



Windows PowerShell Get-Help on Cmdlet 'Update-AzRoleManagementPolicy'

PS:\>Get-HELP Update-AzRoleManagementPolicy -Full

NAME

Update-AzRoleManagementPolicy

SYNOPSIS

Update a role management policy

SYNTAX

```
Update-AzRoleManagementPolicy -Name <String> -Scope <String> [-Description <String>] [-DisplayName <String>]
[-IsOrganizationDefault] [-Rule
    <IRoleManagementPolicyRule[]>] [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>]
[-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>]
[-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]
```

```
Update-AzRoleManagementPolicy -InputObject <IAuthorizationIdentity> [-Description <String>] [-DisplayName <String>]
[-IsOrganizationDefault] [-Rule
    <IRoleManagementPolicyRule[]>] [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>]
[-HttpPipelinePrepend <SendAsyncStep[]>] [-Proxy <Uri>]
[-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]
```

DESCRIPTION

Update a role management policy

PARAMETERS

-Name <String>

The name (guid) of the role management policy to upsert.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Scope <String>

The scope of the role management policy to upsert.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-InputObject <IAuthorizationIdentity>

Identity Parameter

To construct, see NOTES section for INPUTOBJECT properties and create a hash table.

Required? true

Position? named

Default value

Accept pipeline input? true (ByValue)

Accept wildcard characters? false

-Description <String>

The role management policy description.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DisplayName <String>

The role management policy display name.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-IsOrganizationDefault [<SwitchParameter>]

The role management policy is default policy.

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-Rule <IRoleManagementPolicyRule[]>

The rule applied to the policy.

To construct, see NOTES section for RULE properties and create a hash table.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-DefaultProfile <PSObject>

The DefaultProfile parameter is not functional.

Use the SubscriptionId parameter when available if executing the cmdlet against a different subscription.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Break [<SwitchParameter>]

Wait for .NET debugger to attach

Required? false

Position? named

Default value False

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelineAppend <SendAsyncStep[]>

SendAsync Pipeline Steps to be appended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-HttpPipelinePrepend <SendAsyncStep[]>

SendAsync Pipeline Steps to be prepended to the front of the pipeline

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-Proxy <Uri>

The URI for the proxy server to use

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyCredential <PSCredential>

Credentials for a proxy server to use for the remote call

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ProxyUseDefaultCredentials [<SwitchParameter>]

Use the default credentials for the proxy

Required? false

Position? named

Default value False

Accept pipeline input? false
Accept wildcard characters? false

-WhatIf [<SwitchParameter>]

Required? false
Position? named
Default value
Accept pipeline input? false
Accept wildcard characters? false

-Confirm [<SwitchParameter>]

Required? false
Position? named
Default value
Accept pipeline input? false
Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable, and OutVariable. For more information, see about_CommonParameters (<https://go.microsoft.com/fwlink/?LinkID=113216>).

INPUTS

Microsoft.Azure.PowerShell.Cmdlets.Resources.Authorization.Models.IAuthorizationIdentity

OUTPUTS

Microsoft.Azure.PowerShell.Cmdlets.Resources.Authorization.Models.Api20201001Preview.IRoleManagementPolicy

COMPLEX PARAMETER PROPERTIES

To create the parameters described below, construct a hash table containing the appropriate properties. For information on hash tables, run Get-Help about_Hash_Tables.

INPUTOBJECT <IAuthorizationIdentity>: Identity Parameter

[Id <String>]: Resource identity path

[RoleAssignmentScheduleInstanceName <String>]: The name (hash of schedule name + time) of the role assignment schedule to get.

[RoleAssignmentScheduleName <String>]: The name (guid) of the role assignment schedule to get.

[RoleAssignmentScheduleRequestName <String>]: The name of the role assignment to create. It can be any valid GUID.

[RoleEligibilityScheduleInstanceName <String>]: The name (hash of schedule name + time) of the role eligibility schedule to get.

[RoleEligibilityScheduleName <String>]: The name (guid) of the role eligibility schedule to get.

[RoleEligibilityScheduleRequestName <String>]: The name of the role eligibility to create. It can be any valid GUID.

[RoleManagementPolicyAssignmentName <String>]: The name of format {guid_guid} the role management policy assignment to get.

[RoleManagementPolicyName <String>]: The name (guid) of the role management policy to get.

[Scope <String>]: The scope of the role management policy.

RULE <IRoleManagementPolicyRule[]>: The rule applied to the policy.

RuleType <RoleManagementPolicyRuleType>: The type of rule

[Id <String>]: The id of the rule.

[TargetCaller <String>]: The caller of the setting.

[TargetEnforcedSetting <String[]>]: The list of enforced settings.

[TargetInheritableSetting <String[]>]: The list of inheritable settings.

[TargetLevel <String>]: The assignment level to which it is applied.

[TargetObject <String[]>]: The list of target objects.

[TargetOperation <String[]>]: The type of operation.

----- EXAMPLE 1 -----

```
PS C:\>$scope = "/subscriptions/38ab2ccc-3747-4567-b36b-9478f5602f0d/"
```

```
$expirationRule = [RoleManagementPolicyExpirationRule]@{  
    isExpirationRequired = "false";  
    maximumDuration = "P180D";  
    id = "Expiration_Admin_Eligibility";  
    ruleType = [RoleManagementPolicyRuleType]("RoleManagementPolicyExpirationRule");  
    targetCaller = "Admin";  
    targetOperation = @('All');  
    targetLevel = "Eligibility";  
    targetObject = $null;  
    targetInheritableSetting = $null;  
    targetEnforcedSetting = $null;  
}  
$rules = [IRoleManagementPolicyRule[]]@($expirationRule)
```

```
Update-AzRoleManagementPolicy -Scope $scope -Name "33b520ea-3544-4abc-8565-3588deb8e68e" -Rule $rules
```

----- EXAMPLE 2 -----

```
PS C:\>$scope = "/subscriptions/38ab2ccc-3747-4567-b36b-9478f5602f0d/"
```

```
$expirationRule = [RoleManagementPolicyExpirationRule]@{  
    isExpirationRequired = "false";  
    maximumDuration = "P180D";  
    id = "Expiration_Admin_Eligibility";  
    ruleType = [RoleManagementPolicyRuleType]("RoleManagementPolicyExpirationRule");
```



```

        targetCaller = "Admin";
        targetOperation = @('All');
        targetLevel = "Eligibility";
        targetObject = $null;
        targetInheritableSetting = $null;
        targetEnforcedSetting = $null;
    }

$notificationRule = [RoleManagementPolicyNotificationRule]@{
    notificationType = "Email";
    recipientType = "Approver";
    isDefaultRecipientsEnabled = "false";
    notificationLevel = "Critical";
    notificationRecipient = $null;
    id = "Notification_Approver_Admin_Eligibility";
    ruleType = [RoleManagementPolicyRuleType]("RoleManagementPolicyNotificationRule");
    targetCaller = "Admin";
    targetOperation = @('All');
    targetLevel = "Eligibility";
    targetObject = $null;
    targetInheritableSetting = $null;
    targetEnforcedSetting = $null;
}

$rules = [IRoleManagementPolicyRule[]]@($expirationRule, $notificationRule)

Update-AzRoleManagementPolicy -Scope $scope -Name "33b520ea-3544-4abc-8565-3588deb8e68e" -Rule $rules

```

RELATED LINKS

<https://learn.microsoft.com/powershell/module/az.resources/update-azrolemanagementpolicy>

