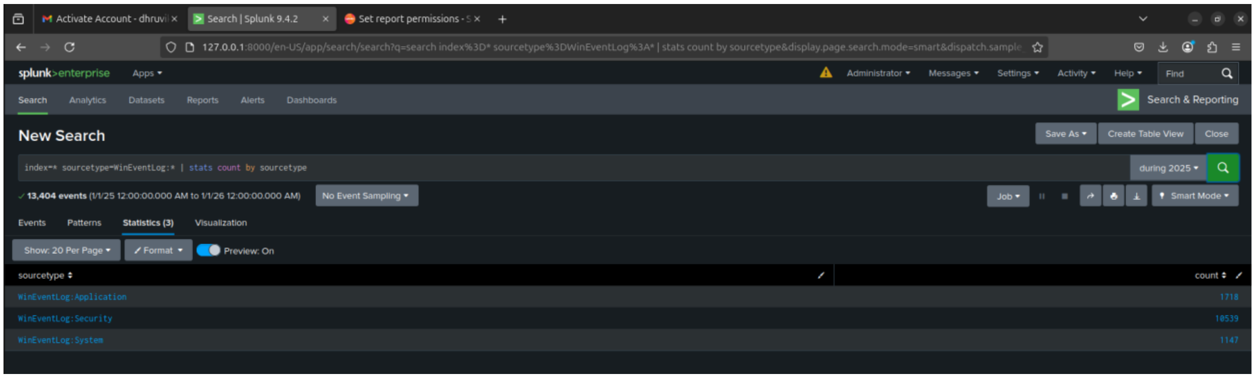
Types of logs

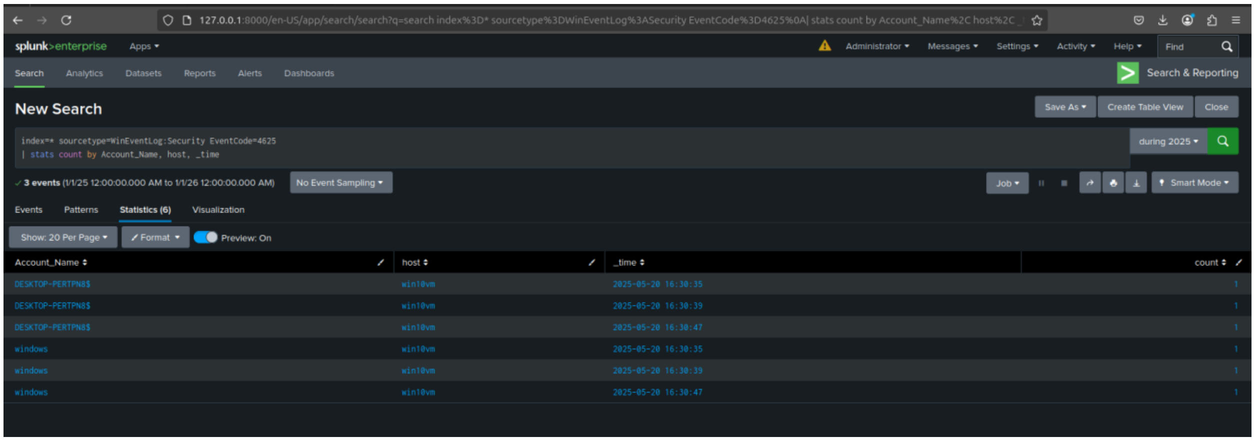


```
index=* sourcetype=WinEventLog:* | stats count by sourcetype
```

✓ 13,404 events (1/1/25 12:00:00.000 AM to 1/1/26 12:00:00.000 AM)

sourcetype	count
WinEventLog:Application	1718
WinEventLog:Security	10539
WinEventLog:System	1147

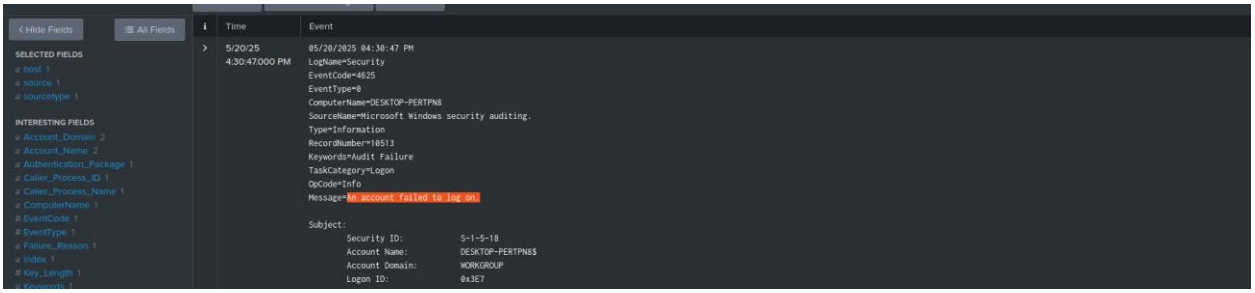
Failed login attempts



```
index=* sourcetype=WinEventLog:Security EventCode=4625
| stats count by Account_Name, host, _time
```

✓ 3 events (1/1/25 12:00:00.000 AM to 1/1/26 12:00:00.000 AM)

Account_Name	host	_time	count
DESKTOP-PERTPN8$	win10vm	2025-05-20 16:30:35	1
DESKTOP-PERTPN8$	win10vm	2025-05-20 16:30:39	1
DESKTOP-PERTPN8$	win10vm	2025-05-20 16:30:47	1
windows	win10vm	2025-05-20 16:30:35	1
windows	win10vm	2025-05-20 16:30:39	1
windows	win10vm	2025-05-20 16:30:47	1

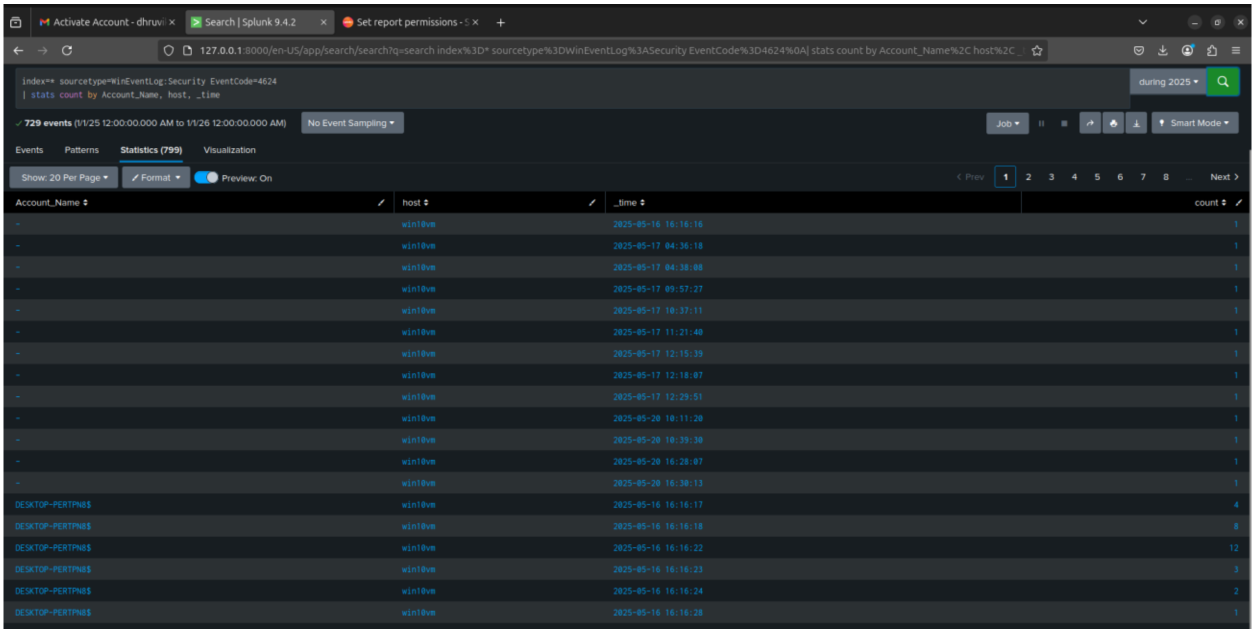


5/20/25 4:30:47.000 PM

```
05/20/2025 04:30:47 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=DESKTOP-PERTPN8
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=10513
Keywords=Audit Failure
TaskCategory=Logon
OpCode=Info
Message=An account failed to log on.

Subject:
        Security ID:            S-1-5-18
        Account Name:           DESKTOP-PERTPN8$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7
```

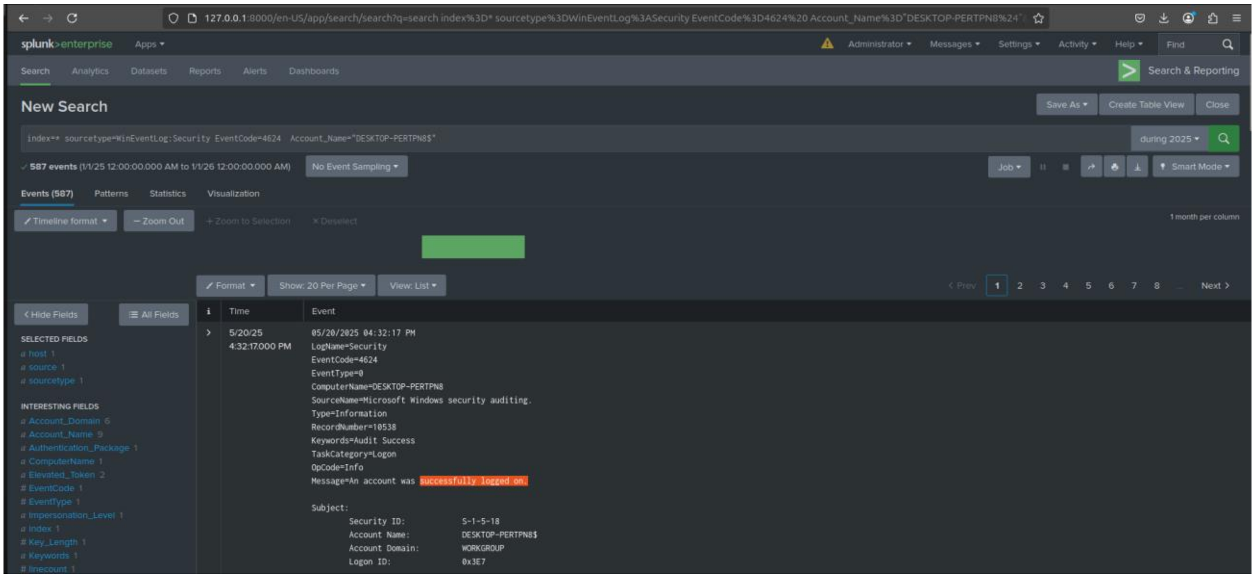
Successful logins


Activate Account - dhruvi
Search | Splunk 9.4.2
Set report permissions - S
127.0.0.1:8000/en-US/app/search/search?q=search index%3D* sourcetype%3DWinEventLog%3ASecurity EventCode%3D4624%0A| stats count by Account_Name%2C host%2C
during 2025
Job
Smart Mode
Events
Patterns
Statistics (799)
Visualization
Show: 20 Per Page
Format
Preview: On
‹ Prev 1 2 3 4 5 6 7 8 ... Next ›

```
index=* sourcetype=WinEventLog:Security EventCode=4624
| stats count by Account_Name, host, _time
```

✓ 729 events (1/1/25 12:00:00.000 AM to 1/1/26 12:00:00.000 AM) No Event Sampling

Account_Name	host	_time	count
-	win10vm	2025-05-16 16:16:16	1
-	win10vm	2025-05-17 04:36:18	1
-	win10vm	2025-05-17 04:38:08	1
-	win10vm	2025-05-17 09:57:27	1
-	win10vm	2025-05-17 10:37:11	1
-	win10vm	2025-05-17 11:21:40	1
-	win10vm	2025-05-17 12:15:39	1
-	win10vm	2025-05-17 12:18:07	1
-	win10vm	2025-05-17 12:29:51	1
-	win10vm	2025-05-20 10:11:20	1
-	win10vm	2025-05-20 10:39:30	1
-	win10vm	2025-05-20 16:28:07	1
-	win10vm	2025-05-20 16:30:13	1
DESKTOP-PERTPN8$	win10vm	2025-05-16 16:16:17	4
DESKTOP-PERTPN8$	win10vm	2025-05-16 16:16:18	8
DESKTOP-PERTPN8$	win10vm	2025-05-16 16:16:22	12
DESKTOP-PERTPN8$	win10vm	2025-05-16 16:16:23	3
DESKTOP-PERTPN8$	win10vm	2025-05-16 16:16:24	2
DESKTOP-PERTPN8$	win10vm	2025-05-16 16:16:28	1



New Search

```
index=* sourcetype=WinEventLog:Security EventCode=4624  Account_Name="DESKTOP-PERTPN8$"
```

✓ 587 events (1/1/25 12:00:00.000 AM to 1/1/26 12:00:00.000 AM) No Event Sampling

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

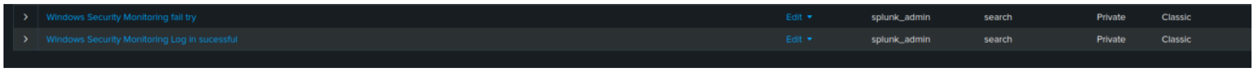
INTERESTING FIELDS
- a Account_Domain 6
- a Account_Name 9
- a Authentication_Package 1
- a ComputerName 1
- a Elevated_Token 2
- # EventCode 1
- # EventType 1
- a Impersonation_Level 1
- a index 1
- # Key_Length 1
- a Keywords 1
- # linecount 1

5/20/25
4:32:17.000 PM

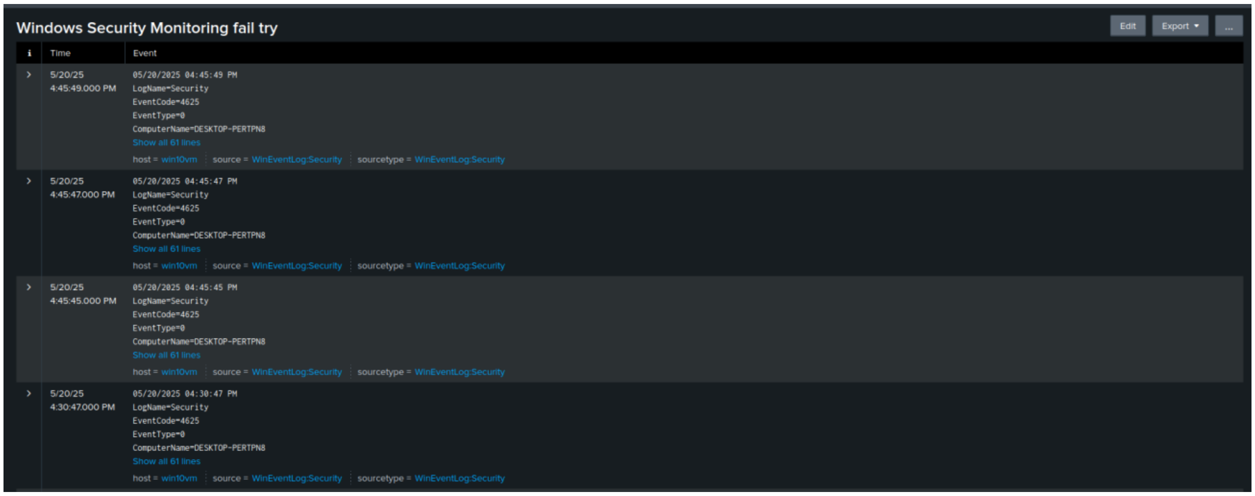
```
05/20/2025 04:32:17 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=DESKTOP-PERTPN8
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=10538
Keywords=Audit Success
TaskCategory=Logon
OpCode=Info
Message=An account was successfully logged on.

Subject:
	Security ID:		S-1-5-18
	Account Name:		DESKTOP-PERTPN8$
	Account Domain:		WORKGROUP
	Logon ID:		0x3E7
```

Save this logs on Dashboard For Monitor:



›	Windows Security Monitoring fail try	Edit ▾	splunk_admin	search	Private	Classic
›	Windows Security Monitoring Log in sucessful	Edit ▾	splunk_admin	search	Private	Classic



Windows Security Monitoring fail try

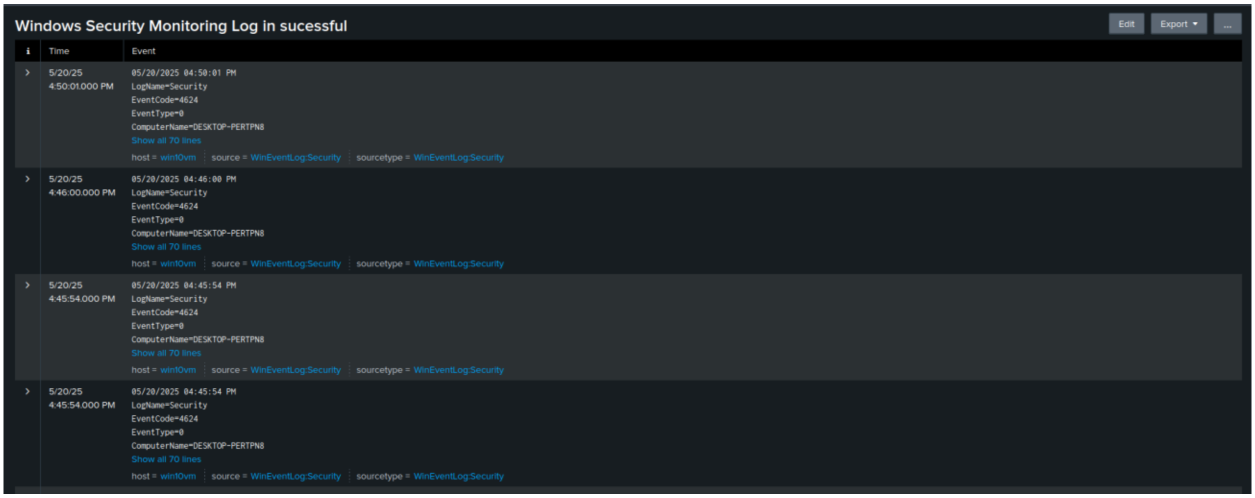
i	Time	Event

>	5/20/25
	4:45:49.000 PM
		05/20/2025 04:45:49 PM
		LogName=Security
		EventCode=4625
		EventType=0
		ComputerName=DESKTOP-PERTPN8
		Show all 61 lines
		host = win10vm ⋮ source = WinEventLog:Security ⋮ sourcetype = WinEventLog:Security

>	5/20/25
	4:45:47.000 PM
		05/20/2025 04:45:47 PM
		LogName=Security
		EventCode=4625
		EventType=0
		ComputerName=DESKTOP-PERTPN8
		Show all 61 lines
		host = win10vm ⋮ source = WinEventLog:Security ⋮ sourcetype = WinEventLog:Security

>	5/20/25
	4:45:45.000 PM
		05/20/2025 04:45:45 PM
		LogName=Security
		EventCode=4625
		EventType=0
		ComputerName=DESKTOP-PERTPN8
		Show all 61 lines
		host = win10vm ⋮ source = WinEventLog:Security ⋮ sourcetype = WinEventLog:Security

>	5/20/25
	4:30:47.000 PM
		05/20/2025 04:30:47 PM
		LogName=Security
		EventCode=4625
		EventType=0
		ComputerName=DESKTOP-PERTPN8
		Show all 61 lines
		host = win10vm ⋮ source = WinEventLog:Security ⋮ sourcetype = WinEventLog:Security



Windows Security Monitoring Log in sucessful

i	Time	Event

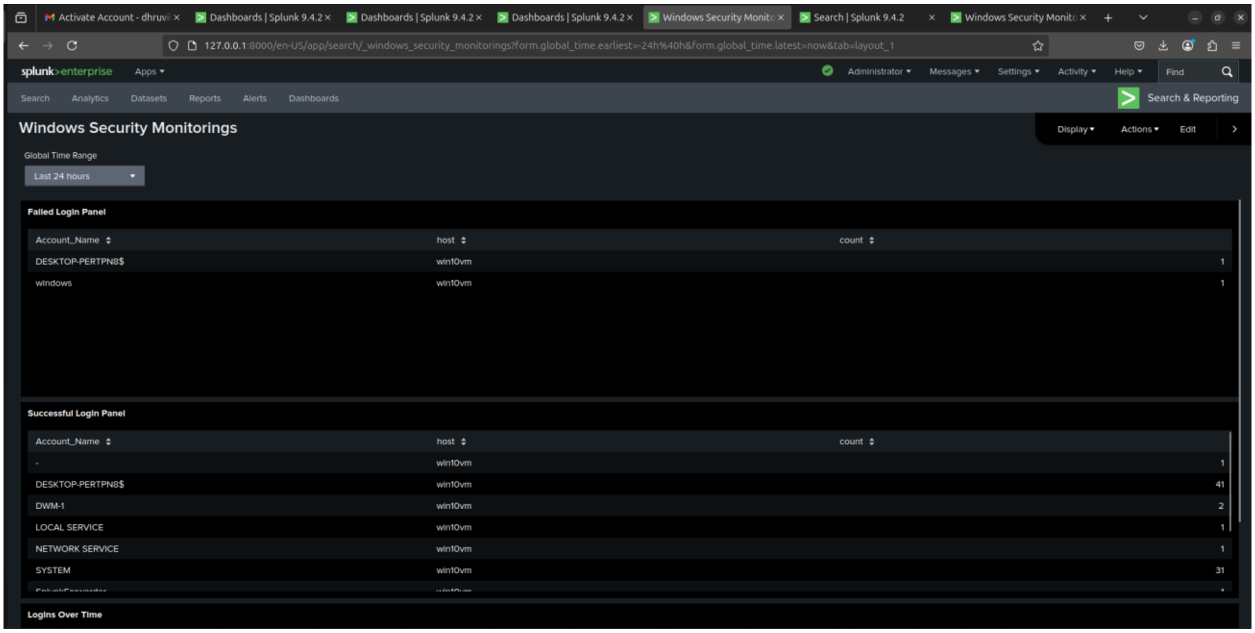
>	5/20/25
	4:50:01.000 PM
		05/20/2025 04:50:01 PM
		LogName=Security
		EventCode=4624
		EventType=0
		ComputerName=DESKTOP-PERTPN8
		Show all 70 lines
		host = win10vm ⋮ source = WinEventLog:Security ⋮ sourcetype = WinEventLog:Security

>	5/20/25
	4:46:00.000 PM
		05/20/2025 04:46:00 PM
		LogName=Security
		EventCode=4624
		EventType=0
		ComputerName=DESKTOP-PERTPN8
		Show all 70 lines
		host = win10vm ⋮ source = WinEventLog:Security ⋮ sourcetype = WinEventLog:Security

>	5/20/25
	4:45:54.000 PM
		05/20/2025 04:45:54 PM
		LogName=Security
		EventCode=4624
		EventType=0
		ComputerName=DESKTOP-PERTPN8
		Show all 70 lines
		host = win10vm ⋮ source = WinEventLog:Security ⋮ sourcetype = WinEventLog:Security

>	5/20/25
	4:45:54.000 PM
		05/20/2025 04:45:54 PM
		LogName=Security
		EventCode=4624
		EventType=0
		ComputerName=DESKTOP-PERTPN8
		Show all 70 lines
		host = win10vm ⋮ source = WinEventLog:Security ⋮ sourcetype = WinEventLog:Security

Create a new dashboard for Windows Monitoring:



Activate Account - dhruvil
Dashboards | Splunk 9.4.2
Dashboards | Splunk 9.4.2
Dashboards | Splunk 9.4.2
Windows Security Monito
Search | Splunk 9.4.2
Windows Security Monito
127.0.0.1:8000/en-US/app/search/_windows_security_monitorings?form.global_time.earliest=-24h%40h&form.global_time.latest=now&tab=layout_1
splunk>enterprise
Apps ▾
Administrator ▾
Messages ▾
Settings ▾
Activity ▾
Help ▾
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Display ▾
Actions ▾
Edit

Windows Security Monitorings

Global Time Range: Last 24 hours

Failed Login Panel

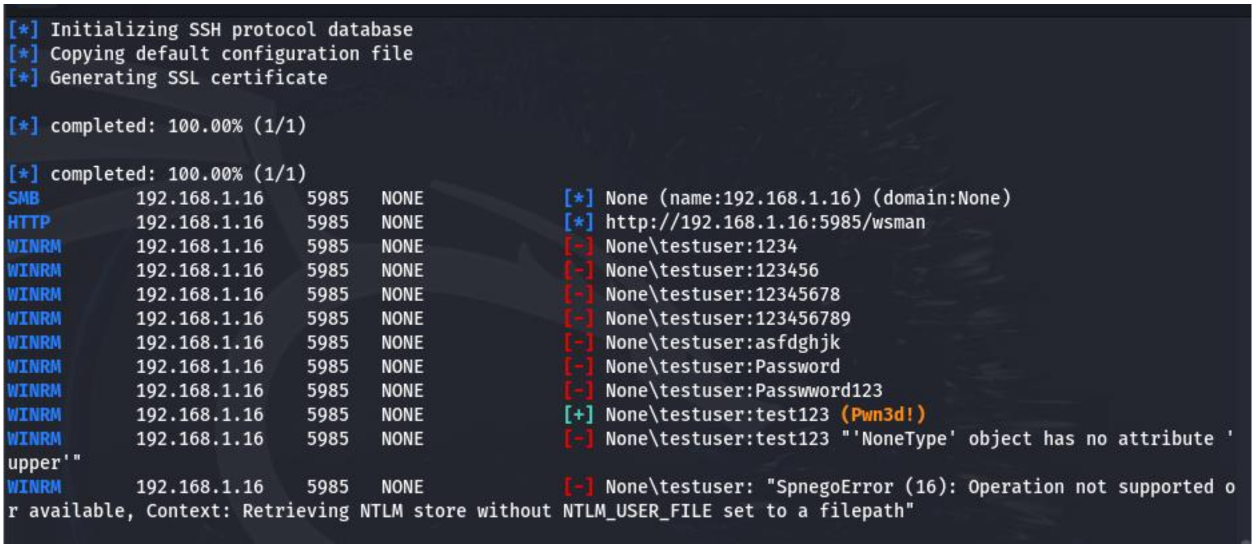
Account_Name	host	count
DESKTOP-PERTPN8$	win10vm	1
windows	win10vm	1

Successful Login Panel

Account_Name	host	count
-	win10vm	1
DESKTOP-PERTPN8$	win10vm	41
DWM-1	win10vm	2
LOCAL SERVICE	win10vm	1
NETWORK SERVICE	win10vm	1
SYSTEM	win10vm	31
SplunkForwarder	win10vm	1

Logins Over Time

Try to brutforce:



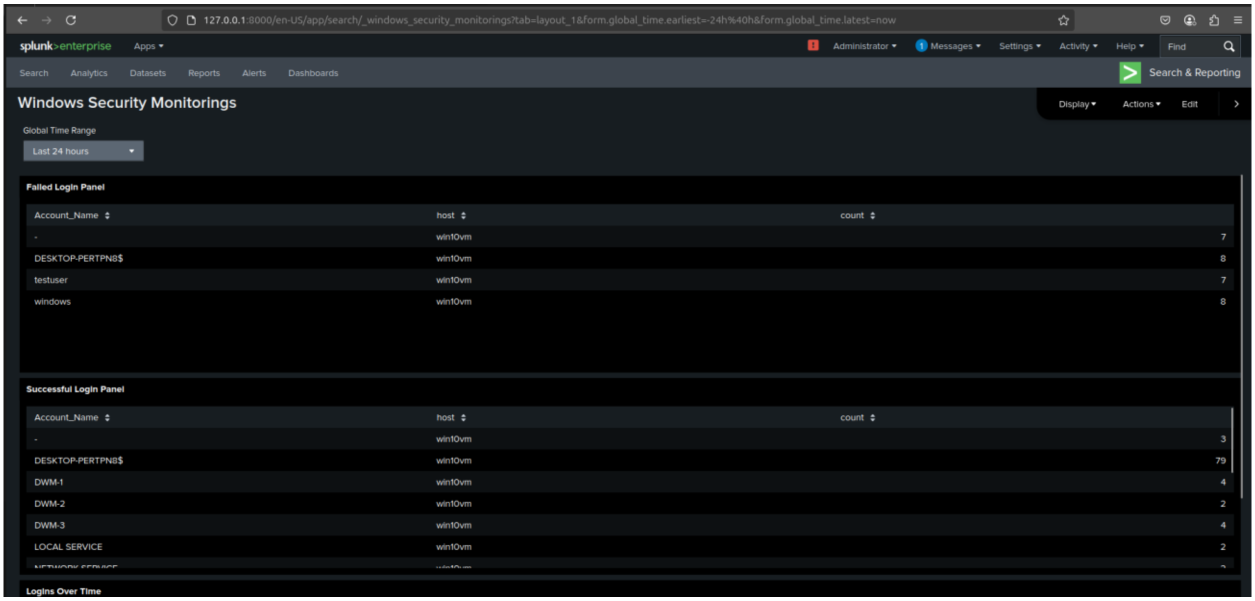
```
[*] Initializing SSH protocol database
[*] Copying default configuration file
[*] Generating SSL certificate

[*] completed: 100.00% (1/1)

[*] completed: 100.00% (1/1)
SMB         192.168.1.16    5985   NONE             [*] None (name:192.168.1.16) (domain:None)
HTTP        192.168.1.16    5985   NONE             [*] http://192.168.1.16:5985/wsman
WINRM       192.168.1.16    5985   NONE             [-] None\testuser:1234
WINRM       192.168.1.16    5985   NONE             [-] None\testuser:123456
WINRM       192.168.1.16    5985   NONE             [-] None\testuser:12345678
WINRM       192.168.1.16    5985   NONE             [-] None\testuser:123456789
WINRM       192.168.1.16    5985   NONE             [-] None\testuser:asfdghjk
WINRM       192.168.1.16    5985   NONE             [-] None\testuser:Password
WINRM       192.168.1.16    5985   NONE             [-] None\testuser:Passwword123
WINRM       192.168.1.16    5985   NONE             [+] None\testuser:test123 (Pwn3d!)
WINRM       192.168.1.16    5985   NONE             [-] None\testuser:test123 "'NoneType' object has no attribute '
upper'"
WINRM       192.168.1.16    5985   NONE             [-] None\testuser: "SpnegoError (16): Operation not supported o
r available, Context: Retrieving NTLM store without NTLM_USER_FILE set to a filepath"
```

Response:

- Brut force detection



127.0.0.1:8000/en-US/app/search/_windows_security_monitorings?tab=layout_1&form.global_time.earliest=-24h%40h&form.global_time.latest=now

Windows Security Monitorings

Global Time Range: Last 24 hours

Failed Login Panel

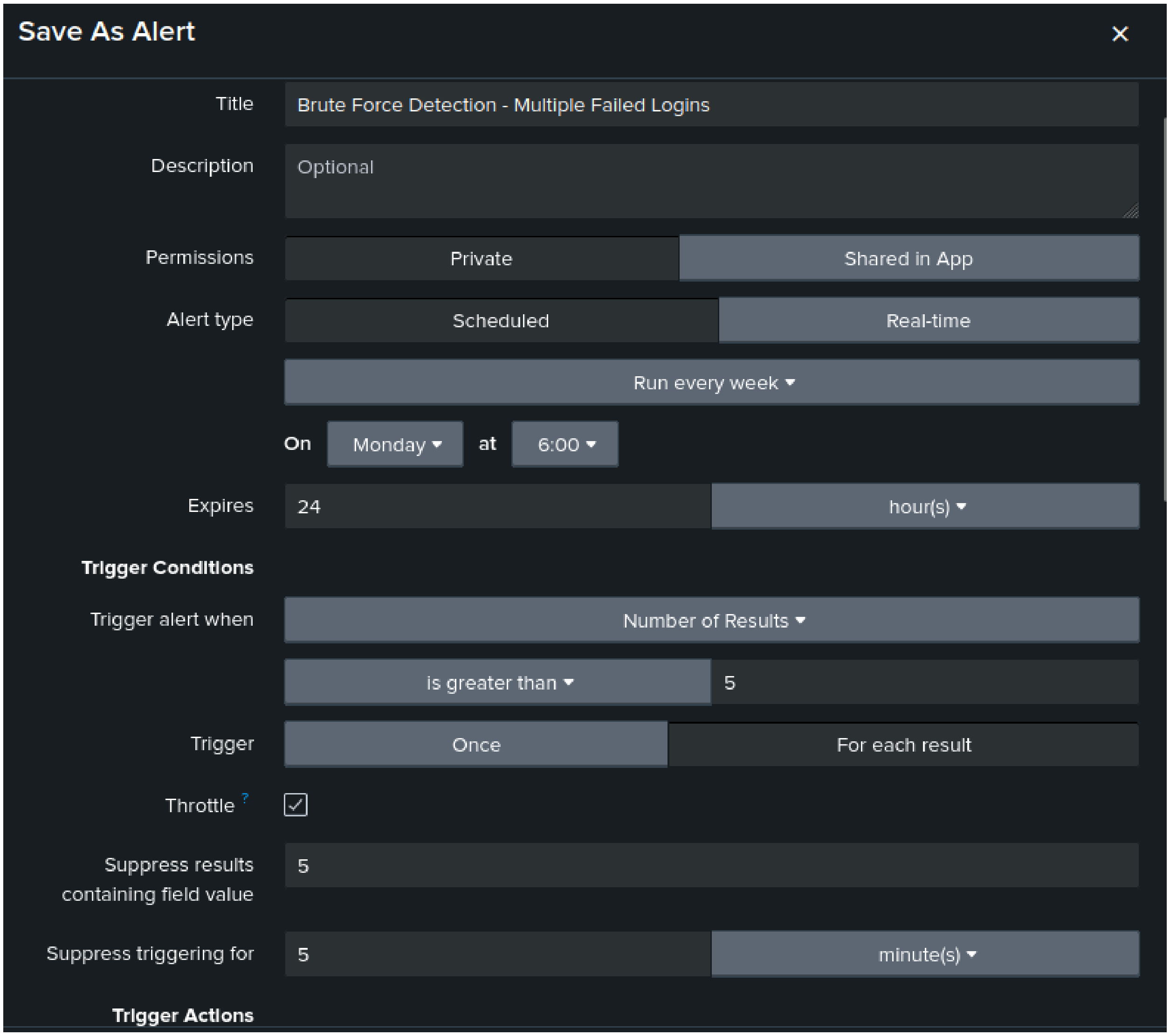
Account_Name	host	count
-	win10vm	7
DESKTOP-PERTPN8$	win10vm	8
testuser	win10vm	7
windows	win10vm	8

Successful Login Panel

Account_Name	host	count
-	win10vm	3
DESKTOP-PERTPN8$	win10vm	79
DWM-1	win10vm	4
DWM-2	win10vm	2
DWM-3	win10vm	4
LOCAL SERVICE	win10vm	2
NETWORK SERVICE	win10vm	[illegible]

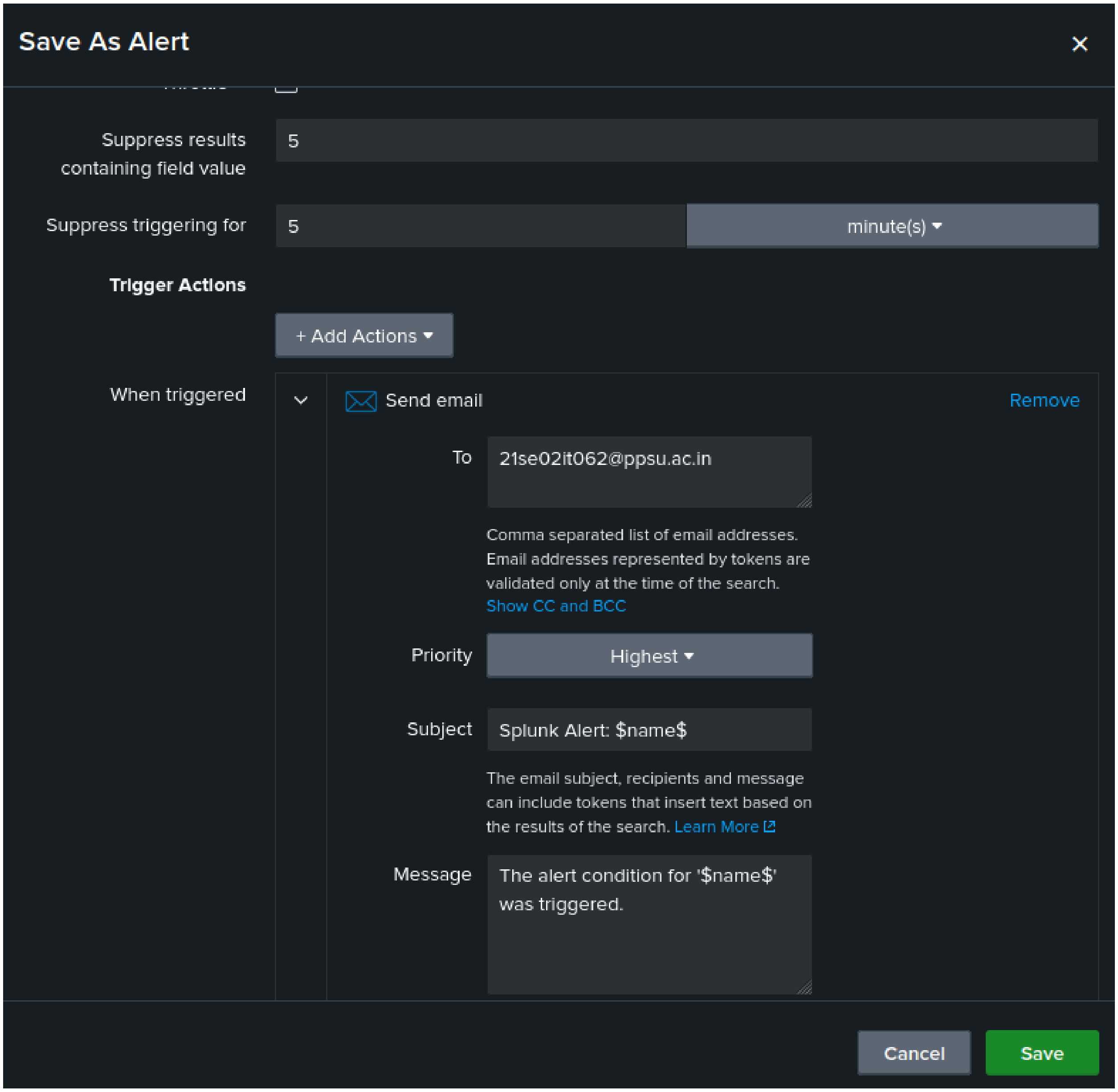
Logins Over Time

Create alert:



Save As Alert

Title	Brute Force Detection - Multiple Failed Logins
Description	Optional
Permissions	Private / Shared in App
Alert type	Scheduled / Real-time
	Run every week ▾
	On Monday ▾ at 6:00 ▾
Expires	24 hour(s) ▾
Trigger Conditions	
Trigger alert when	Number of Results ▾
	is greater than ▾ 5
Trigger	Once / For each result
Throttle ?	☑
Suppress results containing field value	5
Suppress triggering for	5 minute(s) ▾
Trigger Actions	



Save As Alert

Suppress results containing field value: 5

Suppress triggering for: 5 minute(s)

Trigger Actions

When triggered: Send email

To: 21se02it062@ppsu.ac.in

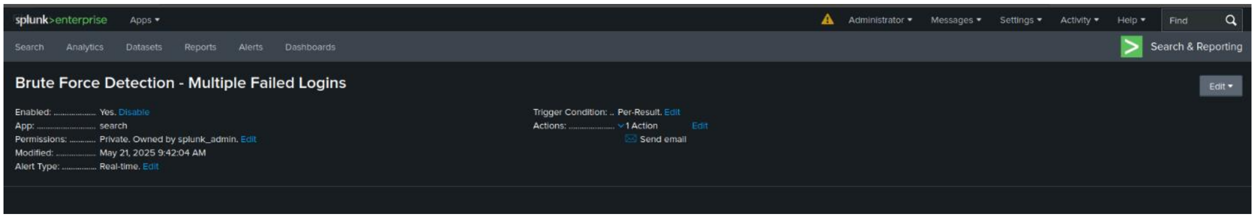
Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search.

Priority: Highest

Subject: Splunk Alert: $name$

The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

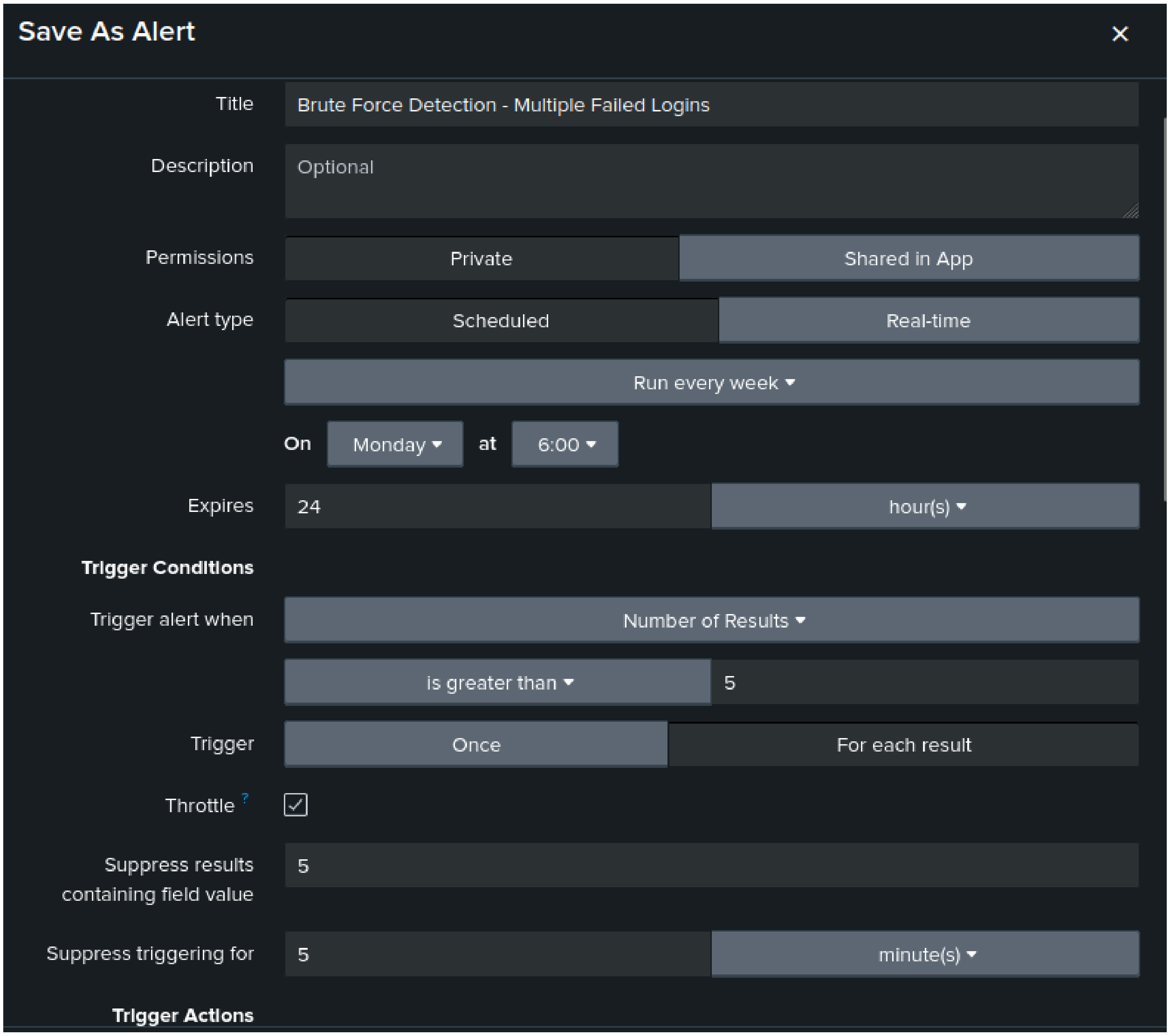
Message: The alert condition for '$name$' was triggered.



Brute Force Detection - Multiple Failed Logins

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by splunk_admin. Edit
Modified: .... May 21, 2025 9:42:04 AM
Alert Type: .... Real-time. Edit

Trigger Condition: .. Per-Result. Edit
Actions: .... 1 Action Edit
Send email



Save As Alert

Title: Brute Force Detection - Multiple Failed Logins

Description: Optional

Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every week

On Monday at 6:00

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Number of Results

is greater than 5

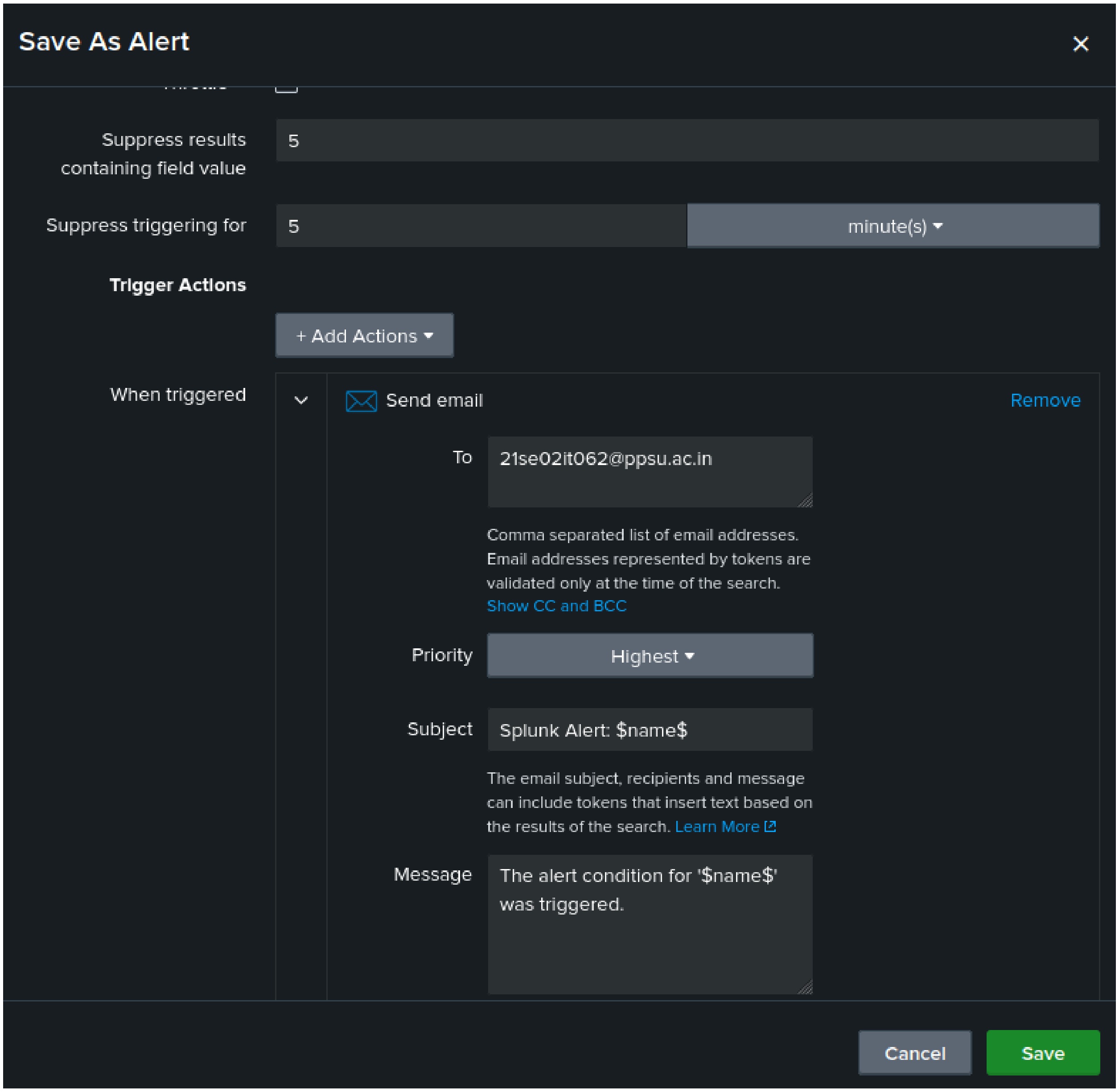
Trigger: Once | For each result

Throttle ? ☑

Suppress results containing field value: 5

Suppress triggering for: 5 minute(s)

Trigger Actions



Suppress results containing field value: 5

Suppress triggering for: 5 minute(s)

Trigger Actions

+ Add Actions

When triggered: Send email — Remove

To: 21se02it062@ppsu.ac.in

Comma separated list of email addresses. Email addresses represented by tokens are validated only at the time of the search. Show CC and BCC

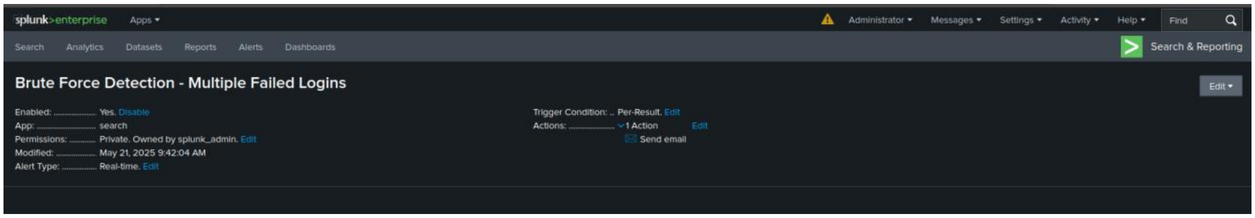
Priority: Highest

Subject: Splunk Alert: $name$

The email subject, recipients and message can include tokens that insert text based on the results of the search. Learn More

Message: The alert condition for '$name$' was triggered.

Set Alert:



Brute Force Detection - Multiple Failed Logins

Enabled: .... Yes. Disable
App: .... search
Permissions: .... Private. Owned by splunk_admin. Edit
Modified: .... May 21, 2025 9:42:04 AM
Alert Type: .... Real-time. Edit

Trigger Condition: .. Per-Result. Edit
Actions: .... 1 Action Edit
Send email