

# Integrate eDirectory

*EventTracker v7.x*

# Abstract

eDirectory™ is a full-service, secure LDAP directory providing incredible scalability and an agile platform to run your organization's identity infrastructure and multi-platform network services.

This guide provides instructions to configure eDirectory to send the syslog to EventTracker Enterprise. Once syslog is been configured to send to EventTracker Manager, alerts and reports can be configured into EventTracker.

## Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, and **NetIQ eDirectory v8.8 SP7 or later**.

## Audience

Administrators who are responsible for Monitoring NetIQ eDirectory using EventTracker Manager.

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

*This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.*

*Prism Microsystems 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 Prism Microsystems, 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.*

*© 2014 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Contents

Abstract.....	1
Scope .....	1
Audience.....	1
eDirectory.....	3
Prerequisites.....	3
Configuring XDas Events.....	3
Configuring the XDASv2 Property File to send events to EventTracker .....	7
Loading Modules .....	8
Import eDirectory knowledge pack into EventTracker.....	9
Import Category.....	10
Import Alerts.....	10
Verify eDirectory knowledge pack in EventTracker .....	11
Verify categories.....	11
Verify alerts.....	11
EventTracker Knowledge Pack (KP) .....	13
Alerts .....	15
Reports.....	15

# eDirectory

Novell® eDirectory™ is a highly scalable, high-performing, secure directory service. It can store and manage millions of objects, such as users, applications, network devices, and data. Novell eDirectory offers a secure identity management solution that runs across multiple platforms, is internet-scalable, and extensible.

Novell eDirectory provides centralized identity management, infrastructure, Net-wide security, and scalability to all types of applications running behind and beyond the firewall. Novell eDirectory 8.7.3 includes Web-based and wireless management capabilities, allowing you to access and manage the directory and users, access rights, and network resources from a Web browser and a variety of handheld devices.

Novell eDirectory natively supports the directory standard Lightweight Directory Access Protocol (LDAP) 3 and provides support for TLS/SSL services based on the OpenSSL source code

## Prerequisites

- EventTracker should be installed
- eDirectory v8.8 SP7 should be installed.
- iManager 2.7.7 or later with NetIQ audit plug-in should be installed.

## Configuring XDAS Events

Use this page to configure XDASv2 events.

1. Log in to the **iManager** console.
2. Open **iManager** from a Web browser, using the following URL:

**`https://ip_address_or_DNS/nps/iManager.html`**

where ip\_address\_or\_DNS is the IP address or DNS name of your iManager server.

Example: **`http://192.168.0.5/nps/iManager.html`**

3. Log in using your username and password.

In iManager, you have access only to those roles for which you have assigned rights. To have full access to all NetIQ iManager features, you must log in as a user with Admin rights to the tree.

4. Select **Audit Configuration** from **Roles and Tasks**.
5. Specify the name of your eDirectory server in NCP Server.

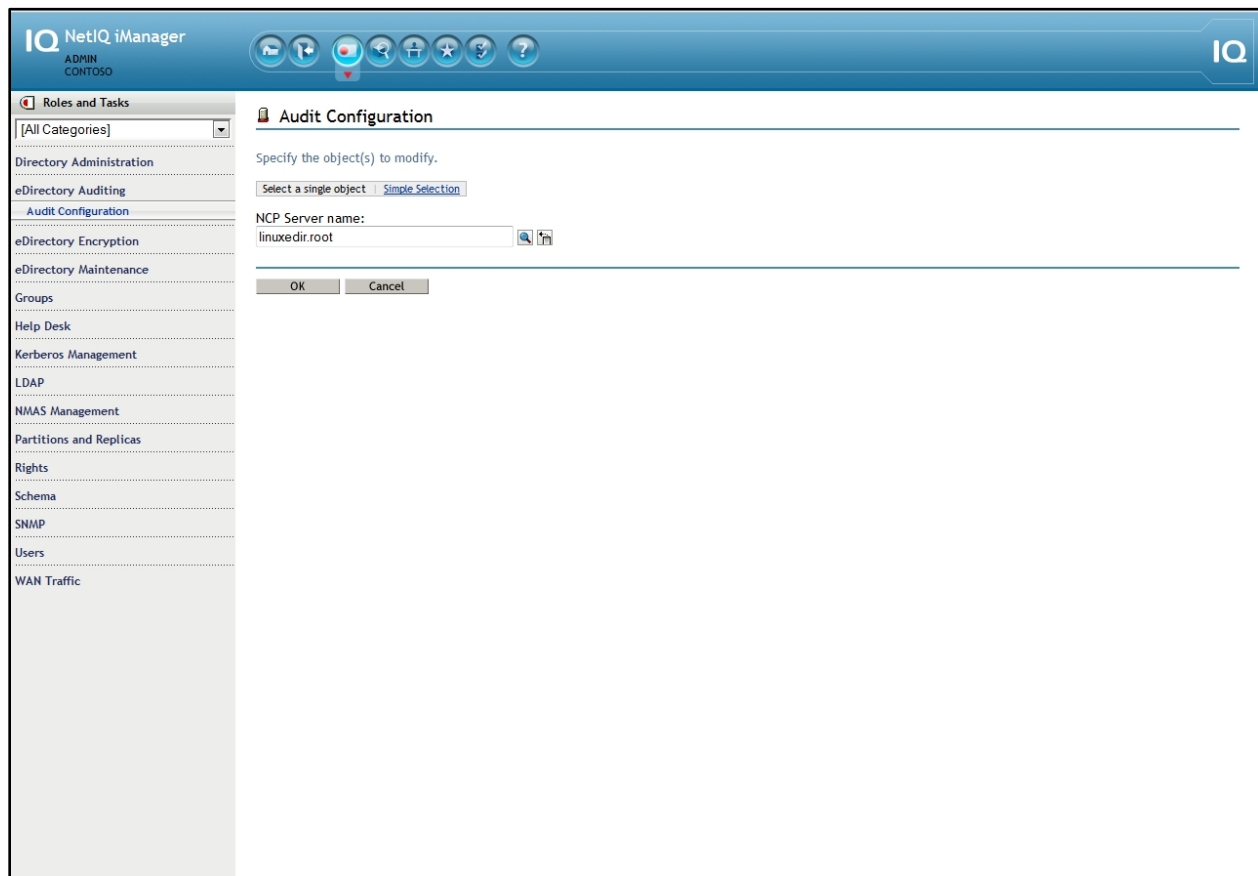


Figure 1

6. Click the Object Selector icon to browse for the eDirectory server.
7. Click **OK**.

The XDASv2 Audit page is displayed. Use this page to configure XDASv2 events.

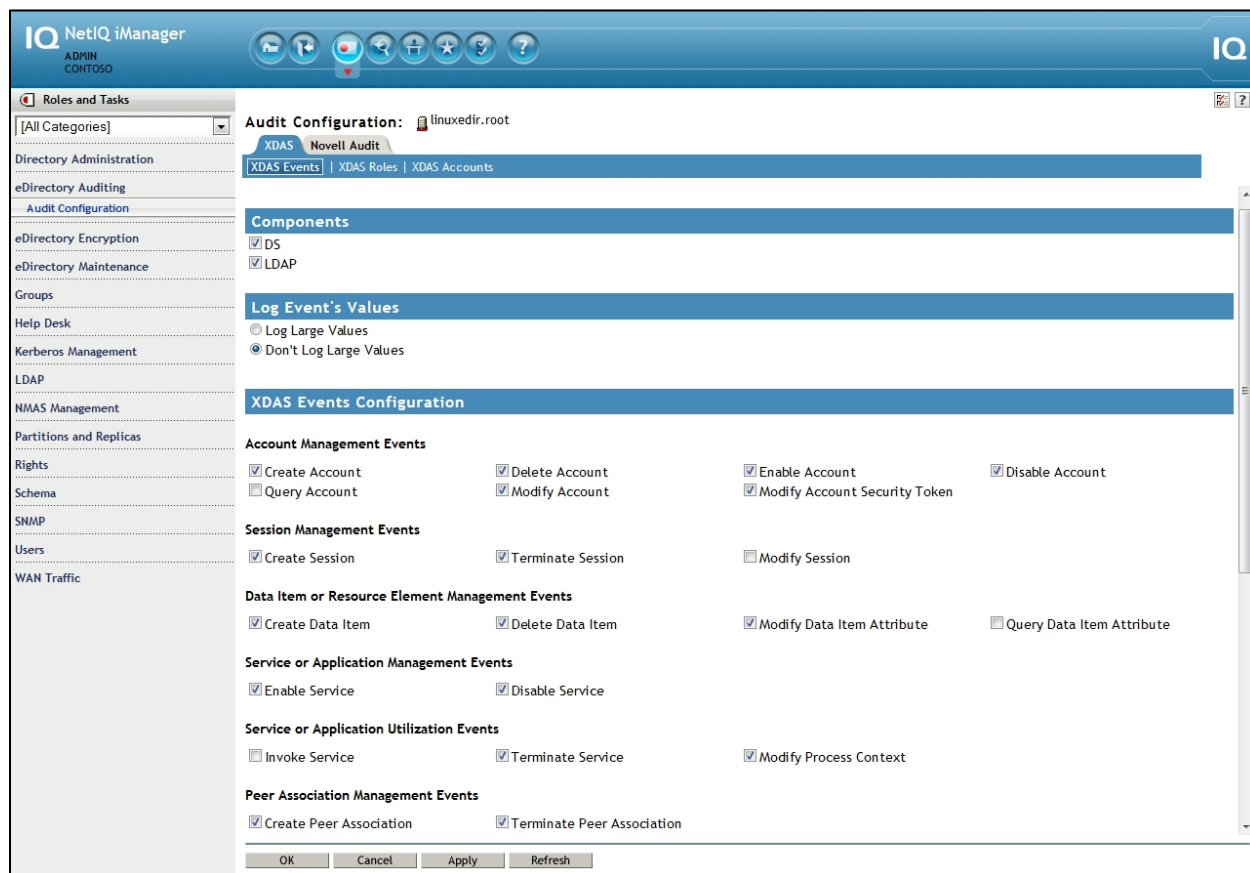


Figure 2

### 8. Log event values:

The events are logged into a text file. Event values with more than 768 bytes in size are considered 'large values.' You can log events of any size.

**Log Large Values:** Select this option to log events that are more than 768 bytes in size.

**Don't Log Large Values:** Select this option to log events that are less than 768 Byte in size. If the event size is more, the event value is truncated and saved to the log file.

### 9. You can select both or either of the following components for XDASv2 event settings:

**DS:** Specifies an eDirectory object. For each DS object, a corresponding LDAP object exists.

**LDAP:** Specifies an LDAP object.

**NOTE**

You can select the DS and LDAP components at the granular level for the XDAS events. Based on the event you select, the appropriate components that are supported for that event are selected.

For example, if you select the Delete Account event, the DS and LDAP components are selected.

10. Specify the following events based on your requirements:

Events	Description
Account Management Events	Select the account management events for which you want to log events. You can log events to create, delete, enable, disable, and query accounts, and also to modify account security token.
Session Management Events	Select the session management events for which you want to log events. You can log events to create, terminate, and modify sessions.
Data Item or Resource Element Management Events	Select the data item or resource element management events for which you want to log events. You can log events to create and delete data items and to modify and query data item attributes.
Service or Application Management Events	Select the service or application management events for which you want to log events. You can log events for enabling and disabling services.
Service or Application Utilization Events	Select the service or application utilization events for which you want to log events. You can log events to start and terminate services, and to modify process contexts.
Peer Association Management Events	Select the peer association events for which you want to log events. You can log events for creating and terminating peer associations.
Data Item or Resource Element Content Access Events	Select the data item or resource element content access events for which you want to log events. You can log events to create, terminate, and modify data item associations.
Role Management Events	Select the role management events for which you want to log events. You can log events to create, delete, query, and modify attributes or objects of eDirectory objects.
Exceptional Management Events	Select the exceptional management events for which you want to log events. You can log events to start and shut down systems and also to back up and recover data stores.
Authentication Management Events	Select the authentication management events for which you want to log events. You can log events to authenticate sessions and create access tokens.
Operational Events	Select the operational management events for which you want to log events. You can log events to generate eDirectory operation IDs.

11. Click **Apply** and then click **OK**.

## Configuring the XDASv2 Property File to send events to EventTracker

When you install eDirectory, the installer lay down the **xdasconfig.properties** in **/etc/opt/novell/eDirectory/conf/** directory. For non-root installations, the XDASv2 property file is located in the conf directory. You can customize the file according to your requirements. To enable the **Syslog appender**, make the following changes in the **xdasxconfig.properties** file:

1. Change the following entry to S, to attach a Syslog appender:log4j.rootLogger=debug, S
2. Uncomment the following entries:
  - log4j.appender.S=org.apache.log4j.net.SyslogAppender
  - log4j.appender.S.Host=localhost (**IP address of EventTracker Manager**)
  - log4j.appender.S.Port=port (**default is 514**)
  - log4j.appender.S.Protocol=UDP
  - log4j.appender.S.SSLCertFile=/etc/opt/novell/mycert.pem
  - log4j.appender.S.Threshold=INFO
  - log4j.appender.S.Facility=USER
  - log4j.appender.S.layout=org.apache.log4j.PatternLayout
  - log4j.appender.S.layout.ConversionPattern=%c : %p%m%n

## Loading Modules

After you have configured the XDASv2 events, run the following commands to load the XDASv2 modules:

**To automatically load the xdasauditds module whenever the ndsd server is started:**

Add xdasauditds to the /etc/opt/novell/eDirectory/conf/ndsmodules.conf file.

**To manually load and unload the xdasauditds module:**

### Linux

To load, run `ndstrace -c "load xdasauditds"`.

# Import eDirectory knowledge pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **ExportImport Utility**, and then click the **Import** tab.

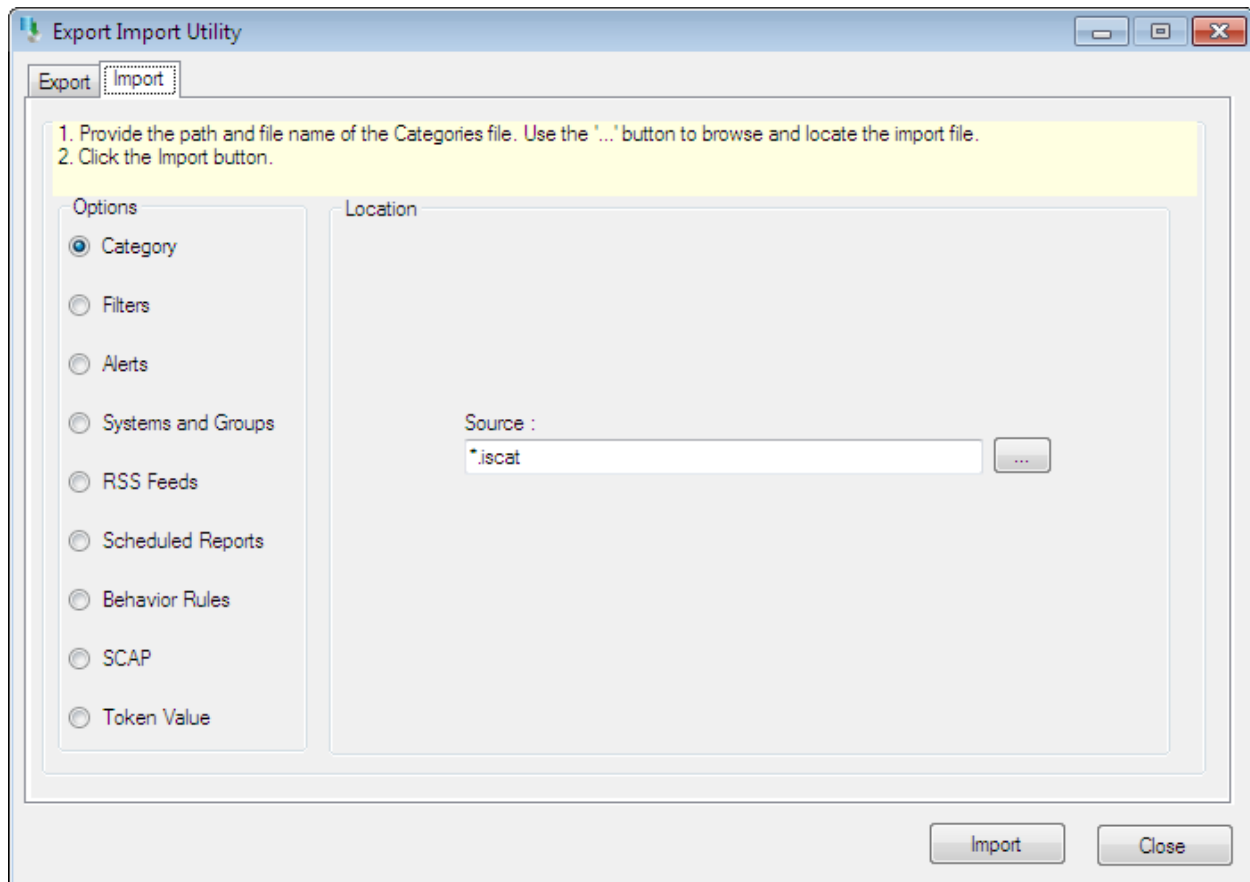



Figure 3

## Import Category

Import **Category/Alert** as given below.

1. Click **Category** option, and then click the **browse**  button.
2. Locate **All eDirectory group of categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

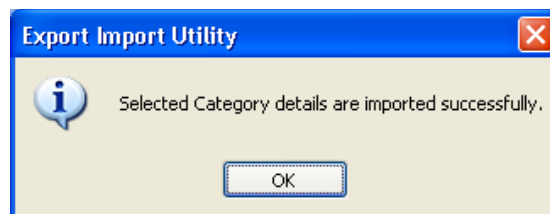



Figure 4

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

## Import Alerts

1. Click **Alert** option, and then click the **browse**  button.
2. Locate **All eDirectory group of alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

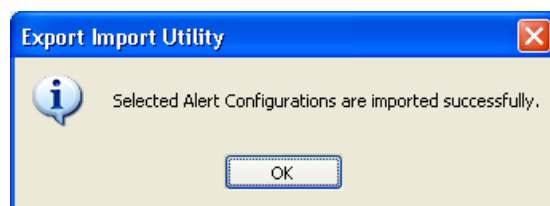


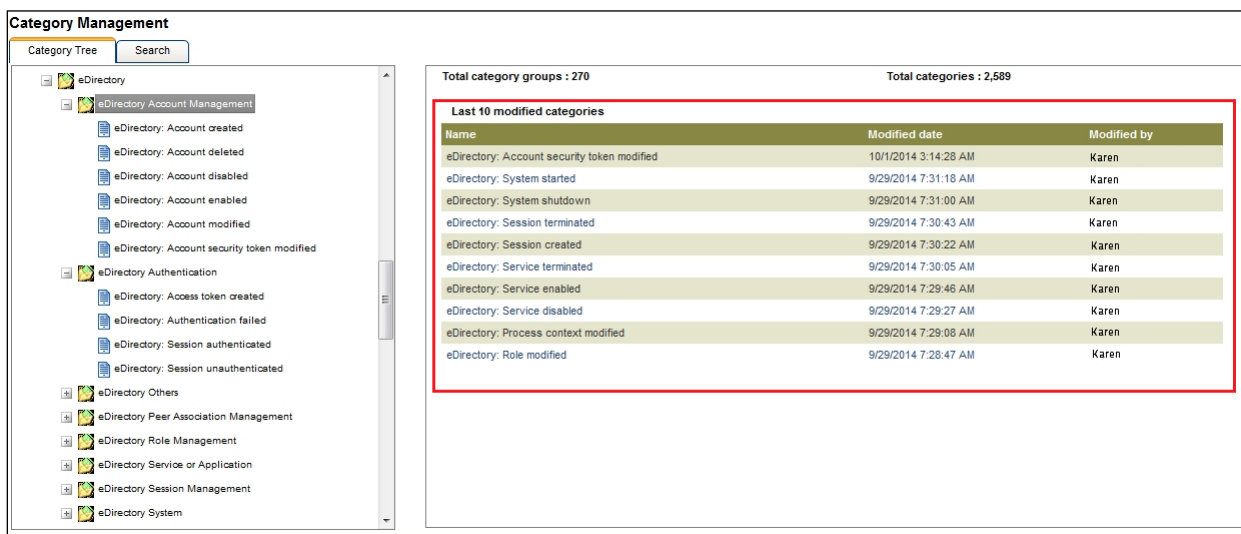
Figure 5

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

# Verify eDirectory knowledge pack in EventTracker

## Verify categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Categories**.
3. To view the imported categories, in the **Category Tree**, expand **eDirectory** group folder.



The screenshot displays the 'Category Management' interface. On the left, the 'Category Tree' shows a hierarchy starting with 'eDirectory', which is expanded to show 'eDirectory Account Management' and its sub-items: 'eDirectory: Account created', 'eDirectory: Account deleted', 'eDirectory: Account disabled', 'eDirectory: Account enabled', 'eDirectory: Account modified', and 'eDirectory: Account security token modified'. Below these are 'eDirectory Authentication' (with sub-items: 'eDirectory: Access token created', 'eDirectory: Authentication failed', 'eDirectory: Session authenticated', 'eDirectory: Session unauthenticated'), 'eDirectory Others', 'eDirectory Peer Association Management', 'eDirectory Role Management', 'eDirectory Service or Application', 'eDirectory Session Management', and 'eDirectory System'.

On the right, the 'Total category groups : 270' and 'Total categories : 2,589' are displayed. Below this, a table titled 'Last 10 modified categories' is shown, listing the most recent category updates.

Name	Modified date	Modified by
eDirectory: Account security token modified	10/1/2014 3:14:28 AM	Karen
eDirectory: System started	9/29/2014 7:31:18 AM	Karen
eDirectory: System shutdown	9/29/2014 7:31:00 AM	Karen
eDirectory: Session terminated	9/29/2014 7:30:43 AM	Karen
eDirectory: Session created	9/29/2014 7:30:22 AM	Karen
eDirectory: Service terminated	9/29/2014 7:30:05 AM	Karen
eDirectory: Service enabled	9/29/2014 7:29:46 AM	Karen
eDirectory: Service disabled	9/29/2014 7:29:27 AM	Karen
eDirectory: Process context modified	9/29/2014 7:29:08 AM	Karen
eDirectory: Role modified	9/29/2014 7:28:47 AM	Karen

Figure 6

## Verify alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In the **Search** box, type '**eDirectory**', and then click the **Go** button.

Alert Management page will display all the imported alerts.

Alert Management													
Search: edirectory Go Show All													
Page Size: 25													
Alert Name	Threat Level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent	Applies To		
<a href="#">eDirectory: Account created</a>	High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	NetIQ eDirectory v8.8 SP7 or later		
<a href="#">eDirectory: Authentication failed</a>	Serious	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	NetIQ eDirectory v8.8 SP7 or later		
<a href="#">eDirectory: Role created</a>	Medium	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	NetIQ eDirectory v8.8 SP7 or later		
<a href="#">eDirectory: Role deleted</a>	High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	NetIQ eDirectory v8.8 SP7 or later		
<a href="#">eDirectory: Service disabled</a>	Serious	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	NetIQ eDirectory v8.8 SP7 or later		
<a href="#">eDirectory: System shutdown</a>	Critical	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	NetIQ eDirectory v8.8 SP7 or later		

\*\*\*Click 'Activate Now' after making all changes

Activate Now Add alert Delete

Figure 7

- To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.



Figure 8

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

# EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Categories and reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker v7 to support eDirectory.

- **eDirectory: Account created** - This category based report provides information about created accounts.
- **eDirectory: Account deleted** - This category based report provides information about deleted accounts.
- **eDirectory: Account disabled** - This category based report provides information about disabled accounts.
- **eDirectory: Account enabled** - This category based report provides information about enabled accounts.
- **eDirectory: Account modified**: This category based report provides information related to account modifications
- **eDirectory: Account security token modified** -This category based report provides information related to account security token has been modified. An account security token may be a password, or any other type of authentication materials associated with a user account.
- **eDirectory: Access token created** - This category based report provides information about created access tokens.
- **eDirectory: Authentication failed** - This category based report provides information about user authentication failures.
- **eDirectory: Session authenticated** - This category based report provides information about user authenticated sessions.
- **eDirectory: Session unauthenticated** - This category based report provides information related to exited sessions.
- **eDirectory: Session created** - This category based report provides information related to sessions which has been created.

- **eDirectory: Session terminated** - This category based report provides information related to sessions which has been terminated.
- **eDirectory: Peer association created** - This category based report provides information about to new peer association creations.
- **eDirectory: Peer association destroyed** - This category based report provides information when a existing peer association is destroyed.
- **eDirectory: Role created** - This category based report provides information related to create a new role, or an attempt is made to create a new role.
- **eDirectory: Role deleted** - This category based report provides information when an existing role is deleted, or an attempt is made to delete an existing role.
- **eDirectory: Process context modified** - This category based report provides information about if any attributes of a process context are modified – this event is somewhat specific to operating systems, but some use can be found in their domain-specific applications.
- **eDirectory: Service disabled** - This category based report provides information related to a service, operation or function which is disabled..
- **eDirectory: Service enabled** - This category based report provides information about a service, operation or function which is enabled..
- **eDirectory: Service terminated** - This category based report provides information about terminated services.
- **eDirectory: Data item association created** - This category based report provides information when rights are granted by an identity to a specific data item when a trust relationship is established between an identity and a data item..
- **eDirectory: Data Item association modified** - This category based report provides information when rights are modified on the previously established relationship between an identity and specific data item.
- **eDirectory: Data Item association terminated** - This category based report provides information when rights are revoked from an identity to a specific data item when a trust relationship is revoked between an identity and a data item.
- **eDirectory: Data item attribute modified** - This category based report provides information about whenever a security-relevant data item or resource element is modified – either the value, or an attribute of the data item.
- **eDirectory: Data item created** - This category based report provides information related to whenever a security-relevant data item or resource element is created..

- **eDirectory: Data item deleted** - This category based report provides information whenever a security-relevant data item or resource element is deleted.

## Alerts

- **eDirectory: Account created** - This alert is generated when an account is created.
- **eDirectory: Authentication failed** - This alert is generated when a user authentication failed.
- **eDirectory: Role created** - This alert is generated when create a new role, or an attempt is made to create a new role.
- **eDirectory: Role deleted** - This alert is generated when an existing role is deleted, or an attempt is made to delete an existing role.
- **eDirectory: Service disabled** - This alert is generated when a service, operation or function is disabled.
- **eDirectory: System shutdown** - This alert is generated when a service, operation or function is enabled.

## Reports

EventTracker provides an exclusive reporting tool to generate requirement specific reports. Below are sample reports created by EventTracker for specific eDirectory logs.

eDirectory -Account modification report								
LogTime	System Address	Organisation	Organisational Unit	Domain Name	User Name	Account Name	Attribute name	Attribute Value
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Jacob	Language	ENGLISH
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Michael	NGW: Visibility	2
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Angel	NGW: Object ID	shaaz
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	William	NGW: Post Office	CN=SLCPO,OU=Japan,O=ETTracker
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Landon	NGW: File ID	bj5
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	James	CONTOSO	admin	Alexander	NGW: GroupWise ID	SLCDDOM.SLCPO.shaaz{106}DA20DC81-071E-0000-A7FA-2BC603B16349
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Gabriel	nspmPasswordKey	3456106496
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Joshua	Internet EMail Address	shaaz.SLCPO.SLCDDOM
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Christopher	modifiersName	CN=admin,O=ETTracker
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Elijah	creatorsName	CN=admin,O=ETTracker
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Elijah	uniqueID	shaaz
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Daniel	GUID	4137111284278219332
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Benjamin	Obituary	72057598332895231
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	James	Revision	12
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Joshua	Surname	shas
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Gabriel	Public Key	72057594105036800
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	James	CN	shaaz
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Gabriel	EMail Address	BwAAACyAAABzAGgAYQBhAHpALgBTAewAQwBQAE8ALgBTAewAQwBEAE8ATQAAAA==
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Joshua	Object Class	User
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Christopher	Object Class	Organizational Person
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Elijah	Object Class	Person
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Elijah	Object Class	ndsLoginProperties
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Daniel	Object Class	Top
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Benjamin	Private Key	4765231815456868954
11/05/2014 01:06:57 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	James	ACL	Entry ID: .T=CONTOSO., Attribute ID: , Privileges: Attribute Read CN=linuxedir,O=ETTracker
11/05/2014 02:30:07 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Joshua	modifiersName	CN=linuxedir,O=ETTracker
11/05/2014 02:30:07 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Gabriel	pwdFailureTime	11/04/14 20:34:59
11/05/2014 02:30:07 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	James	modifiersName	CN=linuxedir,O=ETTracker
11/05/2014 02:30:31 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Gabriel	modifiersName	CN=linuxedir,O=ETTracker
11/05/2014 02:30:31 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Joshua	Login Time	11/04/14 19:06:16
11/05/2014 02:30:31 AM	192.168.1.41	ETTracker	ETUSA	CONTOSO	admin	Christopher	Last Login Time	10/31/14 04:25:59

Figure 9

eDirectory-Authentication failure report					
LogTime	System Address	Account Name	Domain Name	Organisational Unit	Organisation
11/05/2014 02:30:07 AM	192.168.1.41	Anthony	CONTOSO	PRISMUSA	root
11/05/2014 02:30:31 AM	192.168.1.41	Jackson	CONTOSO	LONDON	root
11/05/2014 02:30:31 AM	192.168.1.41	admin	CONTOSO	JAPAN	root
11/05/2014 06:19:35 AM	192.168.1.41	Michael	CONTOSO	ETUSA	root

Figure 10