

Microsoft Sentinel playbook

A playbook is a collection of remediation actions that can be run from Azure Sentinel as a routine. A playbook can help automate and orchestrate your threat response ; it can be run manually or set to run automatically in response to specific alerts or incidents, when triggered by an analytics rule or an automation rule, respectively.

Security playbooks in Microsoft Sentinel are based on Azure logic apps. Which means that you get all the power customizability and built in templates of logic apps. Each playbook is created for the specific subscription.

For example if you are worried about malicious attackers accessing your network resources, you can set an alert that looks for malicious ip addresses accessing your network then we can create a playbook

The following list describes just a few example tasks, business processes, and workloads that you can automate using the Azure Logic Apps service:

- Schedule and send email notifications using Office 365 when a specific event happens, for example, a new file is uploaded.
- Route and process customer orders across on-premises systems and cloud services.
- Move uploaded files from an SFTP or FTP server to Azure Storage.
- Monitor tweets, analyze the sentiment, and create alerts or tasks for items that need review.

Azure services



Create a resource



Azure Sentinel



Azure AD Privileged...



Azure Information...



Virtual machines



Log Analytics workspaces



Logic Apps



Monitor



Azure Monitor Private Link...



More service

Home > Azure Sentinel workspaces

Azure Sentinel workspaces

Microsoft

+ Add Refresh Multiple Workspace View

Add

Subscriptions: 1 of 2 selected - Don't see a subscription? [Open Directory](#) + [Subscription settings](#)

Filter by name

Insight Security Operations Center - Beta

All resource groups

All locations

Workspace

↑↓ ResourceGroup

↑↓ Location

↑↓ Subscription

↑↓ Directory

↑↓ Additional Info ↑↓

Choose a workspace to add to Azure Sentinel

 Search workspaces

 Create a new workspace

Create Log Analytics workspace

Basics Pricing tier Tags Review + Create

i A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#) ✕

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

MSDN

Resource group * ⓘ

ClassDemo

[Create new](#)

Instance details

Name * ⓘ

ClassDemoWorkspace

Region * ⓘ

(US) East US

Review + Create

Create Log Analytics workspace

✓ Validation passed

Basics Pricing tier Tags Review + Create

 **Log Analytics workspace**
by Microsoft

Basics

Subscription

MSDN

Resource group

ClassDemo

Name

ClassDemoWorkspace

Region

East US

Pricing

Pricing tier

Pay-as-you-go (Per GB 2018)

Tags

(none)

 **Create**

Choose a workspace to add to Azure Sentinel

Search workspaces

+ Create a new workspace

 ClassDemoWorkspace
East US

Add Azure Sentinel

Search (Ctrl+/)

<< + Create **3.** Refresh

Guides & Feedback

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE

- Automation rule (Preview)
- Playbook with incident trigger
- Playbook with alert trigger
- Blank playbook **4.**

0 Enabled rules 0 Enabled playbooks

Active playbooks

2. Playbook templates (Preview)

Search by name

Trigger : All

Logic Apps Connectors : All

More (2)

Name ↑↓	Trigger ↑↓	Logic Apps Connec...	Entities	Tags
Add IP Entity To Named Location	Microsoft Senti...	Microsoft Sentinel	IP	Remediation
Block AAD user - Alert	Microsoft Senti...	Azure AD +2 ⓘ	Account	Remediation
Block AAD user - Incident	Microsoft Senti...	Azure AD +2 ⓘ	Account	Remediation
Block IP - Azure Firewall IP gro...	Microsoft Senti...	AzureFirewall... +3 ⓘ	IP	Remediation
Block IP - Cisco ASA	Microsoft Senti...	CiscoASACon... +2 ⓘ	IP	Remediation
Block IP - Cisco Firepower	Microsoft Senti...	CiscoFirepow... +1 ⓘ	IP	Remediation
Block IP - Palo Alto PAN-OS	Microsoft Senti...	PAN-OSCusto... +2 ⓘ	IP	Remediation

< Previous Page 1 of 2 Next >

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Configuration

- Data connectors
- Analytics
- Watchlist
- Automation** **1.**
- Settings

Logic App

* Basics Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details MSDN

Logic App name *

Select the location Region Integration Service Environment

Location *

Associate with integration service environment ⓘ

Integration service environment

Enable log analytics ⓘ

Log Analytics workspace *





[Home](#) >

Logic App

* Basics Tags Review + create

Basics

Subscription

Resource group

Logic App name

Location

MSDN

!ClassDemo

ClassDemoWorkspace

East US

Tags



Create

< Previous: Tags

Next: Review + create >

Download a template for automation

Logic Apps Designer

Save Discard Run Trigger Designer Code view Parameters Templates Connectors Help Info

Search for RSS

trigger

An RSS feed is a file that contains summary of updates from a website often in the form of a list of articles with links. RSS stands for **Really Simple Syndication**, and it offers an easy way to stay up to date on new content from websites you care

Search for RSS

For You All Built-in Standard Enterprise Custom

RSS Cloudmersive Barcode

Triggers Actions

When a feed item is published
RSS

Don't see what you need?
Help us decide which connectors and triggers to add next with [UserVoice](#)

Click on the RSS trigger

Logic Apps Designer ...

Type in the url and also type in how often you want to check for items

When a feed item is published

*The RSS feed URL

Chosen property will be used to determine

How often do you want to check for items?

Connected to RSS. [Change connection.](#)

+ New step

Collapse the trigger's details for now by clicking inside its title bar.

Click on save to save your logic app, which instantly goes live in the Azure portal

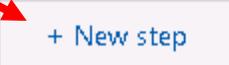
Save logic app completed
Logic app: logicdemoclass was saved successfully

Home > Microsoft.EmptyWorkflow > logicdemoclass >

Logic Apps Designer ...

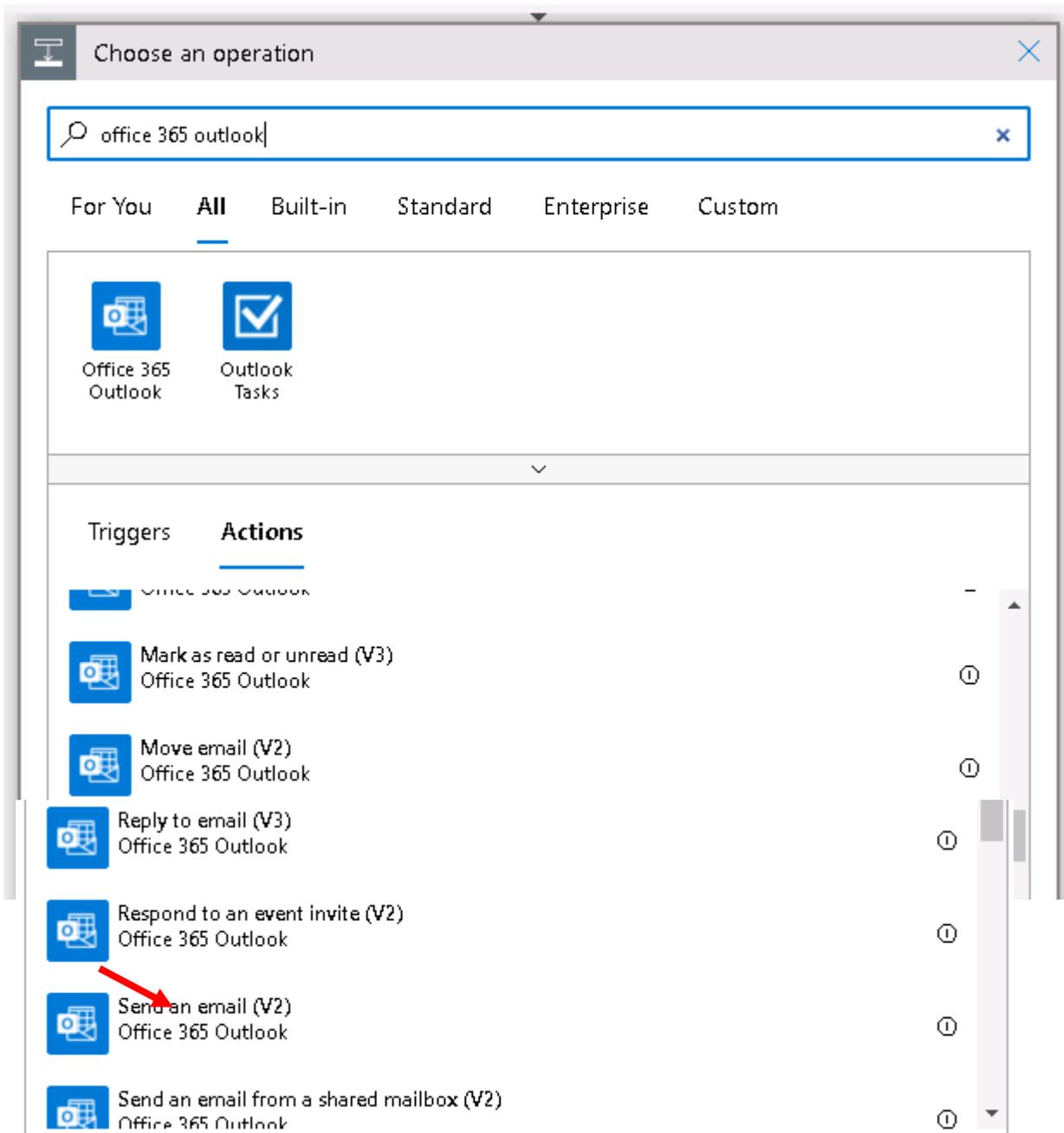
 Save  Discard  Run Trigger  Designer  Code view  Parameters  Templates  Connectors  Help  Info

 When a feed item is published ...



Click on new step

Type office 365 outlook to search for the action you Need. Scroll down and select “Send and email (V2) Office 365 Outlook



Logic Apps Designer ...

Save Discard Run Trigger Designer Code view Parameters Templates Connectors Help Info

The screenshot shows the Logic Apps Designer interface. At the top, there is a menu bar with icons for Save, Discard, Run Trigger, Designer, Code view, Parameters, Templates, Connectors, Help, and Info. Below the menu bar, the workflow canvas is visible. It contains two steps: a trigger step labeled "When a feed item is published" and an action step labeled "Office 365 Outlook". An arrow points from the trigger step to the action step. The "Office 365 Outlook" step is currently in a "Sign in" state, with the text "Sign in to create a connection to Office 365 Outlook." and a blue "Sign in" button. At the bottom right of the canvas, there is a "+ New step" button.

If your selected email service prompts you to sign in and authenticate your identity, complete that step now.

Insert fields using the dynamic data content list

Logic Apps Designer



2

Save Discard Run Trigger Designer Code view Parameters Templates Connectors Help Info

Add dynamic content from the apps and connectors used in this flow.

When a feed item is published

Dynamic content Expression

link

Send an email (V2)

When a feed item is published

*To admin@M365x62464392.onmicrosoft.com

Primary feed link
Primary feed link

*Subject New Rss Item: Feed title

Feed links Item

*Body Font 12 B I U

Feed links
Feed links

Title: Feed title

Date Published: Feed published on

Link: Primary feed link

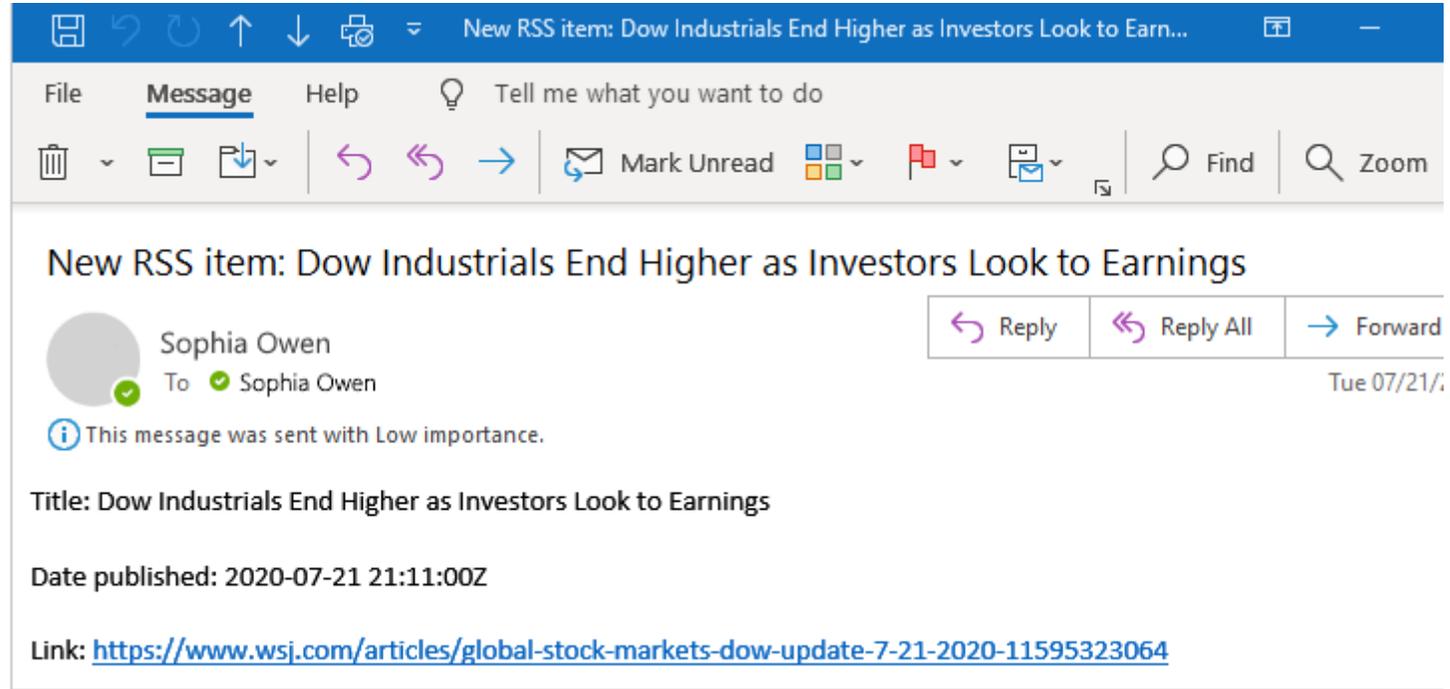
Add dynamic content

Add new parameter

Connected to admin@M365x62464392.onmicrosoft.com. Change connection.

1

Example



The screenshot shows an Outlook message window. At the top, a blue title bar contains the text "New RSS item: Dow Industrials End Higher as Investors Look to Earn...". Below this is a ribbon with tabs for "File", "Message", and "Help". The "Message" tab is active, showing a search bar with the text "Tell me what you want to do" and various icons for actions like "Mark Unread", "Find", and "Zoom". The main content area displays the subject "New RSS item: Dow Industrials End Higher as Investors Look to Earnings". The sender is identified as "Sophia Owen" with a profile picture and a green checkmark. The recipient is "To: Sophia Owen" with a green checkmark. Action buttons for "Reply", "Reply All", and "Forward" are visible. A note states "This message was sent with Low importance." The message title is "Dow Industrials End Higher as Investors Look to Earnings", the date published is "2020-07-21 21:11:00Z", and the link is "https://www.wsj.com/articles/global-stock-markets-dow-update-7-21-2020-11595323064".

New RSS item: Dow Industrials End Higher as Investors Look to Earn...

File Message Help Tell me what you want to do

Mark Unread Find Zoom

New RSS item: Dow Industrials End Higher as Investors Look to Earnings

Sophia Owen
To: Sophia Owen

Reply Reply All Forward

Tue 07/21/20

This message was sent with Low importance.

Title: Dow Industrials End Higher as Investors Look to Earnings

Date published: 2020-07-21 21:11:00Z

Link: <https://www.wsj.com/articles/global-stock-markets-dow-update-7-21-2020-11595323064>

Example of Rss Item

 Reply all |   Delete  Junk  Block ...

New Rss Item: SEC Proposes Rules for More Disclosure from Short Sellers

 This message was sent with Low importance



MOD Administrator

Fri 2/25/2022 8:26 AM

To: MOD Administrator



Title: SEC Proposes Rules for More Disclosure from Short Sellers

Date Published: 2022-02-25 16:21:00Z

Link: https://www.wsj.com/articles/sec-proposes-rules-for-more-disclosure-from-short-sellers-11645804875?mod=rss_markets_main

[Reply](#) | [Forward](#)