



WHITE PAPER
SERVICE DESCRIPTION FOR
IDENTITY & ACCESS MANAGEMENT
APPLICATION
ON SERVICENOW

Public document



Appmore Ltd

<https://appmore.com> | info@appmore.com | +358 (0)9 4282 7663

Copyright© 2024 by Appmore Ltd

All Rights Reserved.

No part of this document may be reproduced, transmitted, transcribed, stored in an electronic database, or translated into any language, in any form by any means, without prior written permission of Appmore Ltd.

The information in these documents is subject to change without notice. Products or corporate names may be trademarks or registered trademarks of their respective companies and are used only for the explanation and to the owner's benefit.

There is no warranty of any kind for the accuracy or usefulness of this information except as required by applicable law or expressly agreed in writing.



CONTENTS

Executive summary	4
Why should we invest in IAM?	5
Reduce IT risks.....	5
Other benefits of ServiceNow IAM solution	5
Concepts of IAM	6
Identities, accounts and access rights	6
Job roles.....	7
Approvals	7
Example approval flows	8
Critical Access Combinations and segregation of duties.....	9
Unauthorized access	9
Employment lifecycle	10
Onboarding (joiner)	10
New employee.....	10
New non-positioned external user	10
Example new employee workflow.....	10
Requesting additional Access and Job Roles	11
User information updated (mover)	12
Terminations (leaver) and long leaves	13
Workflow orchestration	14
Reconciliation.....	14
Automated fulfilment.....	15
Manual fulfilment.....	16
Access certification	17
Recertification	17
External user audit	17
Privilege access review	17
Identity analytics and reporting.....	18
User profiles.....	18
Reporting and dashboards	19
List of features	20
More information	22

EXECUTIVE SUMMARY

Identity and Access Management (IAM) is a critical framework of policies and technologies that ensures the right individuals in an organization have appropriate access to technology resources. Implementing IAM correctly can significantly increase productivity by streamlining user provisioning and deprovisioning, thereby reducing administrative overhead and enabling seamless access to resources. IAM also unifies processes and practices globally, encompassing both internal employees and external personnel.

IAM enhances security by guaranteeing that only authorized users have access to critical systems and data, mitigating the risks of data breaches and insider threats. Additionally, it supports improved compliance with regulatory standards such as GDPR, NIS2, and ISO27001 by enabling the tracking and auditing of user access, ensuring data privacy and integrity.

The ServiceNow IAM application brings the right technology to efficiently enforce policies across an entire organization. It automates the IAM lifecycle from access request to verification, creation, monitoring, and eventual removal. Using a SaaS platform like ServiceNow allows users to request access rights through an intuitive Service Portal, eliminating the need for outdated email or legacy solutions. Managers can easily handle both indefinite and temporary access, ensuring unnecessary access is promptly deprovisioned.

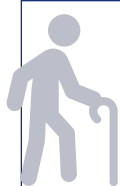
IAM also provides cost savings by automating access management and reducing security incident risks, lowering operational costs and potential fines for non-compliance. It enhances user experience by offering faster access provisioning, day-one access, visibility, self-service capabilities, and ultimately improving employee satisfaction.

For companies in Europe or operating in the European market, IAM is indispensable for GDPR compliance, as it tracks which systems hold personal identifiable information (PII) and who has access to it. IAM facilitates the creation of comprehensive reports for audits, providing detailed information on identities, accounts, and accesses. It simplifies the management of access rights and ensures the timely removal of unnecessary access, thereby supporting both managerial and security department needs.



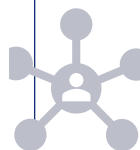
WHY SHOULD WE INVEST IN IAM?

REDUCE IT RISKS



All access and identities will be removed when user leaves the company

- Avoid risk of former employees stealing company secrets, corrupting information or sharing sensitive data to public



Only users who need to have access to certain system has access

- Minimize risk of exposing sensitive data to users who do not need to know



Traceability of who has had the access to system at certain point of time

- If someone from the organization shares sensitive data to public, you can find out who has had the access during this breach



Pass internal and external audits

- Extensive reporting with ServiceNow reporting tools



Comply with GDPR regulations

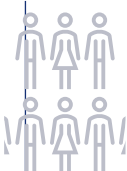
- Fines for not complying with GDPR can be 4% of annual global turnover or €20 million – whichever comes first



Prevent critical access combinations

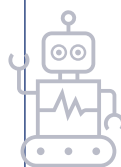
- To avoid fraud, theft and error, critical access combinations should be monitored so single person is not able to solely complete task which constitutes a risk e.g. payment and approval of invoice

OTHER BENEFITS OF SERVICENOW IAM SOLUTION



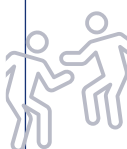
Simplify the lives of end users

- Employees, partners, contractors, customers and guests can easily access systems
- Less security issues, better compliance, reducing IT administrative workloads, lowering breach-related expenses



Automation

- External user access scheduled for contract period
- Productivity gains for example when onboarding
- No 3rd party integrations between IAM and ITSM needed



Ease of use

- One portal and one approval engine
- Thanks to IAM, people can get an identity that provides access to different systems
- Identity changes will affect automatically to access rights



Reduced IT cost

- Less work even with improved security and control
- Fewer access requests to service desk
- Lower TCO compared to on-prem or standalone IAM



Software as a Service

- No hardware cost
- Latest version and automated security upgrades
- Scalability of cloud
- High availability
- Better enterprise architecture



Business changes

- Changes when promotion, transfer or layoffs occur will be more efficient and less risky
- Acquisition and mergers handled fast and efficiently identity wise

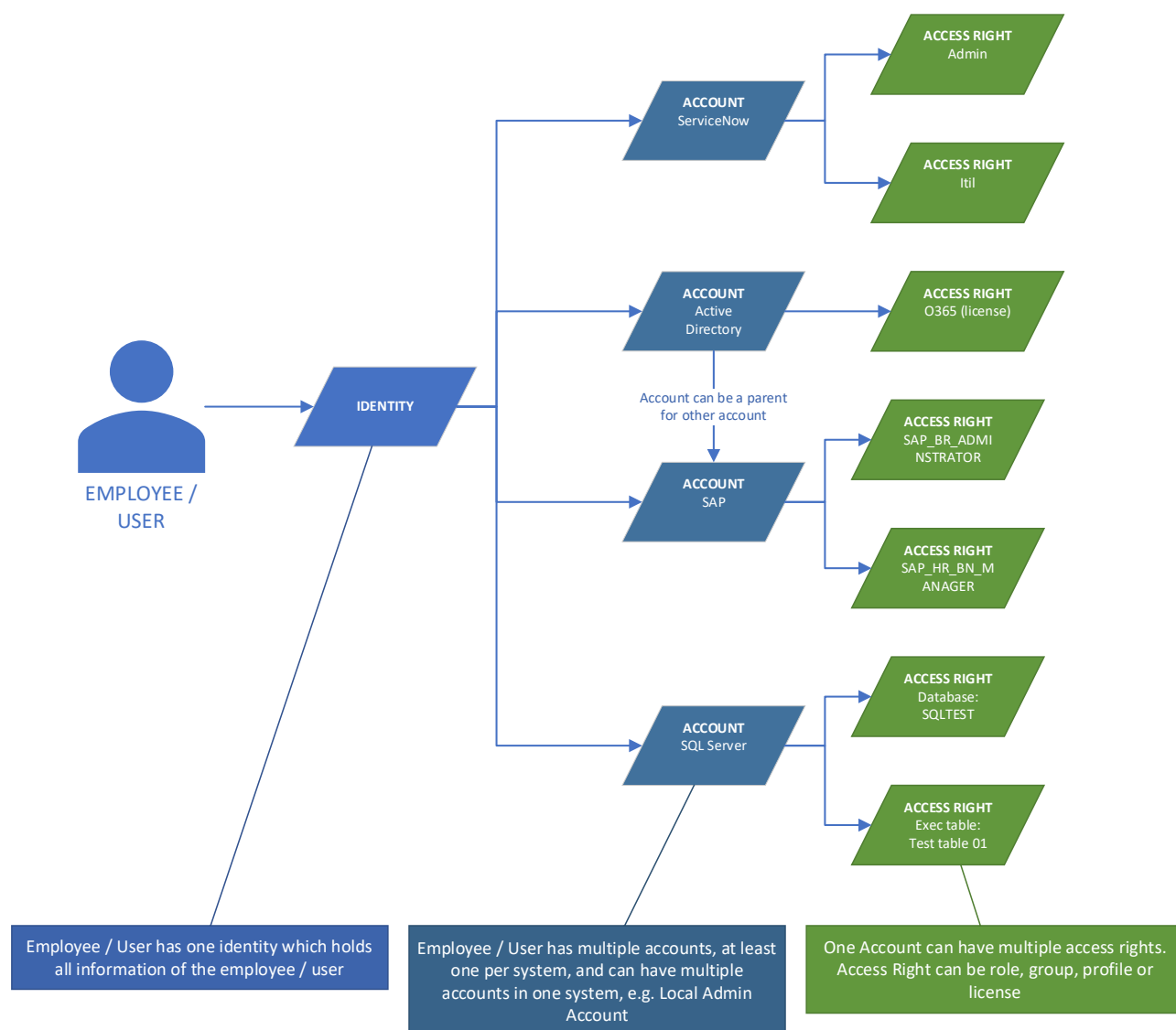


CONCEPTS OF IAM

IDENTITIES, ACCOUNTS AND ACCESS RIGHTS

A person's identity is conjunctive information for one specific person, and this involves information such as first name, last name, email address, etc...

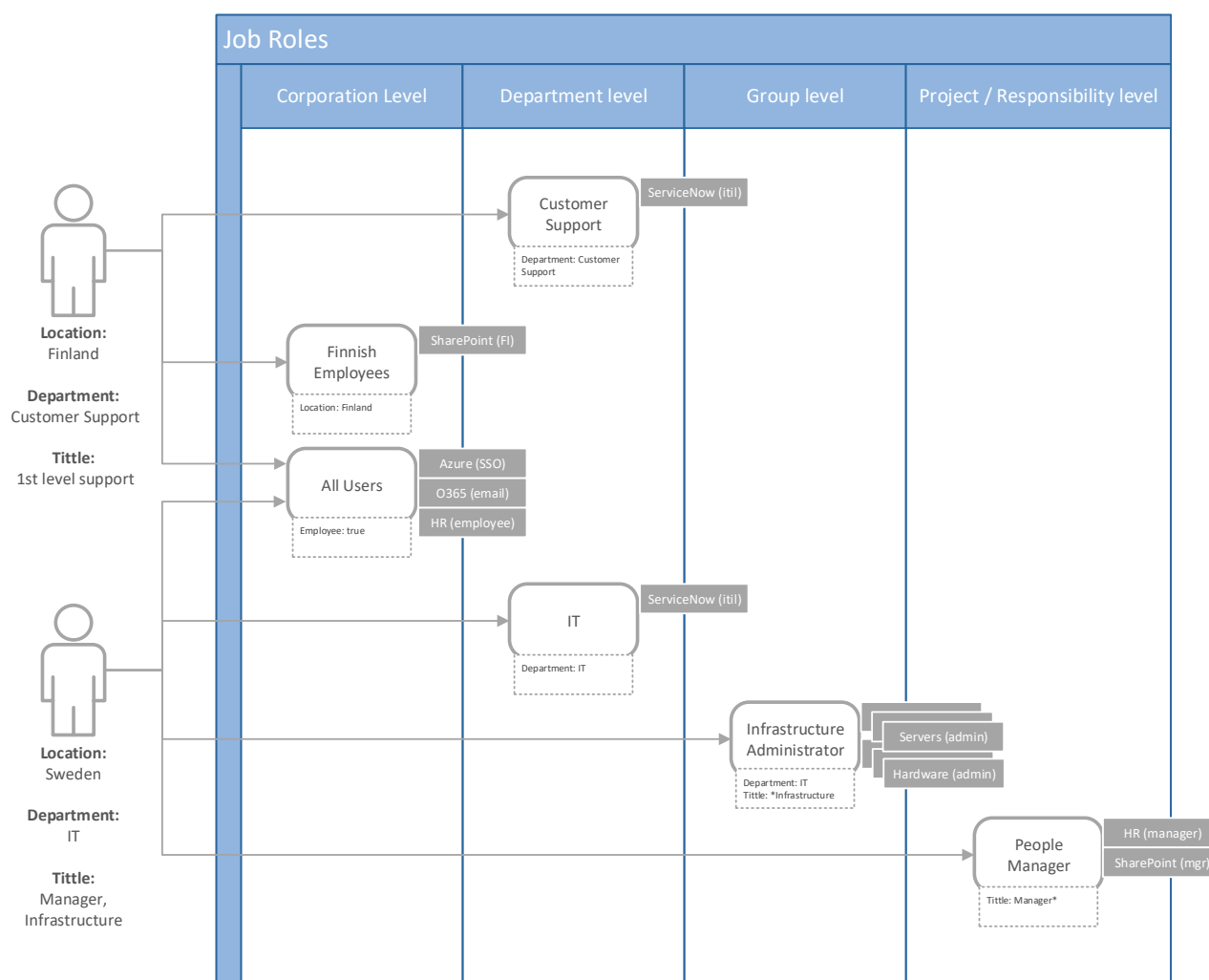
In addition to identity, information is needed about which systems a person can log into. Users have separate accounts (user IDs) in each system, one user can also have several accounts in one system. For example, a person may have a normal user account as well as a local administrative account. In addition to these, you also need to know what a person should and should not be able to do in the system. Management of these Access Rights is usually based on roles, accesses, groups, and licenses. An account can also be a child of another account and controlled from another system, e.g. active directory is provisioning account and access rights to the target system, in this scenario, the active directory would be a parent for the target system.



JOB ROLES

Job roles are among the base processes in IAM. Job roles are combinations of accounts and access rights to different systems that can be granted based on a person's identity. Attributes like department, position, or job title in an "identity card" can be used for assigning job roles. One person can have several job roles, and job roles can also be ordered separately through the ServiceNow portal.

Examples of job roles which can be in different organizational levels.



APPROVALS

The best practice is to make approvals simple as possible, but still, regulate required security levels and company policies. ServiceNow IAM solution makes it possible to define different kinds of approval flows for different use cases, as portal access might require only manager approval compared to administrative access which might require additional approvals from the security team and system owner.

EXAMPLE APPROVAL FLOWS

Here are few examples of approval workflows

Situation	Approvals	Comments
Update from HR system (joiner, mover or leaver)	No approvals	As these are controlled by HR system which has its own controls, separate approvals are usually not required in IAM
New non-positioned external user	1. Internal manager approval 2. Security approval	Internal manager should always approve any additional external users. Security should check for any mandatory contracts and trainings.
New access	1. Manager approval	Managers should approve any additional access
Privilege access	1. Manager approval 2. System owner approval 3. Security approval	As privileged access will give administrative access to the system to perform any operations, it requires both system owner approval so he/she can check if user really requires privilege access, and security who should review any mandatory trainings and any other related security checks for privilege access.
Update or termination of non-positioned external user	1. Internal manager approval	Manager should approve any changes for existing non-positioned user.
Manager changes for non-positioned external user	1. Existing internal manager approval (if active) or existing internal managers manager (if existing manager inactive) 2. New internal manager	Internal manager should always approve any changes for external users. If existing internal manager has been inactivated, then his manager can approve this change.
Automated termination or inactivation created by IAM	No approvals	As these are based on timed tasks approvals are not required to prevent system from completing its tasks.

CRITICAL ACCESS COMBINATIONS AND SEGREGATION OF DUTIES

Critical access combinations or segregation of duties are controls for having more than one person required to complete a task. These are used to prevent fraud, sabotage, theft, misuse of information, and other security compromises.

ServiceNow IAM solution can control critical access combinations and segregation of duties by automatically rejecting these access violations as well as reporting any active violations for further actions.

There can also be cases where violations are allowed and as such IAM solution can also request separate approval for access violations e.g. if a temporary violation is required, or just report if the violation is not critical but there is a need to know if there are such access combinations.

Example situations for critical access combination and segregation of duties check

Situation	Actions	Comments
Payment and approval of invoices is performed by the same user	Automatically reject	It would a great risk of theft to have one user who could approve and pay invoices.
Developers have access to production	Request approval from ECAB	It would be a risk of sabotage or theft to have developers input their own code to production without controls. However, there might be emergency situations where developers might require temporary access to production to manage critical incident.
User accounts with privilege access rights	Report to system owner	Having privilege access rights with your user account add risks for cyber threats for stolen accounts. However, it is still common to have privilege access tight to user accounts and cleaning up and creating separate local admin accounts needs to be separate process.

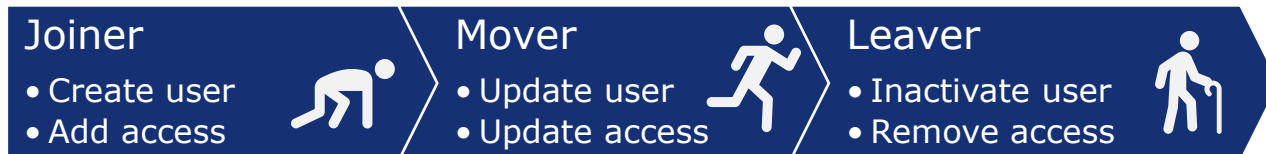
UNAUTHORIZED ACCESS

ServiceNow IAM solution can monitor that the administrators of target systems do not bypass the process and add accounts and access rights without appropriate approvals and processes controlled by IAM solution.

IAM solution can automatically remove any unauthorized accounts and access, or it can be set up to require approval separately for these accounts and accesses.



EMPLOYMENT LIFECYCLE



ONBOARDING (JOINER)

NEW EMPLOYEE

New employees are created in the HR system, and it works as a master for employee data. Employee data is synchronized to ServiceNow IAM solution which will create an identity for the new users and identity is used to take further actions within IAM solution.

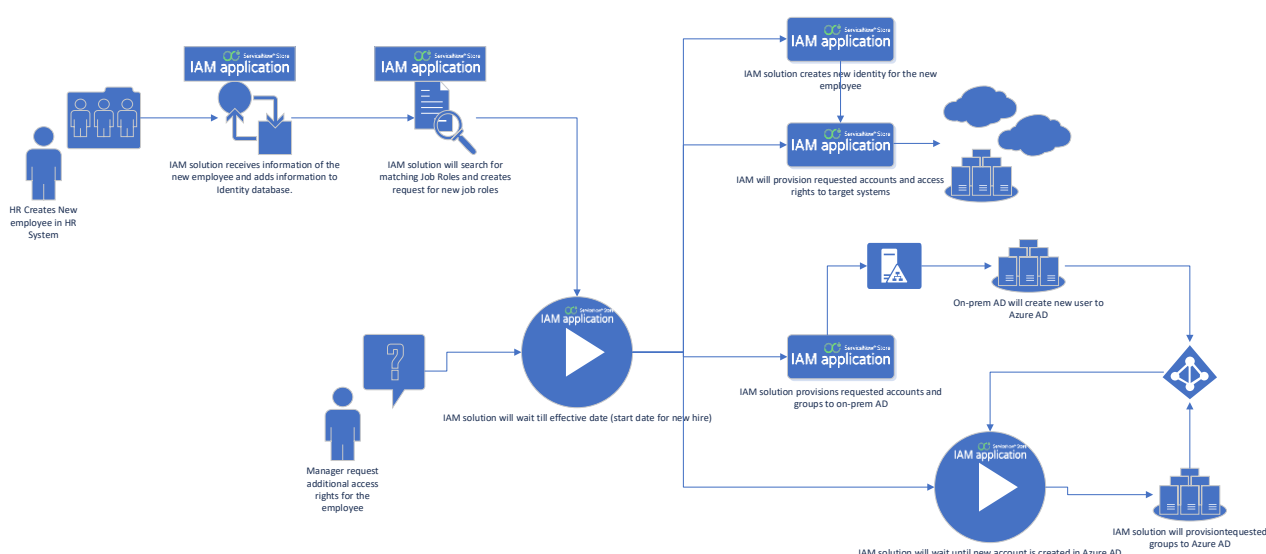
When identity is created, IAM solution will automatically search for any matching job role conditions and require any matched job roles. With policies applied for new employees, you can define also other rules like when to provision a user to different systems, adding separate accounts to systems, just to name a few.

NEW NON-POSITIONED EXTERNAL USER

New non-positioned external users can be requested directly from the ServiceNow portal. Usually, an HR system is not required for these users as they do not require any capabilities of the HR system, but the whole lifecycle can be controlled from the ServiceNow portal with ServiceNow IAM solution. Positioned external users are commonly managed the same way as internal employees, as they will need to be presented in the organization chart and will need to have other HR capabilities as well used.

EXAMPLE NEW EMPLOYEE WORKFLOW

Example workflow for new employee with hybrid active directory setup (on-prem + Azure AD)



REQUESTING ADDITIONAL ACCESS AND JOB ROLES

After an identity has been created in IAM either from the HR System or using the ServiceNow portal, users and managers can be requested additional Access Rights or Job Roles from the ServiceNow portal. You can also use an order guide to fulfil both hardware as well as access right request at the same time, making it easy for the managers when the new employee is starting within the company.

Access Rights can be requested and approved even if employment is starting in the future and the current identity is not yet active. If an effective date was set to request will go to awaiting effective date state and will continue with provisioning tasks after the effective date is reached.

You can also setup access policies to either force or limit access rights based on identity and account information, for example, limit privileged accesses to only local admin accounts.

Example order form for requesting additional access to ServiceNow

ServiceNow Access

Request access rights for ServiceNow

* Requested for ⓘ Abraham Lincoln (external) x ▾

Effective date ⓘ
Optional date when this request should take action. 📅

Account
ServiceNow PRODUCTION » abraham.lincoln · User Account · Active ▾

Account state ▾ Active Account valid until ⓘ
Optional date when account should expire. 📅

Access rights, roles and groups

Justification
Write justification for person to have requested access rights

🔍 Search from access rights... x

All Assignment Group ▾ Core Access Rights IAM Access Rights

Available access rights 6 Assignment Grou... Existing access rights Assignment Grou...

+ CAB Approval ⓘ
CAB approvers

+ Database ⓘ

+ Catalog Request Approvers for Sales ⓘ
This is a group of users that need to approv...

+ Change Management ⓘ
Change Management Group

+ Capacity Mgmt ⓘ

Field Services ⓘ
Provisioned ⓘ

Hardware ⓘ
Provisioned ⓘ
IT department responsible for all hardware...

IT Customer Support (helpdesk) ⓘ
Provisioned ⓘ
IT Customer Support for external customers.

US Presidents Group 2 ⓘ
Provisioned ⓘ
Demo user group for Password Reset Appli...

Submit

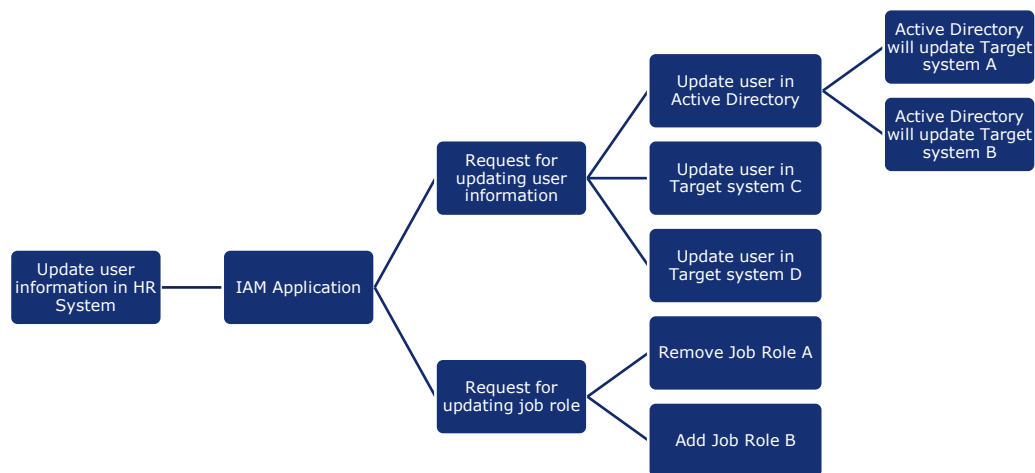


USER INFORMATION UPDATED (MOVER)

Employee information is usually updated in the HR System. HR System will provide new user information to ServiceNow IAM solution and it will create a request for updating identity information for all users accounts in all systems which require updated identity information.

External employees can be updated using the ServiceNow portal. This will create a new request to update information in each of the systems.

When identity information is updated also job roles are re-calculated, where unnecessary job roles which no longer match identity are requested for removal and new job roles now matching new identity are requested.



TERMINATIONS (LEAVER) AND LONG LEAVES

Employee off-boarding is usually initiated within the HR System and ServiceNow IAM solution uses that information to trigger the termination process. With external non-positioned users, the ServiceNow portal is used to request termination for the users.

IAM can also manage any long leaves of the users, adding a layer of security for users not actively using the systems.

There can be different termination processes for different situations, and here are a few examples:

Situation	Termination process	Comments
Default termination for internal or external employee	<ol style="list-style-type: none"> 1. Inactivate all accounts on termination date 2. Remove all access rights after one week of termination 3. Remove all accounts (not needed for internal purposes) after 1 year 	Default termination is launched on date of the termination or last day worked (if available).
Fast exit for internal employee	<ol style="list-style-type: none"> 1. Inactivate all account immediately 2. Remove all access rights after one week of termination 3. Remove all accounts (not needed for internal purposes) after 1 year 	Launched separately within ServiceNow portal to terminate employee immediately.
Long leave	<ol style="list-style-type: none"> 1. Passivate all accounts 2. Remove any licenses which can be removed 	For long leaves we can passivate all accounts and remove any licenses which don't remove any information of the user (this can save license costs). After user returns all passivated accounts are re-activated, and any licenses can be requested again.

WORKFLOW ORCHESTRATION

ServiceNow IAM solution supports both automated and manual handling of IAM tasks when provisioning, deprovisioning, updating, or removing access rights and identities. The level of automation depends on the target system and choice whether to invest for integration if the system is rarely used. With ServiceNow, you can use both workflow and flow engines to automate IAM processes.

RECONCILIATION

It is essential for the IAM process to reconcile actual data from target systems to have the whole truth of current accounts and accesses in IAM. It will increase your security as you know if someone has bypassed the process and added account or access rights directly to the target system. It helps with compliance as you have a real-time actual state for all accounts and accesses in the target system.

Desired state and actual state are not the same and with IAM reconciliation you can handle both. Even if you are handling accounts and access rights manually to the target system, reconciliation will help you make sure that these are done correctly, and there are no mistakes made.

With reconciliation, you can get also critical information of the user's activity like last login time for which you can create audit rules and create removal requests for users who do not require access.

With reconciliation critical access combinations and unauthorized permissions can be monitored, giving you a more secure work environment, and adding a control that no one bypasses the process.

As it is critical for compliance and security to have accurate information of all accounts and access rights it is recommended to reconcile source and target systems to IAM automatically, or if automation is not possible then periodically reconcile target systems manually.



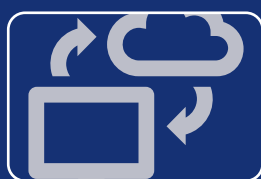
Errors

- How can we be sure that the requested and approved access rights reflect the actual access rights inside the target system?



Bypass the process

- How do we know that administrator of target system has not bypassed approval process and added privileges that might expose the organization to malicious activities?



Sync issues

- What happens if IAM and target system gets out of sync and how can we get in sync again?



AUTOMATED FULFILMENT

Automated fulfilment (also called “provisioning”) is integration with target systems to fully automate the IAM with approvals as the only manual step during the process.

IAM solution includes easy integrations with easy to manage and configure (low-code or no-code) API's and mapping capabilities including auto-mapping.

Full integration with target system usually includes:

- Create, update, inactivate and remove an account
- Add and remove access right membership
- Reconcile accounts, access right metadata, and access rights

Technically integrations can be built using almost any existing integration method including:

- REST API
- SOAP web service
- JSONv2 Web Service
- LDAP
- JDBC
- OIDC
- PowerShell
- File based methods
 - Delivery method
 - File from directory
 - FTP
 - FTPS
 - HTTP
 - HTTPS
 - SCP
 - SFTP
 - Formats
 - JSON
 - XML
 - CSV
 - Excel

MANUAL FULFILMENT


In some cases, there is no possibility to integrate the system fully or partially with IAM application, this is since the target system has no working API or other export/import functionality. There are also some cases when there is no reasoning to use resources to automate the target system, this can be that system will be replaced or retired soon, or that system has only a few changes over the year. This is where manual handling becomes mandatory for the IAM.

IAM will create tasks for all manual tasks to be actioned and you can use either the ServiceNow native view (for administrative users) or ServiceNow portal (for other and 3rd party users) to handle tasks.

IAM will automate everything other than actual provisioning, this will make it easy for users to add new accounts and access rights, as they don't need to worry about creating temporary passwords, sending instructions and passwords for the users, or managing approvals and such.

Users can also utilize systems knowledge base to add instructions directly to tasks and tasks are assigned directly to corresponding fulfilment groups, you can also separate different groups for adding accounts and for those that add access rights.

Example of manual account and access provisioning tasks in ServiceNow portal

IAM Tasks on request [IAMR0002328](#)
Requested for:
 Charlton Rogers
Account ID in SAP ERP:
CROGERS

⊖ Provisioning account for SAP ERP for Charlton N Rogers
Assignment group: SAP Administrators
For fulfillment instructions reference to knowledge base article: KB0010001

Provision new account using following values:
First name: Charlton
Department: IT
Title: Security Specialist
Last name: Rogers
Email: charlton.n.rogers@devlempinen.onmicrosoft.com
Middle name: Nettie
Manager: Lauri Reunamäki
ID in Target System: CROGERS
State: Active

[Show Password](#)
[Complete](#)
[Skip](#)
[Show Knowledge Article](#)

⊖ Provisioning AFLPM_CREATOR_ERASER_EXECUTE (SAP Enterprise Services) access right to SAP ERP for Charlton N Rogers
ⓘ Pending for Related Account to be Provisioned
Assignment group: SAP Administrators

⊖ Provisioning CONTENT_ADMIN (SAP Enterprise Services) access right to SAP ERP for Charlton N Rogers
ⓘ Pending for Related Account to be Provisioned
Assignment group: SAP Administrators



ACCESS CERTIFICATION

With the ServiceNow IAM application you can create different kinds of access reviews to improve your security, pass your internal and external audits, and comply with any security controls. Below are examples of access audits commonly used within organizations.

RECERTIFICATION

Recertification will force the managers to review their underlings' accounts and access rights, to make sure that the users have adequate access, and he should remove any unnecessary accesses from employees if they don't require those anymore.

Recertification usually runs once a year or every 6-months.

EXTERNAL USER AUDIT

External user audits will force the internal managers for external users to review if external users are still active and review that they have adequate access to the systems, and remove any unnecessary access from external users, or terminate the user if he/she is no longer working for the company.

Recertification usually runs once a year or every 6-months.

PRIVILEGE ACCESS REVIEW

Privilege access (administrative access) review will force system owners to review that only necessary users have privileged access to the target systems and remove any unnecessary privilege access from the users if they don't require administrative access anymore.

Recertification usually runs once a year or every 6-months.

IDENTITY ANALYTICS AND REPORTING

USER PROFILES

The ServiceNow IAM solution gives users and managers visibility to their own and their underlings identity information including accounts, job roles and access rights. From this profile view managers can easily request removal of unnecessary access, as well as manage other information of the users.

Example user profile view in ServiceNow portal

The screenshot displays the ServiceNow user profile for Kaarle Sund, a 1st level support user. The interface includes a top navigation bar with links to Access Management, IAM Tasks, Knowledge, Catalog, Requests, System Status, Cart, and Tours. The user's profile card shows their name, status (Active), email, department (Customer Support), location, manager (Lauri Reunamäki), and access validity. Below the profile card, there are sections for Job Roles and Accounts. The Job Roles section lists 'All Internal Users' and 'Customer Support'. The Accounts section lists 'Azure AD', 'SAP SuccessFactors', and 'ServiceNow PRODUCTION'. A right-hand sidebar provides detailed information for the 'ServiceNow PRODUCTION' account, including its ID, status, type, and access rights. The sidebar also includes sections for Assignment Group and Core Access Rights.

appmore Access Management IAM Tasks Knowledge Catalog Requests System Status Cart Tours Lauri Reunamäki

Kaarle Sund
1st level support

✓ Active

Email: kaarle.sund@devlempinen.onmicrosoft.com
Department: Customer Support
Location: -
Mobile phone: -
Manager: Lauri Reunamäki
Access valid until: -

JOB ROLES + Request new job roles

- All Internal Users
Azure AD
- Customer Support
Azure AD
ServiceNow PRODUCTION

ACCOUNTS + Request new accounts

- Azure AD
✓ Active 2
Account ID: kaarle.sund@devlempinen.onmicroso...
- SAP SuccessFactors
✓ Active
Account ID: kaarle.sund@devlempinen.onmicroso...
- ServiceNow PRODUCTION
✓ Active 2
Account ID: kaarle.sund

ServiceNow PRODUCTION

Account ID: kaarle.sund
Status: ✓ Active
Account type: User
Privileged account: No
Justification: -
Last audited: -

Access rights

Search from access rights...

ASSIGNMENT GROUP

Field Services

CORE ACCESS RIGHTS

ServiceNow IR

REPORTING AND DASHBOARDS

IAM solution uses the ServiceNow reporting engine that gives you the power to create, modify and extend data with any data combination required for reporting.

You can create comprehensive reports and lists of identities, accounts, and access rights for all systems.

You can also view individual users' identities, accounts, and access rights. You can also top this with IAM health information of the accuracy of the data collected from target systems.

You can also schedule these reports to automatically send information to users (e.g. managers, security department, or HR).

You can use existing or create your own dashboards within the system to see the reports in your interest.

Example dashboards available:

- Summary
 - Accounts and accesses provisioned
 - Provisioning time per system
 - Active requests
- Access violations
 - Critical access combinations
 - Segregation of duties
 - Unauthorized access
- Licenses (users missing license in target systems)
- Access certification
 - Active certifications state
 - Results of closed certifications
- Orphan accounts

LIST OF FEATURES

Workflow orchestration

- HR based JML
- Self-service JML
- Password reset (automated and manual)
- Long leaves
- External user JML
- Rehire (internal & external)
- Silent recruitment
- Fast exit
- Internal becomes external user (or vice versa)
- No show
- Policy management
- Delegate management
- Administrative (Source & target systems, manual)
- Mass changes

Identity analytics and reporting

- Identity audit trail
- Orphan accounts
- Segregation of Duties
- Account last login and password changes
- Leadtime reports
- Volume reports
- Software License usage
- Unauthorized accounts and accesses
- Source system reports
- Target system reports
- Access certification reports
- Transaction logs
- Integration logs
- Audit logs
- Access Analysis

Fulfilment

- Account Handling policies
- Approval definitions
- Credentials management
- Manual fulfilment (task-based)
- Instructions management
- Error Management
- Source and target system connectors

Entitlements management

- Job role management
- Advanced Job Role management with custom variables



- Account management (User, Local, Test, Admin, Shared, Secondary, Application, Device, Deprecated)
- Account flows (Provisioning, Updating, Deprovisioning, Removal, Password resets)
- Access right management (Access, Role, Group, Profile, Security, Distribution)
- Access flows (provision, deprovision)
- Access right metadata management (group, security group, distribution group)
- Access right metadata flows (create, update, inactivate, remove)
- Privileged Access Management
- Access classes and Access right groups
- Account and access instructions
- Account and access licensing
- Account and Access Ownership
- Automated account and access rules
- Automated Reconciliation
- Role-mining (suggest job roles)
- Suggest access rights

Access certification

- Manager certification
- System owner certification
- Dynamic certification
- Certification portal
- Certification reminders
- Revoke accounts and access rights
- Certify accounts and access rights
- Certification history
- Show common and uncommon accesses

Platform capabilities

- Cloud deployment
- On-Premise deployment (requires additional licenses)
- OAuth 2.0
- SAML
- Service Portal
- Chatbot
- Survey Management
- BI reporting
- CMDB
- E-Signatures
- Email and mobile notifications
- SMS notifications (requires additional licenses)
- REST & SOAP API
- Risk Management (requires additional licenses)
- Security Operations (requires additional licenses)
- IT Service Management (requires additional licenses)
- HR Service Management (requires additional licenses)



MORE INFORMATION

Appmore provides ServiceNow IAM application for all IGA, IAM and IDM needs.

ServiceNow® Store IAM application

IAM application is available at ServiceNow store:

https://store.servicenow.com/sn_appstore_store.do#!/store/application/38e2cb954f2a8f008ef74fa18110c78f

Please contact us for more information about IAM application for ServiceNow.

Appmore Ltd

Tel. +358 9 4282 7663

Email. info@appmore.com

<https://appmore.com>