Tiered OUs / The Admin OU

secframe.com/docs/ramp/phase1/paws/paws_admin_ou

November 1, 2020

Begin work towards the Red Forest.

=======

With a base understanding of tiers, administrators, unique passwords for computers and a brief definition of why a privileged access workstation is needed for Active Directory Security, it's time to start investing time into making changes in the environment.

Prerequisites

1. Download the PAW script from the technet library. PAWS OU Creation Script

PAW Scripts

The zip linked above on the technet article have three scripts with three specific purposes

Script	Purpose
1. Create-pawOU	Set up new OU for tiered administration
2. Create-pawGroups	Import groups.csv to create a sample tiered administrator set
3. Set-PAWOUdelegation	Use the groups above and set the proper delegation on the new OUs created

> Beginning to deploy Active Directory security is as easy as 1, 2, 3

1. Create OUs
2. Create Groups
3. Push delegation

Administrative PAW OU Structure

The Create-PAWOU script sets up an OU structure to allow administrative objects to be separate and secure from standard AD objects. The Script goes through steps to set up the following structure:

Admin OU Drawn Out

What This Post Covers

1. Create Administrative OUs

> Remember there is plenty of work to do. Eventually the focus will shift to Tier 1 and Tier 2 credentials. For this small moment in time, FIRST make sure Tier 0 is secure as possible.

Protecting Active Directory and Admin Users and Privileges by creating an administrative OU

CENTRALIZE ADMINISTRATIVE ACCOUNTS:

The location of the administrative users and groups is often overlooked. If I were to perform an audit on any random domain, there's a major chance that I'd find administrative accounts scattered across multiple Organizational Units.

> Often by accident this scattered user placement creates pathways that attackers exploit to gain higher level of privileges.

---

1. Create Organizations Units

Active Directory PAW & Admin OU Layout

Back to the OU Top

The privileged organization unit deploy is a bit different mindset for administrators. Understand that the admin OU is created specifically to secure the Active Directory Domain.

** These OUs are deployed by running the `create-pawou.ps1`

> Security > Everything Else

Base Admin Organizational Unit Structure

Back to the OU Top

1. The base OUs are created to store all the relative objects.
2. The base OUs are at the top of the domain, the first level of OUs possible to create on the domain

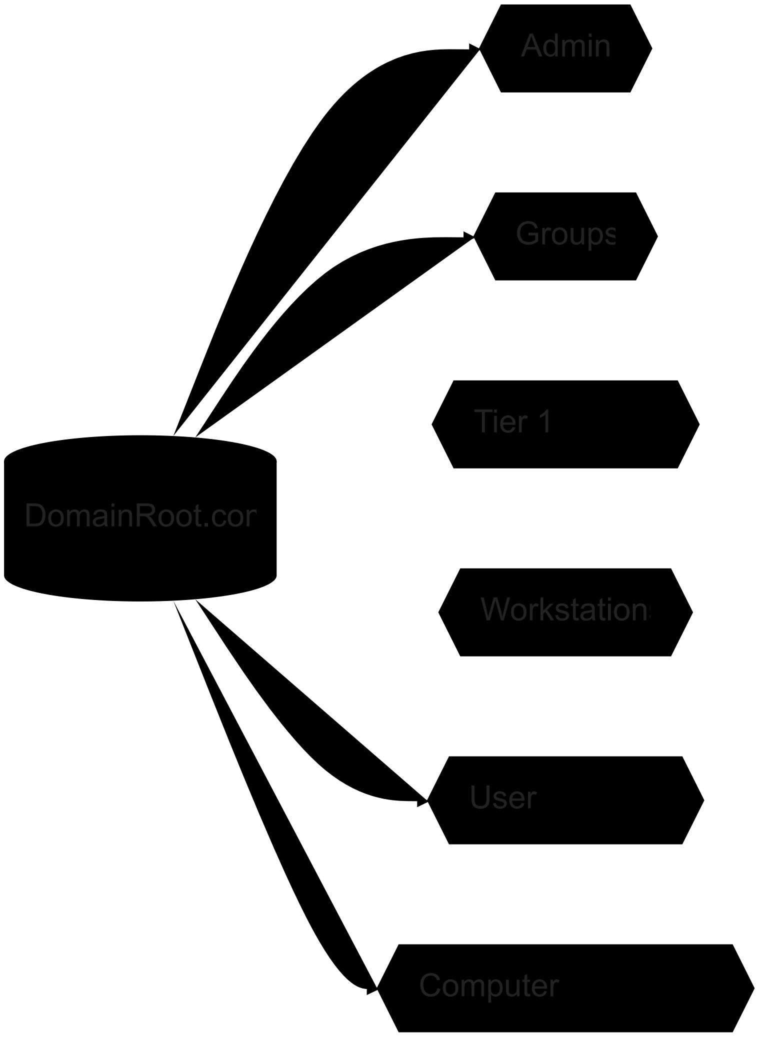
The Create-PAWOUs.ps1 script dynamically generates the working directory, domain name, and default context with the following code:

```
#Get current working directory
$sLocation = Get-Location

$DomainName = (Get-ADDomain).Name
$sDSE = (Get-ADRootDSE).defaultNamingContext

#$sPath = ("OU="+ $DomainName + " Objects," + $($sDSE))
```

It uses the variables stored above to create the following OU structure at the top of the domain:

OU Name	Purpose	Created with the following code:
Admin	Holds all tier 0, 1, 2 user and service accounts, groups, and devices that manage those tiers. Also holds tier 0 computers that are not DCs	`New-ADOrganizationalUnit -Name "Admin" -Path "$sDSE"`
Groups	Holds group objects on the domain. **No tiered** groups here	`New-ADOrganizationalUnit -Name "Groups" -Path "$sDSE"`
Tier 1 Servers	Holds app and data servers. **No PAWs** here	`New-ADOrganizationalUnit -Name "Tier 1 Servers" -Path "$sDSE"`
Workstations	Holds Domain Joined computers (Tier 2 computers)	`New-ADOrganizationalUnit -Name "Workstations" -Path "$sDSE"`
User Accounts	Holds regular user accounts	`New-ADOrganizationalUnit -Name "User Accounts" -Path "$sDSE"`
Computer Quarantine	This is to be the new default computer OU	`New-ADOrganizationalUnit -Name "Computer Quarantine" -Path "$sDSE"`

The Active Directory Secure OU structure now begins to take shape:



Tier OUs, Sub OUs for the Admin OU

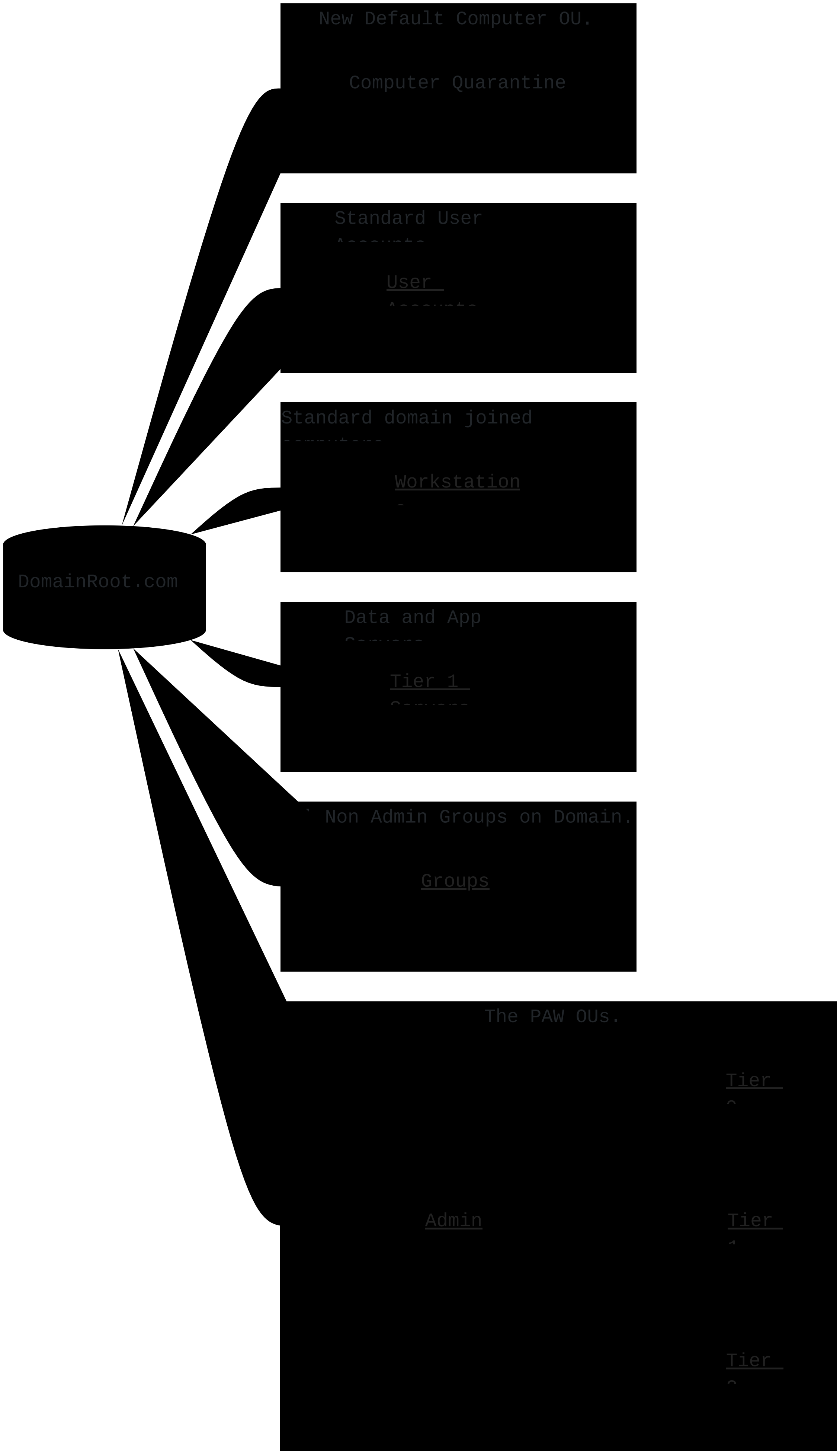
Back to the OU Top

In order to not have a 'flat' domain OU structure, Microsoft deploys multiple OUs underneath the 'Admin OU' to store objects that are tiered objects on the domain.

Admin Sub OU Name	Purpose	Created with the following code:
Tier 0	Holds all Tier 0 users, service accounts, groups, devices (PAWS) and servers	`powershell New-ADOrganizationalUnit -Name "Tier 0" -Path ("OU=Admin,$sDSE")`
Tier 1	Holds all Tier 1 users, service accounts, groups, devices (PAWS). **No servers are stored here**	`powershell New-ADOrganizationalUnit -Name "Tier 1" -Path ("OU=Admin,$sDSE")`

Admin Sub OU Name	Purpose	Created with the following code:
Tier 2	Holds all Tier 2 users, service accounts, groups, devices (PAWS) **No Workstations are stored here**	`powershell New-ADOrganizationalUnit -Name "Tier 2" -Path ("OU=Admin,$sDSE")`

The Active Directory Secure OU structure with the tier OUs is now modified to:


New Default Computer OU.
Computer Quarantine
Standard User Accounts
User Accounts
Standard domain joined computers
Workstations
DomainRoot.com
Data and App Servers
Tier 1 Servers
Non Admin Groups on Domain.
Groups
The PAW OUs.
Tier 0
Admin
Tier 1
Tier 2

Sub OUs under the Tier OUs in the Admin OU

Back to the OU Top

The Active Directory Security Administrator now needs to take the step to expand the OUs underneath the Tiered OUs under the Admin OU. This is also performed by the `Create-PAWOUs.ps1`

Sub Ous for Admin\Tier 0 OU

Tier Sub OU Name	Description	Created with the following code:
Accounts	Tier 0 User (People) accounts	`New-ADOrganizationalUnit -Name "Accounts" -Path ("OU=Tier 0,OU=Admin,$sDSE")`
Groups	Tier 0 Groups - Management groups for Tier 0 Accounts, Service Accounts, Devices, and Tier 0 Servers	`New-ADOrganizationalUnit -Name "Groups" -Path ("OU=Tier 0,OU=Admin,$sDSE")`
Service Accounts	Tier 0 Service Accounts that perform Tier 0 work on schedules	`New-ADOrganizationalUnit -Name "Service Accounts" -Path ("OU=Tier 0,OU=Admin,$sDSE")`
Devices	Tier 0 PAWs	`New-ADOrganizationalUnit -Name "Devices" -Path ("OU=Tier 0,OU=Admin,$sDSE")`

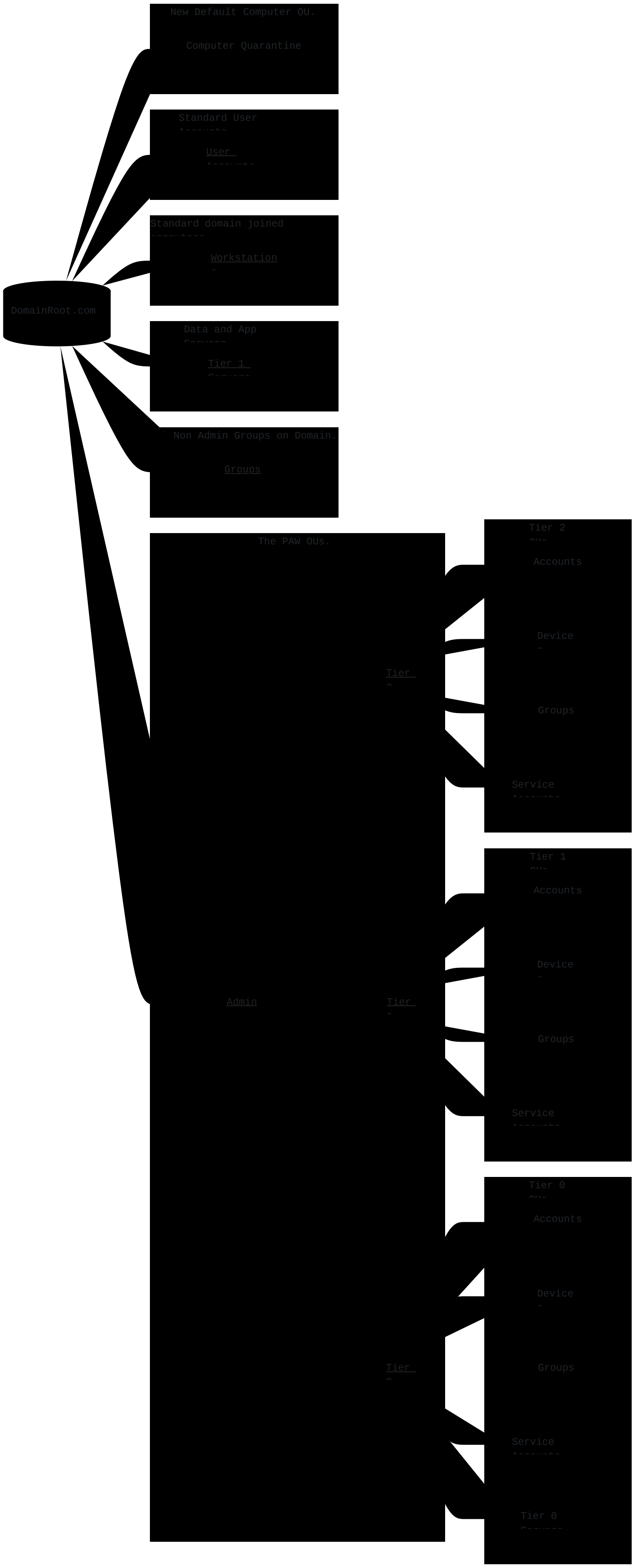
Sub Ous for Admin\Tier 1 OU

Tier Sub OU Name	Description	Created with the following code:
Accounts	Tier 1 User (People) accounts	`New-ADOrganizationalUnit -Name "Accounts" -Path ("OU=Tier 1,OU=Admin,$sDSE")`
Groups	Tier 1 Groups - Management groups for Tier 0 Accounts, Service Accounts, Devices, and Tier 0 Servers	`New-ADOrganizationalUnit -Name "Groups" -Path ("OU=Tier 1,OU=Admin,$sDSE")`
Service Accounts	Tier 1 Service Accounts that perform Tier 1 work on schedules	`New-ADOrganizationalUnit -Name "Service Accounts" -Path ("OU=Tier 1,OU=Admin,$sDSE")`
Devices	Tier 1 PAWs	`New-ADOrganizationalUnit -Name "Devices" -Path ("OU=Tier 1,OU=Admin,$sDSE")`

Sub Ous for Admin\Tier 2 OU

Tier Sub OU Name	Description	Created with the following code:
Accounts	Tier 2 User (People) accounts	`New-ADOrganizationalUnit -Name "Accounts" -Path ("OU=Tier 2,OU=Admin,$sDSE")`
Groups	Tier 2 Groups - Management groups for Tier 1 Accounts, Service Accounts, Devices, and Tier 1 Servers	`New-ADOrganizationalUnit -Name "Groups" -Path ("OU=Tier 2,OU=Admin,$sDSE")`
Service Accounts	Tier 2 Service Accounts that perform Tier 2 work on schedules	`New-ADOrganizationalUnit -Name "Service Accounts" -Path ("OU=Tier 2,OU=Admin,$sDSE")`
Devices	Tier 2 PAWs	`New-ADOrganizationalUnit -Name "Devices" -Path ("OU=Tier 2,OU=Admin,$sDSE")`

The Active Directory Secure Admin OU structure is now modified to:


New Default Computer OU.
Computer Quarantine
Standard User Accounts
User Accounts
Standard domain joined computers
Workstations
DomainRoot.com
Data and App Servers
Tier 1 Servers
Non Admin Groups on Domain.
Groups
The PAW OUs.
Admin
Tier 2
Tier 1
Tier 0
Tier 2 OUs
Accounts
Devices
Groups
Service Accounts
Tier 1 OUs
Accounts
Devices
Groups
Service Accounts
Tier 0 OUs
Accounts
Devices
Groups
Service Accounts
Tier 0 Servers

Sub OUs under Groups, Tier 1, Workstations and User Accounts

Top Level OU: Groups Sub OUs

Groups OU Sub OUs Name	Description	Created with the following code:
Security Groups	Groups that provide access to resources	`New-ADOrganizationalUnit -Name "Security Groups" -Path ("OU=Groups,$sDSE")`
Distribution Groups	Place for all email distribution groups	`New-ADOrganizationalUnit -Name "Distribution Groups" -Path ("OU=Groups,$sDSE")`
Contacts	Contains objects with no security permissions. External Email users	`New-ADOrganizationalUnit -Name "Contacts" -Path ("OU=Groups,$sDSE")`

Top Level OU: Tier 1 Servers Sub OUs

Tier 1 Servers OU Sub OUs Name	Description	Created with the following code
Application	Servers that run necessary applications on the domain. (.Net, Citrix, task servers etc)	`New-ADOrganizationalUnit -Name "Application" -Path ("OU=Tier 1 Servers,$sDSE")`
Collaboration	I honestly think Microsoft just made this one up. It makes no sense. Feel free to delete things that don't make sense in you environment	`New-ADOrganizationalUnit -Name "Collaboration" -Path ("OU=Tier 1 Servers,$sDSE")`
Database	Servers hosting database services	`New-ADOrganizationalUnit -Name "Database" -Path ("OU=Tier 1 Servers,$sDSE")`
Messaging	Servers that host cross team communication apps on the domain	`New-ADOrganizationalUnit -Name "Messaging" -Path ("OU=Tier 1 Servers,$sDSE")`
Staging	Dev/Test OU for testing new deployments	`New-ADOrganizationalUnit -Name "Staging" -Path ("OU=Tier 1 Servers,$sDSE")`

Top Level OU: Workstations Sub OUs

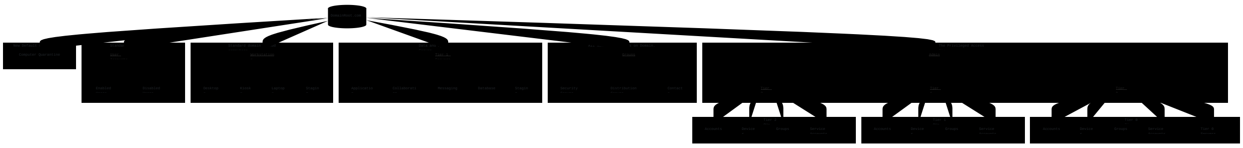
Workstations OU Sub OUs Name	Description	Created with the following code
Desktops	Machines that plug into a wall and don’t move from their location very often	`New-ADOrganizationalUnit -Name "Desktops" -Path ("OU=Workstations,$sDSE")`
Kiosks	SSO machines. Or Workstations on wheels	`New-ADOrganizationalUnit -Name "Kiosks" -Path ("OU=Workstations,$sDSE")`
Laptops	laptops…	`New-ADOrganizationalUnit -Name "Laptops" -Path ("OU=Workstations,$sDSE")`
Staging	Dev/Test OU for testing new deployments	`New-ADOrganizationalUnit -Name "Staging" -Path ("OU=Workstations,$sDSE")`

Top Level OU: User Accounts Sub OUs

User Accounts OU Sub OUs Name	Description	Created with the following code
Enabled Users	Standard accounts for people that have access to log into systems	`New-ADOrganizationalUnit -Name "Enabled Users" -Path ("OU=User Accounts,$sDSE")`
Disabled Users	Standard user accounts that no longer have access to the domain	`New-ADOrganizationalUnit -Name "Disabled Users" -Path ("OU=User Accounts,$sDSE")`

Full Admin OU Structure

The full secure Active Directory PAW Admin OU structure laid out is:



Keep in mind that this OU configuration has zero permissions applied to it. This is just the start of organization that will lead to permissions management.