# TTP Detail – T1606.002

## TTP Information

Name: SAML Tokens

Description: An adversary may forge SAML tokens with any permissions claims and lifetimes if they possess a valid SAML token-signing certificate.(Citation: Microsoft SolarWinds Steps) The default lifetime of a SAML token is one hour, but the validity period can be specified in the <code>NotOnOrAfter</code> value of the <code>conditions ...</code> element in a token. This value can be changed using the <code>AccessTokenLifetime</code> in a <code>LifetimeTokenPolicy</code>.(Citation: Microsoft SAML Token Lifetimes) Forged SAML tokens enable adversaries to authenticate across services that use SAML 2.0 as an SSO (single sign-on) mechanism.(Citation: Cyberark Golden SAML)

An adversary may utilize [Private Keys](https://attack.mitre.org/techniques/T1552/004) to compromise an organization's token-signing certificate to create forged SAML tokens. If the adversary has sufficient permissions to establish a new federation trust with their own Active Directory Federation Services (AD FS) server, they may instead generate their own trusted token-signing certificate.(Citation: Microsoft SolarWinds Customer Guidance) This differs from [Steal Application Access Token](https://attack.mitre.org/techniques/T1528) and other similar behaviors in that the tokens are new and forged by the adversary, rather than stolen or intercepted from legitimate users.

An adversary may gain administrative Entra ID privileges if a SAML token is forged which claims to represent a highly privileged account. This may lead to [Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550), which may bypass multi-factor and other authentication protection mechanisms.(Citation: Microsoft SolarWinds Customer Guidance)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Tools

* AADInternals