

Access Management Best Practices

Author: Vedang Joshi

Published: January 18, 2023 · 4 min read

We are all aware of the importance of data in today's world. Anything valuable always comes with its security risks. The first step in the direction of protecting data is limiting who has access to it as much as possible. Identity and access management is a framework that helps us make sure that the right people have access to the right data and resources for the right duration.

In an organization, we work with many tools, for example - VMs, Databases, SAAS tools, etc. All these tools have their approach to user management. It is a cumbersome process to manage the users across all the platforms as the organization scales and the number of users increases. Thus having policies and procedures for user creation, audit, and removal helps reduce the security risk.

Improving the onboarding process

Centralizing access requests

The onboarding of each user on all platforms should be done by raising a request to a centralized system. The users should inform the team (that manages the tool) about why this particular access is required. This helps in tracking and compliance.

Enforcing MFA

The tools should be configured to let users access the resources only after an MFA device is used to authenticate.

Using emails as usernames

Emails are always unique in an organization. They should be used in place of generic usernames wherever possible. This practice can help us automate exit management.

For places where usernames can't be emails or for emails themselves, an organization should come up with a single pattern that is used to generate the username. This pattern must depend on something unique to the user like her employee ID. Example - <first_name>.<employee_id> etc.

Using SSO

SSO should be used wherever possible. SSO should also be configured to allow only members approved by the admin of the tool to access the resource.

Least Privilege Possible

This is considered a principal in the world of IAM. It refers to the practice of assigning minimum levels of access to users, only essential for their roles and duties. Every tool comes with RBAC - Role-based access control. These are policies that define what privileges a role has, a user is then given the required set of roles.

Enforcing strong password policies

Users should only be allowed to create their accounts when they have a strong password. A strong password is at least 8 characters long, uses special characters, and avoids obvious or guessable phrases.

Admin must apply password expiration policies.

Limiting programmatic access

Never commit credentials to Git

Credentials used to interact with the APIs of any tool should be stored in a secured vault or environment variables and should never be hard-coded or committed to version control. CI integrations can help enforce this.

Timely rotating keys

Access keys should be rotated timely and must be different for all environments in a single tenant setup.

Taking ownership

Each access key must be mapped to the human user who uses it.

Automate offboarding process

Daily user audits

Whenever a user leaves the organization, his email can be searched for and deleted from all the tools he has access. This process can be automated in tools that provide SSO, or it can be done through automation scripts.

Transferring ownership of access keys

After the offboarding of the user, if the keys are preserved they must be rotated and a new owner should be assigned to them.

Regular access audits and cleanup

The security team performs regular cleanup and audit activities to identify misconfigurations like:

- Over Privileged accounts
- Credential sharing
- Stale accounts
- Policy validation

Tips for users

- Users should inform the Admin if they no longer need particular access and get it deleted.
- Users should never share their credentials.
- Users should never use the same password for more than one tool.
- Users should never store their credentials on stick notes and slack channels etc

In conclusion, IAM revolves around people, each digital identity must have an owner - a human user. While teams benefit from using SSO for the majority of the places, it always helps to handle matters of access management with keeping the involved risk in mind.

Thank you