Integrate MAC OS X

EventTracker v8.x and above

Publication Date: February 27, 2019
Abstract

This guide provides instructions to configure MAC OS X (Sierra, High Sierra and Mojave) to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor MAC OS X (Sierra, High Sierra and Mojave).

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v8.x or above and Apple Mac OS X (Sierra, High Sierra and Mojave).

Audience

Administrators who are assigned the task to monitor MAC OS X (Sierra, High Sierra and Mojave) events using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Table of Contents

Abstract .................................................................................................................................................. 1
Scope ................................................................................................................................................... 1
Audience ................................................................................................................................................ 1
Overview ............................................................................................................................................. 4
Prerequisites ....................................................................................................................................... 4
Configure MAC OS X to forward logs to EventTracker ................................................................... 4
  To configure the MAC OS X to forward logs to a syslog server, .................................................... 4
Configuring ETAgent Manually on Client Machine ............................................................................. 9
  For GUI Installation .......................................................................................................................... 9
  For Command line installation ......................................................................................................... 12
Configuring ETAgent using munki package manager ....................................................................... 13
EventTracker Knowledge Pack .......................................................................................................... 17
  Flex Reports .................................................................................................................................... 17
  Alerts ............................................................................................................................................... 21
  Categories and Saved searches ....................................................................................................... 21
  Knowledge Objects .......................................................................................................................... 22
Import MAC OS X knowledge pack into EventTracker .................................................................... 22
  Category ......................................................................................................................................... 23
  Alerts ............................................................................................................................................... 25
  Knowledge Objects .......................................................................................................................... 27
  Flex Reports .................................................................................................................................... 28
  Dashboards ..................................................................................................................................... 29
Verify MAC OS X knowledge pack in EventTracker ......................................................................... 32
  Categories ....................................................................................................................................... 32
  Alerts ............................................................................................................................................... 33
  Token Templates ............................................................................................................................. 33
  Knowledge Objects .......................................................................................................................... 34
  Flex Reports .................................................................................................................................... 34
  Dashboards ..................................................................................................................................... 35
Create Dashlets ................................................................. 35
Sample Flex Dashboards ..................................................... 39
Overview

Apple Macintosh Operating System, a Unix-like Operating system also known as Mac OS. It is a very popular operating system around the world. Mac contains numerous log files, with all sorts of information, sent by various system processes and applications. These logs can be forwarded to Syslog Server.

With EventTracker, you can monitor Mac OS events from a single view. EventTracker checks the status and availability of Mac OS critical processes and it centrally consolidates all the syslog. EventTracker is having capability of generating flex reports and can also trigger alerts whenever it detects any suspicious activity. These alerts and flex reports will help you to analyze login and logout activity, authentication failure, any kind of administrator activity, network activities and process activities.

Prerequisites

- Please make sure the port 514 is open in MAC OS firewall.
- Please add exception for port 514 in firewall if exists in between MAC OS X and EventTracker Manager.

Configure MAC OS X to forward logs to EventTracker

To configure the MAC OS X to forward logs to a syslog server,

1. Contact EventTracker support for MAC_OS_X_Integrator.
2. Download the file on Server MAC OS machine.
3. Save MAC_OS_X_Integrator.zip file and extract the contents of the file to the folder.
4. Go to Utility folder and open the Terminal.
5. Change the directory to where <Extracted MAC_OS_X_Integrator Folder Name> is located.
6. Make sure the below file has executable permission.
   <Extracted MAC_OS_X_Integrator Folder Name>/etintegrator
Integrate MAC OS X

7. If not executable, use below command to make it executable.

   chmod a+x ETlogger/etintegrator

8. Click etintegrator in <Extracted MAC_OS_X_Integrator Folder Name>

9. Enter the password for User ETAdmin

**NOTE:** This user has Admin privilege to collect audit logs from the MAC OS. Hence this user account will be created in all the machine where you are installing the ETAgent with the same credentials. It is recommended to provide a strong password.
10. Re-enter the same password provided above for verification purpose.
11. Provide the EventTracker Manager IP Address.

![Image of terminal session]

Figure 4

12. Provide the EventTracker manager syslog port.

![Image of terminal session]

Figure 5
13. Provide the protocol used for the syslog messages to forward. By default, UDP will be configured.

![Figure 6](image)

14. Once configuration is completed close the terminal window.

![Figure 7](image)
15. Check the `<Extracted MAC_OS_X_Integrator Folder Name>` folder `etagent.pkg` file that will be created.

![Image of ETlogger with etagent.pkg highlighted]

**Figure 8**

**Configuring ETAgent Manually on Client Machine**

**For GUI Installation**

1. Copy the `etagent.pkg` to client MAC machine.
2. Go to Utility folder and open the Terminal.
3. Navigate to the directory where `etagent.pkg` is located using ‘cd’ command.
4. Click on the `etagent.pkg` and proceed as mentioned in the below images.
5. Click **Continue** to proceed further.
6. Select your system disk to install software and click Continue button.
7. Click **Install** button to install the software.

![Figure 11](image)

8. Provide the Admin Username and password. Once you provide the admin user credential, click **Install Software**.

![Figure 12](image)
9. Once installation is completed, click the **Close** button.

![Install Mac OS X]

*Figure 13*

**For Command line installation**

1. Run the below command using admin privilege.
   
   ```bash
   Sudo installer -pkg etagent.pkg -target /
   ```

![Command line installation]

*Figure 14*
Configuring ETAgent using munki package manager

If you have munki package manager configured in your environment, use below method to add the package to the munki repo.

1. Go to Utility folder and open the Terminal.
2. Navigate to the directory where etagent.pkg is located using ‘cd’ command.
3. Enter below command to import the package to munki repository:

   Munkiimport etagent.pkg

   ![Image 15](image15)

   ```
   [Admins-Mac-2:etagent bhawk]$ ls
   etagent.pkg
   [Admins-Mac-2:etagent bhawk]$ munkiimport etagent.pkg
   ```

   **Item name:** etagent  
   **Display name:** ETAgent  
   **Description:** EventTracker logger  
   **Version:** 2.0  
   **Category:** logger  
   **Unattended install:** True  
   **Unattended uninstall:** True  
   **Catalogs:** testing  

   [Import this item? [y/n] y  
   Upload item to subdirectory path []: /apps/etlogger  
   Path /apps/etlogger doesn’t exist. Create it? [y/n] y  
   No existing product icon found.  
   Attempt to create a product icon? [y/n] y  
   Copying etagent.pkg to repo...  
   Copied etagent.pkg to pkgs/apps/etlogger/etagent-2.0.pkg.  
   [Edit pkginfo before upload? [y/n]: n  
   [Saved pkginfo to pkginfo/apps/etlogger/etagent-2.0.  
   Rebuild catalogs? [y/n]: y  
   Rebuilding catalogs at file:///Users/Shared/munki_repo...  
   Admins-Mac-2:etagent bhawk$`

4. Fill the details as mentioned in the above the image.
5. To create a client manifest for the etagent package, enter the command:
   ```manifestutil```
6. Add package in manifest using command:
   ```add-pkg etagent –manifest site_default```
Integrate MAC OS X

For installing and configuring the munki repository navigate to the link: 
https://github.com/munki/munki/wiki/Demonstration-Setup

Verify the ETAgent Installation:

1. Go to System Preferences from apple menu.

2. Select Users & Groups.
3. Check whether the ETAdmin user was created.
4. Open terminal and enter the below command to check whether the following files were created.

\textbf{Sudo ls /Users/ETAdmin/Integrator/}

![Figure 20](image)

5. Check whether the cron job was created under the user ETAdmin.

\textbf{Sudo crontab -u ETAdmin -l}

![Figure 21](image)
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 Enterprise to support MAC OS X.

Flex Reports

- **MAC OS X - Administrative activities** - This report gives the information about any kind of administrative activities in MAC OS X.

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Computer</th>
<th>Username</th>
<th>Activity</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Apr 30 17:38:43</td>
<td>PH 0001-001</td>
<td>administrator</td>
<td>auditon</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:38:43</td>
<td>PH 0001-001</td>
<td>administrator</td>
<td>auditon</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:38:59</td>
<td>PH 0001-001</td>
<td>administrator</td>
<td>auditon</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:38:59</td>
<td>PH 0001-001</td>
<td>administrator</td>
<td>setaudit_addr</td>
<td>failure: Operation not permitted</td>
</tr>
</tbody>
</table>

Sample logs:

```
<timestamp> Apr 30 19:02:29:15 PM
<event_log_type> Application
<event_type> Information
<event_id> 3333
<event_source> Syslog
<event_user_domain> N/A
<event_computer> MAC OS
<event_user_name> N/A
<event_description>

Apr 30 19:02:29:15 PM: PH 0001-001: user=administrator, pid=247, tid=0
```

- **MAC OS X - Authentication and Authorization** - This report gives the information about user authentication and authorization activities in MAC OS X.

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Computer</th>
<th>Username</th>
<th>Terminal Host Address</th>
<th>Activity</th>
<th>Activity info</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Apr 30 17:38:43</td>
<td>PH 0001-001</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>user authentication</td>
<td>Verify password for record type Users file &quot;/etc/audit&quot; node &quot;local_default&quot;</td>
<td>failure: Unknown error: 255</td>
</tr>
<tr>
<td>Mon Apr 30 17:38:43</td>
<td>PH 0001-001</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>user authentication</td>
<td>Verify password for record type Users file &quot;/etc/audit&quot; node &quot;local_default&quot;</td>
<td>failure: Unknown error: 255</td>
</tr>
<tr>
<td>Mon Apr 30 17:38:43</td>
<td>PH 0001-001</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>sudo</td>
<td>/usr/bin/audit /audit /etc/audit file &quot;/etc/audit&quot; node &quot;local_default&quot;</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:38:43</td>
<td>PH 0001-001</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>SecServ AuthEngine</td>
<td>end evaluation</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:38:43</td>
<td>PH 0001-001</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>SecServ AuthEngine</td>
<td>system services, system configuration configuration file &quot;/etc/audit&quot; node &quot;local_default&quot;</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:38:43</td>
<td>PH 0001-001</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>SecServ AuthEngine</td>
<td>system services, system configuration configuration file &quot;/etc/audit&quot; node &quot;local_default&quot;</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:38:43</td>
<td>PH 0001-001</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>SecServ AuthEngine</td>
<td>begin evaluation</td>
<td>success</td>
</tr>
</tbody>
</table>
Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 02 02:29:15 PM</td>
<td>Apr 27 17:36:44 pri-winx-wst01 header,146,11,user authentication,0,Sun Sep 25 18:39:08 2016, + 912 msec,subject_mbsetupsuser_mbsetupsuser_mbsetups</td>
</tr>
</tbody>
</table>

- **MAC OS X - Command executed** - This report gives information about command executed by users.

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Computer</th>
<th>Username</th>
<th>Terminal machine address</th>
<th>Command executed</th>
<th>Path</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Apr 30 17:37:35 2018</td>
<td>PHOENIXS-AR-SYSLOG</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>createhome10dr dir -c</td>
<td>/usr/bin/createmodi r</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:37:35 2018</td>
<td>PHOENIXS-AR-SYSLOG</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>grep, v-shell</td>
<td>/usr/bin/grep</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:37:35 2018</td>
<td>PHOENIXS-AR-SYSLOG</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>grep, v-shell</td>
<td>/usr/bin/grep</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:37:43 2018</td>
<td>PHOENIXS-AR-SYSLOG</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>grep, v-shell</td>
<td>/usr/bin/grep</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:37:43 2018</td>
<td>PHOENIXS-AR-SYSLOG</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>grep, v-shell</td>
<td>/usr/bin/grep</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:37:43 2018</td>
<td>PHOENIXS-AR-SYSLOG</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>grep, v-shell</td>
<td>/usr/bin/grep</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:37:43 2018</td>
<td>PHOENIXS-AR-SYSLOG</td>
<td>administrator</td>
<td>0.0.0.0</td>
<td>grep, v-shell</td>
<td>/usr/bin/grep</td>
<td>success</td>
</tr>
</tbody>
</table>

Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 02 02:29:15 PM</td>
<td>Apr 25 16:29:16 phoenix-air header,184,11,execute(0),0,Tue Apr 24 19:22:59 2018, + 372 msec,exec arg,sh, -c, logger -p install.info &quot;Begin script: updateHel...</td>
</tr>
</tbody>
</table>

- **MAC OS X - Login and Logout activities** - This report gives information about user login and logout activities based on local or remote.
Sample logs:

- **MAC OS X - Network traffic activities** - This report gives information about network traffic flow details.
Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 02 02:29:15 PM</td>
<td>Apr 25 16:30:26 phoenix-air-header,100,11,bind(2,0),Tue Apr 24 15:58:06 2018, + 991 msec, argument,1,0x4fd,socket/inet6,26,25008:0;subject,administrator,staff,472,100007,50331650,0,0.0.0;return,success,0,trailer,100,</td>
</tr>
</tbody>
</table>

- **MAC OS X - File and Folder operations** - This report gives information about operation happening on file and folder like modification, creation and deletion.

Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 02 02:29:15 PM</td>
<td>Apr 25 16:30:26 phoenix-air-header,347,11,mkdir(2),0,Tue Apr 24 13:26:39 2018, + 618 msec,path=/var/folders/yg/11c74w05d9d3ztzg23f40000gn/T/cci...</td>
</tr>
</tbody>
</table>
• **MAC OS X - User and Group management** - This report gives information about user and group management activities like modification, creation and addition.

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Computer</th>
<th>Changed by</th>
<th>Activity</th>
<th>Target name</th>
<th>Activity Info</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon Apr 30 17:41:28 2018</td>
<td>PHOENIXS-AR-SYSLOG</td>
<td>administrator</td>
<td>create user</td>
<td>ETAdmin1</td>
<td>Create record type Users ‘ETAdmin1’ node ‘/Local/Default’</td>
<td>failure: Unknown error 255</td>
</tr>
<tr>
<td>Mon Apr 30 17:42:10 2018</td>
<td>PHOENIXS-AR-SYSLOG</td>
<td>administrator</td>
<td>delete user</td>
<td>ETAdmin1</td>
<td>Delete record type Users ‘ETAdmin1’ node ‘/Local/Default’</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:42:45 2018</td>
<td>PHOENIXS-AR-SYSLOG</td>
<td>administrator</td>
<td>create user</td>
<td>etadmin3</td>
<td>Create record type Users ‘etadmin3’ node ‘/Local/Default’</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:42:46 2018</td>
<td>PHOENIXS-AR-SYSLOG</td>
<td>administrator</td>
<td>modify user</td>
<td>etadmin3</td>
<td>Set values for record type Users ‘etadmin3’ node ‘/Local/Default’</td>
<td>success</td>
</tr>
<tr>
<td>Mon Apr 30 17:42:46 2018</td>
<td>PHOENIXS-AR-SYSLOG</td>
<td>administrator</td>
<td>modify user</td>
<td>etadmin3</td>
<td>Set values for record type Users ‘etadmin3’ node ‘/Local/Default’</td>
<td>success</td>
</tr>
<tr>
<td>Wed Apr 18 14:10:52 2018</td>
<td>PRI-WNK-WST01-SYSLOG</td>
<td>admin</td>
<td>modify user</td>
<td>SSwayne</td>
<td>Set values for record type Users ‘SSwayne’ node ‘/Local/Default’</td>
<td>success</td>
</tr>
<tr>
<td>Wed Apr 18 14:10:52 2018</td>
<td>PRI-WNK-WST01-SYSLOG</td>
<td>admin</td>
<td>modify user</td>
<td>SSwayne</td>
<td>Set values for record type Users ‘SSwayne’ node ‘/Local/Default’</td>
<td>success</td>
</tr>
<tr>
<td>Wed Apr 18 14:10:54 2018</td>
<td>PRI-WNK-WST01-SYSLOG</td>
<td>admin</td>
<td>add to group</td>
<td>ldapadmin</td>
<td>Added Groups membership username to ‘_ldapadmin’ node ‘/Local/Default’</td>
<td>success</td>
</tr>
<tr>
<td>Wed Apr 18 14:10:54 2018</td>
<td>PRI-WNK-WST01-SYSLOG</td>
<td>admin</td>
<td>add to group</td>
<td>appserveran</td>
<td>Added Groups membership username to ‘_appserveran’ node ‘/Local/Default’</td>
<td>success</td>
</tr>
</tbody>
</table>

**Figure 34**

**Sample logs:**

- **MAC OS X: Login failure** - This alert will be generated when the user login failure is attempted.
- **MAC OS X: User authentication failure** - This alert will be generated when the user authentication failure happened.

**Categories and Saved searches**

- **MAC OS X - Administrative activities** - This category based report provides information related to administrative activities.
- **MAC OS X - Authentication and Authorization** - This category based report provides information related to user authentication and authorization activities.
• **MAC OS X - Command executed** - This category based report provides information related to command executed by users.

• **MAC OS X - Login and Logout activities** - This category based report provides information related to user login and logout activities based on local or remote.

• **MAC OS X - Network traffic activities** - This category based report provides information related to network traffic flow details.

• **MAC OS X - File operations** - This category based report provides information related to operation happens on file and folder like modification, creation and deletion.

• **MAC OS X - User and Group management** - This category based report provides information related to user and group management activities like modification, creation and addition.

**Knowledge Objects**

• **MAC OS X - Administrative activities** - This knowledge object helps to analyze logs related to administrative activities.

• **MAC OS X - Authentication and Authorization** - This knowledge object helps to analyze logs related to user authentication and authorization activities.

• **MAC OS X - Command executed** - This knowledge object helps to analyze logs related to command executed by users.

• **MAC OS X - Login and Logout activities** - This knowledge object helps to analyze logs related to user login and logout activities based on local or remote.

• **MAC OS X - Network traffic activities** - This knowledge object helps to analyze logs related to network traffic flow details.

• **MAC OS X - File operations** - This knowledge object helps to analyze logs related to operation happens on file and folder like modification, creation and deletion.

• **MAC OS X - User and Group management** - This knowledge object helps to analyze logs related to all the URL filtering that is done.

**Import MAC OS X knowledge pack into EventTracker**

**NOTE:** Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Templates
- Knowledge Objects
- Flex Reports
- Dashboards
1. Launch **EventTracker Control Panel**.

2. Double click **Export Import Utility**.

3. Click the **Import** tab.

**Category**

1. Click **Category** option, and then click the browse button.
2. Locate Category_MAC OS X.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.
1. Click **Alert** option, and then click the browse button.

   ![Figure 39](image)

2. Locate Alert_MAC OS X.isalt file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

   ![Figure 40](image)

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

1. Click **Parsing rules** under **Admin** option in the EventTracker manager page.

2. Move to **Template** and click on import configuration icon on the top right corner.

3. In the popup window browse the file named **Token Template_ MAC OS X.ettd**.

4. Now select all the check box and then click on **Import** option. EventTracker displays success message.

5. Click **OK**, and then click the **Close** button.
Knowledge Objects

1. Click Knowledge objects under Admin option in the EventTracker manager page.
2. Locate the KO_MAC OS X.etko file.

3. Click the ‘Upload’ option.
4. Now select all the check box and then click on ‘Import’ option.

5. Knowledge objects are now imported successfully.
6. Click **OK**, and then click the **Close** button.

**Flex Reports**

On EventTracker Control Panel,

1. Click **Reports** option, and select new (***.etcrx**) from the option.

2. Locate the **Reports_MAC OS X.etcrx** file, and select all the check box.
3. Click the **Import** button to import the reports. EventTracker displays success message.

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

**Dashboards**

**Note:** If you have EventTracker Enterprise version **v9.0**, you can import dashboards.

1. Open EventTracker Enterprise.
2. Navigate to **Dashboard>My Dashboard**.
   My Dashboard pane is shown.

3. Click the ‘**Import**’ button to import the dashlets.
5. Click the ‘Upload’ option.

![Figure 51](image)

6. Now select all the check box and then click on ‘Import’ option. Dashlets are now imported successfully.
7. Click the ‘Add’ button to create a new dashlets.

![Figure 52](image)
8. Fill suitable Title and Description and click Save button.
9. Click 'Customize' to locate “Mac OS X” dashlets and choose all created dashlets for Mac OS X.
10. Click ‘Add’ dashlet to create dashboard.

![Customize dashlets](image)

**Figure 53**

**Verify MAC OS X knowledge pack in EventTracker Categories**

1. Logon to EventTracker Enterprise.
2. Click Admin dropdown, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand MAC OS X group folder to view the imported categories.

![Category Tree](image)

**Figure 54**
Integrate MAC OS X

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In search box, enter **MAC OS X** and then click the **Search** button.
   
   EventTracker displays alert of **MAC OS X**.

   ![Alerts](image)

   **Figure 55**

Token Templates

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Parsing rules**.
2. On **Template** tab, click on the **MAC OS X** group folder to view the imported Token Values.

   ![Parsing Rules](image)

   **Figure 56**
Knowledge Objects

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

2. In the Knowledge Object tree, expand MAC OS X group folder to view the imported Knowledge objects.

![Knowledge Objects](image)

Figure 57

Flex Reports

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

![Report Configuration](image)

Figure 58

2. In Reports Configuration pane, select Defined option.
3. Click on the MAC OS X group folder to view the imported MAC OS X reports.
Dashboards

1. Open EventTracker Enterprise in browser and logon.
2. Navigate to Dashboard>My Dashboard.
   
   My Dashboard pane is shown.

Create Dashlets

Note: If you have EventTracker Enterprise version v8.0, you can follow the below steps to create dashlets.

1. Open EventTracker Enterprise in browser and logon.
2. Navigate to **Dashboard>My Dashboard**. My Dashboard pane is shown.

3. Click the ‘**Add**’ button to create a new dashlet.

4. Fill suitable Title and Description and click **Save** button.

5. Click **Configure** to configure a new dashlet. Widget configuration pane is shown.
6. Locate earlier scheduled report in Data Source dropdown.
7. Select Chart Type from dropdown.
8. Select extent of data to be displayed in Duration dropdown.
9. Select computation type in Value Field Setting dropdown.
10. Select evaluation duration in As Of dropdown.
11. Select comparable values in X Axis with suitable label.
12. Select numeric values in Y Axis with suitable label.
13. Select comparable sequence in Legend.
14. Click Test button to evaluate.

Evaluated chart is shown.
15. If satisfied, click **Configure** button.

16. Click ‘**Customize**’ to locate and choose created dashlet.

17. Click ‘**Add**’ dashlet to earlier created dashboard.
Sample Flex Dashboards

1. **MAC OS X- Authentication and Authorization**: This dashboard provides information related to user authentication and authorization activities.

![Mac OS X- Authentication and Authorization](image)

2. **MAC OS X- User Authentication failure**: This dashboard provides information related to user authentication failure activities.

![User Authentication failure](image)

Figure 66
3. **MAC OS X- User and Group management**: This dashboard provides information related to user and group management activities like addition, creation and modification.

4. **MAC OS X- File and Folder access denied activities**: This dashboard provides information related to failure file and folder access details.
5. **MAC OS X- Login and Logout activities**: This dashboard provides information related to user login and logout activities.