

# Behavioral Detection Strategy for Use Alternate Authentication Material: Application Access Token (T1550.001), Detection Strategy DET0185

Archived: 2026-04-05 13:35:55 UTC

## AN0526

Use of AWS STS or GCP IAM APIs to request temporary tokens or federation sessions inconsistent with normal account activity, including from unexpected principals or regions.

### Log Sources

### Mutable Elements

| Field                  | Description  |
|------------------------|--|
| GeoIPDistanceThreshold | Distance between token creation and resource use locations |
| RoleScope              | Limit scope of acceptable role assumptions by account type |

## AN0527

OAuth or SAML access tokens reused across multiple sessions or clients without corresponding MFA or login activity.

### Log Sources

### Mutable Elements

| Field            | Description                                       |
|------------------|---|
| MFAEnforcement   | Ensure MFA context exists prior to token issuance |
| TokenReuseWindow | Maximum acceptable window for refresh token reuse |

## AN0528

Application access tokens used to call APIs (e.g., Google Workspace, Salesforce) without interactive logins, often with unusual scopes or elevated permissions.

### Log Sources

**Mutable Elements**

| Field                     | Description   |
|---------------------------|---|
| ApplicationScopeAllowlist | Restrict allowed API scopes for enterprise applications |
| TokenLifetime             | Threshold for detecting unusually long-lived tokens     |

**AN0529**

OAuth token usage for Exchange Online or SharePoint API access without preceding login or from unauthorized clients.

**Log Sources**

**Mutable Elements**

| Field                | Description   |
|----------------------|---|
| ClientAppIDWhitelist | Restrict trusted Office apps authorized to request tokens |

**AN0530**

Compromised service account tokens mounted inside containers and reused for external API calls or lateral movement across services.

**Log Sources**

**Mutable Elements**

| Field          | Description  |
|----------------|--|
| NamespaceScope | Restrict token use to specific namespaces or workloads |

---

Source: <https://attack.mitre.org/detectionstrategies/DET0185#AN0529>