Netsurion®
Powering Secure and Agile Networks

Integration Guide

Integrating JumpCloud with EventTracker

EventTracker v9.3 and above

Publication Date:

April 28, 2021

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 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.

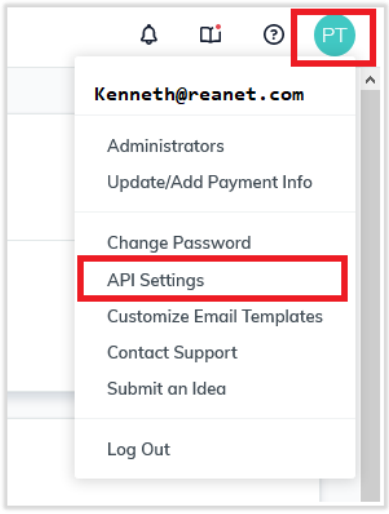
2 Prerequisites

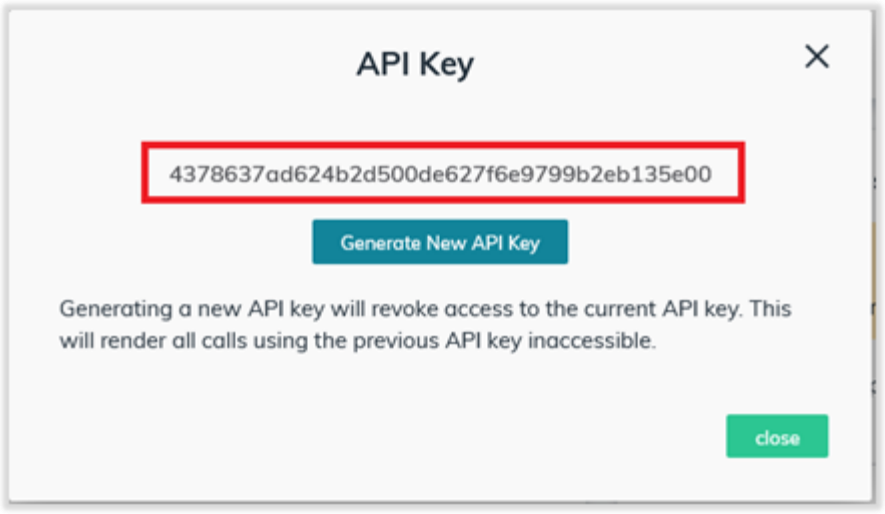
- **EventTracker v9.3x** or **above** should be installed.
- **JumpCloud** should be configured.
- **Admin permission** should be there for configuring JumpCloud API.
- **Local admin permissions** for the workstation.
- **PowerShell 5.0** should be installed on the EventTracker Manager.

3 Integration of JumpCloud with EventTracker

3.1 Getting JumpCloud API key

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

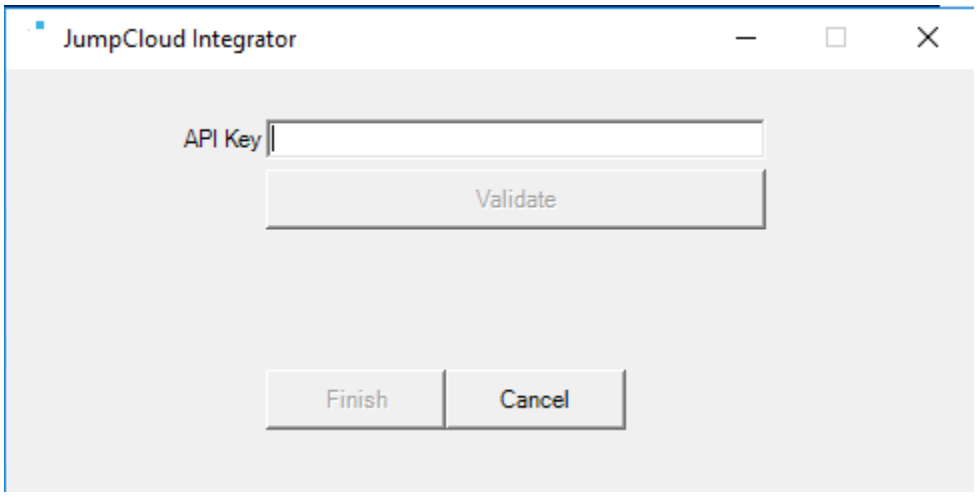




- Retrieve your API key from API Settings.

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**.



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

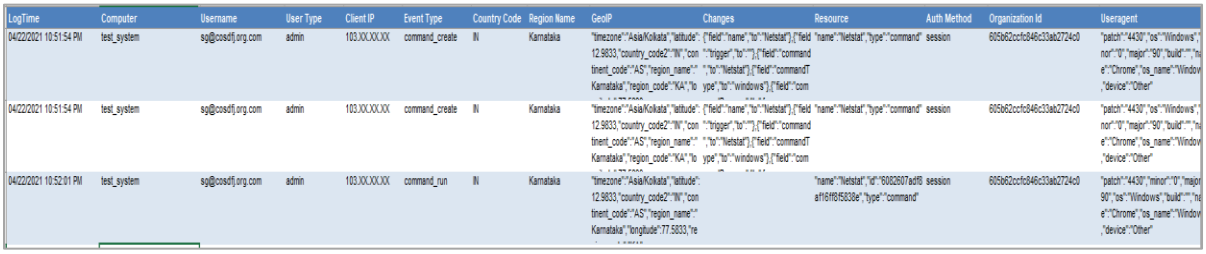
- **JumpCloud: Directory Command and Policy Events -** This category provides information related to command management events, policy management events, file management events, IP list management events.
- **JumpCloud: Login Success Events –** This category provides information related to all the successful 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.

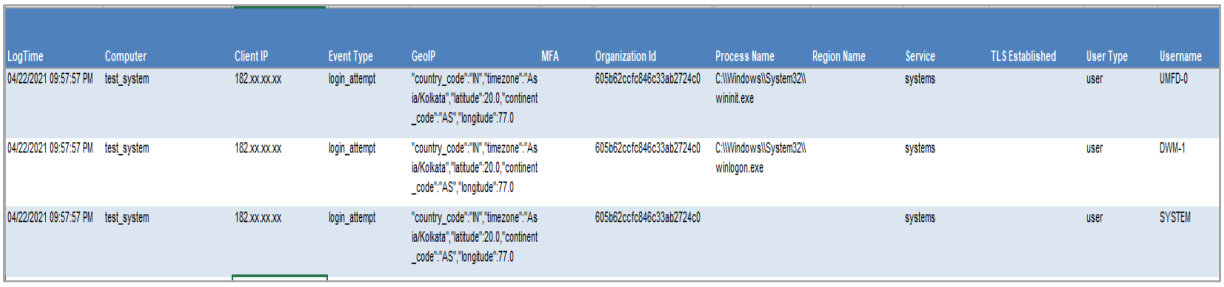


LogTime	Computer	Username	User Type	Client IP	Event Type	Country Code	Region Name	GeoIP	Changes	Resource	Auth Method	Organization Id	Useragent
04/22/2021 10:51:54 PM	test_system	sg@cosdfj.org.com	admin	103.XX.XX.XX	command_create	IN	Karnataka	"timezone":"Asia/Kolkata","latitude": 12.9833,"country_code2":"IN","continent_code":"AS","region_name":"Karnataka","region_code":"KA","to	{"field":"name","to":"Netstat"},{"field":"trigger","to":""},{"field":"commandT ype","to":"windows"},{"field":"com	"name":"Netstat","type":"command"	session	605b62ccfc846c33ab2724c0	"patch":"4430","os":"Windows","minor":"0","major":"90","build":"","name":"Chrome","os_name":"Windows","device":"Other"
04/22/2021 10:51:54 PM	test_system	sg@cosdfj.org.com	admin	103.XX.XX.XX	command_create	IN	Karnataka	"timezone":"Asia/Kolkata","latitude": 12.9833,"country_code2":"IN","continent_code":"AS","region_name":"Karnataka","region_code":"KA","to	{"field":"name","to":"Netstat"},{"field":"trigger","to":""},{"field":"commandT ype","to":"windows"},{"field":"com	"name":"Netstat","type":"command"	session	605b62ccfc846c33ab2724c0	"patch":"4430","os":"Windows","minor":"0","major":"90","build":"","name":"Chrome","os_name":"Windows","device":"Other"
04/22/2021 10:52:01 PM	test_system	sg@cosdfj.org.com	admin	103.XX.XX.XX	command_run	IN	Karnataka	"timezone":"Asia/Kolkata","latitude": 12.9833,"country_code2":"IN","continent_code":"AS","region_name":"Karnataka","longitude":77.5833,"re		"name":"Netstat","id":"6082607adf8 af16ff6f5638e","type":"command"	session	605b62ccfc846c33ab2724c0	"patch":"4430","minor":"0","major":"90","os":"Windows","build":"","name":"Chrome","os_name":"Windows","device":"Other"

Logs Considered

{"initiated_by":{"id":"605b62ccfc846c33ab2724bf","type":"admin","email":"ajsfj.cnsorso.org"},"geoip":{"timezone":"Asia/Kolkata","latitude":12.9833,"country_code2":"IN","continent_code":"AS","region_name":"Karnataka","region_code":"KA","longitude":77.5833},"resource":{"name":"ETAgentInstall","id":"607e6fc239320c1be42a3bfd","type":"command"},"auth_method":"session","event_type":"command_run","provider":null,"service":"directory","organization":"605b62ccfc846c33ab2724c0","@version":"1","client_ip":"103.xx.xx.xx","id":"60825f648035532ceeb27f7e","user_agent":{"patch":"4430","minor":"0","os":"Windows","major":"90","build":"","name":"Chrome","os_name":"Windows","device":"Other"},"timestamp":"2021-04-23T05:47:16.953Z"}

- **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.



LogTime	Computer	Client IP	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":"IN","timezone":"Asia/Kolkata","latitude":20.0,"continent_code":"AS","longitude":77.0		605b62ccfc846c33ab2724c0	C:\Windows\System32\winlnit.exe		systems		user	UMFD-0
04/22/2021 09:57:57 PM	test_system	182.xx.xx.xx	login_attempt	"country_code":"IN","timezone":"Asia/Kolkata","latitude":20.0,"continent_code":"AS","longitude":77.0		605b62ccfc846c33ab2724c0	C:\Windows\System32\winlogon.exe		systems		user	DWM-1
04/22/2021 09:57:57 PM	test_system	182.xx.xx.xx	login_attempt	"country_code":"IN","timezone":"Asia/Kolkata","latitude":20.0,"continent_code":"AS","longitude":77.0		605b62ccfc846c33ab2724c0			systems		user	SYSTEM

Logs Considered

{"initiated_by":{"id":"605b62ccfc846c33ab2724bf","type":"admin","email":"jds@cosdfhy.org"},"geoip":{"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":"admin_login_attempt","provider":null,"success":true,"service":"directory","organization":"605b62ccfc846c33ab2724c0","@version":"1","client_ip":"106.xx.xx.xx","id":"608273997aab62048f3fd3c9","user_agent":{"patch":"4430","os":"Windows","major":"90","minor":"0","build":"","name":"Chrome","os_name":"Windows","device":"Other"},"timestamp":"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	GeoIP	Client IP	Organization Id	Event Type
04/22/2021 10:01:41 PM	test_system	C:\\Windows\\System32\\svchost.exe	systems	user	DemoEventTracker	DESKTOP-EJ8F2TN	"country_code":"IN","timezone":"Asia/Kolkata","latitude":20.0,"continent_code":"AS","longitude":77.0	182.xx.xx.xx	605b62ccfc846c33ab2724c0	login_attempt
04/22/2021 10:01:41 PM	test_system	C:\\Windows\\System32\\svchost.exe	systems	user	DemoEventTracker	DESKTOP-EJ8F2TN	"country_code":"IN","timezone":"Asia/Kolkata","latitude":20.0,"continent_code":"AS","longitude":77.0	182.xx.xx.xx	605b62ccfc846c33ab2724c0	login_attempt
04/22/2021 10:01:41 PM	test_system	C:\\Windows\\System32\\svchost.exe	systems	user	DemoEventTracker	DESKTOP-EJ8F2TN	"country_code":"IN","timezone":"Asia/Kolkata","latitude":20.0,"continent_code":"AS","longitude":77.0	182.xx.xx.xx	605b62ccfc846c33ab2724c0	login_attempt

Logs Considered

{"initiated_by":{"id":"605b62ccfc846c33ab2724bf","type":"admin","email":"jds@cosdfhy.org"},"geoip":{"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":"admin_login_attempt","provider":null,"success":false,"service":"directory","organization":"605b62ccfc846c33ab2724c0","@version":"1","client_ip":"106.xx.xx.xx","id":"608273997aab62048f3fd3c9","user_agent":{"patch":"4430","os":"Windows","major":"90","minor":"0","build":"","name":"Chrome","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.xx.xx.xx	{"field":"account_locked","to":false},{"field":"activated","to":false},{"field":"addresses","to":[	user_create	admin	asfdsj@jhbfvc.org	"id":"60825ee57bf1f3092a54726f","type":"user","username":"Captan.a"	"patch":"4430","os":"Windows","major":"90","minor":"0","build":"","name":"Chrome","os_name":"Windows","device":"Other"	Karnataka
04/22/2021 10:45:10 PM	test_system	session	103.xx.xx.xx	{"field":"account_locked","to":false},{"field":"activated","to":false},{"field":"addresses","to":[	user_create	admin	asfdsj@jhbfvc.org	"id":"60825ee57bf1f3092a54726f","type":"user","username":"Captan.a"	"patch":"4430","os":"Windows","major":"90","minor":"0","build":"","name":"Chrome","os_name":"Windows","device":"Other"	Karnataka
04/22/2021 10:45:10 PM	test_system	session	103.xx.xx.xx	{"field":"account_locked","to":false},{"field":"activated","to":false},{"field":"addresses","to":[	user_create	admin	asfdsj@jhbfvc.org	"id":"60825ee57bf1f3092a54726f","type":"user","username":"Captan.a"	"patch":"4430","os":"Windows","major":"90","minor":"0","build":"","name":"Chrome","os_name":"Windows","device":"Other"	Karnataka
04/22/2021 10:45:10 PM	test_system	session	103.xx.xx.xx	{"field":"account_locked","to":false},{"field":"activated","to":false},{"field":"addresses","to":[	user_delete	admin	asfdsj@jhbfvc.org	"id":"60825ee57bf1f3092a54726f","type":"user","username":"Captan.a"	"patch":"4430","os":"Windows","major":"90","minor":"0","build":"","name":"Chrome","os_name":"Windows","device":"Other"	Karnataka

Logs Considered

{"initiated_by":{"id":"605b62ccfc846c33ab2724bf","type":"admin","email":"ajfjakd@msdlck.org"},"geoip":{"timezone":"Asia/Kolkata","latitude":12.9833,"country_code2":"IN","continent_code":"AS","region_name":"Karnataka","region_code":"KA","longitude":77.5833},"resource":{"id":"60825ee57bf1f3092a54726f","type":"user","username":"Captan.a"},"changes":[{"field":"account_locked","to":false},{"field":"activated","to":false},{"field":"addresses","to":[]},{"field":"allow_public_key","to":true},{"field":"attributes","to":[]},{"field":"company","to":""},{"field":"costCenter","to":""},{"field":"department","to":""},{"field":"description","to":""},{"field":"disableDeviceMaxLoginAttempts","to":false},{"field":"displayname","to":""},{"field":"email","to":"gurmukh.s@eventtracker.com"},{"field":"employeeIdentifier","to":null},{"field":"employeeType","to":""},{"field":"enable_managed_uid","to":false},{"field":"enable_user_portal_multifactor","to":false},{"field":"external_dn","to":""},{"field":"external_source_type","to":""},{"field":"externally_managed","to":false},{"field":"firstname","to":"captan"},{"field":"jobTitle","to":""},{"field":"lastname","to":"america"},{"field":"ldap_binding_user","to":false},{"field":"location","to":""},{"field":"mfa.exclusion","to":false},{"field":"middlename","to":""},{"field":"password_date","to":"2021-04-23T05:45:09.967Z"},{"field":"password_expired","to":false},{"field":"password_never_expires","to":false},{"field":"passwordless_sudo","to":false},{"field":"phoneNumbers","to":[]},{"field":"samba_service_user","to":false},{"field":"sudo","to":false},{"field":"suspended","to":false},{"field":"unix_guid","to":5003},{"field":"unix_uid","to":5003},{"field":"username","to":"Captan.a"},{"field":"created","to":"2021-04-23T05:45:09.722Z"},{"field":"id","to":"60825ee57bf1f3092a54726f"},{"field":"organization","to":"605b62ccfc846c33ab2724c0"},{"field":"relationships","to":[]},{"field":"totp_enabled","to":false},{"field":"password"},{"field":"ssh_keys"}],"auth_method":"session","event_type":"user_create","provider":null,"service":"directory","organization":"605b62ccfc846c33ab2724c0","@version":"1","client_ip":"103.xx.xx.xx","id":"60825ee67bf1f3092a547271","user_agent":{"patch":"4430","os":"Windows","major":"90","minor":"0","build":"","name":"Chrome","os_name":"Windows","device":"Other"},"timestamp":"2021-04-23T05:45:10.159Z"}

- **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	{"field":"id","to":"60825eb0b544064b8027521b"},{"field":"name","to":"Admin Group"},{"field":"type","to":"user_group"},{"field":"attributes","to":{"ldapGroups":[{"name":	103.xx.xx.xx	IN	605b62ccfc846c33ab2724c0	Windows	Karnataka	"name":"Admin Group","id":"60825eb0b544064b8027521b","type":"user_group"	admin	dasfkhk@jksdhf.org	
04/22/2021 10:44:17 PM	test_system	session	{"field":"id","to":"60825eb0b544064b8027521b"},{"field":"name","to":"Admin Group"},{"field":"type","to":"user_group"},{"field":"attributes","to":{"ldapGroups":[{"name":	103.xx.xx.xx	IN	605b62ccfc846c33ab2724c0	Windows	Karnataka	"name":"Admin Group","id":"60825eb0b544064b8027521b","type":"user_group"	admin	dasfkhk@jksdhf.org	
04/22/2021 10:44:17 PM	test_system	session	{"field":"id","to":"60825eb0b544064b8027521b"},{"field":"name","to":"Admin Group"},{"field":"type","to":"user_group"},{"field":"attributes","to":{"ldapGroups":[{"name":	103.xx.xx.xx	IN	605b62ccfc846c33ab2724c0	Windows	Karnataka	"name":"Admin Group","id":"60825eb0b544064b8027521b","type":"user_group"	admin	dasfkhk@jksdhf.org	

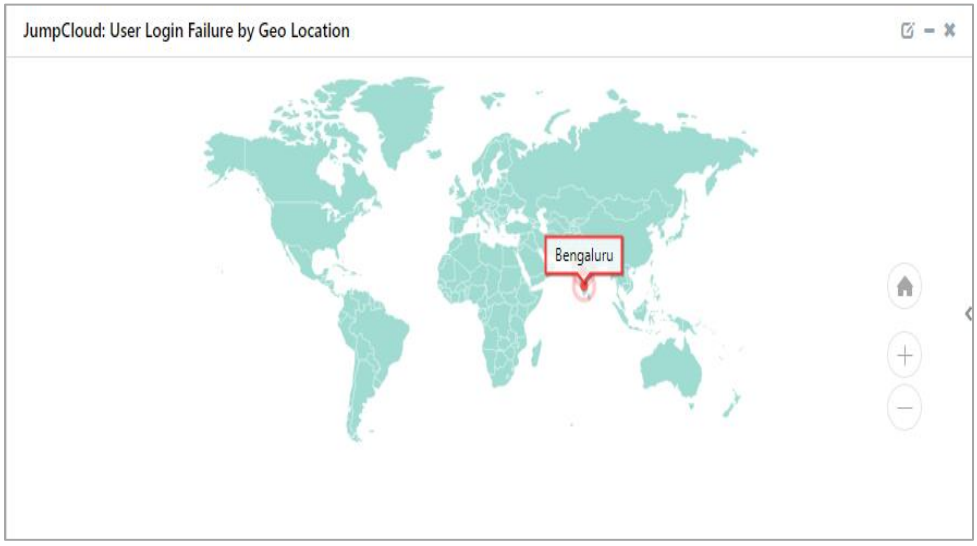
Logs Considered

{"initiated_by":{"id":"605b62ccfc846c33ab2724bf","type":"admin","email":"adgsk@shfdjskh.com"},"geoip":{"timezone":"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":"60825eb0b544064b8027521b"},{"field":"name","to":"Admin Group"},{"field":"type","to":"user_group"},{"field":"attributes","to":{"ldapGroups":[{"name":"Admin Group"}]}}],"auth_method":"session","event_type":"group_create","provider":null,"service":"directory","organization":"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":"Windows","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.

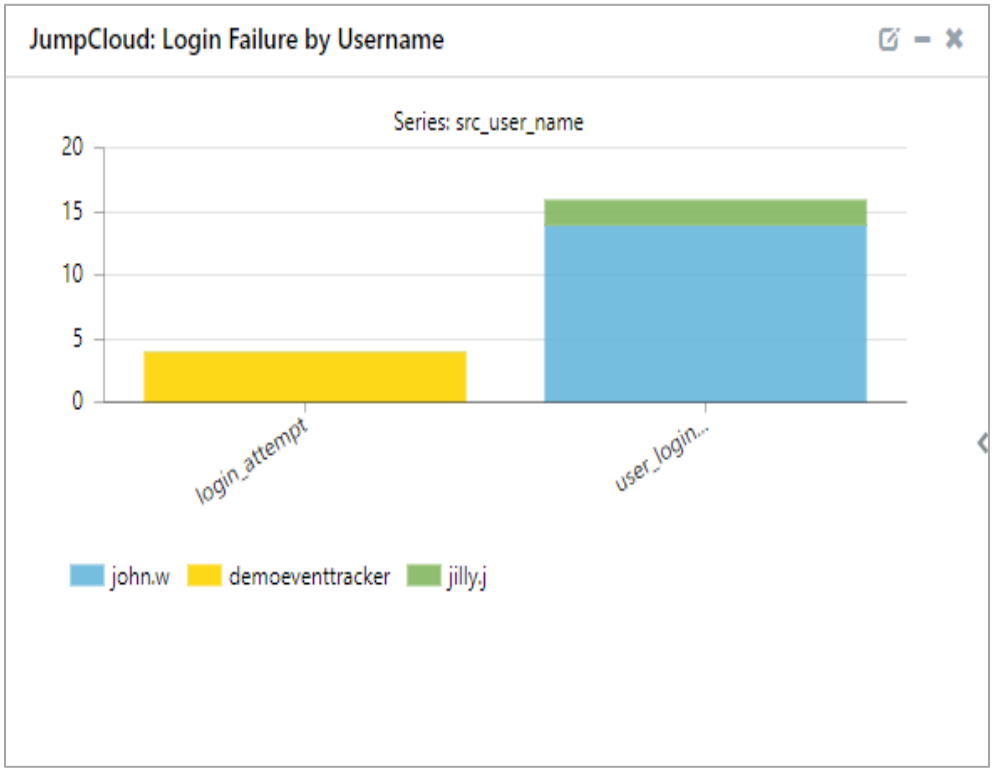
4.4 Dashboards

- **JumpCloud: User Login Failure by Geo Location**

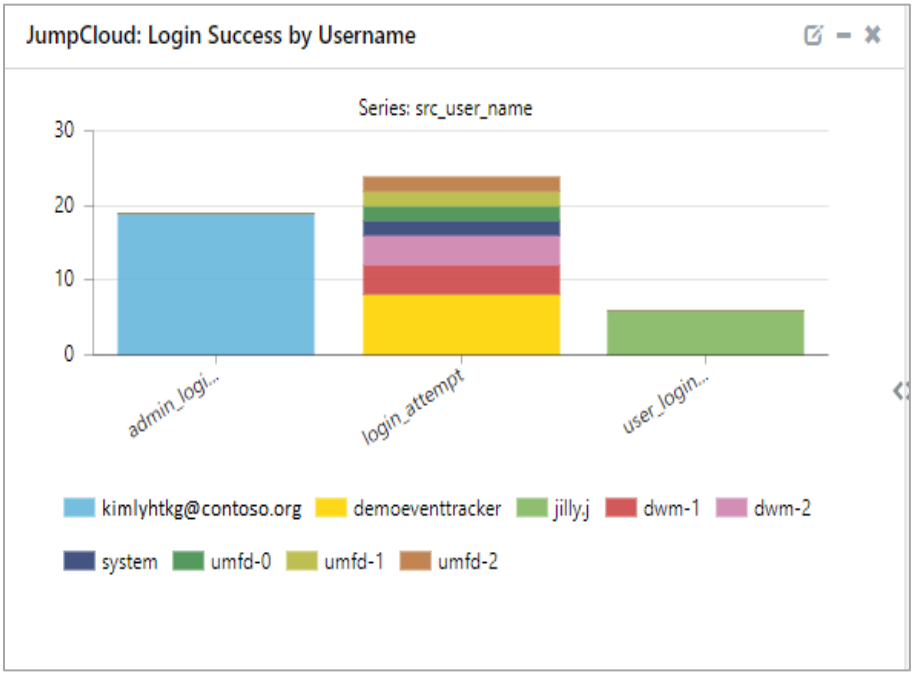


- **JumpCloud: User Login Success by Geo Location**

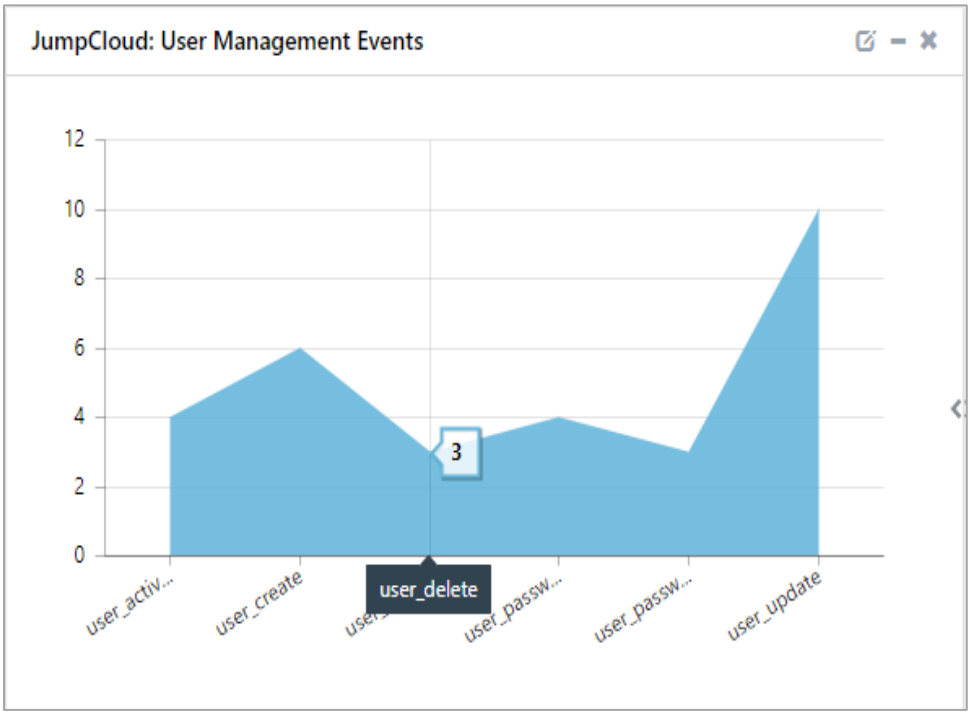
- **JumpCloud: Login Failure by Username**



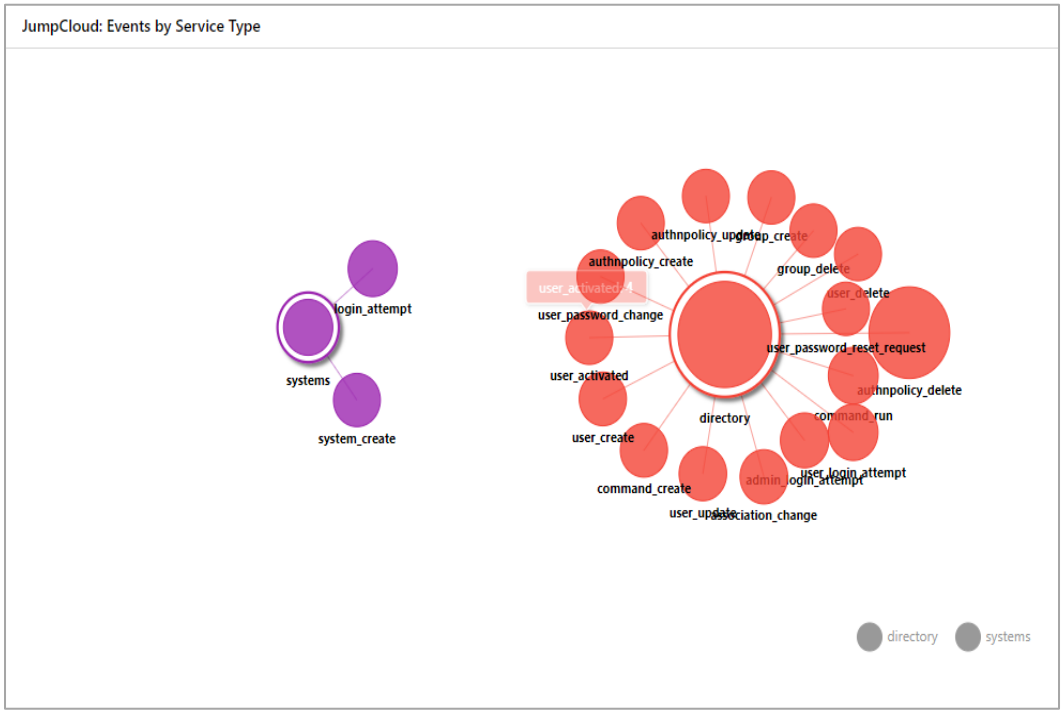
- **JumpCloud: Login Success by Username**



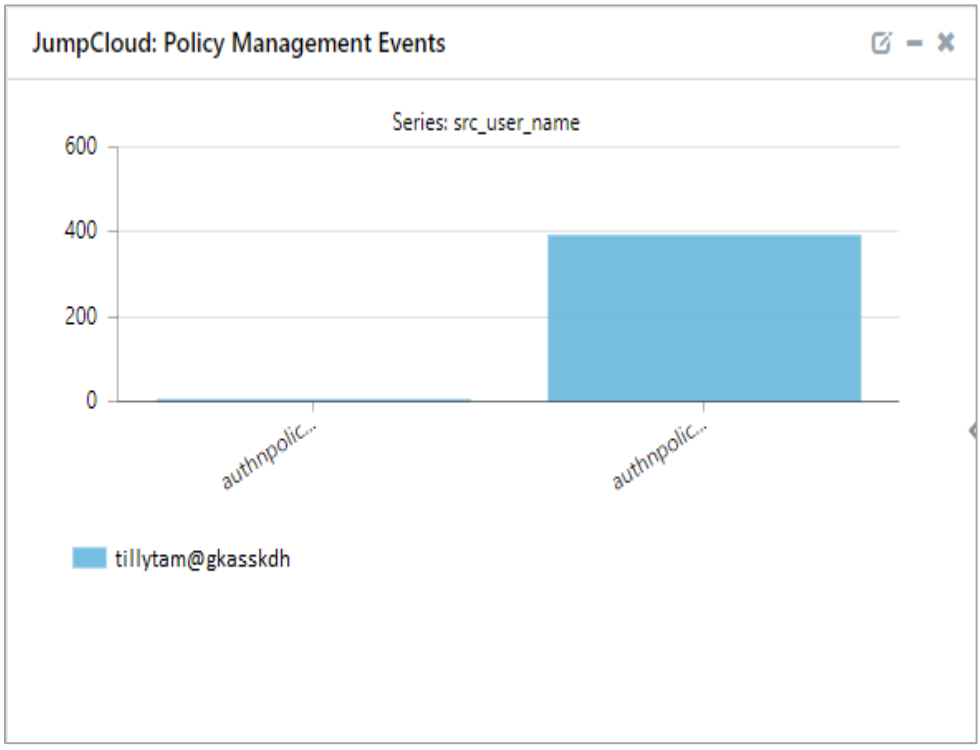
- **JumpCloud: User Management Events**



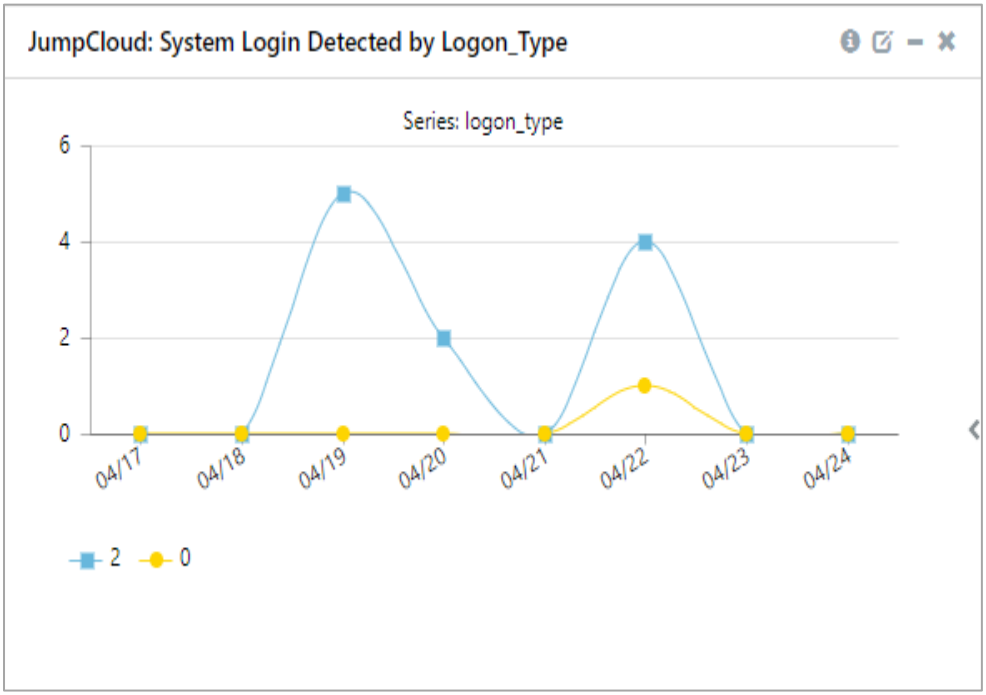
- **JumpCloud: Events by Service Type**



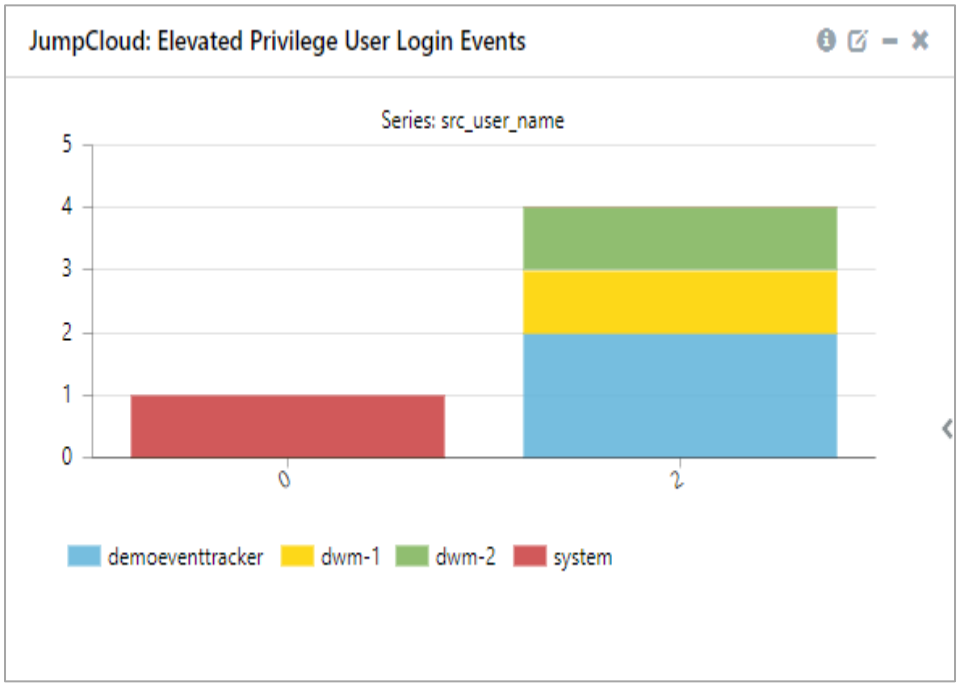
- **JumpCloud: Policy Management Events**



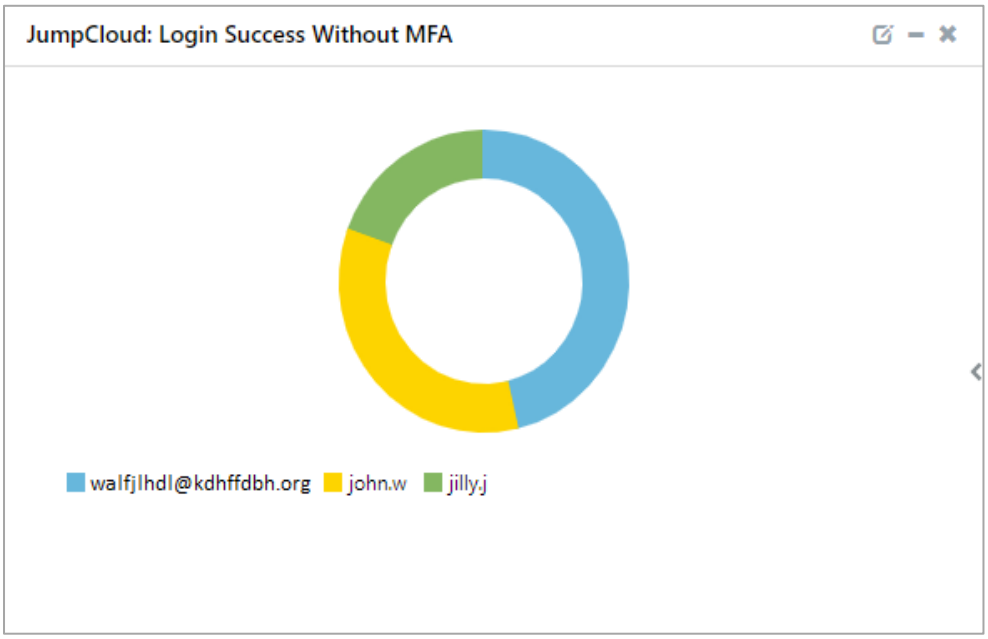
- **JumpCloud: System Login Detected by Logon_type**



- **JumpCloud: Elevated Privilege User Login Events**



- **JumpCloud: Login Success Without MFA**

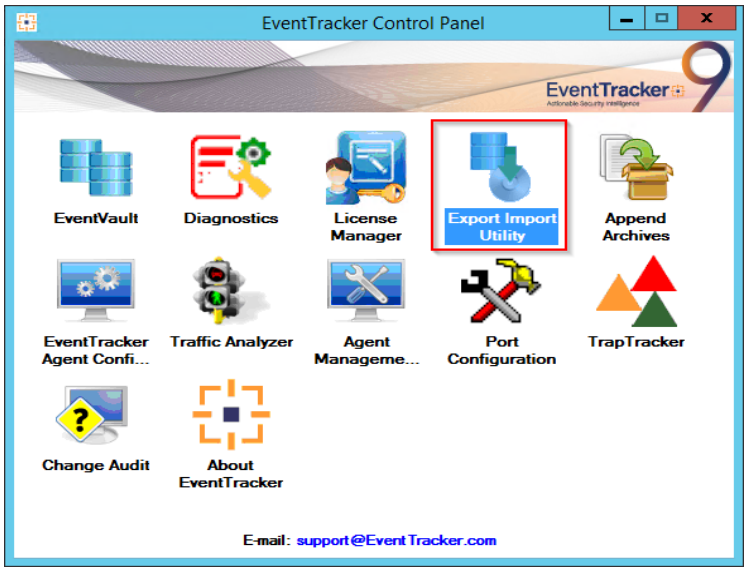


5 Importing JumpCloud Knowledge Pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Category
- Alert
- Knowledge Object
- Report
- Dashboard

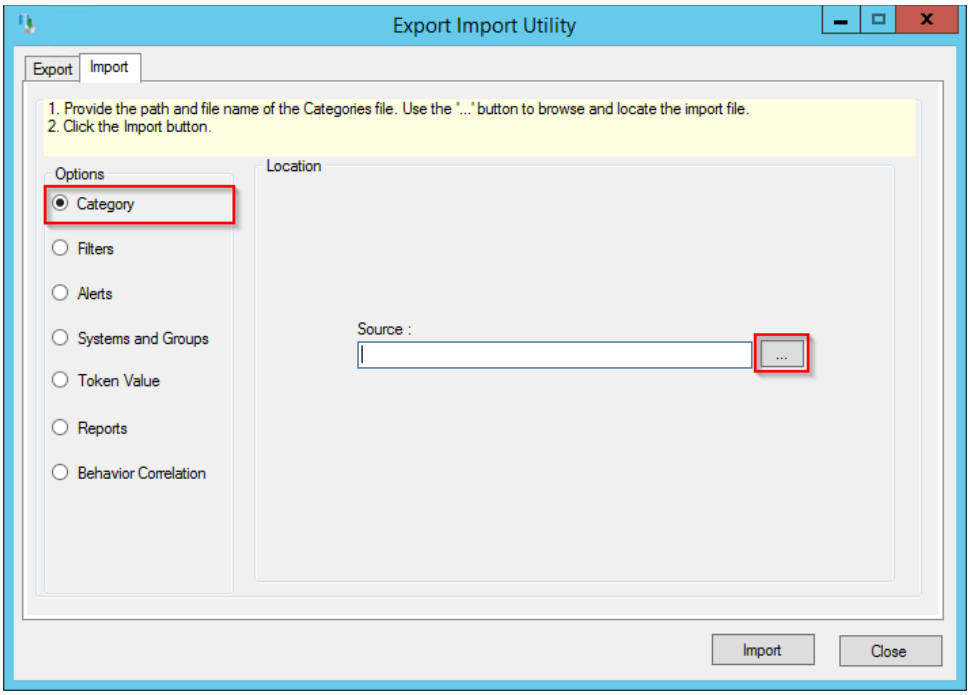
1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.



3. Click the **Import** tab.

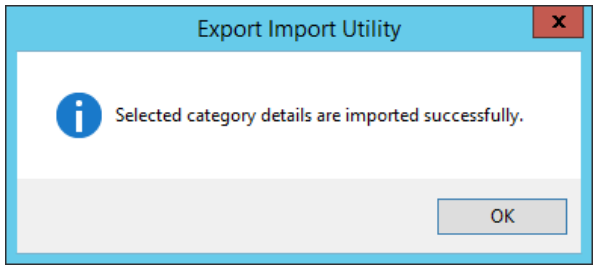
5.1 Category

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



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

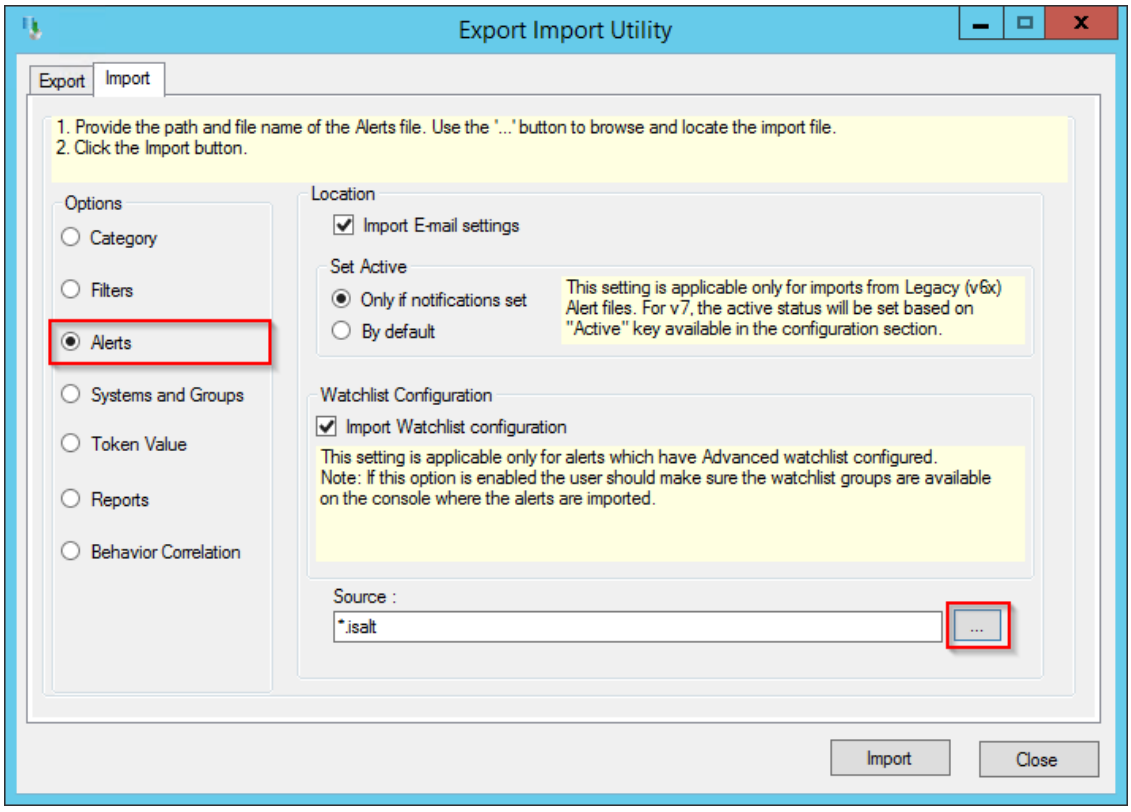
EventTracker displays success message.



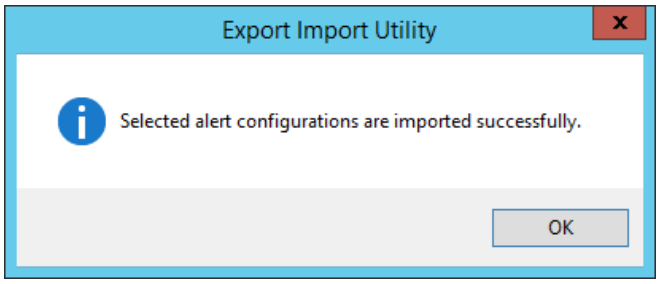
4. Click **OK,** and then click the **Close** button.

5.2 Alert

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



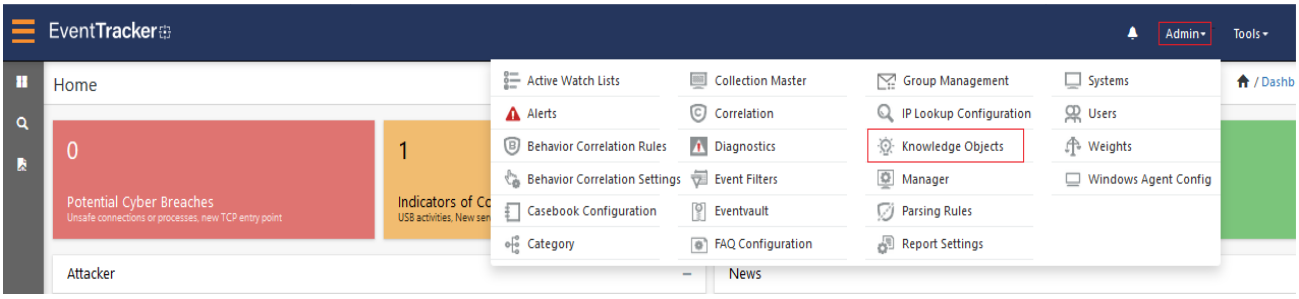
2. Locate **Alert_JumpCloud.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.
   EventTracker displays success message.



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

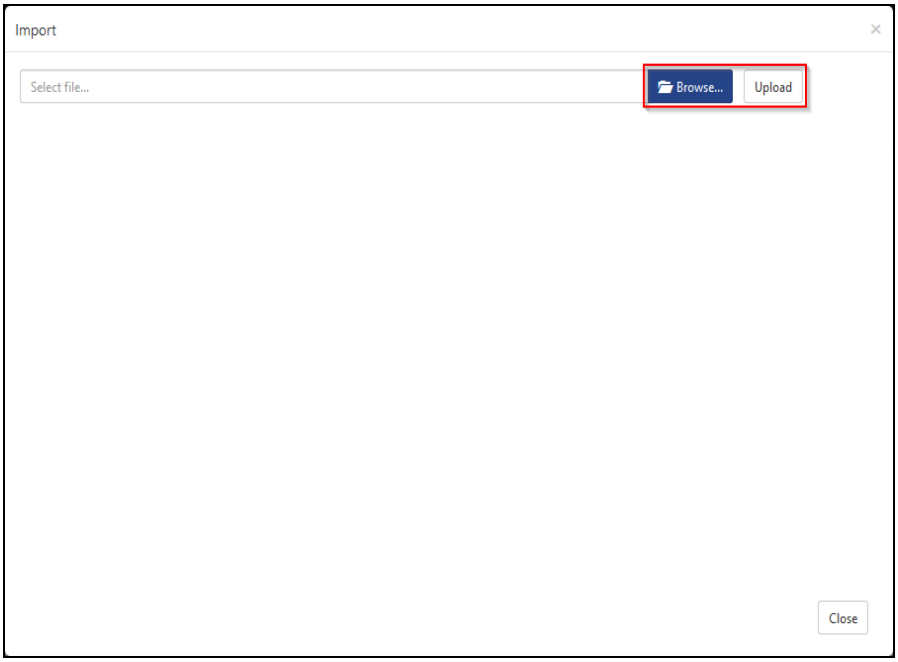
5.3 Knowledge Object

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

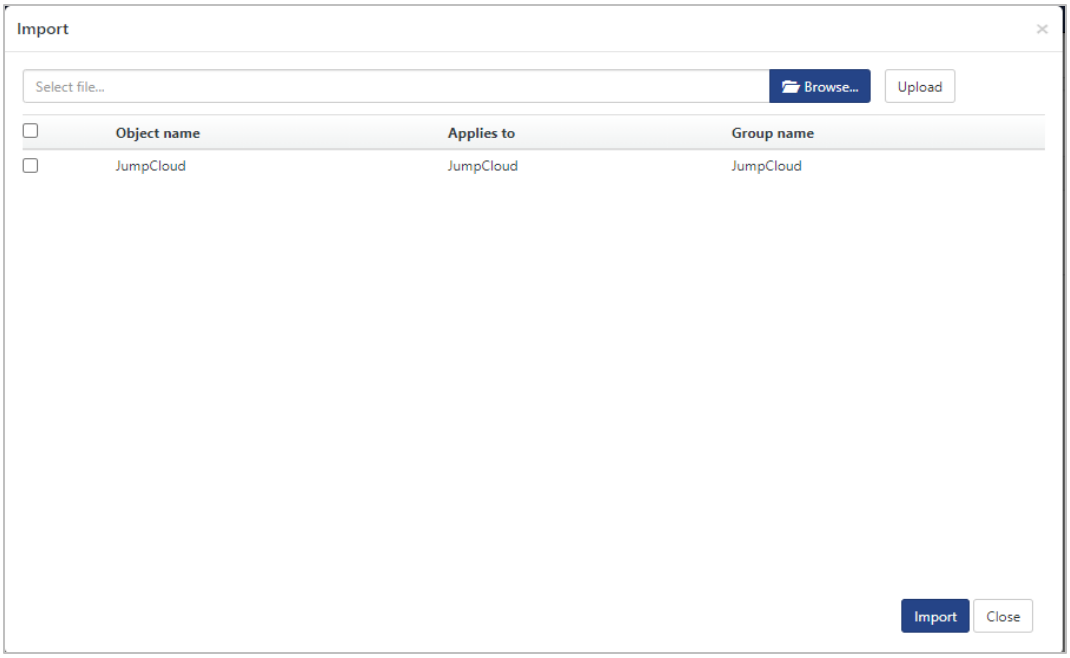


2. Click on **Import** button as highlighted in the below image:

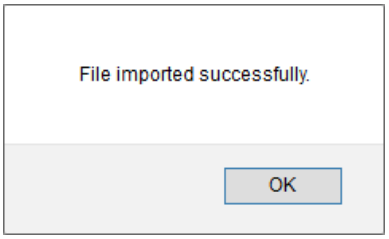
3. Click on **Browse**.



4. Locate the file named **KO_JumpCloud.etko**.
5. Select the check box and then click on **Import** option.

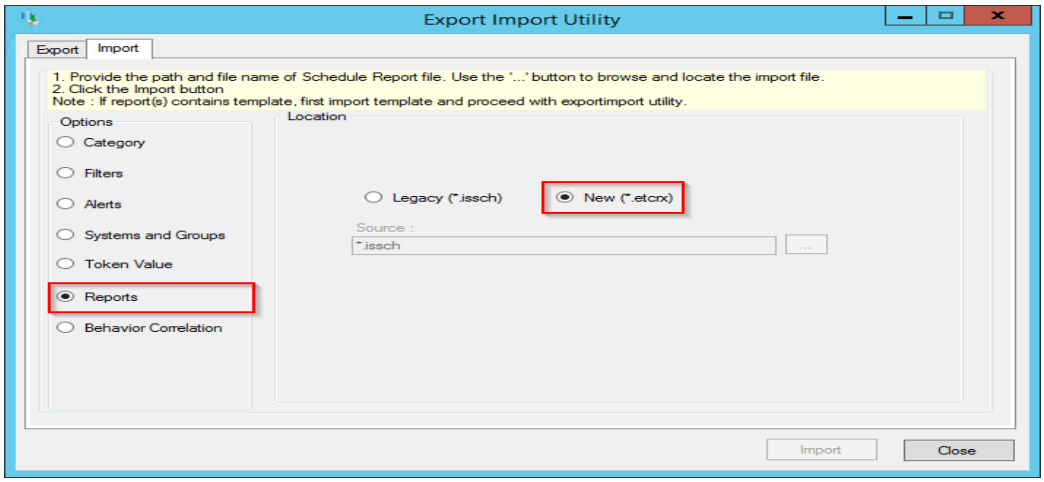


6. Knowledge objects are now imported successfully.

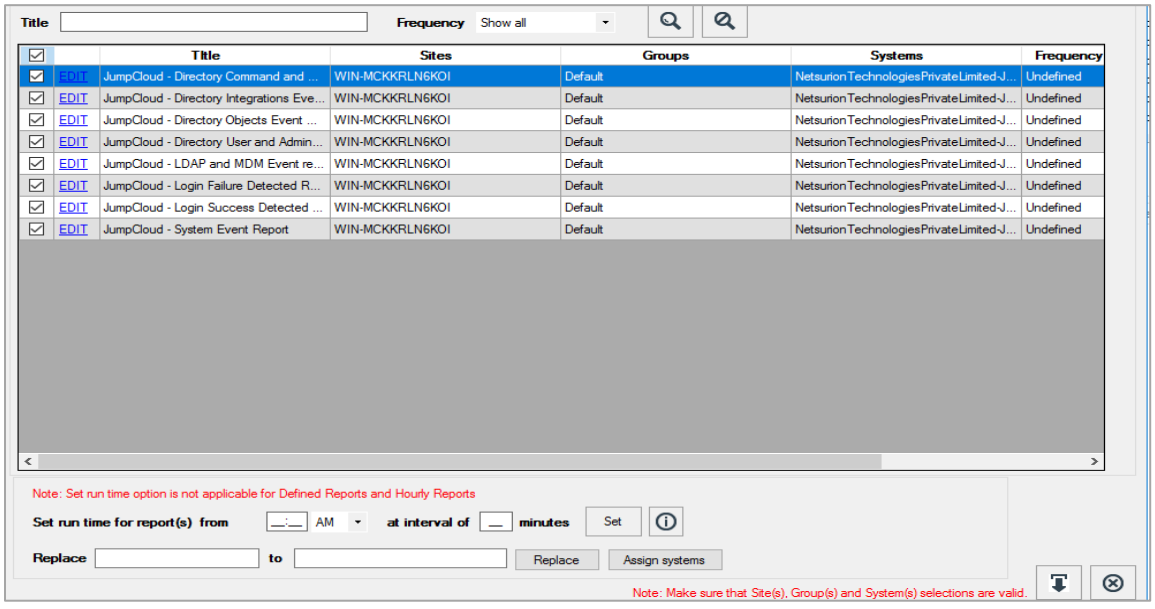


5.4 Report

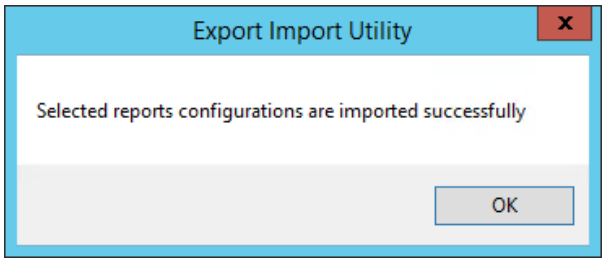
1. Click **Reports** option, and select **New (*.etcrx)** option.



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



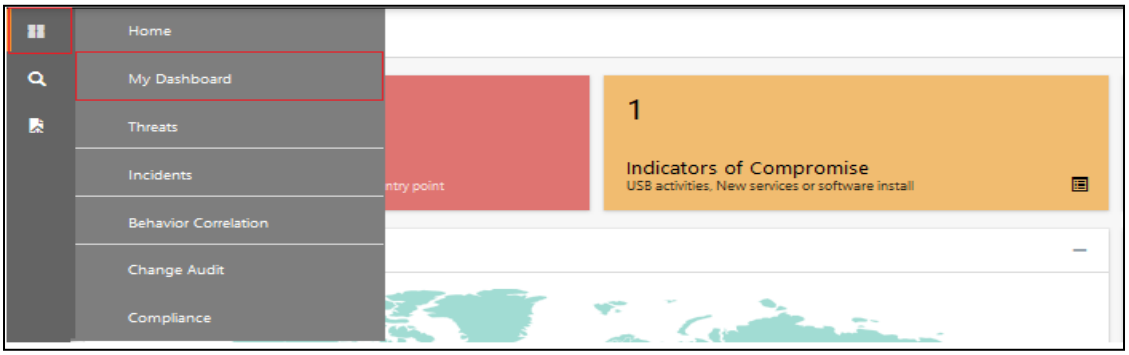
3. Click the **Import** button to import the report. EventTracker displays success message.



5.5 Dashboards

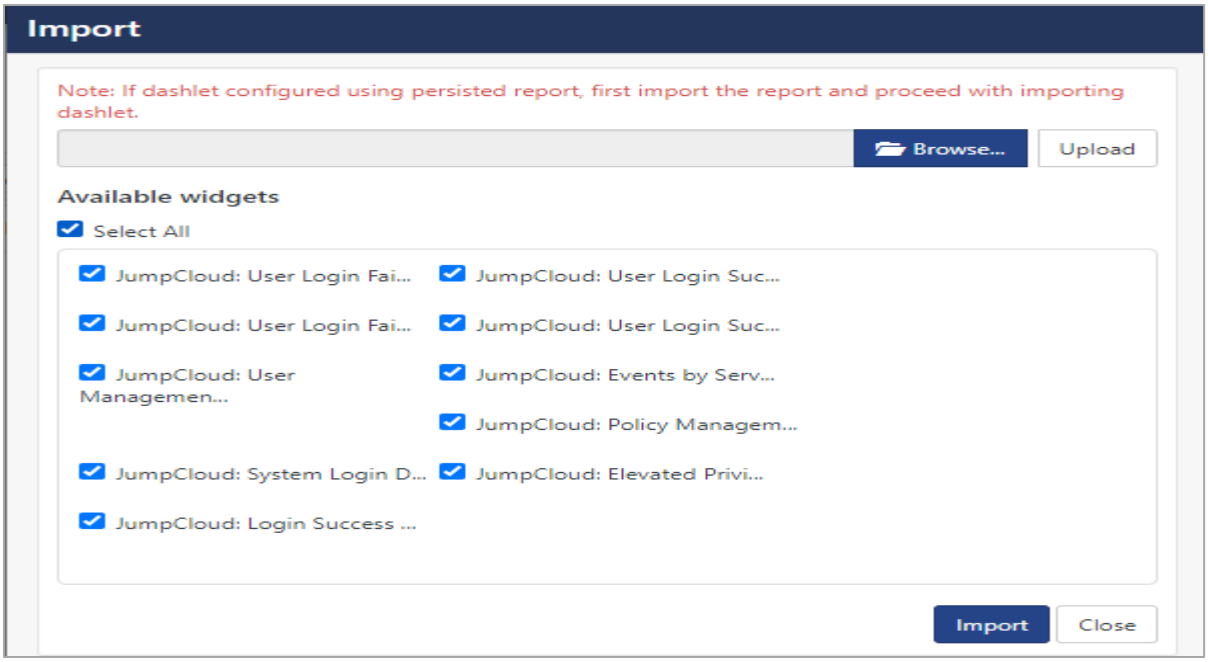
NOTE- Below steps given are specific to EventTracker 9 and later.

1. Open **EventTracker** in browser and logon.

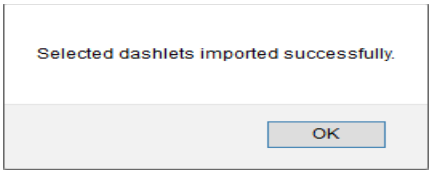


2. Navigate to **My Dashboard** option as shown above.
3. Click on the **Import** button as show below:

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

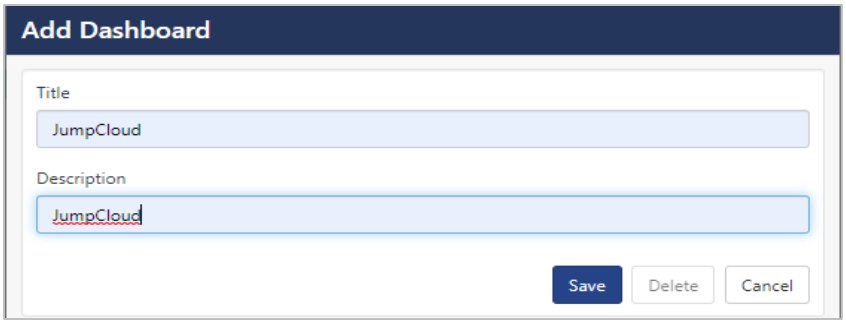


6. Import is now completed successfully.



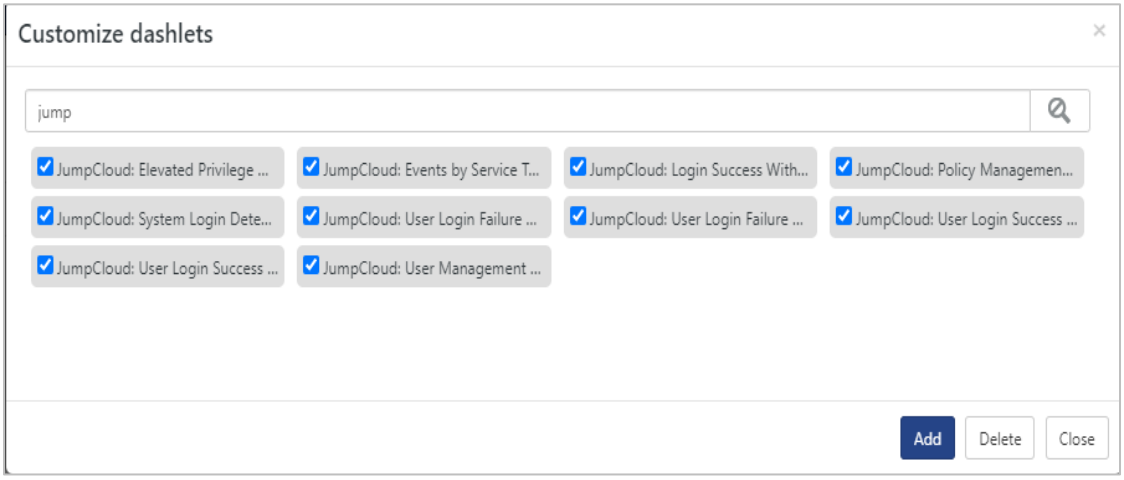
7. In **My Dashboard** page select ⊕ to add dashboard.

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



9. In **My Dashboard** page select to add dashlets.

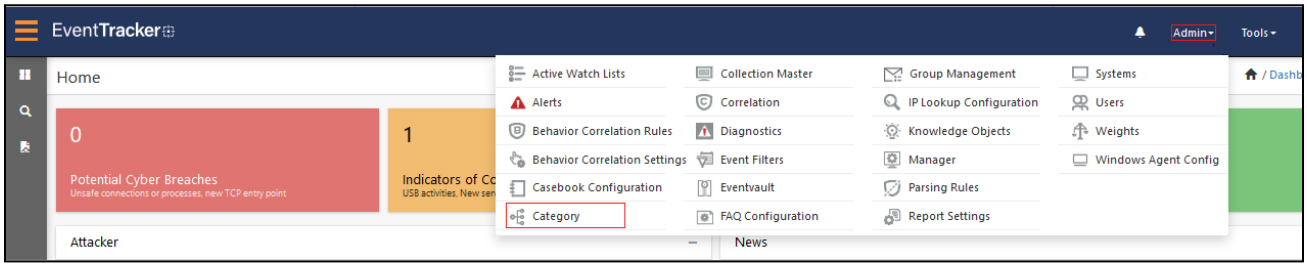
10. Select imported dashlets and click **Add**.



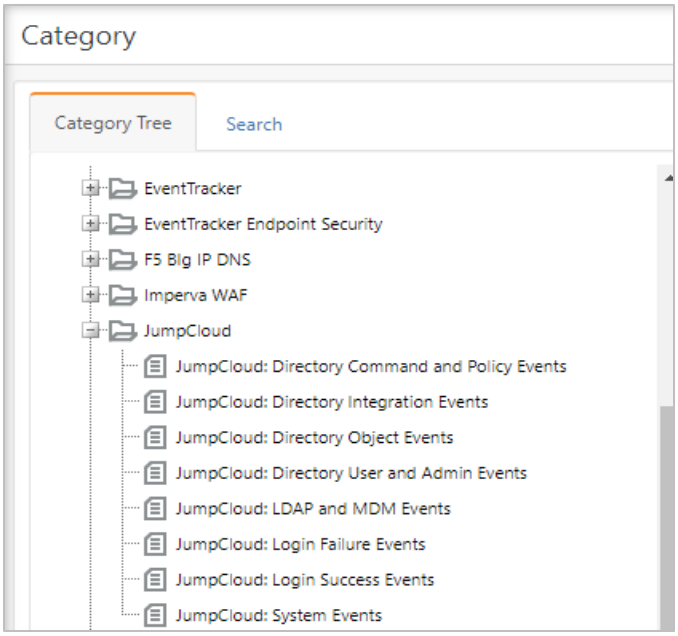
6 Verifying JumpCloud Knowledge Pack in EventTracker

6.1 Category

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

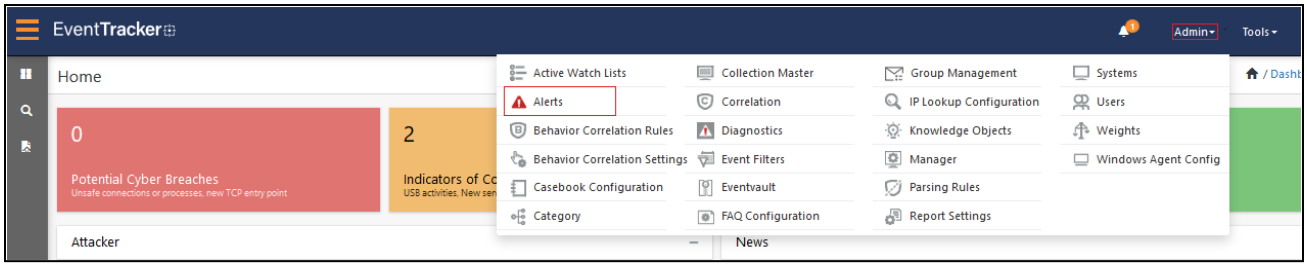


3. In **Category Tree** to view imported category, scroll down and expand **JumpCloud** group folder to view the imported category.

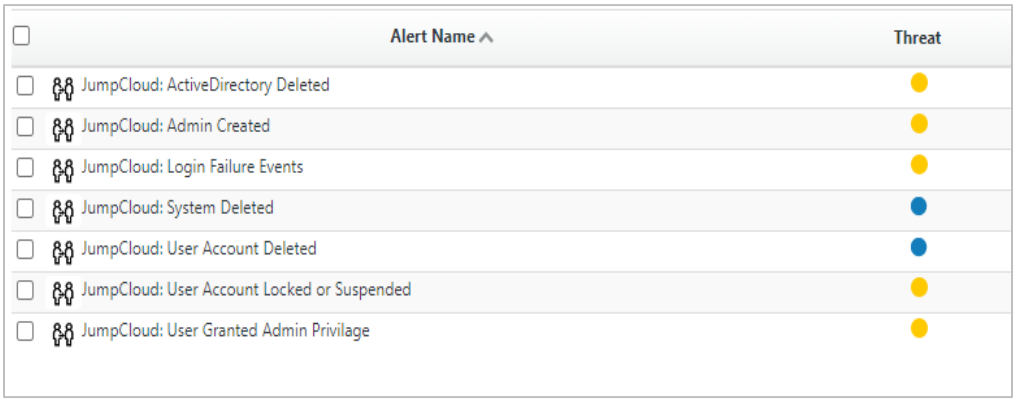


6.2 Alert

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

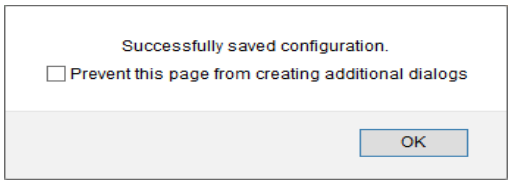


3. In the **Search** box, type '**JumpCloud**, and then click **Go**.
   Alert Management page will display the imported alert.



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

   EventTracker displays message box.

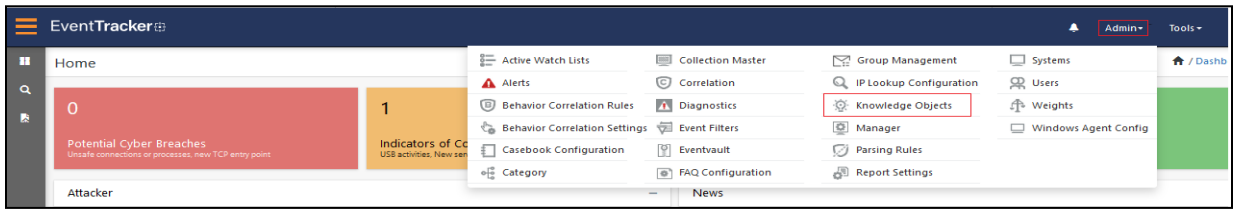


5. Click **OK**, and then click the **Activate Now** button.

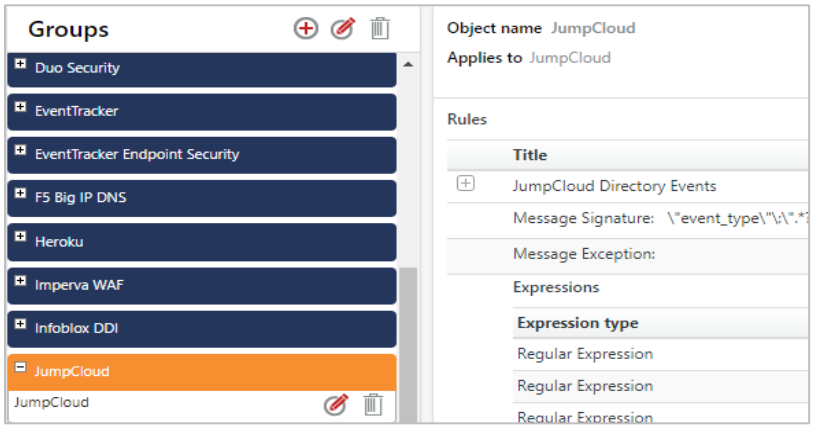
NOTE: Specify appropriate **system** in **alert configuration** for better performance.

6.3 Knowledge Object

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



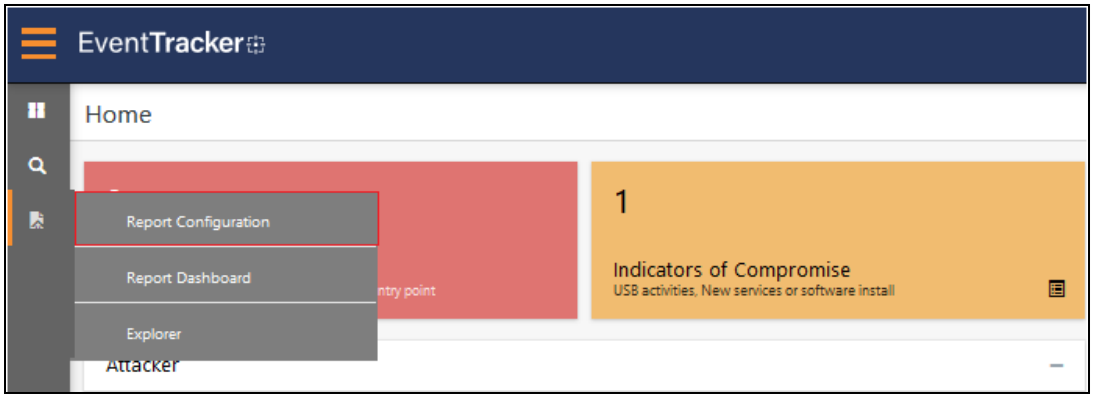
2. In the Knowledge Object tree, expand **JumpCloud** group folder to view the imported knowledge object.



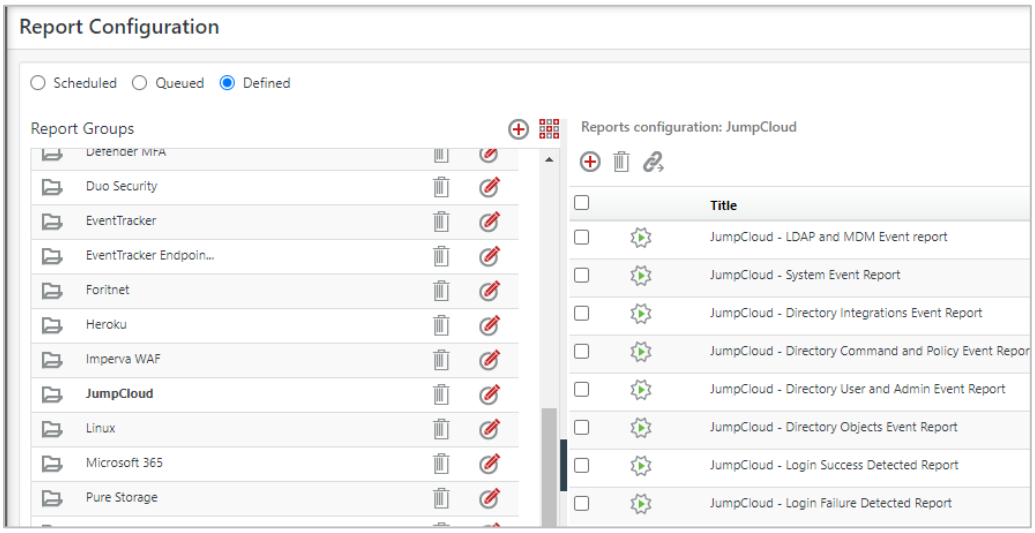
3. Click **Activate Now** to apply imported knowledge objects.

6.4 Report

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

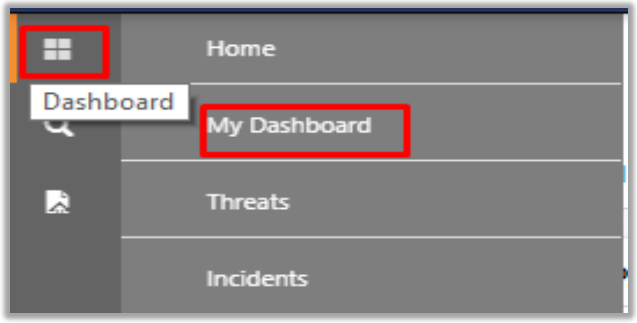


2. In **Reports Configuration** pane, select **Defined** option.
3. Click on the **JumpCloud** group folder to view the imported reports.

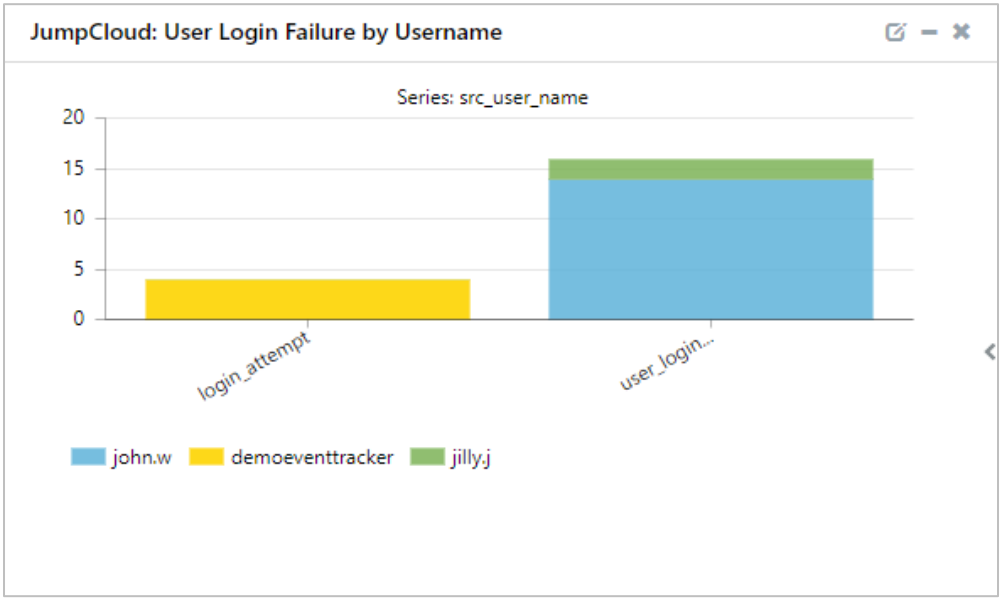


6.5 Dashboards

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



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 EventTracker 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 BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location 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 netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

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