Active Directory Cloud Portal
For IT Service Providers
Version 2.0

Supports AD Management As a Service

Multiple AD Domains

Single Browser Access

Real-Time - Bi-Directional Info

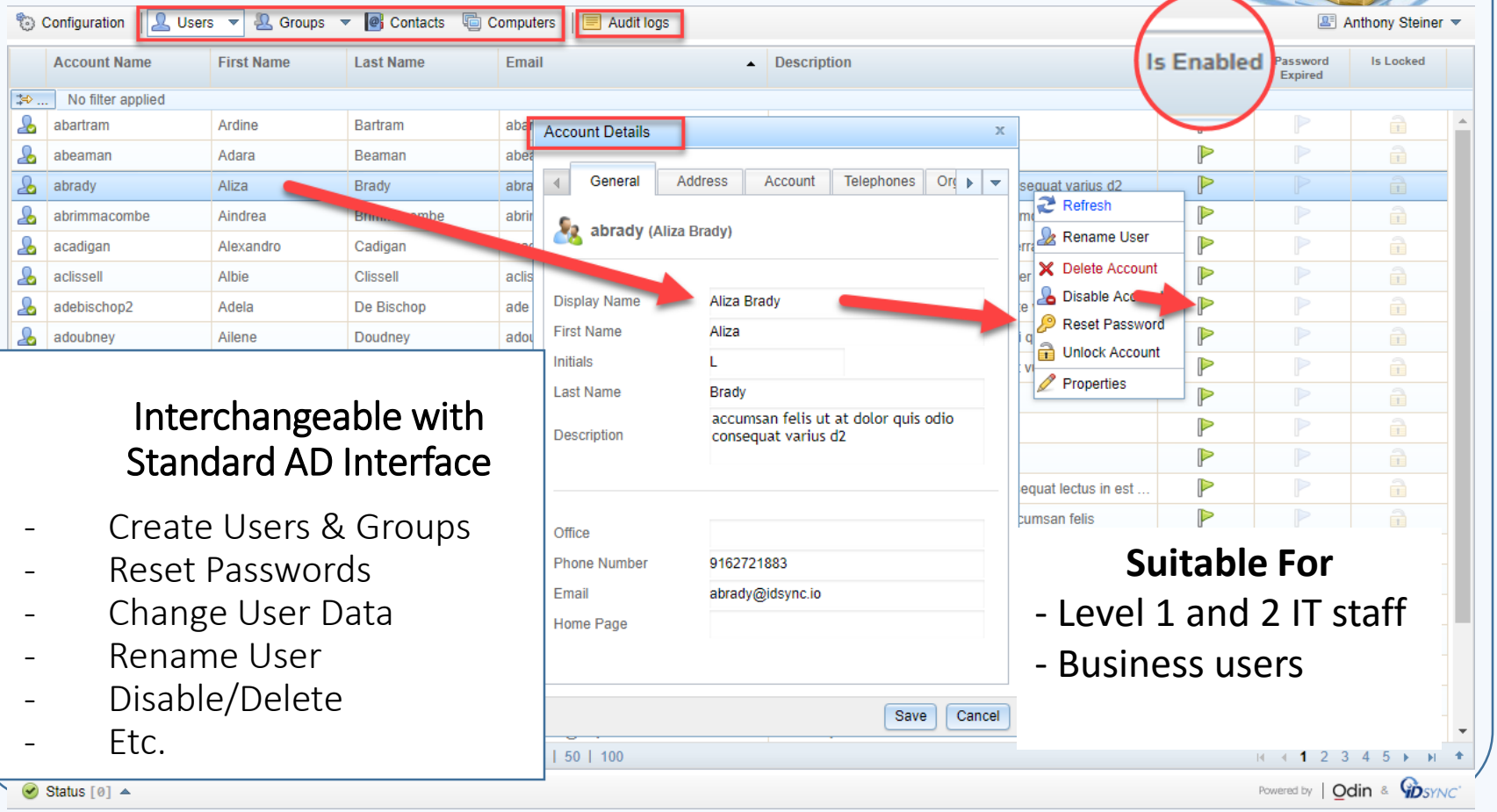
Active Directory Cloud Portal Summary

- The whole intent of the product is to lower the cost of IT support as it pertains to AD management.
- Active Directory Cloud Portal allows a service provider to offer AD Management as a service, using only a web browser to securely manage their many customers' on-premise Active Directories without VPN's, RDP, sharing passwords or other costly, risky practices.
- In short, a quicker, more secure, more effective way for a smaller IT service provider to provide managed AD services to many customer or larger service organization to manage access and changes to their customers multiple AD's through a single web interface without the need to provide highly privileged user accounts to the service engineers.
- Privileges and rights can be managed in such a way that it would tolerate and encourage providing direct AD access to some departments, perhaps human resources or department managers without violating security norms.

AD Cloud Portal - Objectives

- Manage AD Users From Cloud Portal
  - Solves Problems, Cost, Delay of Direct AD Login
    - VPN required, RDP, Firewall Issues, Login Effort/Delay
- Provide secure and limited access to non-IT staff
  - Managed Service for Customers
  - Internal Management of Users & Groups
    - Wide Range of user types
    - From IT to Human Resources & Dept. Managers
- Create service platform/tool for additional revenue
  - “Managed AD Users as a Service”
  - A hosted software service that can be resold to larger customers.
    - Target Market is similar in size to Office 365

AD Cloud Console
Security Trimmed Rights



Interchangeable with Standard AD Interface

- Create Users & Groups
- Reset Passwords
- Change User Data
- Rename User
- Disable/Delete
- Etc.

Suitable For

- Level 1 and 2 IT staff
- Business users

Access to Active Directory Does Not Scale Well

- But Security requirements demand narrow access
  - Usage of AD does not scale well
    - Remote access requires VPN and RDP for each user
    - Or, Desktop sharing
    - Setting access/security limitations in AD is complex technical task, difficult to delegate
  - Result
    - Inhibits Availability of AD
    - Higher Cost, Slower Service
    - Limits Users to IT staff
    - Limits info access to IT staff
    - Limits Geographic access without VPN/RDP tools

Active Directory - Access Limitations

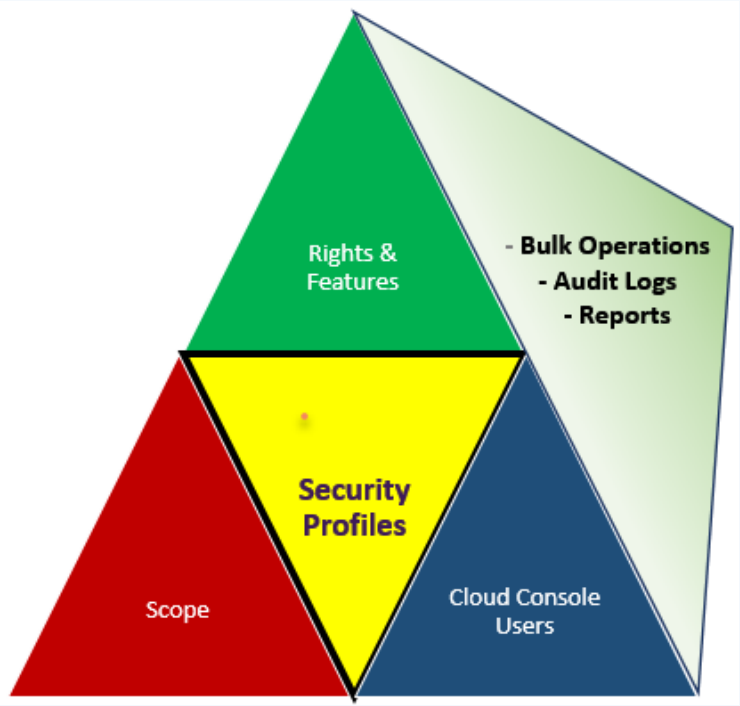
- AD is the Heart of IT – Needs to be safe
  - Restricted to IT Staff
- Excludes other Employees
  - Excludes contractors, vendors, partners
- Local LAN – On Premise Installation
  - Remote or Mobile access to AD requires
    - Privleged AD user, VPN/ RDP Remote Access for each Service Engineer
- If Multiple AD's Quick Access, Login Latency
    - Need to find VPN/RDP login credentials at time of service
    - Results in high logistical complexity
- Sharing of Passwords is many times a typical response.
  - Efficient but risky
- Weak or non-existing Audit trail
- No Sharing of Workload
  - All work must be routed through and performed by IT
  - Slows down both the access and disablement process.

Use Cases for AD Cloud Portal

- IT Help Desk
  - Level 1, Mobile, Multiple AD's, Larger Staffs, Audit Trail
- IT Service Provider
  - With many smaller customers
  - With large enterprise customers
  - With Security Sensitive Customers
    - E.g., Financial, Medical, Government, etc.
- Larger Enterprise
  - Shared AD Management
  - Accountability
  - Human Resources Staff
  - Department Managers
  - Receptionist
  - Security Guard
  - Individual User

What if you could have both secure access and widely distributed access at the same time?

Security Studio Concepts



Security Studio – Access control to limit or enable AD Cloud Portal users.

Security Profile(s) – Used to combine Rights, Scope and Cloud Console Users into a role based template.

Scope – Those AD users or groups or OU's that can be affected by rights or features.

Cloud Console Users – Those authorized to make AD changes per a profile

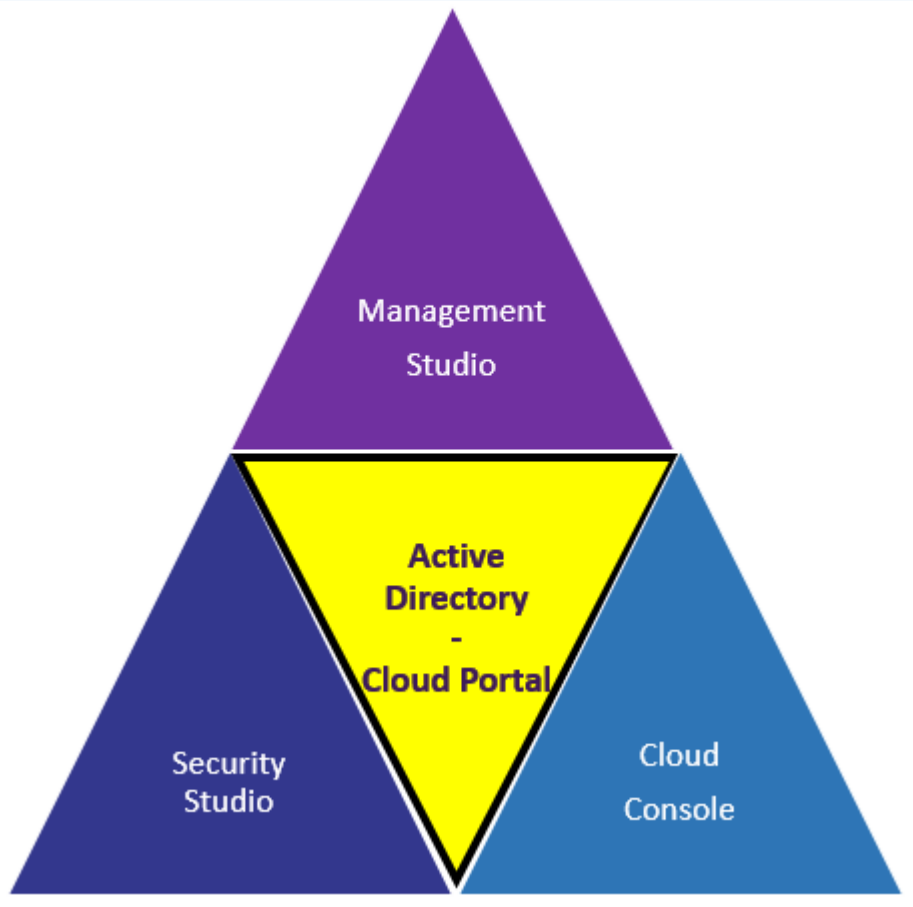
Security First - Rights & Features

AD Cloud Portal - Designed to both Enable & Limit
By Action and By Object Type

Action Type
AddAsMember
AddMember
ChangePassword
Create
Disable
Enable
Read
Registration
Remove
RemoveMember
Rename
Unlock
Update

Object Type
Computer
Contact
Feature
Group
Profile
Report
Scope
User

AD Cloud Portal Components

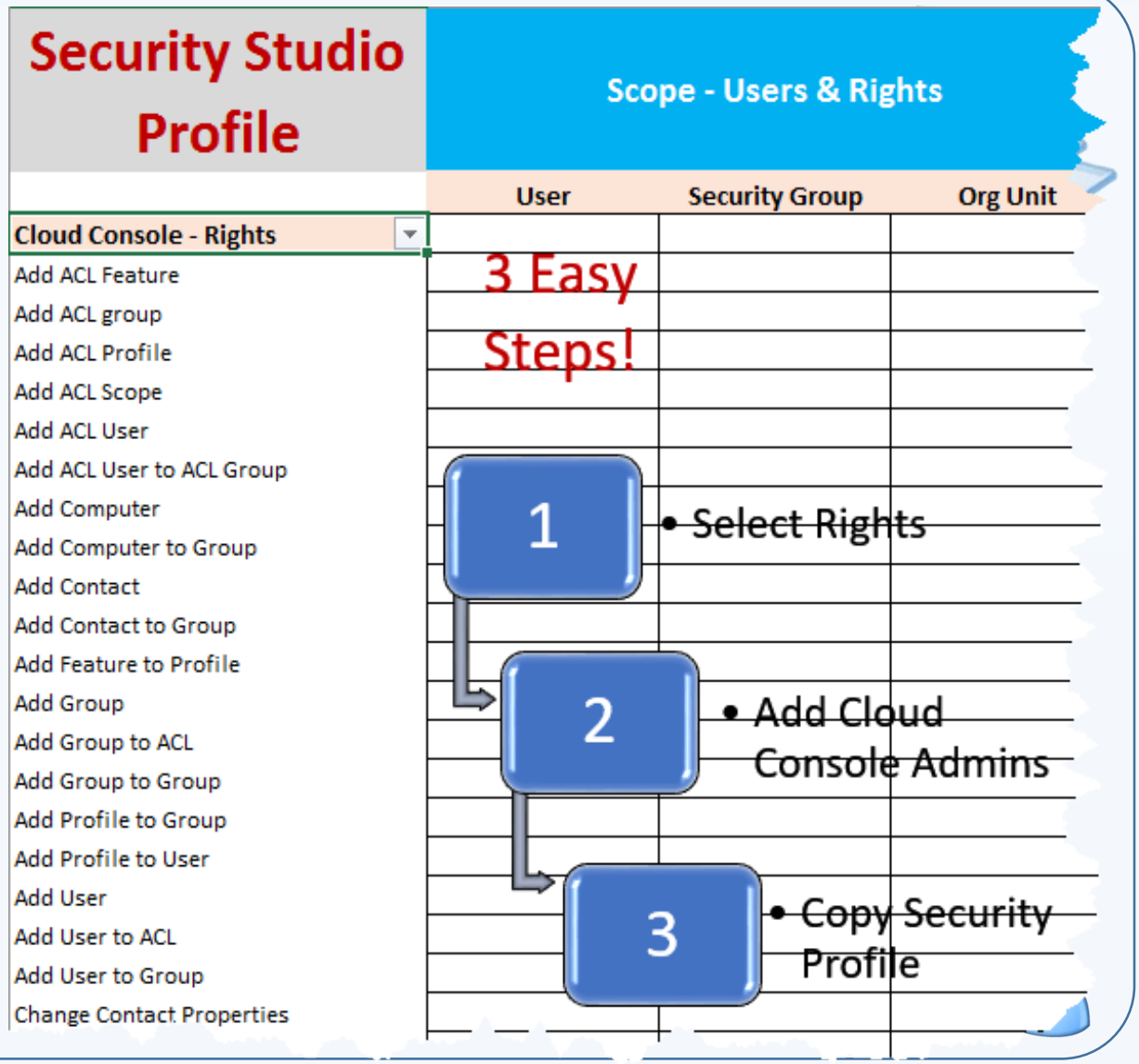


Management Studio – Used for software setup and access to Audit log

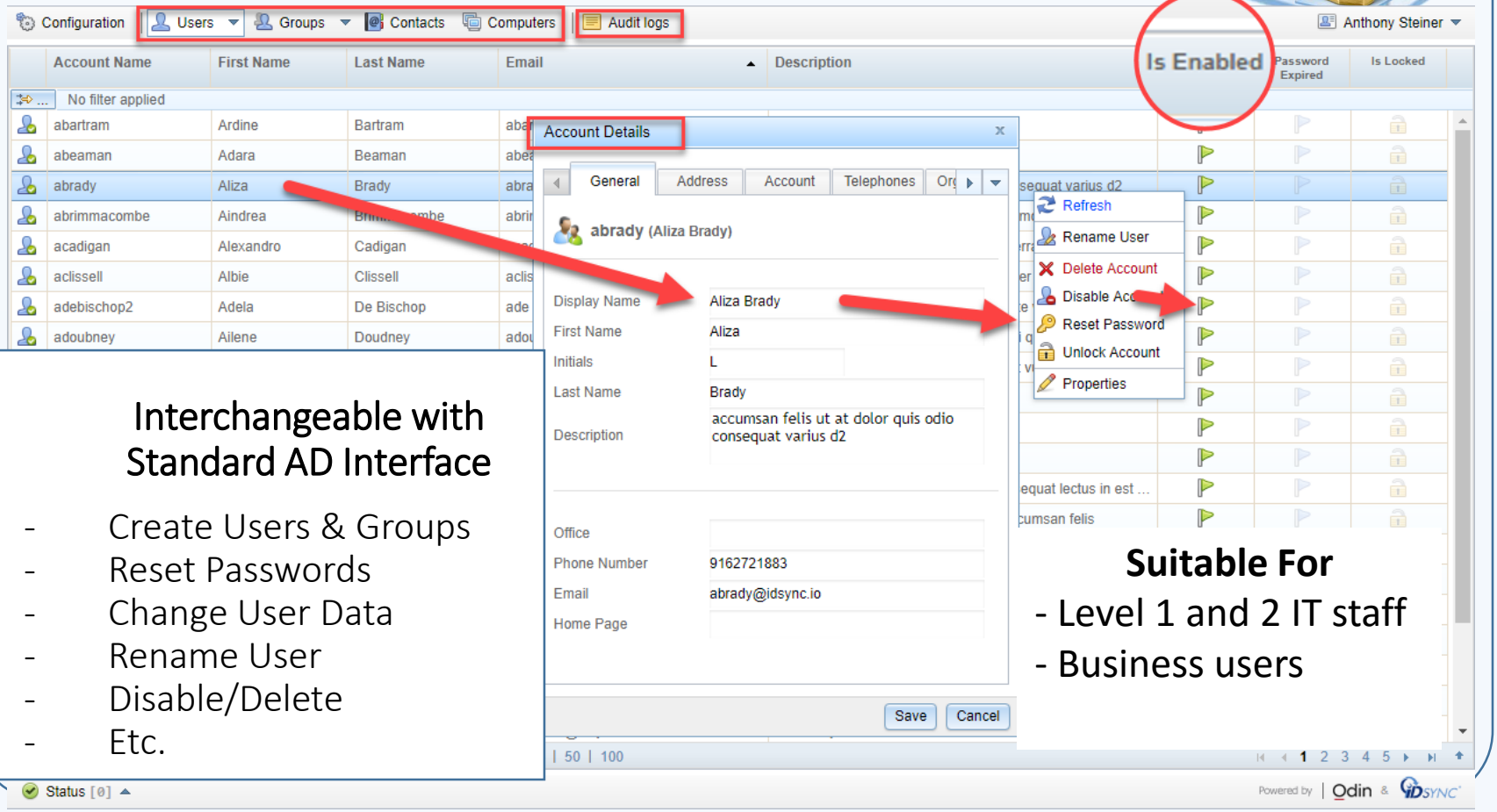
Security Studio – Access Control to enable or limit Cloud Console OR Security Studio use.

Cloud Console – Browser UI used for changes to AD users & groups

Create a Security Template to assign access to rights and users.



AD Cloud Console
Security Trimmed Rights



Interchangeable with Standard AD Interface

- Create Users & Groups
- Reset Passwords
- Change User Data
- Rename User
- Disable/Delete
- Etc.

Suitable For

- Level 1 and 2 IT staff
- Business users

Just Imagine….

- HR adds new employee to AD eliminating delay and communication costs.
- Receptionist resets user passwords reducing cost of help ticket
- Manager changes employee access to department resources providing the tools as needed.
- Security Guard has access to employee data to verify credentials
- IT Service provider can securely manage customer's AD via level 1 help desk staff and transaction is recorded for audit.
- User disablement is convenient for "C" level and HR, no longer having to come in on Friday night to disable user records.
- Auditor and Security staff provided with an audit log that tracks all changes to AD and to Security Studio
  - Access Rights
  - Changes to AD user records

Summary
AD Cloud Portal Benefits

- Ability to change customer AD data from a web browser
  - Reduces IT support costs
  - Enables Business Users
  - Provides easier access to AD
  - Reduces customer frustration with password issues
  - Improves Customer service and response times
  - Increases Revenue Opportunities
  - Improves AD security – No need for shared logins
  - Accountability – Makes audit easier, less expensive
  - “Security Trimmed” access to AD data
  - Two Factor Authentication