# TTP Detail – T1671

## TTP Information

Name: Cloud Application Integration

Description: Adversaries may achieve persistence by leveraging OAuth application integrations in a software-as-a-service environment. Adversaries may create a custom application, add a legitimate application into the environment, or even co-opt an existing integration to achieve malicious ends.(Citation: Push Security SaaS Persistence 2022)(Citation: SaaS Attacks GitHub Evil Twin Integrations)  
  
OAuth is an open standard that allows users to authorize applications to access their information on their behalf. In a SaaS environment such as Microsoft 365 or Google Workspace, users may integrate applications to improve their workflow and achieve tasks.   
  
Leveraging application integrations may allow adversaries to persist in an environment – for example, by granting consent to an application from a high-privileged adversary-controlled account in order to maintain access to its data, even in the event of losing access to the account.(Citation: Wiz Midnight Blizzard 2024)(Citation: Microsoft Malicious OAuth Applications 2022)(Citation: Huntress Persistence Microsoft 365 Compromise 2024) In some cases, integrations may remain valid even after the original consenting user account is disabled.(Citation: Push Security Slack Persistence 2023) Application integrations may also allow adversaries to bypass multi-factor authentication requirements through the use of [Application Access Token](https://attack.mitre.org/techniques/T1550/001)s. Finally, they may enable persistent [Automated Exfiltration](https://attack.mitre.org/techniques/T1020) over time.(Citation: Synes Cyber Corner Malicious Azure Application 2023)  
  
Creating or adding a new application may require the adversary to create a dedicated [Cloud Account](https://attack.mitre.org/techniques/T1136/003) for the application and assign it [Additional Cloud Roles](https://attack.mitre.org/techniques/T1098/003) – for example, in Microsoft 365 environments, an application can only access resources via an associated service principal.(Citation: Microsoft Entra ID Service Principals)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence