

Curated Portal Policy Guide

Curated Portal Policy Implementation 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	2
Assigning Tenant Root Group Role.....	2
Register the Root Management Group Using Azure CLI	6
Register the Root Management Group Using Azure Cloud Shell	6
Apply the Azure Policy for Resource Restrictions	7
Apply the Azure Policy for Azure AI Services Resource Restrictions	11
Apply the Azure Policy for JWCC MOD10 Resource Restrictions.....	11
Implementing Curated Portal policy on a new tenant (via Script)	11
Update existing Curated Portal policy (Overview)	12
Update existing Curated Portal policy (Manual, Step-by-Step)	12
Elevate Role Permissions.....	12
Access Policy and Copy Old Parameters	12
Apply Updated Parameters to Policy Assignment.....	12
Remove Ownership from Tenant Root Management Group.....	14
Update existing Curated Portal policy (via Script)	15

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

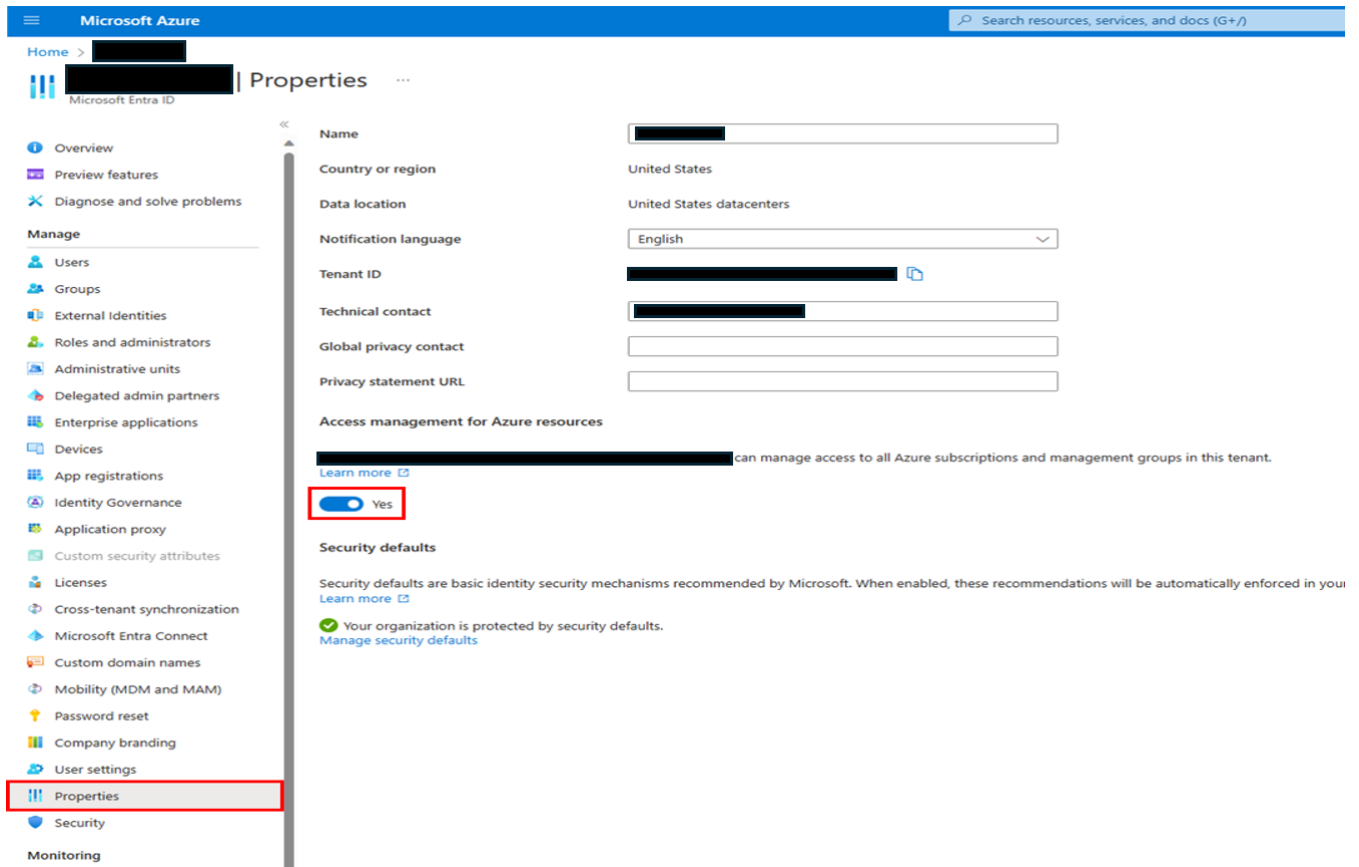
Implementing Curated Portal Policy on a New Tenant

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

Assigning Tenant Root Group Role

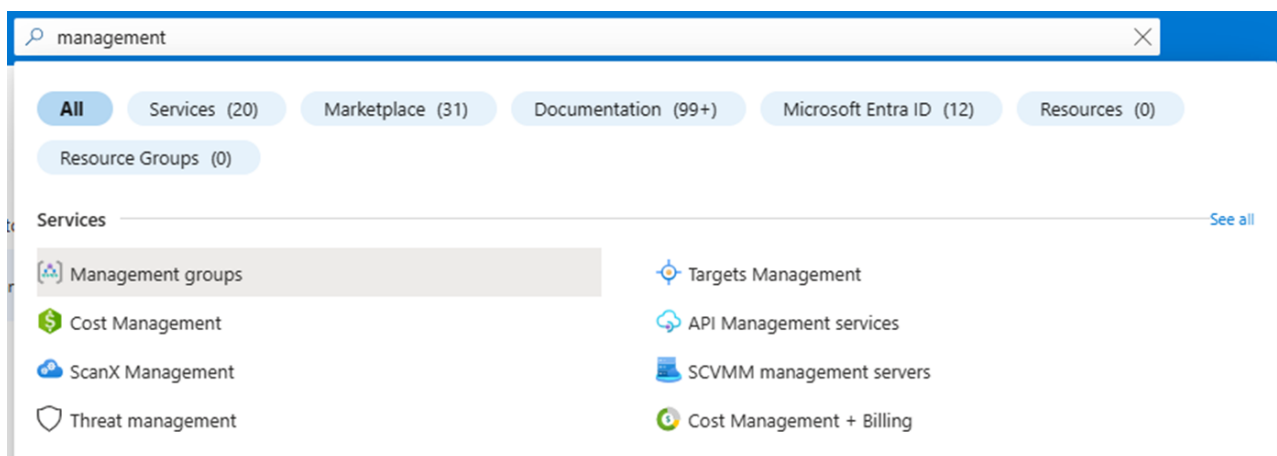
1. Configure tenant to apply Curated Portal utilizing the **Global Administrator** role. *Note – These steps only need to be completed on initial setup.*

- 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.*



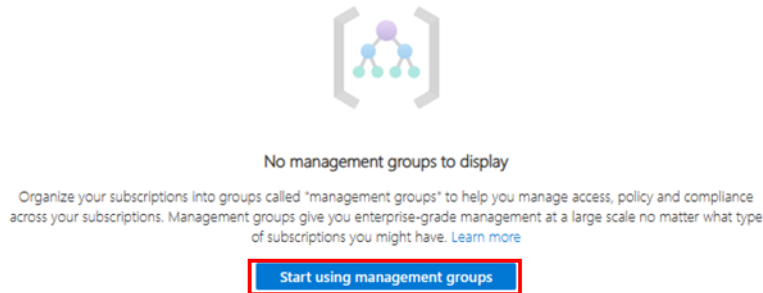
The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane is visible with the 'Properties' option highlighted. The main content area displays the 'Properties' page for 'Microsoft Entra ID'. The 'Access management for Azure resources' section is highlighted with a red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

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



The screenshot shows the Microsoft Azure portal search results for '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, 'Management groups' is highlighted. Other services listed include 'Targets Management', 'API Management services', 'SCVMM management servers', 'Cost Management + Billing', 'Cost Management', 'ScanX Management', and 'Threat management'.

- 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**.

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 assign roles to other users.
Contributor	Grants full access to manage all resources, but does not allow you to assign roles to other users.
Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover and manage access reviews.
Role Based Access Control Administrator (Preview)	Manage access to Azure resources by assigning roles using Azure RBAC.
User Access Administrator	Lets you manage user access to Azure resources.

Showing 1 - 5 of 5 results.

- Choose **Select Members** and choose the correct user from the right hand drop down. Use the **Select** button to confirm user selected and select **Next**

Role Members Conditions Review + assign

Showing a filtered list of roles because your permissions include a condition. [Learn more](#)

Assign access to ☒ User, group, or service principal ☐ Managed identity

Members **+ Select members**

Name	Object ID	Type
No members selected		

Description Optional

Selected members

Yan Zhongman Remove

Review + assign Previous Next

Select Close

- Select **Allow user to assign all role** and select **Review and Assign**

Role Members **Conditions** Review + assign

Selected role Owner

What user can do

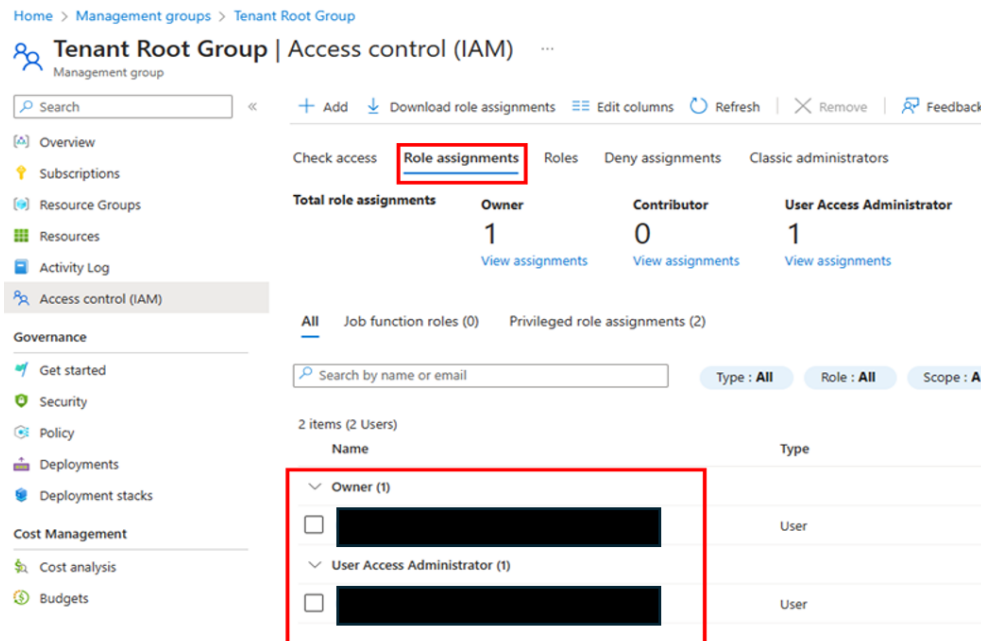
☐ Allow user to only assign selected roles to selected principals (fewer privileges)

☒ Allow user to assign all roles (highly privileged)

⚠ Owner is a privileged admin role that grants privileged administrator access, such as the ability to assign roles to other users. Microsoft recommends that you add a condition to narrow the permissions of this role to least privilege.

Review + assign Previous Next

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



Home > Management groups > Tenant Root Group

Tenant Root Group | Access control (IAM)

Search

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

Register the Root Management Group Using Azure CLI

To enable Policy, you must first register the Tenant Root Management Group with the Microsoft.PolicyInsights resource provider. Customers can run the following command via Azure CLI if logged in with Azure credentials:

Azure Commercial Login

```
az cloud set --name AzureCloud
az login
```

Azure Government Login

```
az cloud set --name AzureUSGovernment
az login
```

Register the Microsoft.PolicyInsights provider at the Tenant Root Management Group scope

```
$aadTenantId = az account list --query "[?isDefault].tenantId" -o tsv
echo $aadTenantId
az provider register --namespace "Microsoft.PolicyInsights" --management-group-id $aadTenantId --debug
```

Register the Root Management Group Using Azure Cloud Shell

***Link provided for new users that have never configured Cloud Shell in their tenant. Users that have Cloud Shell configured can move to running scripts below.

1. Register Cloud Shell resource provide by following the steps in the link:

[Get started with Azure Cloud Shell | Microsoft Learn](#)

2. Using BASH:

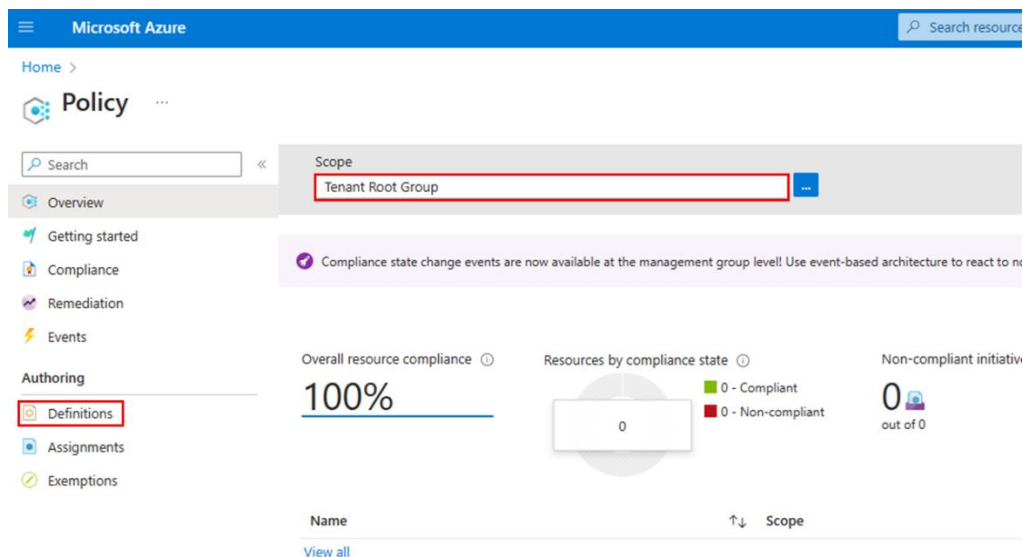
```
aadTenantId=$(az account list --query "[?isDefault].tenantId" -o tsv)
echo $aadTenantId
az provider register --namespace "Microsoft.PolicyInsights" --management-group-id
$aadTenantId --debug
```

3. Verify successful registration with a **Response status: 200**

```
cli.azure.cli.core.sdk.policies: This request has no body
urllib3.connectionpool: Starting new HTTPS connection (1): management.usgovcloudapi.net:443
urllib3.connectionpool: https://management.usgovcloudapi.net:443 "P
0
cli.azure.cli.core.sdk.policies: Response status: 200
cli.azure.cli.core.sdk.policies: Response headers:
cli.azure.cli.core.sdk.policies: 'Cache-Control': 'no-cache'
cli.azure.cli.core.sdk.policies: 'Pragma': 'no-cache'
cli.azure.cli.core.sdk.policies: 'Expires': '-1'
cli.azure.cli.core.sdk.policies: 'x-ms-ratelimit-remaining-tena
cli.azure.cli.core.sdk.policies: 'x-ms-request-id': '59376471-e
cli.azure.cli.core.sdk.policies: 'x-ms-correlation-request-id':
cli.azure.cli.core.sdk.policies: 'x-ms-routing-request-id': 'US
cli.azure.cli.core.sdk.policies: 'Strict-Transport-Security': '
cli.azure.cli.core.sdk.policies: 'X-Content-Type-Options': 'nos
cli.azure.cli.core.sdk.policies: 'Date': 'Wed, 03 Jul 2024 13:1
cli.azure.cli.core.sdk.policies: 'Content-Length': '0'
```

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

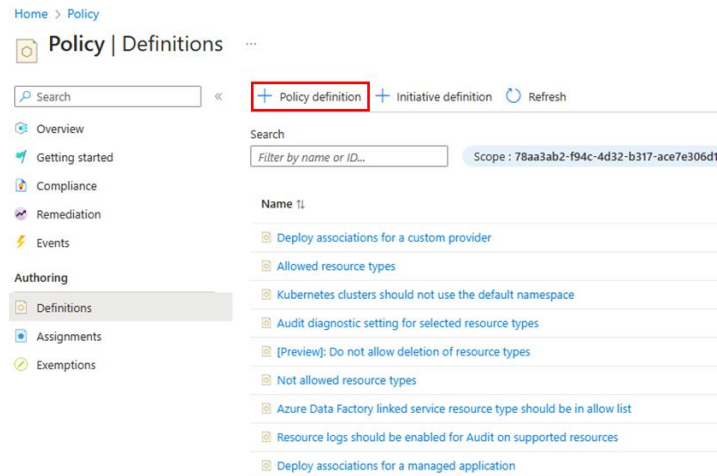
Exemptions

Name

Scope

View all

2. Select **Policy Definition**



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 [Allowed resource types.json](#) 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

 Assign  Edit definition  Duplicate definition  Delete 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": ,
9       "createdOn": "2023-10-25T19:53:47.7165204Z",
10      "updatedBy": null,
11      "updatedOn": null
12    }
13 }

```

- Parameter file is in the [Curated Portal Policy file repository](#). Grab all the Resource Providers (RPs) from the JSON file and place them within `[]` in the **Editor** and click **Save**.

Note – Parameter file name should be in format listed below.

Format -> **JWCC_CuratedPortal_USGov_<Year>.<Month>.<Version>.json**

Example -> **JWCC_CuratedPortal_USGov_2025.04.01.json**

The screenshot shows the 'Allowed Resources' configuration page in the Microsoft Azure portal. The 'Parameters' tab is selected, and a red box highlights the 'Add' button. A red arrow points from this button to the 'Allowed resource types' editor, which shows a list of resource providers.

- 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**.

The screenshot shows the 'Non-compliance messages' configuration page in the Microsoft Azure portal. The 'Non-compliance messages' tab is selected, and a red box highlights the message text: "This resource has been restricted per [redacted] Catalog Policy - Please contact your Microsoft Account team for more details."

Apply the Azure Policy for Azure AI Services Resource Restrictions

1. Follow **steps 1-3** from [Apply the Azure Policy for Resource Restrictions](#) section above to set the new definition location for the **Azure AI Services** policy definition.
2. Create a new **policy definition** using a file called [Curated Portal Azure AI Services.json](#) in GitHub file repository and then click **Save**.
3. Click on **Assign** to assign the policy definition.
4. Parameter file is in the [Curated Portal Policy file repository](#). Grab the parameter value for **allowedKinds** from the JSON file and place them within **[]** in the **Editor** and click **Save**.

Note – Parameter file name should be in format listed below.

Format -> **JWCC_CuratedPortal_AzureAIServices_USGov_<Year>.<Month>.<Version>.json**

Example -> **JWCC_CuratedPortal_AzureAIServices_USGov_2025.04.01**

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**.

Apply the Azure Policy for JWCC MOD10 Resource Restrictions

1. Follow **steps 1-3** from [Apply the Azure Policy for Resource Restrictions](#) section above to set the new definition location for the **JWCC MOD10** policy definition.
2. Create a new **policy definition** using a file called [Curated Portal Mod10.json](#) in GitHub file repository and then click **Save**.
3. Click on **Assign** to assign the policy definition.
4. Parameter file is in the [Curated Portal Policy file repository](#). Grab all the JWCC MOD10 Resource Providers (RPs) from the JSON file and place them within **[]** in the **Editor** and click **Save**.

Note – Parameter file name should be in format listed below.

Format -> **JWCC_CuratedPortal_Mod10_USGov_<Year>.<Month>.<Version>.json**

Example -> **JWCC_CuratedPortal_Mod10_USGov_2025.04.01**

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

Note: For any services consumed that are in the Mod10 parameter files, users will see in their Mod10 Policy Assignment Compliance dashboard that these services are listed as **non-compliant. That is to alert users that these services are allowed for non-production consumption only.*

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

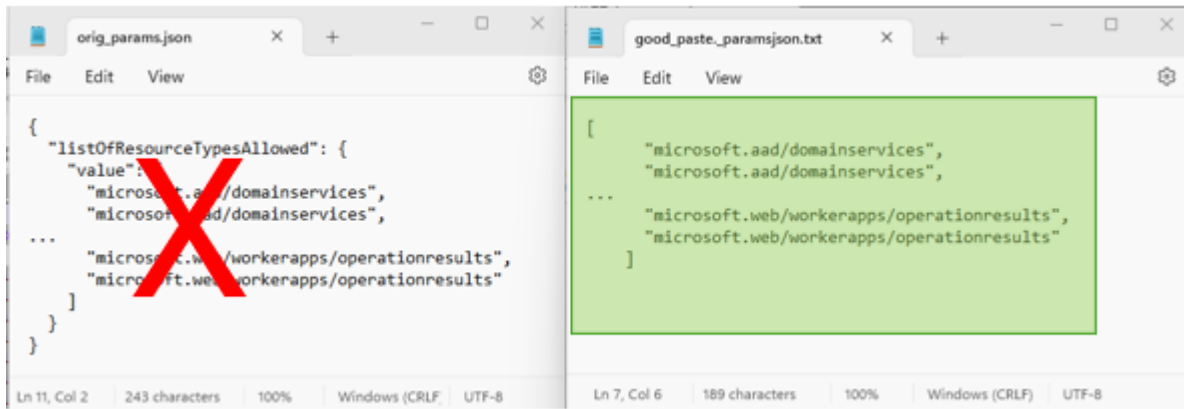
1. Login to the Azure Portal, to the applicable tenant
2. Elevate Role Permissions to **Global Administrator**

Access Policy and Copy Old Parameters

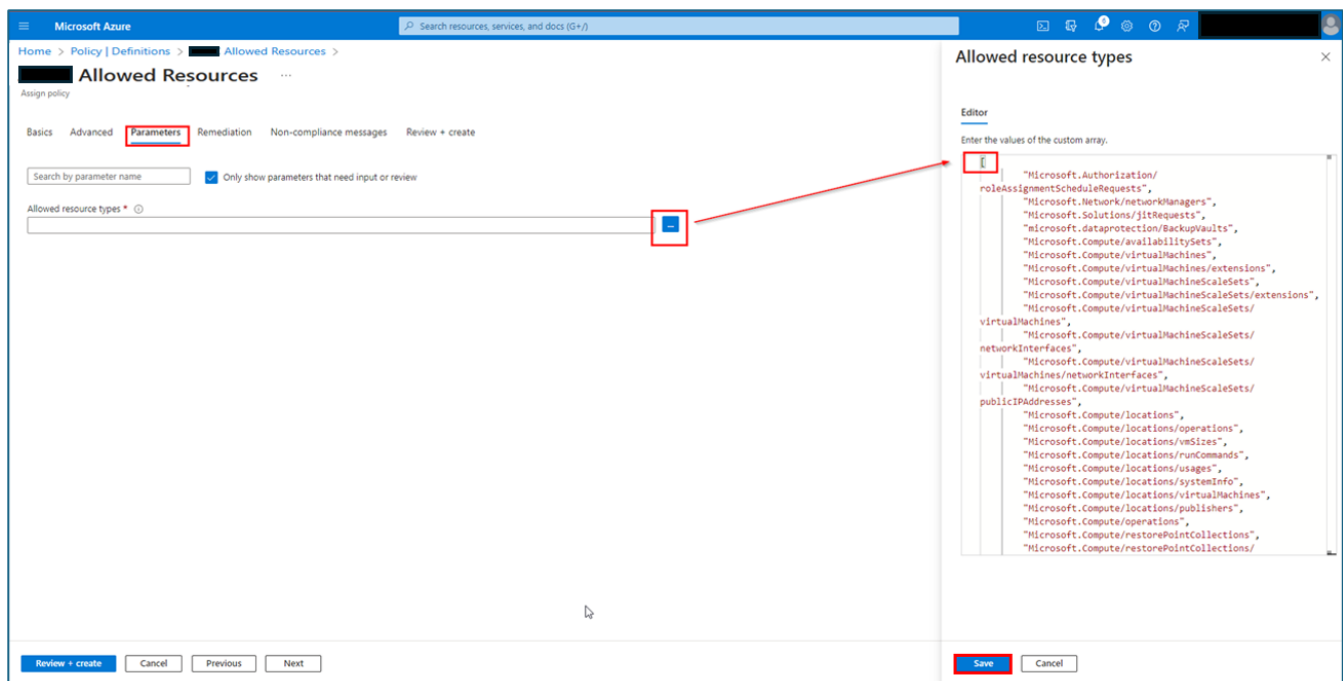
1. Navigate to **Azure Policy** via All Services or the search box
2. From Azure Policy service page, select **Assignments** from the Authoring section.
3. Under **Assignments**, select the existing assignment relating to Curated Portal assigned to the tenant Root Management Group
4. Select **Edit Assignment**
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

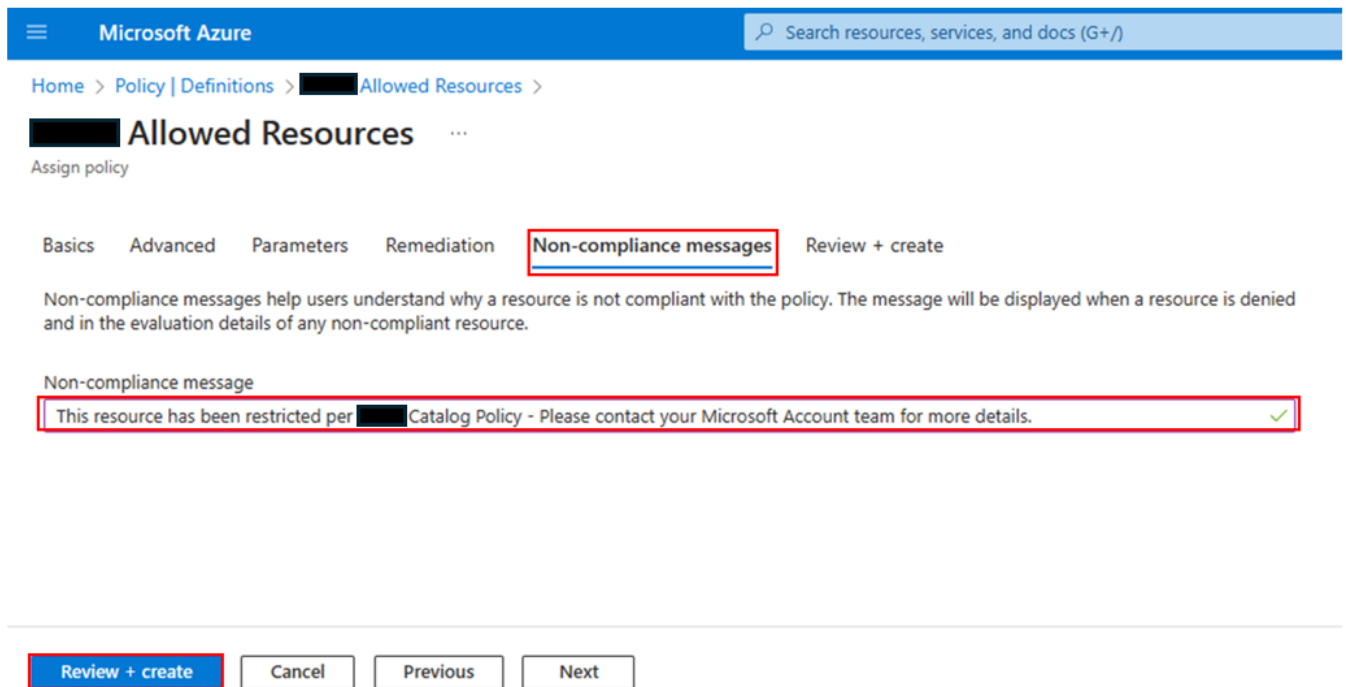
1. Obtain the updated files from the **Curated Portal file repository**.
2. **Open** the JSON file for the most recent **Curated Portal policy parameters** in a new text editor
Note: If necessary, remove the first two layers of curly braces "{" from the top of bottom so that the contents start and end 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

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

- 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.

Remove Ownership from Tenant Root Management Group

After verification of registration, remove ownership over the Tenant Root Management Group to reduce privilege footprint.

- Access the IAM blade for the Tenant Root Management Group in Step 5. Select the **User** and then **Remove** and **Yes** to remove the selected role assignment.

+ Add
Download role assignments
Edit columns
Refresh
Remove
Feedback

Check access
Role assignments
Roles
Deny assignments
Classic administrators

All
Job function (0)
Privileged (12)

Search by name or email
Type : All
Role : All
Scope : All scopes
Group by : Role

12 items (12 Users)

Name	Type	Role
Owner (6)		
<input type="checkbox"/> AC [redacted]	User	Owner ⓘ
<input type="checkbox"/> BJ [redacted]	User	Owner ⓘ
<input type="checkbox"/> DL [redacted]	User	Owner ⓘ
<input type="checkbox"/> TF [redacted]	User	Owner ⓘ
<input checked="" type="checkbox"/> TZ Tim Zimmerman	User	Owner ⓘ
<input type="checkbox"/> ZE [redacted]	User	Owner ⓘ
> User Access Administrator (6)		

Update existing Curated Portal policy (via Script)

A script is available in the Curated Portal file repository.