Azure Sentinel Repositories - TSG

Last updated by | Naser Mohammed | Mar 19, 2023 at 7:18 AM CDT

PG troubleshooting guide

Access Instructions: Join the following Security Group on IDWeb to access our logs: SentinelEcosystemCustomerSupportSG

ICM Path: Team: Sentinel US-1 Service: Ecosystem -- ContentAsCode, Solution, Metadata

Known Limitation	What	Why/Available workaround
Deleting Content	if any content templates are removed from the source repository, their corresponding content will not be removed from the Azure Sentinel UX	Design Limitation.The deployed content can be deleted from UX afte its deletion from the source control, or directly through the REST API. If you prefer to do everything from the repository as opposed to the workspace, you can choose to disabl content such as analytic rules instea of deleting them.
Authorizing GitHub	If you are already signed into GitHub in your browser, you can't authorize your repos connection to a different GitHub account unless you sign out of your currently signed-in one.	By Design -- If you are already signec into GitHub in your browser, you wil not need to enter your credentials tc Authorize and would successfully authorize by simply clicking the "Authorize" button.
Authorizing Azure DevOps	If users is logged into a different account on Azure DevOps from the one in Azure Sentinel in the same browser, connection creation may fail.	Please make sure that you are **not** logged into Azure DevOps using a different email at the time of creatin a connection. If Azure DevOps is attempting to authorize to a differer account, using an Private window might help.
Deployments Limit	Each resource group in is limited to 800 deployments in its deployment history.	By Design due to dependency - If yo have a high volume of ARM templat deployments in your resource group(s), visit DeploymentQuotaExceeded for troubleshooting and additional details.
Deleting a GitHub connection after uninstalling the AS app on GitHub	You cannot properly delete a connection from the Repositories blade UI if you've uninstalled the Azure Sentinel App	Each app installation has a unique id which is used when removing a connection. Please note that in this case, you would need to manually remove the workflow from your GitHub repository to stop any future deployments in addition to removin the connection from the UI.

	from your connected GitHub repository	
Content Type Filtering	If your branch contains content types beyond the ones chosen in your connection, your deployments will display warnings confirming that those content type templates have not been deployed.	By Design – the deployments check i the content in the repo’s branch matches the selected content from the connection creation page, if it does not then it throws a warning and does not deploy it. This is norma behavior and relevant content types will be deployed normally.
Cross-workspace queries	Content that requires access to resources outside of your workspace’s resource group, such as cross-workspace analytics, is not currently deployable through Repositories	By Design - It requires the Repositories service application to have more access than that granted by the existing Sentinel Contributor role.

Playbooks missing parameter	If your playbook templates deployment fail with a missing parameter error, please add a parameter “workspace” definition to the playbook ARM template as a workaround. We are working to fix this during the preview.	Bug – We are working to fix this during the preview.
		`"parameters": {`
		`        "workspace": {`
		`            "type": "string`
		`        }`
		`    },`

Content Types: Hunting Queries and Parsers	Anytime you choose hunting queries, parsers will	They both use the Saved Searches API, meaning if one is selected, both content types would be deployed from the connected branch if they a present.

	also be deployed from your repo if they are present and Vice Versa. Filtering between the two does not work.	
Playbooks Support	Only basic playbook cases are currently supported. Playbooks with more advanced components such as KeyVault, Managed Identities, Azure Functions, Linked templates, parameter files are not yet supported.	By Design – more support coming in the next semester
Creating an ADO connection for multi-tenant/MSSP scenario	If user is on a guest account on the Azure Sentinel workspace (meaning they are not on their native tenant), they might not be able to see their ADO organization when creating a connection.	
Invalid User Access Token: IDX10223: Lifetime validation failed. The token is expired. ValidTo: '[PII is hidden. For more details, see [https://aka.ms/IdentityModel/PII.]'](https://aka.ms/IdentityModel/PII.), Current time: '[PII is hidden. For more details, see [https://aka.ms/IdentityModel/PII.]'](https://aka.ms/IdentityModel/PII.).	Session timed out	Refresh the page and try again
Role assignment failed with error: The client 'user@email.com' with object id 'PII' does not have authorization to perform action 'Microsoft.Authorization/roleAssignments/write' over scope '/subscriptions/PII/resourcegroups/PII/providers/Microsoft.Authorization/roleAssignments/xxxxxxxx' or the scope is invalid. If access was recently granted, please refresh your credentials.	User is not owner of RG	Connection must be created by a user with Owner role of the Resource Group containing this Azure Sentinel workspac
TF402455: Pushes to this branch are not permitted; you must use a pull request to update this branch.	No sufficient permissions on the source control to access repository or branch / create	Adjust user settings on the source control. E.g. on ADO user must be Contributor or higher in the project and must at least have "basic" access level i the organization. User must also be able to bypass any enabled branch policies.
The user 'PII\\user@email.com' is not authorized to access this resource		

	a connection with them	

FAQs :

- What is the trigger for new deployments?

Anytime content in the connected repository branch is modified, or new content templates are added, a deployment will be triggered and deploy all the content of the branch to the connected Azure Sentinel workspace(s).

- How can I check the health of my connections and deployments?

There is currently no mechanism to monitor the health of your connections and deployments directly from the Azure Sentinel UX. However, we've added a link to each connection's side panel that takes you to your deployment history and logs.

- How many connections can I have in my workspace?

The current limit on total number of connections per workspace is 5. This limit is expected to change as more content types are added in the future. If you have a request for more connections let us know.

- Is there a current mechanism for safe or smart deployments?

The current Repositories experience deploys content from the source repository branch to all connected Azure Sentinel Workspaces at the same time. We understand that in some scenarios, customers prefer to deploy content to their connected workspaces in staged or controlled timeline. This is a capability that we are exploring and hope to support in the future.

- Does this feature validate my content templates?

The Repositories experience is not intended to validate any of the content in the connected repositories. Content templates are deployed as they are. You should validate all content templates using your regular validation process.

- Is there a way to programmatically manage my CICD pipeline with this new feature?

The process to programmatically manage your CICD pipeline programmatically with this new feature (through REST API) is possible but is extremely manual. This capability is not officially supported at this time, but we plan to make this more feasible in the future.