



[Course](#) > [LAB GUIDE](#) > [Lab 5 - Using rules](#) > Using rules

Using rules

Using rules

In this lab, we will create Rules to monitor the Login Activity. Below is the use case.

An Organization wants to monitor the user accounts of terminated employees.

- a. Create a rule to generate offenses for invalid login activities.
- b. Reference set should be used to store and look up for the usernames of terminated employees.

Create an Event Rule

Perform the below steps in this lab.

1. Login in the Qradar Interface, on Home page, Click the **Log Activity** tab.

[illegible]




Lab 5 Employees Login Activity




Apply on events which are detected by the system

6. Add the following tests by clicking  to the rule under these conditions:

- when any of these event properties are contained in any of these reference set(s)
- when an event matches any | all of the following rules






Apply on events which are detected by the system

   and when any of these event properties are contained in any of these reference set(s)

   and when an event matches any of the following rules

To add the first rule test, when any of these event properties are contained in any of these reference set(s), perform the following steps:

- Filter the options in the **Test Group** list. For **Type to filter**, enter ref

ref
 when any of these event properties are contained in any of these reference set(s)
 when any of these event properties is the key and any of these event properties is the value in any of these reference maps
 when any of these event properties is the key and any of these event properties is the value in any of these reference map of sets
 when any of these event properties is the key of the first map and any of these event properties is the key of the second map and any of these event properties is the value in any of these reference map of maps
 when Reference Table Key data matches any/all selected event properties and selected reference table column Select operator the value of selected event property

ii. Click the green **plus (+)** icon next to the when any of these event properties are contained in any of these reference set(s) test.

iii. Click the parameter **these event properties**.

iv. Filter the fields in the event property list. In the **Type to filter field**, enter user.

Select an event property and click 'Add'

user

- Identity Username
- Originating_User (custom)
- Recipient_User (custom)
- Target User Name (custom)
- User ID (custom)
- Username**

Add +

Selected Items

Remove -

Submit Cancel

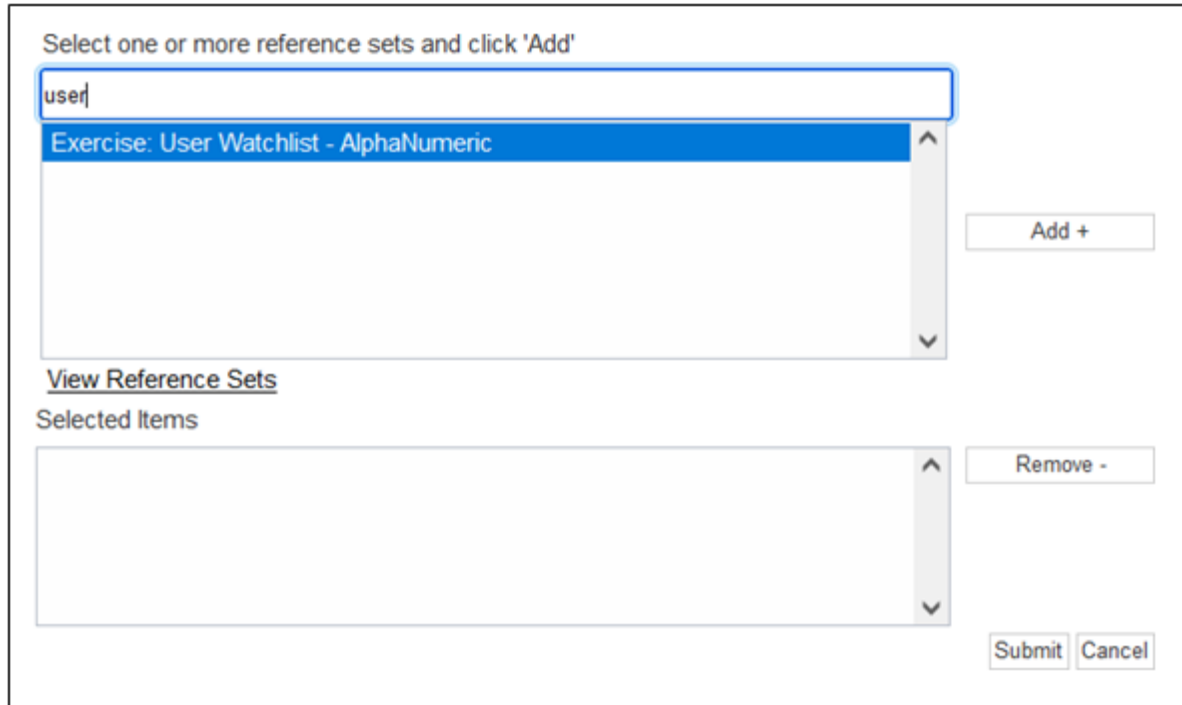
v. Select **Username** and click **Add**.

Add +

vi. Click Submit.

vii. Click the parameter **these reference set(s)**.

viii. Select the reference set **Exercise: User Watchlist** and click **Add** and Click **Submit**.



The screenshot shows a web interface for selecting reference sets. At the top, it says "Select one or more reference sets and click 'Add'". Below this is a search bar containing the text "user". A dropdown menu is open, showing a single item: "Exercise: User Watchlist - AlphaNumeric". To the right of the dropdown is an "Add +" button. Below the dropdown is a link that says "View Reference Sets". Underneath that is a section titled "Selected Items" with an empty list box. To the right of the list box is a "Remove -" button. At the bottom right of the interface are "Submit" and "Cancel" buttons.

7. To add the second rule test, when an event matches any | all of the following rules, perform the following steps:

i. In the **Test Group** drop-down list, select **Functions - Simple**.

ii. Click the **green plus (+)** icon next to the only test listed.


Which tests do you wish to perform on incoming events?

Test Group **Functions - Simple** Export as Building Block

Type to filter

 when an event matches **any**all of the following **rules**

iii. Click the parameter **rules**.

  and when an event matches any of the following rules

iv. Filter the options in the rules list. In the **Type to filter** field, enter the following text:

BB: Category

v. Select **BB: Category Definition: Authentication Success** and click **Add**, and Click Submit.

Select the rule(s) to match and click 'Add'

BB:Category
BB:CategoryDefinition: Application or Service Installed or Modified
BB:CategoryDefinition: Auditing Changed
BB:CategoryDefinition: Authentication Failures
BB:CategoryDefinition: Authentication Success
BB:CategoryDefinition: Authentication to Disabled Account
BB:CategoryDefinition: Authentication to Expired Account

Add +

Selected Items

BB:CategoryDefinition: Authentication Success

Remove -

Submit Cancel

8. Assign the rule to the group **Authentication**.

Please select any groups you would like this rule to be a member of:

☐ Anomaly
☐ Asset Reconciliation Exclusion
☒ Authentication
☐ Botnet
☐ Category Definitions

9. To document the rule in the **Notes** field, enter the following text.

This rule tracks the successful login of terminated users accounts.

10. Click **Next**.

The screenshot shows the 'Rule Wizard: Rule Test Stack Editor' window. At the top, it asks 'Which tests do you wish to perform on incoming events?'. Below this, there's a 'Test Group' dropdown set to 'Functions - Simple' and an 'Export as Building Block' button. A search bar labeled 'Type to filter' is present. The main area contains a single rule: a green plus icon followed by 'when an event matches anyall of the following rules'. Below this, a note says 'Rule (Click on an underlined value to edit it) Invalid tests are highlighted and must be fixed before rule can be saved.' The rule configuration shows 'Apply Lab 5 Employees Login Activity' on events detected by the 'Local' system. It includes two conditions: 'and when any of Username are contained in any of Exercise: User Watchlist - AlphaNumeric' and 'and when an event matches any of the following BB: CategoryDefinition: Authentication Success'. Below the rule, there's a section 'Please select any groups you would like this rule to be a member of:' with a list of categories: Anomaly, Asset Reconciliation Exclusion, Authentication (checked), Botnet, and Category Definitions. A 'Notes' section at the bottom contains the text 'This rule tracks the successful login of terminated users accounts.' Navigation buttons '<< Back', 'Next >>', 'Finish', and 'Cancel' are at the bottom right.

11. Configure the rule action and response as shown below

Rule Action

- Ensure the detected event is part of an offense: **enable**
- Index offense based on list: **Username**
- Annotate this offense: **enable, User Watchlist login success**
- Annotate event: **enable, User Watchlist login success**

Rule Action
Choose the action(s) to take when an event occurs that triggers this rule

☐ Severity Set to

☐ Credibility Set to

☐ Relevance Set to

☒ Ensure the detected event is part of an offense

Index offense based on

☒ Annotate this offense:

☐ Include detected events by Username from this point forward, in the offense, for : second(s)

☒ Annotate event

Enter annotation for this event:

☐ Bypass further rule correlation event

Rule Response

- Dispatch New Event: **enable**
- Type Event Name: **User Watchlist login**
- Type Event Description: **User Watchlist login**
- Severity: **8**
- Credibility: **10**
- Relevance: **10**

- High Level Category: **Authentication**
- Low Level Category: **User Login Success**
- Annotate this offense: **enable, User Watchlist login success**
- Ensure the dispatched event is part of an offense: **enable**
- Index offense based on: **Username**
- This information should contribute to the naming of the associated offense(s): **enable**

Rule Response

Choose the response(s) to make when an event triggers this rule

☒ Dispatch New Event

Enter the details of the event to dispatch

Event Name:

Event Description:

Event Details:

Severity Credibility Relevance

High-Level Category: Low-Level Category:

☒ Annotate this offense:

☒ Ensure the dispatched event is part of an offense

Index offense based on

☐ Include detected events by Username from this point forward, in the offense, for : second(s)

Offense Naming

☒ This information should contribute to the name of the associated offense(s)

☐ This information should set or replace the name of the associated offense(s)

☐ This information should not contribute to the naming of the associated offense(s)

☐ Email

☐ Send to Local Syslog

☐ Send to Forwarding Destinations

☐ Notify

☐ Add to a Reference Set

☐ Add to Reference Data

☐ Remove from a Reference Set

☐ Remove from Reference Data

☐ Execute Custom Action

12. Click Next.

13. Verify that your rule summary looks similar to the one in the screen capture and click Finish

Rule Summary

Review this rule summary to ensure all the details you have specified are correct. You may click 'Back' to change incorrect settings.

Note that your rule has not yet been saved or deployed. It will be saved when you select 'Finish' and only be deployed if you chose the 'Enable Rule' checkbox on the previous screen.

Rule Description

Apply Lab 5 Employees Login Activity on events which are detected by the Local system and when any of Username are contained in any of Exercise: User Watchlist - AlphaNumeric and when an event matches any of the following BB: CategoryDefinition: Authentication Success

Rule Notes

This rule tracks the successful login of terminated users accounts.

Rule Actions

- Force the detected Event to create a NEW offense, select the offense using Username
 - Annotate this offense with: User Watchlist login success
- Annotate the Event with: User Watchlist login success

Rule Responses

- Dispatch New Event
 - Event Name: User Watchlist login
 - Event Description: User Watchlist login
 - Severity: 8 Credibility: 10 Relevance: 10
 - High-Level Category: Authentication
 - Low-Level Category: User Login Success
 - Annotate the offense with User Watchlist login success
 - Force the dispatched event to create a NEW offense, select the offense using Username

This Rule will be: Enabled

<< Back Next >> Finish Cancel

14. Open a remote shell to the QRadar VM. Use the procedure as outlined in Running commands on the QRadar VM.

15. To feed prepared syslog messages to QRadar, run the following commands:

```
cd /labfiles
```

```
./sendWindows.sh
```

```
[root@allinone742 labfiles]# ./sendWindows.sh
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
generating 35 messages per second to 10.10.9.30:514
Ctrl-c to stop
```

Wait for five minutes and return to the Offenses tab in browser



The screenshot shows the QRadar user interface for the Offenses tab. At the top, there's a search bar and a 'Last Refresh' timestamp of 00:05:10. Below the search bar, it says 'Offenses with last EventFlow received from Jun 18, 2021, 11:22:44 PM to Jun 19, 2021, 12:22:44 AM'. A dropdown menu for 'View Offenses with:' is set to 'Select An Option'. Under 'Current Search Parameters:', there are links for 'Exclude Hidden Offenses (Clear Filter)' and 'Exclude Closed Offenses (Clear Filter)'. The main table has columns: ID, Description, Offense Type, Offense Source, Magnitude, Source IPs, Destination IPs, Users, and Log Sources. Two offenses are listed, both with ID 18 and a description 'User Watchlist login containing Success Audit: Authentication Ticket Granted'. The first offense has a source IP of 10.2.121.29 and a user of CF000297. The second offense has a source IP of 10.128.140.40 and a user of gg000565. Both have a magnitude of 5 (indicated by a red bar) and multiple log sources.

ID	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources
18	User Watchlist login containing Success Audit: Authentication Ticket Granted	Username	CF000297	5	10.2.121.29	10.0.120.11	CF000297	Multiple (2)
18	User Watchlist login containing Success Audit: Authentication Ticket Granted	Username	gg000565	5	10.128.140.40	10.0.120.11	gg000565	Multiple (2)

Investigate the offenses created. Answer the following questions:

- How many offenses did the BQX Watchlist User Activity rule create? On the Rule list page, select the rule and look for the offense count parameter.
- List the user IDs that created offenses. In the QRadar user interface, double-click the Offenses tab and find offenses that have Watchlist in the description.
- What is the source IP address of the offenses created?

Working with rule parameters

To work with the parameters of a rule, perform the following steps:

1. In the QRadar user interface, navigate to the Offenses tab.

2. Click Rules in the left pane.



3. Sort the Offense Count column in descending order, Click the header for the Offense Count column to sort in descending order.

Rule Name	Group	Rule Category	Rule Type	Enabled	Response	EventFlow Count	Offense Count ▲	Origin ▲
Login Failures Followed By Success to the same Destination IP	Authentication, Intrusion Detection	Custom Rule	Event	True	Dispatch New Event	8,037	1	System
Multiple Login Failures for Single Username	Authentication, Intrusion Detection	Custom Rule	Event	True	Dispatch New Event	36	1	System
Multiple Login Failures to the Same Destination	Authentication, Intrusion Detection	Custom Rule	Event	True	Dispatch New Event	307	1	System
Remote _RDP_Access	Authentication, Intrusion Detection	Custom Rule	Flow	True		3	1	User
All Exploits Become Offense	Intrusion Detection	Custom Rule	Event	False		0	0	System
Anomaly: Excessive Firewall Accepts Across Multiple Hosts	Recan	Custom Rule	Event	False	Dispatch New Event	0	0	System
AssetExclusion: Exclude DNS Name By IP	Asset Recon:IdB	Custom Rule	Event	True	ReferenceSet	0	0	System
AssetExclusion: Exclude DNS Name By MAC Address	Asset Recon:IdB	Custom Rule	Event	True	ReferenceSet	0	0	System
AssetExclusion: Exclude DNS Name By NetBIOS Name	Asset Recon:IdB	Custom Rule	Event	True	ReferenceSet	0	0	System
AssetExclusion: Exclude IP By DNS Name	Asset Recon:IdB	Custom Rule	Event	True	ReferenceSet	0	0	System
AssetExclusion: Exclude IP By MAC Address	Asset Recon:IdB	Custom Rule	Event	True	ReferenceSet	0	0	System

a. What rule created the most offenses?

4. On the **Rules** page, from the **Display** drop-down list, select **Rules**.

5. From the **Group** drop-down list, do **not** select any group.

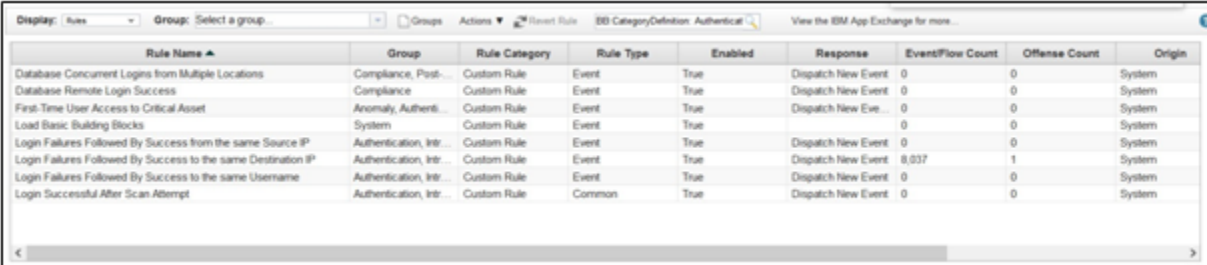
6. In the Search Rules field, enter the following name:

BB:CategoryDefinition: Authentication Success

The Rules display lists all the rules that meet the search criteria.

7. Select several of the rules and review the rule tests.

Notice that the rules listed include the BB:CategoryDefinition: Authentication Success building block. Before editing a building block or rule, determine which other rules use it.



The screenshot shows the IBM App Exchange Rules page. The search filter is set to 'BB:CategoryDefinition: Authentication Success'. The table displays the following rules:

Rule Name	Group	Rule Category	Rule Type	Enabled	Response	EventFlow Count	Offense Count	Origin
Database Concurrent Logins from Multiple Locations	Compliance, Post...	Custom Rule	Event	True	Dispatch New Event	0	0	System
Database Remote Login Success	Compliance	Custom Rule	Event	True	Dispatch New Event	0	0	System
First-Time User Access to Critical Asset	Anomaly, Authenti...	Custom Rule	Event	True	Dispatch New Eve...	0	0	System
Load Basic Building Blocks	System	Custom Rule	Event	True		0	0	System
Login Failures Followed By Success from the same Source IP	Authentication, Intr...	Custom Rule	Event	True	Dispatch New Event	0	0	System
Login Failures Followed By Success to the same Destination IP	Authentication, Intr...	Custom Rule	Event	True	Dispatch New Event	8,037	1	System
Login Failures Followed By Success to the same Username	Authentication, Intr...	Custom Rule	Event	True	Dispatch New Event	0	0	System
Login Successful After Scan Attempt	Authentication, Intr...	Custom Rule	Common	True	Dispatch New Event	0	0	System