

Curated Portal: Policy Application Guide

TABLE OF CONTENTS

Technical Background	2
Implementing Curated Portal policy on a new tenant (Overview)	2
Implementing Curated Portal policy on a new tenant (Manual, Step-by-Step)	2
Assigning Tenant Root Group Role	2
Register the Root Management Group.....	6
Apply the Azure Policy for Resource Restrictions	7
Implementing Curated Portal policy on a new tenant (via Script)	10
Update existing Curated Portal policy (Overview)	10
Update existing Curated Portal policy (Manual, Step-by-Step)	10
Elevate Role Permissions	10
Access Policy and Copy Old Parameters	10
Apply Updated Parameters to Policy Assignment	10
Update existing Curated Portal policy (via Script)	12

Technical Background

Azure Policy is a service which measures configuration (and optionally mitigates deviations or blocks activity) on resources according to built-in or custom sets of rules called “policies”. These policies often accept arguments called parameters, and the policies can be enforced at various scopes (levels) from the tenant, management groups, subscriptions, resource groups, down to individual resources.

For Curated Portal, Microsoft provides a custom policy and AllowList in the form of Javascript Object Notation (JSON) files, which are applied to the tenant to have the desired effect. This custom policy will block the provisioning of resources not included in the contract’s Catalog.

As the contractually agreed upon Curated Catalog list of approved services grows over time, the implemented policy needs to be updated to include these new services. This document outlines the various methods to apply the Curated Portal policy to your tenants and keep them updated as the contract Catalog of services grows.

Implementing Curated Portal policy on a new tenant (Overview)

Curated Portal policy can be implemented via two means: 1) manually via a series of steps in the Azure Portal and execution of PowerShell and Azure Command Line Interface (CLI) steps, or 2) via execution of a command line tool, also available in the Curated Portal file repository repo. Both methods require Azure PowerShell and Azure CLI to be installed on the operating system used. The steps are:

1. Login
2. Elevate Role Permission to Global Administrator
3. Enable the Policy resource provider
4. Create a tenant Root Management Group (MG)
5. Elevate to Owner and User Access Administrator in the MG
6. Register the Policy Insights resource provider
7. Creating a new custom AllowList policy and assignment
8. Creating a new Curated Portal assignment with current parameters
9. Save and wait for up to 30 minutes for Policy changes to take effect

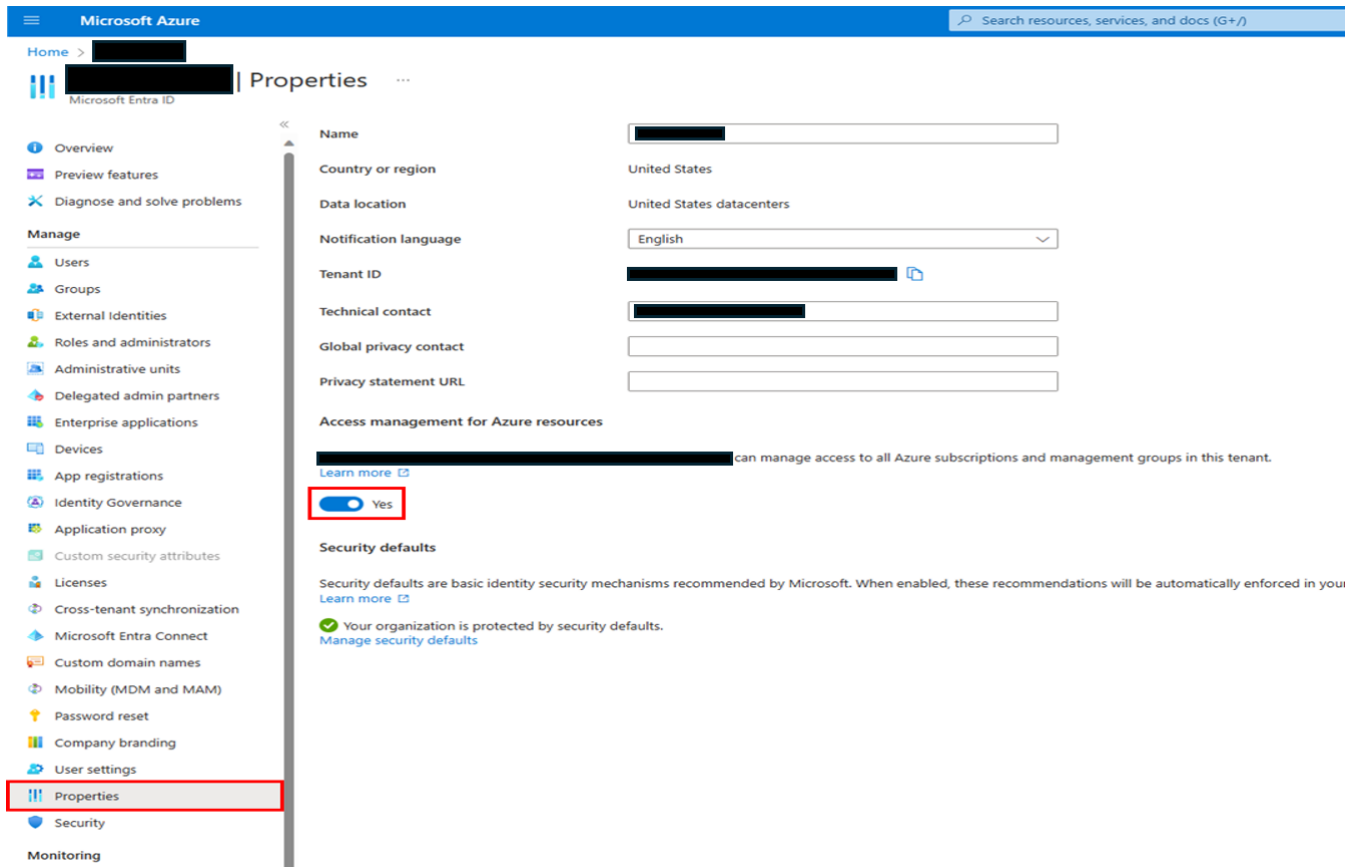
Implementing Curated Portal policy on a new tenant (Manual, Step-by-Step)

This section reviews all the steps needed to implement policy on a brand-new tenant.

Assigning Tenant Root Group Role

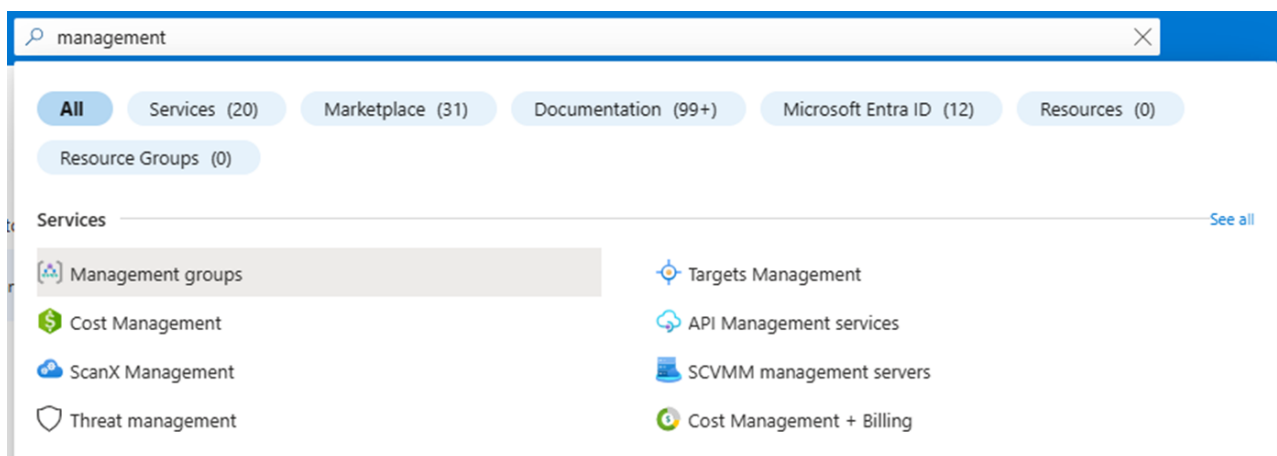
1. Configure tenant to apply Curated Portal utilizing the **Global Administrator** role. *Note – These steps only need to be completed on initial setup.*

- Turn on **Access Management** for Azure Resources from the Entra ID Service page and select **Properties**. *Note – Ensure to turn Access Management back **OFF** once Group Role assignment is completed.*



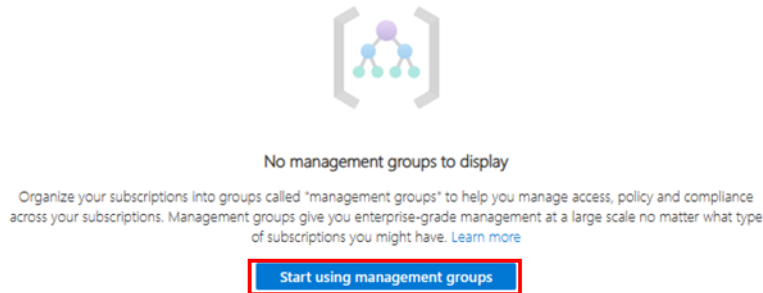
The screenshot shows the Microsoft Azure portal interface. The left-hand navigation pane is visible, with the 'Properties' option under the 'Microsoft Entra ID' section highlighted with a red box. The main content area displays the 'Properties' page for the selected service. The 'Access management for Azure resources' section is expanded, showing a toggle switch set to 'Yes', which is also highlighted with a red box. Below this, the 'Security defaults' section is visible, indicating that security defaults are enabled for the organization.

- Select **Management Groups** in "All Services" or search for it via the search bar.



The screenshot shows the Microsoft Azure portal search results for the term 'management'. The search bar at the top contains the text 'management'. Below the search bar, there are tabs for 'All', 'Services (20)', 'Marketplace (31)', 'Documentation (99+)', 'Microsoft Entra ID (12)', and 'Resources (0)'. The 'All' tab is selected. Under the 'Services' section, the 'Management groups' service is highlighted with a grey background. Other services listed include 'Cost Management', 'ScanX Management', 'Threat management', 'Targets Management', 'API Management services', 'SCVMM management servers', and 'Cost Management + Billing'.

- If this is an initial tenant set up, you may see the message below. Click **Start Using Management Groups**.



- Select **Tenant Root Group**

↑↓ Name	Type	ID	↑↓ Total subscriptions
<div> Tenant Root Group </div>	Management group		1
<div> </div>	Subscription		

- Select the **Access Control (IAM)** blade on the left side then select **Add** and **Add Role Assignment**.

Microsoft Azure

Search resources, services, and more

Home > Management groups > Tenant Root Group

Tenant Root Group | Access control (IAM)

Management group

Search

[Add](#)
[Download role assignments](#)
[Edit columns](#)
[Refresh](#)
[Remove](#)
[Feedback](#)

[Overview](#)
[Subscriptions](#)
[Resource Groups](#)
[Resources](#)
[Activity Log](#)
[Access control \(IAM\)](#)

[Add role assignment](#)
[Add co-administrator](#)
[Add custom role](#)

View my access

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Check access

- Choose the **Privileged Administrator Roles** tab and select **Owner**. Click **Next** to **Review + Assign**.

Role Members Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Assignment type

Job function roles **Privileged administrator roles**

Grant privileged administrator access, such as the ability to assign roles to other users.

⚠ Can a job function role with less access be used instead?

Search by role name, description, or ID Type: All Category: All

Name ↑↓	Description ↑↓
Owner	Grants full access to manage all resources, including the ability to
Contributor	Grants full access to manage all resources, but does not allow you
Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover i
Role Based Access Control Administrator (Preview)	Manage access to Azure resources by assigning roles using Azure f
User Access Administrator	Lets you manage user access to Azure resources.

Showing 1 - 5 of 5 results.

- Confirm role assignment by navigating to the **Role Assignments** Tab.

Home > Management groups > Tenant Root Group

Tenant Root Group | Access control (IAM)

Search Add Download role assignments Edit columns Refresh Remove Feedback

Check access **Role assignments** Roles Deny assignments Classic administrators

Total role assignments

Owner	Contributor	User Access Administrator
1	0	1
View assignments	View assignments	View assignments

All Job function roles (0) Privileged role assignments (2)

Search by name or email Type: All Role: All Scope: A

2 items (2 Users)

Name	Type
Owner (1)	
<input type="checkbox"/> [Redacted]	User
User Access Administrator (1)	
<input type="checkbox"/> [Redacted]	User

Register the Root Management Group with the Microsoft.PolicyInsights resource provider using the [Management Group registration](#) API for Unclassified tenants. Verify success by noting **Response Code 200**.

- **groupID = TenantID**
- **resourceProviderNamespace = Microsoft.PolicyInsights**

Parameters

groupId*

resourceProviderNamespace*

Microsoft.PolicyInsights

api-version*

2021-04-01

name

value

+

Headers

Content-Type*

application/json

name

value

+

Request Preview

HTTP

Copy

POST https://management.azure.com/providers/Microsoft.Management/managementGroups/[REDACTED]/providers/Mic
Authorization: Bearer eyJ0eXA1OjIKVlQ1LCJhbGciOiJIUzI1NiIsInRldC16IjklHwS5R1BraGMzaE91UjYyZXZmdmduTG83WS1letpZCI6IjlHbwS5R1BraGMzaE
Content-type: application/json

< >

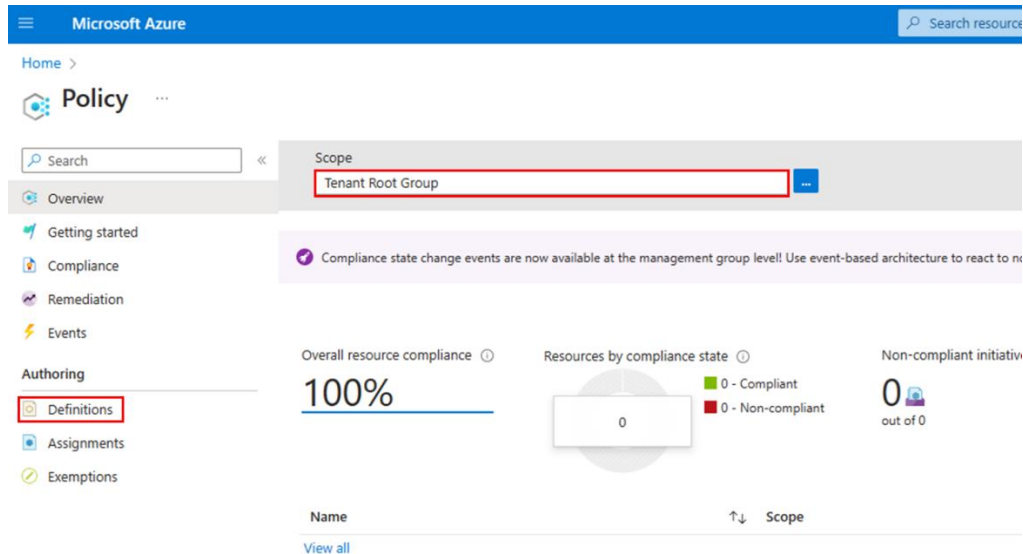
Run ▶

Response Code: 200

Note: Customers will need to use PowerShell for registration in air-gapped clouds using the [Invoke-AZRestMethod](#). PowerShell access is available via Azure Toolbox.

Apply the Azure Policy for Resource Restrictions

1. From Azure Policy service page, set scope to **Tenant Root Group** and select **Definitions** from the Authoring section.



Microsoft Azure

Home > Policy

Search

Scope: Tenant Root Group

Compliance state change events are now available at the management group level! Use event-based architecture to react to n

Overall resource compliance 100%

Resources by compliance state 0

Non-compliant initiatives 0 out of 0

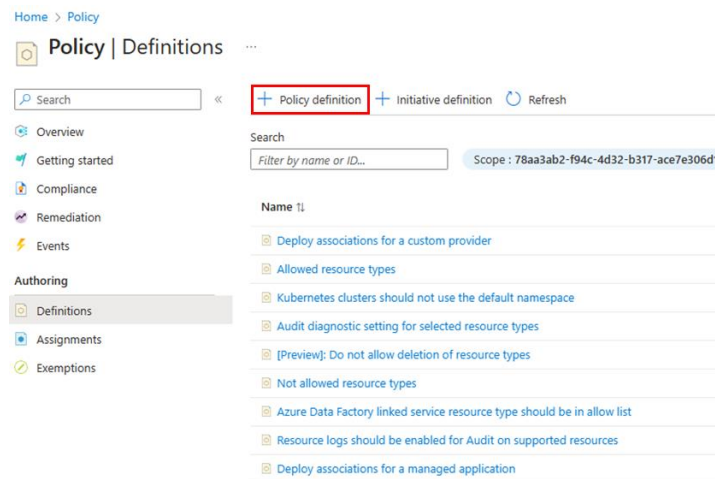
Authoring

- Definitions
- Assignments
- Exemptions

Name

View all

2. Select **Policy Definition**



Home > Policy

Policy | Definitions

Search

Filter by name or ID...

Scope: 78aa3ab2-f94c-4d32-b317-ace7e306d1

Policy definition

Initiative definition

Refresh

Name

- Deploy associations for a custom provider
- Allowed resource types
- Kubernetes clusters should not use the default namespace
- Audit diagnostic setting for selected resource types
- [Preview]: Do not allow deletion of resource types
- Not allowed resource types
- Azure Data Factory linked service resource type should be in allow list
- Resource logs should be enabled for Audit on supported resources
- Deploy associations for a managed application

3. Set definition location to **Tenant Root Group** and Name the policy **"*ContractName* Allowed Resources"**



Home > Policy | Definitions >

Policy definition

New Policy definition

BASICS


Definition location *

Tenant Root Group

Name *

ContractName Allowed Resources

4. **Create new** policy and grab the [listOfResourceTypesAllowed](#) code from Curated Portal file repository and add it to the policy rule and update "**mode**" from *Indexed* to **All** and then **Save**.

Category 
☒ Create new ☐ Use existing

Category

POLICY RULE

[Import sample policy definition from GitHub](#)
[Learn more about policy definition structure](#)

```

1 {
2   "properties": {
3     "displayName": "Allowed resource types",
4     "policyType": "BuiltIn",
5     "mode": "All",
6     "description": "This policy enables you to specify the resource types that your organization can deploy. Only resource types that support 'tags'
7   },
8   "metadata": {
9     "version": "1.0.0",
10    "category": "General"
11  },
12  "parameters": {
13    "listOfResourceTypesAllowed": {
14      "type": "Array",
15      "metadata": {
16        "description": "The list of resource types that can be deployed.",
17        "displayName": "Allowed resource types",
18        "strongType": "resourceTypes"
19      }
20    }
21  },
22  "policyRule": {
23    "if": {
24      "not": {
25        "field": "type",
26        "in": "[parameters('listOfResourceTypesAllowed')]"
27      }
28    },
29    "then": {
30      "effect": "deny"
31    }
32  }
33 },
34 "id": "/providers/Microsoft.Authorization/policyDefinitions/a08ec900-254a-4555-9bf5-e42af04b5c5c",
35 "name": "a08ec900-254a-4555-9bf5-e42af04b5c5c"
36 }

```

5. **Assign** the created policy definition.

Home > Policy | Definitions >

Allowed Resources

Policy definition

Essentials

Name: Allowed Resources

Description: --

Available effects: Deny

Category: --

Definition location: Tenant Root Group

Definition ID: /providers/Microsoft.Management/managementGroups/ /providers/Microsoft.Authorization/policyDefinitions/

Type: Custom

Mode: All

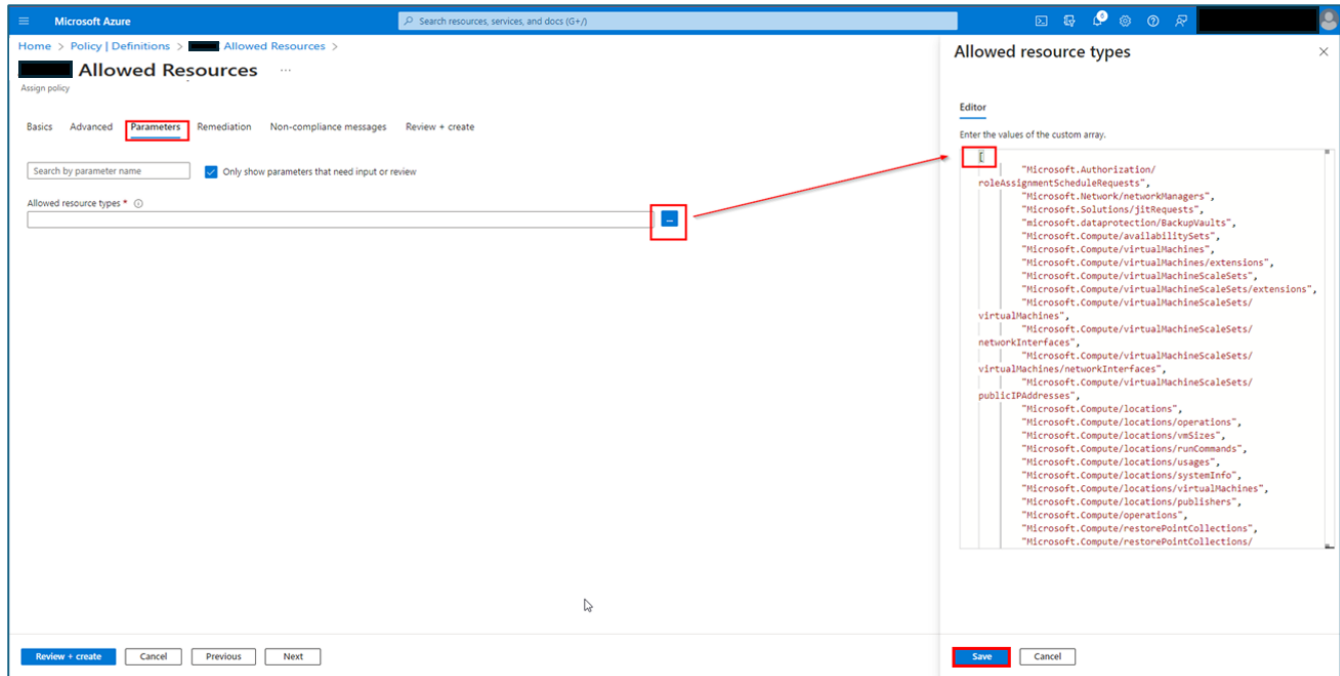
Definition Assignments (0) Parameters

```

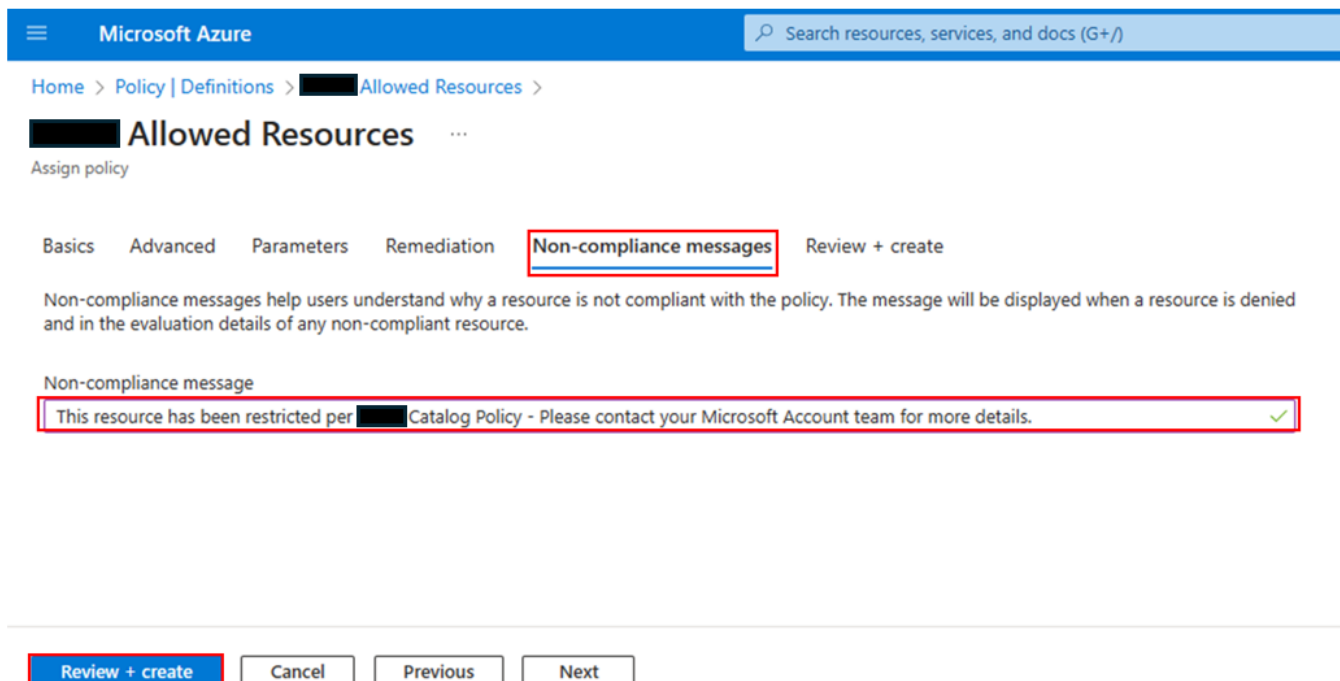
1 {
2   "properties": {
3     "displayName": "Allowed Resources",
4     "policyType": "Custom",
5     "mode": "All",
6     "metadata": {
7       "version": "1.0.0",
8       "createdBy": "2023-10-25T10:53:47.7163204Z",
9       "createdOn": "2023-10-25T10:53:47.7163204Z",
10      "updatedBy": null,
11      "updatedOn": null
12    }
13 }

```


- Parameter files are in the **Curated Portal Policy file repository**. Pull all the Resource Providers (RPs) from the JSON file and place them within [] in the **Editor** and click **Save**. *Note: If necessary, remove the first two layers of curly braces "{" so that the contents start and end with square brackets "[" per the below sample illustration. Spaces do not matter, but there must not be a comma after the last double-quoted item. Any red typographical errors such as missing double-quotes, missing square brackets, additional brackets, or missing or extra commas must be fixed.*



- Select the **Non-Compliance Messages** tab and add the recommended message: ***This resource has been restricted per *ContractName* Catalog Policy – Please contact your Microsoft Account team for more details.*** Select **Review + Create**.



Implementing Curated Portal policy on a new tenant (via Script)

A script is available in the Curated Portal file repository.

Update existing Curated Portal policy (Overview)

Updating an existing Curated Portal policy can be done via two methods:

1. Paste replacement text into the assignment parameters in the Azure Portal
2. Execute a command line tool with the "update" mode specified

The steps are:


1. Login
2. Elevate role permissions
3. Update the parameters and message
4. Save and wait for up to 30 minutes for Policy changes to take effect

Update existing Curated Portal policy (Manual, Step-by-Step)

Elevate Role Permissions

1. Login to the Azure Portal, to the applicable tenant
2. Elevate Role Permissions to **Global Administrator**

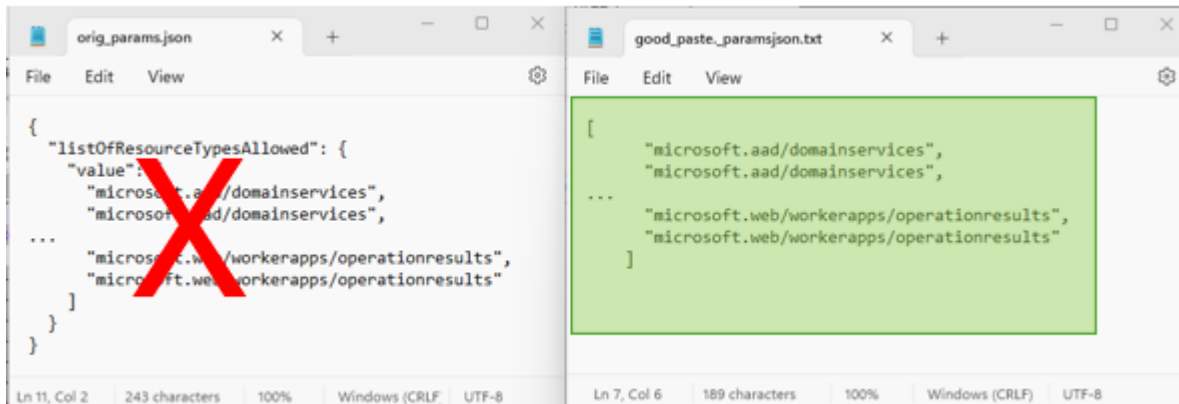
Access Policy and Copy Old Parameters

1. Navigate to **Azure Policy** via All Services or the search box
2. From Azure Policy service page, select **Assignments** from the Authoring section.
3. Under **Assignments**, select the existing assignment relating to Curated Portal assigned to the tenant Root Management Group
4. Select **Edit Assignment**
5. Select **Parameters** and then click the ellipsis  to open the [listOfResourceTypesAllowed](#) editor on the right side of the page
6. Select All (**Ctrl+A**) content in the editor window
7. Copy (**Ctrl+C**) all content from the editor and paste (**Ctrl+V**) to an empty text editor
8. **Save** the copied Resource Types as a backup in case you need to revert later, due to an error.
9. **Delete** the web editor content to have a blank space to enter the updated parameters.

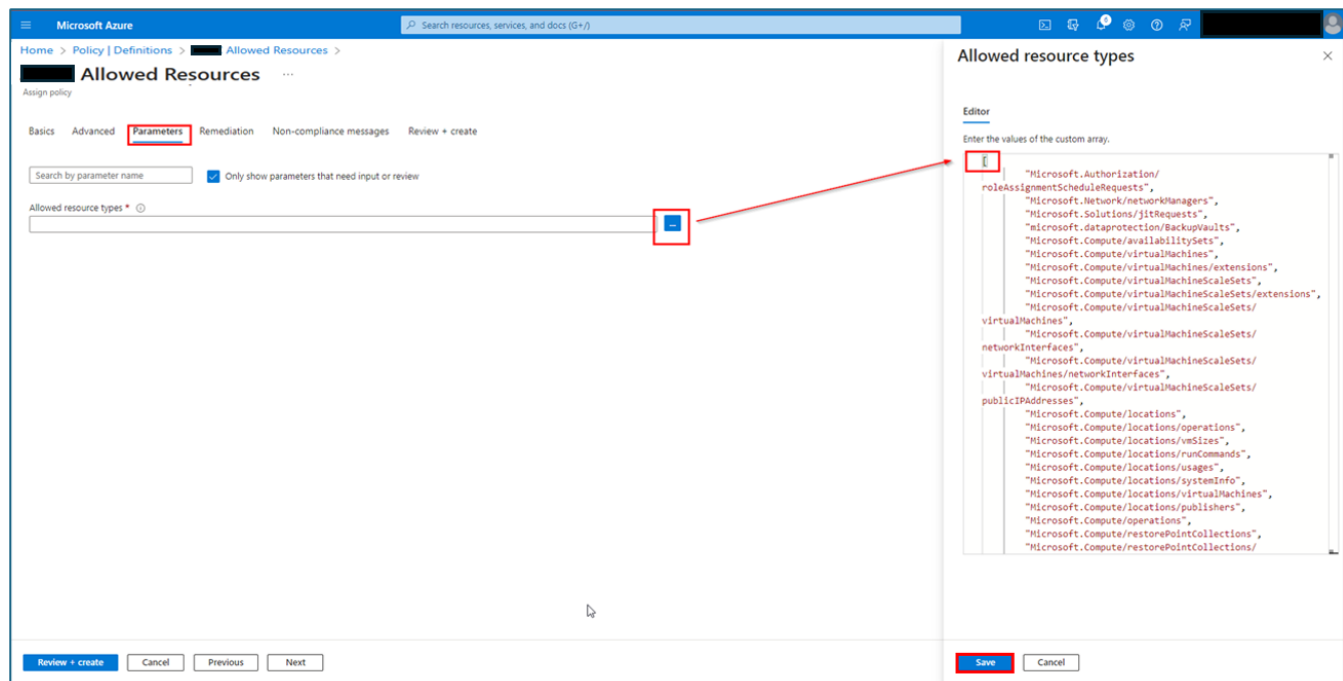
Apply Updated Parameters to Policy Assignment

1. Obtain the updated files from the **Curated Portal file repository**.

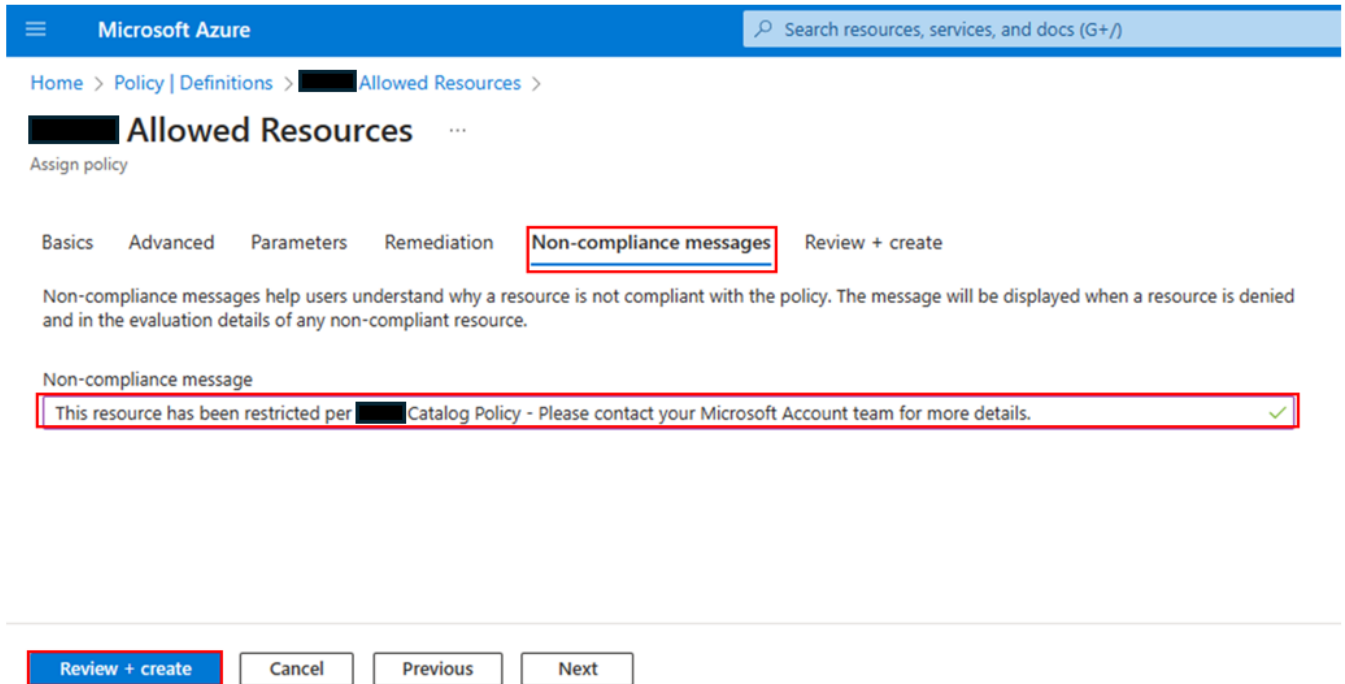
2. **Open** the JSON file for the most recent **Curated Portal policy parameters** in a new text editor
Note: If necessary, remove the first two layers of curly braces "{" from the top of bottom so that the contents start and end with square brackets "[" per this sample illustration:



3. In the text editor, Select All (**Ctrl+A**) and Copy (**Ctrl+C**) contents. *Note: Spaces do not matter, but there must not be a comma after the last double-quoted item.*
4. Paste (**Ctrl+V**) all copied content from the text editor to the empty web editor window, replacing the old parameters with the new list, then click **Save**. *Note: Any red typographical errors such as missing double-quotes, missing square brackets, additional brackets, or missing or extra commas must be fixed.*



5. Select the **Non-Compliance Messages** tab and add the recommended message: ***This resource has been restricted per *ContractName* Catalog Policy – Please contact your Microsoft Account team for more details.*** Select **Review + Create**.



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Policy | Definitions > [redacted] Allowed Resources >

[redacted] Allowed Resources ...

Assign policy

Basics Advanced Parameters Remediation **Non-compliance messages** Review + create

Non-compliance messages help users understand why a resource is not compliant with the policy. The message will be displayed when a resource is denied and in the evaluation details of any non-compliant resource.

Non-compliance message

This resource has been restricted per [redacted] Catalog Policy - Please contact your Microsoft Account team for more details. ✓

Review + create Cancel Previous Next

6. Optionally, click the **Basics** section, and review the assignment metadata and update the "Assigned by", "Assignment description" for versioning. Microsoft recommends not renaming the assignment name, so that it is consistently detectable in the environment by tools.

Update existing Curated Portal policy (via Script)

A script is available in the Curated Portal file repository.