Security — Learning Path

September 11, 2026

Security — Learning Path

Learning Paths › Security

This learning path is for security administrators and authorized users who need to manage access to the business application. You will learn how to review and maintain user access, work with roles and teams, manage your own security profile and trusted devices, and make informed periodic access-review decisions.

Learning objectives

- By the end of this path you can review the application’s user and role records to understand how access is administered.
- By the end of this path you can create and maintain user security records through the available user screens.
- By the end of this path you can review role and team security records when investigating access requirements.
- By the end of this path you can maintain your own security profile and trusted login devices.
- By the end of this path you can use user, role, and team records to support recurring access reviews.

Prerequisites

- Access to the **Security** app.
- Authorization to view or manage users, roles, and teams as appropriate for your organization.
- A user account for accessing and updating your own security information.
- Familiarity with your organization’s access-control and approval procedures before making changes to another user’s access.

Module 1: Understand the access-management workspace

Learn where to review users, roles, and related security records before making access decisions.

Lesson 1.1: Start an access review from the user list

When someone requests access or an administrator needs to investigate an existing account, begin by locating the relevant user rather than changing access immediately. Open **Users** to review the available user records, then open the relevant **Security record (with data)** to examine that user's security information in context.

Practice task: Open **Users** and select one existing user's **Security record (with data)** for review.

Lesson 1.2: Review the roles that support access decisions

When a user's access needs to be understood or validated, review the role records used by the organization. Open **Roles**, select the relevant role, and inspect its **Security record (with data)** before deciding whether the role is appropriate for the requested work.

Practice task: From **Roles**, open a role's **Security record (with data)** and note the business purpose it appears to support.

Lesson 1.3: Consider team-based security during investigation

Some access questions require you to consider team security as well as individual user and role records. When investigating a user's access context, open the applicable Teams and compare that team context with the user and role records you reviewed.

Practice task: Open a Teams and identify when you would include team information in an access review.

Module 2: Manage the user lifecycle

Learn how to create and maintain user records while using existing access information to guide your work.

Lesson 2.1: Create a user record for a new colleague

When an approved new colleague needs application access, create their security record through the user-management workflow. Start from **Users**, initiate the new-user

process, and complete the available Principal Users. Use your organization's approved access request as the basis for the information you enter.

Practice task: Navigate from **Users** to the new-user Principal Users and identify the point at which you would apply your organization's approval process.

Lesson 2.2: Update an existing user after an approved change

When a colleague changes jobs, needs revised access, or requires a security-related correction, first locate their existing record. Use **Users** to find the account, open its **Security record (with data)**, and make only the approved changes after reviewing the access context.

Practice task: Open an existing **Security record (with data)** and describe the approval you would verify before changing it.

Lesson 2.3: Validate a requested change against role information

A request to alter a user's access should be evaluated against the role that supports the person's work. From the user's **Security record (with data)**, review the relevant role through **Roles** and its **Security record (with data)**. Return to the user record only after confirming the request aligns with the intended role.

Practice task: Review one user record and one role record, then state whether you would need additional approval before proceeding with an access change.

Module 3: Maintain personal security and perform periodic reviews

Learn how to keep your own security information current and use the available records for ongoing governance.

Lesson 3.1: Maintain your own security profile

When your own security details need attention, use the self-service security record rather than changing another user's account. Open My Profile, review your information, and update it according to your organization's security policy.

Practice task: Open My Profile and review your profile for information that should be kept current.

Lesson 3.2: Review trusted login devices

When you need to confirm which devices are trusted for your account, review the trusted-device area. Open My Profile, examine the devices presented, and follow your organization's process for any device you do not recognize or no longer use.

Practice task: Open My Profile and determine whether every displayed device is expected.

Lesson 3.3: Run a focused periodic access review

During an access-review cycle, work from evidence across user, role, and team records. Begin with **Users**, open each relevant **Security record (with data)**, validate the supporting role in **Security record (with data)**, and consider the related Teams where team context is relevant. Record or escalate exceptions through your organization's established process.

Practice task: Choose one user record and outline the user, role, and team records you would review before confirming access.

Final assessment

1. A manager requests access for a newly approved employee. Which Security screens should you use to begin creating the account, and what should guide the information you enter?
2. You receive a request to change an existing employee's access after a job change. What should you review before making the update, and which screens support that review?
3. During an audit, you need to determine whether a user's access is supported by the intended role and relevant team context. What sequence of records should you inspect?
4. You notice a device in your account's trusted-device list that you do not recognize. Which screen should you use, and what should you do next?
5. A user asks you to update details in your own account while you are reviewing their record. Which security record should be used for your personal information, and why should it be kept separate from the other user's record?

Answers

1. Start with **Users** and use the new-user Principal Users; enter information based on the approved access request.

Why: New-user creation should follow the authorized request and user-management workflow.

2. Review the user's **Security record (with data)** and the relevant role in **Security record (with data)**, accessed through **Roles.**
   Why: The requested change must align with the user's approved role and work needs.

3. Inspect the user's **Security record (with data)**, the applicable **Security record (with data)**, and the relevant Teams.
   Why: User, role, and team records together provide the access context needed for review.

4. Use My Profile and follow the organization's process for an unrecognized device.
   Why: Trusted devices are reviewed from the dedicated trusted-login-device screen.

5. Use My Profile for your own information.
   Why: Your personal security profile is separate from the other employee's user security record.