TRUESEC

Active Directory Tiering Implementation

What is AD Tiering?

The principle of safeguarding our most valuable assets in the most secure environments is as old as security itself. While the concept of tiering within Active Directory (AD) is more recent, it has been recognized as a best practice for over a decade. Despite the fact that nearly 90% of Global Fortune 1000 companies rely on AD as their primary authentication platform, AD tiering remains underutilized.

This hesitation often stems from the perception that implementing AD tiering is a complex, high-risk undertaking that could disrupt business operations. At Truesec, we challenge that notion.

Our extensive experience has proven that AD tiering can be implemented efficiently and securely—typically within days—without impacting business continuity.

Our Experience:

As a trusted leader in cyber incident response, Truesec works closely with global organizations to both learn from and educate the cybersecurity community.

Time and again, we see cybercriminals exploiting lateral movement within networks, seeking privileged credentials to escalate their access—often culminating in domain admin compromise. AD tiering is a proven defense, restricting attackers to the tier they have breached and preventing them from moving freely across your environment.

By segmenting your AD environment into multiple zones—or “tiers”—you create clear boundaries between commonly targeted devices, such as user workstations, and your most critical assets, like domain controllers, backup systems, and PKI infrastructure. This layered approach significantly enhances your organization’s resilience against advanced threats.

About Truesec

An international cybersecurity company that offers market-leading managed services, incident management, and expert consulting services. Truesec operates the largest Security Operations Center (SOC) in the Nordics and has conducted over 100,000 hours of incident management.

The company’s goal is to prevent breach and minimize impact. Since 2005, Truesec has delivered advanced security solutions to clients in both the private and public sectors worldwide. Today, the company comprises over 330 cyber specialists with deep expertise and a leading role in cybersecurity in the Nordics. For more information, visit Truesec.com.

Benefits of AD Tiering

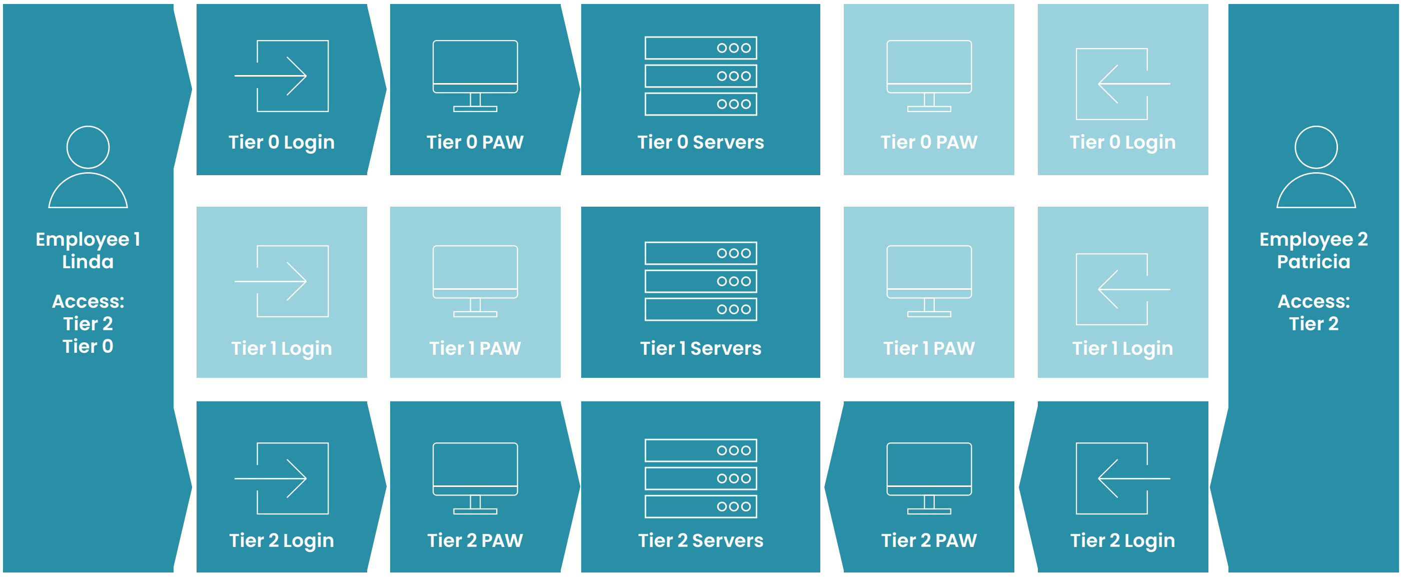
- A team leveraging proven methodologies to implement and document AD tiering seamlessly ensuring zero disruption to your business
- Maximized security and efficiency from your existing infrastructure investments.
- Enhanced protection that raises the bar for attackers seeking to compromise sensitive systems
- Strong safeguards for your most valuable assets, without introducing unnecessary complexity for your organization
- Ongoing expert guidance from Truesec to help you continually strengthen your cyber resilience

TRUESEC

Active Directory Tiering Implementation

A Brief Look Into a Tiered Active Directory

When the AD is tiered, you limit the exposure of sensitive credentials. The result will look something like this:



Employee 1
Linda

Access:
Tier 2
Tier 0

Tier 0 Login | Tier 0 PAW | Tier 0 Servers | Tier 0 PAW | Tier 0 Login

Tier 1 Login | Tier 1 PAW | Tier 1 Servers | Tier 1 PAW | Tier 1 Login

Tier 2 Login | Tier 2 PAW | Tier 2 Servers | Tier 2 PAW | Tier 2 Login

Employee 2
Patricia

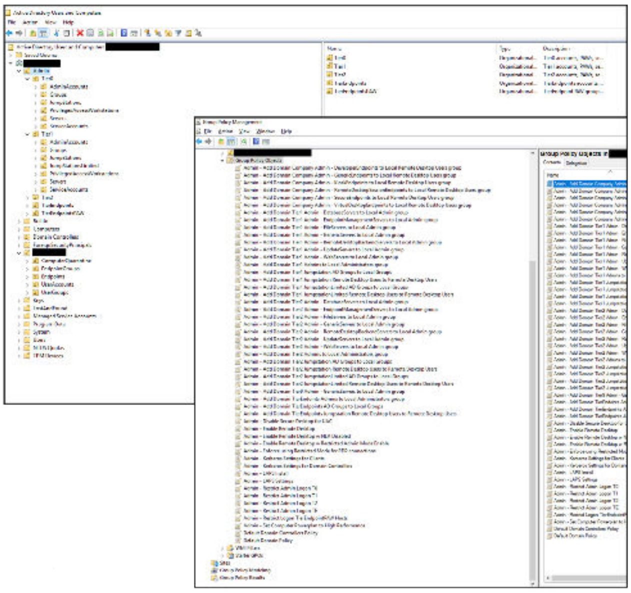
Access:
Tier 2

This image illustrates that Employee 1 (let's call her Linda) can perform administrative tasks in Tier 0 and Tier 2. Employee 2 (who we'll call Patricia) can only perform administrative tasks in Tier 2.

When Linda works in Tier 0, she logs in with her Tier 0 admin account, using the Tier 0 privileged access workstation (PAW), and can only move horizontally within Tier 0. Neither the admin account nor the PAW can be used to access any other tier. This is due to the logon and control restrictions put in place by the group policy objects (GPOs) created in AD when implementing the Truesec tiering model.

Similarly, when Linda performs administrative tasks on any server in Tier 2, she logs in with her Tier 2 admin account on the Tier 2 PAW.

Patricia can only do administrative tasks in Tier 2. She uses her Tier 2 admin account on her Tier 2 PAW and then she can access the servers, or systems, she should be able to administer within Tier 2. An example of the GPOs and the organizational unit (OU) structure created by the Truesec tiering model is shown here as an overview.

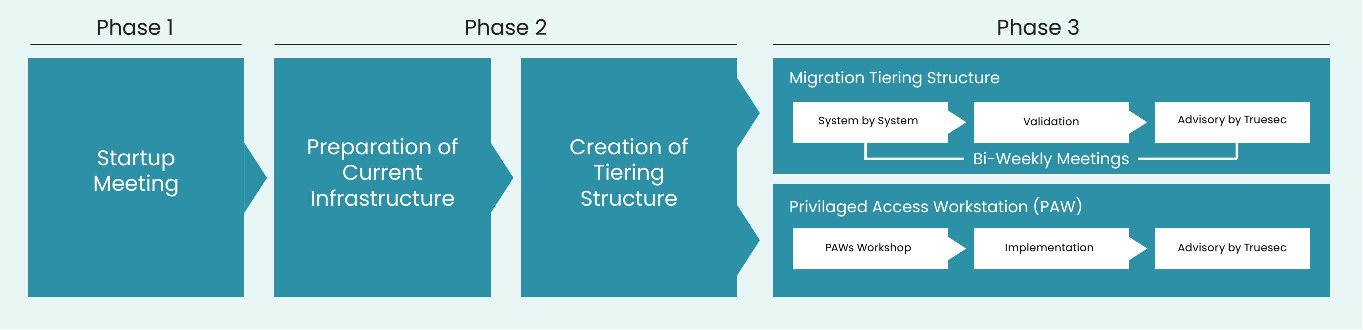


TRUESEC

Active Directory Tiering Implementation

Methodology

This is best done together with the experts from Truesec and the team that manages the operation of the IT resources. This ensures that information and knowledge are transferred quickly and efficiently.



Phase 1

Startup Meeting

Phase 2

Preparation of Current Infrastructure

Creation of Tiering Structure

Phase 3

Migration Tiering Structure

System by System

Validation

Advisory by Truesec

Bi-Weekly Meetings

Privilaged Access Workstation (PAW)

PAWs Workshop

Implementation

Advisory by Truesec

The Three Phases

Phase 1 – Knowledge

We conduct a startup meeting that includes the concepts and benefits of working with a tiering model.

Examples of areas covered:

Why to use a tiering model.

- The tiering model.
- Why and when to use a PAW
- Ways of working for admins.

Phase 2 – Implementation

In Phase 2, the environment is prepared, and information regarding current and future privileged users is collected. Then the new tiering structure is created with all the policies and settings required. “Break glass” accounts are also created.

Phase 3 –Guidance

In Phase 3, the systems are protected one by one in the new tiering model by your team. Also, the implementation of privileged access workstations (PAW) is completed. As this establishes a new way of accessing the environment for some administrators, experts from Truesec are there to guide and assist during this phase. This is supported by a bi-weekly meeting with Truesec experts to answer questions and provide further guidance.

TRUESEC

Active Directory Tiering Implementation

What's Included

Scoping	✓
Startup Meeting	✓
Preparation of Current Infrastructure	✓
Creation of Tiering Structure in Active Directory	✓
Creation of Group Policy Objects to Govern Access in AD	✓
Creation of New Admin Accounts Per Tier	✓
PAW Workshop	✓
Implementation of Authentication Policy Silos	✓
Migration of Critical Infrastructure to Tier 0 (AD, PKI, Entra ID Connect Sync)	✓
Identification of Other Critical Infrastructure That Should Be in Tier 0	✓
Any additional security improvements (delivered with a time & material approach)	*Optional*
Advisory Services Provided by Truesec	*Optional*

How to Get Started

Start by contacting your Truesec expert. Together, we'll scope the assignment and identify the best actions to protect your sensitive information and brand.

Our AD Tiering Implementation uses proven methods to secure your key assets efficiently and without business disruption.

If You're Under Attack, Call Truesec.

+46 (0) 8 107 200
incident@truesec.com

Truesec Group AB
Corp ID: 556690-8074
truesec.com

Sweden
Headquarters Stockholm
Luntmakargatan 18, 111 37 Stockholm
+46(0)8 107 200

Denmark
Headquarters Copenhagen
Glentevej 69, 1. 2400 Copenhagen
+45 32 24 00 70

Finland
Truesec Oy
Keilaniementie 1, 02150 Espoo
+358 655 700 40

Germany
Truesec GmbH
Rosenheimer Str. 143c, 81671 München
+49 (0)89 380 30 900