



Windows PowerShell Get-Help on Cmdlet 'Remove-AzSentinelIncident'

PS:\>Get-HELP Remove-AzSentinelIncident -Full

NAME

Remove-AzSentinelIncident

SYNOPSIS

Delete the incident.

SYNTAX

Remove-AzSentinelIncident -Id <String> -ResourceGroupName <String> [-SubscriptionId <String>] -WorkspaceName <String> [-DefaultProfile <PSObject>] [-Break]

[-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend <SendAsyncStep[]>] [-PassThru] [-Proxy <Uri>] [-ProxyCredential <PSCredential>]

[-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

Remove-AzSentinelIncident -InputObject <ISecurityInsightsIdentity> [-DefaultProfile <PSObject>] [-Break] [-HttpPipelineAppend <SendAsyncStep[]>] [-HttpPipelinePrepend

<SendAsyncStep[]>] [-PassThru] [-Proxy <Uri>] [-ProxyCredential <PSCredential>] [-ProxyUseDefaultCredentials] [-WhatIf] [-Confirm] [<CommonParameters>]

DESCRIPTION

Delete the incident.

PARAMETERS

-Id <String>

Incident ID

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-ResourceGroupName <String>

The name of the resource group.

The name is case insensitive.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-SubscriptionId <String>

The ID of the target subscription.

Required? false

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-WorkspaceName <String>

The name of the workspace.

Required? true

Position? named

Default value

Accept pipeline input? false

Accept wildcard characters? false

-InputObject <ISecurityInsightsIdentity>

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

-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

-PassThru [<SwitchParameter>]

Returns true when the command succeeds

Required? false
Position? named
Default value False
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.SecurityInsights.Models.ISecurityInsightsIdentity

OUTPUTS

System.Boolean

NOTES

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.

[ActionId <String>]: Action ID

[AlertRuleTemplateId <String>]: Alert rule template ID

[AutomationRuleId <String>]: Automation rule ID

[BookmarkId <String>]: Bookmark ID

[ConsentId <String>]: consent ID

[DataConnectorId <String>]: Connector ID

[EntityId <String>]: entity ID

[EntityQueryId <String>]: entity query ID

[EntityQueryTemplateId <String>]: entity query template ID

[Id <String>]: Resource identity path

[IncidentCommentId <String>]: Incident comment ID

[IncidentId <String>]: Incident ID

[MetadataName <String>]: The Metadata name.

[Name <String>]: Threat intelligence indicator name field.

[RelationName <String>]: Relation Name

[ResourceGroupName <String>]: The name of the resource group. The name is case insensitive.

[RuleId <String>]: Alert rule ID

[SentinelOnboardingStateName <String>]: The Sentinel onboarding state name. Supports - default

[SettingsName <String>]: The setting name. Supports - Anomalies, EyesOn, EntityAnalytics, Ueba

[SourceControlId <String>]: Source control Id

[SubscriptionId <String>]: The ID of the target subscription.

[WorkspaceName <String>]: The name of the workspace.

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

```
Remove-AzSentinelIncident -ResourceGroupName "myResourceGroup" -WorkspaceName "myWorkspaceName" -Id
<IncidentId>
```

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

```
$myIncident = Get-AzSentinelIncident -ResourceGroupName "myResourceGroup" -WorkspaceName  
"myWorkspaceName" -Id <IncidentId> | Where-Object {$_.Number -eq "780"}
```

RELATED LINKS

<https://learn.microsoft.com/powershell/module/az.securityinsights/remove-azsentinelincident>