

Build an NRT Analytics Rule



Real-Time Threat Detection with Microsoft Sentinel

- **NRT (Near Real-Time) rules** trigger on *every single event* with almost **zero delay**
- Ideal for **high-risk signals** that can't wait for scheduled rule intervals
- Unlike Scheduled rules that run every 5 mins, NRT rules fire **instantly** when data is ingested
- Best used for **critical sign-ins, privileged actions, or malware detections**
- Powered by Kusto Query Language (KQL) for precise event logic
- Sentinel is the SIEM workspace; Defender XDR is the unified SecOps portal where rules now live.

 **Pro Insight:** Use NRT only for **low-volume, high-value** detections — they can be expensive if triggered often.

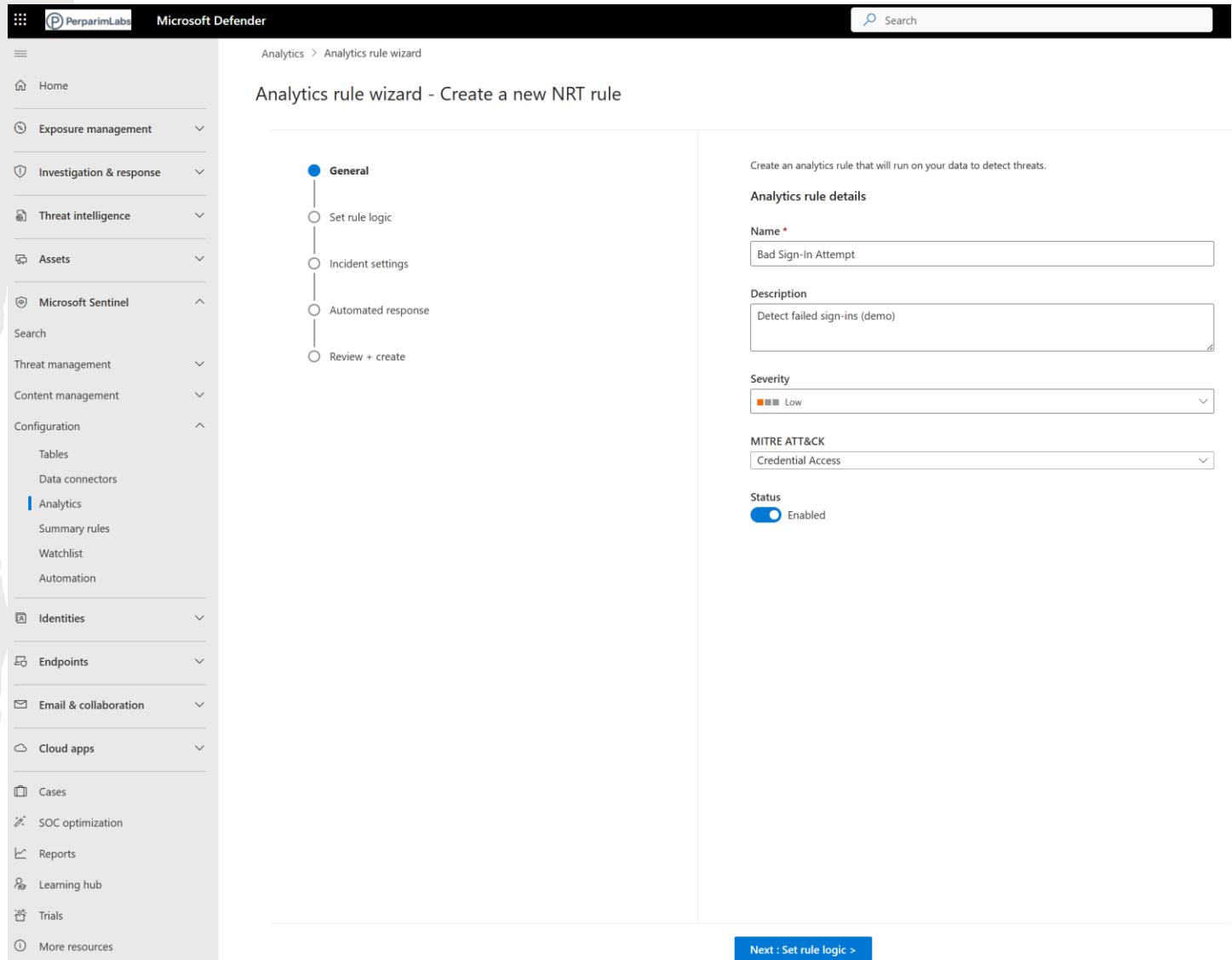
Navigate to Analytics

- Open **Microsoft Azure portal** → **Microsoft Sentinel**
- Select your **Sentinel workspace**
- Under **Configuration**, click **Analytics**
- This will open the **Microsoft Defender XDR** portal
- In Microsoft Defender XDR, click **Create** → **NRT query rule**

📌 *NRT = Near Real-Time — triggers on every event*

Define Rule Basics

- **Name:** Bad Sign-In Attempt
- **Description:** Detect failed sign-ins (demo)
- **Severity:** Low
- **MITRE ATT&CK:** Credential Access
- **Status:** Enabled



The screenshot shows the Microsoft Defender Analytics rule wizard interface. The left sidebar navigation includes Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel (selected), Search, Threat management, Content management, Configuration (Tables, Data connectors, Analytics, Summary rules, Watchlist, Automation), Identities, Endpoints, Email & collaboration, Cloud apps, Cases, SOC optimization, Reports, Learning hub, Trials, and More resources. The main content area is titled 'Analytics rule wizard - Create a new NRT rule' and shows the 'General' step. The 'General' step has four sub-options: Set rule logic, Incident settings, Automated response, and Review + create. To the right, the 'Analytics rule details' section is displayed, containing fields for Name (Bad Sign-In Attempt), Description (Detect failed sign-ins (demo)), Severity (Low), MITRE ATT&CK (Credential Access), and Status (Enabled). A 'Next : Set rule logic >' button is at the bottom right.

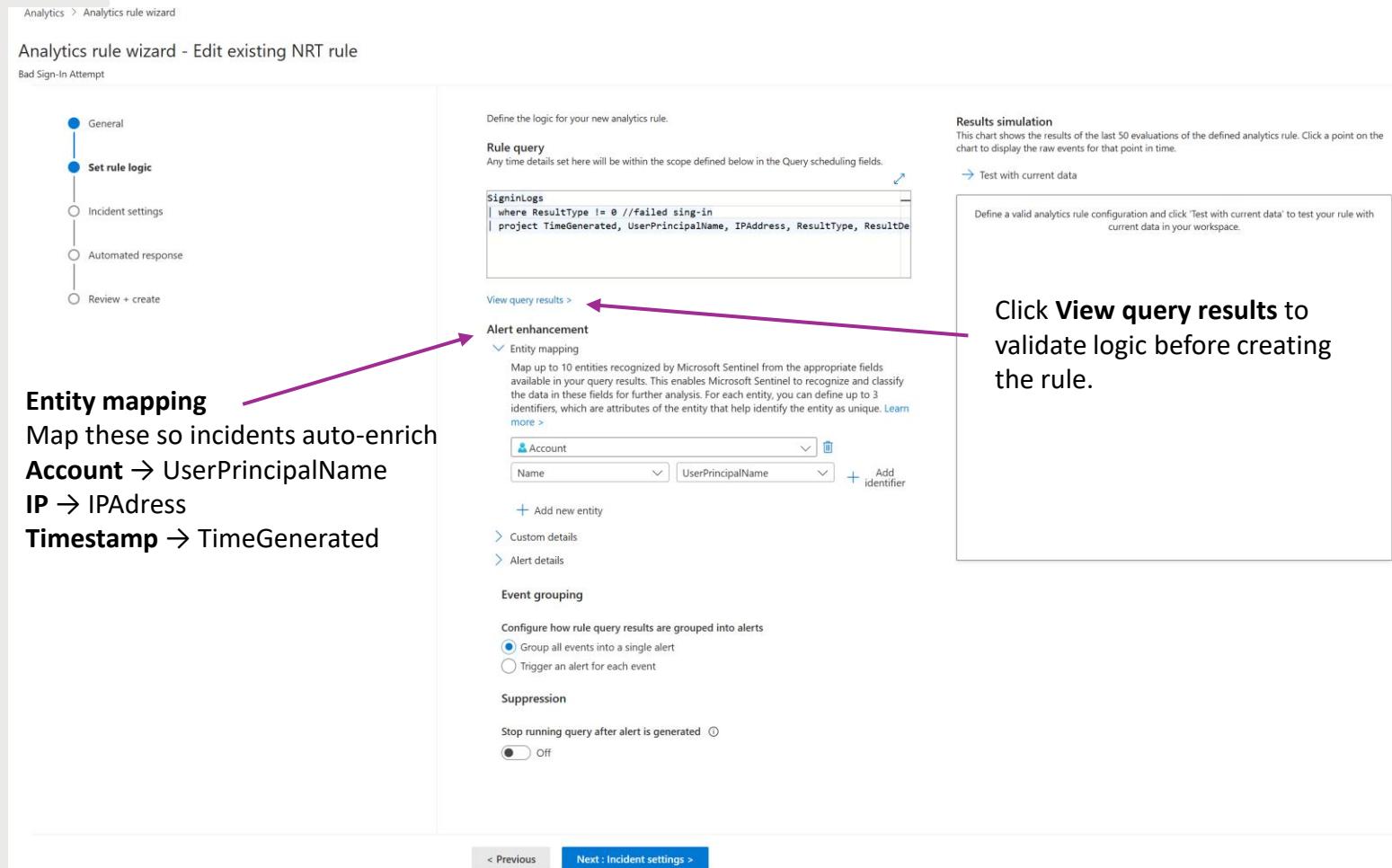
Write the KQL Query

- Use this query to detect failed sign-ins:

SigninLogs

```
| where ResultType != 0  
| project TimeGenerated,  
UserPrincipalName,  
IPAddress, ResultType,  
ResultDescription
```

- Runs on every event (no schedule needed)
- Click **View query results** to test



Entity mapping
Map these so incidents auto-enrich
Account → UserPrincipalName
IP → IPAddress
Timestamp → TimeGenerated

Analytics rule wizard - Edit existing NRT rule
Bad Sign-In Attempt

General
Set rule logic
Incident settings
Automated response
Review + create

Rule query
Any time details set here will be within the scope defined below in the Query scheduling fields.

```
SigninLogs  
| where ResultType != 0 //failed sing-in  
| project TimeGenerated, UserPrincipalName, IPAddress, ResultType, ResultDescription
```

View query results > ←

Alert enhancement

Entity mapping
Map up to 10 entities recognized by Microsoft Sentinel from the appropriate fields available in your query results. This enables Microsoft Sentinel to recognize and classify the data in these fields for further analysis. For each entity, you can define up to 3 identifiers, which are attributes of the entity that help identify the entity as unique. [Learn more >](#)

Account
Name UserPrincipalName + Add identifier

+ Add new entity
> Custom details
> Alert details

Event grouping
Configure how rule query results are grouped into alerts

Group all events into a single alert
 Trigger an alert for each event

Suppression
Stop running query after alert is generated
Off

< Previous Next : Incident settings >

 *This runs immediately on every SigninLogs event ingested.*

Enable Incident Creation

- Enable **Create incidents from alerts**
- Keep **Group related alerts** disabled
 - This lets each alert create a new incident

Analytics rule wizard - Create a new NRT rule

General

Set rule logic

Incident settings

Automated response

Review + create

Incident settings

alerts can be grouped together into an Incident that should be looked into. You can set whether the alerts that are triggered by this analytics rule should generate incidents.

Create incidents from alerts triggered by this analytics rule

Enabled

Alert grouping

Microsoft Defender correlation activities can link other alerts or merge existing incidents to the generated incident, regardless of the alert grouping settings defined in the analytics rule.

Set how the alerts that are triggered by this analytics rule, are grouped into incidents. Grouping alerts into incidents provides the context you need to respond and reduces the noise from single alerts.

Group related alerts, triggered by this analytics rule, into incidents

Disabled

Limit the group to alerts created within the selected time frame *

5 Hours

Group alerts triggered by this analytics rule into a single incident by

Grouping alerts into a single incident if all the entities match (recommended)

Grouping all alerts triggered by this rule into a single incident

Grouping alerts into a single incident if the selected entity types and details match:

Select entities

Select details

Re-open closed matching incidents

Disabled

< Previous

Next : Automated response >

Attach Automation (Optional)

- You can link automation rules or playbooks
- We'll skip this for now

Analytics > Analytics rule wizard

Analytics rule wizard - Create a new NRT rule

General

Set rule logic

Incident settings

Automated response

Review + create

Automation rules

View all automation rules that may be triggered by this analytics rule and create new automation rules.

+ Add new

Order	Automation rule name	Trigger	Action	Status
No automation rules				

Alert automation (classic)

⚠ As of June 2023, you can no longer select playbooks to run directly from an analytics rule by adding it to the following list. Playbooks already in the list will continue to run until March 2026, when this method will be deprecated.

Instead, to run a playbook in response to an alert generated by this analytics rule, create an Automation rule (see above), choose "When alert is created" as the rule's trigger, and add the playbook to the rule's Actions list. We strongly encourage you to migrate any playbooks in the following list to run from automation rules. [Learn more](#).

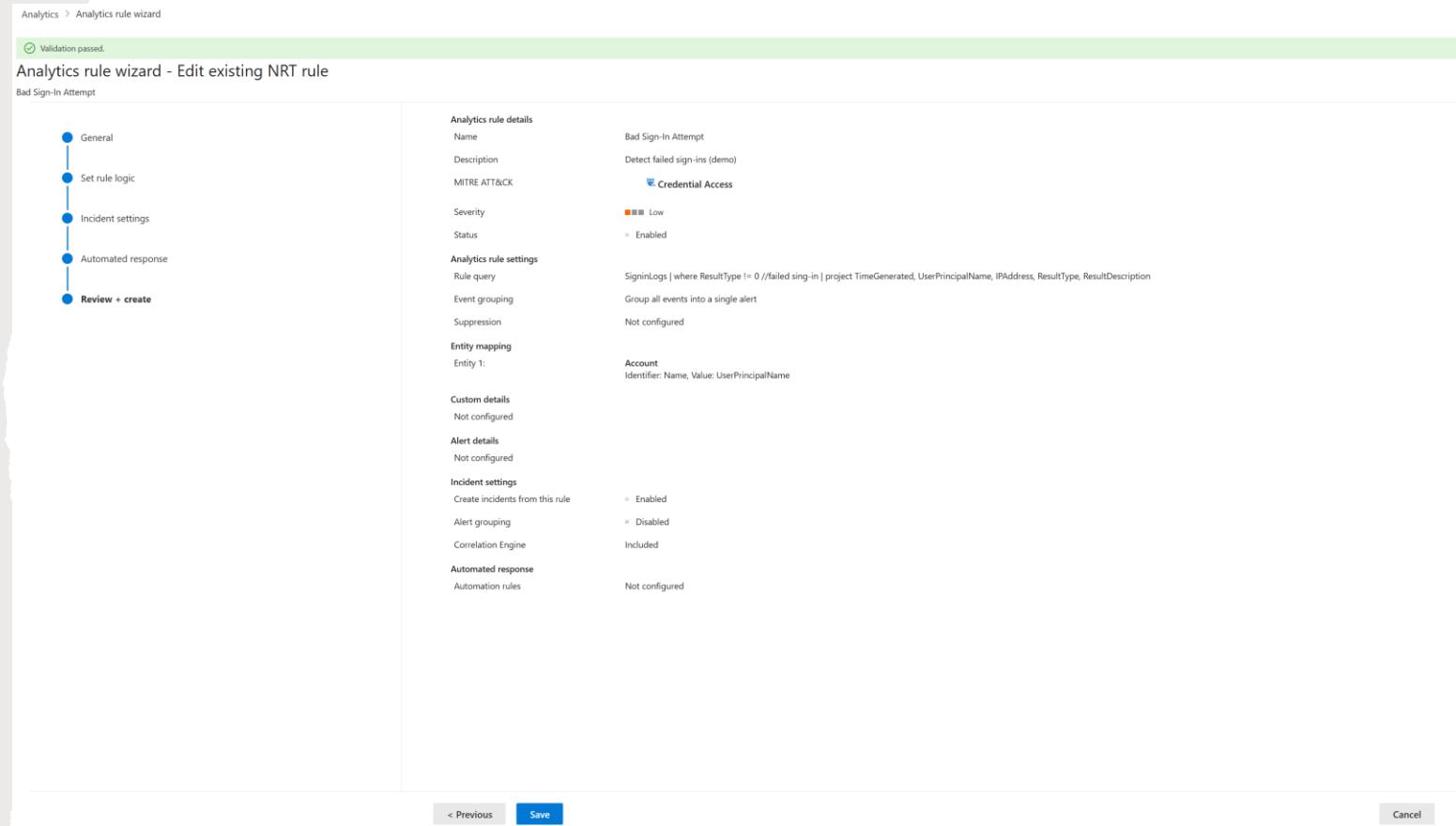
< Previous

Next : Review + create >

Cancel

Review and Deploy

- Review all rule settings
- Click **Create** to deploy your NRT rule



Analytics > Analytics rule wizard

Validation passed.

Analytics rule wizard - Edit existing NRT rule

Bad Sign-In Attempt

General

Set rule logic

Incident settings

Automated response

Review + create

Analytics rule details

- Name: Bad Sign-In Attempt
- Description: Detect failed sign-ins (demo)
- MITRE ATT&CK: Credential Access
- Severity: Low
- Status: Enabled

Analytics rule settings

- Rule query: SigninLogs | where ResultType != 0 //failed sing-in | project TimeGenerated, UserPrincipalName, IPAddress, ResultType, ResultDescription
- Event grouping: Group all events into a single alert
- Suppression: Not configured

Entity mapping

- Entity 1: Account
Identifier: Name, Value: UserPrincipalName

Custom details

- Not configured

Alert details

- Not configured

Incident settings

- Create incidents from this rule: Enabled
- Alert grouping: Disabled
- Correlation Engine: Included

Automated response

- Automation rules: Not configured

< Previous **Save** Cancel

Rule is Live

- Go to **Analytics** → **Active rules**
- Confirm:
 - **Type:** NRT
 - **Severity:** Low
 - **Status:** Enabled
- Your rule will now trigger on **every bad sign-in attempt**

The screenshot shows the Microsoft Defender Analytics interface. The left sidebar lists various security modules: Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel, Threat management, Content management, Configuration, Tables, Data connectors, Analytics (selected), Summary rules, Watchlist, Automation, Identities, Endpoints, Email & collaboration, Cloud apps, Cases, SOC optimization, Reports, Learning hub, Trials, More resources, and System. The main content area is titled 'Analytics' and features a section 'Manage all your rules in one place' with a sub-section 'Rules by severity' showing a color-coded bar for High (1), Medium (0), Low (1), and Informational (0). Below this, a table lists 'Active rules':

Severity	Name	Rule type	Status	Tactics	Techniques	Sub techniques	Source name	Last modified
Low	Bad Sign-In Attempt	NRT	Enabled	Credential Aco			Custom Content	...
High	High Risk Login Rule	Scheduled	Enabled	Credential Aco			Custom Content	...

On the right, a detailed view of the 'Bad Sign-In Attempt' rule is shown, including its description ('Detect failed sign-ins (demo)'), MITRE ATT&CK mapping ('Credential Access'), rule query ('Rule query SigninLogs | where ResultType != 0 //Failed sign-in | project TimeGenerated, UserPrincipalName, IPAddress, ResultType'), suppression ('Not configured'), and alert grouping ('Enabled').

NRT fires on every event—use for low-volume, high-value detections to avoid noise & cost.



NRT Rule Successfully Deployed

- Real-Time Detection — Powered by Microsoft Sentinel
- You just built an **NRT Analytics Rule** that triggers on **every failed sign-in**
- This enables **instant detection and response** for high-risk activity
- A core step in building a **proactive SOC strategy**
- Keep optimizing with KQL and automation playbooks