key helps you identify a specific account and entitlement association.
LIKELY_APPROVAL	bigint	The value of the field will be either null or 1.
AEOUTLIERKEY (PK)	bigint	This primary key field gets auto-incrementally updated with the number of

Column Name	Column Type	Description
		records.
SCORE	Float	Indicates the organization's risk score. This field is managed by Saviynt Identity Cloud.
JUSTIFICATION	mediumtext	Justification fields help you to understand the reason for the outlier score.

Paa_uk_rk table

The paa_uk_rk table stores the outlier scores for Role User Account entries from the RUA table.

Column Name	Column Type	Description
USERKEY	bigint	Stores the key of the users table that helps you to identify a specific user from

Column Name	Column Type	Description
		the table. You can use this key to map the user to other tables. For instance, to obtain account details of a single user, use userkey from the users table with userkey from the user_account table and, use the join query using accountkey from the user_account table with accountkey (PK) from the accounts table.
ROLEKEY	bigint	Indicates the SAV role key.
ROLETYPEY	bigint	Indicates the role type.
RUAKEY	bigint	This is the key that helps you identify a specific account and entitlement association.

Column Name	Column Type	Description
RUAOUTLIERKEY(PK)	bigint	This is the primary key that gets auto-incrementally updated with the number of records.
SCORE	Float	Indicates the organization's risk score. This field is managed by Saviynt Identity Cloud.
JUSTIFICATION	mediumtext	Justification fields help you to understand the reason for the outlier score.