

## Identity lifecycle and governance in the cloud: it's here!

Easy to use, fast to implement, 100% based on industry best practices, and built on IdentityNow

Identity management is difficult and takes a long time to implement, right? Not if you do it our way. No more endless role modelling or mining exercises. Use our simple and practical 'reason for access' based methodology to kick-start your new identity management initiatives. Together with our *ReadytoUse ID Lifecycle* cloud solution based on the industry leading IdentityNow platform you have all the tools and knowledge required to efficiently automate any identity lifecycle in your company. You can get in control of who has access to what. Quickly. All while providing your end users with an easy to use self-service experience, greatly improving general buy-in. Your identity governance needs are also covered: optional approval processes, Segregation of Duties (SoD) support and simple certification processes. Everything cloud based and ready to use.

### Automated *identity lifecycle*

Ensure the *right* access to the *right* resources for your employees or business partners, at any point in time. Automatically grant access to specific resources based on *existing* data in your *current* business processes. And also automatically *revoke* that access once the reason for access no longer applies, with an optional *grace period*. Future dated business events, as often announced by HR systems, are fully supported. So future changes, like a pending change of department or position, can be used to drive changes in access rights.

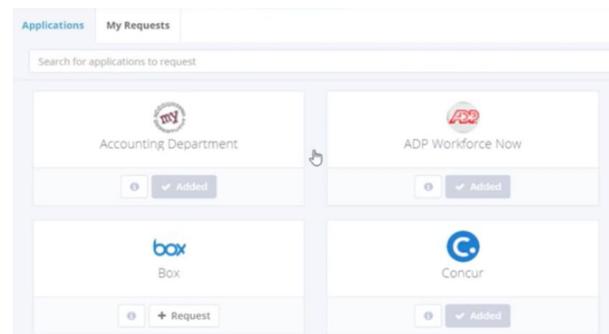
### Self-service

Allow members of your organization to request access to applications or even preconfigured sets

of needs based on your business. Access can be granted automatically or by an assigned approver.

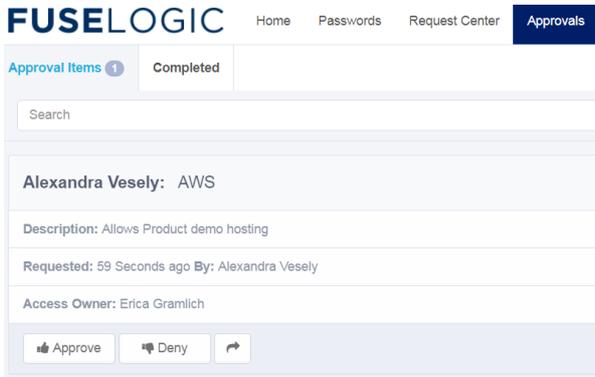
### Context-aware *self-service*

Later this year, the self-service feature becomes even more powerful. IdentityNow Makes requesting access to resources as smooth as possible by personalizing the process using *existing* data in your *current* business processes. For example, only offer relevant access request options based on someone's position in the organisation, or only to members of specific projects. Any data source that can provide this information will do. And of course, also automatically *revoke* the requested access once the reason for access no longer applies.



### Turn-key *approval workflow*

Access requests may optionally require approval by, for example, application/business owners, managers or both. The solution supports this without having to invest time in creating your own approval process. We have seen what works, and it's there for you to use. Ready to go.



### Simple certification process

Certification (or attestation) is an integral part of the solution. It enables the periodic review of all access rights. This review can be performed by managers, application owners or business owners. The solution aims at making certification campaigns in your company as simple and easy as possible. The results of a campaign are available for reporting and auditing purposes. Revocation of access based on the certification outcome is fully supported.

Name	Exceptions	Decisions Left	Status
<input type="checkbox"/> Aaron Nichols (Aaron.Nichols)	>	0	Certified
<input type="checkbox"/> Adam Kennedy (Adam.Kennedy)	>	0	Certified
<input type="checkbox"/> Alan Bradley (Alan.Bradley)	>	0	Certified
<input type="checkbox"/> Albert Woods (Albert.Woods)	>	0	Certified
<input type="checkbox"/> Alice Ford (Alice.Ford)	>	2	Pending
<input type="checkbox"/> Allen Burton (Allen.Burton)	>	1	Pending
<input type="checkbox"/> Amanda Ross (Amanda.Ross)	>	3	Pending

### Segregation of Duties support

Some permissions are better not granted simultaneously. For example: sales should not be allowed to approve their own proposed compensation plans in the HR system. Or no one should be allowed to both approve and pay vendor invoices. It can be anything, depending on your company’s specifics. Defining and enforcing these Segregation of Duties (SoD) is supported. Specified SoD policies can be scheduled to automate the reporting of violations.

### Easy to configure

All configuration of the solution is done within IdentityNow. The solution uses the concept of a ‘Model User’ to define all required information around a resource access object (like resource accounts, entitlements or groups). Model Users are fictional users whose user and lifecycle properties resemble those of a specific group of people.

### Fully cloud based

Sailpoint IdentityNow is the secure foundation of the solution. Sailpoint is a leading Identity-as-a-Service provider. The IdentityNow platform is leveraged for all your user management, account and entitlement (de)provisioning and governance requirements. All features of the IdentityNow platform are at your disposal.

#### About FuseLogic:

FuseLogic implements solutions, consults and improves processes in the field of Identity and Access Management. We create pragmatic solutions, based on the existing business processes of an organization. Our starting point is the daily reality of the customer, not a strict theoretical framework. We provide clear, user-friendly identity management solutions, even for very dynamic environments.

FuseLogic brings specialist knowledge, years of experience - established in 2007 - and a proactive approach.