Why define roles and support paths now?

The goal is not more process – it is clearer ownership, safer access and better enterprise visibility.

Right access

Match platform permissions to the work each user is expected to perform.

Clear ownership

Make it obvious where users should go first and who owns escalation.

Enterprise governance

Reduce fragmented vendor relationships and improve issue tracking, patterns and accountability.

Working principle

Access should be role-based and purposeful. Support should be self-service first, centrally governed when escalation is needed, and routed to Birdeye specialty teams when appropriate.

Proposed SSO role framework

Discussion – terminology and permission boundary definitions in process.

Role	Access	Intended user
Enterprise Administrator	Enterprise-wide configuration, users, reporting and governance	System Office / enterprise ORM platform owners
Business Extension Administrator	Broad access within assigned business extension; local oversight and reporting	Designated business-extension ORM lead(s)
Ministry / Location Manager	Manage assigned ministries/locations; reviews, listings workflows and reporting as approved	Marketing leaders or designated ORM owners
Ministry / Location User	Day-to-day access for assigned ministries/locations with limited administrative rights	Local marketing / operational users
Reporting Only	View dashboards, reports and performance data; no content or configuration changes	Leaders, analysts or stakeholders who need visibility

Trinity Health

SSO access: proposed operating principles

IT manages access requests via the ServiceNow Self Service portal; the assigned ORM role determines what the user can do once inside the platform.

1. Purpose-based access

Every user should have a defined business reason for platform access.

2. Least privilege

Provide the lowest level of access needed to perform the user's responsibilities.

3. Scoped visibility

Business-extension and ministry users should see only the locations/data required for their role.

4. Named ownership

Each elevated role should have a clear accountable owner and periodic review.

5. Central governance

Enterprise administrators maintain standards, role definitions and cross-enterprise oversight.