Keys of the Kingdom 365

Improve the protection of the privileged credentials applying the tiering model to Active Directory.

The theft or compromise of the «keys of the kingdom» (Active Directory privileged credentials) causes extensive damage, disruption and data exfiltration
Therefore, protection of the «keys of the kingdom» is one of the main task to increase the general security posture of every environment.
Protection is achieved by defining management levels in Active Directory isolated from each other, called "Tier", which together are the «Tiering model».
Thanks to the Tiering model, the probability of success of the attack techniques defined by MITRE as Privilege Escalation and Lateral Movement can be reduced.

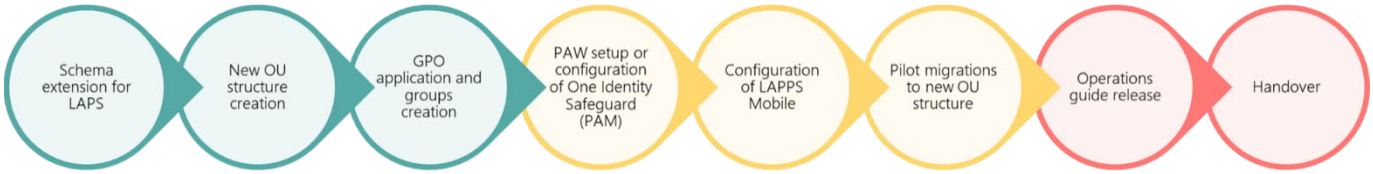
The definition and application of the "Tiering model" in Active Directory can be done in two ways:

- Custom: it requires a deep analysis to build a “tailormade” Tiering model.
- Secure Privilege Access (SPA) model by Microsys: predefined, optimized and low-impact method to apply the Tiering model to Active Directory.

SPA model by Microsys:
Based on ESAE model by Microsoft, but easier to implement and manage. SPA model introduce:

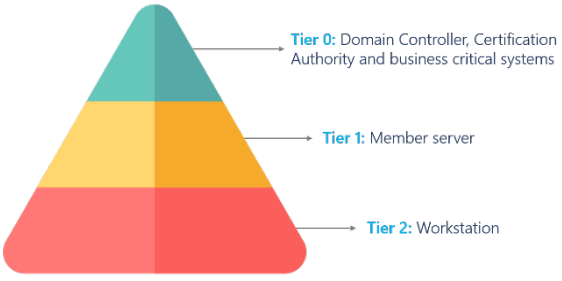
- A new Organizational Unit structure, groups and delegations.
- Policy and configurations to manage accesses of privileged credentials to computers (server and workstation) in Active Directory.

SPA model application steps

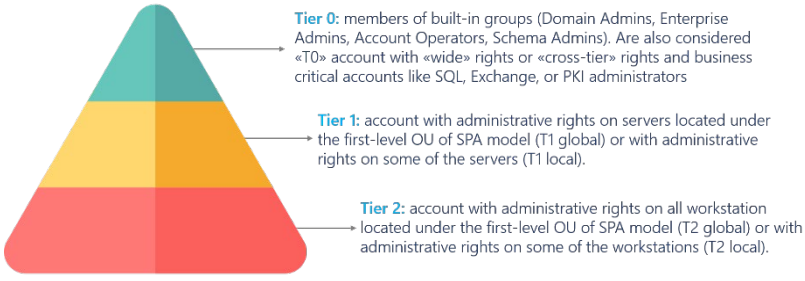


LAPPS mobile is a web app (developed by Microsys) to obtain password of local Administrator or workstations. It is useful when a Help Desk operator is in physically in front of the workstation and need a temporary administrative access (LAPS reset the local Administrator password automatically after 90 minutes).

Computers in SPA model

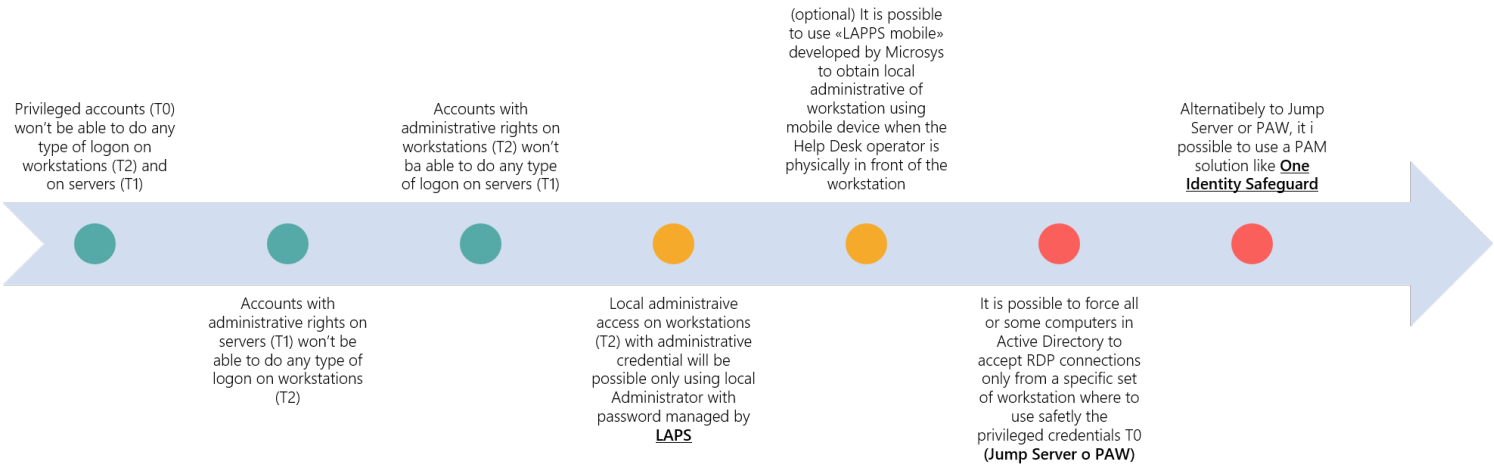


Users in SPA model



MICROSYS

Scenario after application of SPA model



Tools to improve security and management of SPA model

After the application of the SPA model, the adoption of tools is recommended for:

- further increase the security of privileged credentials
- manage and monitor the quality of the SPA model over time
- add reactive/proactive detection and response capabilities.