**Date**

kpmg.com

IdentityNow solution designXYZ Powered Enterprise

# Document control

## Change record

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Date | Revision |
| < 1.0 > | < Author Name > | < Creation Date > | < Revision Description > |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Reviewers

This document has been reviewed by:

|  |  |  |
| --- | --- | --- |
|  | Reviewer | Date reviewed |
| <Sr.No.> | <Reviewer Name> | < Review Date> |
|  |  |  |
|  |  |  |
|  |  |  |

## Approvals

This document has been approved by:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Name | Signature | Date approved |
| <Sr.No.> | <Approver Name> | <Approver’s Signature> | <Approval Date> |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1 Document control 1](#_Toc128042802)

[1.1 Change record 1](#_Toc128042803)

[1.2 Reviewers 1](#_Toc128042804)

[1.3 Approvals 1](#_Toc128042805)

[2 Introduction 2](#_Toc128042806)

[2.1 Purpose of document 2](#_Toc128042807)

[2.2 Background 2](#_Toc128042808)

[2.3 Implementation team and responsibilities 2](#_Toc128042809)

[2.4 Key project principles 2](#_Toc128042810)

[2.5 Design considerations and constraints 3](#_Toc128042811)

[2.6 Implementation methodology 3](#_Toc128042812)

[2.7 Current identity governance environment 3](#_Toc128042813)

[3 Powered enterprise key points 4](#_Toc128042814)

[3.1 Summary 4](#_Toc128042815)

[4 Business & technical requirements 7](#_Toc128042816)

[4.1 Summary 7](#_Toc128042817)

[5 IdentityNow product overview 8](#_Toc128042818)

[5.1 Introduction 8](#_Toc128042819)

[5.2 Source integration 9](#_Toc128042820)

[6 Key challenges & risks 10](#_Toc128042821)

[6.1 Key challenges & risks 10](#_Toc128042822)

[7 Solution architecture 11](#_Toc128042823)

[7.1 High level architecture 11](#_Toc128042824)

[7.2 Data architecture 11](#_Toc128042825)

[7.3 Physical architecture 11](#_Toc128042826)

[7.4 Technical architecture 11](#_Toc128042827)

[8 Solution design 18](#_Toc128042828)

[8.1 Connections 18](#_Toc128042829)

[8.2 Applications 18](#_Toc128042830)

[8.3 Application servers 19](#_Toc128042831)

[8.4 Identities 19](#_Toc128042832)

[8.5 Access 20](#_Toc128042833)

[8.6 System settings 21](#_Toc128042834)

[8.7 Security settings 22](#_Toc128042835)

[8.8 Email templates 23](#_Toc128042836)

[9 Business processes 24](#_Toc128042837)

[9.1 Joiner event process 24](#_Toc128042838)

[9.2 Mover event process 24](#_Toc128042839)

[9.3 Leaver event process 24](#_Toc128042840)

[9.4 Access request process 25](#_Toc128042841)

[9.5 Certification process 25](#_Toc128042842)

[10 Reporting 26](#_Toc128042843)

[10.1 Reporting documentation 26](#_Toc128042844)

[11 System maintenance 27](#_Toc128042845)

[11.1 Performing system maintenance & updates 27](#_Toc128042846)

[11.2 Monitoring & maintaining tasks 28](#_Toc128042847)

[12 Appendices 30](#_Toc128042848)

[12.1 Glossary of terms 30](#_Toc128042849)

[12.2 Reference documents and sources 30](#_Toc128042850)

[13 Open and closed issues 31](#_Toc128042851)

[13.1 Open issues 31](#_Toc128042852)

[13.2 Closed issues 31](#_Toc128042853)

© 2024 Copyright owned by one or more of the XYZ International entities. XYZ International entities provide no services to clients. All rights reserved.

# Introduction

## Purpose of document

The purpose of this document is to describe the IdentityNow Cloud solution to be implemented at <CLIENT> as part of the Identity and Identity Governance (IAM) Program. This document is intended solely for <CLIENT>’s internal use and is designed in accordance with the statement of work agreed upon by <CLIENT> and XYZ.

This document provides an overview of the solution being deployed covering both the technology and process sides of the IdentityNow solution covering the following areas:

* Business & Technical Requirements
* Design Considerations & Key Risks
* IdentityNow Solution Architecture & Design

## Background

The objective of this project is to transform [CLIENT]’s current Identity Governance System, replacing existing technology solutions, manual processes and standardizing for scalability.

The project will achieve this by implementing leading business processes and organizational design enabled by cloud technology. This will involve implementation of an IdentityNow Cloud solution through the implementation of Powered Enterprise solution approach. The IdentityNow platform will be hosted in the cloud by SailPoint and configured with [CLIENT] specific configuration requirements.

## Implementation team and responsibilities

|  |  |  |
| --- | --- | --- |
| Name | Company | Role/Function |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Key project principles

The key project principles are as follows:

* The Business owns the identity governance system
* The project is aligned to the strategy of simplification by making use of industry standard tools
* The project will leverage cloud technology to support the Identity Governance initiatives
* Focus on using delivered functionality to achieve business needs and not duplicating existing non-standard functionality
* Project team members will escalate risks and issues as appropriate
* Best of breed (industry) products will be used to augment the technical solution
* An operating model will be embedded, based on leading practice, with high levels of maturity across the six strands of Functional Processes, People, Service Delivery Model, Technology, Performance Insights & Data, and Governance
* XYZ "know how" will be brought into the project through the team that has practical experience of previous implementations and through predefined tools and accelerators

## Design considerations and constraints

This section is intended for any constraints and considerations that have influenced the solution design. If non-standard design approaches have been agreed upon with [CLIENT], they should be described here, referencing any relevant meetings, discussions or correspondence.

## Implementation methodology

This section aims to describe the implementation methodology that can be used during the execution of the project. The project can be implemented in multiple phases with each phase focusing on a particular aspect of the identity governance lifecycle such as onboarding authoritative sources and critical applications, performing access reviews, implementing RBAC, implementing business process such as employee/contractor lifecycle changes and access request.

## Current identity governance environment

This section is intended to provide a current state of the identity governance environment before implementation of IdentityNow. This could be a brief description of environment, referencing any cloud or on-prem technologies in place. This might also include a high-level as-is environment diagram.

# Powered Enterprise key points

**For the latest TOM assets, please refer to the** [**Insights Wiki Page**](https://deliverybackbone.kpmg.com/collaboration/display/public/SOURCE/Insights+Wiki).

## Summary

The Powered Enterprise is XYZ’s flagship offering for business transformation in the Cloud. It brings an integrated, market-leading solution to transform business functions such as finance, EPM, HR, procurement, supply chain management, marketing, sales and service, and IT.

It provides clients with a pre-defined set of business functions, pre-configured cloud technologies and the confidence to successfully navigate change. Powered Enterprise is an outcome driven business transformation solution that combines deep industry knowledge, global delivery capability and cloud technology.

This implementation followed the structure of a Powered Enterprise Implementation by leveraging a Target Operating Model (TOM) for Identity Governance that was designed with industry standards and leading best practices in mind. The TOM is broken down into six categories: Functional Processes, People, Service Delivery Model, Technology, Performance Insights & Data, and Security & Controls. These categories represent vital functions of a successful Identity Governance program and what it should reflect. A summary of each of these categories can be found below:

### Functional processes

This category of the TOM describes the Functional Processes of the TOM Tileboard. This includes a Process Taxonomy Tileboard with attached functional sub-processes that provide and end-to-end process decomposition that serves as a framework, enabling a common understanding of the end-to-end process for all stakeholders. The Taxonomy can be thought of as the bread and butter of the Powered Implementation, as it is the main value-add driver that informs the rest of the implementation program.

**[Please refer to ARIS to view latest Identity Governance Taxonomy]**

This category also includes a Maturity Model that is rated on a five-point maturity rating scale for the Identity Governance division. This helps facilitate the discussion of how mature an organization needs to be to achieve organizational goals.

**[Please refer to ARIS to view latest Identity Governance Maturity Model]**

Finally, this category also includes leading practices that provide a specific XYZ developed point of view on how a mature Identity Governance system should be designed and have a benefit that can be realized. Design consideration are significant decisions a client must make when designing a platform solution and can be accelerated with industry standards and best practices.

**Leading practices – Identity Governance**

**[Please refer to ARIS to view latest Identity Governance Leading practices]**

### People

The People category of the Powered TOM defines who is responsible for different parts of the implementation. This includes a Global Process Owners template that captures executive process governance accountability for the design of each end-to-end process. It also includes an organizational chart that shows the hierarchy and report streams of different roles - as well as a role-based job profile for each functional role with defined required skills and capabilities mapped to their position.

**For the latest TOM assets, please refer to the** [**Insights Wiki Page**](https://deliverybackbone.kpmg.com/collaboration/display/public/SOURCE/Insights+Wiki).

**[Please refer to ARIS to view latest Identity Governance Functional Position Job Profiles]**

### Service delivery model

The Service Delivery Model category defines “what” the work is that is being performed, “who” should perform the work, and “where” the work should be performed based on defined characteristics of the work. The diagram below identifies those aspects:

<<Insert CLIENT Service Delivery Model diagram>>

### Technology

The Technology category of the TOM focuses on the end-to-end processes of the underlying supporting technology application(s). Powered is unique in that it brings together predefined leading industry practices that are customized to individual organization’s based on their requirements. The Supporting Technology Overlay gives a high-level glimpse of the supporting technologies and how they interact together within respect of the TOM.

Further description of the Technology component, including Physical and Environment architectures is discussed later in this document.

**[Please refer to ARIS to view latest Identity Governance Supporting Technology Overlay]**

### Performance insights & data

Performance Insights & Data is centered on reporting and reporting tools. This primarily revolves around KPI’s that are used to measure the health of an organization’s Identity Governance initiatives. These KPI’s were designed around industry leading standards and practices.

**[Please refer to ARIS to view latest Identity Governance Key Performance Indicators (KPIs)]**

### Governance

#### Security & controls

The Security and Controls category is concerned with key controls and risks to be identified and mitigated in processes that includes governance, risk and compliance (GRC) and automated intelligence (AI) opportunities. These controls are based off of industry standards such as NIST, ISO, and OWASP.

**[Please refer to ARIS to view latest Security & Controls]**

# Business & technical requirements

## Summary

Business and Technical Requirements were collected in a series of interviews with project stakeholders to understand the needs and success factors for an optimal IdentityNow implementation. Those requirements were used in the design of the IdentityNow solution for <CLIENT>. These requirements are as follows:

### Business requirements

This section describes the business requirements of the IdentityNow implementation.

|  |  |
| --- | --- |
| Requirement ID | Requirement description |
|  |  |
|  |  |
|  |  |
|  |  |

### Technical and functional requirements

This section describes the technical and functional requirements of the IdentityNow implementation.

|  |  |
| --- | --- |
| Requirement ID | Requirement description |
|  |  |
|  |  |
|  |  |
|  |  |

# IdentityNow product overview

## Introduction

SailPoint IdentityNow is a full-featured, cloud-based identity governance solution that delivers password management, provisioning, access request, and access certification services for cloud, mobile, and  
on-premises applications. The SailPoint IdentityNow platform brings you the power of enterprise-grade identity governance coupled with the agility and convenience of the cloud. Identity services can be rapidly deployed, and administration can take place from anywhere at any time.

### Access certification

Automate the process of reviewing and reporting user access privileges across the organization. Quickly plan, schedule and execute comprehensive campaigns to ensure all types of users have the appropriate access to corporate resources.

### Provisioning

Enable business users to be productive from day one. Streamline onboarding and off-boarding process with best practice configurations and workflows, enabling IT to automatically manage user access to the applications they need to perform their job.

### Access request

Empower the entire business with a self-service platform for requesting and approving access to applications, collection of entitlements within applications or application bundles, called “roles.” IdentityNow secures and automates the access request process and frees IT to work on strategic projects while quickly delivering business users the access they need to do their jobs.

### Password management

Offer business users an intuitive, self-service experience for managing and resetting their own passwords from any location and on any device, on- or off-network. Leveraging industry best practices, such as sequential multi-factor authentication, this service enforces consistent and secure password policies across all systems and users in the business, while eliminating helpdesk calls and strengthening your security posture.

### Artificial intelligence and machine learning

Apply advanced governance capabilities, using the power of SailPoint Predictive Identity to discover suspicious or anomalous access, maintain continuous compliance and enjoy greater productivity across the entire organization. Utilize generated insights and recommendations to help guide decisions around your security and compliance related efforts.

### File access management

Extend your identity governance capabilities to control access to sensitive data with SailPoint File Access Manager. Provided as an extension to the IdentityNow platform, you can discover where sensitive data resides, apply appropriate access controls to improve security, mitigate compliance risks, and support greater efficiency across on-premises or cloud storage systems.

### Connect to everything across your hybrid IT environment

The power of IdentityNow resides in its ability to connect to applications, mainframes, cloud infrastructure, and data sources from across a hybrid IT environment. IdentityNow also provides standards-based connectors to additional applications that leverage information exchange protocols such as REST, SCIM, JDBC, CSV and LDAP.

### Cloud platform services

* **Updates and Patching** – Updates are pushed seamlessly without the need for system downtime
* **Scaling** – Easily add users and dynamically scale to fit changing organizational needs
* **Alerting** – SailPoint provides proactive notifications of added services or status updates
* **Monitoring** – SailPoint delivers 24/7 oversight and support

### Meets security standards

SailPoint eliminates the need for organizations to choose between security or convenience. We’ve architected IdentityNow around fundamental principles that ensure best of breed security practices:

* Meets security standards ISO 27001:2013 and SOC 2 Type 2
* Allows your business-critical data to stay where it belongs, behind your firewall
* “Zero Knowledge Encryption” protects administrative access and interaction with external systems



## Source integration

IdentityNow offers a one-stop solution for identity governance on a variety of target systems through its wide range of application sources/connectors. IdentityNow application sources/connectors provide interfaces to the managed resources for reading user account data and provisioning changes from IdentityNow down to target IT systems and applications. IdentityNow offers two types of sources/connectors which enable the connectivity between IdentityNow and target system.

A detailed overview of IdentityNow’s supported connectors and their associated operations is available here: [Supported Connectors for IdentityNow - Compass (sailpoint.com)](https://community.sailpoint.com/t5/IdentityNow-Connectors/Supported-Connectors-for-IdentityNow/ta-p/80019).

# Key challenges & risks

## Key challenges & risks

As part of the discovery phase for [PROJECT] the [CLIENT] and XYZ team identified key challenges and risks to the project’s success. These can be found below:

### **Key challenges**

Below are some of the key challenges identified during assessment of the project implementation plan:

|  |  |
| --- | --- |
| No. | Challenge |
| KC-1 |  |
| KC-2 |  |
| KC-3 |  |
| KC-4 |  |

### Key risks

With any transformation, there will be factors that pose risks. Some perceived risks to this implementation are as follows:

|  |  |
| --- | --- |
| No. | Summary |
| KR-1 | Project may be delayed by unforeseen circumstances |
| KR-2 | Regular and unobstructed supply of data feeds from integrated applications |
| KR-3 | Legacy technology components lack extensibility |

# Solution architecture

## High level architecture

The following diagram illustrates the high-level architecture for the solution:



<< insert client specific high-level architecture at time of implementation >>

## Data architecture

The following diagram illustrates the data architecture for the solution:

<< insert client specific data architecture diagram >>

## Physical architecture

The following diagram illustrates the data architecture for the solution:

<<insert CLIENT Physical Architecture Diagram>>

## Technical architecture

### URL for SailPoint IdentityNow

|  |  |
| --- | --- |
| Domain registrar | --- |
| Primary domain registered |  |
| IdentityNow sub-domain URL |  |
| Sandbox | Client specific |
| Production | Client specific |
| Security | TLS, HTTPS |
| Supported private keys | 2048 bit keys |

### Virtual appliance

SailPoint IdentityNow is a SaaS solution, therefore it does not require traditional on-premise deployments. However, to enable communication between IdentityNow and the source systems in the <CLIENT> environment, it is necessary to deploy a Virtual Appliance (VA).

A virtual appliance (VA) is a Linux-based virtual machine that connects to the organization’s sources and apps using APIs, connectors, and integrations. Each SailPoint VA is deployed on the organization’s infrastructure and managed by SailPoint.



While SailPoint doesn’t connect directly to the VA, each VA must be able to make continuous outbound-only calls to the cloud environment to execute actions such as installing patches and updating images. SailPoint moreover have monitoring built in to alert us when a VA goes down.

**Location**

To ensure a reliable connection between a VA and the source system, the VA will be located locally on the <CLIENT> environment where each cluster will be installed in close proximity to the connected source system(s).



The IdentityNow virtual appliances will be rolled out on VSphere 6.5 server virtualization software and machines.

**Cluster Size**

To ensure connectivity during updates and based on SailPoint recommendations, <CLIENT> will deploy at least **two virtual appliances** per cluster, enabling the VAs to take turns updating.

To support the sandbox environment, the ‘**<CLIENT> SB Cluster**’ has been set-up, including two dedicated virtual appliances:

* VA-XXXX
* VA-XXXX

**Virtual Machine Ratio**

To avoid a single point of failure in the environment, a 1:1 ratio of virtual appliance to virtual machine will be maintained. To build in fault tolerance, the local VAs will be configured in the same cluster to run on different servers whenever possible.

The virtual machines defined to host the virtual appliances have the following IP-address:

* Client specific
* Client specific

**Sandbox and Production Clusters**

<CLIENT> will set-up two environments will closely monitor the sandbox VA clusters and test any connectivity changes before they go to production.

### VA configuration

This section provides an overview of the selected configuration option, where <CLIENT> has chosen to go with the ‘*Standard Configuration*’.

*Standard* is the default VA configuration option, as it allows the VA to connect to SailPoint and other required endpoints directly through the firewall. There is no additional setup required to achieve connectivity after the network requirements are met.



### System and network requirements

#### VA image size

A virtual appliance is a Virtual Machine Image (VMI) that is designed and packaged to be deployed on a VM platform. A VMI is a self-contained package that consists of a software stack and metadata. The software stack consists of a set of pre-configured applications, the guest OS, middleware, libraries, containers, and all of the other required software, while the metadata represents information that can assist in the deployment and execution process of the VMI on the VM platform.

Packaging applications in the form of virtual machine desk images are used to facilitate the distribution, installation, configuration, management, and execution of applications under an optimal VM platform. This also improves the application’s portability and allows workload migration. The requirements for the virtual machines have been detailed below.

|  |  |
| --- | --- |
| Minimum | Recommended |
| 1 processor 8 GB memory 128 GB storage | 2 processors 16 GB memory 128 GB storage |

#### Ports

Network proxy, security, firewall, or caching products such as Websense can interfere with the VA. To avoid this problem, all outbound traffic to any destination must be allowed, through the ports specified in the network requirements.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Port | Reason | Direction | IP addresses | Description |
| 53 | DNS | Outbound | All | Used for name resolution |
| 123 | NTP | Outbound | All | Used for time synchronization. You can [configure a local NTP server](https://community.sailpoint.com/t5/Connectors/Virtual-Appliance-Reference-Guide/ta-p/74641#localNTPServer) instead of using the default |
| 22 | SSH | Inbound | Internal Only (Recommended) | Only required if you want to SSH into or copy files onto the VA |
| 443 | HTTPS | Outbound | All | Used for all HTTPS communication (source endpoints and/or update endpoints) |

By default, virtual appliances are configured to communicate with external network time protocol (NTP) servers using port 123. If you do not want to allow outbound access for port 123, you can configure the virtual appliances to communicate with NTP servers behind your firewall.

Each virtual appliance must be configured individually. While you do not have to configure every virtual appliance to use your NTP server, you cannot close port 123 until all of the virtual appliances have been configured to use internal NTP servers.

### VA deployment

This section discusses strategy for deploying the VA, beyond the basics of selecting a local or cloud virtualization environment.

**High Availability and Disaster Recovery**

High Availability means ensuring that there are enough VAs running to meet the processing needs of the business, as well as sufficient redundancy to be able to compensate for a single VA becoming temporarily unavailable due to an upgrade process, loss of connectivity, or other activity that could otherwise result in downtime.

Disaster Recovery means making sure that the organization has VAs deployed in more than one location, as part of a failover strategy that ensures business continuity in the face of a disaster (natural or otherwise).

<https://community.sailpoint.com/t5/IdentityNow-Connectors/Virtual-Appliance-Planning-and-Best-Practices/ta-p/78056>

**DMZ Deployment**

This section will describe the network architecture of the DMZ if it exists.

### IQService

IQService, also referred to as the Integration Service, is a native Windows service that enables IdentityNow to participate in a Windows environment and access information only available through Windows APIs. It is a lightweight service that must be installed on any supported Windows Server that has connectivity to the target systems you want to manage in IdentityNow. IQService allows IdentityNow to make updates (write operations) for new/modified users on the Active Directory domain(s).



**IQService Prerequisites**

Minimum software and hardware requirements have been defined to ensure the basic working of IQService with an average processing load, when used with one application. The requirement proportionately increases with an increase in the request processing load and number of applications it caters to.

* Operating Systems:
* Microsoft Windows Server 2012 (R2) / 2016 / 2019
* .NET Framework:
* Minimum .NET Framework version required 4.5.2
* Hardware:

|  |  |
| --- | --- |
| Component | Minimum hardware requirement |
| CPU | 1-Core |
| RAM | 500 MB |
| Free Disk Space | 250 MB |

**IQService Service Account**

The service account defined in the IdentityNow source that connects to IQService, is used for provisioning operations, aggregation (terminal services attributes/Skype attributes), and server-less binding for respective target system.

For the Active Directory connector, the user must be a Local Administrator and an Account Operator or Domain Administrator in Active Directory. Moreover, Windows PowerShell 3.0 must be in place and the Domain Controller must be accessible from IQService host computer.

User Account:

**Ports Used with Active Directory Integrations**

The IQService provisioning agent calls functions exposed by Microsoft’s .net packages that are a “black box” that communicate to Active Directory indirectly. IdentityNow does not control what port numbers these APIs leverage to interact with Active Directory. Microsoft publishes a list of ports that the .net API and ADSI interfaces use to communicate with an Active Directory server. Were a firewall to be placed between IQService and the Active Directory domain controllers it would need to be exceedingly permissive by opening a large number of dynamic ports.

The IQService agent uses a sub-set of these ports documented by Microsoft. For communication between IQService and a domain controller SailPoint recommends at least the following ports must be opened:

* LDAP Ports 389 and 636
* Kerberos port 88
* Active Directory Web Services 9389
* Active Directory port 3268
* Active Directory port 3269
* Active Directory DNS port 53
* Active Directory Replication, Login services port 445
* Kerberos Passwords, port 464
* Authentication port UDP 137
* Authentication port TCP 137

# Solution design

## Connections

### Active directory

The Active Directory target system will be integrated with the IAM solution using the specific direct connector provided out of the box by SailPoint. To use this connector, it is required to use IQService, which is a native Windows service that enables IdentityNow to participate in a Windows environment. Once installed, all the existing accounts and groups can be managed by and through IdentityNow.

**Connection data**

To be able to correctly use the IDN connector to Active Directory, it is necessary to configure the source fields existing inside the IdentityNow connector:

| Field | DEV value | PROD value |
| --- | --- | --- |
| Forest Configuration |  |  |
| Domain Configuration |  |  |
| Search DN |  |  |
| IQService Host |  |  |
| IQService Port |  |  |
| IQService User |  |  |
| IQService Password |  |  |

### Authoritative source

An authoritative source is a system which is the “source of truth” for (a piece of) identity information. Using authoritative sources, we can ensure that the consistency and integrity of identity attributes are maintained across different systems, which in turn governs access for identities within those systems.

This section describes the authoritative source that are in the <Client> system.

## Applications

Applications often require different processes for the purposes of service fulfillment, both automated and manual. This section describes the applications to integrated with IdentityNow.

### Application A

Short explanation of what application is and the integration pattern it will follow. (JDBC, Webservice connector, Delimited file). Will it be using API’s to pass information? All pertinent information to specific application should be presented here.

### Application B

Short explanation of what application is and the integration pattern it will follow. (JDBC, Webservice connector, Delimited file). Will it be using API’s to pass information? All pertinent information to specific application should be presented here.

### Application C

Short explanation of what application is and the integration pattern it will follow. (JDBC, Webservice connector, Delimited file). Will it be using API’s to pass information? All pertinent information to specific application should be presented here.

## Application servers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Application name | Server / Hosts names | OS | Hardware specification | IP address |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Identities

### Administrative roles

Administrators (or admins) are SailPoint IdentityNow users with the permission to access the IdentityNow administration dashboard. Admin access can be granted to all sections of the application or limit their access to only certain modules. IdentityNow Admin Roles will be assigned to individuals based on job function and need.

Main administrator accounts are uploaded through a separate flat file and do not require authentication from AD to log in.

**Administrative Users:**

* <<TBD based on specific requirements>>
* SailPoint Services
* SailPoint Support

### Identity profiles

An identity profile represents the identity information loaded from a specific, authoritative source, the authentication method assigned to users from that source, and a variety of other information specific to that group of users. It also loads the users from the specified source into the system as identities.

**Active Directory**

To load the accounts, the attribute “sAMAccountName” in the active directory accounts will be used to correlate with the corresponding identity defined in IdentityNow.

**Authoritative Source**

The following table provides the mandatory attributes needed from authoritative source to integrate the HR system into IdentityNow to map with the identity profiles.

|  |  |
| --- | --- |
| Attribute | Description |
| First Name (firstname) | Given name |
| Last Name (lastname) | Alias |
| Work Email (email) | Email |
| SailPoint User Name (uid) | Username in IdentityNow |

### Reconciliation process

A reconciliation is the reading process performed by IdentityNow to update the information of accounts, group or any kind of available objects in the targets systems.

In order to keep all the information updated in the Identity Manager, it is necessary to read this information on a daily basis from the authoritative sources and the different target systems (Active Directory, Business Applications, etc.). During the reconciliation process, every account should be correlated with an identity following the custom-defined correlation rules.

### Governance groups

A governance group is a group of users that can make governance decisions. Currently, these decisions center around Access Requests. A governance group can determine whether the access level is appropriate for the user requesting that access.

Before reviewing access, a governance group must be configured and have members. The group structure provides both control over who will see the request and flexibility beyond a single reviewer. When it's a group's turn to review an access request, everyone in the governance group will receive the access request, and only one member of the group needs to approve or revoke it.

## Access

### Access profiles

An access profile is a group of one or more entitlements that grants a specific set of access rights associated with a source. One of the fundamental benefits of access profiles is that if an identity has all of the entitlements in an access profile, those entitlements are automatically bundled together as an access profile. Any apps associated with it are added to their Launchpad automatically.

### Roles

A role is a name for a bundle of access that you can grant to an employee or group of employees in the system. When users are granted a specific role within IdentityNow, they will receive the specific access profiles relevant to their position.

### Access profiles and role reconciliation

IdentityNow manage the user rights to the targets system. To be able to maintain this access and perform the different subprocess, it is mandatory to reconciliate ServiceNow daily because the information about this roles and profiles are storage in it.

## System settings

### Product branding

**User Interface**

The IdentityNow user interface allows for very basic branding to be applied such as the company logo and color scheme.

* The Product Name has been set as ‘**<CLIENT> IdentityNow**’
* The color scheme of the solution has been defined as the following values:
* Navigation Bar Color: **###**
* Action Button Color**: ###**

**Email Notification Branding**

By default, the emails generated by IdentityNow follow a basic format. IdentityNow has a basic email editor but we recommend lining up a resource with basic HTML editing skills to assist further in the project for more complex email customization such as changing links, variables, and performing logic.

### Usage agreement

<CLIENT> can define a usage agreement that applies to the IdentityNow application. When enabled, the system prompts users to accept the terms based on their status in the system.

When using certain apps, an end-user may need to accept a usage agreement to remind them when the company has specific policies related to the use of the specific application. Usage agreements might include confidentiality agreements or restricted usage guidelines, such as prohibitions on storing confidential data in that particular app. These policies are set by the IT administrator.

### Network settings

**Network Definition**

The organization might need to define network IP address blocks using the Network Definition panel for several reasons. For example, you might want to:

* Define the scope of the network if you're using Integrated Windows Authentication (IWA). Users on any network, including VPNs, configured using this procedure will be automatically signed in when they go to your IdentityNow site or any app on their launchpad. Any network not configured using this procedure will automatically use the normal sign in window and process
* Require strong authentication for any users who are not on your network, for apps or for signing in to IdentityNow
* Prevent the user from launching certain apps at all if they are not on your network
* Restrict access to the IdentityNow sign in page for users who are not on your network

**Trusted Countries**

It is possible to configure an application to require strong authentication when a user's IP address is located in a country that have been designated as untrusted. The organization can define untrusted countries using the following methods:

* *Add countries to a blacklist* - The blacklist defines the countries that are untrusted
* *Add countries to a whitelist* - The whitelist defines the countries that are trusted. As a result, any countries that are not on this list are designated as untrusted

### System notifications

<CLIENT> can configure IdentityNow to send all <CLIENT> IdentityNow Admins an email when certain components of the organization aren't working properly. Notifications have been enabled for **Applications**, **Sources** and **Virtual Appliances**.

## Security settings

### Security questions

IdentityNow allow users to answer security questions as a form of strong authentication. This might be appropriate for password resets or step-up authentication for apps that require it:

* Number of questions from master list that must be set up by user
* Number of questions a user must answer correctly to authenticate

### Integrated Windows Authentication (IWA)

Integrated Windows Authentication (IWA) refers to a configuration that provides a true single sign-on experience for all users' Launchpad apps without the need to enter a separate SailPoint password.

### Lockout management

IdentityNow lockout settings are designed to protect users' accounts from brute force attacks by tracking the number of times a person fails to verify their identity correctly.

**Sign in Lockout Settings:**

* Maximum Attempts
* Minutes Until Attempt Count Resetz
* Minutes User is Locked Out

**Password Reset Lockout Settings:**

* Maximum Attempts
* Minutes User is Locked Out

### Session management

<CLIENT> can configure the IdentityNow default session lengths by changing them to values more suitable for the specific organization's environment.

* Maximum Session Length: **\_\_ hours,** sessions end when the user closes the window
* Idle Session Expiration: **\_\_ minutes**

### Redirect patterns

Redirection allows an organization to configure a federated app to sign out of IdentityNow and send users to a different website when they sign out of the app. Redirect patterns allow you to define which websites are safe for your users to be redirected to. By identifying safe redirect patterns in IdentityNow, you can control where your users are allowed to go when they sign out of IdentityNow.

### Service provider

To be defined for SAML authentication.

To use SAML to authenticate into IdentityNow, <CLIENT> can use one of many SSO solutions as an identity provider and IdentityNow as a service provider. Users can authenticate into their identity provider, then federate into IdentityNow to do their work:

* The Entity ID
* The Login URL for Post
* The Login URL for Redirect
* The Logout URL (optional)

The Signing Certificate:

## Email templates

Email notifications are generated automatically and sent to end users generally triggered by a process. IdentityNow supports custom email templates as a way for individual corporations to customize their email templates to meet their company’s communication standards. Custom templates created for this implementation are found in the table below:

|  |  |
| --- | --- |
| Name | Description |
|  | |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |

<<insert image or example of custom template for client>>

# Business processes

**For the latest TOM assets, please refer to the** [**Insights Wiki Page**](https://deliverybackbone.kpmg.com/collaboration/display/public/SOURCE/Insights+Wiki)**. The images below are for reference only and may not reflect the latest TOM updates.**

Business processes contain a sequence of steps or activities and are typically triggered by an event in such as editing a role or updating a user identity. This section will describe custom business processes that will be implemented to support <CLIENT>’ Identity Governance business requirements.

## Joiner event process

Graphical user interface, application, Word

Description automatically generated

For a detailed explanation of the process flow, we refer to the Target Operating Model.

## Mover event process

A picture containing diagram

Description automatically generated

For a detailed explanation of the process flow, we refer to the Target Operating Model.

## Leaver event process

Graphical user interface, diagram, application

Description automatically generatedFor a detailed explanation of the process flow, we refer to the Target Operating Model.

## Access request process

Diagram

Description automatically generatedFor a detailed explanation of the process flow, we refer to the Target Operating Model.

## Certification process

Graphical user interface, application

Description automatically generated

For a detailed explanation of the process flow, we refer to the Target Operating Model.

# Reporting

## Reporting documentation

Please see reporting deliverable document for reports utilized in this implementation.

# System maintenance

This section provides an overview of the system maintenance tasks that need to be performed periodically.

## Performing system maintenance & updates

### IdentityNow platform update validation

Perform the following validations to ensure that the IdentityNow platform is working correctly following any upgrades to the IdentityNow infrastructure:

* Check Virtual Appliance Health - Validate that VA clusters have a status of **Connected**
* Check the health of sources:
* Check the System Status dashboard to validate that no errors are displayed on sources
* Navigate to a source and click **Test Connection**, ensure that the **Connected** message is displayed
* Validate that user/group aggregations are functioning appropriately
* Validate user password resets in IdentityNow are working as expected
* For JDBC Sources, validate that Discover Schema operates as expected

### Virtual appliance updates

Virtual appliance updates are managed by SailPoint. When a VA image is updated, it is deployed in a cluster on a rolling basis followed by a reboot of the VA. Ensure that there are at least two VAs per cluster in order to maintain connectivity with sources during the VA updates. If any VA in a cluster is down, no software or maintenance updates are made to any of the VAs in that cluster.

### Monitoring virtual appliance infrastructure

IdentityNow has the following features available to monitor VA health:

* **Notifications** - Configure IdentityNow to send an email when a VA goes down
* **Admin Dashboard** - Cluster’s tile of the system components status panel
* **Virtual Appliance Clusters page** - Navigate to **Admin > Connections > Virtual Appliances** to see the status of VA clusters. Click on a cluster name and select **Virtual Appliances** to see the status of that cluster's VAs

#### VA cluster status

The Virtual Appliances page displays the following information about clusters:

* **Pinned** - This column displays "Yes" when a cluster is configured to a specific CCG version and is not being updated automatically
* **Configured CCG Version** - This column displays the version of the Cloud Connector Gateway (CCG) that the VA cluster is configured to use. This could be the pinned CCG version, or the latest CCG version that has been automatically updated

**Status** - This column displays the current status of the cluster, based on the following options:

* **Normal**- All VAs are operating as expected
* **Configuring** - At least one VA in the cluster is in the configuring state
* **Warning** - At least one VA in the cluster is in the Warning state, has a configuration warning, or has failed
* **Failed** - All of the VAs in the cluster are in the Failed state

**Alerts** - This column displays the appropriate alert in each of the following scenarios:

* **Limited Resources** - There is only a single VA in the cluster. (A minimum of two VAs in the cluster is required for the cluster to operate effectively
* **No active appliances** - There are no VAs in the cluster

#### Review the VAs connected to a source

Complete the following steps to review the VAs connected to a specific source:

1. In the Admin interface, click **Connections > Sources**
2. Click the source to be reviewed
3. Click the **Connections** tab. The VA cluster connected to the source is displayed under **Virtual Appliance**
4. Click the cluster name to view more details about the cluster

#### Review the sources connected to a VA

Complete the following steps to review the sources connected to a specific VA:

1. In the Admin interface, click **Connections > Virtual Appliances**
2. Click the cluster name you want to review
3. Click the **Connections** tab. The names of all sources connected to the cluster and what they are used for are displayed
4. To make changes to a source connection, click the Edit icon for the source

## Monitoring & maintaining tasks

Perform the following steps in order to monitor the status of tasks and if necessary, perform troubleshooting:

1. In the Admin interface, navigate to **Dashboard > Monitor**
2. Review the list of **Active Queues** and **Active Jobs**
3. Validate that the status of each task is **Success**
4. If the status of a task is **Failure**, navigate to the Source and ensure that connections between the source and IdentityNow are operational. If there are any issues with identity correlation, then the data field issues need to be identified and resolved before the task is re-executed
5. If the status of a task is **No Activity**, navigate to the Application, ensure that all configurations  
   are correct
6. Execute the task in order to ensure that the issue has been resolved

# Appendices

## Glossary of terms

|  |  |
| --- | --- |
| Name | Description |
| Active Directory | Active Directory (AD) is a directory service that Microsoft developed for the Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management |
| AD | Active Directory |
| Admin | An abbreviation of administrator. This is the individual(s) who have access to the IdentityNow Administrator Dashboard. They control the provisioning and deprovisioning of end users, the assigning of apps, the resetting of passwords, and the overall end user experience. Only administrators have the Administration button on the upper right side of the My Applications page |
| HRM | Human Resource Management |
| IAM | Identity and Access Management |
| IDN | IdentityNow |
| IG | Identity Governance |
| LDAP | Lightweight Directory Access Protocol (LDAP) is a lightweight client-server protocol for accessing directory services, specifically X.500-based directory services. LDAP runs over TCP/IP or other connection-oriented transfer services |
| SaaS | Software-as-a-Service |
| SAML | An acronym for Security Assertion Markup Language, SAML is an XML-based standard for exchanging authentication and authorization data between an identity provider (IdP) and a service provider (SP) |
| SSO | An acronym for single sign-on. In a SSO system, a user logs in once to the system and can access multiple systems without being prompted to sign in for each one |
| VA | Virtual Appliance |
| VM | Virtual Machine |

## Reference documents and sources

The documents listed are available in conjunction with this document.

# Open and closed issues

## Open issues

Note: The open items should not impact the document approval.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Issue | Resolution | Responsibility | Target date | Impact date |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Closed issues

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Issue | Resolution | Responsibility | Target date | Impact date |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | Contact us  Name Surname  **Sector name**  T +1 (0)00 [0000 0000]  E name.surname@XYZ.com  Name Surname  **Sector name**  T +1 (0)00 [0000 0000]  E name.surname@XYZ.com  Name Surname  **Sector name**  T +1 (0)00 [0000 0000]  E name.surname@XYZ.com  www.XYZ.com |  |  | |  |  |  | | **kpmg.com/powered**  **kpmg.com/socialmedia**  **kpmg.com/app** | | | | The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.  © 2024 Copyright owned by one or more of the XYZ International entities. XYZ International entities provide no services to clients. All rights reserved.  The XYZ name and logo are registered trademarks or trademarks of XYZ International. | | | |  |  |