

**XYZ - Accompagnement Transformation GIA​​**

***Design Document***

***IDN Application Onboarding: OIPA***

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

**Document History**

***Revision History***

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Revision Date** | **Author** | **Comments** |
| 1.0 | 2024-06-18 | KPMG | Initial version of document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

***Reviewers***

This document has been sent to the following people for their review and comments.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date of review** | **Name** | **Comments** |
| 1.0 | 2024-06-18 | KPMG | Initial version of document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

***Signoffs***

This document has been sent to the following people for their review and a sign-off approval.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Sign-off Date** | **Name** | **Comments** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

1. Introduction 4

1.1. Summary 4

1.2. Project Overview 4

1.3. Scope 4

1.4. Out of scope 4

1.5. Identified Limitations and Constraints 4

2. Application Infrastructure 5

2.1. SailPoint IDN Architecture 5

2.2. Virtual Appliance 6

2.3. Virtual Appliance Configuration 7

2.4. Hardware and environment configuration 7

3. Application technical Overview 8

3.1. Pre-requisites 8

3.1.1. Network Requirement 8

3.1.2. Service Account Permissions 8

3.2. OIPA Source Configuration 8

3.2.1. Connection Details 8

3.2.2. Aggregation Schedule 12

3.2.3. Correlation 13

3.2.4. Account Schema 13

3.2.5. Account Group Schema 13

3.2.6. Entitlements Glossary 14

3.2.7. Access Profile 15

3.2.8. Roles 15

3.2.9. Provisioning/De-provisioning Data Flow 15

3.3. Certification 17

3.3.1. Design 18

3.3.2. Certification Campaign 18

3.3.3. Certification Email Template 18

3.3.4. Manager Certification 19

3.3.5. Source Owner Certification Campaign 19

3.4. Lifecycle change events 20

4. Conclusion 20

# Introduction

## Summary

This introductory section explains the purpose and scope of this document. It provides the background and context for creating the SailPoint IdentityNow(IDN) Technical Design Specification document for XYZ.

## Project Overview

XYZ has engaged KPMG to perform technical design, of their SailPoint IDN implementation. Prior to the technical design phase, KPMG has been involved in documenting detailed functional requirements.

## Scope

The scope of this document is to provide overall design for application onboarding in SailPoint. The onboarding process will offer a comprehensive overview of the configuration process for the application, including instructions on how to use attributes and the values that are necessary.

* OIPA

## Out of scope

The following items are out of scope from the current phase of work:

* + Configurations on Joiner, Mover, and Leaver and other lifecycle processes
  + Enabling access request
  + Application Monitoring and Application Restoration related to XYZ IT infrastructure components (for example network, cloud, hardware, and infrastructure or equivalent)
  + Manual monitoring services such as health monitoring of the SailPoint infrastructure.
  + Configure approval details on the entitlements.
  + Automate SSO group provisioning.

## Identified Limitations and Constraints

* Description, Requestable, Privileged attributes cannot be updated for entitlements having French accent characters in the name.

# Application Infrastructure

This section of the document provides the overview of different capabilities offered in SailPoint IDN implementation, Virtual Appliances and, IQService configuration details.

## SailPoint IDN Architecture

The diagram below provides physical architecture for IdentityNow implementation integrating HR authoritative source, Active Directory and business applications.

**HR Authoritative Source**

(User Type: Employees, Non-Employees & Contractor)

SailPoint IdentityNow

*(capabilities)*

Virtual Appliance



IQService

Active Directory

Flat File Application

Other Applications

JDBC Application

AD Based Application

Target Sources

Provisioning  
Access Certification

Access Certification

Separation of Duties

Lifecycle Management – Joiner, Leaver, LOA

Reporting, Auditing and Monitoring

IDN is integrated with Workday, LDAP as authoritative sources using Workday and Open LDAP direct connector. IDN is integrated with non-authoritative sources. Admins and Helpdesk login to IDN user interface to perform their day-to-day job functions. IDN does not interact with target source systems directly, instead it contacts through the Virtual Appliance. Refer to below section for more info about Virtual Appliance.

**IQService** is a small and important component that is installed on Windows servers connected to your Active Directory domain(s) to make updates (write operations) for new/modified users. IQService is usually installed in a small, dedicated virtual machine within the Windows domain that contains only the IQService agent.

## Virtual Appliance

The **Virtual Appliance (VA)** is a virtual machine (black box) that is deployed on XYZ network and is remotely managed by SailPoint. The VA communicates with the IdentityNow(IDN) service (outbound) and takes instructions to perform on your target systems (inbound). This includes any cloud applications with which the VA will communicate (outbound).

A VA cluster provides connectivity to one or more source systems within your IT environment. Multiple clusters can be used, and you choose the number of clusters and the number of VAs within each cluster. However, ensure that production systems have at least two VAs in a cluster.

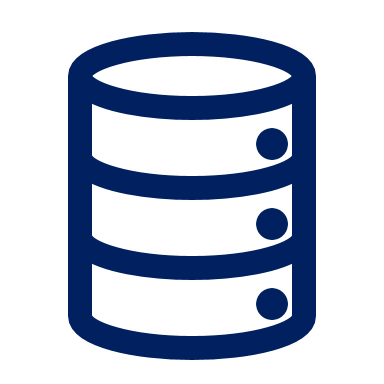
A connectivity gateway enables data communications between your tenant and the directly connected source systems of your IT environment. The communication is always initiated by the VA as outbound traffic, making it more secure and easier for your corporate firewall to manage.

**VA Communication Flow:**

1. VAs poll cluster queue: VAs from the same cluster continuously poll the same cluster queue monitoring for work. The tenant submits work to VAs by adding messages to a VA cluster queue.
2. VAs process messages in queue: A VA in the cluster reads a message, such as scheduled activities or end-user actions to be processed and removes it from the cluster queue. Each message is decrypted with the private key so that the VA can communicate with the systems in your environment. In case of more than one VA, each one will take messages one at a time, and only one VA in a cluster will respond to a message.
3. VA processes message and communicates back to tenant: The VA communicates internally with the cloud connector gateway (the CCG) to complete the work. The completion status and results are communicated back to the tenant from the VA.

Communication Flow

**VA Cluster Queue**



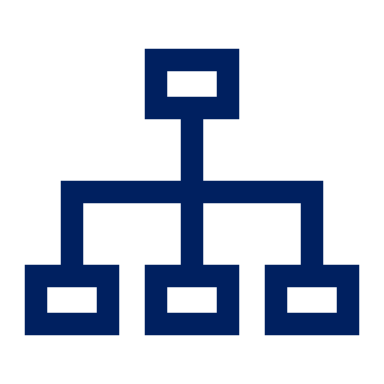
**Read Messages**

**Virtual Appliance**

**Cloud Connector Gateway**

**Enterprise Connectors**

**Custom Connectors**



**Post Results/Status**

## Virtual Appliance Configuration

The table below summarizes IDN’s VA Configurations:

|  |  |  |
| --- | --- | --- |
| VA Server Configurations | IDN Sandbox | IDN Production |
| Server Type | Linux | Linux |
| Server Hosting: | On-Premises | On-Premises |
| RAM | 8GB | 8GB |
| Storage | 150GB | 150GB |
| VAs in Cluster | 2 | 2 |

## Hardware and environment configuration

Below table represents VA server configurations belongs to Sandbox and Production.

|  |  |  |
| --- | --- | --- |
| VA Server Configurations | IDN Sandbox | IDN Production |
| IdentityNow Cloud URL | https://XYZ-sb.identitynow.com/ | https://XYZ.identitynow.com/ |
| Virtual Appliance 1 | H100DA-SAIL-001.ad.devXYZ.ca | H100PA-sail-001.ad.XYZ.ca |
| 10.31.72.29 | 10.31.8.20 |
| Virtual Appliance 2 | H106DA-SAIL-002.ad.devXYZ.ca | H106PA-sail-002.ad.XYZ.ca |
| ID: 10.231.72.20 | 10.231.8.20 |
| IQService Load Balancer | sailpointiq.devXYZ.ca | sailpointiq.XYZ.ca |
| 10.3.251.209 | 10.3.251.210 |
| IQService 1 | H100DW-SAIL-011.ad.devXYZ.ca | h100pw-sail-011.ad.XYZ.ca |
| 10.31.64.44 | 10.31.0.34 |
| IQService 2 | H106DW-SAIL-012.ad.devXYZ.ca | H106PW-SAIL-012.ad.XYZ.ca |
| 10.231.64.23 | 10.231.0.22 |

# Application technical Overview

This section includes detailed design for IDN and OIPA integration. This section of the document outlines the solution design for the OIPA as a target application.

## Pre-requisites

The following pre-requisites exist for OIPA integration with IDN:

* Determine REST API endpoint URL for SailPoint IDN to connect.
* Create a client application in Azure AD with OIPA admin Role.
* Client application must support client credentials grant type of OAuth authentication.

**Note:** As a best practice we should use “Refresh Token” grant type instead of client credentials.

* Configure Virtual Appliance (VA) to communicate with OIPA.

### Network Requirement

Not applicable

### Service Account Permissions

Below are the service account details for OIPA application.

|  |  |
| --- | --- |
| **Environment** | **Service account name** |
| **Sandbox** | Client ID:47501341-1d61-4bae-9da3-83c714adf8e7 |
| **PROD** | Client ID: TBD |

## OIPA Source Configuration

This section depicts the OIPA application, which has been designed to correlate to the existing identity.

### Connection Details

Below are the connection details for OIPA application.

|  |  |
| --- | --- |
| Connector Details | |
| Base Configuration | |
| Source Name | OIPA |
| Description | web pour gérer les prestation d'invalidité et de vie pour les adhérants aux ass collectives |
| Connector Type | Web Services |
| Source Owner | Donald Grenier |
| Virtual Appliance Cluster | **Sandbox**: Sandbox-Cluster  **Prod**: Production-Cluster |
| Connection Settings | |
| Authentication Type | OAuth 2.0 |
| Base Url | **Sandbox**:  [https://aisf.dev-int.XYZ.ca/pir-uat3/pir-oipa-security-api/api/v1](https://aisf.dev-int.beneva.ca/pir-uat3/pir-oipa-security-api/api/v1)  **Prod**: TBD |
| Grant Type | Client Credentials |
| Token Url | **Sandbox**:  <https://login.microsoftonline.com/1392f9fc-e4e8-4bcf-bbd9-8051278854f3/oauth2/v2.0/token>  **Prod**:  TBD |
| Client ID | **Sandbox:** 47501341-1d61-4bae-9da3-83c714adf8e7  **Prod: TBD** |
| Client Secret | **\*\*\*\*\*\*** |
| OAuth Request Parameters | **Sandbox**:  47501341-1d61-4bae-9da3-83c714adf8e7/.default  **Prod**:  TBD <Client ID/.default> |
| Account Enable Status Attribute | status=A |
|  |  |
| HTTP Operations | |
| Test Connection | |
| General Information | |  |  | | --- | --- | | **Operation Name** | Test Connection | | **Operation Type** | Test Connection | | **Context Url** | /users?status=ALL | | **HTTP Method** | GET | |
| Headers | N/A |
| Body | N/A |
| Response Information | |  |  | | --- | --- | | **Root Path** | $ | | **Success Codes** | 200 | |
| Response Mapping | N/A |
| XPath Namespace Mapping | N/A |
| Account Aggregation | |
| General Information | |  |  | | --- | --- | | **Operation Name** | Account Aggregation | | **Operation Type** | Account Aggregation | | **Context URL** | /users?status=ALL | | **HTTP Method** | GET | |
| Headers | N/A |
| Body | N/A |
| Response Information | |  |  | | --- | --- | | **Root Path** | $[\*] | | **Success Codes** | 200 | |
| Response Mapping | |  |  | | --- | --- | | Schema Attribute | Attribute Path | | firstName | firstName | | lastName | lastName | | gender | Gender | | language | Language | | securityGroups | securityGroups[\*].securityGroupGuid | | clientNumber | clientNumber | | email | Email | | status | Status | |
| XPath Namespace Mapping | N/A |
| Parent Endpoint Name | N/A |
| Paging | N/A |
| Group Aggregation | |
| General Information | |  |  | | --- | --- | | **Operation Name** | Group Aggregation | | **Operation Type** | Group Aggregation | | **Context Url** | /groups/all | | **HTTP Method** | GET | |
| Headers | N/A |
| Body | N/A |
| Response Information | |  |  | | --- | --- | | **Root Path** | $[\*] | | **Success Codes** | 200 | |
| Response Mapping | |  |  | | --- | --- | | Schema Attribute | Attribute Path | | descriptionEn | descriptionEn | | groupName | groupName | | highProfileIT | highProfileIT | | description | descriptionFr | | highProfileBusiness | highProfileBusiness | | securityGroupGUID | securityGroupGUID | | status | Status | |
| XPath Namespace Mapping | N/A |
| Parent Endpoint Name | N/A |
| Paging | N/A |
| Disable Account | |
| General Information | |  |  | | --- | --- | | **Operation Name** | Disable Account | | **Operation Type** | Disable Account | | **Context Url** | /users?clientNumber=$plan.nativeIdentity$ | | **HTTP Method** | DELETE | |
| Headers | N/A |
| Body | N/A |
| Response Information | |  |  | | --- | --- | | **Root Path** | $ | | **Success Codes** | 200 | |
| Response Mapping | N/A |
| XPath Namespace Mapping | N/A |
| Disable User - Get Account | |
| General Information | |  |  | | --- | --- | | **Operation Name** | Disable User - Get Account | | **Operation Type** | Disable Account | | **Context URL** | /users?status=ALL&clientNumber=$plan.nativeIdentity$ | | **HTTP Method** | GET | |
| Headers | N/A |
| Body | N/A |
| Response Information | |  |  | | --- | --- | | **Root Path** | $[0] | | **Success Codes** | 200 | |
| Response Mapping | |  |  | | --- | --- | | Schema Attribute | Attribute Path | | firstName | firstName | | lastName | lastName | | gender | gender | | language | language | | securityGroups | securityGroups[\*].securityGroupGuid | | clientNumber | clientNumber | | email | email | | status | status | |
| XPath Namespace Mapping | N/A |
| Add Group Membership | |
| General Information | |  |  | | --- | --- | | **Operation Name** | Add Group Membership | | **Operation Type** | Add Entitlement | | **Context Url** | /users/groups | | **HTTP Method** | PUT | |
| Headers | N/A |
| Body | {  "clientNumber": "$plan.nativeIdentity$",  "securityGroupGuids" : [ "$plan.securityGroups$"]  } |
| Response Information | |  |  | | --- | --- | | **Root Path** | $ | | **Success Codes** | 200 | |
| Response Mapping | N/A |
| XPath Namespace Mapping | N/A |
| Configuration using IDN API | **Rule** : BeforeOperation-OIPA-Entitlement-AddRemove |
| Remove Group Membership | |
| General Information | |  |  | | --- | --- | | **Operation Name** | Remove Group Membership | | **Operation Type** | Remove Entitlement | | **Context Url** | /users/groups | | **HTTP Method** | PUT | |
| Headers | N/A |
| Body | {  "clientNumber": "$plan.nativeIdentity$",  "securityGroupGuids" : [ "$plan.securityGroups$"]  } |
| Response Information | |  |  | | --- | --- | | **Root Path** | $ | | **Success Codes** | 200 | |
| Response Mapping | N/A |
| XPath Namespace Mapping | N/A |
| Configuration using IDN API | **Rule** : BeforeOperation-OIPA-Entitlement-AddRemove |
| Get Account | |
| General Information | |  |  | | --- | --- | | **Operation Name** | Get Account | | **Operation Type** | Get Object | | **Context Url** | /users?status=ALL&clientNumber=$getObject.nativeIdentity$ | | **HTTP Method** | GET | |
| Headers | N/A |
| Body | N/A |
| Response Information | |  |  | | --- | --- | | **Root Path** | $[0] | | **Success Codes** | 200 | |
| Response Mapping | |  |  | | --- | --- | | Schema Attribute | Attribute Path | | firstName | firstName | | lastName | lastName | | gender | gender | | language | language | | securityGroups | securityGroups[\*].securityGroupGuid | | clientNumber | clientNumber | | email | email | | status | Status | |
| XPath Namespace Mapping | N/A |
|  |  |
| Additional Settings | |
| Create Account With "Ent" Request | true |
| Throw Provisioning Before And After Rule Exception | false |
| Throw Provisioning After Rule Exception | false |
| Throw Provisioning Before Rule Exception | true |
| Update Attribute with Change Password | false |
| Get Object Required for PTA | true |

### Aggregation Schedule

The table below shows aggregation schedule details for OIPA:

|  |  |  |
| --- | --- | --- |
| **Activity** | **Sandbox** | **Production** |
| Account aggregation schedule | On demand basis | Yes |
| Account aggregation recurring schedule | On demand basis | Daily 8AM (Recurring Every 24 hours) |
| Account Delete Threshold | 10%(Default) | 10%(Default) |
| Entitlement aggregation schedule | On demand basis | Yes |
| Entitlement aggregation recurring schedule | On demand basis | Daily 7:30AM (Recurring Every 24 hours) |

### Correlation

Correlation refers to the process of correlating, or combining, all the information discovered by IdentityNow (identity attributes, entitlements, activity, policy violations, history, certification status, etc.) to create and maintain the IdentityNow Identity Cubes. Correlation does not involve accessing external application to discover information. Correlation reviews the information contained within the IdentityNow application and updates Identity Cubes as necessary.

Table: Correlation Mapping

|  |  |
| --- | --- |
| SailPoint Attribute Name | Target Application Attribute |
| SailPoint Username (uid) | ClientNumber |

### Account Schema

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Attribute name | Type | Description | Multi-valued | Entitlement/AccountID/Name |
| firstName | String | User’s first name |  |  |
| lastName | String | User’s first name |  |  |
| gender | String | Gender |  |  |
| language | String | Language |  |  |
| securityGroups | Group | User’s security groups | Multi-valued | Entitlement |
| clientNumber | String | Id of the user |  | Account ID, Name |
| email | String | Email Address |  |  |
| status | String | Account Status |  |  |

**Table**: Account Schema Attribute Details

### Account Group Schema

OIPA source is configured to reconcile security groups. Below table lists account group schema attributes.

|  |  |  |
| --- | --- | --- |
| Attribute name | Type | Description |
| descriptionEn | String | Description in English |
| groupName | String | Name of the Security Group |
| highProfileIT | String | High Profile IT |
| description | String | Description in French |
| highProfileBusiness | String | Privileged Group |
| securityGroupGUID | String | Id of the group |
| status | String | Status of the group |

### Entitlements Glossary

A business-friendly dictionary of user access descriptions that can be associated with individual entitlements and permissions. We can use the standard import/export functionality to update the entitlement metadata (Description, Owner, etc.) in bulk. As part of OIPA, entitlement description upload is not required.

Below is the list of entitlements which must be marked as privileged in IDN.

|  |  |
| --- | --- |
| Entitlement Name | Description |
| Admin - Claims / POS | Accès à la plupart des activités d'administration des polices d'invalidité (incluant les réclamations) de même qu'à certaines activités de base pour l'administration des clients (expirer une adresse, modifier les informations du client). |
| Remun - Gestion force de vente (avancé) | Accès à toutes les fonctionnalités de gestion des intermédiaires (MGA, AGA, agents et délégués) et de rémunération dans OIPA, incluant les transactions plus avancées (ex.: Ajustement monétaire avancé).  Profil normalement réservé aux équipes de mise sous contrat et de remuneration. |

### Access Profile

An access profile is a bundle of access entitlements that represent a specific set of access for a particular source. As part of OIPA, access profile creations are out of scope.

### Roles

Roles allow you to group related sets of access, from a single source or across multiple sources, to simplify access management for your users. Roles often group access according to job functions or other shared user attributes such as departments or locations. You can then configure roles for automated provisioning or for access requests so they can be granted to your users. As part of OIPA, role-based provisioning is out of scope.

### Provisioning/De-provisioning Data Flow

Process flow showing provisioning steps are provided in the diagram below:



Process flow steps are provided in the table below:

|  |  |
| --- | --- |
| Provisioning : Data Flow Diagram | |
| Steps | **Description** |
| 1 | IdentityNow converts provisioning request to a provisioning plan |
| 2 | IdentityNow adds provisioning request in the form of provisioning plan to VA Cluster queue |
| 3 | Virtual Appliance polling Virtual Appliance Cluster queue for new work – gets the provisioning request |
| 4 | Virtual Appliance sends provisioning request to OIPA (Webservices) source connector |
| 5 | Webservices source connector converts provisioning plan to application native REST API calls |
| 6 | Webservices application allows to execute account update request |
| 7 | Webservices source executes the operation on the OIPA system by calling appropriate API. |
| 8 | Webservices Source connector converts results to provisioning plan result |
| 9 | Virtual Appliance queues provisioning result data to be sent to IdentityNow cloud |
| 10 | Decision point – what is provisioning result status?   * If success, go to step 14. * If failure, go to step 11. |
| 11 | IdentityNow marks operations for retry and increment retry (not configured) |
| 12 | Decision point – Retry max reached? (Not configured)   * If yes, go to step 13. * If no, go to step 2. |
| 13 | IdentityNow returns provisioning failure. |
| 14 | IdentityNow updates the provisioning request status on the UI |
| 15 | Account data updated with the aggregation. |

## Certification

Certification enables you to automate the review and approval of identity access privileges, account group membership and permissions, and role membership and composition. IDN collects fine‑grained access (or entitlement) data and formats the information into reports, which are routed to the appropriate reviewers. Each report is annotated with descriptive business language – highlighting changes, flagging anomalies, and calling out violations where they appear.

Identity certifications enable reviewers to approve certifications for identities or take corrective actions (such as removing entitlements that violate policy).

Role membership and composition certification enables reviewers to approve the composition of roles – the entitlements and roles that define the role being reviewed, and the identities to which the role is assigned, or take corrective actions.

As per our discussion with application team, XYZ can use the process below to review the user access.

|  |  |  |
| --- | --- | --- |
| **Req#** | **Requirement** | **Requirement Description** |
| 1 | Exclude inactive accounts | All OIPA accounts which are inactive, will be excluded from the certification campaign. |
| 2 | Individual certifier who is not the source owner or manager | Certification must be assigned to “**Ben Khemis, Atef**” who is not the source owner for the OIPA source. |

### Design

* The certification process in SailPoint allows Identities’ access privileges to be reviewed and managed by designated reviewers through system-generated Access Reviews.
* There are different types of certification configuration available in SailPoint. Manager certification and Source owner certification will be created in XYZ SailPoint environment to review user’s accesses.
* Certification Campaign will be created using out of box Manager/Source owner certification configuration. IAM Governance team will use these configurations to schedule certification periodically.

### Certification Campaign

Campaign filter is used to create a certification campaign that includes a subset of your entitlements or users.

* **Exclusion filters** exclude entitlements or identities from the campaign if they meet any of the criteria listed in the Filter Builder.
* **Inclusion filters** include the entitlements or identities from the campaign if they meet any of the criteria listed in the Filter Builder.

Below is the exclusion filter for OIPA application.

|  |  |  |
| --- | --- | --- |
| **Campaign filter Name** | **Filter type** | **Filter Builder** |
| APP\_OIPA\_CERT\_FILTER | Exclusion | Exclude non OIPA account and disabled OIPA accounts |

### Certification Email Template

Email notifications are sent to users by IDN to inform them of system or process status changes, to alert them to assigned work, and more. You can customize notification messages using variable values provided by the system through a fixed set of variables specific to the notification and global variables available across multiple email templates. SailPoint's email templates are defined using the Apache Velocity templating syntax. This allows the emails to support variable substitutions as well as simple logic like conditional contents.

|  |  |
| --- | --- |
| **OOTB Email Template Name** | **Description** |
| Certification | Sent to reviewers whenever a certification campaign is created. |
| Certification Due | Sent to certification reviewers one week after a certification campaign starts and every seven days after that, until they sign off or the campaign ends. |
| Certification Reassignment | Notifies a reviewer when they have been reassigned identities from an existing certification. |
| Remediation Work item | Sent to a user when a new remediation work item has been assigned to them. |

### Manager Certification

Managers use certifications to verify access requirements for their employees. When an administrator creates a certification campaign, it will automatically appear in their Certifications menu along with an email notification.

The table below has Certification Definition names and Corresponding Scheduled Task names, to be used as a sample.

|  |  |
| --- | --- |
| **Manager Certification Details** | **Value** |
| Name | **<<Certification Name>>** |
| Description | OIPA Manager Certification |
| Deadline | **<<Select certification end date>>** |
| Campaign filter | APP\_OIPA\_CERT\_FILTER |
| Email Options | Enable Email Notifications |
| Undecided Access Items | TBD |
| Require Comments | TBD |

**Note:** Refer to the OIPA Runbook Documents for the steps to create Manger Certification in IDN

### Source Owner Certification Campaign

The IAM solution shall support the capability to create access review task periodically for source owners to certify all access to entitlements of application accounts.

The table below has Certification configuration details, to be used as a sample.

|  |  |
| --- | --- |
| **Source Owner Certification Details** | **Value** |
| Name | <<Certification Name>> |
| Description | OIPA source owner certification |
| Deadline | TBD |
| Email Notifications | On |
| Undecided Access Items | TBD |
| Require Comments | TBD |
| Select Source(s) | OIPA |

**Note:** Refer to the OIPA Runbook Documents for the steps to create Certification in IDN

## Lifecycle change events

Below table lists the actions to be taken when Identity’s lifecycle state changes.

|  |  |
| --- | --- |
| **Lifecycle state name** | **Action performed on OIPA account** |
| Inactive | OIPA accounts are disabled |

# Conclusion

This document provides detailed design to onboard OIPA application in SailPoint IDN. We have currently promoted **16** entitlements as part of the entitlement aggregation. Further, we have also provided instructions to configure manager/source owner certification which can be further enhanced or remodeled based on certification requirements.