**Security:**

Identity Access Management:

It provides control over user validation and resource access. This technology ensures that right person access the right resource at right time for right reason. Using IAM technology we can create users, groups, and permissions for cloud services. It provides fine grain control options and supports federated users or users outside of the organisation by integration with either organisation’s active directory or 3rd party identity provider such as Facebook or google. It also provides the facility to right policy so that users can be authorised to access resources under some specific conditions.

Multi-Factor Authentication:

MFA adds a layer of security during login that requires users to provide more than one credentials to prove their digital identity. MFA reduces the likelihood of many types of cyber-attacks. It's common for third parties to steal usernames and passwords or programmatically attack user accounts. An additional MFA factor, such as a thumbprint or one-time password, impedes these violations. MFA works by requiring additional verification information (known as factors).

MFA factors, including:

* Push notifications.
* SMS notifications
* Voice notifications
* One-time passwords
* WebAuthn with security keys
* WebAuthn with device biometrics
* Email notifications.
* Cisco Duo security
* Recovery codes

Role Based Access Control:

Role-based access control (RBAC) refers to the idea of assigning permissions to users based on their role within an organization. It offers a simple, manageable approach to access management that is less prone to error than assigning permissions to users individually.

Three primary rules are defined for RBAC:

* Role assignment: A user or resource can exercise a permission only if the user or resource has selected or been assigned a role.
* Role authorization: A user’s or resource’s active role must be authorized for the user’s or resources. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.
* Permission authorization: A resource can peroform a permission only if the permission is authorized for the resource’s active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorized.

With RBAC, access management is easier if you adhere strictly to the role requirements. RBAC helps you:

* create systematic, repeatable assignment of permissions.
* easily audit user privileges and correct identified issues
* quickly add and change roles, as well as implement them across APIs.
* cut down on the potential for error when assigning user permissions.
* integrate third-party users by giving them pre-defined roles.
* more effectively comply with regulatory and statutory requirements for confidentiality and privacy

Single Sign On:

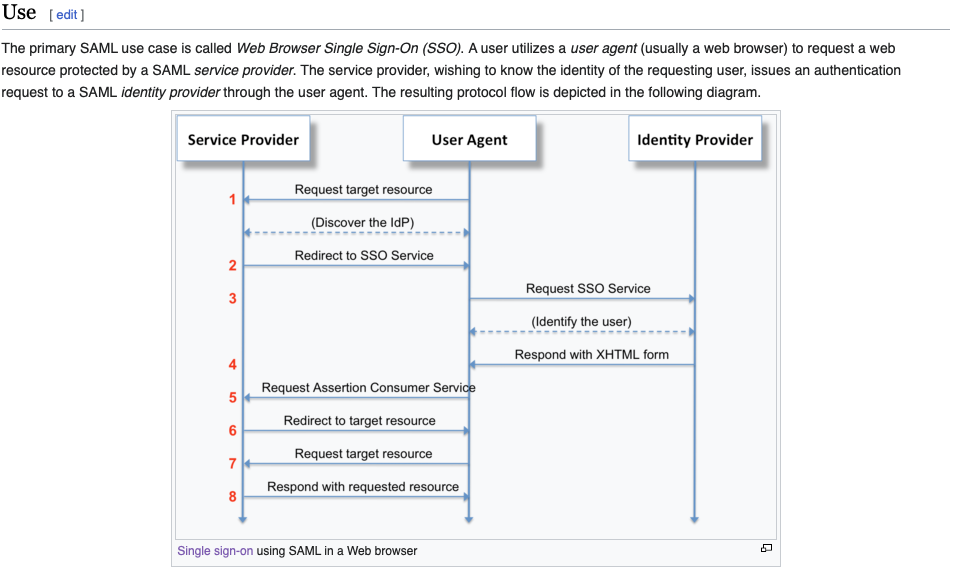
SSO is an authentication solution that allows users to log in to multiple applications and websites with one-time user authentication. SSO establishes trust amongst the application or service and an external service provider, also known as an identity provider (IdP). An SSO service is a central service that applications rely on when a user logs in. A simple version of single sign-on can be achieved over IP networks using cookies but only if the sites share a common DNS parent domain.

The SSO process is as follows:

* When a user signs in to an application, the app generates an SSO token and sends an authentication request to the SSO service.
* The service checks if the user was previously authenticated in the system. If yes, it sends an authentication confirmed response to the application to grant access to the user.
* If the user does not have a validated credential, the SSO service redirects the user to a central login system and prompts the user to submit their username and password.
* Upon submission, the service validates the user credentials and sends the positive response to the application.
* Otherwise, the user receives an error message and must re-enter credentials. Multiple failed login attempts could result in the service blocking the user from further attempts for a fixed period.

SAML (Security assertion markup language):

It is an open standard for exchanging authorization and authentication data between parties between an identity provider and a service provider. SAML is an xml based (extensible markup language; a file format for storing, transferring, and structuring arbitrary data. It defines set of roles for encoding document that are both machine and human readable) markup language for security assertion. An important use case that SAML addresses is web browser single sign on.



SAML assertions are usually transferred from identity providers to service providers. Assertions contain *statements* that service providers use to make access-control decisions. Three types of statements are provided by SAML:

* Authentication statements.
* Attribute statements.
* Authorization decision statements.

AAA Framework:

AAA refers to Authentication (to prove identity), Authorization (to give permission) and Accounting (to log an audit trail). It is a framework used to control and track access within a computer network.

**What are the (AAA) Protocols?**

* TACACS+ (Terminal access controller access control system): Cisco Based and Less popular.
* Radius: Open Standard and More Popular
* Diameter

Based on OSI Model — All Protocols are running on Layer 7 which means they have a payload to carry information to the network.

Security Best Practices for Identity:

* Implement least privilege access controls to ensure that users only have access to the resources necessary to perform their job functions.
* Regularly review and update access permissions to reflect changes in roles, responsibilities, or business requirements.
* Enforce strong password policies, including requirements for complexity, length, and regular password changes.
* Monitor user activities and access logs for suspicious behaviour, unauthorized access attempts, or policy violations.
* Educate users about security awareness and best practices to mitigate the risk of social engineering, phishing attacks, and other security threats.

Compromised Systems

If your system has been compromised, somebody is probably using your machine--possibly to scan and find other machines to compromise. There is no automated method for cleaning up a compromised machine. Our recommendation:

* Back up important personal files
* Reformat the hard drive.
* Reinstall the operating system and software.

signs indicating a system is compromised:

* Fake antivirus messages
* Unwanted browser toolbars
* Redirected Internet searches.
* Frequent random popups
* Your friends receive fake emails from your email account.
* Your online passwords suddenly change.
* Unexpected software installs
* Your mouse moves between programs and makes correct selections.
* Your antimalware software, Task Manager, or Registry Editor is disabled and can't be restarted.
* Your bank account is missing money.
* You get calls from stores about non-payment of shipped goods.