4. Security and compliance

└ **4.2 Permissions and access**

└ **4.2.2 Access levels: stakeholders, collaborators**

---

1. What are the main access levels available in Azure DevOps?
2. What capabilities are included with Stakeholder access?
3. How do access levels differ from security group permissions?
4. Who should be assigned the Stakeholder access level?
5. What are the limitations of Stakeholder access compared to Basic?
6. How do you manage access levels for users in Azure DevOps?
7. What is the recommended approach for granting outside collaborator access?
8. What restrictions apply to outside collaborators in Azure DevOps?
9. How can you audit and review access levels across an organization?
10. What are best practices for assigning access levels in Azure DevOps?

---

1. **What are the main access levels available in Azure DevOps?**
   - Stakeholder,
   - Basic,
   - and Visual Studio Subscriber.

---

2. **What capabilities are included with Stakeholder access?**
   - Stakeholders can
     - view & edit work items,
     - create & manage backlogs and boards,
     - and run some queries.
   - They cannot access code, pipelines, or advanced features.

---

3. **How do access levels differ from security group permissions?**

Access levels determine feature visibility and availability; security groups control specific permissions within those features.

---

4. **Who should be assigned the Stakeholder access level?**

Users who need visibility into project work but do not require code or pipeline access, such as business analysts, sponsors, and some external partners.

---

5. **What are the limitations of Stakeholder access compared to Basic?**

Stakeholders cannot contribute code, manage pipelines, view test plans, or access advanced reporting and dashboards.

---

6. **How do you manage access levels for users in Azure DevOps?**

Go to Organization *Settings* > *Users*, select the user, and assign the appropriate access level (Stakeholder, Basic, etc.).

---

7. **What is the recommended approach for granting outside collaborator access?**

Invite external users with the minimum required access level, typically as Stakeholders or limited Basic users, and restrict security group membership as needed.

8. **What restrictions apply to outside collaborators in Azure DevOps?**
   - They may have limited access to organization-wide resources,
   - cannot be assigned certain licenses,
   - and may be restricted by policies (e.g., limited to specific projects).

---

9. **How can you audit and review access levels across an organization?**
In *Organization Settings > Users*, filter or export the user list to review assigned access levels and license usage.

---

11. **What are best practices for assigning access levels in Azure DevOps?**
   - Assign the lowest access level that meets business needs,
   - review user assignments regularly,
   - and update access as roles or requirements change.