# TTP Detail – T1556.007

## TTP Information

Name: Hybrid Identity

Description: Adversaries may patch, modify, or otherwise backdoor cloud authentication processes that are tied to on-premises user identities in order to bypass typical authentication mechanisms, access credentials, and enable persistent access to accounts.

Many organizations maintain hybrid user and device identities that are shared between on-premises and cloud-based environments. These can be maintained in a number of ways. For example, Microsoft Entra ID includes three options for synchronizing identities between Active Directory and Entra ID(Citation: Azure AD Hybrid Identity):

\* Password Hash Synchronization (PHS), in which a privileged on-premises account synchronizes user password hashes between Active Directory and Entra ID, allowing authentication to Entra ID to take place entirely in the cloud
\* Pass Through Authentication (PTA), in which Entra ID authentication attempts are forwarded to an on-premises PTA agent, which validates the credentials against Active Directory
\* Active Directory Federation Services (AD FS), in which a trust relationship is established between Active Directory and Entra ID

AD FS can also be used with other SaaS and cloud platforms such as AWS and GCP, which will hand off the authentication process to AD FS and receive a token containing the hybrid users’ identity and privileges.

By modifying authentication processes tied to hybrid identities, an adversary may be able to establish persistent privileged access to cloud resources. For example, adversaries who compromise an on-premises server running a PTA agent may inject a malicious DLL into the `AzureADConnectAuthenticationAgentService` process that authorizes all attempts to authenticate to Entra ID, as well as records user credentials.(Citation: Azure AD Connect for Read Teamers)(Citation: AADInternals Azure AD On-Prem to Cloud) In environments using AD FS, an adversary may edit the `Microsoft.IdentityServer.Servicehost` configuration file to load a malicious DLL that generates authentication tokens for any user with any set of claims, thereby bypassing multi-factor authentication and defined AD FS policies.(Citation: MagicWeb)

In some cases, adversaries may be able to modify the hybrid identity authentication process from the cloud. For example, adversaries who compromise a Global Administrator account in an Entra ID tenant may be able to register a new PTA agent via the web console, similarly allowing them to harvest credentials and log into the Entra ID environment as any user.(Citation: Mandiant Azure AD Backdoors)

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence

## Tools

* AADInternals

## APTs (Intrusion Sets)

* APT29