Domain or Tenant Policy Modification: Trust Modification, Sub-technique T1484.002 - Enterprise

Archived: 2026-04-05 15:30:57 UTC

Adversaries may add new domain trusts, modify the properties of existing domain trusts, or otherwise change the configuration of trust relationships between domains and tenants to evade defenses and/or elevate privileges.Trust details, such as whether or not user identities are federated, allow authentication and authorization properties to apply between domains or tenants for the purpose of accessing shared resources.[1] These trust objects may include accounts, credentials, and other authentication material applied to servers, tokens, and domains.

Manipulating these trusts may allow an adversary to escalate privileges and/or evade defenses by modifying settings to add objects which they control. For example, in Microsoft Active Directory (AD) environments, this may be used to forge SAML Tokens without the need to compromise the signing certificate to forge new credentials. Instead, an adversary can manipulate domain trusts to add their own signing certificate. An adversary may also convert an AD domain to a federated domain using Active Directory Federation Services (AD FS), which may enable malicious trust modifications such as altering the claim issuance rules to log in any valid set of credentials as a specified user.[2]

An adversary may also add a new federated identity provider to an identity tenant such as Okta or AWS IAM Identity Center, which may enable the adversary to authenticate as any user of the tenant.[3] This may enable the threat actor to gain broad access into a variety of cloud-based services that leverage the identity tenant. For example, in AWS environments, an adversary that creates a new identity provider for an AWS Organization will be able to federate into all of the AWS Organization member accounts without creating identities for each of the member accounts.[4]
