Tier 1 Admins - Secframe

Tier 1 Admins

Tier 1: Why focus on it at all?

Attackers may be after a full domain compromise. However, sometimes they lucky and find an easy way to get what they want: valuable data. Remember the Capital One data beach from 2019? This breach is an example of a very public, very messy data beach that targeted Tier 1 systems, and had no access to Tier 0.

I often focus conversations onto what is valuable information is being created for new projects or implementations. I then focus on walking through the access chain for the data in these projects: identifying the people with access to the servers, the hard drives, the disk drives, the software management servers, the users that manage all the access? Companies often overlook swaths of people who have access to the critical servers holding PHI or credit card data.

> The over-provisioning of access to critical data **will** cause a major breach one day in your company's future

Defining what the entire Tier 1 is who and what manages it takes a bit of time. To begin the secure deployment of Tier 1 in a domain, spend time understanding what the tier is, why a person needs a tiered account and when he or she can and should use it.

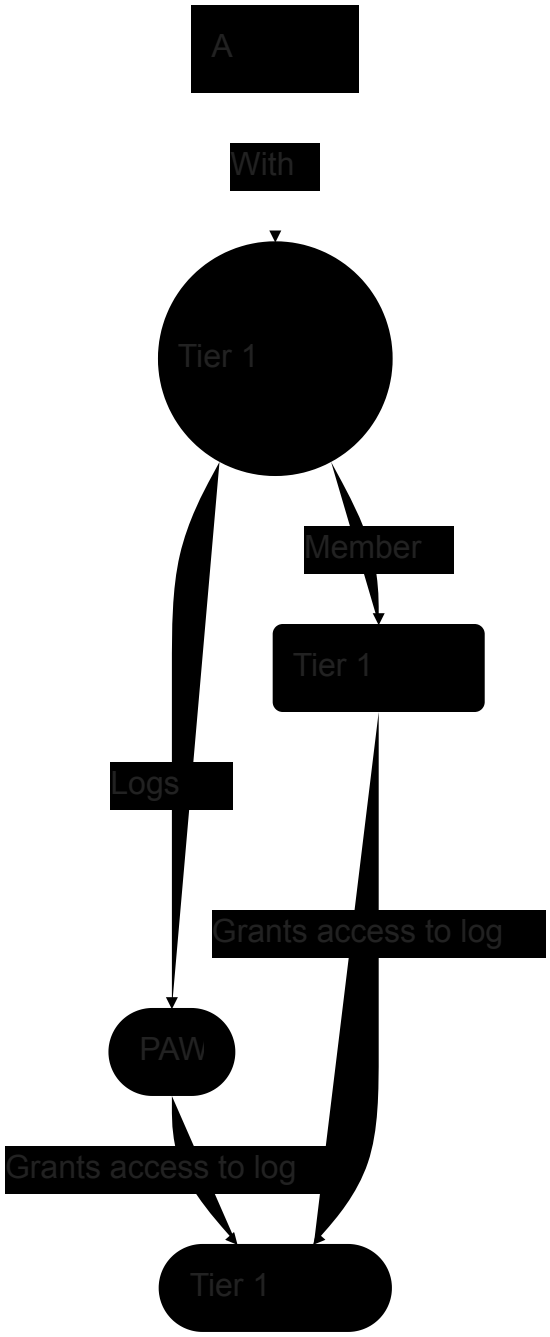
There are 5 main categories of Tier 1 objects.

> There are not just users, or servers.

1. User Accounts
2. Service accounts
3. Groups
4. Devices
5. Servers

There are also service accounts that run jobs in those specific servers. Groups manage and grant permissions across the entire tier. Also PAWs (Devices) are used to add security into all areas of this tier. These five object types are the basics of how Microsoft begins deployment of securing Tier 1 in a domain.

In a best case, fully secure environment, with tiers fully deployed, the workflow to log into a Tier 1 Server and manage the server looks like this



Who is a Tier 1 Administrator?

The Users

- These are the people who manage the tiers themselves.
- These people create Tier 1 users, groups, service accounts devices
- These are the people who provision the PAWs.
- He or she is the person who logs into a server to do daily tasks.
- These are also the people who manage the hardware for the tier itself
- The people who manage the software patches and deoyment across PAWs, servers, and devices across this tier.

The service account

- A scheduled job or task that has access to data on a Tier 1 Server

- A scheduled task that has the ability to change any tier 1 object

What are Tier 1 devices?

Looking back at the definition of tiers remember that Tier one is a more trusted zone than public data or even standard workstations. Describing Tier 1 on an Active Directory domain usually begins with enterprise application servers and data servers. Describing the servers is the standard way to describe the classification of data.

The servers

A tier 1 device can be described as:

- A database Server
- An application server
- A messaging server

PAWs and Other Devices

- The PAW that the tier 1 admin logs into to do his or her work on tier 1 objects
- A server or computer that manages software or hardware on a Tier 1 machine
- The hypervisor admin or hardware admin that can control the tier 1 systems

When are Tier 1 Accounts Used?

Admin accounts are not used for daily tasks such as browsing the web or viewing email.

Tier 1 Admin accounts are only used to manage the tier 1 objects, the five Tier 1 objects outlined above. A standard, non administrative account should not be used to manage tier 1 objects on a domain. That would create a direct path up from a workstation to a server. A common example is when a person needs to log into a server to manage the software on it.

Where Are the Tier 1 Objects Stored?

Tier 1 objects have a special location in the domain to keep them secure. The very basic understanding of where they need to go is:

> Domain Root
>
> > Admin <– New administrative OU
> >
> > > Tier 1 <– Users, groups, Devices go here
> >
> > Tier 1 Servers <– Servers go here

For a full understanding of the PAW/ Secure Administrative OU, please see Admin OU

Why Use Tier 1 accounts?

Please refresh with What is Microsoft Redforest Phase 1

How do you ‘do’ Tier 1?

Please reach out to me for more details. I’d love to schedule some training and help define access to new systems being deployed in your environment today. With a basic understanding of Tier 1 under your belt, you may be ready to deploy the tiers. For more pages on Tiers and Admin accounts, please see the deploy steps on the PAWs

Back To The Top