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

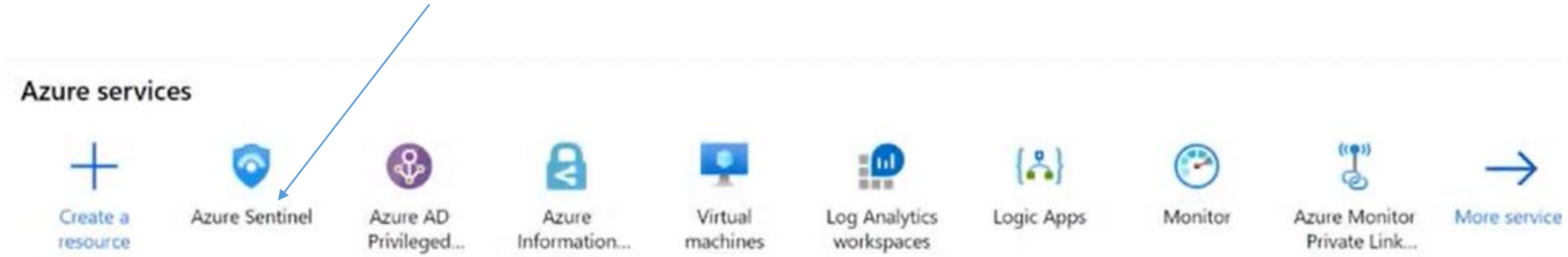
The following list describes just a few example tasks, business processes, and workloads that you can automate using the Azure Logic Apps service:

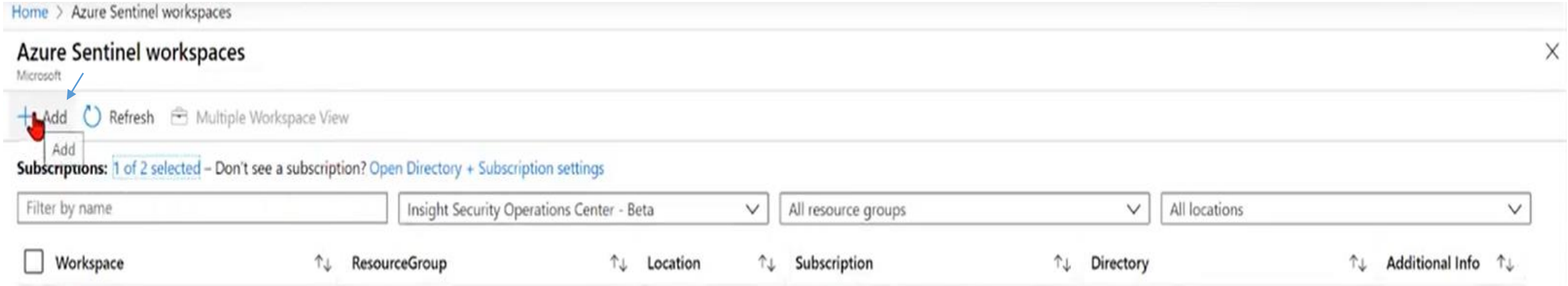
•Schedule and send email notifications using Office 365 when a specific event happens, for example, a new file is uploaded.

•Route and process customer orders across on-premises systems and cloud services.

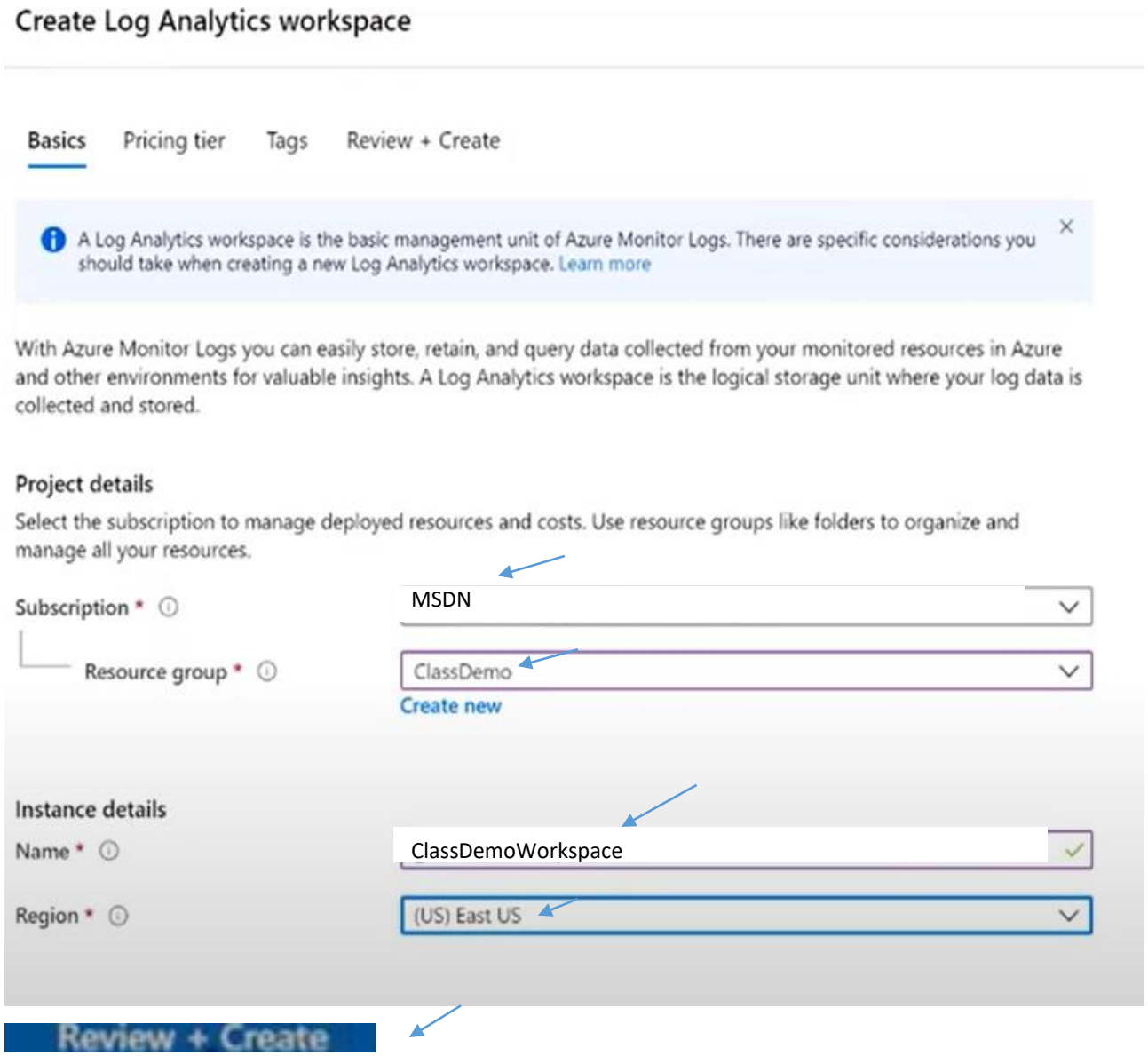
•Move uploaded files from an SFTP or FTP server to Azure Storage.

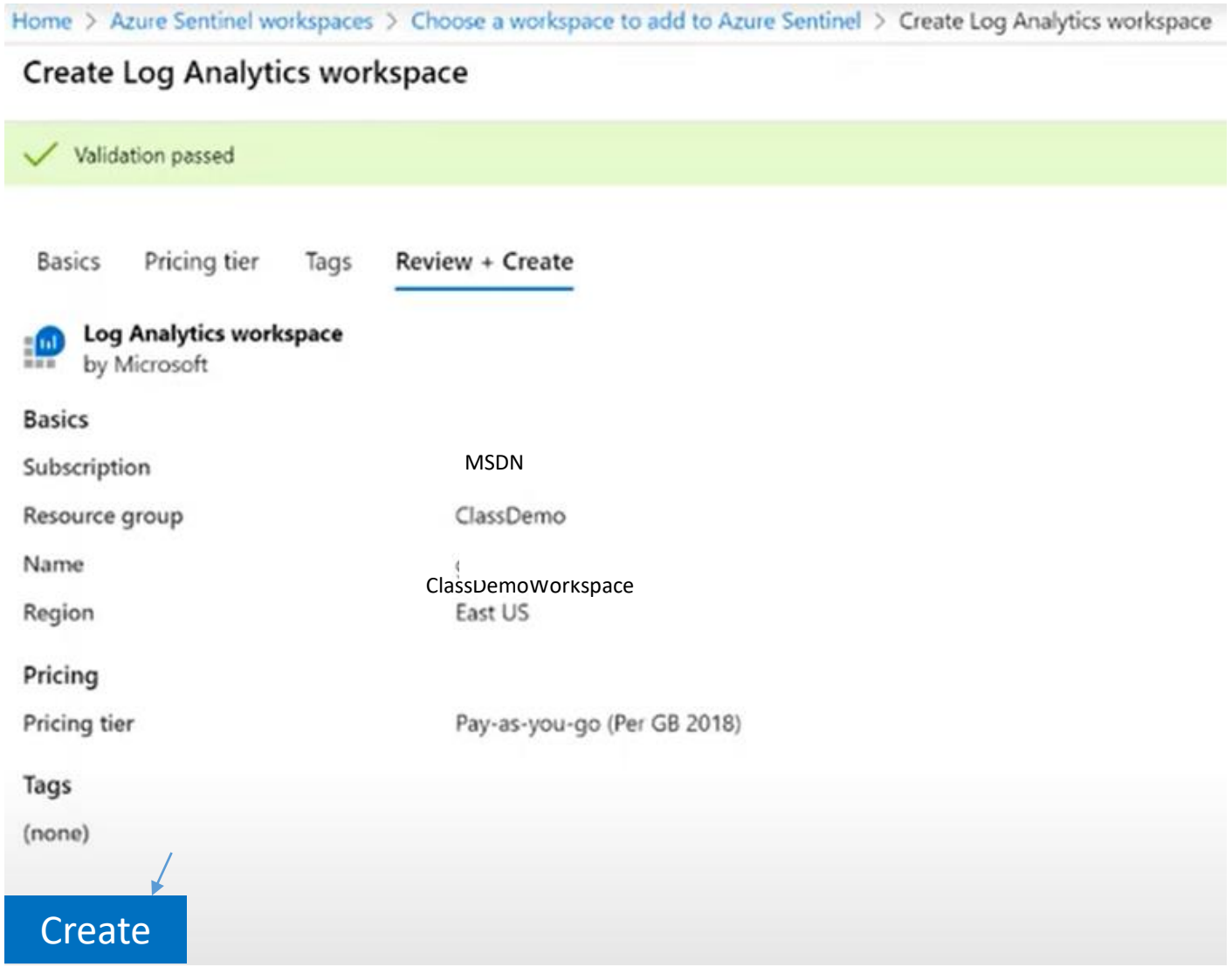
•Monitor tweets, analyze the sentiment, and create alerts or tasks for items that need review.

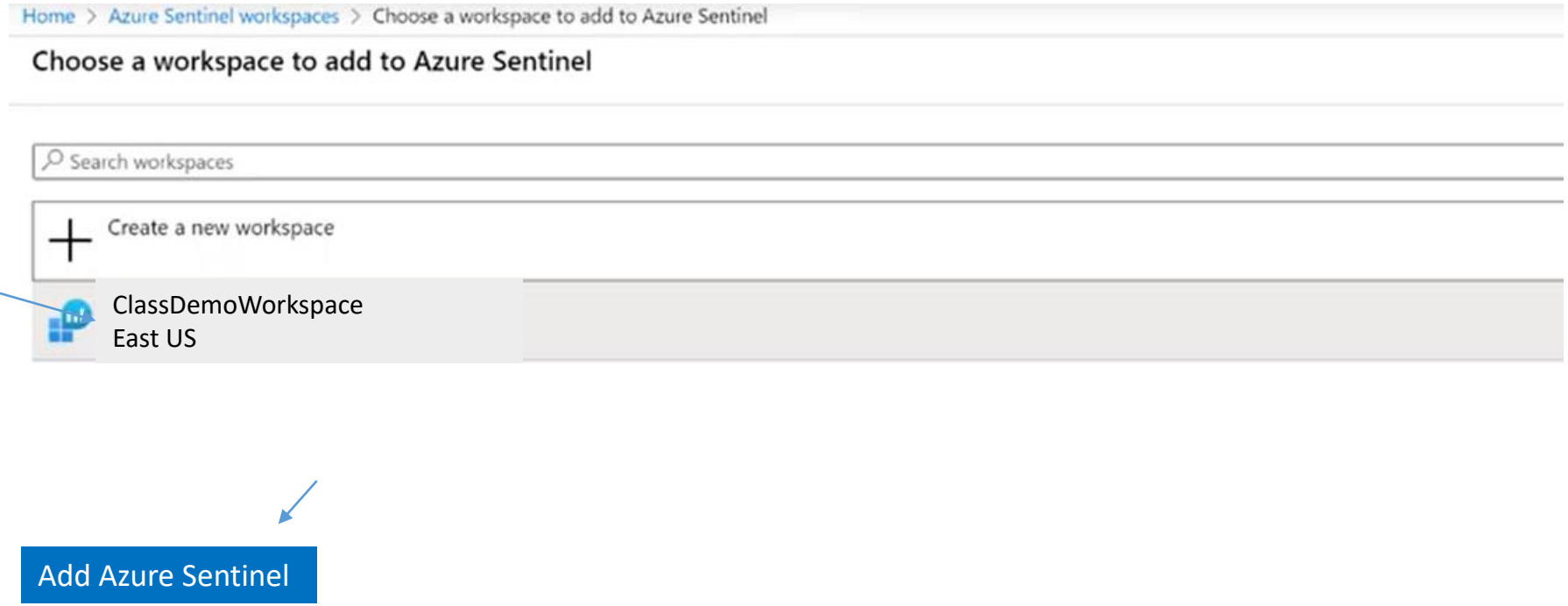

Azure services
Create a resource
Azure Sentinel
Azure AD Privileged...
Azure Information...
Virtual machines
Log Analytics workspaces
Logic Apps
Monitor
Azure Monitor Private Link...
More service


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

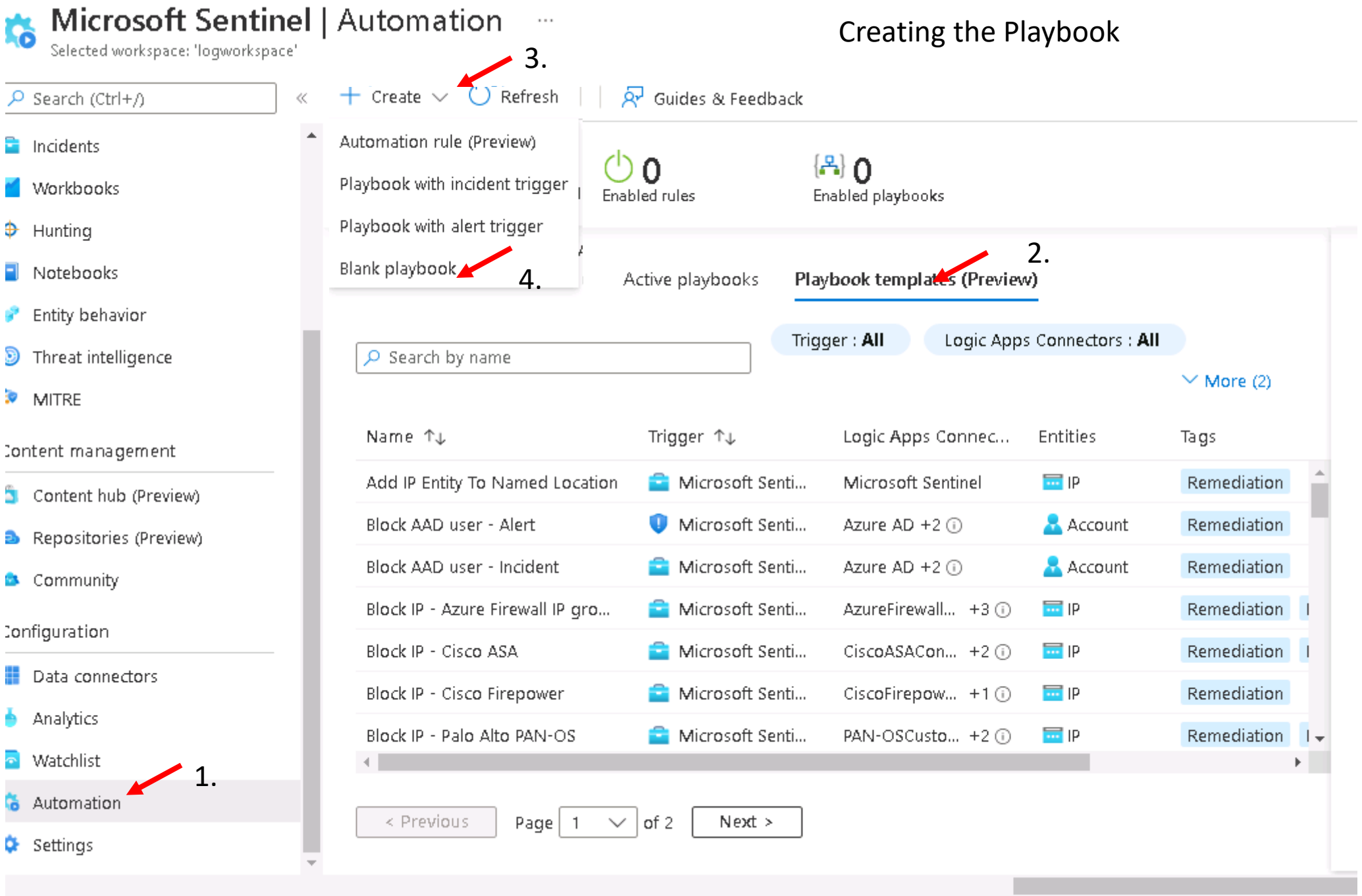

Home > Azure Sentinel workspaces > Choose a workspace to add to Azure Sentinel
Choose a workspace to add to Azure Sentinel
Search workspaces
Create a new workspace

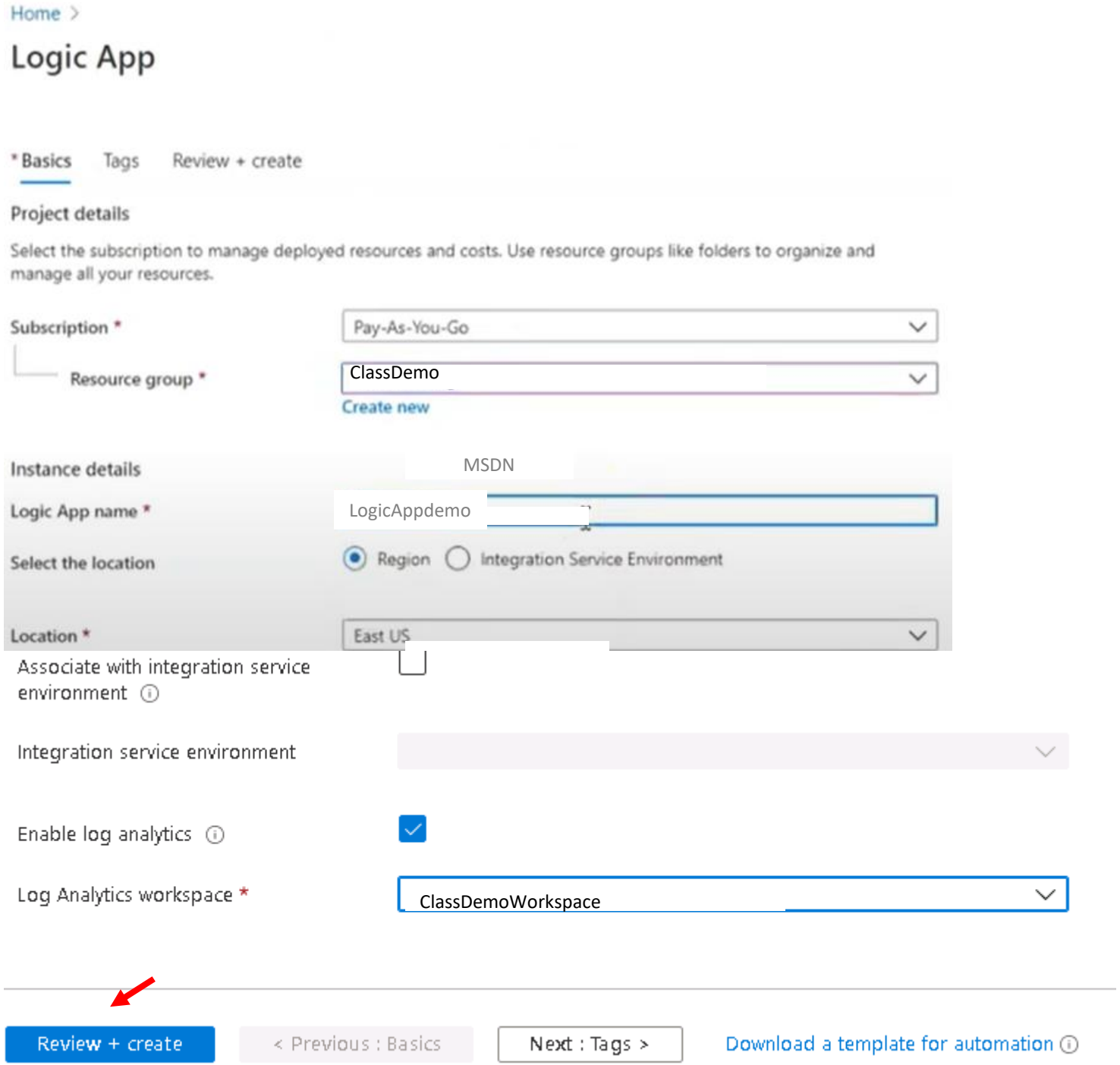

Create Log Analytics workspace
Basics
Pricing tier
Tags
Review + Create
A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more
With Azure Monitor Logs you can easily store, 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

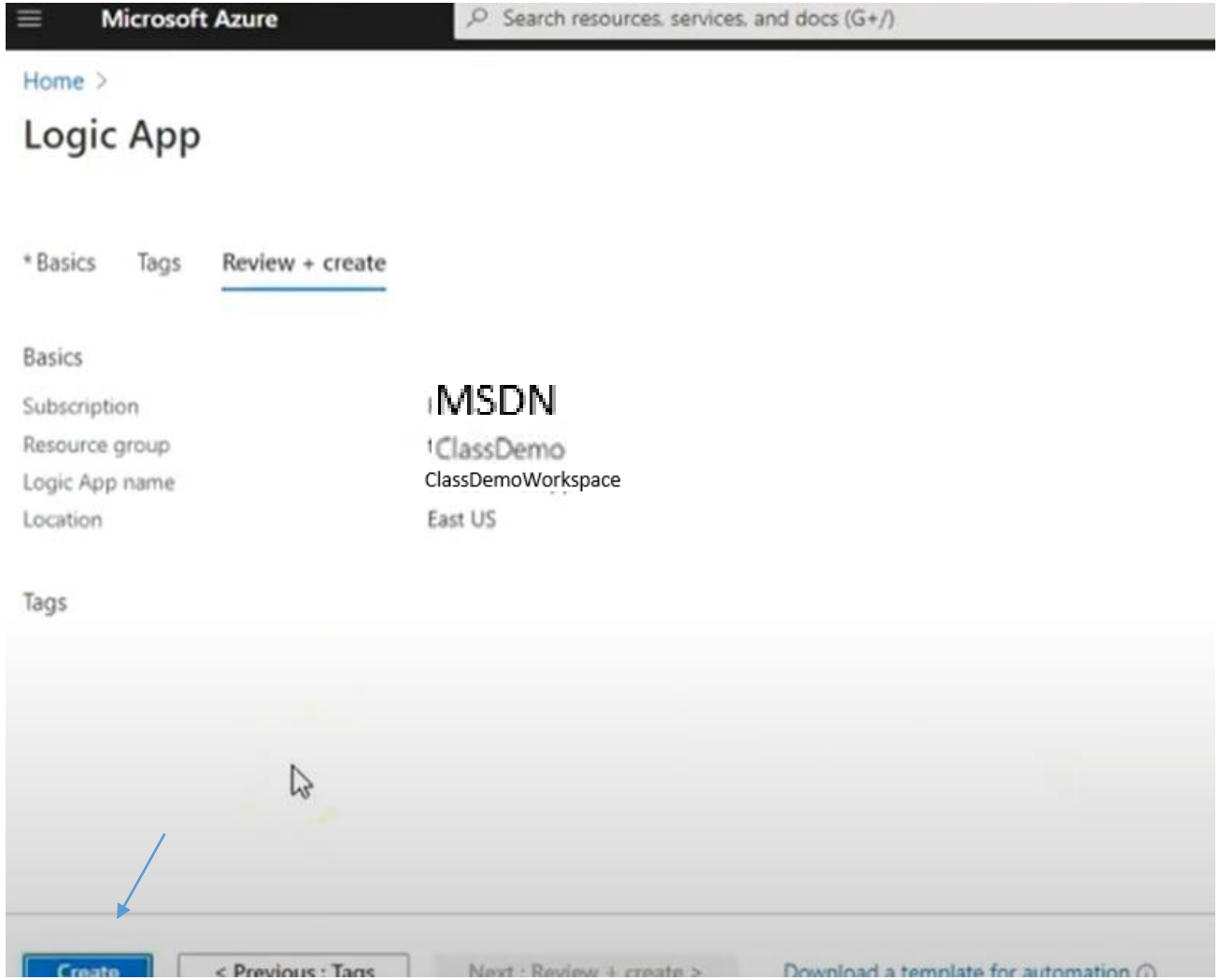

Home > Azure Sentinel workspaces > Choose a workspace to add to Azure Sentinel > Create Log Analytics workspace
Create Log Analytics workspace
Validation passed
Basics
Pricing tier
Tags
Review + Create
Log Analytics workspace
by Microsoft
Basics
Subscription
MSDN
Resource group
ClassDemo
Name
ClassDemoWorkspace
Region
East US
Pricing
Pricing tier
Pay-as-you-go (Per GB 2018)
Tags
(none)
Create


Home > Azure Sentinel workspaces > Choose a workspace to add to Azure Sentinel
Choose a workspace to add to Azure Sentinel
Search workspaces
Create a new workspace
ClassDemoWorkspace
East US
Add Azure Sentinel

Creating the Playbook




Home
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 *
Pay-As-You-Go
Resource group *
ClassDemo
Create new
Instance details
MSDN
Logic App name *
LogicAppdemo
Select the location
Region
Integration Service Environment
Location *
East US
Associate with integration service environment
Integration service environment
Enable log analytics
Log Analytics workspace *
ClassDemoWorkspace
Review + create
< Previous : Basics
Next : Tags >
Download a template for automation

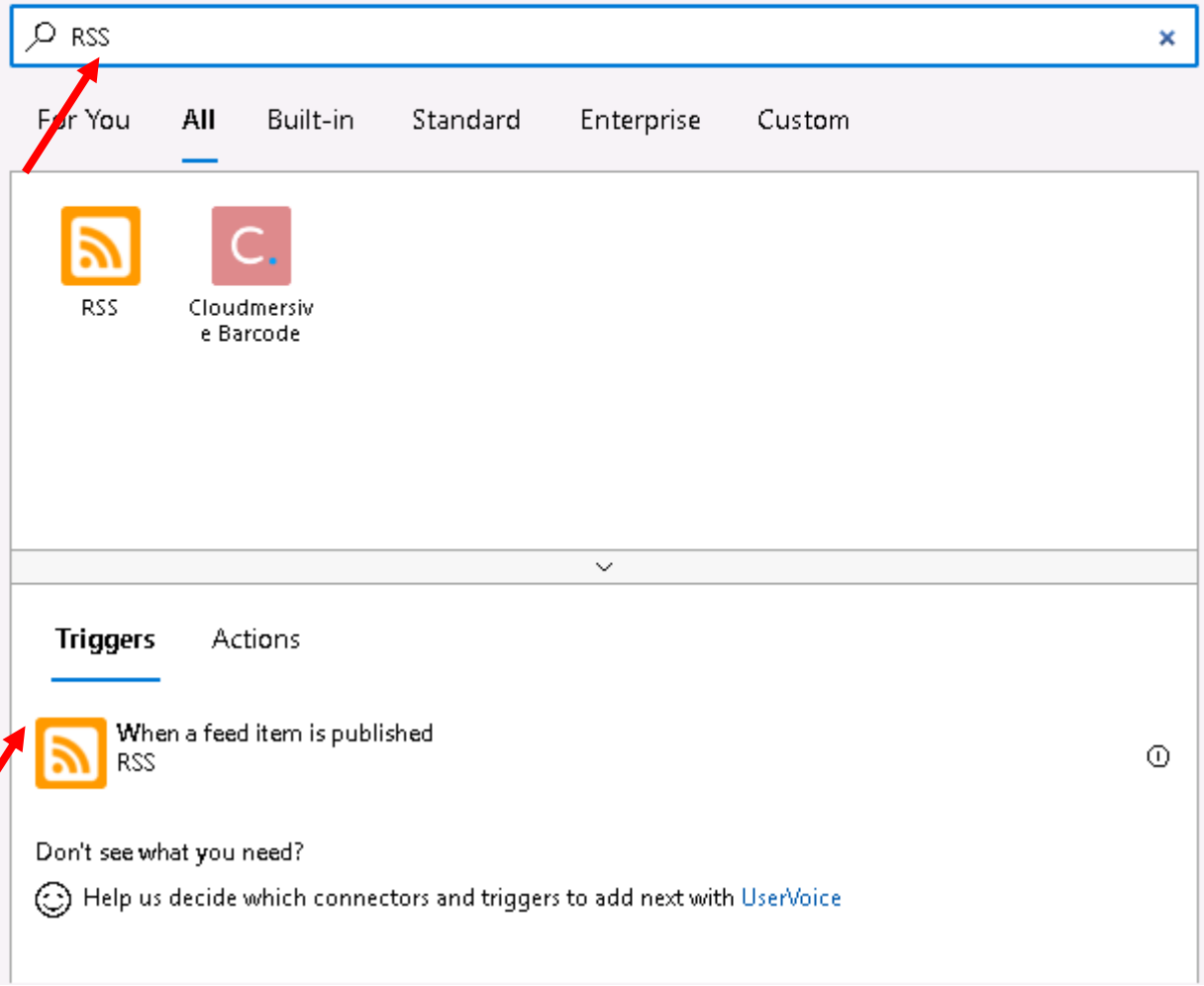

Microsoft Azure
Search resources, services, and docs (G+/)
Home >
Logic App
* Basics
Tags
Review + create
Basics
Subscription
MSDN
Resource group
ClassDemo
Logic App name
ClassDemoWorkspace
Location
East US
Tags
Create
< Previous : Tags
Next : Review + create >
Download a template for automation

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 webs often in the form of a list of article with links. RSS stands for **Really Simple Syndication**, and it offers a easy way to stay up to date on new content from websites you care



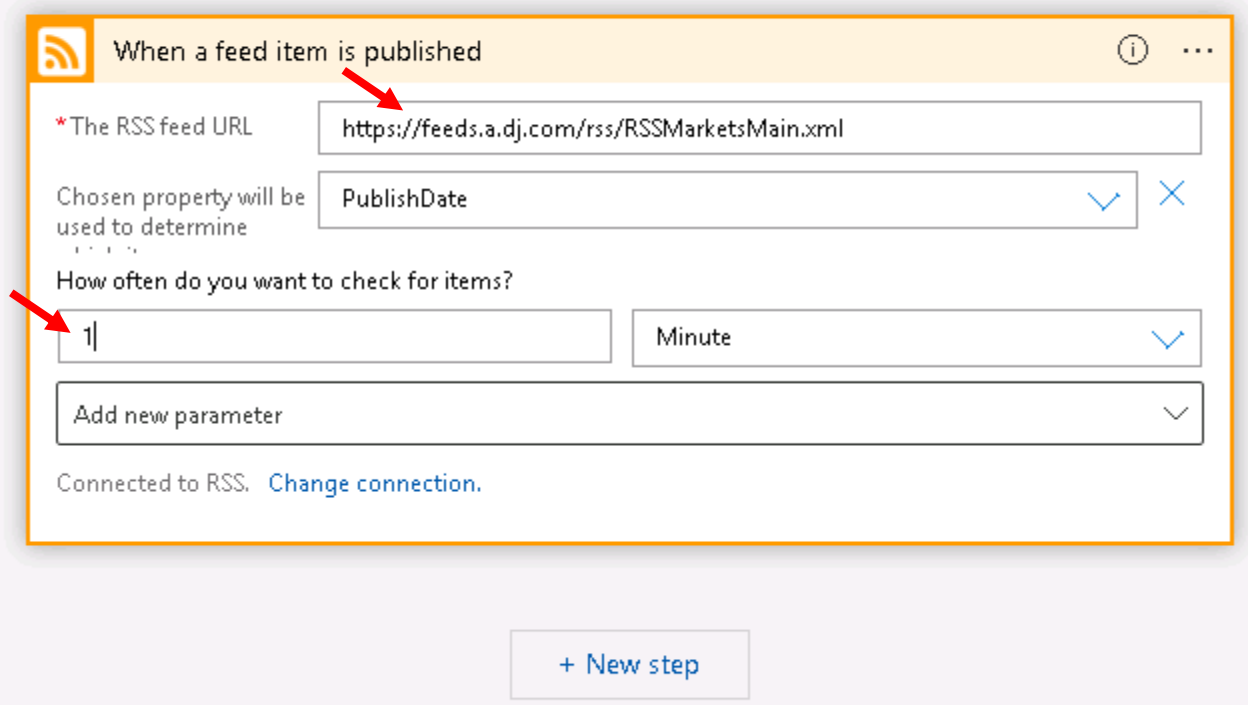
Click on the RSS trigger

Home > Microsoft.EmptyWorkflow > logicdemoclass >

Logic Apps Designer ...

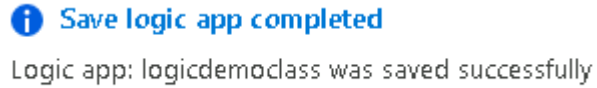
Save | Discard | Run Trigger | Designer | Code view | Parameters | Templates | Connectors | Help | Info

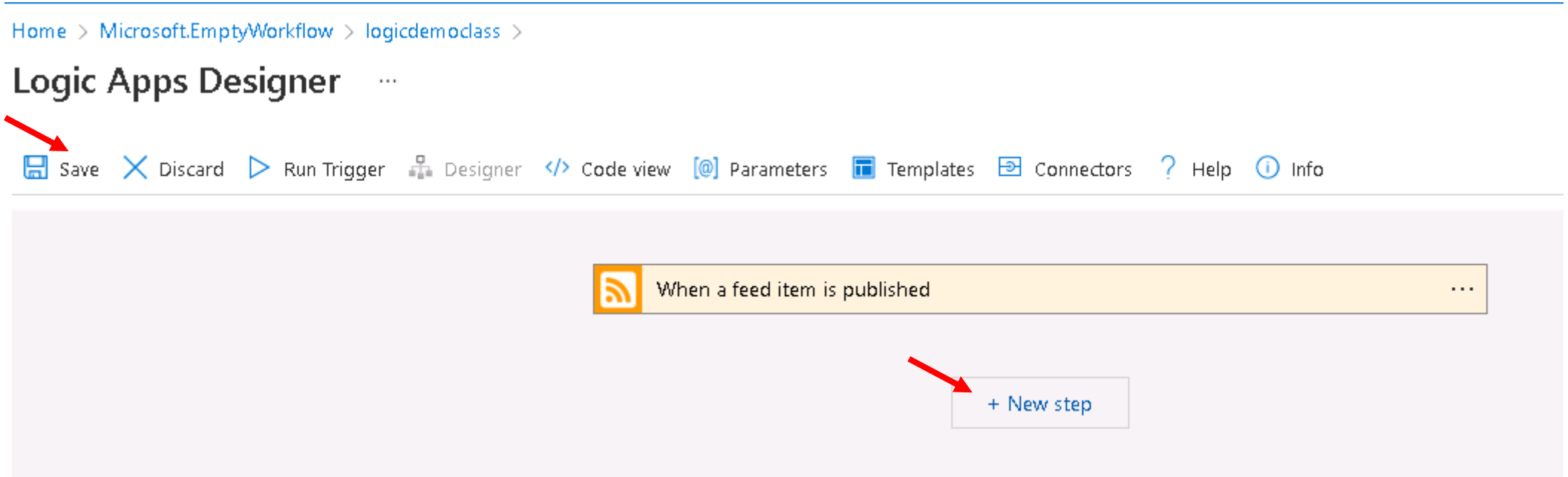
Type in the url and also type in how often you want to check for items



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

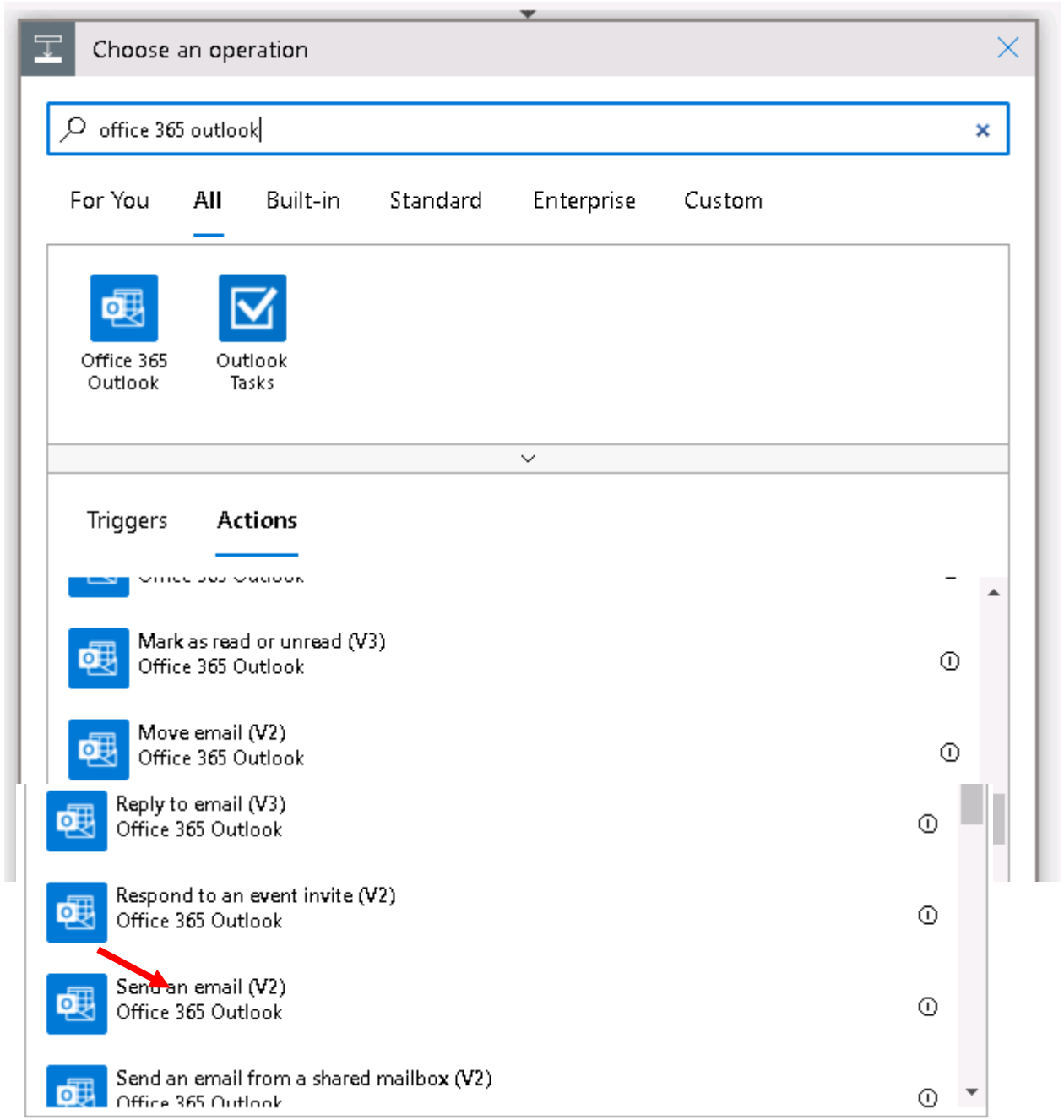
Click on save to save your logic app, which instantly goes live in the Azure portal

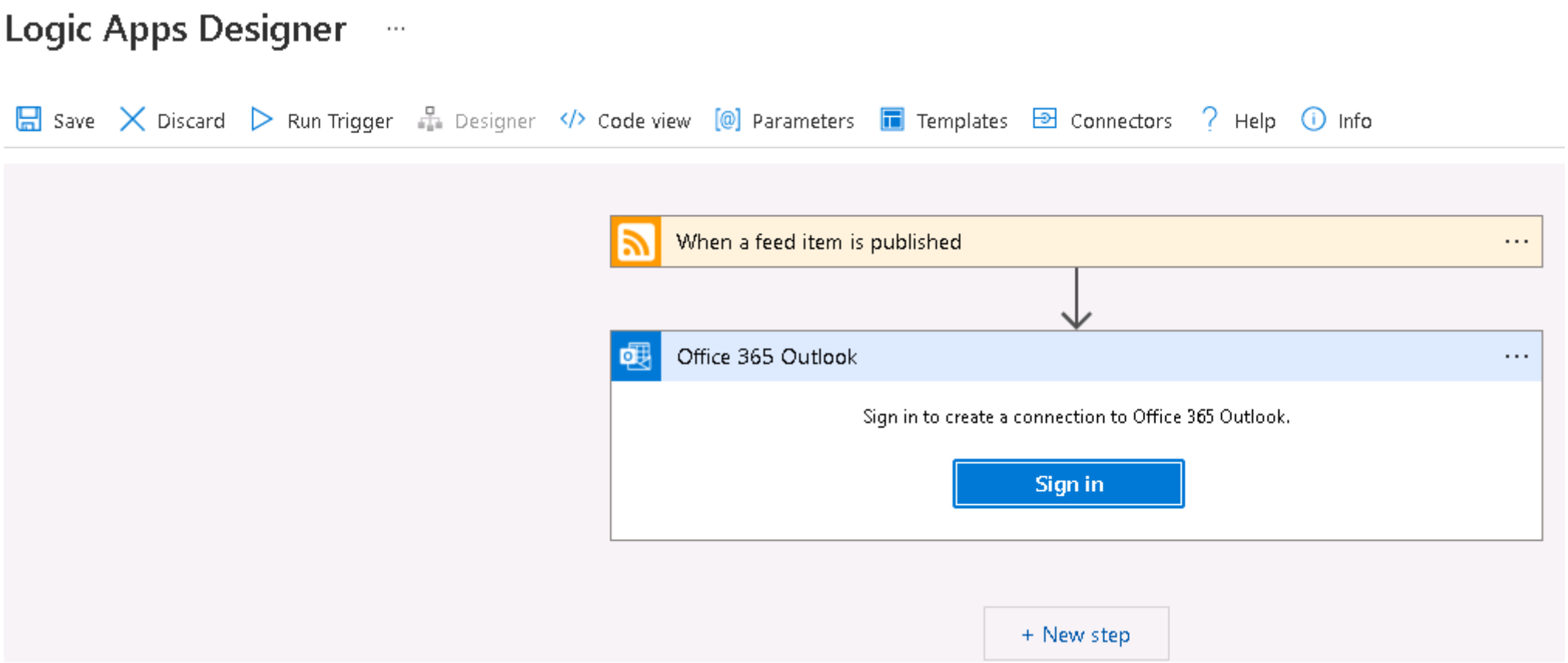




Click on new step

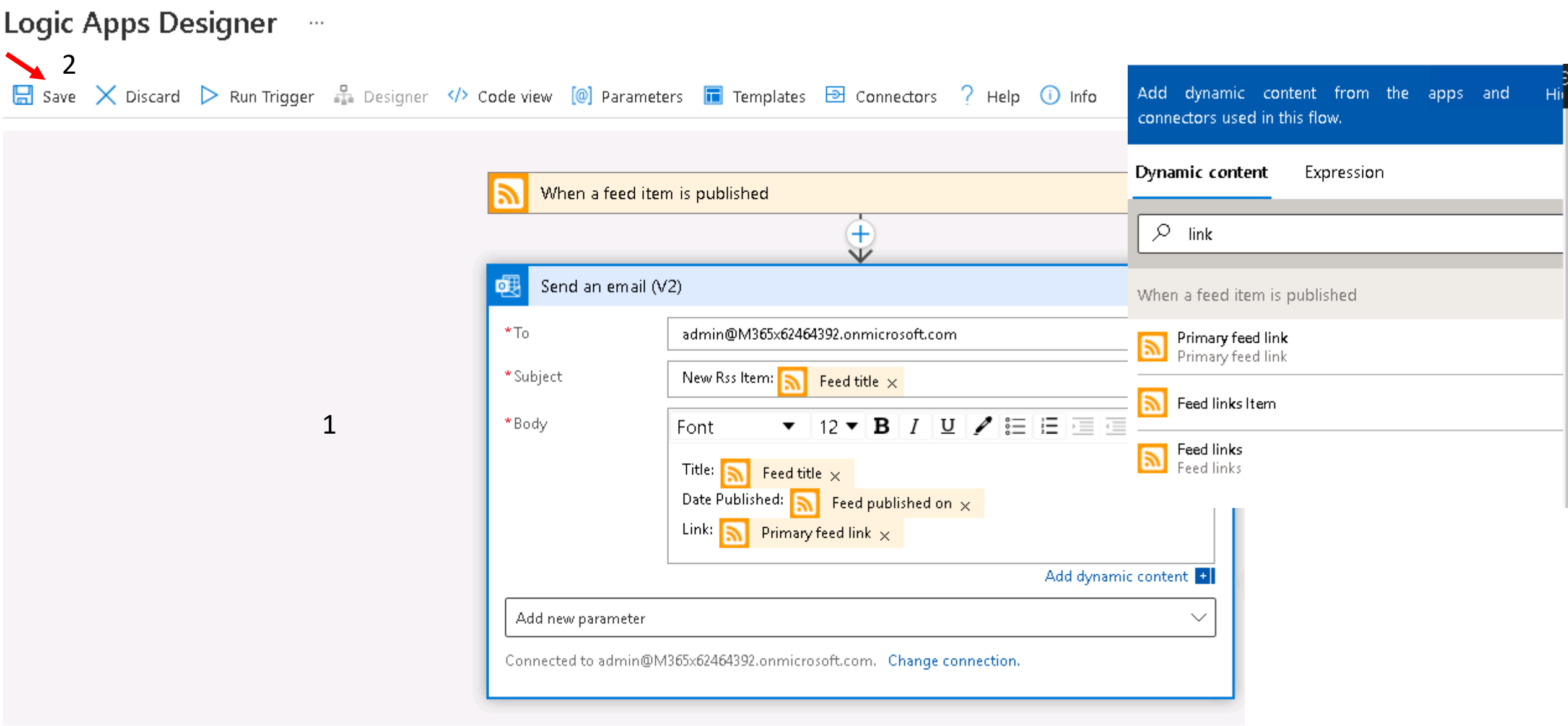
Type office 365 outlook to search for the action you Need. Scroll down and select “Send and email (V2) Office 365 Outlook



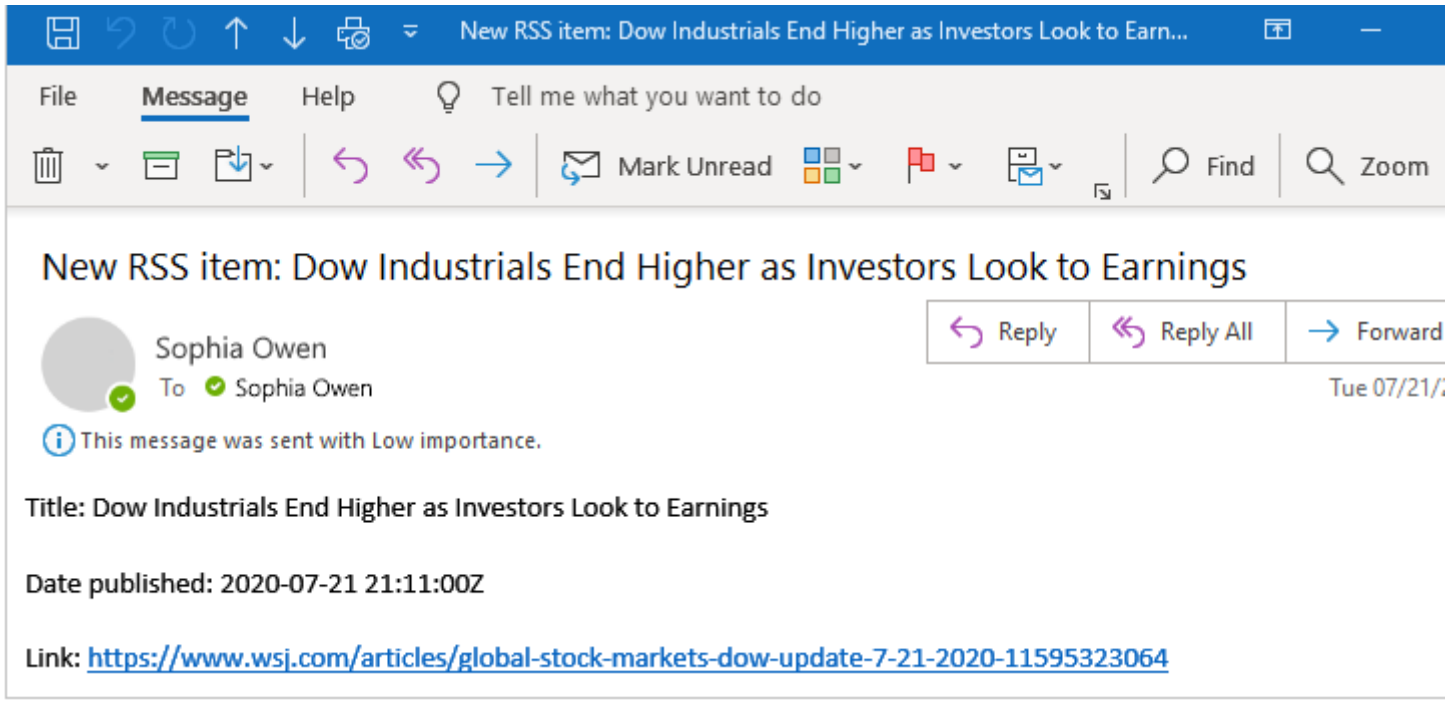


If your selected email service prompts you to sign in and authenticate your identity, complete that step now.

Insert fields using the dynamic data content list



Example


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
Reply
Reply All
Forward
Sophia Owen
To Sophia Owen
Tue 07/21/
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