Azure DevOps – Project Administrator Checklist

DevOps team has prepared this document to help you get started with the first steps in your Azure DevOps project. You can find more details on Azure DevOps, including training information, on our FAQ page. For consulting topics, you can contact our team at devops_support@henkel.com.

Table of Contents

1. Prerequisites

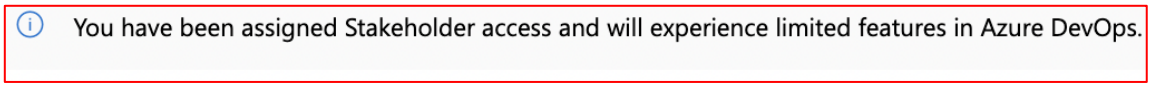
1.1. Request new Azure DevOps project

You can request a new Azure DevOps project through ServiceNow Azure DevOps request form. This request form is only for the below Azure DevOps organizations managed by DevOps team at Henkel:

- https://dev.azure.com/henkel-west-europe/
- https://dev.azure.com/henkel-east-asia/
- https://dev.azure.com/henkel-central-us/
- https://dev.azure.com/henkeldx/

1.2. Check your access level (license)

You can check your current access level by going to *Organization settings – Users*. Project administrators need a **Basic** access level, otherwise feature visibility and permissions within your Azure DevOps project will be limited. If you currently have the below notification in your Azure DevOps page, your access level is **Stakeholder** (the default access level for all new Azure DevOps users).



1.3. Request access level change to Basic

If your access level is **Stakeholder**, you must request access level change to **Basic** through ServiceNow Azure DevOps request form, *Request type: User Management: Access Level - Basic*.

2. Project setup

2.1. Select visibility of services

To simplify the web portal interface, if there are any Azure DevOps services (Boards, Repos, Pipelines, Test Plans, Artifacts) which will not be used in your project, you can hide them from all members of the project. Turning off services only hides them, if you choose to enable this service later, all your existing data will be available. You can do this by going to *Project settings – Overview – Azure DevOps Services* and Remove Service by using the toggle button. Refresh page to see changes.

2.2. Create and organize wiki

Use Azure DevOps wiki to share information with your team and as an overall place of documentation by going to *Overview – Wiki – Create project wiki.* After you created the first wiki pages, you can re-organize it in pages and subpages by using either the drag-and-drop option or by using the *Move page* option. More details on wiki and markdown in official Microsoft documentation here.

2.3. Set Dashboard permissions

Permissions to edit or delete dashboards or manage permissions can be set for both team or project dashboards. To add, edit, or manage a team dashboard, an Azure DevOps user must have **Basic** access. Based on project members knowledge of Azure DevOps, we recommend disabling the option that allows team members to delete dashboards by going to *Project settings – General – Dashboards – Security*.

2.4. Create teams

When you create a new team, Azure DevOps automatically creates a Board/Backlog and a Dashboard for that team. Team names must be unique in your Azure DevOps project. You can do this by going to *Project settings – General – Teams – New Team – Create.* We recommend adding a team description and at least two team

administrators (team administrators have the necessary permissions to add team members and configure all team settings).

2.5. Create permissions groups

You can create permission groups by going to *Project settings – General – Permissions – New Group.* Example of Permission groups can be different company names, when working in a project where several external companies are involved (e.g., Microsoft, Accenture, etc.), department names (Accounting, IT, Marketing, HR, etc.), different roles within the project (QA, Developers, Design, etc.). Permission group names must be unique in your Azure DevOps project. You can change settings of each permission group by going to *Project settings – General – Permissions – Select team - Permissions*.

2.6. Assign permission groups to teams

You can add a permission group to a team by going to *Project settings – General – Teams – Select team – Add - Add users and/or groups* – select desired permission group.

2.7. Activate Epics on hierarchy level

The Epics work item type level is not activated by default for the following default processes: Agile, Scrum, CMMI. If your team is using the Basic process, you can enable Epics by going to *Project settings – Team configuration – General – Backlogs* and enable Epics for all project teams using the dropdown menu for each team.

2.8. Configure and customize team backlogs/boards

Customize your Kanban boards by adding, removing, or renaming columns and swimlanes. Columns support the flow of work across the board. Swimlanes allow you to manage different classes of work as horizontal lanes on the board. In the Boards section, you can customize the settings for backlogs/boards for each project team. Detailed information from Microsoft here.

2.9. Define iteration paths (sprints) and configure team iterations

Two work item fields, Area Path and Iteration Path, provide a tree structure hierarchy for grouping work. Area paths group work items by product, functional, or feature area. Iteration paths group work items into sprints, milestones, or time periods for addressing those work items. We recommend defining a set of naming conventions for iterations and areas. Detailed information from Microsoft here.

2.10. Inherited process

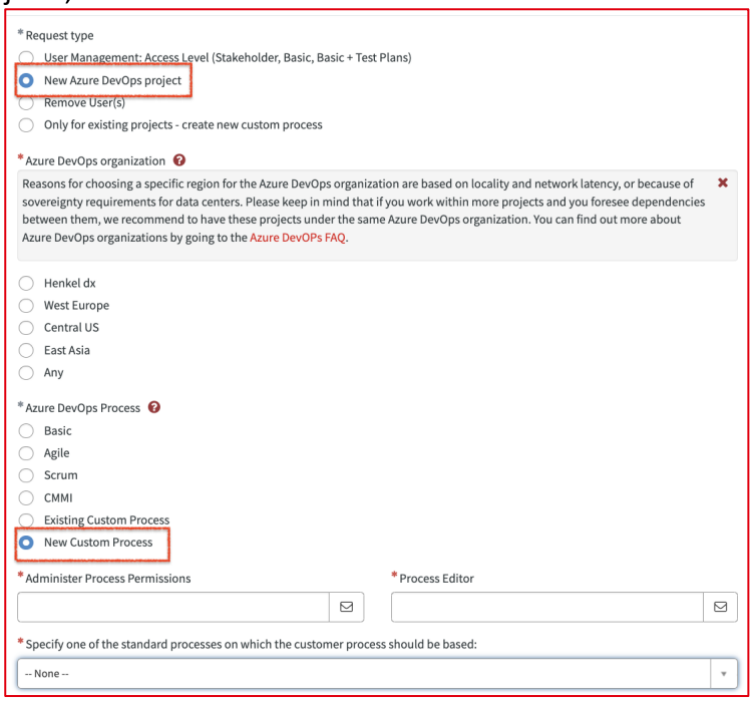
If you need additional fields and states in your project, you can request the creation of an inherited process. All projects that use an inherited process get the

customizations made to that process. In Azure DevOps, the four default processes (Basic, Agile, Scrum or CMMI) cannot be directly modified, therefore DevOps team can make a copy of one of the default processes and give you permissions to modify as you wish. You can check which process you are currently using in your project by going to *Project settings – Project details – Process*.

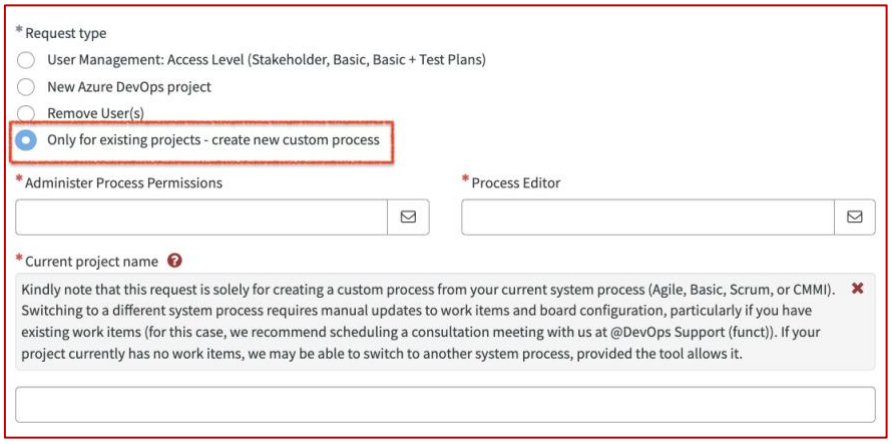
2.10.1. Request inherited process

If your project currently uses one of the system processes (by default, the system processes cannot be customized), request creation of new custom process through Azure DevOps ServiceNow form.

For new projects, select *New Custom Process.*



For existing projects, select *Only for existing projects - create new custom process*.



After the ServiceNow request has been completed by dxT DevOps team, go to *Organization settings – Process*, find your new custom process and customize as you wish.

2.10.2. Manage process permissions

It is not mandatory that project administrators are also process administrators/editors. By going to *Organization settings – Boards – Process – Process settings – Security*, you can add additional users to administer process permissions, delete or edit process. In Azure DevOps, 'Not set' equals 'Deny'.

2.10.3. Make changes to inherited process

We recommend aligning internally and informing your project members when you plan to make process changes, so that project work is not interrupted while performing these changes. Microsoft documentation on process customization here.

3. User Access

3.1. Prepare external user access

To avoid double licensing, decide whether the external users in your project will use the Henkel ID account or the Business Partner account for access to Azure DevOps. If Business Partner accounts will be used, you can invite the Business partner account by going to *myID* - *Business Partner Management* - *Invite Business Partner*. If you can't see the Manage Business Partner section in myID, after visiting this training video, you can click the Enable me button in order to be enabled for the myID menu. You can find detailed information in our Azure DevOps FAQ.

3.2. Add users to your project teams

After project setup is ready and business partner invites are created, you can invite users to your project teams. Users can be added to multiple teams and projects. You can do this by going to *Project settings – Teams – Select team – Add*. Keep in mind that the default access level for new users is **Stakeholder** and you can request the change to **Basic** access level through ServiceNow Azure DevOps request form.

3.3. Request access levels changes

First, decide which access level is needed by your project members:

- **Stakeholder**: default access level for new users to the organization. Assign to users who need access to a limited set of features
- **Basic**: Provides access to most features, including creating and working with Test Cases
- **Basic + Test Plans:** Provides access to all features included in Basic, as well as Test Plans. Assign only to users who need to create new Test Plans and Suites.

For new users, request access level change through ServiceNow Azure DevOps request form, *Request type: User Management: Access Level*. Detailed information from Microsoft on access levels here.

3.4. Organize Azure DevOps project onboarding session

Once initial project setup is complete, we recommend organizing a project onboarding session and going through the following topics:

- Azure DevOps tool introduction
- Azure DevOps overall project setup, including wiki as place of documentation
- information on Necessity / Data Minimization measures, to make sure that no personal information is added to Azure DevOps free-text fields
- links to Azure DevOps available trainings
- share Azure DevOps FAQ and ServiceNow Azure DevOps request form

- inform users on how to set user preferences (e.g., profile picture, notification settings, color scheme, etc.), detailed information from Microsoft here
- inform on difference between DevOps team (dxT), responsible for Azure DevOps tool governance and integration and Data Center & Cloud Architecture team (dxV), responsible for Henkel cloud infrastructure platform
- inform users on points of contact for Azure DevOps issues.

4. Project maintenance

4.1. Standard backlog items

All new Azure DevOps projects already include an optional template for Product Backlog Items/User Stories which should be considered for operational readiness. If your project does not contain this already, you can import a standard set of backlog items to cover non-functional requirements relevant for Operations, detailed steps on our FAQ page.

4.2. Regular reviews

It is one of the main responsibilities of project administrators to keep a clean Azure DevOps project environment, on top of quarterly reviews performed by DevOps team to comply with Henkel Security Unified Controls.

4.2.1. Review project description and SPOC

Keep an updated project description and single point of contact (SPOC) by going to *Project settings – Overview – Description*.

4.2.2. Review project administrators

Since members of this group have permissions to manage project configuration, repositories, pipeline resources, teams, and all project-level permissions, we recommend a regular review of your project administrators. A project must have a minimum of two project administrators, familiar with the content of the project, with at least one of them being a Henkel employee (in this context, Project Administrator is not the same as people manager). For this, go to *Project settings – Permissions - Project Administrators – Members – Add/Remove* users.

4.2.3. Review project members

If there are users who no longer need to have access to your project, you can remove them by going to *Project settings – Teams – Select team – Select user – Remove.*

If there are users whose responsibility changed within your project and they need a different access level (license), you can request an access level change through ServiceNow Azure DevOps request form – *User Management: Access Level (Stakeholder, Basic, Basic + Test Plans).*

If there are users who will no longer work for Henkel, you can request complete removal from Azure DevOps organization through ServiceNow Azure DevOps request form – *Remove User(s).* This action removes the user, together with its assigned access level, from all assigned projects within that organization (work items are not impacted by user deletion).

4.2.4. Review process editors/administrators

If your project is using an inherited process, go to *Organization settings – Boards – Process – Process settings – Security*, and review the current users and their permissions to administer process permissions, delete and edit process. If you switched from one inherited process to another inherited process, please inform DevOps team at devops_support@henkel.com to delete the process.

4.3. Project deletion

If your project is no longer needed, you can delete it by going to *Project settings – General – Overview – Delete project.* We highly recommend to save project data before deletion, you can find Microsoft documentation here. You will have up to 28 days to recover this project. After, this project will be deleted resulting in a loss of all project artifacts including work items, repos, teams, and builds.

5. Useful links

5.1. Henkel

- ServiceNow Azure DevOps requests here
- Azure DevOps FAQ here
- Supercharger Academy, Azure DevOps trainings:
  - Azure DevOps Basics Training
  - Azure DevOps Technical Training
  - Azure DevOps Basics (Recorded Training Modules)
- Henkel Cloud Portal here

5.2. Microsoft

- Microsoft Azure DevOps Roadmap and feature release here
- Microsoft best practices for "light-weight" Agile project management here
- Microsoft recommendation for Scrum and best practices here
- Microsoft guidance on Scaling Agile to large teams here.