

Integration Guide

Integrating JumpCloud with EventTracker

EventTracker v9.3 and above

Publication Date:

April 28, 2021

© Copyright Netsurion. All Rights Reserved.



Abstract

This guide helps you in configuring **JumpCloud** with EventTracker to receive **JumpCloud** events. In this guide, you will find the detailed procedures required for monitoring **JumpCloud**.

Scope

The configuration details in this guide are consistent with EventTracker version v9.3x or above and JumpCloud.

Audience

Administrators, who are assigned the task to monitor and manage JumpCloud events using EventTracker.



Table of Contents

1	Ove	rview	4
2	Prei	requisites	4
3	Inte	gration of JumpCloud with EventTracker	4
	3.1	Getting JumpCloud API key	4
	3.2	Integrating JumpCloud to EventTracker	5
4	Eve	ntTracker Knowledge Pack	6
	4.1	Category	6
	4.2	Alert	6
	4.3	Report	7
	4.4	Dashboards	10
5	Imp	orting JumpCloud Knowledge Pack into EventTracker	15
	5.1	Category	16
	5.2	Alert	17
	5.3	Knowledge Object	18
	5.4	Report	20
	5.5	Dashboards	21
6	Ver	ifying JumpCloud Knowledge Pack in EventTracker	23
	6.1	Category	23
	6.2	Alert	24
	6.3	Knowledge Object	25
	6.4	Report	25
	6.5	Dashboards	26
	About	Netsurion	28
	Conta	ct Us	28

1 Overview

JumpCloud is a Directory-as-a-Service (DaaS) solution that customers use to authenticate, authorize, manage users, devices, and applications. JumpCloud provides directory, system (Mac, Linux and Windows), Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial-In User Service (RADIUS), Single sign-on (SSO), Mobile Device Management (MDM) events.

EventTracker helps to monitor events from JumpCloud. Its built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

2 Prerequisites

- EventTracker v9.3x or above should be installed.
- JumpCloud should be configured.
- Admin permission should be there for configuring JumpCloud API.
- Local admin permissions for the workstation.
- **PowerShell 5.0** should be installed on the EventTracker Manager.

3 Integration of JumpCloud with EventTracker

3.1 Getting JumpCloud API key

- 1. Login to the <u>Jumpcloud</u> admin portal.
- 2. Go to the username drop down located in the top-right of the portal.



	API Key	×							
4378637	ad624b2d500de627f6e9799b2eb135e00	þ							
Generating a new Af will render all calls u	Generate New API Key Generating a new API key will revoke access to the current API key. This will render all calls using the previous API key inaccessible.								
		close							

• Retrieve your API key from API Settings.

3.2 Integrating JumpCloud to EventTracker

1. Download the JumpCloudintegrator on EventTracker manager/EventTracker agent machine from below link:

https://downloads.eventtracker.com/kp-integrator/JumpCloudIntegrator.exe

- 2. Run the downloaded JumpCloudIntegration.exe. Integration window opens.
- 3. Provide your API key retrieved earlier from JumpCloud console.
- 4. Click Validate.

JumpCloud Integrator	r		-	×
API Key				
		Validate		
-	Finish	Cancel		
-	1 111311	Cancer		

5. Once validated, click Finish.



4 EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support JumpCloud.

4.1 Category

- JumpCloud: Directory Command and Policy Events This category provides information related to command management events, policy management events, file management events, IP list management events.
- JumpCloud: Login Success Events This category provides information related to all the successful login events to user portal, systems (Mac, OS, Linux), RADIUS server, LDAP and SSO application.
- JumpCloud: Login Failure Events This category provides information related to all the login failure events to user portal, systems (Mac, OS, Linux), RADIUS server, LDAP and SSO application.
- **JumpCloud: Directory Integration Events** This category provides information related to active directory events, ids resource events, samba domain events, workday and integration events.
- JumpCloud: Directory User and Admin Events This category provides information related to all user and admin management events.
- JumpCloud: Directory Object Events This category provides information related to directory application, group, translation rule, system, organization, notification and RADIUS server management events.
- JumpCloud: System Events- This category provides information related to user lockout, password change and other system (Mac, Linux, Windows) events.
- JumpCloud: LDAP and MDM Events: This category provides information about LDAP search events and MDM command result.

4.2 Alert

- JumpCloud: Login Failure Events- This alert is generated when any login failure is detected on JumpCloud user portal, LDAP directory server, SSO application, system (Mac, Linux, Windows), RADIUS server.
- JumpCloud: User Granted Admin Privilege This alert is generated when any user is granted admin sudo privileges on devices by admin. This action will give the user access to create accounts and amend system settings.
- JumpCloud: Active Directory Deleted This alert is generated when an active directory is deleted.
- JumpCloud: Admin Created This alert is generated when an admin is created. Admin account has privilege to amend setting affecting the whole organization and should be monitored closely.
- JumpCloud: System Deleted This alert is generated when any system is deleted in directory.
- JumpCloud: User Account Deleted This alert is generated when any user is deleted.
- JumpCloud: User Account Locked or Suspended This alert is generated when any user account is locked or suspended. Lockout or account suspension should be monitored as it can be a result of brute force attack.



4.3 Report

JumpCloud: Directory Command and Policy Event Report- This report gives the information about the directory command, policy, file, IP list events. Reports contains IP address, username, organization id, log type and other fields which will be helpful for further investigation.

LogTime	Computer	Username	User Type	Client IP	Event Type	Country Code	Region Name	GeolP	Changes	Resource	Auth Method	Organization Id	Useragent
04/22/2021 10:51:54 PM	test_system	sg@cosdfj.org.com	admin	103300300300	command_create	N	Karnataka	"tmezone":"Asia/Kokata","lattude 12.9833,"country_code2":"N","con tinent_code":"AS","region_name"." Kamataka","region_code"."KA","lo	: ("field":"name","to":"Netstat"),("field ":"trigger","to":""},("field":"command ","to":"Netstat"),("field":"commandT ype","to":"windows?),("field":"com	"name":"Netstat","type":"command"	session	605b62ccfc846c33ab2724c0	"patch":"4430","os":"Windows"," nor":"0","major":"90","build":"","n e":"Chrome","os_name":"Window ,"device":"Other"
04/22/2021 10:51:54 PM	test_system	sg@cosdfj.org.com	admin	103300300300	command_create	N	Karnataka	"tmezone":"Asia/Kokata", "attude 12.9833,"country_code2":"N","con tinent_code":"AS", "region_name"." Kamataka", "region_code"."KA","lo	: ("field":"name","to":"Netstat"),("field ":"trigger","to":""},("field":"command ","to":"Netstat"),("field":"commandT ype","to":"windows"),("field":"com	"name":"Nelstat", "type":"command"	session	605b62ccfc846c33ab2724c0	"patch":"4430","os":"Windows"," nor":"0","major":"90","build":"","n e":"Chrome","os_name":"Window ,"device":"Other"
04/22/2021 10:52:01 PM	test_system	sg@cosdfj.org.com	admin	103300300300	command_run	N	Karnataka	"tmezone":"Asia/Kokata","lettude 12.9833,"country_code2":"N","cor tinent_code":"AS","region_name". Kamataka","longhude":77.5833,"re		"name":"Netstat","id":"6082607adfc af16ff8f5838e","type":"command"	session	605b62ccfc846c33ab2724c0	"patch":"4430","minor":"0","major 90","os":"Windows","build":"","në e":"Chrome","os_name":"Window ,"device":"Other"

Logs Considered



 JumpCloud: Login Success Detected Report - This report gives the information about all the successful login events to user portal, systems (Mac, OS, Linux), RADIUS server, LDAP and SSO application. Reports contains username, IP address, organization ID, log type, location details, etc. which can be used for further investigation.

LTime	Computer	05	-	010	1174	Occurring the	Deserve News	Desire None	6	TIATALELA		
Lognine	computer	Cilentip	Event Type	Geoip	MFA	organization id	Process name	Region Name	Service	TLS Established	user type	Username
04/22/2021 09:57:57 PM	test_system	182.xx.xx.xx	login_attempt	"country_code":"N","timezone":"A: ia/Kolkata","lattude":20.0,"continen _code":"AS","longitude":77.0	s t	605b62ccfc846c33ab2724c0	C:\\Windows\\System32\\ wininit.exe		systems		user	UMFD-0
04/22/2021 09:57:57 PM	test_system	182.xx.xx.xx	login_attempt	"country_code":"N","timezone":"As ia/Kokata","latitude":20.0,"continen _code":"AS","longitude":77.0	s t	605b62ccfc846c33ab2724c0	C:\\Windows\\System32\\ winlogon.exe		systems		user	DWM-1
04/22/2021 09:57:57 PM	test_system	182.00.00	login_attempt	"country_code":"N","timezone":"As ia/Kokata","lattude":20.0,"continen _code":"AS","longtude":77.0	s t	605b62ccfc846c33ab2724c0			systems		user	SYSTEM



Logs Considered

{"initiated_by":{"id":"605b62ccfc846c33ab2724bf","type":"admin","email":"jds@ cosdfhy.org"},"geoip":{"timezone":"Asia/Kolkata","latitude":12.9833,"country_c ode2":"IN","continent_code":"AS","region_name":"Karnataka","region_cbde":" KA","longitude":77.5833},"mfa":false,"event_type":"admin_login_attempt","provi der":null,"success":true,"service":"directory","organization":"605b62ccfc846c33 ab2724c0","@version":"1","client_ip":"106.xx.xx.xx","id":"608273997aab62048f 3fd3c9","user_agent":{"patch":"4430","os":"Windows","major":"90","minor":"0", "build":"","name":"Chrome","os_name":"Windows","device":"Other"},"timestam p":"2021-04-23T07:13:29.394Z"}

 JumpCloud: Login Failure Events – This report gives the information about all the login failure events to user portal, systems (Mac, OS, Linux), RADIUS server, LDAP and SSO application. Reports contains username, IP address, organization ID, log type, location details, etc. which can be used for further investigation.

LogTime	Computer	Process Name	Service	User Type	Username	Hostname	GealP	Client IP	Organization Id	Event Type
0422/2021 10:01:41 PM	test_system	C:11Windows11System321isvchost xe	ie systems	user	DemoEventTracker	DESKTOP-EJ8F2TN	"country_code":"N","timezone":"/ iaKokata","lattude":20.0,"contine _code":"AS","longitude":77.0	is 182.oc.oc.oc nt	605b62ccfc846c33ab2724c0	login_attempt
04/22/2021 10:01:41 PM	test_system	C:1Windows1/System32liavchost xe	le systems	user	DemoEventTracker	DESKTOP-EJ8F2TN	"country_code":"N","timezone":"/ iaKokata","lattude":20.0,"contine _code":"AS","longitude":77.0	is 182.000000 nt	605b62ccfc846c33ab2724c0	login_attempt
04/22/2021 10:01:41 PM	test_system	C:11Windows11System321isvchost xe	le systems	USET	DemoEventTracker	DESKTOP-EJ8F2TN	"country_code":"N","timezone":"/ ia/Kokata","lattude":20.0,"contine _code":"AS","longitude":77.0	is 182.oc.oc.oc nt	605b62ccfc846c33ab2724c0	login_attempt

Logs Considered

{'initiated_by':{"id":"605b62ccfc846c33ab2724bf","type":"admin","email":"jds@cosdfhy.org"},"ge oip":{"timezone":"Asia/Kolkata","latitude":12.9833,"country_code2":"IN","continent_code":"AS"," region_name":"Karnataka","region_code":"KA","longitude":77.5833},"mfa":false,"event_type":"ad min_login_attempt","provider":null,"success":false,"service":"directory","organization":"605b62cc fc846c33ab2724c0","@version":"1","client_ip":"106.xx.xx.xx","id":"608273997aab62048f3fd3c9", "user_agent":{"patch":"4430","os":"Windows","major":"90","minor":"0","build":"","name":"Chrom e","os_name":"Windows","device":"Other"},"timestamp":"2021-04-23T07:13:29.394Z"}

• JumpCloud: Directory Integration Events – This report gives information about active directory events, ids resource events, samba domain events, workday and integration events. Report contains IP address, username, changes, resource, auth method, log type and other useful information.

 JumpCloud: Directory User and Admin Events - This report gives information regarding all user and admin management events such as create, update, delete, password expired, password reset, account locked, suspended among others. Reports contains IP address, log type, username and other useful information for further analysis.

LogTime	Computer	Auth Method	Client IP	Changes	Event Type	User Type	Username	Resource	Useragent	Region Name
04/22/2021 10:45:10 PM	test_system	session	103.00.000	{"field"."account_locked","to":false ,{"field"."activated","to":false},{"fie d"."addresses","to".[e) user_create I	admin	asfdsj@jhbfvc.org	"id":"60825ee57bf1f3092a54726f", "type":"user","username":"Captan. a"	"patch":"4430","os":"Windows","m ajor":"90","minor":"0","build":"","nan e":"Chrome","os_name":"Windows" ,"device":"Other"	Karnataka n
04/22/2021 10:45:10 PM	test_system	session	103.00.000	{"field":"account_locked","to":false ,{"field":"activated","to":false},{"fie d":"addresses","to":[e} user_create I	admin	asfdsj@jhbfvc.org	"d":'60825ee57bf1f3092a54726f", "type":"user","username":"Captan. a"	"patch":"4430","os":"Windows","m ajor":"90","minor":"0","build":"","nan e":"Chrome","os_name":"Windows" ,"device":"Other"	Karnataka
04/22/2021 10:45:10 PM	test_system	session	103.00.000	{"field":"account_locked","to":false ,{"field":"activated","to":false},{"fie d":"addresses","to":[e} user_create I	admin	asfdsjØjhbfvc.org	"id":"60825ee57bf1f3092a54726f", "type":"user","username":"Captan. a"	"patch":"4430","os":"Windows","m ajor":"90","minor":"0","build":"","nan e":"Chrome","os_name":"Windows" ,"device":"Other"	Karnataka
04/22/2021 10:45:10 PM	test_system	session	103.00.000	{"field"."account_locked","to":false ,{"field"."activated","to":false},{"fie d"."addresses","to":[e) user_delete I	admin	asfdsj@jhbfvc.org	"ld":"60825ee57bf1f3092a54726f", "type":"user","username":"Captan. a"	"patch":"4430","os":"Windows","m ajor":"90","minor":"0","build":"","nan e":"Chrome","os_name":"Windows" ,"device":"Other"	Karnataka n

Logs Considered

{'initiated_by'':{'id'.':605b62ccfc846c33ab2724bf', 'type''.'admin'', 'email''.''ajfjakd@msdlck.org'}, 'geoip':{'timezone''.'Asia/Kolkata'', 'latitude':12.9833, 'countr y_code2''.'IN'', 'continent_code''.'AS'', 'region_name''.'Karnataka', 'region_code''.'KA'', 'longitude''.77.5833}, 'resource'', '['d''':60825ee57bfff3092a54726f'', typ e''.'user', 'username''.'Captan.a'', 'changes': [{'field''.'account_locked'', 'to''.false}, {'field''.'attivated'', 'to''.false}, 'field''.'addresses, ''to'': []}, {'field''.'addresses, ''to'':]}, {'field''.'attivated'', 'to''.false}, 'field''.'addresses, ''to':]]}, {'field''.'attivates'', 'to''.'To''.'', {'field''.'attivated'', 'to''.false}, 'field''.'addresses, ''to'':]}, {'field''.'attivates'', 'to''.''', {'field''.'attivated'', 'to''.'''', {'field''.'attivated'', 'to''.''', {'field''''', 'astivated'', 'to''.''', {'field''''', 'astivated'', 'to''.''', {'field''''', 'astivated'', 'to''.''', {'field''''', 'astivated'', 'to''.'', 'astivated'', 'to''.''', {'field'''', 'astivated''', 'to''.''', {'field''''', 'astivated'', 'to''.''', 'astivated'', 'to''.'', 'astivated'', 'astivated'', 'astivated'', 'astiva

 JumpCloud: Directory Object Events - This report gives information regarding all directory application, group, translation rule, system, organization, notification and RADIUS server management events.

LogTime	Computer	Auth Method	Changes	Client IP	Country Code	Organization Id	OS Name	Region Name	Resource	User Type	Username	Result
04/22/2021 10:44:17 PM	test_system	session	{"feld":10",10":160825e005440646802752 16"};{"feld":1name",10":14dmin Group"};{"field":1type",10":1user_group"};{"t eld":1atributes";10";"(dapGroups";{"name"	103.00.0000 1	N	605b62ccfc846c33ab2724c0	Windows	Karnataka	"name":"Admin Group","d":"60825eb0b544064680 27521b","type":"user_group"	admin	dasfiltik@jksdhf.org	
04/22/2021 10:44:17 PM	test_system	session	{"feld":10","to":60825e005440646802752 1b"};{"feld":1name","to":"Admin Group");{"feld":1type","to":"user_group");{"t eld":1tributes";"to";"(dapGroups");{"name"	103.00.0000 1	N	605062ccfc846c33ab2724c0	Windows	Kamataka	"name":"Admin Group","d":"6082Seb0b544064b80 27521b","type":"user_group"	admin	dasfikhk@jksdhf.org	
04/22/2021 10:44:17 PM	test_system	session	("feld":10","to":60025eb0544064b802752 1b");{"feld":hame","to":"Admin Group");{"field":type","to":"user_group");{"t eld":"attributes";"to";"(dapGroups";["hame"	103.00.0000	N	605062ccfc846c33ab2724c0	Windows	Karnataka	"name":"Admin Group","d":"6082Seb0b544064680 27521b","type":"user_group"	admin	dasfitik@jisdhf.org	

Logs Considered

{"initiated_by":{"id":"605b62ccfc846c33ab2724bf","type":"admin","email":"adgsk@shfdjskh.com"},"geoip":{"timez one":"Asia/Kolkata","latitude":12.9833,"country_code2":"IN","continent_code":"AS","region_name":"Karnataka"," longitude":77.5833,"region_code":"KA"},"resource":{"name":"Admin Group","id":"60825eb0b544064b8027521b","type":"user_group"},"changes":[{"field":"id","to":"60825eb0b544064b 8027521b"},{"field":"name","to":"Admin Group",{"field":"type","to":"user_group"},{"field":"attributes","to":{"IdapGroups":[{"name":"Admin Group"},]}]},"auth_method":"session","event_type":"group_create","provider":null,"service":"directory","organizatio n":"605b62ccfc846c33ab2724c0","@version":"1","client_ip":"103.xx.xx.xx","id":"60825eb04ffd2e6affe6af7f","user _agent":{"patch":"4430","os":"Windows","major":"90","minor":"0","build":"","name":"Chrome","os_name":"Windo ws","device":"Other"},"timestamp":"2021-04-23T05:44:16.880Z"}

- JumpCloud: System Events This report gives information regarding user lockout, password change and other system(Mac, Linux, Windows) events. Reports contains IP address, log type, changes, resource, username and other useful information for further analysis.
- JumpCloud: LDAP and MDM Events This report gives information regarding LDAP search events and MDM command result.

4.4 Dashboards

• JumpCloud: User Login Failure by Geo Location







• JumpCloud: User Login Success by Geo Location



• JumpCloud: Login Failure by Username



• JumpCloud: Login Success by Username



• JumpCloud: User Management Events



• JumpCloud: Events by Service Type





• JumpCloud: Policy Management Events





• JumpCloud: System Login Detected by Logon_type

• JumpCloud: Elevated Privilege User Login Events







• JumpCloud: Login Success Without MFA

5 Importing JumpCloud Knowledge Pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Knowledge Object
- Report
- Dashboard
- 1. Launch EventTracker Control Panel.
- 2. Double click Export Import Utility.

63	Even	tTracker Contro	l Panel	– – X
		No.	Ev	entTracker
	= ?		•	
EventVault	Diagnostics	License Manager	Export Import Utility	Append Archives
00		X	*	
EventTracker Agent Confi	Traffic Analyzer	Agent Manageme	Port Configuration	TrapTracker
?	-63			
Change Audit	About EventTracker			
	E-mail: s	support@Event Tra	icker.com	

3. Click the **Import** tab.

5.1 Category

1. Click **Category** option, and then click the browse button.

	Export Import Utility
port Import	Source :
	Import

- 2. Locate Category_JumpCloud.iscat file, and then click the Open button.
- 3. To import categories, click the **Import** button.

EventTracker displays success message.

	Export Import Utility	x
0	Selected category details are imported successfully.	
	ОК	

4. Click **OK**, and then click the **Close** button.

5.2 Alert

1. Click **Alert** option, and then click the **browse** button.

9	Export In	nport Utility	- 🗆 X						
Export Import									
1. Provide the path and file name 2. Click the Import button.	of the Alerts file. Use the '' butt	on to browse and locate the import file.							
Options	Location								
Category	 Import E-mail settings 								
 Filters 	Set Active Only if notifications set	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on							
 Alerts 	 By default 	Active key available in the configuration section.							
Systems and Groups	Watchlist Configuration								
O Token Value	✓ Import Watchlist configuration								
⊖ Reports	Note: If this option is enabled the only for on the console where the alerts	or alerts which have Advanced watchlist configured he user should make sure the watchlist groups are a s are imported.	vailable						
Behavior Correlation									
	Source :								
	*.isalt								
		Import	Close						

- 2. Locate Alert_JumpCloud.isalt file, and then click the Open button.
- 3. To import alerts, click the **Import** button. EventTracker displays success message.



Export Import Utility
Selected alert configurations are imported successfully.
ОК

4. Click **OK**, and then click **Close**.

5.3 Knowledge Object

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.

≡	EventTracker @					.▲ Admin•	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩		_	Alerts	© Correlation	🔍 IP Lookup Configuration	🛱 Users	_
	0	1	Behavior Correlation Rules	Diagnostics	·@ Knowledge Objects	r Weights	
k			🇞 Behavior Correlation Settings	⊽ Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
				FAQ Configuration	Report Settings		
	Attacker			– News			

2. Click on **Import** ^T button as highlighted in the below image:

-	Knowledge Obj	jects		🕈 / Admin / Knowledge Objects
Q R	Search objects	Q	Q Activate Now	Objects 🕀 耳 🏦 🌣
UK.				
	Groups	🕀 🖉 🗓		±
	E Cylance			
	EventTracker			

3. Click on Browse.



Import		×
Select file	🗁 Browse Up	load
		Close

- 4. Locate the file named **KO_JumpCloud.etko**.
- 5. Select the check box and then click on \mathbb{T} Import option.

Import			×	
Select file			🖀 Browse Upload	
	Object name	Applies to	Group name	
	JumpCloud	JumpCloud	JumpCloud	
			Import Close	

6. Knowledge objects are now imported successfully.



5.4 Report

1. Click **Reports** option, and select **New (*.etcrx)** option.

 Provide the path and file na Click the Import button Note : If report(s) contains tem 	ime of Schedule Report file. Use the `' button to browse and locate the import file. splate, first import template and proceed with exportimport utility.
Options	Location
 Filters 	
 Alerts 	Legacy (*.issch) New (*.etcrx)
 Systems and Groups 	Source :
O Token Value	33601
 Reports 	
Behavior Correlation	

2. Locate the file named **Reports_JumpCloud.etcrx** and select the check box.

litle			Frequency Show all	- Q Q		
\checkmark		Title	Sites	Groups	Systems	Frequency
	EDIT	JumpCloud - Directory Command and	WIN-MCKKRLN6KOI	Default	Netsurion Technologies Private Limited - J	Undefined
	<u>EDIT</u>	JumpCloud - Directory Integrations Eve	WIN-MCKKRLN6KOI	Default	NetsurionTechnologiesPrivateLimited-J	Undefined
\sim	EDIT	JumpCloud - Directory Objects Event	WIN-MCKKRLN6KOI	Default	NetsurionTechnologiesPrivateLimited-J	Undefined
\triangleleft	<u>EDIT</u>	JumpCloud - Directory User and Admin	WIN-MCKKRLN6KOI	Default	Netsurion Technologies Private Limited - J	Undefined
\sim	<u>EDIT</u>	JumpCloud - LDAP and MDM Event re	WIN-MCKKRLN6KOI	Default	Netsurion Technologies Private Limited - J	Undefined
\leq	<u>EDIT</u>	JumpCloud - Login Failure Detected R	WIN-MCKKRLN6KOI	Default	Netsurion Technologies Private Limited - J	Undefined
	<u>EDIT</u>	JumpCloud - Login Success Detected	WIN-MCKKRLN6KOI	Default	Netsurion Technologies Private Limited - J	Undefined
\sim	EDIT	JumpCloud - System Event Report	WIN-MCKKRLN6KOI	Default	Netsurion Technologies Private Limited-J	Undefined
Note	e: Set ru	In time option is not applicable for Defined F	Reports and Hourly Reports			>
Set	run tin	ne for report(s) from At	at interval of minute	es Set		
_						
Rep	blace	to	Repl	lace Assign systems		



3. Click the Import I button to import the report. EventTracker displays success message.



5.5 Dashboards

NOTE- Below steps given are specific to EventTracker 9 and later.

1. Open EventTracker in browser and logon.

	Home			
٩	My Dashboard			
	Threats		1	
	Incidents	ntry point	Indicators of Compromise USB activities, New services or software install	
	Behavior Correlation			
	Change Audit	l		-
	Compliance		Carlos and	

- 2. Navigate to My Dashboard option as shown above.
- 3. Click on the **Import** show below:

Event Tracker ⊕	ņ	Admin -	Tools •	💽 ETAdmin 🔹
My Dashboard		A	/ Dashboar	d / My Dashboard
		÷	g 🕲 🌣	1 3 0

- 4. Import dashboard file **Dashboard_JumpCloud.etwd** and select **Select All** checkbox.
- 5. Click on **Import** as shown below:

Import					
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.					
🗁 Browse Upload					
Available widgets					
Select All					
☑ JumpCloud: User Login Fai ☑ JumpCloud: User Login Suc					
JumpCloud: User Login Fai I JumpCloud: User Login Suc					
✓ JumpCloud: User ✓ JumpCloud: Events by Serv Managemen					
JumpCloud: Policy Managem					
☑ JumpCloud: System Login D ☑ JumpCloud: Elevated Privi					
JumpCloud: Login Success					
Import Close					

6. Import is now completed successfully.

Selected dashlets impo	rted successfully.
	ОК

7. In **My Dashboard** page select ⊕ to add dashboard.



8. Choose appropriate name for **Title** and **Description**. Click **Save**.

Add Dashboard				
Title				
JumpCloud				
Description				
JumpCloud				
Save Delete Cancel				

9. In **My Dashboard** page select (Section 4) to add dashlets.

My Dashbo	ard		🕈 / Dashboard / My Dashboar
CheckPoint	Trend Micr	Microsoft	+ 0 0 4 1 5 0

10. Select imported dashlets and click Add.

Customize dashlets			×
jump			Q
JumpCloud: Elevated Privilege	✓ JumpCloud: Events by Service T	JumpCloud: Login Success With	✓ JumpCloud: Policy Managemen
JumpCloud: System Login Dete	JumpCloud: User Login Failure	JumpCloud: User Login Failure	✓ JumpCloud: User Login Success
✔ JumpCloud: User Login Success	☑ JumpCloud: User Management		
			Add Delete Close

6 Verifying JumpCloud Knowledge Pack in EventTracker

6.1 Category

- 1. Logon to EventTracker.
- 2. Click Admin dropdown, and then click Category.

≡	Event Tracker ⊕					🐥 🛛 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩			Alerts	Correlation	Q IP Lookup Configuration	QQ Users	
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	A Weights	
~			🗞 Behavior Correlation Settings	Event Filters	Manager	🛄 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	Eventvault	😥 Parsing Rules		
			📲 Category	FAQ Configuration	Report Settings		
	Attacker			- News			

3. In **Category Tree** to view imported category, scroll down and expand **JumpCloud** group folder to view the imported category.

Category	
Category Tree	Search
EventTr	acker
🗄 🔁 EventTr	acker Endpoint Security
😐 🔁 F5 Big	IP DNS
💷 🔁 Imperv	a WAF
JumpC	loud
🗐 Jur	npCloud: Directory Command and Policy Events
🗐 Jur	npCloud: Directory Integration Events
🗐 Jur	npCloud: Directory Object Events
···· 🗐 Jur	npCloud: Directory User and Admin Events
🗐 Jur	npCloud: LDAP and MDM Events
···· 🗐 Jur	npCloud: Login Failure Events
nut 🗐 …	npCloud: Login Success Events
nut 🗐	npCloud: System Events

6.2 Alert

- 1. Logon to EventTracker.
- 2. Click the Admin menu, and then click Alerts.

	Event Tracker ⊕					🔎 🗚 Admin 🗸	Tools -
	Home		Active Watch Lists	Collection Master	Croup Management	Systems	🕈 / Dashb
a			Alerts	Correlation	Q IP Lookup Configuration	🛱 Users	_
	0	2	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	T Weights	
<u>~</u>			🇞 Behavior Correlation Setting	s ⊽ Event Filters	Manager	🛄 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			ol [®] Category	FAQ Configuration	Report Settings		
	Attacker			- News			

3. In the **Search** box, type '**JumpCloud**, and then click **Go**. Alert Management page will display the imported alert.

Alert Name 🔨	Threat
ξδ JumpCloud: ActiveDirectory Deleted	•
දිරි JumpCloud: Admin Created	•
ដូកូ JumpCloud: Login Failure Events	•
දිරි JumpCloud: System Deleted	•
ដូក្ញុំ JumpCloud: User Account Deleted	•
នូត្ JumpCloud: User Account Locked or Suspended	•
ដូស្លុ JumpCloud: User Granted Admin Privilage	•



4. To activate the imported alert, toggle the **Active** switch.

EventTracker displays message box.

Successfully saved configuration. Prevent this page from creating additional dialogs
ОК

5. Click **OK**, and then click the **Activate Now** button.

NOTE: Specify appropriate **system** in **alert configuration** for better performance.

6.3 Knowledge Object

1. In the EventTracker web interface, click the Admin dropdown, and then select Knowledge Objects.

III	Event Tracker ⊕					🐥 🛛 Admin 🕶	Tools +
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			Alerts	Correlation	Q IP Lookup Configuration	🙊 Users	
	0	1	Behavior Correlation Rules	1 Diagnostics	Knowledge Objects	r Weights	
►			🗞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	P Eventvault	🧭 Parsing Rules		
			o-∰ Category	FAQ Configuration	Report Settings		
	Attacker			 News 			

2. In the Knowledge Object tree, expand **JumpCloud** group folder to view the imported knowledge object.

Groups	🕀 🧭 📋	Object	name JumpCloud	
Duo Security	A	Applie	Applies to JumpCloud	
EventTracker		Rules		
EventTracker Endpoint Security			Title	
F5 Big IP DNS		+	JumpCloud Directory Events	
■ Heroku			Message Signature: \"event_type\"\:\".*	
Imperva WAF			Expressions	
Infoblox DDI			Expression type	
JumpCloud			Regular Expression Regular Expression	
JumpCloud	Ø 🗓		Regular Expression	

3. Click Activate Now to apply imported knowledge objects.

6.4 Report

1. In the EventTracker web interface, click the Reports menu, and then select Report Configuration.

	Event Tracker ⊕			
	Home			
Q 	Report Configuration]	1	
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install	
	Explorer Attacker			-

- 2. In **Reports Configuration** pane, select **Defined** option.
- 3. Click on the JumpCloud group folder to view the imported reports.

Repor	t Configuration					
O Sch	eduled 🔿 Queued 💿 Defined					
Report	t Groups		+		Reports co	onfiguration: JumpCloud
D	Detender MFA		Ø.		0 🕅 d	ê.
	Duo Security		1		_	
	EventTracker	Ē	1			Inte
	EventTracker Endpoin	Ē	1			Jumpcioud - LDAP and MDM Event report
B	Foritnet	Ē	Ø			3 JumpCloud - System Event Report
B	Heroku	1	0		- 🌣	JumpCloud - Directory Integrations Event Report
B	Imperva WAF	 ∭∏	0		D 🔅	JumpCloud - Directory Command and Policy Event Report
D	JumpCloud	Û	0		0 🔅	JumpCloud - Directory User and Admin Event Report
	Linux	Ē	1		D 🔅	JumpCloud - Directory Objects Event Report
	Microsoft 365	Ē	0		□ 🄅	JumpCloud - Login Success Detected Report
	Pure Storage	Ē	1	Ľ		JumpCloud - Login Failure Detected Report
		-0-			~	4

6.5 Dashboards

1. In the EventTracker web interface, Click on Home Button and select My Dashboard.

	Home
Dashb	My Dashboard
R	Threats
	Incidents

2. In the JumpCloud dashboard you should be now able to view the following screen.





About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's <u>EventTracker</u> cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multilocation businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #19 among <u>MSSP Alert's 2020 Top 250 MSSPs</u>.

Contact Us

Corporate Headquarters

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2) EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3) EventTracker Essentials SOC: 877-333-1433 (Option 4) EventTracker Software Support: 877-333-1433 (Option 5) https://www.netsurion.com/eventtracker-support