Security Section — Learning Path

September 11, 2026

Security Section — Learning Path

Learning Paths › Security Section

This learning path is for security administrators and application owners who manage access in the Security Section. You will learn how to establish an access model with roles and teams, provision and maintain user accounts, and perform ongoing reviews and updates using the available security screens.

Learning objectives

- By the end of this path you can create and maintain user records in the Security Section.
- By the end of this path you can create roles and configure role access using the role maintenance screens.
- By the end of this path you can organize users into teams for shared access administration.
- By the end of this path you can update existing users, teams, and roles as organizational needs change.
- By the end of this path you can choose the appropriate security screen for common access-management scenarios.

Prerequisites

- Access to the Security Section.
- Permission to view and maintain Users, Teams, and Roles.
- Familiarity with your organization’s user-access and approval process.
- A basic understanding of which people need access and how your organization groups work responsibilities.

Module 1: Establish the access model

Goal: Build the foundational structure for managing security by defining the roles and teams your organization needs.

Lesson 1.1: Review the existing security structure

When you are taking responsibility for security administration, first identify the roles and teams already in use so that you do not create duplicate structures. Open **Roles** to review the available roles, then open Teams to review existing team records. Use this review to determine whether the required access structure already exists or whether new security records are needed.

Practice task: Review the available role and team records and identify one role or team that may need to be updated.

Lesson 1.2: Create a role for a new responsibility

When a new job responsibility requires a distinct access pattern, create a role rather than relying on an informal or unmanaged approach. From **Roles**, open **Roles** and create the role record. Configure the role using the options available on the role screen, then save it so it can be used as part of your security model.

Practice task: Create a role for a hypothetical new business responsibility.

Lesson 1.3: Create a team for a working group

When several users belong to the same department, project, or operational group, create a team to manage them as a group. From Teams, open Teams and create the team record. Use a clear, recognizable team name that helps future administrators understand the group's purpose.

Practice task: Create a team for a hypothetical department or project group.

Module 2: Provision users for daily work

Goal: Add users and maintain their records so people can securely access the application.

Lesson 2.1: Add a new user

When a new employee or approved external user needs application access, create their user record through the user administration area. Open **Users**, then select **Users**. Enter the required user information and complete the available configuration before saving the new user record.

Practice task: Create a user record for a hypothetical new team member.

Lesson 2.2: Update an existing user after a change

When a user's details or access-related configuration must change, update the existing record instead of creating a duplicate user. Start from **Users**, locate the user, and open **Users**. Review the current configuration, make the approved changes using the available options, and save the record.

Practice task: Open an existing user record and make one approved test update, if your training environment allows it.

Module 3: Manage team membership and shared administration

Goal: Keep team membership accurate as people join, move between, or leave working groups.

Lesson 3.1: Add users to a team

When a user joins a department or project group, update the team so its membership reflects the current organization. Open Teams, select the appropriate team, and open Teams. Use the available team-user maintenance options to add the user to the team, then save the update.

Practice task: Add a hypothetical new team member to the team you created or selected.

Lesson 3.2: Review and correct team membership

When a person transfers, changes responsibilities, or no longer needs group-based access, review their team membership and update it promptly. Open the relevant team from Teams, then use Teams to review the listed users. Remove or adjust membership according to the approved change.

Practice task: Review one team's users and identify one membership change you would make in a transfer scenario.

Module 4: Maintain roles and perform access reviews

Goal: Keep role definitions and user access structures aligned with changing business needs.

Lesson 4.1: Update an existing role safely

When business responsibilities change, update the existing role that represents that responsibility. Open **Roles**, select the role to review, and open **Roles**. Confirm that you have selected the intended role, adjust its available configuration to match the approved requirement, and save the changes.

Practice task: Open an existing role and document the change you would request before making it.

Lesson 4.2: Perform a periodic security review

During a scheduled review, validate that users, teams, and roles still reflect current organizational needs. Review individual user records in **Users** and **Users**, team membership in Teams and Teams, and role definitions in **Roles** and **Roles**. Record or apply approved corrections through the appropriate maintenance screen.

Practice task: Choose one user, one team, and one role to review and list the evidence you would check for each.

Final assessment

1. A new business function requires a distinct access setup that does not match any existing role. Which screen should you use to create the new security role?
2. A new employee has been approved for application access. Where do you begin, and which screen do you use to create their user record?
3. A user has moved from one department to another and should no longer belong to their former working group. Which screen should you use to update the team's membership?
4. During an audit, you find that an existing role no longer matches the organization's approved access requirements. Which screen should you use to revise it?
5. You need to determine whether a user's details require maintenance, whether their team membership is current, and whether the team's role structure remains appropriate. Which Security Section areas should you review?

Answers

1. ****Roles. This is the role creation screen for establishing a new role record.
2. **Begin at **Users**, then use **Users. The Users area is the entry point for creating a new user record.

3. **Teams.** This screen is used from a team record to maintain the users in that team.
4. ****Roles. This is the screen for reviewing and updating an existing role.
5. **Review Users, Teams, and Roles, then use their relevant edit screens as needed.** A complete review considers the individual user, their team membership, and the roles that support the access model.