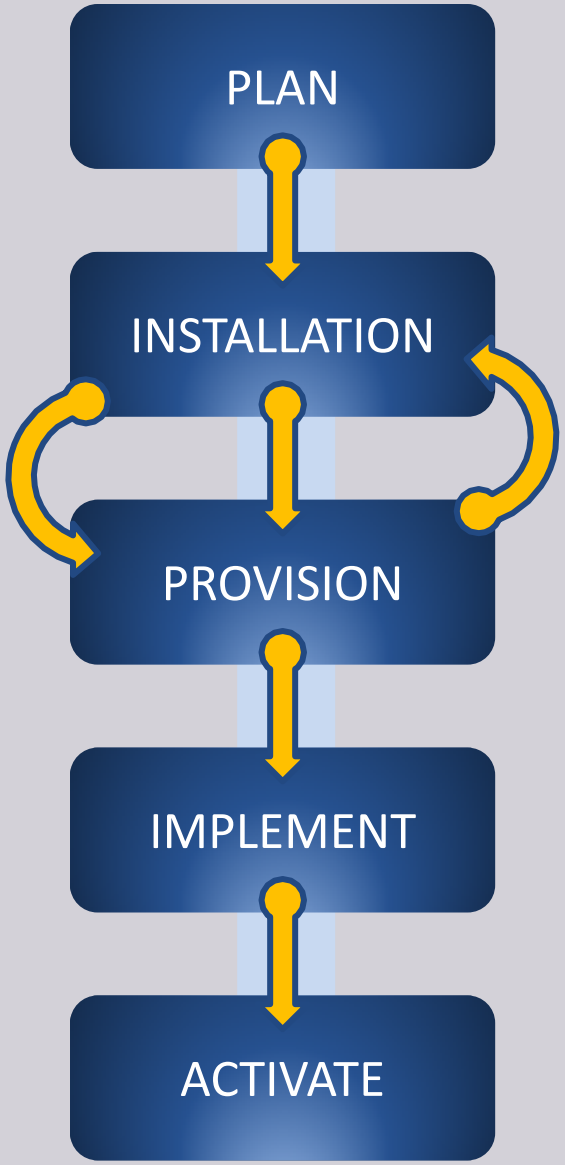
CyberArk University

Application Identity Manager (AIM)
4: Implementation

CyberArk University

Implementation Overview

Application Identity Manager Implementation Overview

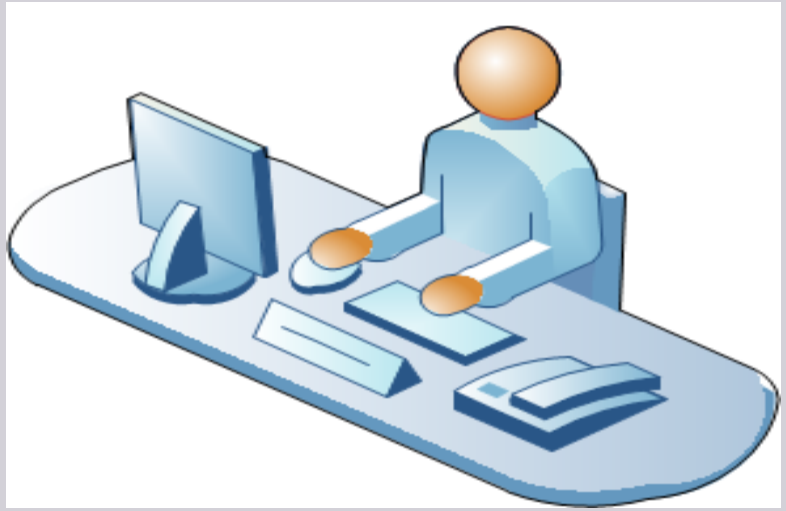


- Planning & Designing Deployment
- Provider Installation (Configuration Optional)
- Provision Provider & Application(s) in Vault
- Implement Application Password SDK
- Activate Application Password Request(s) Initially

Developers Enablement

The Key to Success!!

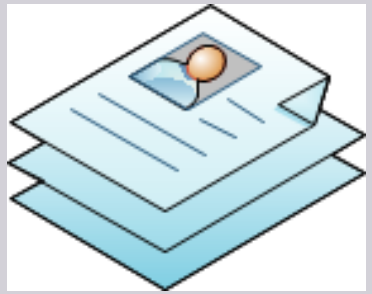
- Standard interface
- Decision matrix
- Training
- Documentation



Provide the right tools

Developers Tool Kit

Decision Matrix



- Pull or Push modes?
- Application Platform?
- Manual, Semi-Automated, or Fully Automated Change?
  - Manual: No CPM Involved
  - Semi: High-Load Applications (on demand CPM request)
  - Fully – No Human Intervention Required

Training and Documentation

- What is the wrapper?
- How does the development process look like?
- Testing techniques

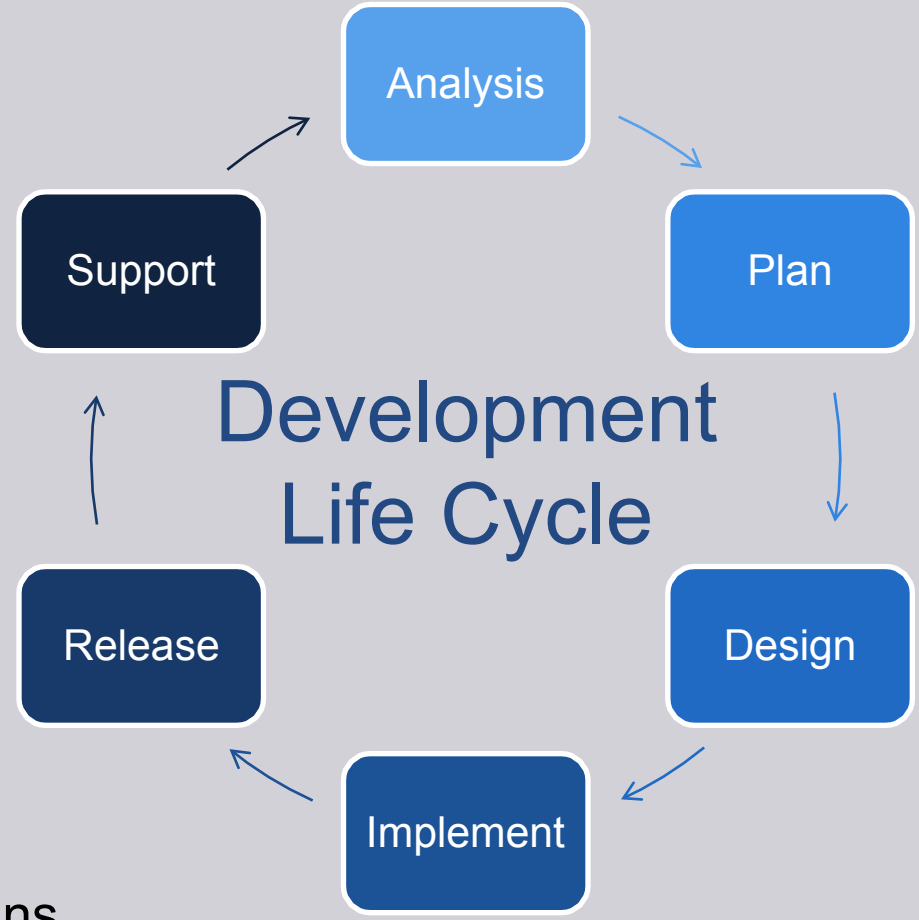
CyberArk University

Planning & Design

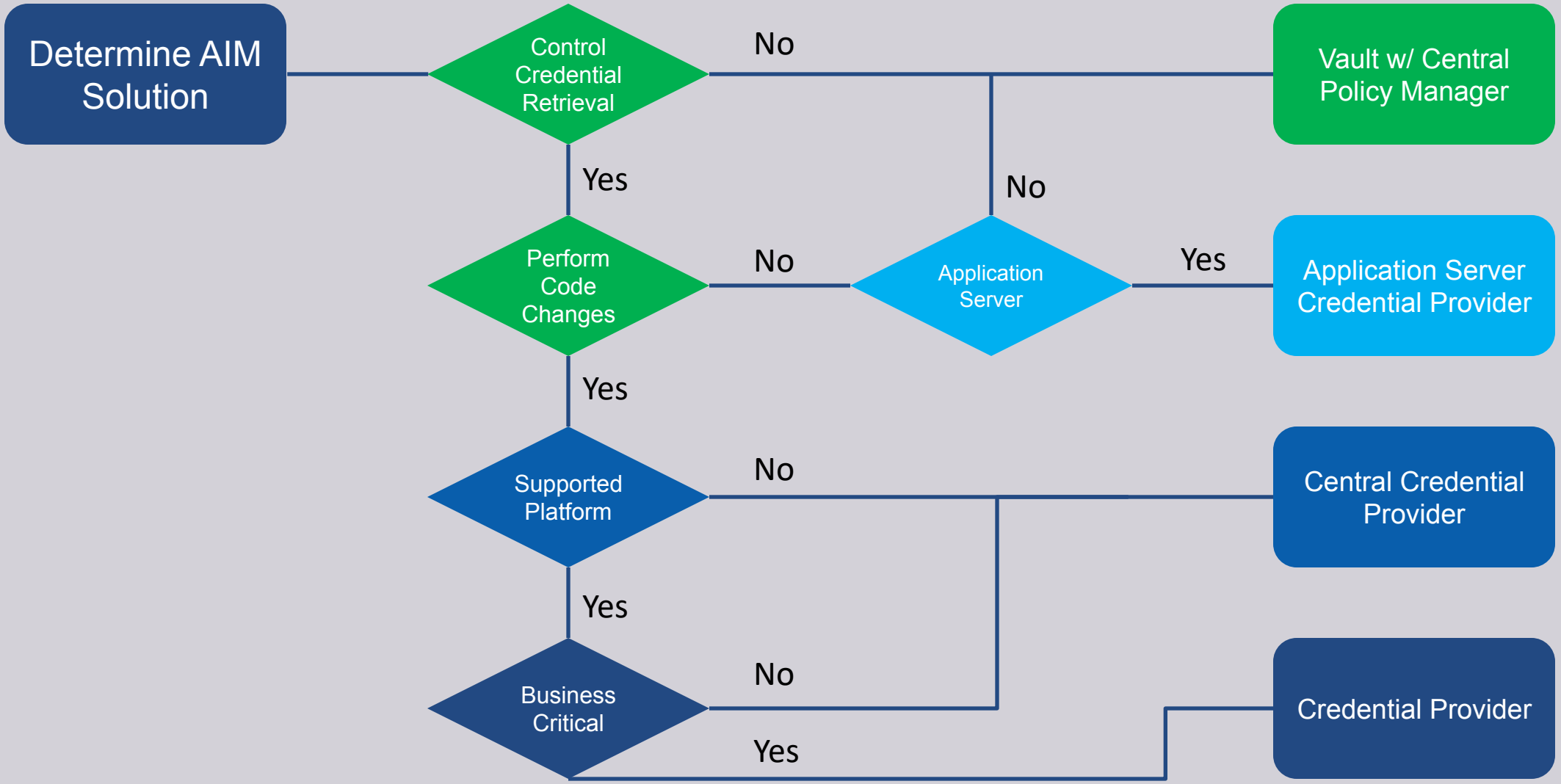
Implementation Life Cycle

Initial Application Integration

- Dev Environment
  - No provider is required
  - Focus on application code changes
- Test
  - Integrate standard interface w/ Provider
  - Test AIM configuration and processes
- Production
  - Verify before deploying the application
- Ongoing Life Cycle
  - Define which application changes require Vault Admins
  - Use change management system



Decision Matrix



Roles and Responsibilities

Vault Admins

- Application Provisioning
- Safes Provisioning
- Provider Provisioning

Application Owners

- Accounts Provisioning

Developers

- Code Changes
- Application QA & Testing

Operations

- Provider Provisioning

Vault Admins

Application Teams

Developers & DBAs

Project Planning – Design Phase

Administration

- ✓ Roles & Responsibilities
- ✓ Workflows
- ✓ Provider Installation & Provisioning
- ✓ Maintenance & Support

Development

- ✓ Standard Interface
- ✓ Password SDK Integration
- ✓ Provider Account Query Methods
- ✓ Change Methods & Procedures

Application Provisioning

- ✓ Safe Design & Naming Convention
- ✓ Access Control List
- ✓ Application ID Convention
- ✓ Application Authentication

Tips & Pointers

The formula to a successful project

Project Milestones

- Identify applications with hard-coded credentials
  - CyberArk Discovery & Audit (DNA) can help
- Prioritize according to business needs
- Define internal policies

Identify & Involve Stakeholders Early

- Development teams, application server teams, information security teams, audit department, project managers, architects, IT, etc

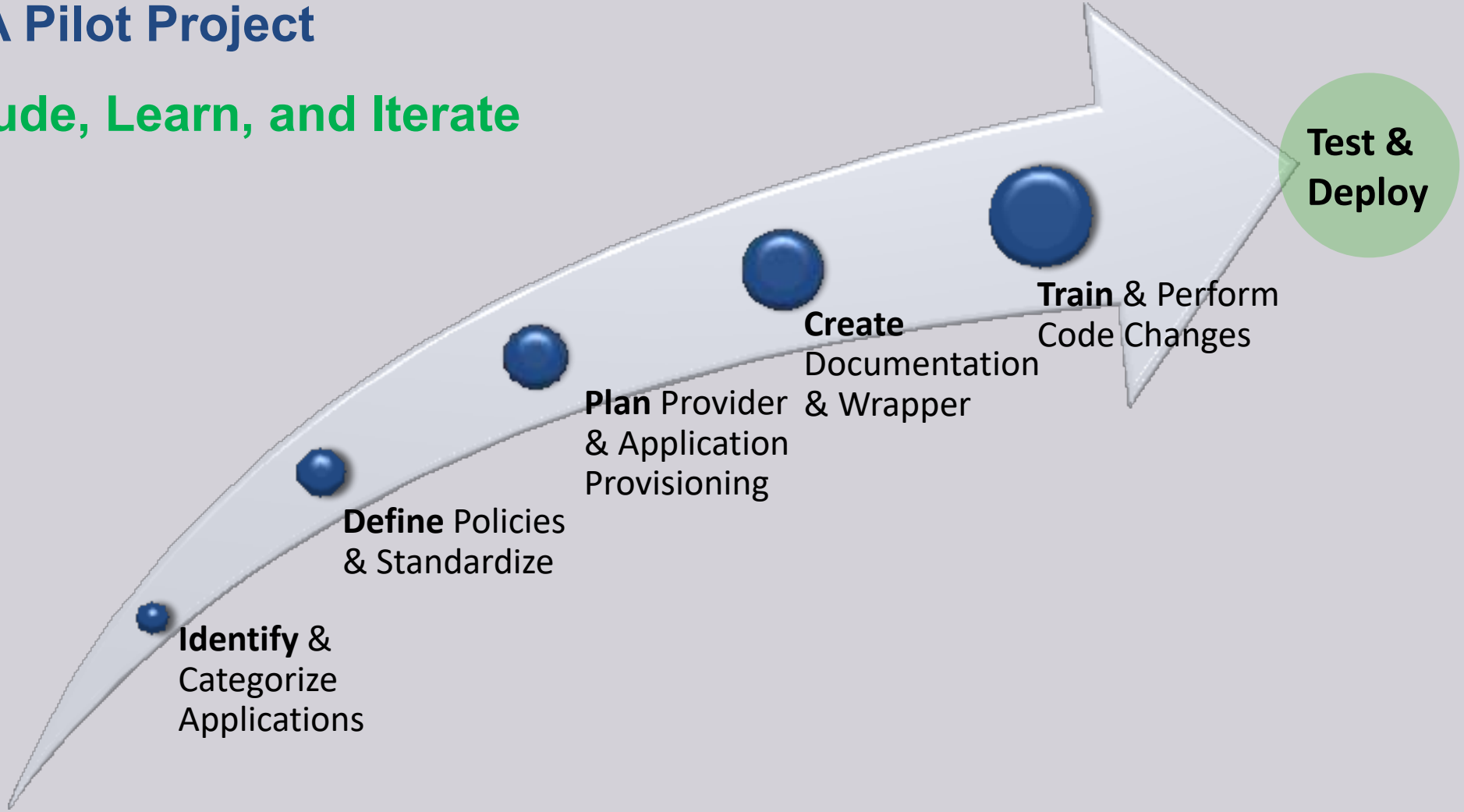
Phased Approach

- Start with what's easiest to implement:
  - Improve Security Posture → frequently "push" credentials and automatically rotate. At a later phase, move on to completely eliminating credentials.
  - Application Server Credential Provider → robust and secure solution (**requires no code changes)**
- New applications – develop applications without hard-coded credentials
- Existing applications – slowly migrate and eliminate hard-coded credentials

Project Deployment Schedule

Start A Pilot Project

Conclude, Learn, and Iterate

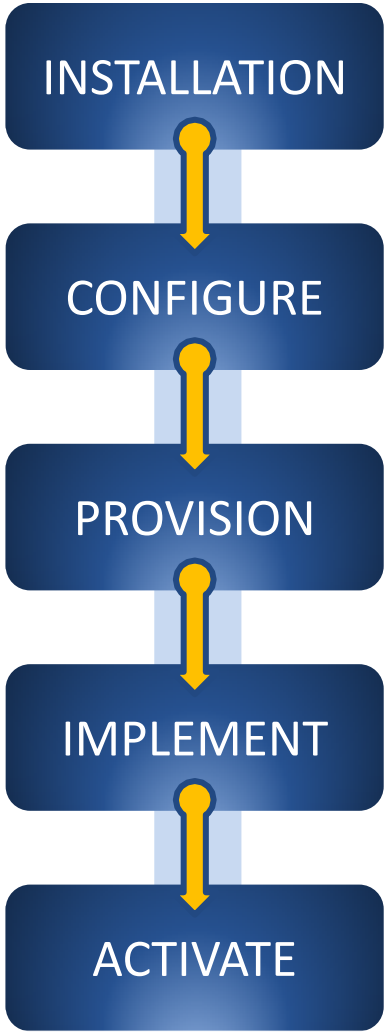


CyberArk University

Provider Installation & Configuration

Installation Workflow

- 1. Install the Credential Provider.
- 2. Configure the Credential Provider. This determines which features will be implemented and how they will work.
- 3. In the Vault, define each application that will request passwords. This will enable the Credential Provider to retrieve passwords for applications.
- 4. Implement the Application Password SDK in your code.
- 5. Using the SDK, activate the application password request manually the first time to retrieve passwords to the cache.



Install / Upgrade Methods

Interactive Installation / Upgrade

Vault administrator or other user is required to manually initiate the installation executable and to provide information throughout the process interactively.

Silent Installation / Upgrade

Installation procedure is initiated either by a user or by a script, and is performed without any human interaction. This is useful when installing multiple Credential Providers in a large environment, providing a fluent and automatic installation process.

Manual vs. Automated Provider Provisioning

- Installation wizard / package installer will provision all necessary Vault settings automatically
- Manual provisioning provides custom controls on a per Provider basis
- Automated provisioning using the installer packages offer no customization or control

Provider Provisioning – Vault Settings

Initial Provider Provisioning

- ✓ Create \Application Location
- ✓ Create Configuration Safe (***AppProviderConf)***
- ✓ Upload Shared Provider Config Files
- ✓ Create Provider Group (***AIMProviders)***
- ✓ Assign Group to AppProviderConf membership
- ✓ Create Provider User **Prov_<hostname>**
- ✓ Assign Provider User to Account Safe(s) membership

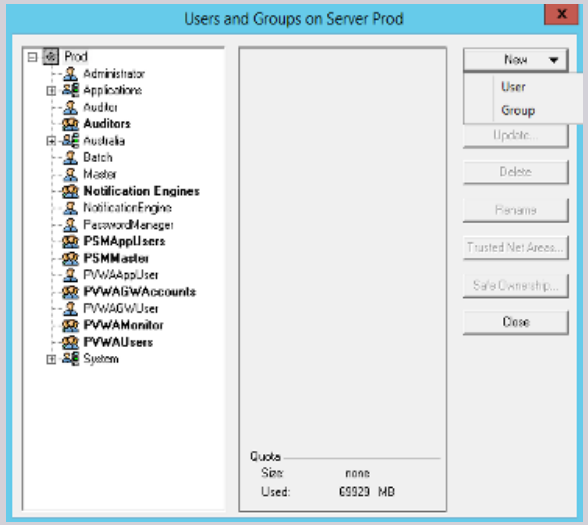
Additional Provider Provisioning

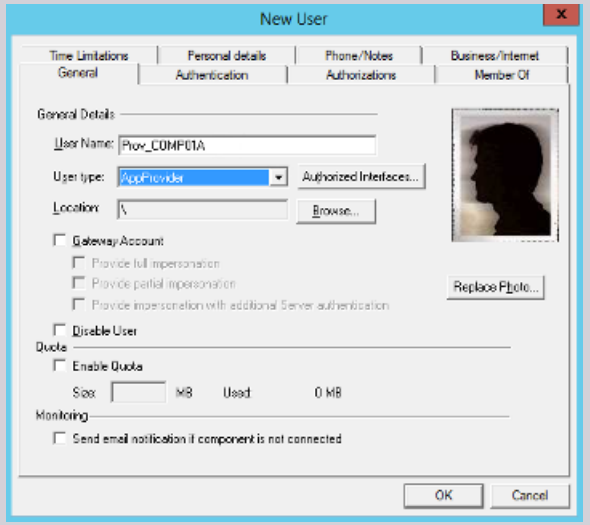
- ✓ Create Provider User **Prov_<hostname>**
- ✓ Add Provider User to **AIMProviders** Group
- ✓ Assign Provider User to Account Safe(s) membership

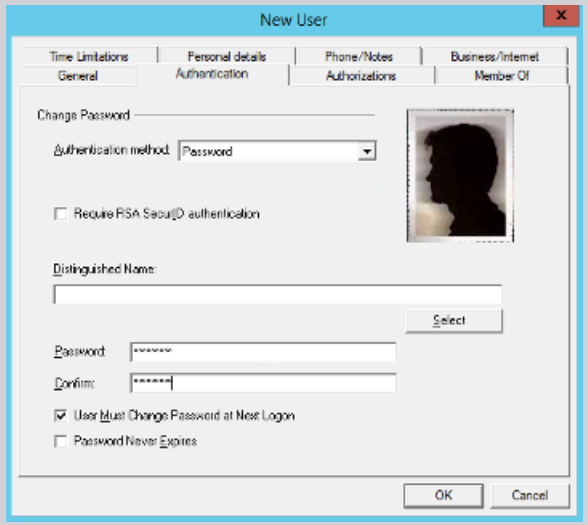
Create Provider User

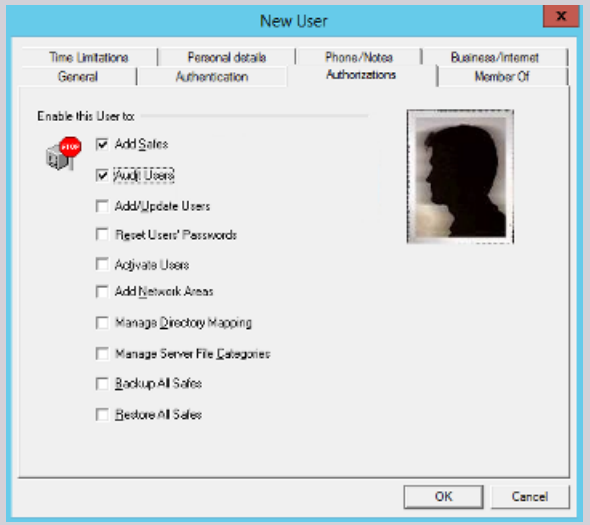
Create Provider User

- Log into PrivateArk Client as Vault Admin
- Create Provider User and assign initial password
  - Set "User type" as AppProvider
  - Add Provider User(s) to **AIMProviders** Group (optionally add Provider User during Providers Group creation)
  - Grant **Add Safes** and **Audit Users** vault authorizations to user









Password will be changed by Vault upon first login

Create Providers Group

Create Providers Group

Used to grant safe authorizations to each Provider to access AppProviderConf safe

- Log into PrivateArk Client as Vault Admin
- Create **AIMProviders** Group, add Provider User(s) membership
- Add AIMProviders → **AppProviderConf** safe membership

Authorizations:

Access: List Files, Retrieve Files

Update: Create Files, Update Files, Update File Properties, Rename Files

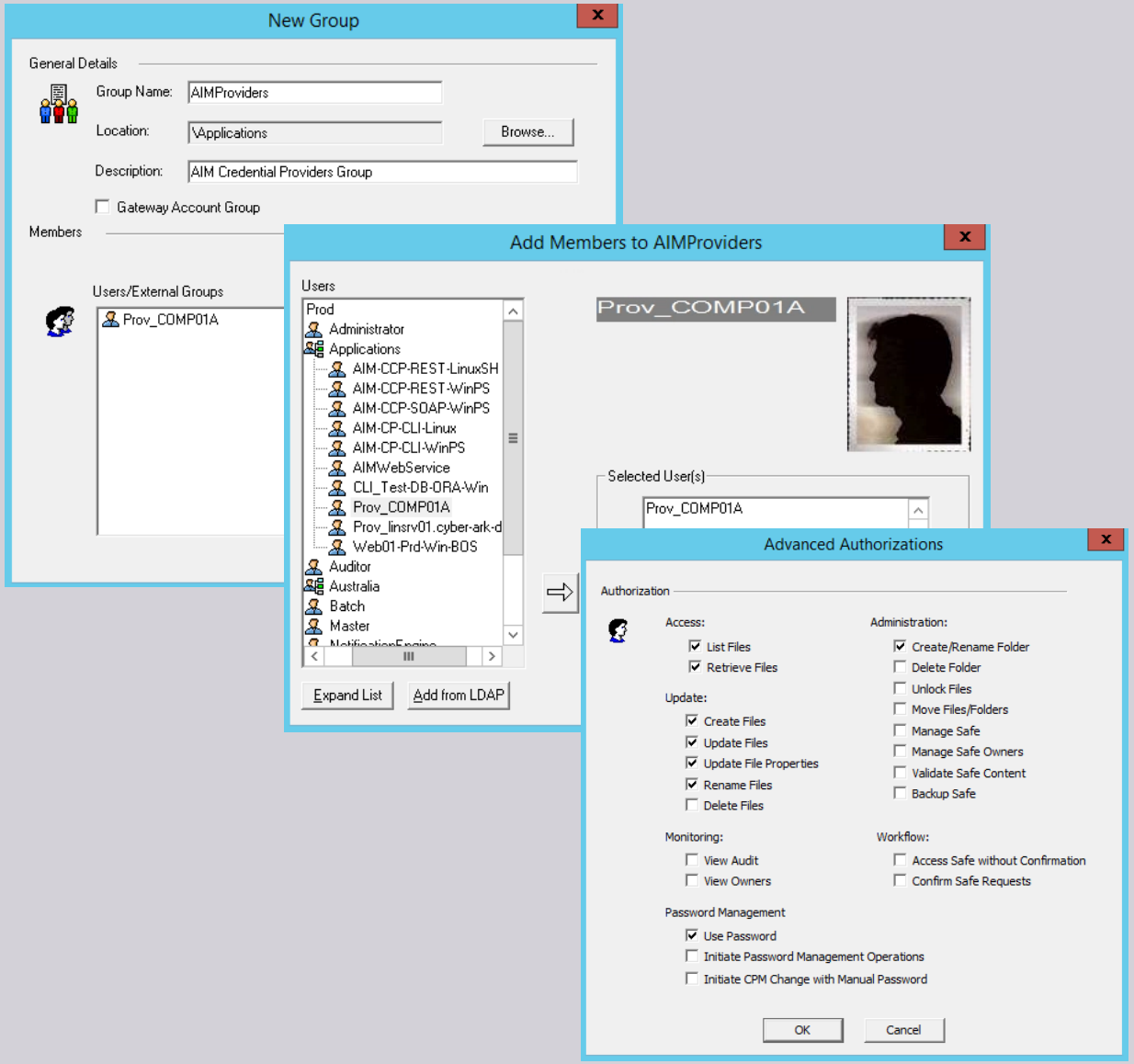
Password Management: Use Password

Administration: Create/Rename Folder

- Add AIMProviders to **PVWAConfig** safe membership

Authorizations:

Access: List Files, Retrieve Files



Provider Provisioning – Manual Install Settings

1. Install Provider

- Install Credential Provider without having the installer automatically setup and configure the Provider settings

2. Vault.ini

- Add Vault IP Address
- (Optional) Add parameters

3. Credential File

CreateCredfile <filename> Password – Username <username> -Password <password>

4. Create Environment

CreateEnv [Username][Password][InstallationFolder][AppProviderConfSafe][MainAppProviderConfFilePath][AppProviderUser][AppProviderUserLocation][OverrideExistingConfFile]

5. Verify Environment

- Check logs to verify Credential Provider environment successfully created
- <Install_Dir>/Logs/CreateEnv.log

6. Start Provider

Start Credential Provider Service

Windows: CyberArk Application Password Provider

Linux: *aimprv start*

Install, uninstall, and start/stopping running services require root and/or administrator user privileges

Create Provider Configuration & Environment

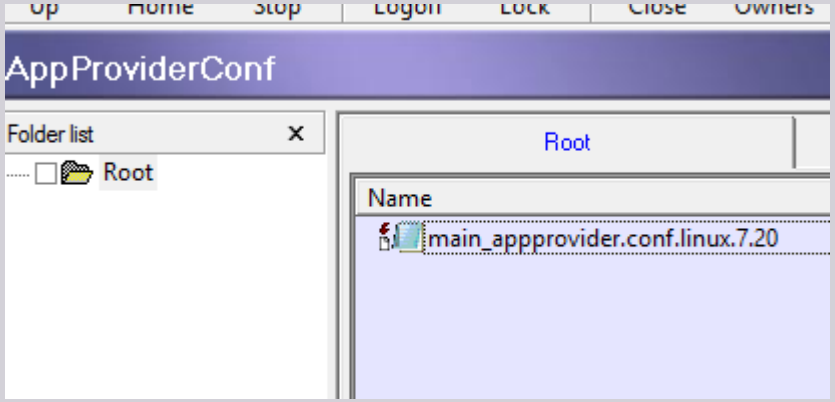
Provider Configuration

- Create configuration and environment for each platform and Credential Provider operating system environment

1. Install Provider via installer package manually initially for each platform

OR

2. Execute **CreateEnv** utility for each platform

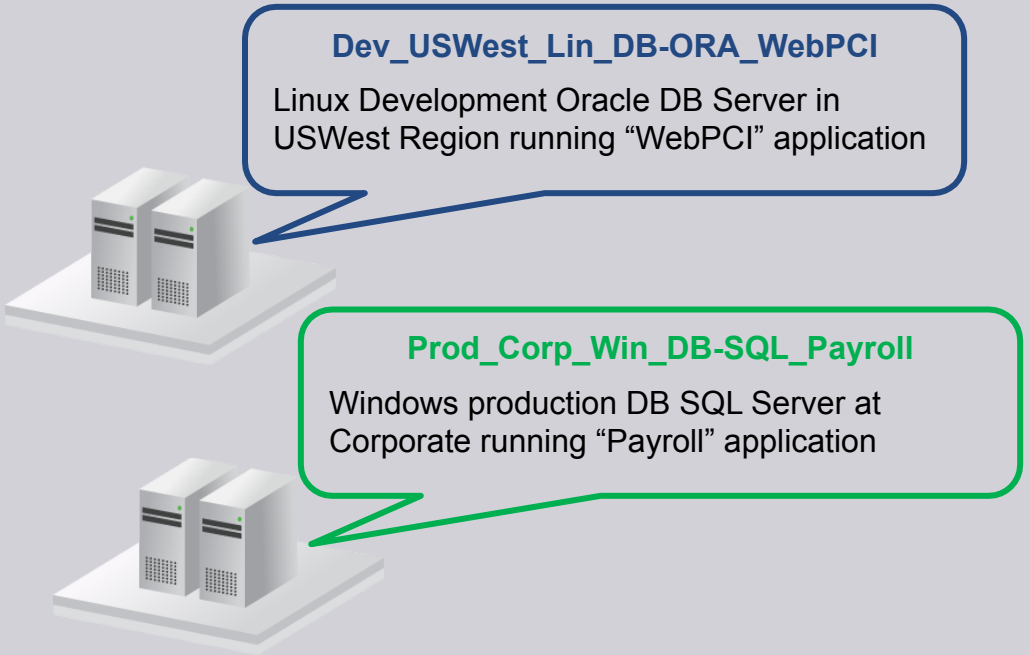



```
[Main]
MaxConcurrentRequests=40
AutomaticParmsRefreshInterval=3600
ProviderCacheFolder=/var/opt/CARKaim/cache
OfflineUpdateInterval=1800
OfflineUpdateRetries=600
#DefaultDomain=
#UnixUserFormatRegexp=1,2,(.*)\\(.*)

[Debug]
#CacheDebugLevels=1,2
#AppProviderDebugLevels=1,2,3,4,5
#ProtocolDebugLevels=1,2
#PIMSuDebugLevels=1,2,3,4,5

[Cache]
CacheLevel=persistent
CacheFile=/var/opt/CARKaim/cache/appprovider_cache.dat
CacheRefreshInterval=180
VaultAccessInterval=31536000
```

Safe Provisioning

Safe Design Best Practices

- ✓ Naming convention should follow existing convention
- ✓ Typically includes application identifier (AppID)
- ✓ Define Access Control
  - What Privileged Account Credentials?
  - Who Requires Interactive Access?
  - What Application and/or Services Require Access?



Convention Sample:

<Phase>_<Location>_<Environment>_<Function>_<Application>

Phase: Dev, Test, Prod

Location: Datacenter Location

Environment: Operating System Architecture

Function: Functional Use / Credential Type (i.e. Oracle Database)

Application: Application Name or Identifier