Data Segmentation

Data Segmentation is a new capability from SailPoint that solves a challenge faced by large, complex organizations needing better record-level access controls to meet internal security, partner enablement, and least privilege enforcement. It provides a programmatic method for restricting data within core Identity Security Cloud objects (access model items, identities, sources, etc.). This segmentation of data ensures users can only see the data records they are authorized to see. An example of this control would be ensuring sub-administrators only see those entitlements in administrative UIs and entitlement APIs that they should be allowed to see. Entitlement administration is our first object on the platform, but we will expand to additional functionality throughout the platform for every user.

Features

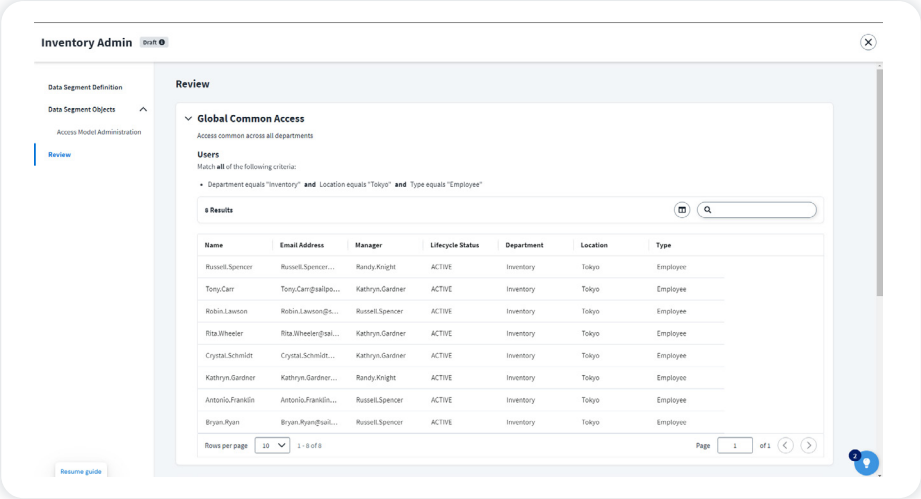
- **Least privilege enforcement:** Ensure users only have access to the identities, roles, access profiles, entitlements, and requestable item records they should be given for their role.
- **Delegated administration:** Offload the effort of building and maintaining an Identity Security Cloud implementation to the teams closest to the access and administration by only allowing them to see appropriate records.
- **Privacy:** Customers who have individuals who, due to internal privacy policies or regulatory pressure, need to ensure no user or admin can see every other user identity record.

BENEFITS

- **Better platform security:** Enforcement of least privilege at the record level to enhance security and ensure only the right users can see the right records and data
- **Expand ownership/share operating costs:** Teams will need to rely less on a single, centralized team to manage and maintain entitlements (and more functionality in the future)
- **Reduced costs:** Only requires one tenant for extremely complex organizations with data segmentation requirements (e.g., an organization with multiple subsidiaries that needs strong firewalls between organizations for their data)

Common use cases

- Administrators can easily create a security policy that limits specific users' access to specific records within key administrative objects (access model, identities, identity profiles, sources) and internally outsource the running of their IAM program.
- IAM teams can delegate more administrative tasks to the business, bringing them closer to the local experts, helpdesk, and IT teams.
- A consortium bank organization is made up of many banks and wants to ensure the sub-administrators at Bank A can only see the data associated with Bank A.



About SailPoint
SailPoint equips the modern enterprise to seamlessly manage and secure access to applications and data through the lens of identity – at speed and scale. As a category leader, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency. SailPoint helps many of the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.