ID North | Smart Identity on Azure™

Identity Security

Critical component of cybersecurity

Identity security is a critical component of cybersecurity since it involves **protecting the digital identities of individuals, devices, and systems** from unauthorized access, theft, or misuse. In today's digital landscape, the significance of this cannot be overstated, as sensitive data and information are stored on digital platforms, encompassing both internal data centers and cloud environments.

Access control is a fundamental aspect of cybersecurity and involves ensuring only authorized users can access resources and data. Effective access control mechanisms can help prevent data breaches, unauthorized access, and other security incidents that could compromise an organization's data and systems. For access control to operate properly, it needs a reliable and governed source of identity and access data.

Identity security is also critical for **compliance with regulations and standards**, such as the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), ISO 27000, NIS2. Such regulations require organizations to implement effective identity and access control, administration, and governance measures to protect access to sensitive data and information.

Microsoft has for many years been a trusted identity security vendor, now taking identity security capabilities to the next level in their Azure cloud.

Many organizations are adopting cloud technologies in lieu of their own data centre infrastructure. However, **making a full-scale cloud transition is demanding** and organizations tend to embrace a hybrid infrastructure for numerous years. During this time, it can be challenging to justify replacing investment of existing and fully functional technologies in favour of just a cloud alike.

ID North has developed the identity administration and governance product – Smart Identity on Azure™ – that is designed to embrace a hybrid approach and support organizations' identity security transition to the cloud. The solution is built on top of Microsoft technologies such as Azure AD, SharePoint, Teams, Power Automate, and it leverages any existing on-prem MIM solutions to synchronize identity data between Azure and applications in the own data center.

Key features of Smart Identity on Azure™ are:

- Identity and access administration and governance of all user types; employees, business partners, contractors, students, etc
- User-friendly UI for administration and governance tasks
- Automated user on- and off-boarding processes
- Role-based identity lifecycle and access management
- Self-servicing and delegation
- Digital Access Review process
- Easy workflows for approvals and requests
- Analytics and Reporting

In summary, identity security is a crucial aspect of cybersecurity because it helps organizations protect sensitive data, prevent unauthorized access, and comply with regulations and standards. Smart Identity on Azure™ provides a cloud-based solution for identity and access administration and governance designed for organizations living in a hybrid IT environment.


Cybersecurity
The challenges

Cybersecurity threats have been on the rise for decades. Research has year after year pointed out that **humans are the weakest link in the cybersecurity chain**, i.e., shown to be susceptible to letting in malware, sharing credentials through phishing or social engineering, or negligence in keeping software and devices updated and correctly configured. The consequences are apparent in reputation and costs such as data leakage, ransoms, penalties, or withdrawn operation permits. Therefore, it is no surprise that statements like “identity is the new perimeter” and “identity-first approach” have risen from analysts, vendors, and academics. Today **identity security is seen as one of the most critical components** when building up cybersecurity defense mechanisms.

Also, proper identity security controls are required by most regulations and standards, which makes it a necessity for organizations to address to avoid sanctions.

In combination with the threat landscape, **many organizations are moving to a cloud-first strategy** and are making a transition from on-prem applications in the datacenter to alike cloud applications. Due to complexity, making a full-scale transition is non-trivial, so we are now living in the era of hybrid IT environments, which needs to be considered when implementing new identity security capabilities. It must be ensured that both cloud and on-prem applications and infrastructures are covered, e.g. modern identity security capabilities must function frictionless in a hybrid IT environment. Otherwise, there is a substantial risk that same identity security capabilities are realized multiple times in silos.

Identity security capabilities are often long-lived mechanisms and are not replaced with ease as they tend to have evolved with organizational and business changes throughout many years. In hybrid IT environments it therefore can be more advisable to protect existing investments and retain existing technology and build new capabilities on top of those. The struggle is to glue new identity security capabilities with existing ones.

Microsoft's on-prem identity administration technology stack has a long history, evolving from Microsoft Metadirectory Server (MMS) in late nineties, to Microsoft Identity Integration Server (MIIS), to Identity Lifecycle Manager (ILM), to Forefront Identity Manager (FIM), to today's Microsoft Identity Manager (MIM).

Organizations who have invested and evolved with Microsoft's technology are likely to have well-functioning automated employee onboarding, synchronization, and offboarding processes based on a HR source feed that administer basic on-prem applications and Active Directory. **However, they might lack identity security capabilities when it comes to managing other user types than employees, role-based access provisioning, and identity governance such as reporting, self-service access requesting with approvals, and recurring access reviewing.**

Common characteristics for these organizations are:

- missing an identity repository and central UI for all identity administration tasks for all user types,
- Azure AD is just a continuous mirroring of on-prem Active Directory through utilization of Microsoft Azure Active Directory Connect,
- user administration of on-prem Active Directory is performed with legacy tools
- inadequate governance processes are infamous in audits.


Cybersecurity
The solution

Resolving identity administration and governance challenges in a hybrid IT environment without a significant re-investment through a complete replacement of the existing technology stack with a new one has been uncommon. Luckily, now there is Smart Identity on Azure™ that fills this gap.

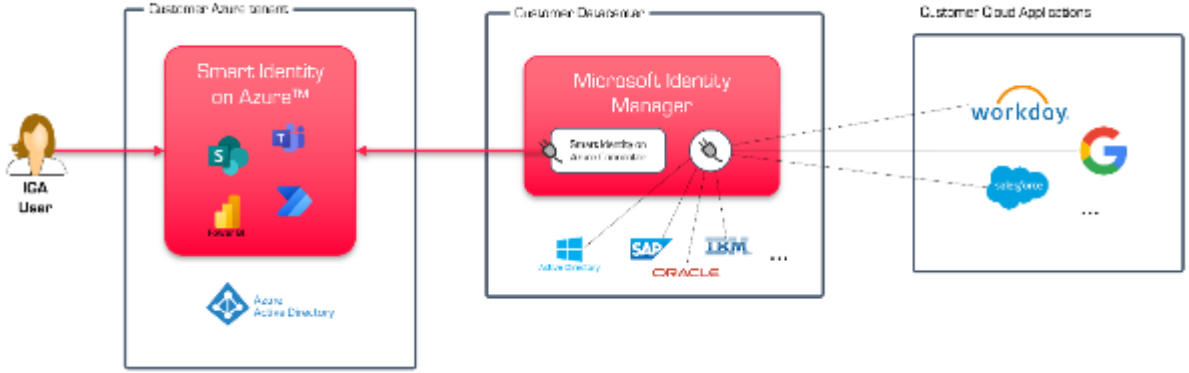
Developed by ID North **and designed to embrace hybrid IT environments**, Smart Identity on Azure™ protects and maximizes organizations' investments in Microsoft on-prem identity administration technology and support their identity security transition to the cloud.

The platform achieves an identity repository in the cloud, covering all user types. **Administration and governance tasks can then be performed through a central UI, and Azure AD and on-prem Active Directory can become separated user directories with distinct set of administrative rules.**

By letting administration and governance tasks leverage a single central identity repository, properness of governance processes be proven in audits, which is hard to achieve when legacy tools are in-use.

The platform is **built on top of Microsoft cloud technologies such as Azure AD, SharePoint, Teams, and Power Automate,** all operating in the customer's own Azure tenant. Though it is not required, Smart Identity on Azure™ leverages existing on-prem *Microsoft Identity Manager* (MIM) solutions to synchronize identity data between Azure and applications in the datacenter.

Any existing MIM automated employee onboarding, synchronization, and offboarding processes based on a HR source feed are preserved and extended with a connector to feed identity data to the Smart Identity on Azure™ platform in the customer's own Azure tenant.



With Smart Identity on Azure™ on-prem Active Directory and other on-prem applications' user administration are facilitated both through automation and use of a consolidated modern and user-friendly UI in the cloud. Use of cumbersome legacy administration tools can be deprecated, and a more audited user administration process can be achieved.

Smart Identity on Azure™ is continuously developed on top of the Microsoft Azure technology stack and tailoring *a* **solution to customer needs is easy and intuitive by leveraging built-in no-code/low-code technologies**.

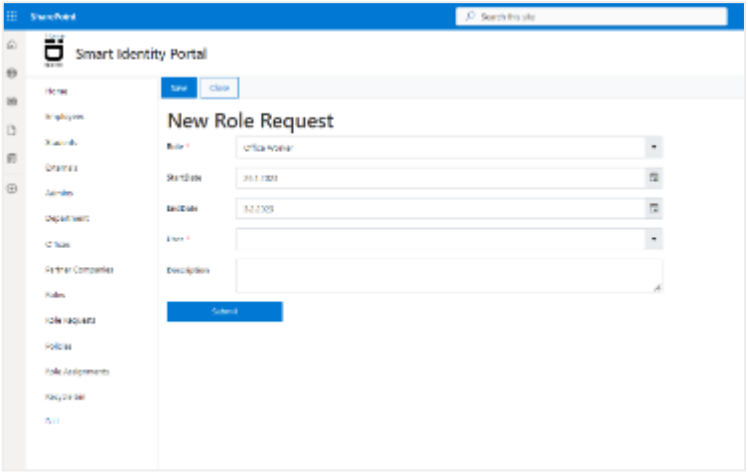
Also, the platform can integrate with any Azure based identity and access management (IAM) services provided by Microsoft. Since the solution capitalizes on the customer's existing Microsoft licenses, they also **maximize performance of the existing Azure investment**.

Key features

1. Central UI for administration and governance tasks

Smart Identity on Azure™ provides a unified and user-friendly UI to perform identity administration and governance tasks, such as create/update/delete/view users, disable users, request access and access reviewing.

With Smart Identity on Azure™ common on-prem Active Directory user administration operation is transferred from use of legacy tools to a modern cloud based one.



3. Role-based identity lifecycle and access provisioning

Smart Identity on Azure™ uses the concept of roles for bundling together a bunch of accesses to different applications as a single administrative item. By assigning a role, the user gets provisioned with all those accesses bundled into the role. **When the role is removed from the user, all bundled accesses get deprovisioned.**

Roles can also be automatically assigned to a user, based on conditions. For example, if a user has the value “Sales” in identity attribute “Department” then the role “Sales Team Member” gets assigned automatically to the user. **When the user changes department, then the role is automatically removed from the user.** This concept is also called **Birthright Roles.**

4. Automated user on- and off-boarding processes

Smart Identity on Azure™ supports automation of identity on- and off-boarding processes where changes in a master source, eg a HR system, triggers events for an identity in the Smart Identity on Azure™ platform. Identity master source systems are integrated through Microsoft Identity Manager (MIM). Upon identity data changes in the master source the identity repository in SharePoint is updated accordingly. This optionally triggers workflows for custom handling or assignment/removal of accesses via birthright roles.

Automated on-boarding and off-boarding provides lifecycle management for the most common services, such as AD, Azure AD and Microsoft 365, managing different distribution lists and network groups, license assignment, and ultimately allowing users to manage their own data as self-service.

A great benefit of **an automated off-boarding process is that it provides relief for license asset management**. As part of the removal of an access, removal of licenses from different systems can also be triggered, thus optimizing license use as no unnecessary licenses are assigned any longer.

Customers already having MIM, probably already have identity master sources integrated in existing on- and off-boarding processes. In this case the cloud-based identity repository is hooked into the existing processes through a ready-made Smart Identity on Azure™ connector and all cloud-based administration and governance capabilities become available.

Customers not having any existing technology to drive on- and off-boarding processes and integrating identity master sources can also leverage the MIM approach with the ready-made Smart Identity on Azure™ connector. MIM will then be configured from scratch.

Customers having some other technology than MIM for integrating identity master sources and driving on- and off-boarding processes can also leverage Smart Identity on Azure™ identity repository in the cloud. This is achieved by tying in Smart Identity on Azure™ into existing processes by connecting to the web services available in the Smart Identity on Azure™ platform.

In case a HR system is missing, then Smart Identity on Azure™ can act as the identity master and the customer the manages identity lifecycle processes directly from the central UI.

5. Self-servicing and delegation

Smart Identity on Azure™ contains self-service capabilities where **users themselves can perform identity administration and governance tasks.** This relieves task tickets from the service desk and ultimately the users get a faster task execution.

Self-servicing means that tasks are delegated to the users themselves from other organization units, such as service desk and application administration teams. Delegation can also occur to others than the users themselves. Typically, delegation also occurs to managers to also perform identity administration and governance tasks on its managed users.

Common self-service and delegated tasks include access requesting, approvals, identity registration and updates, and access reviewing. Also, passwords re-setting is a common self-service case.

Making use of self-servicing and delegation means that identity administration and governance processes become digitalized and are conducted in same way every time. No need to send random emails or text messages to someone to get administrative tasks performed. Digitization and use of a central UI brings a proper audit trail for who has performed what tasks.

6. Digital Access Review process

Smart Identity on Azure™ can execute digital access reviews where users' assigned accesses get re-assessed. A reviewing round is typically assigned to be conducted by managers or application owners, but it could be appointed to any user.

In a reviewing round the appointed reviewers are presented with a list of current accesses for each user that is to be reviewed. Each reviewer then either approve or reject each assigned access. Any rejection triggers removal of the assigned access.

A reviewing round produces an audit trail of the re-approvals or rejections that reviewers perform. This also means that the decision log gets updated, which is a necessity for being compliant with regulations.

7. Analytics and Reporting

Smart Identity on Azure™ contains a centralized identity repository that include identity attributes, roles, accesses, audit trails, among others. All this data is directly available for analytics and reporting.

The data from the identity repository is made available to Microsoft Power BI, which is a powerful tool for analyzing data, visualizing results, and compiling reports.

8. Easy workflows for approvals and requests

Smart Identity on Azure™ make use of workflows for automating tasks or implementing logic in digitalized processes. Workflows are typically triggered by a schedule or on various events in the platform.

Workflows are realized with Microsoft Power Automate, which is a powerful platform that enables users to create and automate workflows without the need for extensive coding knowledge. It offers a no code or low code approach, allowing individuals with limited programming experience to visually construct workflows using a user-friendly interface.

The Smart Identity on Azure™ platform offers a library of pre-defined Power Automate templates, which serve as default processes or starting points for building tailored workflows. Templates cover a wide range of common use cases, such as email notifications, data synchronization, approval processes, and more.

Power Automate also includes a robust set of built-in actions, conditions, loops and data manipulation that are available via drag and drop to create complex workflows. These components enable logic and easy decision-making within the workflows, allowing for dynamic and responsive automation.

By making use of Microsoft Power Automate no code or low code approach in Smart Identity on Azure™ repetitive tasks are automated and business processes streamlined. Workflow creation gets enabled for individuals with limited coding skills to achieve efficient automation solutions.


Cybersecurity
Use cases

Use cases

Below are some typical use cases where Smart Identity on Azure™ has been used to resolve identity management challenges:

- **Workforce management**
  Smart Identity on Azure™ has been used to digitize and automate Joiner, Mover, Leaver, Rehire (JMLR) processes. Customers have achieved an automated management of user access to resources throughout their lifecycle for their workforce. With JMLR processes in place, users have the appropriate birthright access at the right time, and any unnecessary access is promptly removed, maintaining a secure and compliant environment.

- **External user management**
  Organizations lacking a master system for keeping master records of external users, have used Smart Identity on Azure™ as the master where those users get registered through the central UI. The same UI is then used for delegation of administrative and goverance tasks of external users.

- **Identity visibility**
  Organizations lacking proper visibility of what accounts in different systems belong to an identity, and what roles are assigned to an identity, have deployed Smart Identity on Azure™ on top of Microsoft Identity Manager (MIM) to achieve such visibility. This have been the starting point for digitalizing governance processes and enabling self-service.

- **Role-based access governance**
  Organizations having informal processes for requesting and assigning accesses in Active Directoy and different systems, have made use of Smart Identity on Azure™ to bundle a bunch of accesses together into business roles that are then made available for self-service requesting and approvals, or event automatic assignment as birthright business roles.

- **Access review**
  Organizations having a highly manual access review process where data is collected into various Excel sheets, have made use of Smart Identity on Azure™ for performing automated collection of access data into the identity repository and obtain re-approvals/rejections from reviewer, for example managers.


Cybersecurity
Benefits

Benefits

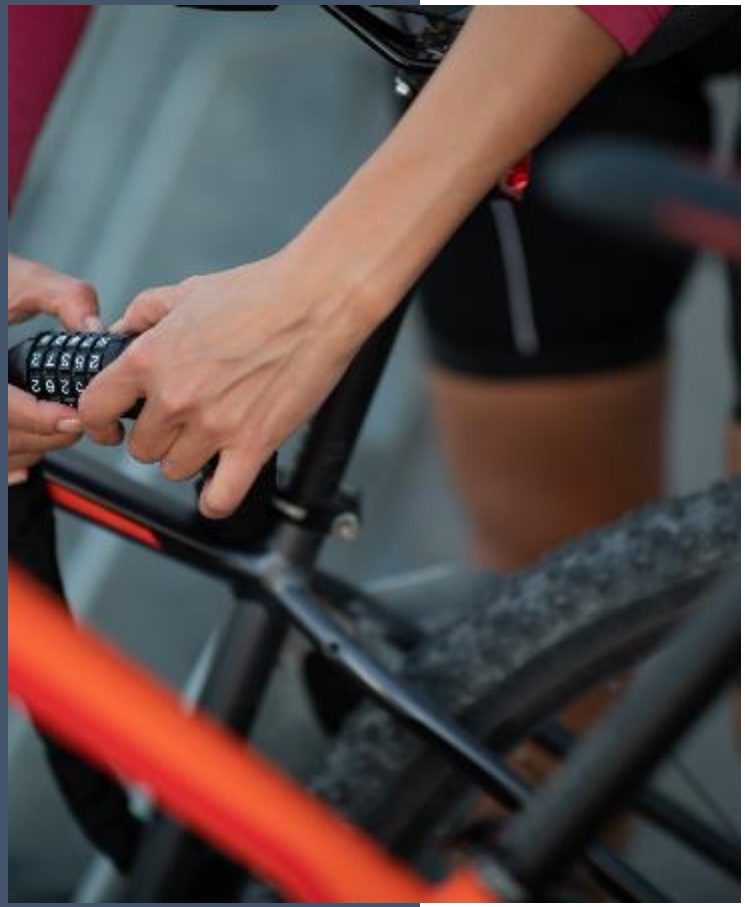
Smart Identity on Azure™ cuts identity administration and governance costs and improves efficiency by automating dataflows and management of accesses, enabling self-servicing and delegation, and building up a central identity repository that can be used as a single source for analytics, reporting, and auditing.

Security is improved by having processes digitized so they are no longer conducted informally, and a proper audit trail gets produced on who has done what. By achieving visibility into each identity's accesses and bundling accesses into business roles manageability of the accesses improves and it is more likely that inappropriate accesses do not get assigned. Executing access review rounds with some frequency drive removal of inappropriately assigned accesses. As part of off-boarding processes, Smart Identity on Azure™ helps in deprovisioning all current accesses and disabling accounts for the leaving user.

Regulatory compliance becomes easier to fulfil. Smart Identity on Azure™ provides proof of performed access reviews, audit trails for who has approved what accesses for a user, and identity visibility, analytics and reporting helps proving that an organization is in full control of all identities and accesses.

Smart Identity on Azure™ is designed to work in hybrid IT environments and protects an organization's previous investments in on-prem identity management technologies, in particular investments in Microsoft Identity Manager (MIM). Organizations no longer need to replace their existing identity management technology stack in order to achieve the benefits from cloud-based identity administration and governance.


Cybersecurity
Implementation
and services



Implementation and service

Smart Identity on Azure™ is implemented in the customer's Azure tenant. ID North has both a proven delivery methodology and a toolset for implementing a solution at a rapid pace.

The delivery methodology contains a structured approach for an implementation project that includes:

- capturing requirements,
- design a solution architecture,
- tenant deployment,
- tailor configuration of dataflows, forms, workflows, access rights, reports, etc
- perform end-to-end testing,
- initial identity repository dataloading,
- training and communications, and
- go-live

When the Smart Identity on Azure™ is in production, ID North provides continuous services to customers. Services range from a basic ticket-based product Support to a fully Managed operation of the platform. All services are provided under SLA timeframes which are monitored in the ticketing system.

Conclusion

Conclusion

Smart Identity on Azure™ is a platform designed to add on cloud-based identity administration and governance capabilities to organizations with hybrid IT environments and lacking an identity repository and central UI for managing users.

Its technology stack is built on top of Microsoft Azure cloud services, and it leverages any existing on-prem identity management technology. While adding on modern identity security capabilities, it also protects and maximizes the investment organizations have put down previously in on-prem identity management technologies, there is a benefit for customers with Microsoft Identity Manager (MIM) in use.

If you want to learn more about Smart Identity on Azure™ and perhaps see a demo, do not hesitate to contact us at sales@id-north.com

Stay in touch

info@id-north.com

id-north.com

Please visit our page

Vasagatan 23
111 20 Stockholm

Stay in touch

info@id-north.com

id-north.com

Please visit our page

Workery West, Tripla
Firdonkatu 2 T 63 00520 Helsinki