# Identity Manager

Identity manager provides the following 4 key capabilities:

1. User Portal
2. Enterprise Identity Management
3. Enterprise SSO
4. Enterprise App Store

You can implement Identity Manager using on-premises or SAAS model.

In an on-premise implementation, Identity Manager is deployed as a windows installer to handler authentication and provide SSO services to application. In a SAAS implementation Identity Manager Connector synchronizes user account from Active Directory (AD) to Identity Manager Service. Apps can then be accessed from browser based portal.

Because Identity Manager tenant is cloud based you do not have to make design decisions regarding database, network access, or storage considerations. Identity Manager service scales to meet virtually any organization size.

Connectivity to the Identity Manager service is through port 443. This connection is used for directory synchronization, authentication, and syncing entitlements for resources. Organization can take advantage of this with no additional inbound firewall port open to the internet.

Initial configuration involves logging on to Identity Manager service with provided credentials.