

# New Search

```
index=_audit action="search" user="kimjoe" "botsv3"
| table _time user action search
| sort - _time
```

Time range: All time

✓ **1,848 events** (before 15/12/2025 09:58:33.000)      No Event Sampling

## Statistics (1,848)






	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1	2025-12-02 03:00:28.2	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	84	e	h	="ConsoleLogin"   search *MFA*   head 5   table _time, event
0				Name, additionalEventData.*'
1				
1	2025-12-02 03:00:09.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail   search *MFA
4	90	e	h	*   fieldsummary   search field="*MFA*"'
0				
2				
1	2025-12-02 02:59:59.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail   search *MFA
4	14	e	h	*   fieldsummary   search field="*MFA*"'
0				
3				

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1404	2025-12-02 02:54:09.4	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"'
1305	2025-12-02 02:54:04.8	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"'
6406	2025-12-02 02:53:09.3	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where additionalEventData.MFAUsed="yes"   head 3   table _time, eventName, additionalEventData.MFAUsed'
7707	2025-12-02 02:52:51.8	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where additionalEventData.MFAUsed="yes"   head 3   table _time, eventName, additionalEventData.MFAUsed'
2208	2025-12-02 02:52:39.4	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where additionalEventData.MFAUsed="No"   head 3   table _time, eventName, additionalEventData.MFAUsed'
0709	2025-12-02 02:52:32.5	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where additionalEventData.MFAUsed="No"   head 3   table _time, eventName, additionalEventData.MFAUsed'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1 4 1 0	2025-12-02 02:52:09.3 60	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA* OR *mfa*   head 10   fieldsummary   search field="*MFA*"   table field, count'
1 4 1 1	2025-12-02 02:51:43.9 91	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA* OR *mfa*   head 10   fieldsummary   search field="*MFA*"   table field, count'
1 4 1 2	2025-12-02 02:51:39.4 83	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA* OR *mfa*   head 10   fieldsummary   search field="*MFA* OR *mfa*"   table field, count'
1 4 1 3	2025-12-02 02:51:39.4 70	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA* OR *mfa*   head 10   fieldsummary   search field="*MFA*"   table field, count'
1 4 1 4	2025-12-02 02:51:39.4 55	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA* OR *mfa*   head 5   fieldsummary   search field="*MFA*"   table field, count'
1 4 1 5	2025-12-02 02:51:36.9 24	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA* OR *mfa*   head 10   fieldsummary   search field="*MFA* OR *mfa*"   table field, count'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
14616	2025-12-02 02:51:16.401	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA* OR *mfa*   head 10   fieldsummary   search field="*MFA*"   table field, count'
14617	2025-12-02 02:51:10.014	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA* OR *mfa*   head 5   fieldsummary   search field="*MFA*"   table field, count'
14618	2025-12-02 02:51:09.374	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA* OR *mfa*   head 2   fieldsummary   search field="*MFA*"   table field, count'
14619	2025-12-02 02:51:09.357	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA* OR *mfa*   head 1   fieldsummary   search field="*MFA*"   table field, count'
14620	2025-12-02 02:51:03.216	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA* OR *mfa*   head 2   fieldsummary   search field="*MFA*"   table field, count'
14621	2025-12-02 02:50:54.212	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA* OR *mfa*   head 1   fieldsummary   search field="*MFA*"   table field, count'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1	2025-12-02 02:50:39.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	63	e	h	= "ConsoleLogin"   search *MFA*   head 1   fieldsummary   sea
2				rch field="*MFA*"   table field, count'
2				
1	2025-12-02 02:50:39.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	51	e	h	= "ConsoleLogin"   search *MFA* or *mfa*   head 1   fieldsumm
2				ary   search field="*MFA*"   table field, count'
3				
1	2025-12-02 02:50:39.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	39	e	h	= "ConsoleLogin"   search *MFA* or   head 1   fieldsummary
2				search field="*MFA*"   table field, count'
4				
1	2025-12-02 02:50:38.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	63	e	h	= "ConsoleLogin"   search *MFA*   head 1   fieldsummary   sea
2				rch field="*MFA*"   table field, count'
5				
1	2025-12-02 02:50:28.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	41	e	h	= "ConsoleLogin"   search *MFA* or *mfa*   head 1   fieldsumm
2				ary   search field="*MFA*"   table field, count'
6				
1	2025-12-02 02:50:17.9	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	20	e	h	= "ConsoleLogin"   search *MFA* or   head 1   fieldsummary
2				search field="*MFA*"   table field, count'
7				











	 _time	 user	 action	 search	
1	2025-12-02 02:50:09.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName	
4	31	e	h	= "ConsoleLogin"   search *MFA*   head 1   fieldsummary   sea	
2				rch field="*MFA*"   table field, count'	
8					
1	2025-12-02 02:50:09.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName	
4	16	e	h	= "ConsoleLogin"   stats values(additionalEventData.MFAUsed)	
2				as MFA_Values, count by eventName   where MFA_Values="No"	
9				head 10'	
1	2025-12-02 02:50:07.0	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName	
4	47	e	h	= "ConsoleLogin"   search *MFA*   head 1   fieldsummary   sea	
3				rch field="*MFA*"   table field, count'	
0					
1	2025-12-02 02:49:55.1	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName	
4	91	e	h	= "ConsoleLogin"   stats values(additionalEventData.MFAUsed)	
3				as MFA_Values, count by eventName   where MFA_Values="No"	
1				head 10'	
1	2025-12-02 02:49:09.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail   stats value	
4	19	e	h	s(additionalEventData.MFAUsed) AS MFAUsed, values(userIdenti	
3				ty.sessionContext.attributes.mfaAuthenticated) AS mfaAuthent	
2				icated'	
1	2025-12-02 02:49:06.5	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail   stats value	
4	65	e	h	s(additionalEventData.MFAUsed) AS MFAUsed, values(userIdenti	
3				ty.sessionContext.attributes.mfaAuthenticated) AS mfaAuthent	
3				icated'	

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
143	2025-12-02 02:48:39.386	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail   fieldsummary   search field="*mfa*" OR field="*MFA*"   table field, count'
144	2025-12-02 02:48:27.685	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail   fieldsummary   search field="*mfa*" OR field="*MFA*"   table field, count'
145	2025-12-02 02:48:09.382	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail   search "MFA Used"   head 5   table _time, eventName, additionalEventData.MFAUsed'
146	2025-12-02 02:48:09.368	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated)   stats count by userIdentity.sessionContext.attributes.mfaAuthenticated'
147	2025-12-02 02:48:04.546	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail   search "MFA Used"   head 5   table _time, eventName, additionalEventData.MFAUsed'
148	2025-12-02 02:47:43.335	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(userIdentity.sessionContext.attributes.mfaAuthenticated)   stats count by userIdentity.sessionContext.attributes.mfaAuthenticated'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1440	2025-12-02 02:47:39.375	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   stats values(userIdentity.sessionContext.attributes.mfaAuthenticated) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
1441	2025-12-02 02:47:11.589	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   stats values(userIdentity.sessionContext.attributes.mfaAuthenticated) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
1442	2025-12-02 02:47:09.406	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   stats values(userIdentity.sessionContext.attributes.mfaAuthenticated) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
1443	2025-12-02 02:46:46.350	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   stats values(userIdentity.sessionContext.attributes.mfaAuthenticated) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
1444	2025-12-02 02:46:09.358	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA*   head 1   fieldsummary   search field="*MFA*"   table field, count'
1445	2025-12-02 02:45:40.426	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   search *MFA*   head 1   fieldsummary   search field="*MFA*"   table field, count'



	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1 4 4 6	2025-12-02 02:45:39.3 76	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
1 4 4 7	2025-12-02 02:45:09.1 58	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   stats values(additionalEventData.MFAUsed) as MFA_Values, count by eventName   where MFA_Values="No"   head 10'
1 4 4 8	2025-12-02 02:42:39.5 12	kimjo e	searc h	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\"ConsoleLogin\" a" max_time="1" count="50" use_cache=1'
1 4 4 9	2025-12-02 02:42:39.5 01	kimjo e	searc h	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\"ConsoleLogin\" addi" max_time="1" count="50" use_cache=1'
1 4 5 0	2025-12-02 02:42:39.4 88	kimjo e	searc h	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\"ConsoleLogin\" additionalEventData" max_time="1" count="50" use_cache=1'
1 4 5 1	2025-12-02 02:42:39.4 79	kimjo e	searc h	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NOT eventName=\"ConsoleLogin\" additionalEventData.MFAUsed" max_time="1" count="50" use_cache=1'

	 _time 	 user 	 action  	 search  
1	2025-12-02 02:42:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	69	e	h	="ConsoleLogin"   search *MFA*   head 1   fieldsummary   sea
5				rch field="*MFA*"   table field, count'
2				
1	2025-12-02 02:42:18.7	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	67	e	h	="ConsoleLogin"   search *MFA*   head 1   fieldsummary   sea
5				rch field="*MFA*"   table field, count'
3				
1	2025-12-02 02:42:09.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail   foreach *
4	17	e	h	[eval <<FIELD>>_exists = if(isnotnull('
5				
4				
1	2025-12-02 02:42:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	61	e	h	="ConsoleLogin" additionalEventData.MFAUsed=*   stats count
5				by additionalEventData.MFAUsed'
5				
1	2025-12-02 02:42:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	49	e	h	="ConsoleLogin" additionalEventData.MFAUsed=*'
5				
6				
1	2025-12-02 02:41:55.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail   foreach *
4	22	e	h	[eval <<FIELD>>_exists = if(isnotnull('
5				
7				

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1	2025-12-02 02:41:44.0	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	65	e	h	="ConsoleLogin" additionalEventData.MFAUsed=*   stats count
5				by additionalEventData.MFAUsed'
8				
1	2025-12-02 02:41:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	54	e	h	="ConsoleLogin" additionalEventData.MFAUsed=*
5				
9				
1	2025-12-02 02:41:39.4	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	35	e	h	="ConsoleLogin"'
6				
0				
1	2025-12-02 02:41:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	64	e	h	="ConsoleLogin" additionalEventData.MFAUsed=*
6				
1				
1	2025-12-02 02:41:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	63	e	h	="ConsoleLogin" additionalEventData.MFAUsed=*
6				
2				
1	2025-12-02 02:41:37.2	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	53	e	h	="ConsoleLogin" additionalEventData.MFAUsed=*
6				
3				

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1	2025-12-02 02:41:23.7	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	36	e	h	="ConsoleLogin" '
6				
4				
1	2025-12-02 02:41:22.7	kimjo	searc	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO
4	75	e	h	T eventName=\"ConsoleLogin\" a" max_time="1" count="50" use_
6				cache=1 '
5				
1	2025-12-02 02:41:22.3	kimjo	searc	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO
4	42	e	h	T eventName=\"ConsoleLogin\" addi" max_time="1" count="50" u
6				se_cache=1 '
6				
1	2025-12-02 02:41:21.8	kimjo	searc	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO
4	74	e	h	T eventName=\"ConsoleLogin\" additionalEventData" max_time
6				="1" count="50" use_cache=1 '
7				
1	2025-12-02 02:41:21.4	kimjo	searc	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail NO
4	32	e	h	T eventName=\"ConsoleLogin\" additionalEventData.MFAUsed" ma
6				x_time="1" count="50" use_cache=1 '
8				
1	2025-12-02 02:41:15.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
4	69	e	h	="ConsoleLogin" additionalEventData.MFAUsed=*
6				
9				

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1 4 7 0	2025-12-02 02:41:09.3 32	kimjo e	searc h	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" max_time="1" count="50" use_cache=1'
1 4 7 1	2025-12-02 02:40:39.4 89	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)'
1 4 7 2	2025-12-02 02:40:39.4 77	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
1 4 7 3	2025-12-02 02:40:39.4 64	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"'
1 4 7 4	2025-12-02 02:40:39.3 95	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"'
1 4 7 5	2025-12-02 02:40:37.7 65	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1 4 7 6	2025-12-02 02:40:31.3 37	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
1 4 7 7	2025-12-02 02:40:26.7 48	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"'
1 4 7 8	2025-12-02 02:40:17.2 48	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"'
1 4 7 9	2025-12-02 02:40:09.3 19	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
1 4 8 0	2025-12-02 02:40:09.3 07	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
1 4 8 1	2025-12-02 02:40:04.4 56	kimjo e	searc h	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1	2025-12-02 02:39:40.8	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail eventName="Co
4	23	e	h	nsoleLogin"   where isnotnull(additionalEventData.MFAUsed)
8				stats count by additionalEventData.MFAUsed'
2				
1	2025-12-02 02:39:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName=
4	97	e	h	"ConsoleLogin"   where isnotnull(additionalEventData.MFAUse
8				d)   stats count by additionalEventData.MFAUsed'
3				
1	2025-12-02 02:39:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName=
4	81	e	h	"ConsoleLogin"   where isnotnull(additionalEventData.MFAUse
8				d)   stats count by additionalEventData.MFAUsed'
4				
1	2025-12-02 02:39:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName=
4	68	e	h	"ConsoleLogin"   where isnotnull(additionalEventData.MFAUse
8				d)   stats count by additionalEventData.MFAUsed'
5				
1	2025-12-02 02:39:39.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName=
4	56	e	h	"ConsoleLogin"   where isnotnull(additionalEventData.MFAUse
8				d)   stats count by additionalEventData.MFAUsed'
6				
1	2025-12-02 02:39:39.2	kimjo	searc	'typeahead prefix="index=botsv3 sourcetype=aws:cloudtrail" m
4	88	e	h	ax_time="1" count="50" use_cache=1'
8				
7				

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
148	2025-12-02 02:39:21.858	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
149	2025-12-02 02:39:19.357	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
150	2025-12-02 02:39:17.236	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
151	2025-12-02 02:39:14.093	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
152	2025-12-02 02:39:09.331	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
153	2025-12-02 02:39:09.320	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" additionalEventData.MFAUsed=*   stats count by additionalEventData.MFAUsed'



	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
149	2025-12-02 02:39:07.654	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
149	2025-12-02 02:38:46.929	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin" additionalEventData.MFAUsed=*   stats count by additionalEventData.MFAUsed'
149	2025-12-02 02:38:39.325	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
149	2025-12-02 02:38:20.626	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
149	2025-12-02 02:38:09.325	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'
149	2025-12-02 02:38:03.457	kimjoe	search	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName="ConsoleLogin"   where isnotnull(additionalEventData.MFAUsed)   stats count by additionalEventData.MFAUsed'

	<div><div>_time</div><div></div></div>	<div><div>user</div><div></div></div>	<div><div>action</div><div></div></div>	<div><div>search</div><div></div></div>
1	2025-12-02 02:37:09.3	kimjo	searc	'search index=botsv3 sourcetype=aws:cloudtrail NOT eventName
5	03	e	h	= "ConsoleLogin"   search *MFA*   head 5   table _time, event
0				Name, additionalEventData.*'
0				