# TTP Detail – T1556.009

## TTP Information

Name: Conditional Access Policies

Description: Adversaries may disable or modify conditional access policies to enable persistent access to compromised accounts. Conditional access policies are additional verifications used by identity providers and identity and access management systems to determine whether a user should be granted access to a resource.

For example, in Entra ID, Okta, and JumpCloud, users can be denied access to applications based on their IP address, device enrollment status, and use of multi-factor authentication.(Citation: Microsoft Conditional Access)(Citation: JumpCloud Conditional Access Policies)(Citation: Okta Conditional Access Policies) In some cases, identity providers may also support the use of risk-based metrics to deny sign-ins based on a variety of indicators. In AWS and GCP, IAM policies can contain `condition` attributes that verify arbitrary constraints such as the source IP, the date the request was made, and the nature of the resources or regions being requested.(Citation: AWS IAM Conditions)(Citation: GCP IAM Conditions) These measures help to prevent compromised credentials from resulting in unauthorized access to data or resources, as well as limit user permissions to only those required.

By modifying conditional access policies, such as adding additional trusted IP ranges, removing [Multi-Factor Authentication](https://attack.mitre.org/techniques/T1556/006) requirements, or allowing additional [Unused/Unsupported Cloud Regions](https://attack.mitre.org/techniques/T1535), adversaries may be able to ensure persistent access to accounts and circumvent defensive measures.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence

## APTs (Intrusion Sets)

* Scattered Spider