Domain or Tenant Policy Modification, Technique T1484 - Enterprise

Archived: 2026-04-05 13:52:44 UTC

Adversaries may modify the configuration settings of a domain or identity tenant to evade defenses and/or escalate privileges in centrally managed environments. Such services provide a centralized means of managing identity resources such as devices and accounts, and often include configuration settings that may apply between domains or tenants such as trust relationships, identity syncing, or identity federation.

Modifications to domain or tenant settings may include altering domain Group Policy Objects (GPOs) in Microsoft Active Directory (AD) or changing trust settings for domains, including federation trusts relationships between domains or tenants.

With sufficient permissions, adversaries can modify domain or tenant policy settings. Since configuration settings for these services apply to a large number of identity resources, there are a great number of potential attacks malicious outcomes that can stem from this abuse. Examples of such abuse include:

- modifying GPOs to push a malicious Scheduled Task to computers throughout the domain environment[1][2][3]
- modifying domain trusts to include an adversary-controlled domain, allowing adversaries to forge access tokens that will subsequently be accepted by victim domain resources[4]
- changing configuration settings within the AD environment to implement a Rogue Domain Controller.
- adding new, adversary-controlled federated identity providers to identity tenants, allowing adversaries to authenticate as any user managed by the victim tenant [5]

Adversaries may temporarily modify domain or tenant policy, carry out a malicious action(s), and then revert the change to remove suspicious indicators.

Source: https://attack.mitre.org/techniques/T1484