# TTP Detail – T1098.005

## TTP Information

Name: Device Registration

Description: Adversaries may register a device to an adversary-controlled account. Devices may be registered in a multifactor authentication (MFA) system, which handles authentication to the network, or in a device management system, which handles device access and compliance.

MFA systems, such as Duo or Okta, allow users to associate devices with their accounts in order to complete MFA requirements. An adversary that compromises a user’s credentials may enroll a new device in order to bypass initial MFA requirements and gain persistent access to a network.(Citation: CISA MFA PrintNightmare)(Citation: DarkReading FireEye SolarWinds) In some cases, the MFA self-enrollment process may require only a username and password to enroll the account's first device or to enroll a device to an inactive account. (Citation: Mandiant APT29 Microsoft 365 2022)

Similarly, an adversary with existing access to a network may register a device to Entra ID and/or its device management system, Microsoft Intune, in order to access sensitive data or resources while bypassing conditional access policies.(Citation: AADInternals - Device Registration)(Citation: AADInternals - Conditional Access Bypass)(Citation: Microsoft DEV-0537)

Devices registered in Entra ID may be able to conduct [Internal Spearphishing](https://attack.mitre.org/techniques/T1534) campaigns via intra-organizational emails, which are less likely to be treated as suspicious by the email client.(Citation: Microsoft - Device Registration) Additionally, an adversary may be able to perform a [Service Exhaustion Flood](https://attack.mitre.org/techniques/T1499/002) on an Entra ID tenant by registering a large number of devices.(Citation: AADInternals - BPRT)

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: persistence

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

## Tools

* AADInternals

## APTs (Intrusion Sets)

* APT29