# TTP Detail – T1484

## TTP Information

Name: Domain or Tenant Policy Modification

Description: 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](https://attack.mitre.org/techniques/T1053/005) to computers throughout the domain environment(Citation: ADSecurity GPO Persistence 2016)(Citation: Wald0 Guide to GPOs)(Citation: Harmj0y Abusing GPO Permissions)
\* modifying domain trusts to include an adversary-controlled domain, allowing adversaries to forge access tokens that will subsequently be accepted by victim domain resources(Citation: Microsoft - Customer Guidance on Recent Nation-State Cyber Attacks)
\* changing configuration settings within the AD environment to implement a [Rogue Domain Controller](https://attack.mitre.org/techniques/T1207).
\* adding new, adversary-controlled federated identity providers to identity tenants, allowing adversaries to authenticate as any user managed by the victim tenant (Citation: Okta Cross-Tenant Impersonation 2023)

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

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: privilege-escalation