ACR task network bypass policy

The ACR tasks networkRuleBypassAllowedForTasks setting is a new policy setting being introduced allowing customers to opt-in to network bypass for tasks. As discussed in [ACR trusted services](<https://learn.microsoft.com/en-us/azure/container-registry/allow-access-trusted-services>), some users require network restricted access to a container registry. This network restriction allows for certain services or identities to bypass network controls based on defined rule access.

Why is the change happening?

ACR users can configure tasks to use System Assigned Managed Identity (SAMI) to authenticate with a container registry. However, when the registry is network isolated, the registry owner can specify Allow trusted Microsoft services to access this container registry. ACR tasks have transitioned from listing as a [trusted service](<https://learn.microsoft.com/en-us/azure/container-registry/allow-access-trusted-services)>. Because registry owners can enable the trusted service setting to continue to allow tasks as a trusted service, the new policy setting disables this by default ensuring customers workflows remain secured.

When will the change take effect?

There are two phases:

* On **16 May 2025**, the registry policy setting called networkRuleBypassAllowedForTasks will be introduced and there will be no disruptions to existing workflows.
* Starting on **1 June 2025**, the default network bypass policy behavior will change. If the new setting is unset, network bypass for tasks using System-Assigned Managed Identity (SAMI) tokens will be denied by default and will require explicit configuration to restore functionality. Customers who rely on network bypass for their container registry tasks but have not explicitly set the new policy setting will encounter **403 forbidden errors**.

**Important:** There is no impact to customers using [User-Assigned Identity](<https://learn.microsoft.com/en-us/azure/container-registry/container-registry-tasks-authentication-managed-identity>)

**Required action:** Beginning 1 June 2025, newly configured tasks workflows will be required to use the new network bypass policy. To avoid any potential issues, ensure your configurations are updated to use this new feature or alternatively use Agent Pool. Customers who rely on network bypass for their container registry tasks but have not explicitly set the new policy setting will encounter 403 forbidden errors. Alternatively, you may use the container registry Agent Pool feature to also restrict access. Review [Use Dedicated Pool to Run Tasks in Azure Container Registry](<https://learn.microsoft.com/en-us/azure/container-registry/tasks-agent-pools>) to configure firewall rules and/or advanced network configuration per your desired requirements.

Enabling and disabling the network rule bypass policy setting

To enable or disable the new policy setting, please run the relevant command and required variables as it pertains to your scenario.

Enable

registry="myregistry"   
resourceGroup="myresourcegroup"   
   
# enable networkRuleBypassAllowedForTasks   
az resource update \   
--namespace Microsoft.ContainerRegistry \   
--resource-type registries \   
--name $registry \   
--resource-group $resourceGroup \   
--api-version 2025-05-01-preview \   
--set properties.networkRuleBypassAllowedForTasks=true

Disable

registry="myregistry"   
resourceGroup="myresourcegroup" 

# disable networkRuleBypassAllowedForTasks   
az resource update \   
--namespace Microsoft.ContainerRegistry \   
--resource-type registries \   
--name $registry \   
--resource-group $resourceGroup \   
--api-version 2025-05-01-preview \   
--set properties.networkRuleBypassAllowedForTasks=false

Customer Scenarios

Here are some scenarios which may be most appropriate for your use case. The steps can be accomplished using either the Azure CLI or ARM Template. The following examples focus on the Azure CLI.

Scenario #1: Use Agent Pool.

**Steps to enable**:

1. Review [Use Dedicated Pool to Run Tasks in Azure Container Registry](<https://learn.microsoft.com/en-us/azure/container-registry/tasks-agent-pools>) to configure firewall rules and/or advanced network configuration per your desired method.
2. Provision a dedicated agent pool:   
   az acr agentpool create --name <agent-pool-name> --registry \

<registry-name> --vnet <vnet-name>

1. Configure a quick task to run in the agent pool using acr build or automatically triggered task using acr task commands.
2. az acr build --registry <registry-name> --agent-pool \

<agent-pool-name> --image <image:tag> --file Dockerfile \ <path>

1. az acr task create --name <task-name> --agent-pool \

<agent-pool-name> --registry <registry-name> --schedule \ <cron\_format>

Scenario #2: Opt in to enable the new network bypass policy setting.

1. registry="myregistry"   
   resourceGroup="myresourcegroup"   
      
   # enable networkRuleBypassAllowedForTasks   
   az resource update \   
   --namespace Microsoft.ContainerRegistry \   
   --resource-type registries \   
   --name $registry \   
   --resource-group $resourceGroup \   
   --api-version 2025-05-01-preview \   
   --set properties.networkRuleBypassAllowedForTasks=true
2. Verify that tasks can continue bypassing network restrictions successfully by running az acr build, az acr run, or az acr task run commands and viewing the [streamed logs](https://learn.microsoft.com/en-us/azure/container-registry/container-registry-tasks-logs).

Scenario #3: No action is taken (default behavior) to enable the new network bypass policy setting.

**Phase 1**: ACR continues to honor the existing networkRuleBypassAllowed setting until May 16, 2025.

**Phase 2**: After June 1, 2025, if the networkRuleBypassAllowedForTasks setting is not explicitly set, network bypass for tasks is denied by default, resulting in 403 errors for tasks requiring network bypass.

Scenario #4: Use az acr purge](<https://learn.microsoft.com/en-us/azure/container-registry/container-registry-auto-purge>)locally for image cleanup

Users who prefer not to opt into the new policy setting and are not using network bypass can manage their ACR cleanup tasks locally using the az acr purge command. To do this, they can download the ACR CLI binary from [Azure ACR CLI GitHub](<https://github.com/azure/acr-cli)> and execute commands on their own machine. This enables them to remove unneeded or stale images from their registry without relying on ACR tasks or altering their current configuration. Running the purge locally ensures all operations occur within their trusted environment (customer managed trust boundary), avoiding any dependency on network bypass.

Scenario #5: Build and manage images on self-hosted environments

Users who wish to build container images or manage registries without opting in can use self-hosted environments. By running Docker or container runtime commands (e.g., docker build and docker push) on their own agents or machines that have direct access to the ACR registry, they can perform these tasks securely. This approach eliminates the need for ACR Tasks and/or network bypass, as operations are conducted entirely within their infrastructure, maintaining full control over their workflows (customer manages trust boundary).

Help and support

If you have a support plan and need technical help, open the ⁠[Azure portal](https://portal.azure.com/#blade/Microsoft_Azure_Support/HelpAndSupportBlade/overview) and select the question mark icon at the top of the page.