SYNTHETIC · fictional tenant · not a live run

Sample output · synthetic tenant · State of Trescott Department of Transportation (fictional)

# Tenant reach sheet

Produced in your tenant · nothing left it · as of 2026-11-04T12:00:00Z · sheet 0.4.0 · commercial

**7**

**privileged identities (active assignments only)**

4 user accounts, 3 service principals (non-human)

5 direct, 2 via group only (0 also via group)

User accounts and service principals holding at least one pinned privileged role, directly or through a role-assignable group. PIM-eligible-only administrators are not listed.

**2**

**service principals with no enabled owner recorded**

Listed service principals whose directory owners are none, or all disabled.

**2**

**tenant-wide consents**

High-privilege: Records Sync Bridge (Directory.ReadWrite.All)

Application consents granted for every user in the tenant (AllPrincipals).

**1**

**privileged identities holding admin-class delegated consents**

Listed privileged user accounts that also hold a delegated grant with a high-privilege scope.

**3**

**reachable grants from a privileged session**

1 delegated, 2 tenant-wide

Distinct delegated grants held by the listed user accounts, plus the tenant-wide grants, counted separately. Service principals have no delegated session.

3 delegated grants held by non-privileged identities; not listed.

Reach is session reach. The sheet does not say any component holds these grants. A privileged identity's session holds them, so anything riding that session can reach them.

## What to do with this

1. Review the tenant-wide grant to Records Sync Bridge: it carries Directory.ReadWrite.All for every user.

2. Confirm each listed privileged identity still needs its role: Case Exporter, Fleet Telemetry Agent, Permit Sync, a.ramirez@trescott-dot.example, j.chen@trescott-dot.example, svc-backup@trescott-dot.example, t.nguyen@trescott-dot.example.
3. PIM-eligible administrators are not counted. Consent RoleEligibilitySchedule.Read.Directory and rerun, or review PIM separately.
4. This sheet does not show who approved each grant or whether they still stand; that declared-authority column is what Cerydora's paid product adds.

## Qualifiers

- eligible-only administrators: not evaluated (eligibility not consented)

## Privileged roles by identity kind

| Role | User accounts | Service principals (non-human) |
|---|---|---|
| Global Administrator | 1: a.ramirez@trescott-dot.example | 1: Permit Sync |
| Helpdesk Administrator | 1: t.nguyen@trescott-dot.example | 0 |
| Intune Administrator | 0 | 1: Fleet Telemetry Agent |
| Privileged Role Administrator | 0 | 1: Case Exporter |
| Security Administrator | 1: j.chen@trescott-dot.example | 0 |
| User Administrator | 1: svc-backup@trescott-dot.example | 0 |

A user account may be a person or a service account; the directory does not say which.

## Service principals holding privileged roles

| Service principal | Type | Enabled | Privileged roles | Owners | Notes |
|---|---|---|---|---|---|
| Permit Sync | Application | yes | Global Administrator | 1 user account (1 enabled) | application permissions: not read by this sheet |
| Case Exporter | Application | yes | Privileged Role Administrator | 1 user account (0 enabled) | no enabled owner recorded; application permissions: not read by this sheet |
| Fleet Telemetry Agent | ManagedIdentity | yes | Intune Administrator · via group Trescott DOT Device Admins | none recorded | no enabled owner recorded; application permissions: not read by this sheet |

## Prerequisites

| Check | State |
|---|---|
| Active role assignments | read |
| Consent grants | read |
| PIM eligibility | not consented |
| Role-holding groups expanded | 2 of 2 role-holding groups expanded |
| Role definitions (display names) | read |
| Device reach | Device reach requires browser-extension inventory (Defender Vulnerability Management). Not read by this sheet; the CVE sheet adds it where it is licensed. |

## Privileged user accounts and what their sessions hold

| Identity | Privileged roles | Grant | Tier |
|---|---|---|---|
| a.ramirez@trescott-dot.example · Entra object id | Global Administrator | Trescott Admin Console → Microsoft Graph: Directory.ReadWrite.All User.Read · + tenant-wide grants | Privileged role · Admin-class consent · Tenant-wide reach |
| j.chen@trescott-dot.example · Entra object id | Security Administrator | — · + tenant-wide grants | Privileged role · Tenant-wide reach |
| t.nguyen@trescott-dot.example · Entra object id | Helpdesk Administrator · via group Trescott DOT Helpdesk Admins | — · + tenant-wide grants | Privileged role · Tenant-wide reach |
| svc-backup@trescott-dot.example · Entra object id | User Administrator | — · + tenant-wide grants | Privileged role · Tenant-wide reach |

## Tenant-wide grants (AllPrincipals)

| Client | Resource | Scopes |
|---|---|---|
| Trescott Intranet | Microsoft Graph | User.Read openid profile |
| Records Sync Bridge | Microsoft Graph | Directory.ReadWrite.All User.Read |

## Sources

Privileged-role list content/reach-sheet/privileged-roles-0.1.0.json v0.1.0, sha256 `650e4d31dd867d5c988fd2083f1a451f4029cdb9b18f22327a037d9cbd042440`

## Limitations

- The listed population is every user account and every service principal holding at least one pinned privileged role, directly or through a role-assignable group. No other user account or service principal is enumerated, and the sheet carries no count of either.
- Identity kind is the directory object type. A service principal is non-human; a user account may be a person or a service account, and the directory does not say which.
- Role assignments are read in one walk of the tenant's directory role assignments; a role assigned to a role-assignable group is expanded to the group's transitive user and service-principal members. PIM-eligible administrators are not counted unless eligibility is consented; eligibility held through a group, and PIM for Groups membership, are not expanded.
- For each listed service principal the sheet reads its details and its owners (object id, object type, enabled state). An owner is whoever the directory records as owner; the sheet draws nothing else from it. Application permissions of service principals are not read.
- Role names are display only. Privilege is matched on the role template id against the pinned privileged-role list.
- Every AllPrincipals grant is treated as in reach of every listed session; app-assignment-required narrowing is not evaluated.
- Delegated grants held by user accounts outside the population are counted in one number and not listed.
- This tier set is the sheet's own. It does not replace or feed the operator queue's privileged state.

---

This sheet is an effective-permission inventory join. It carries no record of who authorized any grant or whether that person still holds the role that let them.