Internship In Support Operations

Project report submitted in partial fulfillment of the requirement for the degree of Bachelor of Technology
in
Computer Science and Engineering/Information Technology
By
Dev Kumar (181326)

Under the supervision of

Dr. Monika Bharti

to

Department of Computer Science & Engineering and Information Technology **Jaypee University of Information Technology Waknaghat, Solan-173234, Himachal Pradesh**

Candidate's Declaration

I hereby declare that the work presented in this report entitled **"Internship in Support Operations"** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology**,** Jaypee University of Information Technology Waknaghat is an authentic record of my own work carried out over a period from February 2022 to May 2022 under the supervision of Dr. Monika Bharti (Assistant Professor(Senior Grad) and Computer Science and Engineering & Information Technology).

The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Dev Kumar
181326

This is to certify that the above statement made by the candidate is true to the best of my knowledge.

(College Supervisor Signature)
Dr. Monika Bharti
Assistant Professor (SG)
Computer Science and Engineering & Information Technology
Dated:

ACKNOWLEDGEMENT

I would like to thank and express my gratitude to the project supervisor Dr. Monika Bharti for her constant support and guidance. This project would not have been possible without her help. I would always like to give a big thanks to my mentors in Saviynt who help me in each and every step of this wonderful learning experience. This internship taught me many new things and each concept was very interesting. I would also like to express my thanks to the lab assistant for contacting me and helping me in finishing the project within the stipulated time period.

Last, I would like to thank my friends and family for their support and love.

Dev Kumar
181326

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

● HTTP	HyperText Transfer Protocol
● URL	Uniform Resource Locator
● URI	Uniform Resource Identifier
● SSL	Secure Sockets Layer
● CA	Certificate Authority
● SOAP	Simple Object Access Protocol
● RESTful	Representational State Transfer
● WSDL	Web Services Description Language
● Hmac	Hash-based message authentication code
● IKE	Internet Key Exchange

LIST OF FIGURES

ABSTRACT

Saviynt enables enterprises to secure application data, and infrastructure in a single platform for Cloud (Office 365, AWS, Salesforce, Workday) and Enterprise (SAP, Oracle EBS). Saviynt is pioneering IGA 3.0 by integrating advanced risk analytics and intelligence with fine-grained privilege management.

Saviynt provides up with various services to a large number of clients in IT industry they also have tie with one of the fastest growing companies. Work culture is just as professional as expected.

At Internship program in Saviynt, we are divided into certain domains, each domain has specific amount of training period of 12 weeks. Internship includes various events such as educational workshops, webinars, live courses, and work assignments.

Fig 1: Saviynt Logo

CHAPTER - 1
INTRODUCTION

1.1 INTRODUCTION

After the end of 7th semester, various company visited to our college for the placement of the student, one such company was Saviynt, due to my good fortune, I was selected for Intern profile, after selection, I was offered internship program by the Saviynt before the full time role and completing internship is necessary for the full time role in the Saviynt. The internship was of 3 months containing various sessions, webinar, online Live courses, assessment and project.

Saviynt enables enterprises to secure application data, and infrastructure in a single platform for Cloud (Office 365, AWS, Salesforce, Workday) and Enterprise (SAP, Oracle EBS). Saviynt is pioneering IGA 3.0 by integrating advanced risk analytics and intelligence with fine-grained privilege management.

Saviynt can import Access and Usage data from applications in real time or batch basis, analyze the data against industry leading controls, provide exceptions / violations and remediate exceptions. In addition, Saviynt provides the ability to Mine / Design Functional Roles and Attribute Based Rules based on user data, attributes, and usage. These roles can be provisioned back in the application where applicable and can be monitored in real time for violations.

If you take a look at online resources, for example, AWS, Google Cloud, and Azure have different definitions for users, roles, groups, and attributes. Once you start connecting collaboration tools such as Box or O365, you add another layer of user, role, group, and attribute definitions. Moreover, as users move throughout your organization, their roles and access needs change. In short, IT infrastructures are dynamic. Applications are dynamic. Users are dynamic. Creating an effective IAM policy and maintaining compliance with it requires a flexible and dynamic approach to defining users, resources, and access.

What is an Identity and Access Management Policy?

An Identity and Access Management Policy defines access controls inside your IT infrastructure. Unlike different written documentation like cyber security policy, associate IAM policy needs you to align specific business must technical identity and access definition making a good IAM policy ensures that the proper users have the proper access to the proper resources at the proper time and for the proper reason.

1.2 PROBLEM STATEMENT

Security leaders must reckon with the modern risk landscape, accelerating Zero Trust demands, competing transformation initiatives, coordinated cyber attacks, and unique access issues with the rise of machine identities. No roadmap through these exists, but consider the trend insights and guidance in this report an ideal starting point.

Take a “lifecycle management” approach to every identity: Apply intelligence and analytics to discover identities and consolidate them within a governance framework.

The problem several organizations face is that they began increasing their infrastructures before making a cohesive approach to IAM. As such, they need inconsistent identity knowledge. Moreover, as users and identities modify roles inside the organization, the proliferation of identities makes managing joiner/mover/leaver provisioning and deprovisioning a burden. Thus, several of those “orphaned accounts” stay active, which ends up in a security risk as a result of they typically stay unmonitored and forgotten.

1.3 OBJECTIVE

Moving to Zero Trust brings significant and tangible benefits, including the most obvious one: a stronger cyber security posture for the entire organization. Zero Trust adoption can also simplify and streamline security operations, enhance defenders' visibility of the entire attack surface, and reduce the risk posed by insider threats — all while enabling users to have the right access to the right resources at the right time.

However, embracing Zero Trust is neither simple nor effortless. The process involves a learning curve, and despite what cyber security vendors may want you to believe, Zero Trust isn't a technology that you can just buy. Instead, you'll need to redefine your organization's entire approach to identity and security. You'll need to move from a mindset of implicit trust to an approach that involves the continuous re-evaluation of risk and a shift in focus — away from the network perimeter security layer and towards the identity security layer.

Saviynt's Gartner-recognized Identity Governance and Administration (IGA) platform uses intelligent peer and usage-based analytics that alter organizations to make comprehensive, cross-application and cloud-platform IAM policies. Our Cloud PAM provides a period of time detection and monitoring to facilitate discovery and correct risky workloads, instances, containers, and alternative code-based identities.

- Building out a Zero Trust Identity strategy.
- Designing a new identity-based architecture.
- Shifting organizational cultures and mindsets.

1.4 METHODLOGY

- Authoritative HRMS – The HR data for its employees and contractors is currently stored in a file. This information will have to be imported into Saviynt for creation of user records.
- Active Directory – Internal LDAP. Only accounts and entitlements will be imported (AD groups) here and linked to imported user records.
- Generic Applications – Only accounts and entitlements (privileges) will be imported from here and linked to imported user records (from HRMS). This application is an ERP solution and financially significant from SOX perspective. This application will be configured as a Disconnected Application from fulfilment (provisioning) perspective.
- Oracle EBS – This is another financially critical application for which Segregation of Duties (SOD) policies need to be modelled.
- Entitlement Management – The entitlement repository would be enriched for glossary and metadata for one or more entitlements. Additional meta data may include catalogue search tags, risk level assessments (possible values High, Medium, Low), and Compliance objectives (possible values SOX, PCI-DSS, HIPPA). This enrichment could be automated through a csv. file upload or could be manually executed by application or entitlement owners.
- SAV Roles - SAV Roles are defined by Saviynt and are automatically available in Saviynt Security Manager (SSM). They are defined the privileges granted to users, such as, accessibility and functional limit on an application. Each SAV Role allows specific usage of the application and imposes certain restrictions.
- Access Request System - Access Request System (ARS) is used to manage access management process, access request, and approvals. An intuitive user interface that is seamless across web and mobile (iOS and Android), giving end users complete flexibility in managing their requests, checking status, setting up delegation of authority, managing access certifications, etc. Workflows involve orchestrating tasks to enable functions, such as access approvals, notifications, escalations, and integration with other business processes. Most often, this allows managers or resource owners to approve or deny requests.

- Identities - Identities have their lifecycle of getting onboarded, updated, and terminated as part of an enterprise ecosystem driven by users joining, getting promoted, transferred, and leaving. Saviynt provides different types of rules to automatically assign, or revoke access based on different conditions.
- Segregation of Duties - Segregation of Duties (SOD) is a fundamental building block to manage risks related to internal fraud or error by requiring different people to perform different tasks to complete a business process.
    - SOD – Preventive Analysis - Preventive Analysis emphasises on proactive controls to ensure risks that are defined within the ruleset are not violated or are mitigated while requesting access via Saviynt.
    - SOD – Detective Analysis - Detective Analysis is designed in Saviynt to identify conflicts or violations after they have occurred and weighed against predefined rulesets. Users with pre-existing access to applications that are later defined as ruleset violations are identified and classified as Detective SOD evaluations.
- Access certification - Access certification has been introduced to reduce rubber stamping of certification, identify the risky assets in your identity application, perform certification review for risky or high-risk entitlement and user assets. Access certifications maximizes compliance adherence and ensures security. Access certification can either be scheduled or can be configured on events when triggered.
- Campaign - A campaign is a new approach designed by Saviynt as part of certification. Through a campaign, certification reviews can be launched for a selected set of certifiers. Campaigns can be used to group and launch certifications based on organizational requirements.
- Identity Analytics - Identity Analytics is the discipline that applies logic and science to identity and access data to provide insights for making better IAM decisions. Identity Analytics tools employ features that move organizations towards a contextual, dynamic, risk-based approach to IAM. With identity Analytics, the organization can bridge the gap between administrative

controls and runtime activities, detect and remediate malicious behavior, and make more informed access-policy decisions.

- Group Management - Group Management is an important part of the overall identity management system of an enterprise. It is applied by grouping users based on common or shared characteristics. Groups can contain users from a single organization, multiple organizations, or be independent of an organization. Most applications support groups either at the application level or within the application to specific resources. Permissions associated with user groups can be modified to create additional user groups using Saviynt.
- Role - Role is a collection of entitlements. A Role enables the users have entitlements; thus, lessening the tedious task of manually assigning entitlements to users. A Role is created with applicable entitlements and users are assigned these roles to perform their day-to-day tasks in an application. Roles can also be created based on scenarios and can be merged if required with any suitable roles already available in the application.
- Role-Based Access Control - Role-Based Access Control (RBAC) is an access control method that assigns permissions to end-users based on their role within an organization. RBAC provides fine-grained control, offering a simple, manageable approach to access management that is less error-prone than individually assigning permissions. This can reduce cyber security risk, protect sensitive data, and ensure employees can only access information, and perform actions they need as per their job requirements. This is known as the principle of least privilege. Because of this, RBAC is popular in large organizations that need to grant access to hundreds or even thousands of employees based on their roles and responsibilities. It is increasingly popular among smaller organizations as it is often easier to manage than access control lists.
- Role Mining - Role Mining is the process of analyzing user-to-resource mapping data, to determine or modify user permissions for Role-Based Access Control in an enterprise. In a business setting, Roles are defined according to job competency, authority, and responsibility. The ultimate intent of Role Mining is to achieve optimal security administration based on the role each individual has within an organization.

- Service Account - Service Account is an account in an application with privileged responsibilities and is provided for a temporary period to the users. Further, a Service Account has access to critical Accounts, Entitlements, and Roles. Every service account in Saviynt has at least one owner who has permission to manage the account. A Service Account Owner can perform different actions on existing service accounts owned by him. However, for creating service accounts, one does not need to be the owner of any existing service accounts. If an end user has access to the Manage Service Account tile, he can create new service accounts.

1.5 ORGANIZATION

1.5.1 ABOUT

CLOUD ACCELERATION

Next generation cloud architecture provides fast setup, easier upgrades, and agile cloud security delivered in a modern, no-code experience to drive adoption.

ACTIONABLE INTELLIGENCE

Work smarter with real-time insights and automated workflows generated from diverse risk and activity data collected in the Saviynt cloud.

PLATFORM POWER

A centralized identity cloud breaks down isolated security apps and provides a unified experience, even as new integrations and capabilities get added.

1.5.2 VISION & MISSION

To secure the digital frontier's safety with disruptive identity technologies, creating innovative, intelligent solutions that equip organizations with smarter security to protect today's identity and prepare them for tomorrow's digital transformation.

CHAPTER - 2

SYSTEM DEVELOPMENT

2.1 Different Process

2.1.1 How to obtain an SSL Certificate?

SSL certificates can be obtained directly from a Certificate Authority (CA).The cost of an SSL certificate can range from free to hundreds of dollars, depending on the level of security you require. Once you decide on the type of certificate you require, you can then look for Certificate Issuers, which offer SSLs at the level you require.

● Prepare by getting your server set up and ensuring your WHOIS record is updated and matches what you are submitting to the Certificate Authority (it needs to show the correct company name and address, etc.)

● Generating a Certificate Signing Request (CSR) on your server. This is an action your hosting company can assist with.

● Submitting this to the Certificate Authority to validate your domain and company details

● Installing the certificate they provide once the process is complete. Once obtained, you need to configure the certificate on your web host or on your own servers if you host the website yourself.

2.1.2 Handshaking

1. A browser sends a request to a secure server.

2. The server sends its SSL certificate which includes the public key and the other data about the server’s identity.

3. The browser confirms the SSL Certificate is valid. The simplest way to do so is by looking

at the expiration date.

4. The browser encrypts a very long password using a public key and sends it to the server.

5. The server decrypts the data using its private key and retrieves the password.

The server and the browser both possess the same password. Now, they use the shared password to encrypt all future communications with symmetric-key cryptography. We switch to symmetric so that we can take advantage of both the algorithms and can have private and efficient communication.

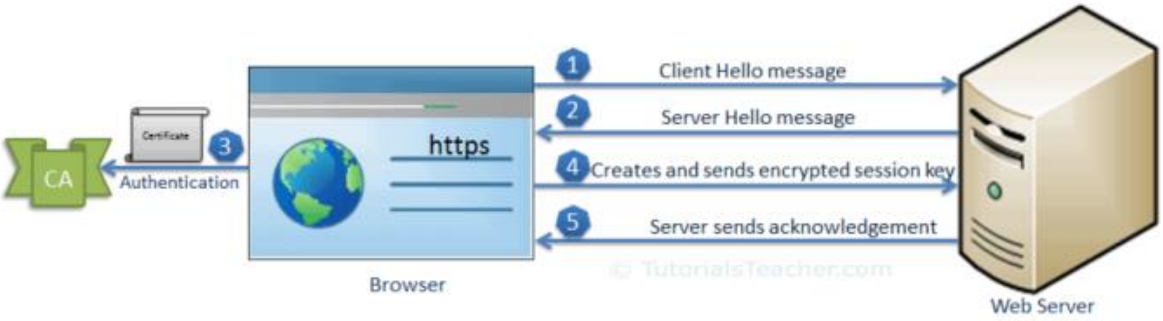


Fig 2: SSL Handshake

2.1.3 HTTP Flow

1. The browser opens a TCP connection to the server. This ensures that the data can be sent back and forth over the network and the data sent from one end is put together the same way at the other end. If the connection happened over HTTPs, TLS Certificates are sent to ensure only the computer and the server can encrypt and decrypt the data, thus preventing it from stealing while transmitting.

2. The browser sends HTTP messages. It contains a method and an address pointing to the resource. IT can also contain header like cookie etc.

3. Server performs the requested action and sends back the response. This response has an

HTTP status message, header about the response and other information. This data can be HTML documents, CSS etc.

4. TCP connection is closed.

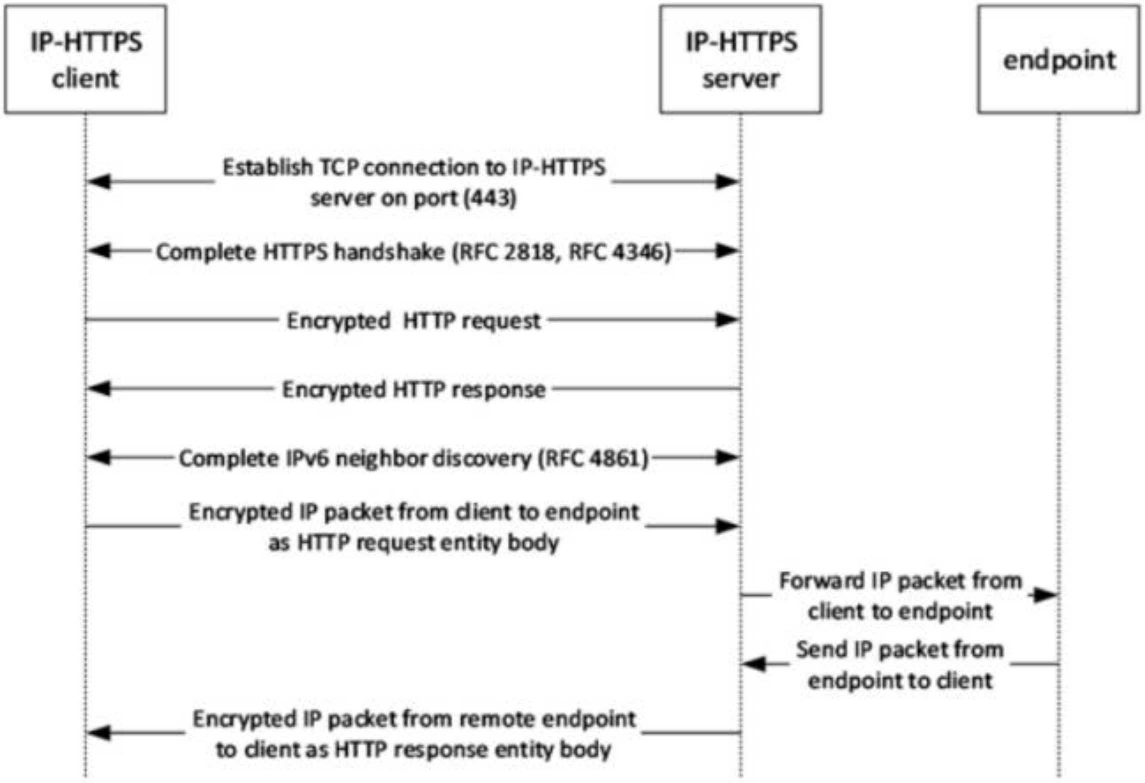

IP-HTTPS client
IP-HTTPS server
endpoint
Establish TCP connection to IP-HTTPS server on port (443)
Complete HTTPS handshake (RFC 2818, RFC 4346)
Encrypted HTTP request
Encrypted HTTP response
Complete IPv6 neighbor discovery (RFC 4861)
Encrypted IP packet from client to endpoint as HTTP request entity body
Forward IP packet from client to endpoint
Send IP packet from endpoint to client
Encrypted IP packet from remote endpoint to client as HTTP response entity body

Fig 3: HTTP Flow

2.2 Softwares Used:

2.2.1 Openvpn

VPN stands for virtual private network. Openvpn is a software which executes some techniques in the backend to create secure point to point connection in routed or bridged configurations and remote access facilities. This software provides the standard norm of authentication like pre-shared secret keys, username/password and certificates. When there are multiple clients for a single server, it provides certificates to each client for authentication by having a certificate authority and signatures. It has many security as well as control features. It uses OpenSSL library and TLS protocol.

2.2.1.1 Architecture

1. Encryption

OpenSSL is used for providing encryption to both the data and the control channels. For adding an additional layer of security to the connection, it uses the HMAC packet authentication.

2. Authentication

As stated earlier, this software uses the standards measures used by several other servers and browsers for providing authentication. Pre-shared keys are one of the easiest methods and certificates are robust and feature-rich. In the new versions, we can also use the username/password method for authentication with or without certificates.

3. Networking

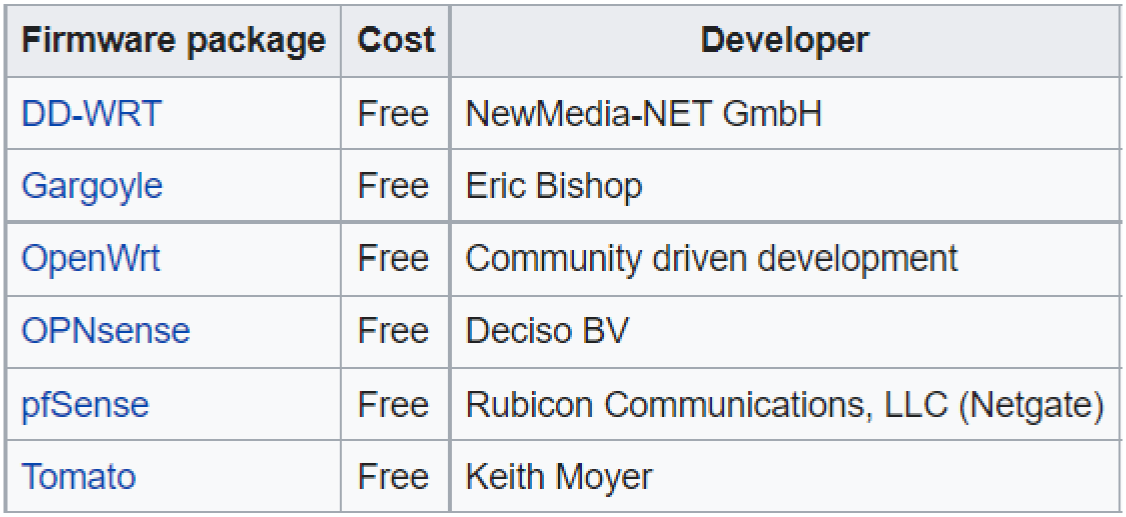
It uses both UDP and TCP for the successful creation of SSL tunnels on a single TCP/UDP port. Now, Openvpn supports the complete package of IPv6 as protocols. It can even use it for establishing connections. These new protocols help in getting through the proxy servers and getting out of firewalls. In the Openvpn server configuration, we can even push certain network configuration options to the clients. It offers two types of interfaces. They are: layer-3 based IP tunnel and layer-2 based Ethernet TAP.

4. Security

With the help of OpenSSL, it achieves upto 256-bit encryption. Furthermore, instead of using an IP stack for running, it uses userspace. It does not provide support for IKE, IPsec, or PPTP but use SSL and TLS based custom security protocols.

5. Extensibility

Third-party plugins or scripts can be used for the extension of Openvpn so that the software can be used with more advanced logging, enhanced authentication, dynamic firewall updates and RADIUS integration and so on.



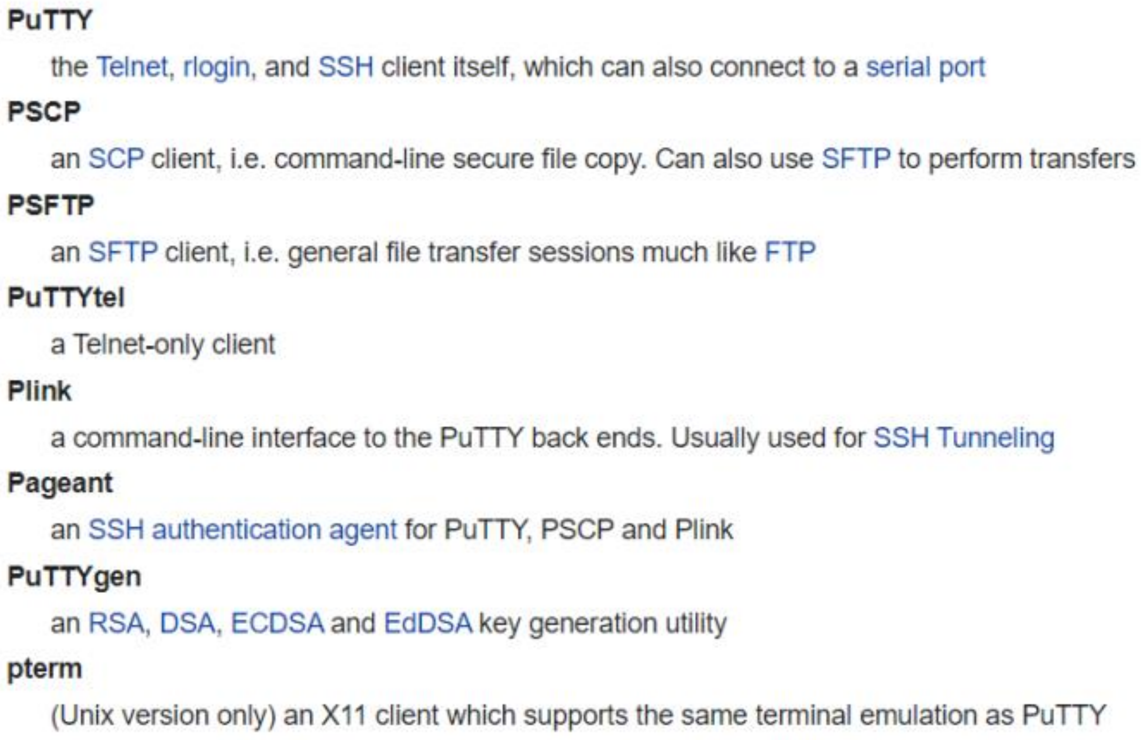
Firmware package	Cost	Developer
DD-WRT	Free	NewMedia-NET GmbH
Gargoyle	Free	Eric Bishop
OpenWrt	Free	Community driven development
OPNsense	Free	Deciso BV
pfSense	Free	Rubicon Communications, LLC (Netgate)
Tomato	Free	Keith Moyer

Fig 4: Notable firmware packages with Openvpn Integrations

2.2.2 PuTTY

It may sound like the word PuTTY has a full form or any official meaning but in reality, none are present. It is an free and open source terminal emulator which helps in file transmission over a network. It supports various protocols. It was originally written for Microsoft Windows.

Now, it can be used for different operating systems. This software was developed by Simon Tatham who is a british programmer and is looking after it.



PuTTY

the Telnet, rlogin, and SSH client itself, which can also connect to a serial port

PSCP

an SCP client, i.e. command-line secure file copy. Can also use SFTP to perform transfers

PSFTP

an SFTP client, i.e. general file transfer sessions much like FTP

PuTTYtel

a Telnet-only client

Plink

a command-line interface to the PuTTY back ends. Usually used for SSH Tunneling

Pageant

an SSH authentication agent for PuTTY, PSCP and Plink

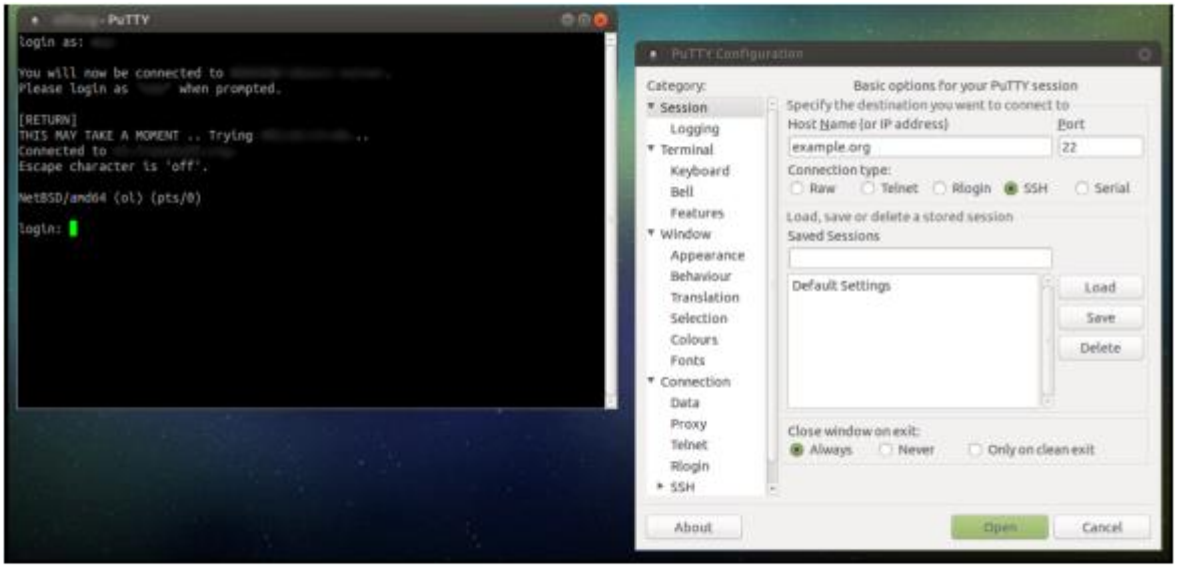
PuTTYgen

an RSA, DSA, ECDSA and EdDSA key generation utility

pterm

(Unix version only) an X11 client which supports the same terminal emulation as PuTTY

Fig 5: Components of PuTTY



```
login as: [redacted]

You will now be connected to [redacted].
Please login as [redacted] when prompted.

[RETURN]
THIS MAY TAKE A MOMENT .. Trying [redacted] ..
Connected to [redacted]
Escape character is 'off'.

NetBSD/amd64 (ol) (pts/0)

login: 
```

PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): example.org

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ● Always ○ Never ○ Only on clean exit

Fig 6: PuTTY running in Ubuntu

2.2.3 AWS Console

It is a browser based GUI which can be used for controlling features provided by amazon web services. The users can use the drag/ drop for the service links required. Users can also view resources and applications that are sharing common tags. They can use tag editors to view and make quick changes to all the resources and applications sharing common tags. It supports almost all the operating systems.

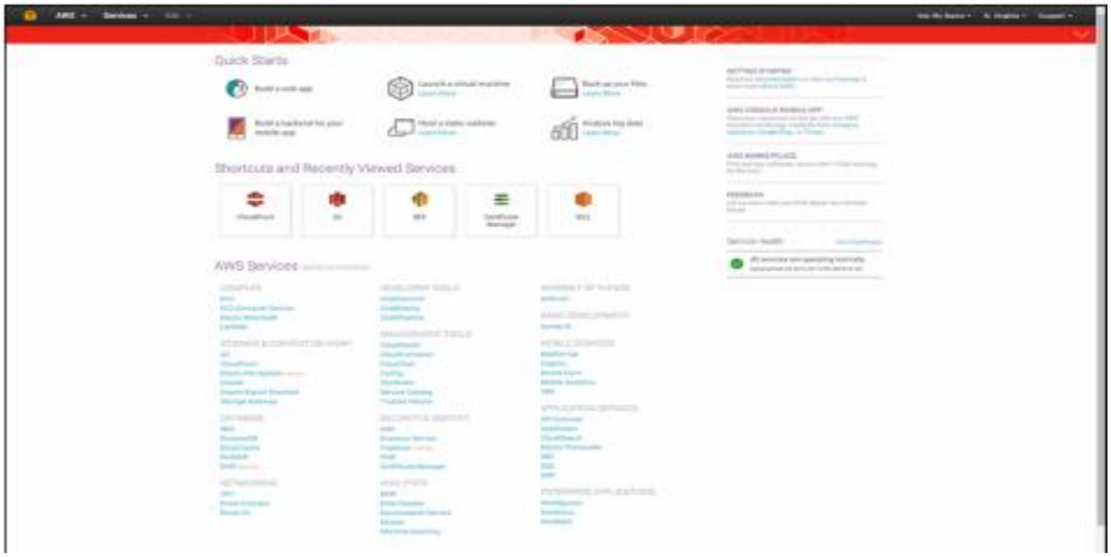


Fig 7: AWS Console Interface

2.2.4 Jumpbox

It is a system that is used to access and manage devices in a separate security zone on a network. It monitors the service that spans the two dissimilar security zones and provides a controlled means of access between them.

2.2.5 Azure

It is also known as Microsoft azure. It provides cloud computing services which are managed by microsoft data centers. It gives software as a service(SaaS), platform as a service(PaaS) and infrastructure as a service(IaaS). It supports various programming languages, tools and frameworks.

2.2.6 Amazon Web Services

They provide different cloud computing services and it is a subsidiary of amazon. These cloud computing internet offerings offer dispensed computing processing ability and software program equipment thru AWS server farms. One of those offerings is Amazon Elastic Compute Cloud (EC2), which lets in customers to have at their disposal a digital cluster of computer systems, to be had all of the time, thru the Internet. AWS's digital computer systems emulate maximum of the attributes of an actual computer, along with hardware significant processing units (CPUs) and photographs processing units (GPUs) for processing; local/RAM memory. AWS offerings are added to clients through a community of AWS server farms positioned throughout the world. Fees are primarily based totally on a mixture of utilization (referred to as a "Pay-as-you-go" model), hardware, running system, software program, or networking functions selected with the aid of using the subscriber required availability, redundancy, safety, and provider options. Subscribers pay for a digital AWS computer, a devoted bodily computer, or clusters of either. Amazon presents pick out quantities of safety for subscribers (e.g. bodily safety of the statistics centers) even as different factors of safety are the duty of the subscriber (e.g. account management, vulnerability scanning, patching). AWS operates from many worldwide geographical areas along with 6 in North America.

2.2.7 Freshdesk

It is an American cloud based customer engagement company.

Features:

1. Support channels: It has different channels like chat, email, phone, twitter and facebook etc.

2. Productivity hacks:

● Tags: It helps in categorizing the tickets.

● Dispatch: Rules can be created for tickets and workflows automation can be done for support.

● Automatic email notification: Agents and customers are sent an email when changes are made.

● Canned responses: Templates can be created and saved for reusing while replying to a customer.

● Customizable help desk.

3. Helpdesk management:

● Notes: Public notes can be added for informing customers and private notes can be added to inform fellow team members.

● Ticket Activities: Changes made in the ticket can be viewed in the history for that day.

● Team Inbox: Shared inbox is present for the team members.

● Merge Tickets: Tickets from different channels can be merged in chronological order.

● To-dos: Add a task in the ticket or in the dashboard. Prioritize your work.

● Freshconnect collaboration: Connect with other team members within the freshdesk.

4. Self- Service:

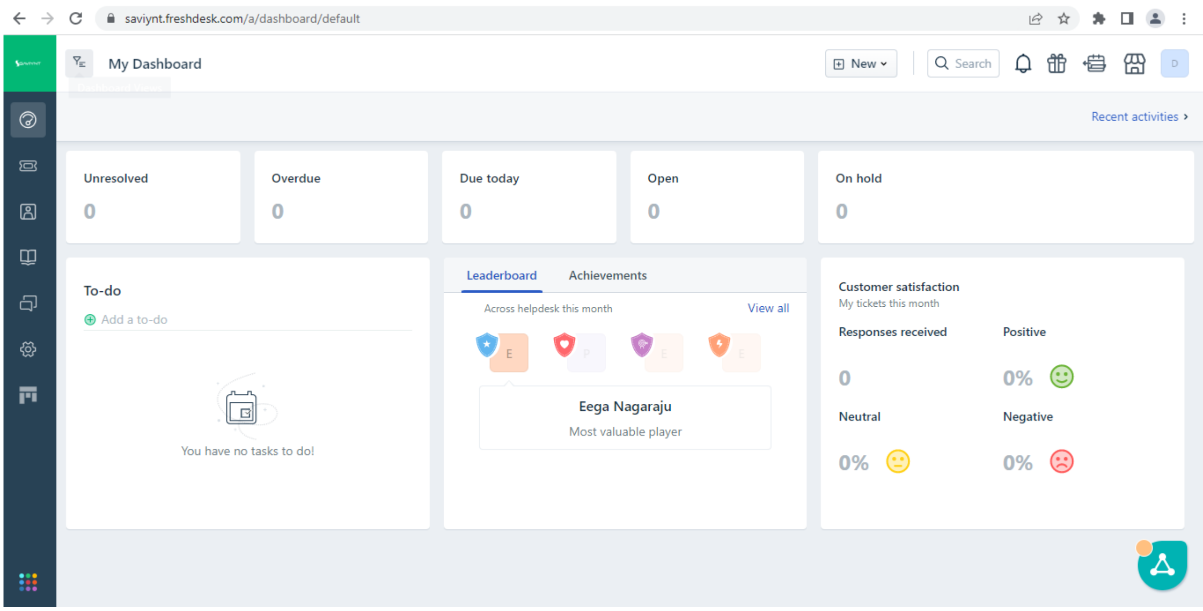
- Knowledge Base: Knowledge pages can be created to share important information with customers.

- Email to knowledge base.

5. Reporting:

- Default Dashboard: We can view trends in the tickets, recent activities, forums etc.

- Freshdesk analytics (beta): View performances of agent, ticket lifecycle, group performance etc.



Unresolved 0

Overdue 0

Due today 0

Open 0

On hold 0

To-do

Add a to-do

You have no tasks to do!

Across helpdesk this month

Eega Nagaraju

Most valuable player

Customer satisfaction

My tickets this month

Responses received 0

Positive 0%

Neutral 0%

Negative 0%

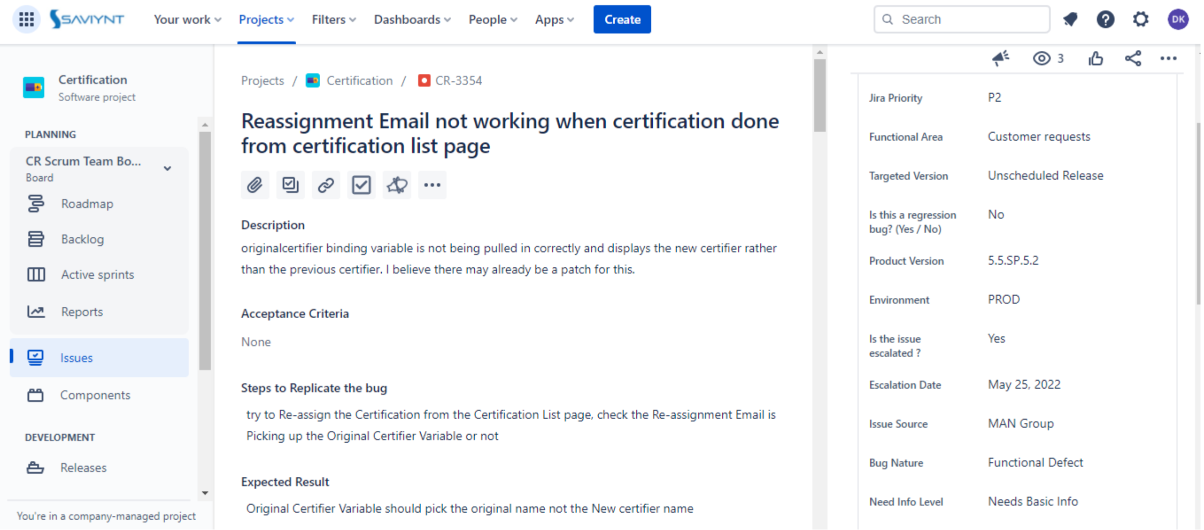
Fig 8: FreshDesk Dashboard

2.2.8 Jira

This software was developed by Atlassian which tracks issues and allows agile project management.

Jira is offered in four packages:

1. Jira Work Management: A generic project management.
2. Jira software: It is the base software which includes agile project management.
3. Jira Service Management: It is used for IT operations and business service desks.
4. Jira Align: It is strategic product and portfolio management.



Reassignment Email not working when certification done from certification list page

Description

originalcertifier binding variable is not being pulled in correctly and displays the new certifier rather than the previous certifier. I believe there may already be a patch for this.

Acceptance Criteria

None

Steps to Replicate the bug

try to Re-assign the Certification from the Certification List page, check the Re-assignment Email is Picking up the Original Certifier Variable or not

Expected Result

Original Certifier Variable should pick the original name not the New certifier name

Jira Priority	P2
Functional Area	Customer requests
Targeted Version	Unscheduled Release
Is this a regression bug? (Yes / No)	No
Product Version	5.5.SP.5.2
Environment	PROD
Is the issue escalated ?	Yes
Escalation Date	May 25, 2022
Issue Source	MAN Group
Bug Nature	Functional Defect
Need Info Level	Needs Basic Info

Fig 9: JIRA Project

CHAPTER - 3

TASK ASSIGNED DETAILS

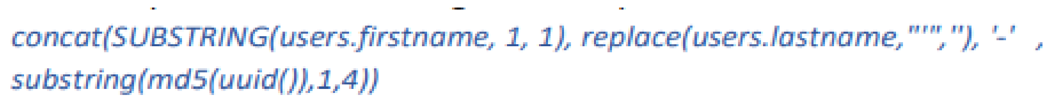
3.1 BUILDING IDENTITY WAREHOUSE

Import User Records from Authoritative Applications (HRMS)

- Users from a third-party application can be added to SSM in many ways.

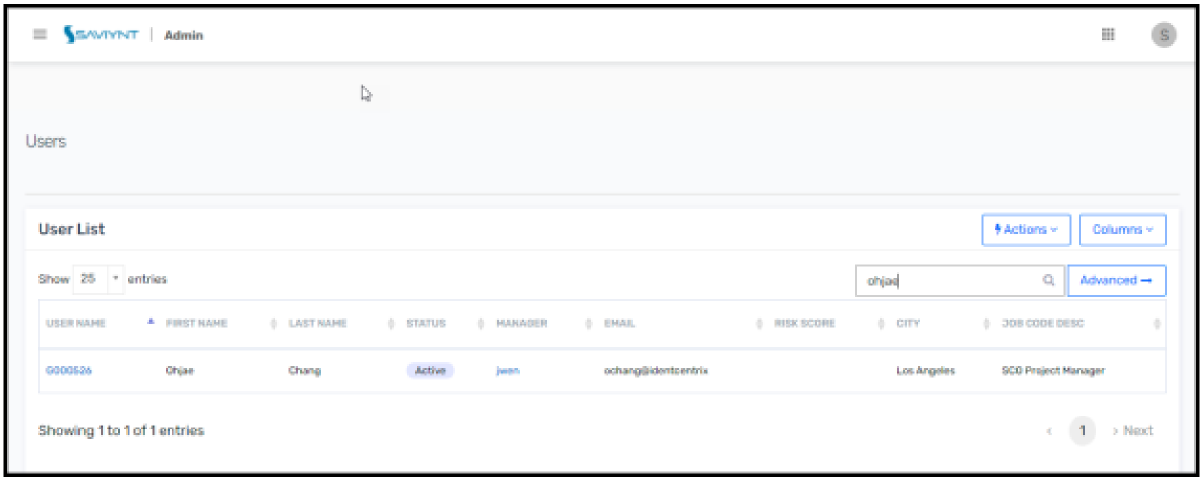
- Users are always reconciled from an authoritative source of an application.

- Users can be imported using Full Import or Incremental Import features in SSM. Examples of Authoritative Applications are: Oracle EBS, Lawson, PeopleSoft, etc.



```
concat(SUBSTRING(users.firstname, 1, 1), replace(users.lastname,"'",''), '-'  ,
substring(md5(uuid()),1,4))
```

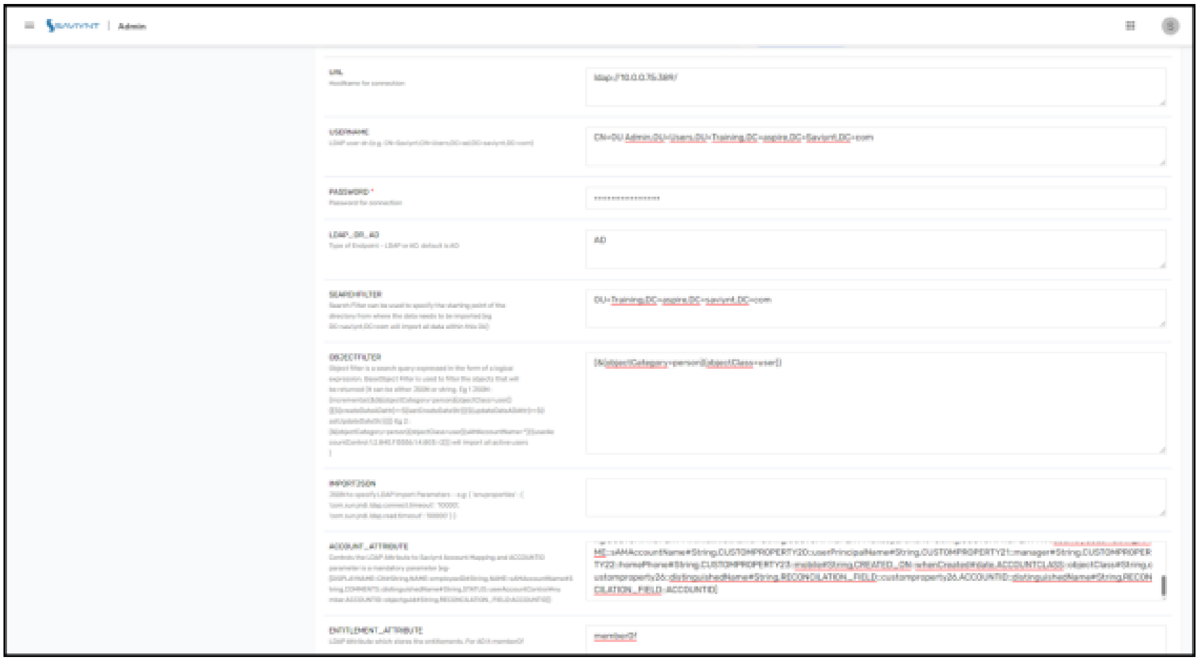
Fig 10: System Username Generation Rule



USER NAME	FIRST NAME	LAST NAME	STATUS	MANAGER	EMAIL	RISK SCORE	CITY	JOB CODE DESC
G000526	Ohjae	Chang	Active	jwen	ochang@identcentrix		Los Angeles	SCO Project Manager

Showing 1 to 1 of 1 entries

Fig 11: Validate Creation of Users



URL
Hostname for connection
ldap://10.0.0.75:389/

USERNAME
LDAP user dn (e.g. CN=Saviynt,CN=Users,DC=ad,DC=saviynt,DC=com)
CN=OU Admin,OU=Users,OU=Training,DC=aspire,DC=Saviynt,DC=com

PASSWORD *
Password for connection
****

LDAP_OR_AD
Type of Endpoint - LDAP or AD, default is AD
AD

SEARCHFILTER
Search Filter can be used to specify the starting point of the directory from where the data needs to be imported (eg DC=saviynt,DC=com will import all data within this DC)
OU=Training,DC=aspire,DC=saviynt,DC=com

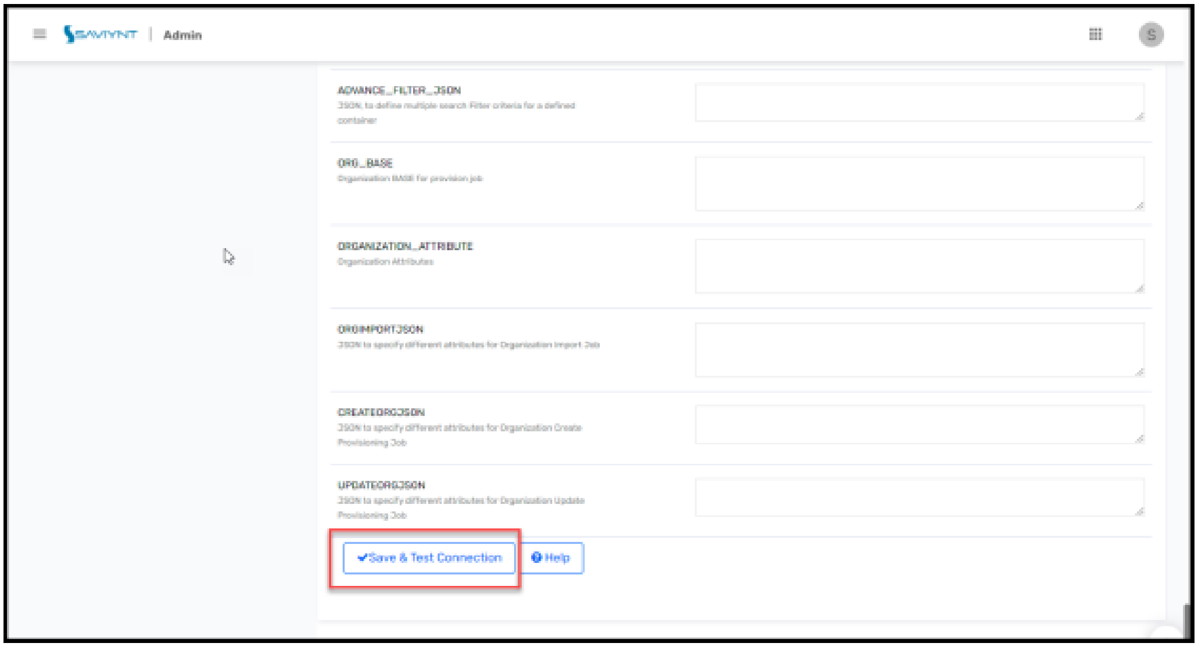
OBJECTFILTER
Object filter is a search query expressed in the form of a logical expression. BaseObject Filter is used to filter the objects that will be returned (It can be either JSON or string. Eg 1 JSON: {incremental:(&(objectCategory=person)(objectClass=user)(|(${createDateAttr}>=${setCreateDateStr})(${updateDateAttr}>=${setUpdateDateStr})))} Eg 2: (&(objectCategory=person)(objectClass=user)(sAMAccountName=*)(!(userAccountControl:1.2.840.113556.1.4.803:=2))) will import all active users
)
(&(objectCategory=person)(objectClass=user))

IMPORTJSON
JSON to specify LDAP Import Parameters - e.g: { "envproperties" : { "com.sun.jndi.ldap.connect.timeout": "10000", "com.sun.jndi.ldap.read.timeout": "50000" } }

ACCOUNT_ATTRIBUTE
Controls the LDAP Attribute to Saviynt Account Mapping and ACCOUNTID parameter is a mandatory parameter (eg: [DISPLAYNAME::CN#String,NAME::employeeID#String,NAME::sAMAccountName#String,COMMENTS::distinguishedName#String,STATUS::userAccountControl#number,ACCOUNTID::objectguid#String,RECONCILATION_FIELD:ACCOUNTID])
ME::sAMAccountName#String,CUSTOMPROPERTY20::userPrincipalName#String,CUSTOMPROPERTY21::manager#String,CUSTOMPROPERTY22::homePhone#String,CUSTOMPROPERTY23::mobile#String,CREATED_ON::whenCreated#date,ACCOUNTCLASS::objectClass#String,customproperty26::distinguishedName#String,RECONCILATION_FIELD::customproperty26,ACCOUNTID::distinguishedName#String,RECONCILATION_FIELD::ACCOUNTID]

ENTITLEMENT_ATTRIBUTE
LDAP Attribute which stores the entitlements. For AD it memberOf
memberOf

Fig 12: Create Connection for Security System and Endpoint



ADVANCE_FILTER_JSON
JSON, to define multiple search Filter criteria for a defined container

ORG_BASE
Organization BASE for provision job

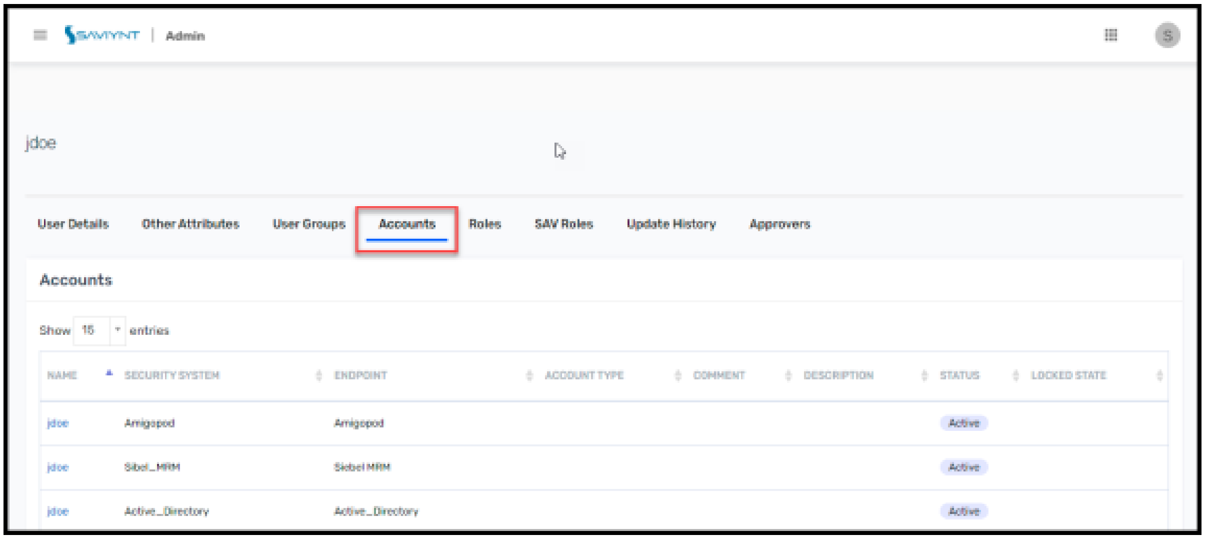
ORGANIZATION_ATTRIBUTE
Organization Attributes

ORGIMPORTJSON
JSON to specify different attributes for Organization Import Job

CREATEORGJSON
JSON to specify different attributes for Organization Create Provisioning Job

UPDATEORGJSON
JSON to specify different attributes for Organization Update Provisioning Job

Fig 13: Save & Test Connection



jdoe

Accounts

Show 15 entries

NAME	SECURITY SYSTEM	ENDPOINT	ACCOUNT TYPE	COMMENT	DESCRIPTION	STATUS	LOCKED STATE
jdoe	Amigopod	Amigopod				Active	
jdoe	Sibel_MRM	Siebel MRM				Active	
jdoe	Active_Directory	Active_Directory				Active	

Fig 14: Validate Associated Entitlements

3.2 SAV ROLES

SAV Role Personas

• Through SAV Roles, you can control what end-users can do at both broad and granular levels.

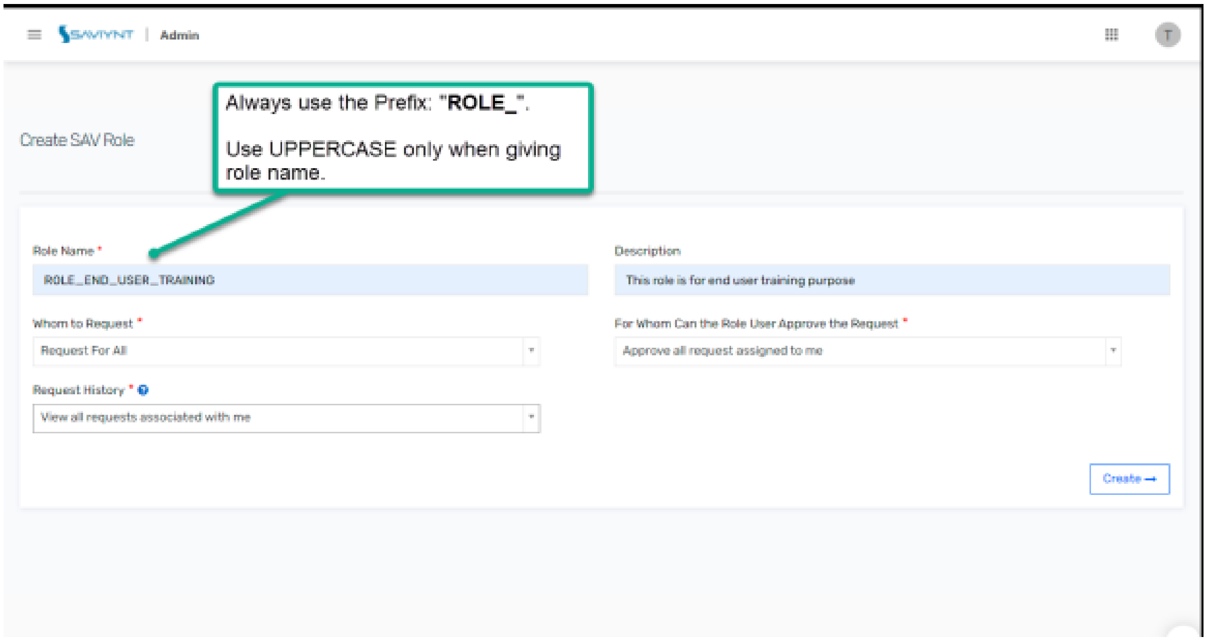
• You can designate whether the user is an administrator, a specialist user, or an end-user, and align SAV Roles and access permissions with your employee position in the organization.

• Permissions are allocated only with enough access as required for employees to do their jobs.

Here are a few examples of Personas for SAV Roles:

1. **Reporting Manager:** Jim, who is a reporting manager, requires access in SSM to approve access requests and complete certification, and delegate ownership.

2. **End User:** John, who is an SSM end user, is required to request access for self and others for various applications and view the request history.



Create SAV Role

Always use the Prefix: "**ROLE_**".

Use UPPERCASE only when giving role name.

Role Name *: ROLE_END_USER_TRAINING

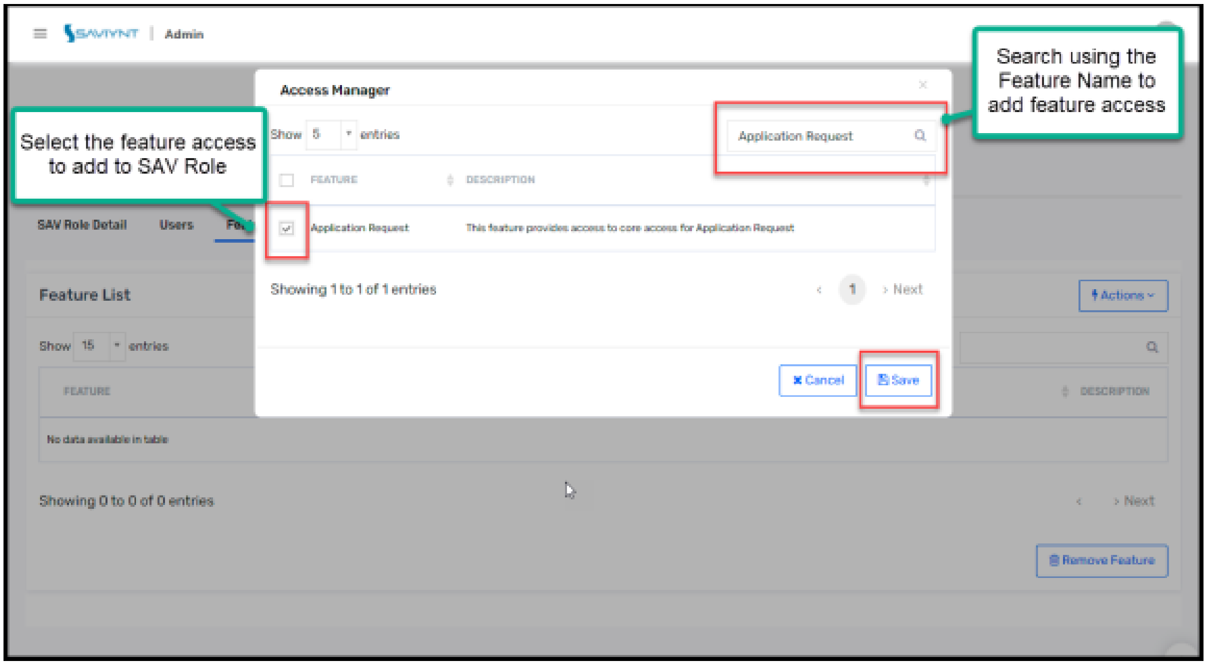
Description: This role is for end user training purpose

Whom to Request *: Request For All

For Whom Can the Role User Approve the Request *: Approve all request assigned to me

Request History *: View all requests associated with me

Fig 15: Create SAV Role



Search using the Feature Name to add feature access

Select the feature access to add to SAV Role

Access Manager

Show 5 entries

Application Request

☐	FEATURE	DESCRIPTION
☑	Application Request	This feature provides access to core access for Application Request

Showing 1 to 1 of 1 entries

Feature List

Show 15 entries

FEATURE	DESCRIPTION
No data available in table	

Showing 0 to 0 of 0 entries

Fig 16: Add New Access

3.3 ACCESS REQUEST SYSTEM

The Access Request System (ARS) is primarily used by two personas – End User and Reviewer (Manager). Saviynt 2020.0 introduces a brand-new ARS user interface developed with modern-design principles and targeted for these personas and their goals rather than being a mere capability-based module.

For End Users, the Homepage serves as the primary entry page. It allows users to make requests and displays all user requests and their statuses along with the following activities:

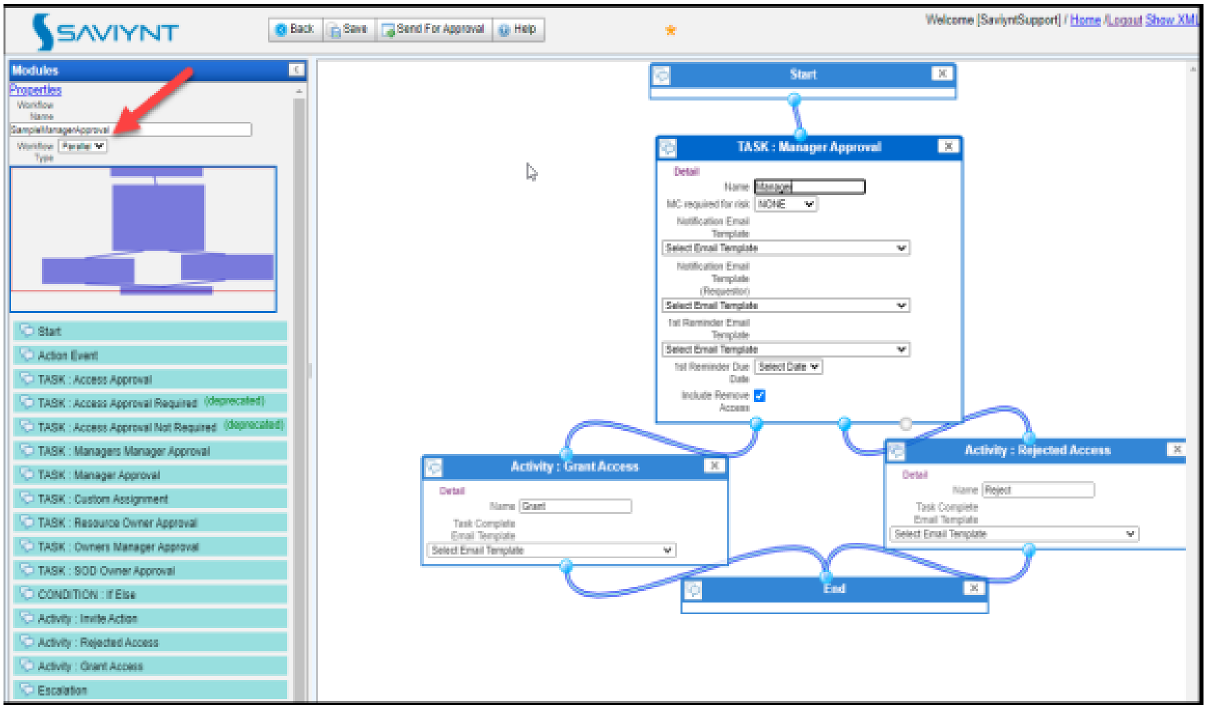
- Overview of the Interfaces
- Managing Access Request
- Viewing Request History

For Reviewers (Managers), the Homepage shows all the tasks that are pending action for Managers (review and approval). Managers can raise Requests on behalf of their team members and perform the following tasks:

- Managing Teams
- Managing Request Approval

Set Up Workflows

Workflows include the business process flows which are followed for approvals of Access Requests submitted in Saviynt.


SAVIYNT
Back
Save
Send For Approval
Help
Welcome [SaviyntSupport] / Home /Logout Show XML
Modules
Properties
Start
Action Event
TASK : Access Approval
TASK : Access Approval Required (deprecated)
TASK : Access Approval Not Required (deprecated)
TASK : Managers Manager Approval
TASK : Manager Approval
TASK : Custom Assignment
TASK : Resource Owner Approval
TASK : Owners Manager Approval
TASK : SOD Owner Approval
CONDITION : If Else
Activity : Invite Action
Activity : Rejected Access
Activity : Grant Access
Escalation
Start
TASK : Manager Approval
Activity : Grant Access
Activity : Rejected Access
End

Workflow Name: SampleManagerApproval

Workflow Type: Parallel

TASK : Manager Approval

Detail

Name: Manager

MC required for risk: NONE

Notification Email Template: Select Email Template

Notification Email Template (Requestor): Select Email Template

1st Reminder Email Template: Select Email Template

1st Reminder Due Date: Select Date

Include Remove Access: ☑

Activity : Grant Access

Detail

Name: Grant

Task Complete Email Template: Select Email Template

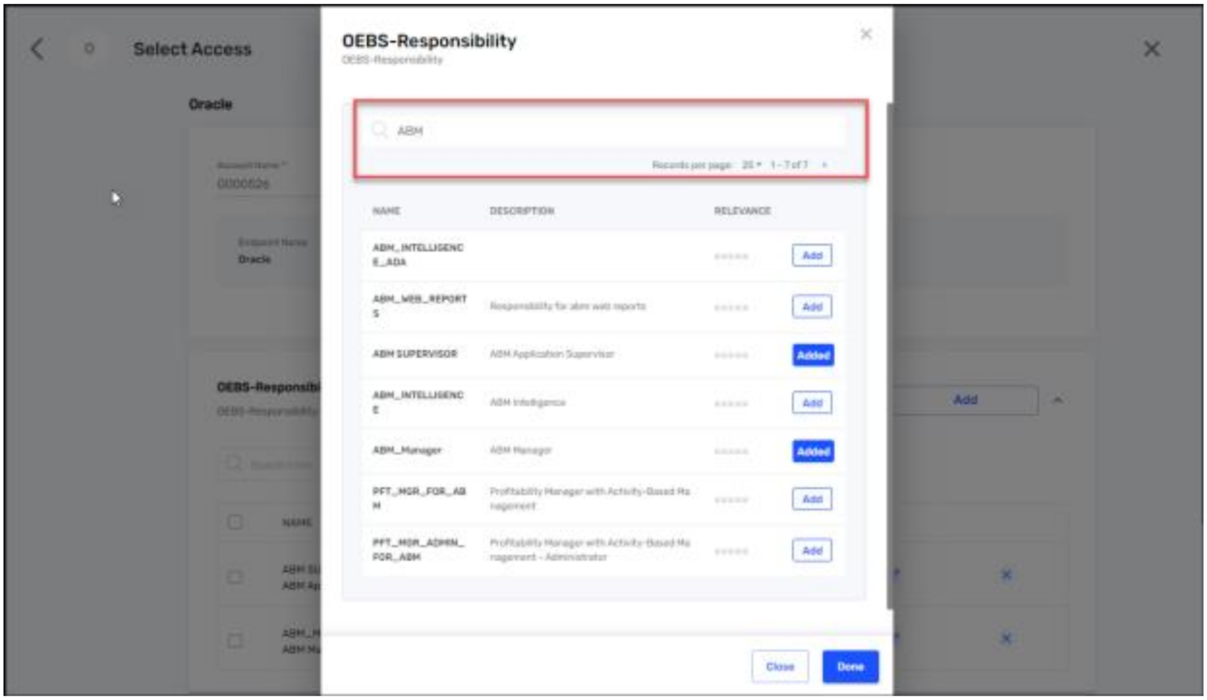
Activity : Rejected Access

Detail

Name: Reject

Task Complete Email Template: Select Email Template

Fig 17: Create New Workflow

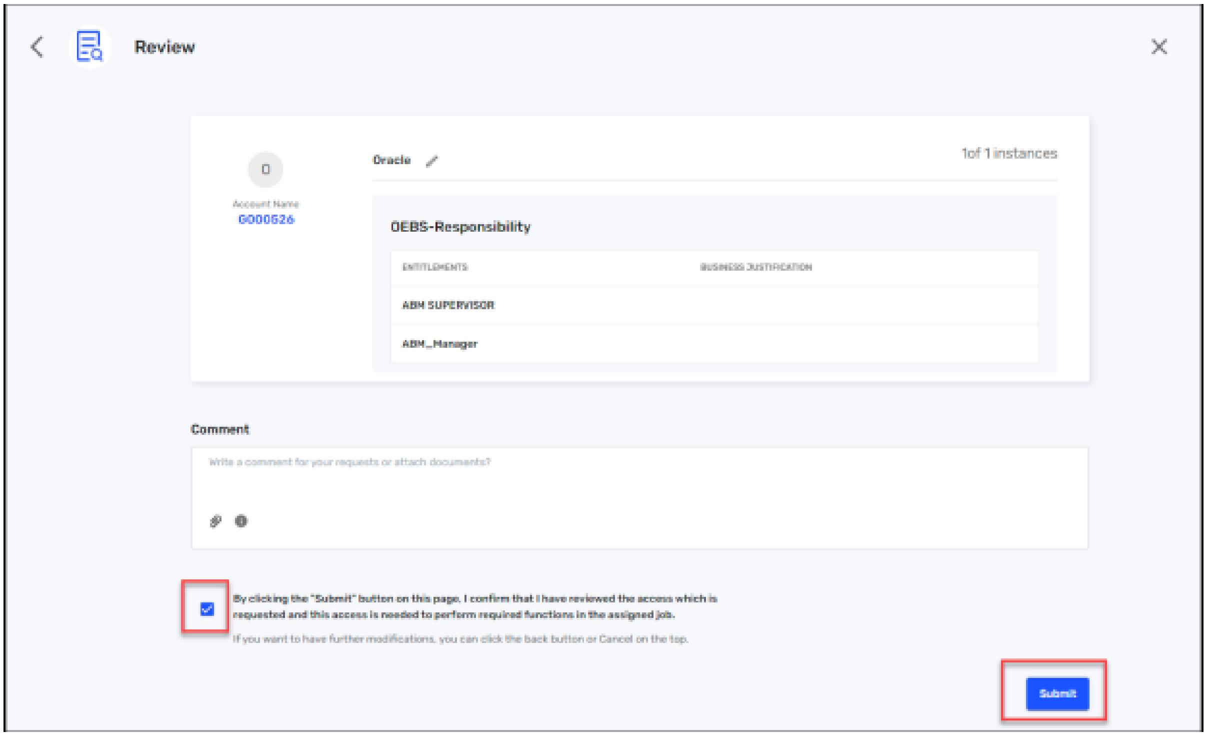


ABM

Records per page: 20 ▾ 1 - 7 of 7

NAME	DESCRIPTION	RELEVANCE	
ABM_INTELLIGENCE_ADA			Add
ABM_WEB_REPORTS	Responsibility for abm web reports		Add
ABM SUPERVISOR	ABM Application Supervisor		Added
ABM_INTELLIGENCE	ABM Intelligence		Add
ABM_Manager	ABM Manager		Added
PFT_MGR_FOR_ABM	Profitability Manager with Activity-Based Management		Add
PFT_MGR_ADMIN_FOR_ABM	Profitability Manager with Activity-Based Management - Administrator		Add

Fig 18: Create New Request for Workflow



Oracle

1of 1 instances

Account Name
G000526

OEBS-Responsibility

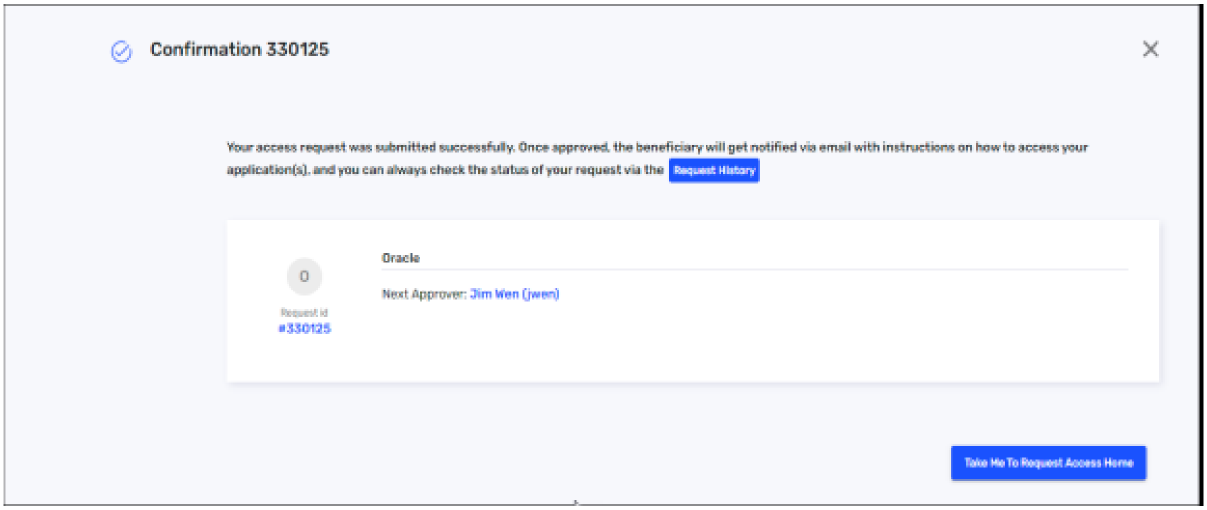
ENTITLEMENTS	BUSINESS JUSTIFICATION
ABM SUPERVISOR	
ABM_Manager	

Write a comment for your requests or attach documents?

☑ By clicking the "Submit" button on this page, I confirm that I have reviewed the access which is requested and this access is needed to perform required functions in the assigned job.

If you want to have further modifications, you can click the back button or Cancel on the top.

Fig 19: Review Created Workflow



Your access request was submitted successfully. Once approved, the beneficiary will get notified via email with instructions on how to access your application(s), and you can always check the status of your request via the Request History

Oracle

Next Approver: Jim Wen (jwen)

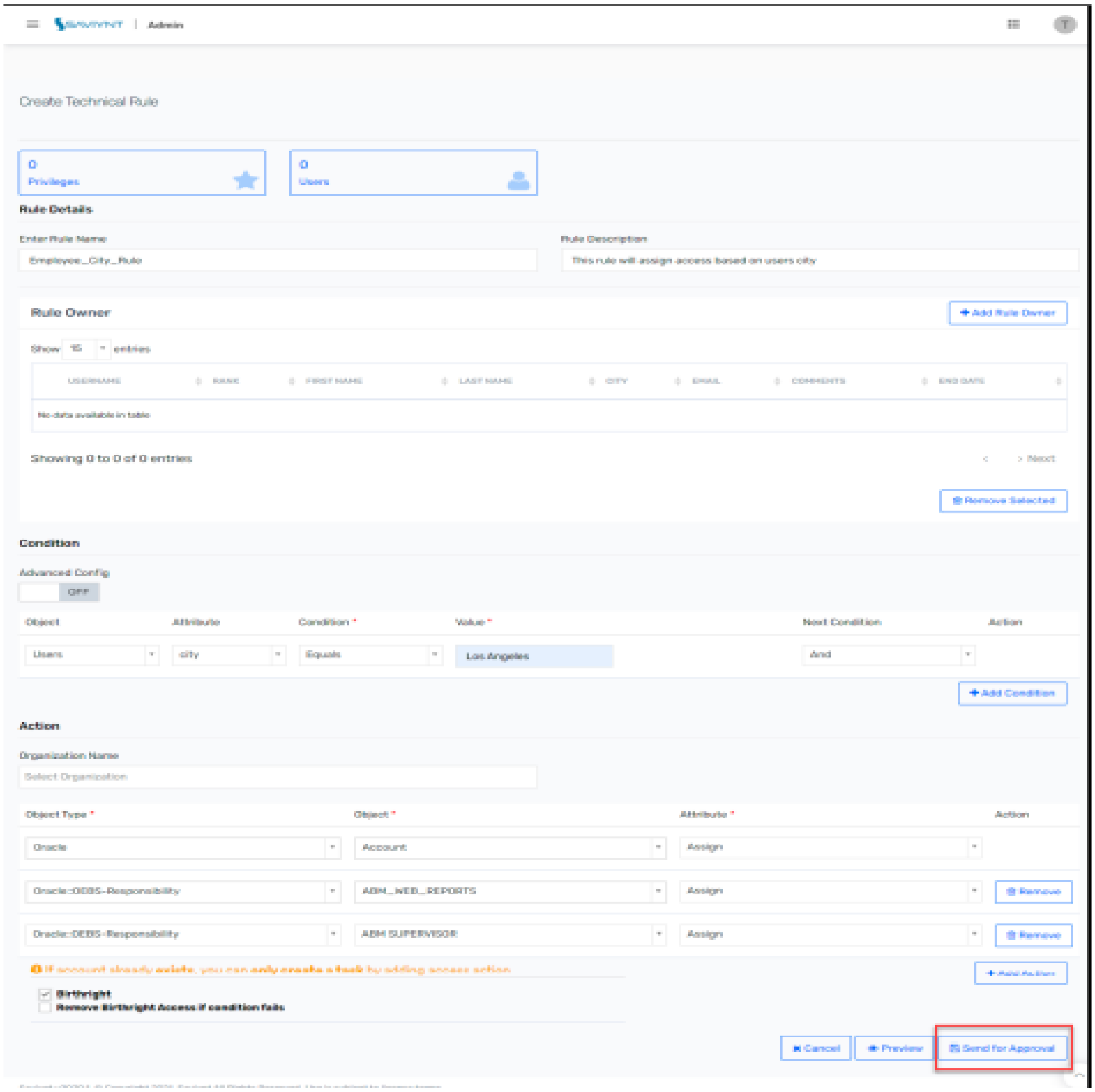
Request id
#330125

Fig 20:Confirmation for Created Workflow

3.4 RULES ENGINEERING

Rules Management

Use case: Add privileges for an employee as a part of birthright access. Take appropriate user actions for employee termination, user transfer, and future-dated off boarding as part of the User Update Rule.



Create Technical Rule

0 Privileges

0 Users

Rule Details

Enter Rule Name: Employee_City_Rule

Rule Description: This rule will assign access based on users city

Rule Owner

Show 15 entries

USERNAME	RANK	FIRST NAME	LAST NAME	CITY	EMAIL	COMMENTS	END DATE
No data available in table							

Showing 0 to 0 of 0 entries

Condition

Advanced Config: OFF

Object	Attribute	Condition *	Value *	Next Condition	Action
Users	city	Equals	Los Angeles	And	

Action

Organization Name: Select Organization

Object Type *	Object *	Attribute *	Action
Oracle	Account	Assign	
Oracle::OEBS-Responsibility	ABM_WEB_REPORTS	Assign	Remove
Oracle::OEBS-Responsibility	ABM SUPERVISOR	Assign	Remove

If account already exists, you can only create a task by adding access action.

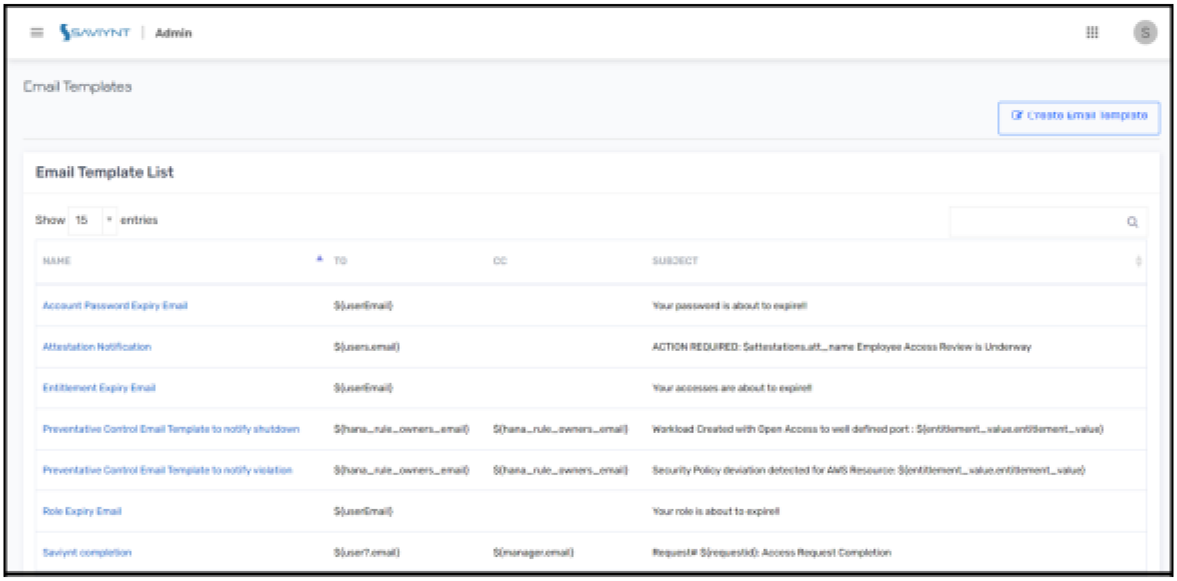
☑ Birthright

☐ Remove Birthright Access if condition fails

Fig 21: Create Provisioning Rules for Birthright Access

Email Templates and Delegates

Use case: An end-user or an administrator should be able to view or create email templates and should be able to create delegates.



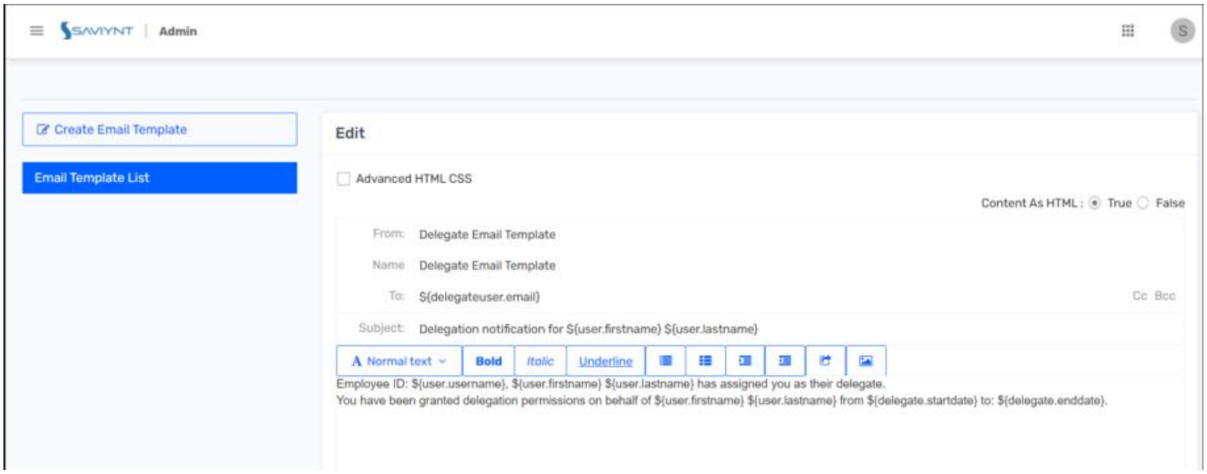
Email Templates

Email Template List

Show 15 entries

NAME	TO	CC	SUBJECT
Account Password Expiry Email	${userEmail}		Your password is about to expire!!
Attestation Notification	${users.email}		ACTION REQUIRED: $attestations.att_name Employee Access Review is Underway
Entitlement Expiry Email	${userEmail}		Your accesses are about to expire!!
Preventative Control Email Template to notify shutdown	${hana_rule_owners_email}	${hana_rule_owners_email}	Workload Created with Open Access to well defined port : ${entitlement_value.entitlement_value}
Preventative Control Email Template to notify violation	${hana_rule_owners_email}	${hana_rule_owners_email}	Security Policy deviation detected for AWS Resource: ${entitlement_value.entitlement_value}
Role Expiry Email	${userEmail}		Your role is about to expire!!
Saviynt completion	${user7.email}	${manager.email}	Request# ${requestid}: Access Request Completion

Fig 22: View Email Templates



Edit

☐ Advanced HTML CSS

Content As HTML : ● True ○ False

From: Delegate Email Template

Name Delegate Email Template

To: ${delegateuser.email} Cc Bcc

Subject: Delegation notification for ${user.firstname} ${user.lastname}

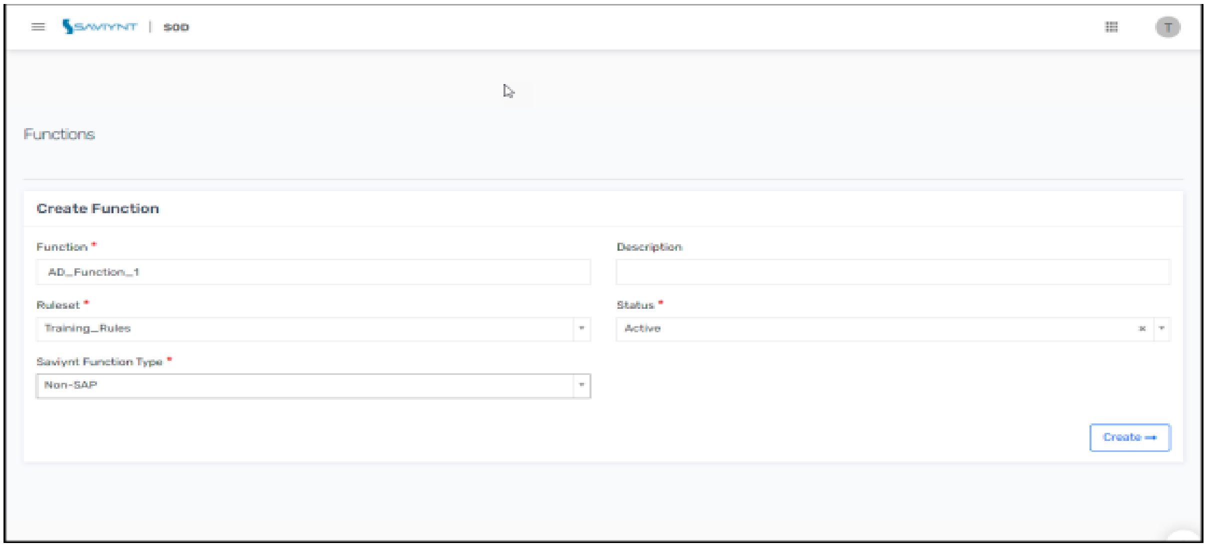
Employee ID: ${user.username}, ${user.firstname} ${user.lastname} has assigned you as their delegate.
You have been granted delegation permissions on behalf of ${user.firstname} ${user.lastname} from ${delegate.startdate} to: ${delegate.enddate}.

Fig 23: Create Email Templates

3.5 SEGREGATION OF DUTES

Create Functions

Use case: If a user requests access for two conflicting functions in Active Directory, SSM should flag this as a SOD violation.



Functions

Create Function

Function * AD_Function_1

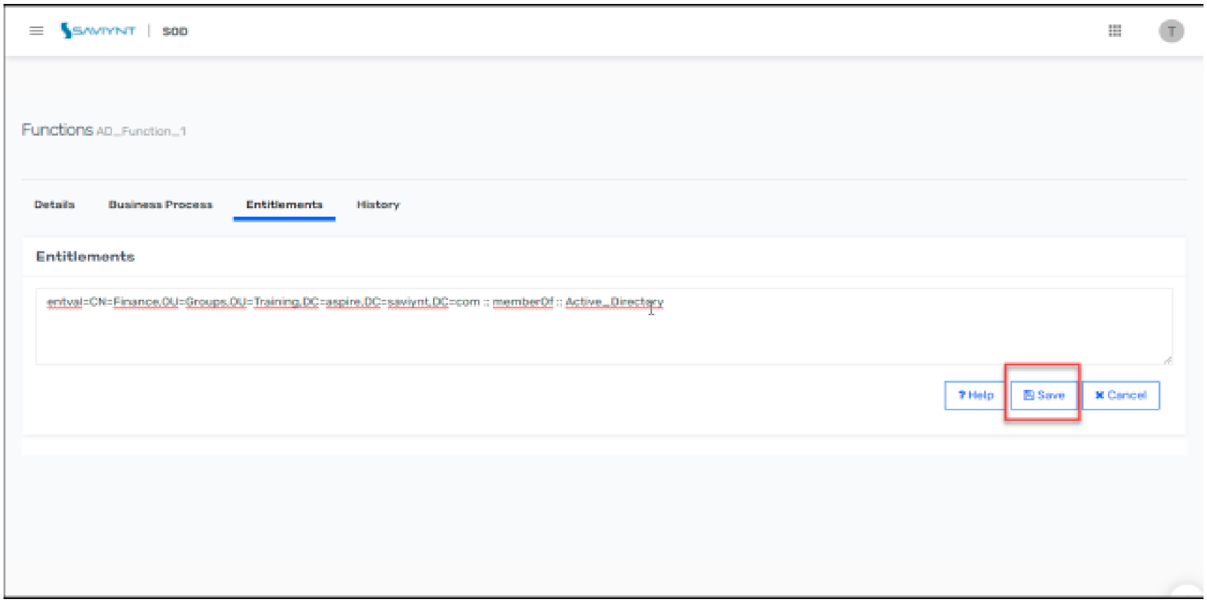
Description

Ruleset * Training_Rules

Status * Active

Saviynt Function Type * Non-SAP

Fig 24: Create Function

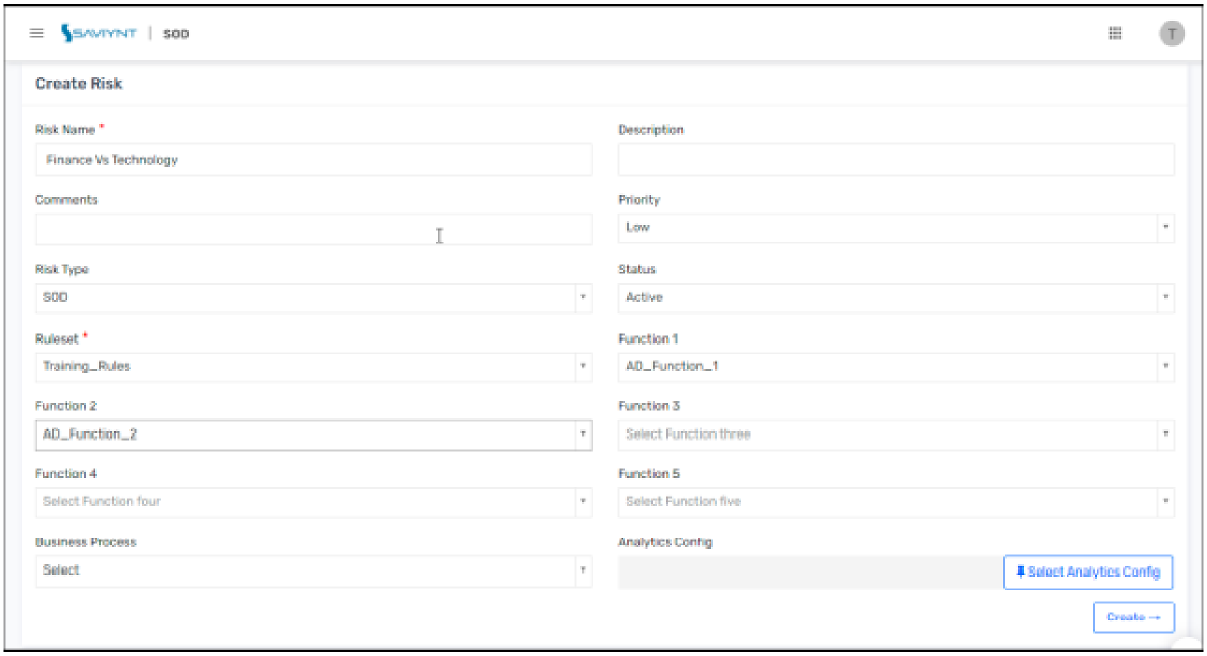


Functions AD_Function_1

Entitlements

```
entval=CN=Finance,OU=Groups,OU=Training,DC=aspire,DC=saviynt,DC=com :: memberOf :: Active_Directory
```

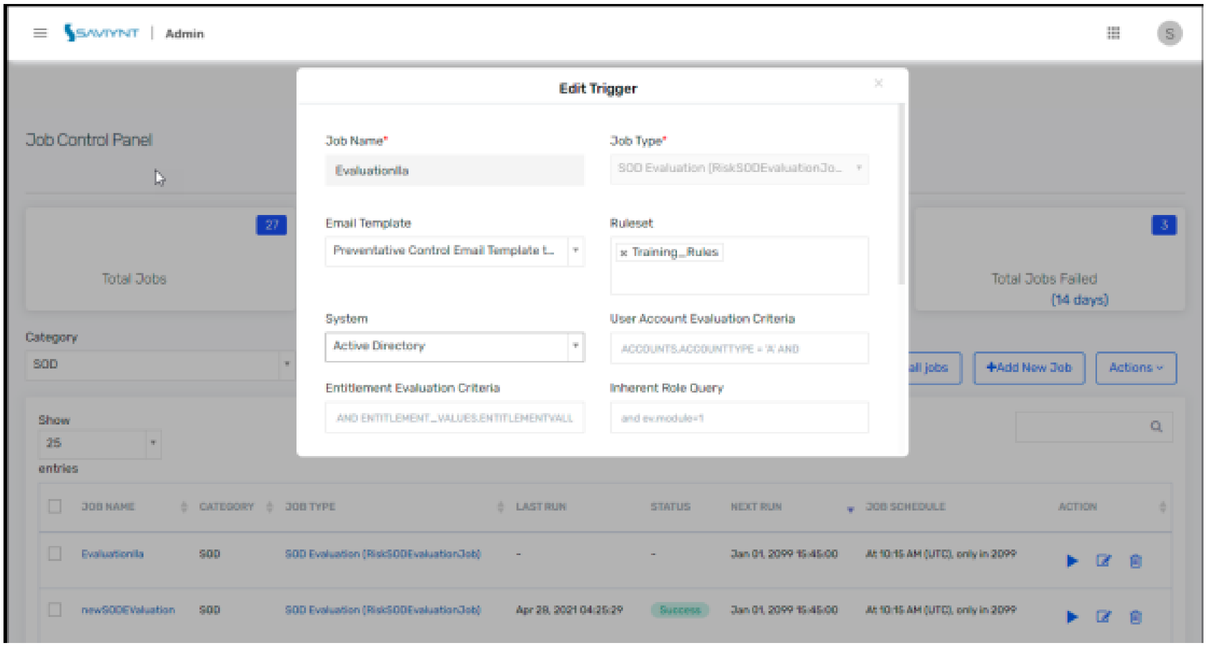
Fig 25: Create Entitlement for above Function



Create Risk

Risk Name *	Finance Vs Technology
Description	
Comments	
Priority	Low
Risk Type	SOD
Status	Active
Ruleset *	Training_Rules
Function 1	AD_Function_1
Function 2	AD_Function_2
Function 3	Select Function three
Function 4	Select Function four
Function 5	Select Function five
Business Process	Select
Analytics Config	

Fig 26: Create Risks



Edit Trigger

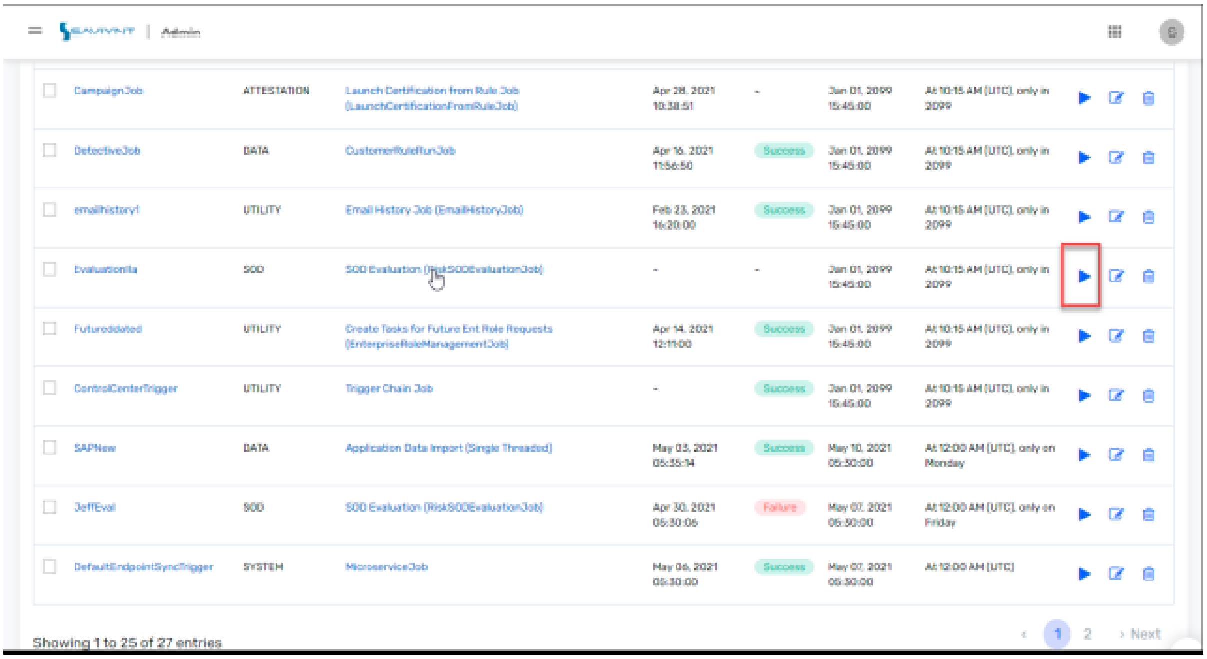
Job Name*	Evaluationlla
Job Type*	SOD Evaluation (RiskSODEvaluationJo...
Email Template	Preventative Control Email Template t...
Ruleset	× Training_Rules
System	Active Directory
User Account Evaluation Criteria	ACCOUNTS.ACCOUNTTYPE = 'A' AND
Entitlement Evaluation Criteria	AND ENTITLEMENT_VALUES.ENTITLEMENTVALL
Inherent Role Query	and ev.module=1

Category: SOD

Show 25 entries

□	JOB NAME	CATEGORY	JOB TYPE	LAST RUN	STATUS	NEXT RUN	JOB SCHEDULE	ACTION
□	Evaluationlla	SOD	SOD Evaluation (RiskSODEvaluationJob)	-	-	Jan 01, 2099 15:45:00	At 10:15 AM (UTC), only in 2099	
□	newSODEValuation	SOD	SOD Evaluation (RiskSODEvaluationJob)	Apr 28, 2021 04:25:29	Success	Jan 01, 2099 15:45:00	At 10:15 AM (UTC), only in 2099	

Fig 27: Add New Job to Evaluate SOD



□	CampaignJob	ATTESTATION	Launch Certification from Rule Job (LaunchCertificationFromRuleJob)	Apr 28, 2021 10:38:51	-	Jan 01, 2099 15:45:00	At 10:15 AM (UTC), only in 2099
□	DetectiveJob	DATA	CustomerRuleRunJob	Apr 16, 2021 11:56:50	Success	Jan 01, 2099 15:45:00	At 10:15 AM (UTC), only in 2099
□	emailhistory1	UTILITY	Email History Job (EmailHistoryJob)	Feb 23, 2021 16:20:00	Success	Jan 01, 2099 15:45:00	At 10:15 AM (UTC), only in 2099
□	Evaluationlla	SOD	SOD Evaluation (RiskSODEvaluationJob)	-	-	Jan 01, 2099 15:45:00	At 10:15 AM (UTC), only in 2099
□	Futuredidated	UTILITY	Create Tasks for Future Ent Role Requests (EnterpriseRoleManagementJob)	Apr 14, 2021 12:11:00	Success	Jan 01, 2099 15:45:00	At 10:15 AM (UTC), only in 2099
□	ControlCenterTrigger	UTILITY	Trigger Chain Job	-	Success	Jan 01, 2099 15:45:00	At 10:15 AM (UTC), only in 2099
□	SAPNew	DATA	Application Data Import (Single Threaded)	May 03, 2021 05:35:14	Success	May 10, 2021 05:30:00	At 12:00 AM (UTC), only on Monday
□	JeffEval	SOD	SOD Evaluation (RiskSODEvaluationJob)	Apr 30, 2021 05:30:06	Failure	May 07, 2021 05:30:00	At 12:00 AM (UTC), only on Friday
□	DefaultEndpointSyncTrigger	SYSTEM	MicroserviceJob	May 06, 2021 05:30:00	Success	May 07, 2021 05:30:00	At 12:00 AM (UTC)

Showing 1 to 25 of 27 entries

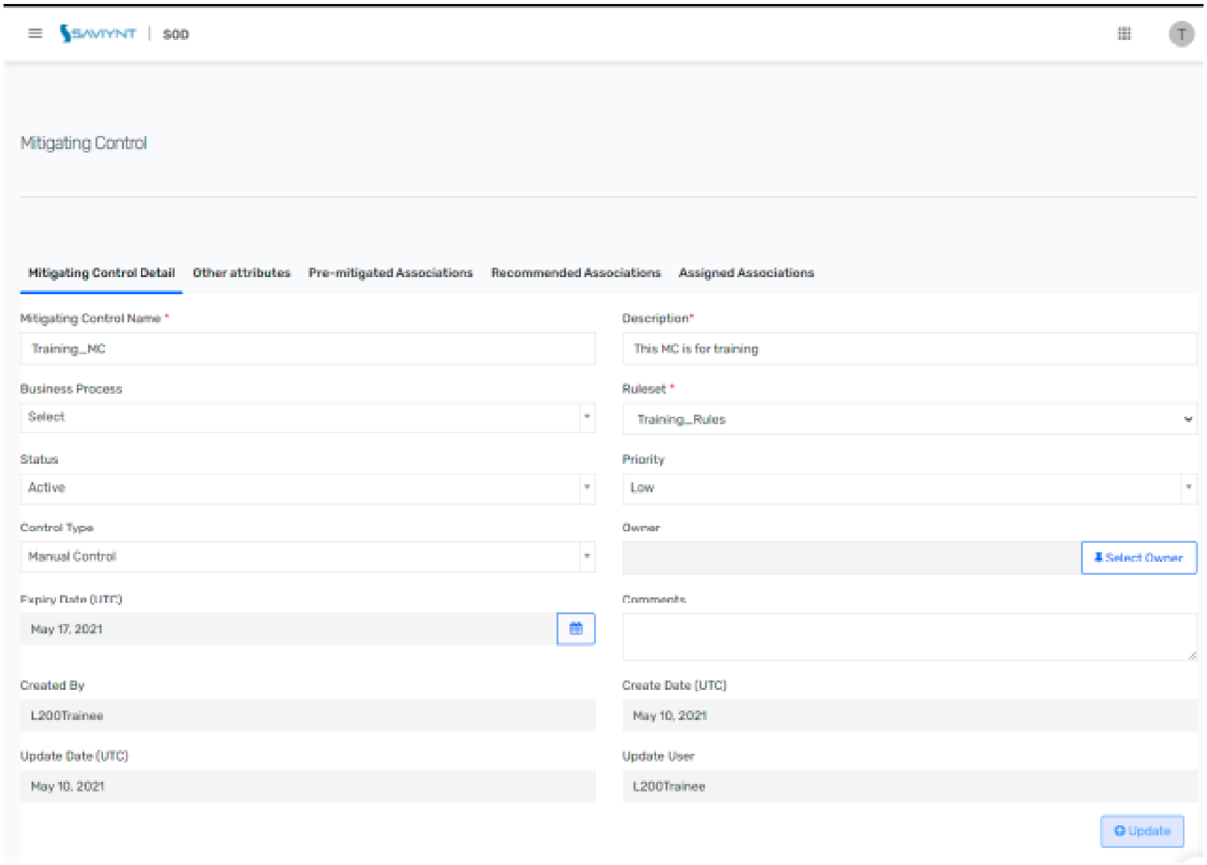
Fig 28: Start SOD Evaluation

Mitigating Controls

Mitigating controls are additional controls that can be implemented in SSM to mitigate sensitive access or SOD Risks. A SOD Violation can be ACCEPTED for a limited period by assigning Mitigating control. Mitigated control is created and associated with violation that has an expiry date. Once the expiry date is passed, violation is moved to OPEN state again. There are two types of mitigating controls:

- Pre-mitigated Associations: Mitigating controls can be configured automatically and applied to specific risks, which are defined.

- Recommended Associations: When applying Mitigating control to an SOD Violation scenario, specific controls can be recommended for the risks, which are defined.



Mitigating Control

Mitigating Control Name *: Training_MC

Description*: This MC is for training

Business Process: Select

Ruleset *: Training_Rules

Status: Active

Priority: Low

Control Type: Manual Control

Owner:

Expiry Date (UTC): May 17, 2021

Comments:

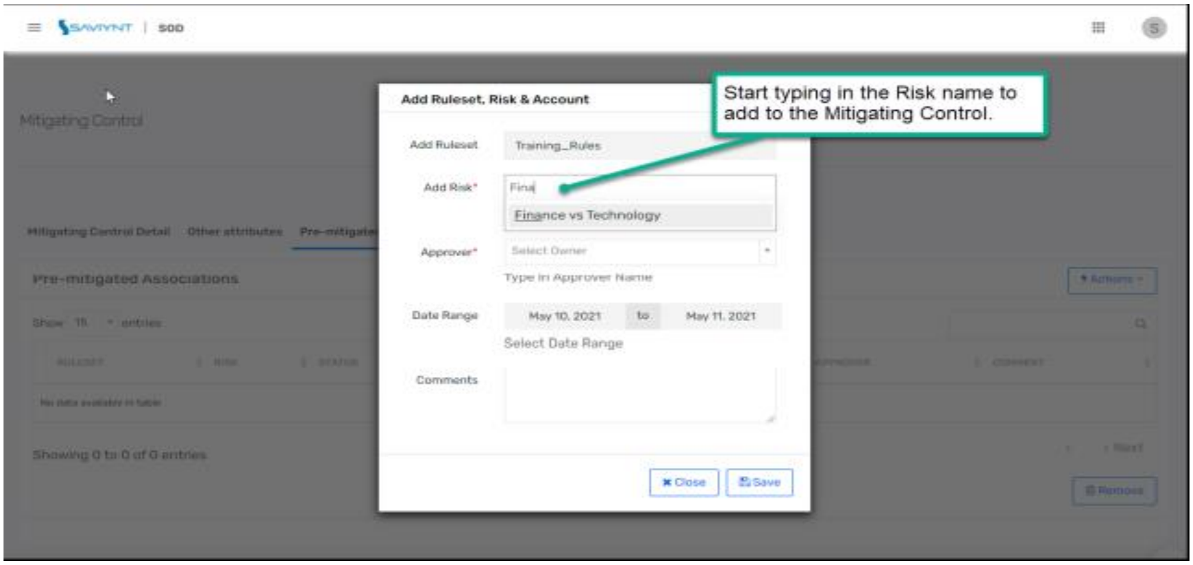
Created By: L200Trainee

Create Date (UTC): May 10, 2021

Update Date (UTC): May 10, 2021

Update User: L200Trainee

Fig 29: Create Mitigating Control


SAVIYNT | SOD
S
Mitigating Control
Mitigating Control Detail
Other attributes
Pre-mitigated
Pre-mitigated Associations
Actions
Showing 0 to 0 of 0 entries
Next
Remove

Add Ruleset, Risk & Account

Start typing in the Risk name to add to the Mitigating Control.

Add Ruleset: Training_Rules

Add Risk*: Fina

Finance vs Technology

Approver*: Select Owner

Type in Approver Name

Date Range: May 10, 2021 to May 11, 2021

Select Date Range

Comments:

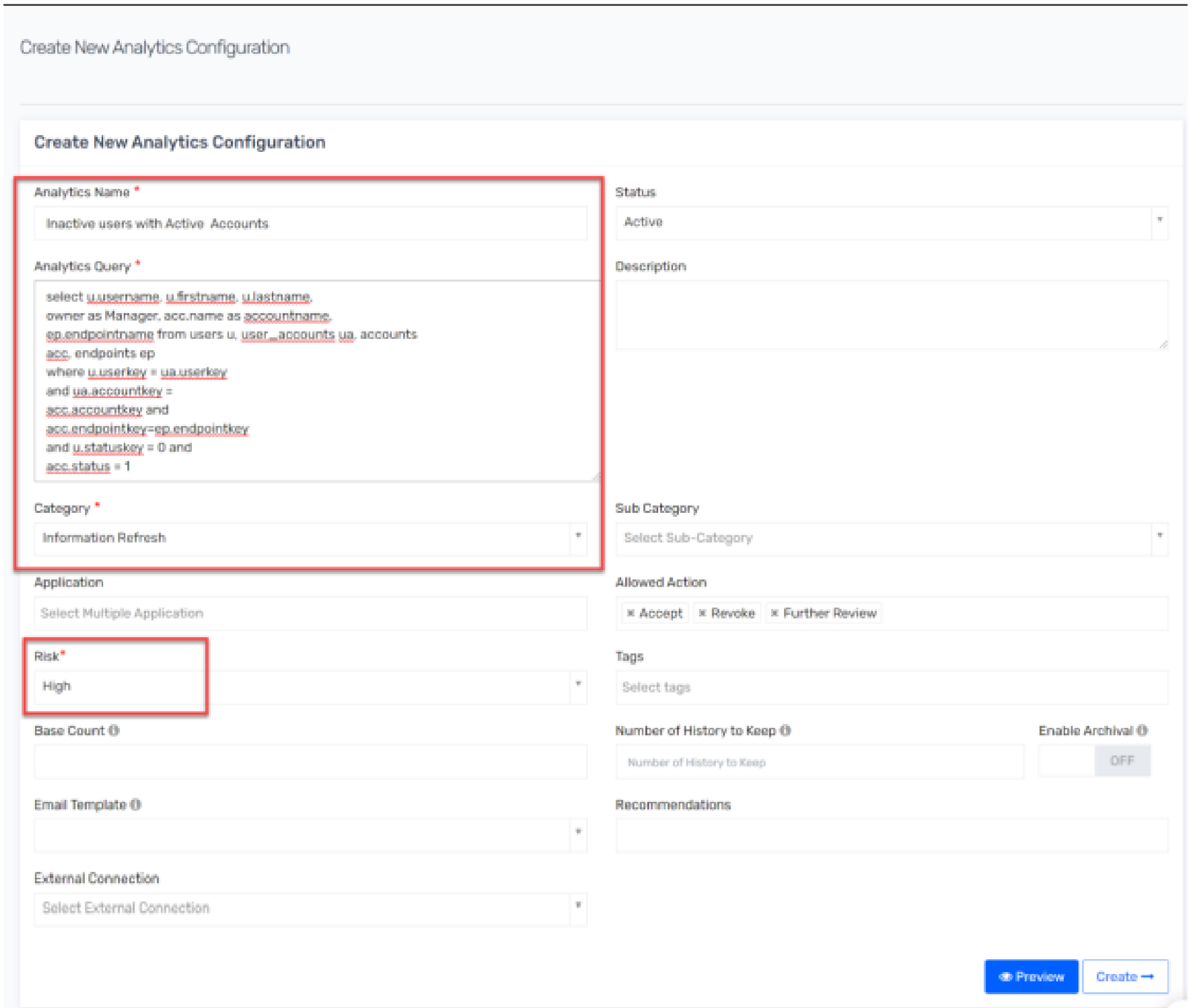
Fig 30: Add Pre-Mitigated Associations

3.6 ANALYTICS

Analytics Using SQL Query

Use case: Run an Analytics based on SQL Query defined conditions. The application will fetch data from the database and display the analytics in the form of a graphical representation based on the written SQL Query.

31:


Create New Analytics Configuration
Create New Analytics Configuration
Select Sub-Category
Select Multiple Application
Select tags
Number of History to Keep
OFF
Select External Connection
Preview
Create →

Analytics Name *: Inactive users with Active Accounts

Status: Active

Analytics Query *:

```
select u.username, u.firstname, u.lastname,
owner as Manager, acc.name as accountname,
ep.endpointname from users u, user_accounts ua, accounts
acc, endpoints ep
where u.userkey = ua.userkey
and ua.accountkey =
acc.accountkey and
acc.endpointkey=ep.endpointkey
and u.statuskey = 0 and
acc.status = 1
```

Description:

Category *: Information Refresh

Sub Category:

Application:

Allowed Action: × Accept × Revoke × Further Review

Risk*: High

Tags:

Base Count

Number of History to Keep

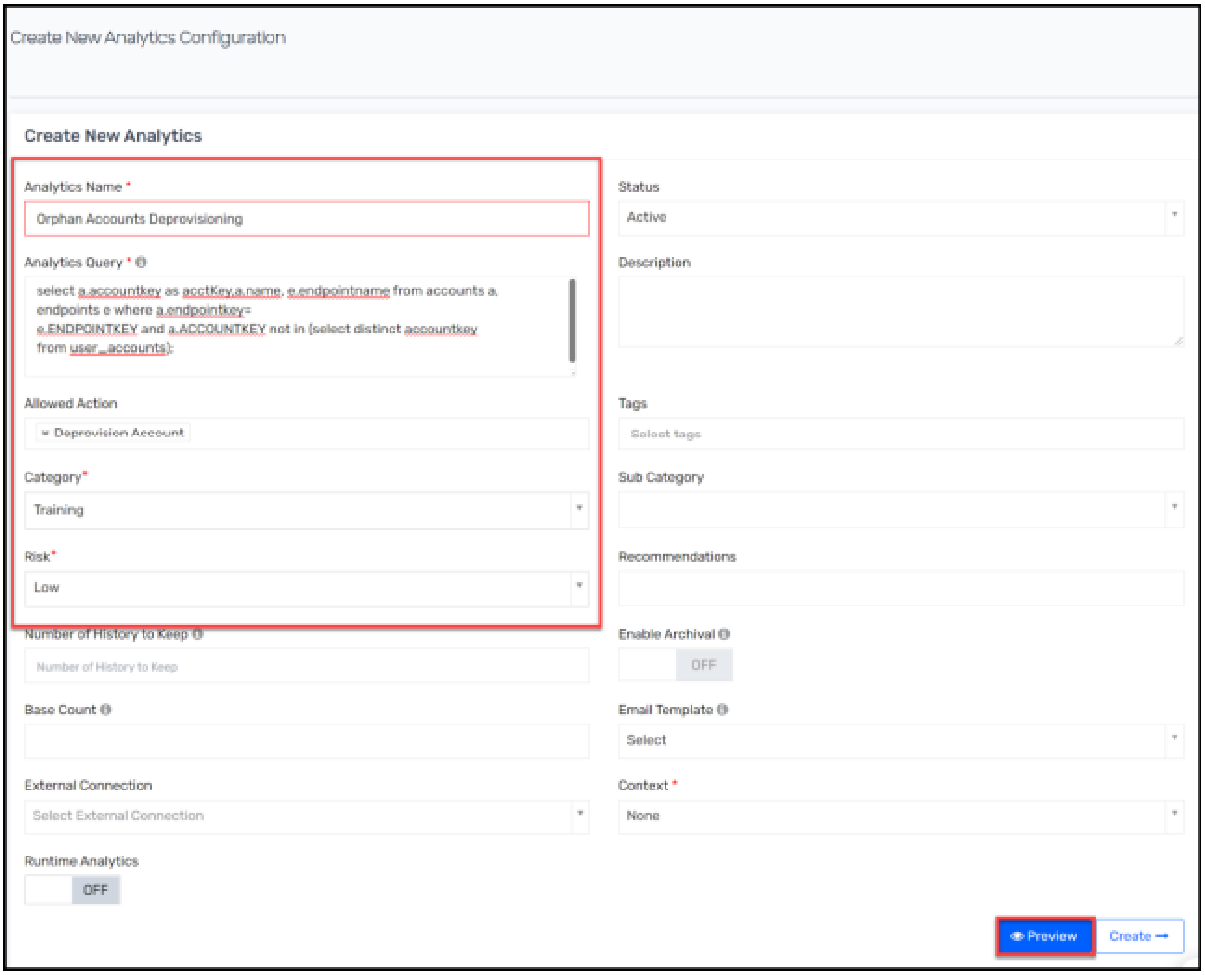
Enable Archival

Email Template

Recommendations

External Connection

Fig 31: Analytics Report to Take Action on Inactive Users with Active Accounts



Create New Analytics Configuration

Create New Analytics

Analytics Name *: Orphan Accounts Deprovisioning

Analytics Query *:

```
select a.accountkey as acctKey,a.name, e.endpointname from accounts a,
endpoints e where a.endpointkey=
e.ENDPOINTKEY and a.ACCOUNTKEY not in (select distinct accountkey
from user_accounts);
```

Allowed Action: × Deprovision Account

Category*: Training

Risk*: Low

Number of History to Keep: Number of History to Keep

Base Count:

External Connection: Select External Connection

Runtime Analytics: OFF

Status: Active

Description:

Tags: Select tags

Sub Category:

Recommendations:

Enable Archival: OFF

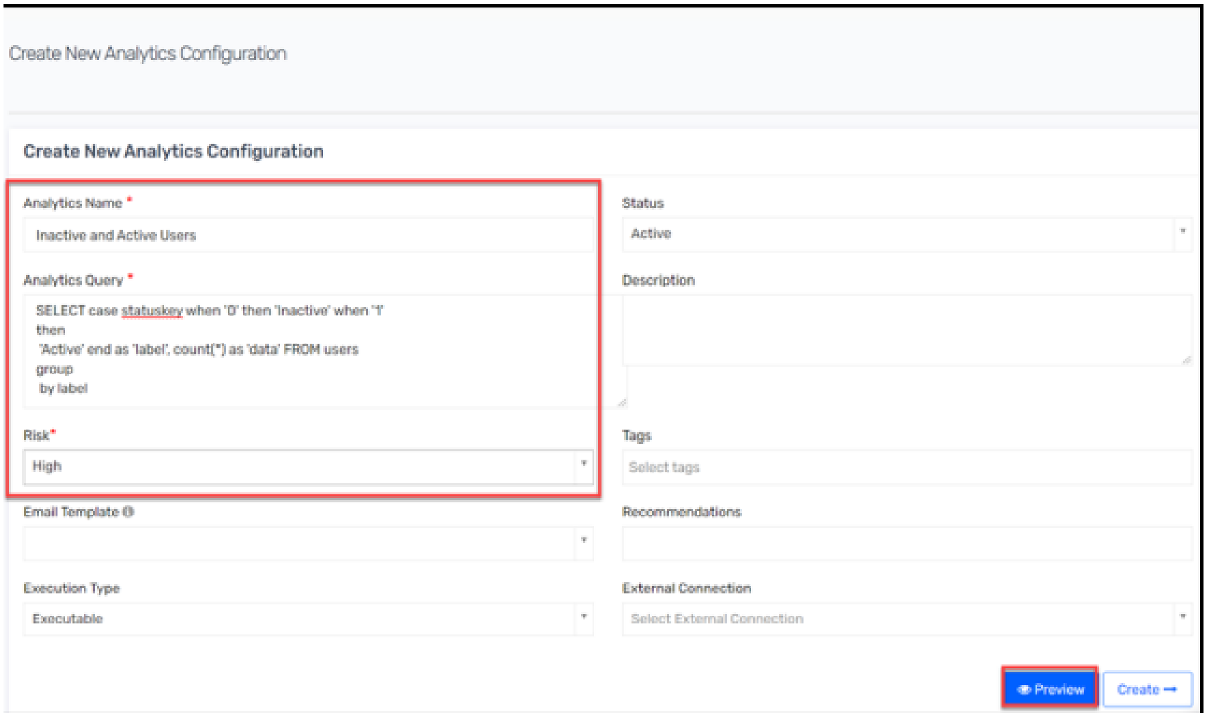
Email Template: Select

Context *: None

Fig 32: Analytics Report for Deprovisioning Orphan Accounts

Analytics Using Runtime Analytics

Use case: Create a Runtime Analytics Report based on the defined conditions. The application will fetch the data from the database and display the Analytics in the form of a graphical representation based on the SQL Query written in real time. The Analytics report will then be exported.



Create New Analytics Configuration

Create New Analytics Configuration

Analytics Name *
Inactive and Active Users

Status
Active

Analytics Query *

```
SELECT case statuskey when '0' then 'Inactive' when '1'
then
 'Active' end as 'label', count(*) as 'data' FROM users
group
 by label
```

Description

Risk*
High

Tags
Select tags

Email Template

Recommendations

Execution Type
Executable

External Connection
Select External Connection

Fig 33: Analytics Report to Export Inactive and Active Data

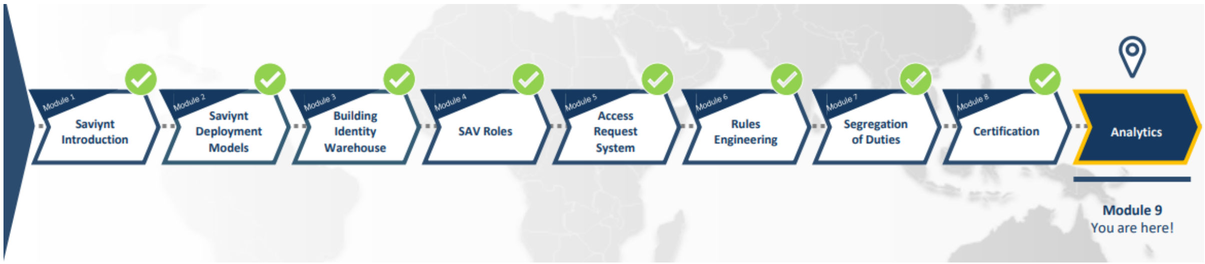


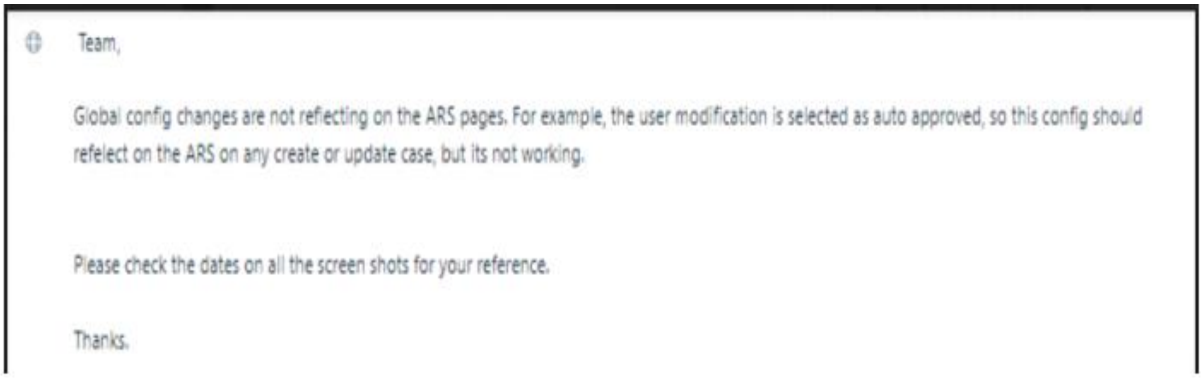
Fig 34: Training Flow

CHAPTER - 4

PERFORMANCE ANALYSIS

4.1 Ticket Resolved

Being in the customer support, my work is to handle customers and solve their doubts.



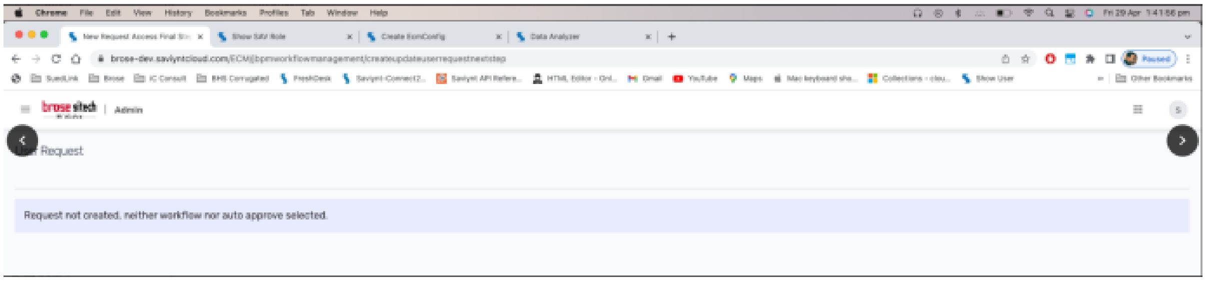
Team,

Global config changes are not reflecting on the ARS pages. For example, the user modification is selected as auto approved, so this config should refelect on the ARS on any create or update case, but its not working.

Please check the dates on all the screen shots for your reference.

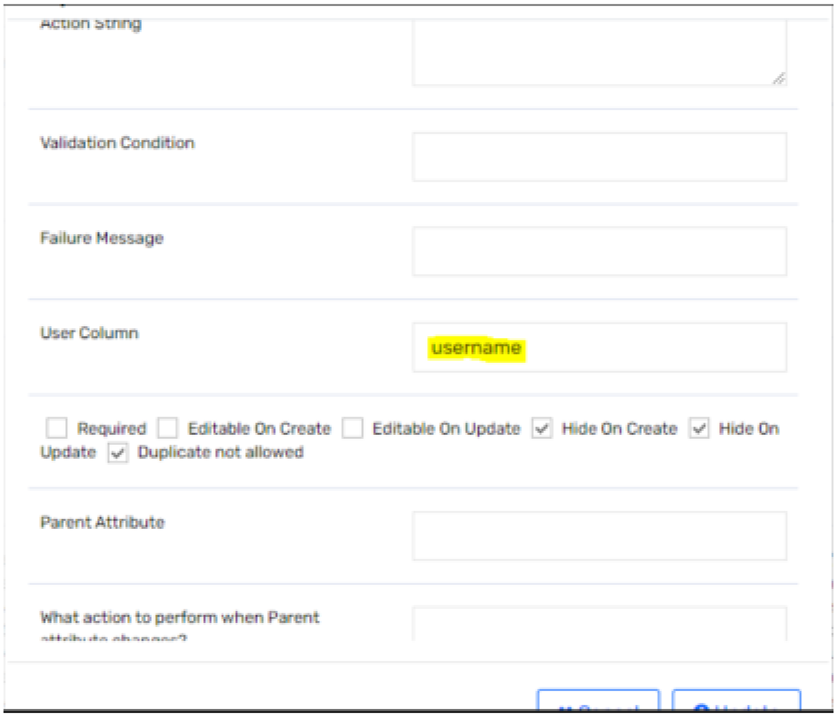
Thanks.

The issue faced by them while using the Saviynt product was that they were trying to update the user that uses the dynamic attribute. They were unable to do so even after correcting all the settings.



Request not created, neither workflow nor auto approve selected.

In order to understand the error and to check whether the same error occurs when we try to do it, we replicate it in our system. We created the same dynamic attributes used by the customer. We found out that while creating the dynamic attribute "username", they were using wrong spelling and the word was not matching with the word used in the database. They were using "Username" instead of "username". So we correct the same.



Action String

Validation Condition

Failure Message

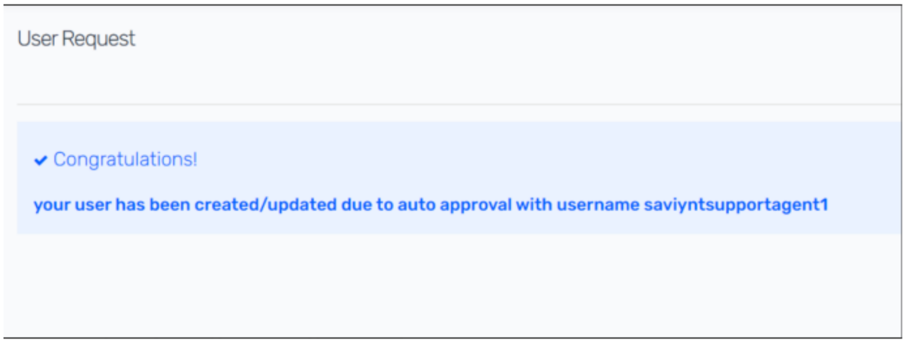
User Column: username

□ Required □ Editable On Create □ Editable On Update ☑ Hide On Create ☑ Hide On Update ☑ Duplicate not allowed

Parent Attribute

What action to perform when Parent attribute changes?

After making the following changes, the issue was resolved.



User Request

✓ Congratulations!

your user has been created/updated due to auto approval with username saviyntsupportagent1

CHAPTER - 5

CONCLUSION

5.1 Conclusion

The past one month has been great for learning. The concepts I learnt have cleared my basics. These topics were ones I have not explored before. They raise my curiosity and I wish to learn more. Cyber security is one of the main concerns. Saviynt is on a mission to safeguard enterprises through intelligent, cloud-first identity governance & access management solutions. Saviynt was created to challenge the status quo. We always realized that identity could be so much more – and the leading solutions weren't up to the task. So we set out to build the most innovative cloud identity & access governance platform on the market. It hasn't always been easy, but we're here to solve challenges, not hide from them. Today we've grown into a global organization scaling at breakneck speed to help the largest enterprises in the world transform their identity programs and protect their people, assets, and infrastructure.

I like to thanks in advance to the coaches, SME, mentor and trainer of Saviynt who guided me through the whole journey of my internship in Saviynt and solved all my doubts during the internship. The Coaches, SME, Mentor and trainer were all of good nature and at every moment helped me when I was doing wrong and shaped me during my whole internship. Specially my mentor gave his more effort during the internship and passed my all query to the higher authority in the company whether it was related to the reattempt of the assessment, technical issue faced in the assessment or providing extra time to complete the work.

I like thank you my TNP officer Mr. Pankaj Kumar for his support and hard work during the whole placement process because I know how complex is the management of the placement drive.

REFERENCES

1. https://www.linkedin.com/learning/introducing-postman

2. https://www.linkedin.com/learning/programming-foundations-apis-and-web-services

3. https://www.linkedin.com/learning/http-essential-training

4. https://www.linkedin.com/learning/ssl-certificates-for-web-developers

5. https://www.linkedin.com/learning/learning-groovy

6. https://www.linkedin.com/learning/learning-apache-tomcat

7. Saviynt Internship Handbook

8. Internship experience