

Integrate Azure Stack

EventTracker v8.x and above

Abstract

EventTracker allows you to effectively manage your systems and provides operational efficiencies – reducing IT costs and freeing resources for other duties that increase the business value of your organization. EventTracker’s built-in knowledge base enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, and Azure Stack.

Audience

EventTracker users, who wish to monitor Azure Stack.

Table of Contents

Abstract	1
Scope	1
Audience	1
Introduction.....	3
Enable Syslog Forwarding on Azure Stack.....	3
EventTracker Knowledge Pack	3
Flex Reports	3
Alerts	5
Import Azure Stack knowledge pack into EventTracker	6
Alerts	7
Token Templates	8
Flex Reports	9
Verify Azure Stack knowledge pack in EventTracker	11
Alerts	11
Token Templates	11
Flex Reports	12

Introduction

Azure Stack is a hybrid cloud computing software solution developed by Microsoft based on the company's Azure cloud platform. Azure Stack is designed to help organizations deliver Azure services from their own data center.

Azure Stack combines infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) services in a software stack that spans on-premises datacenter environments as well as Microsoft's Azure cloud. Azure and Azure Stack share a standardized architecture, including the same portal, a unified application model and common DevOps tools.

Enable Syslog Forwarding on Azure Stack

To enable syslog forwarding on Azure stack, execute the following command in Azure Stack PowerShell.

```
Set-SyslogServer -ServerName <Eventtracker_IP> -ServerPort <Syslog_Port> -NoEncryption
```

Example:

```
Set-SyslogServer -ServerName 192.168.1.52 -ServerPort 512 -NoEncryption
```

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 Azure Stack.

Flex Reports

- **Azure Stack - User Logon Failed:** This report provides information about the logon failures by users.

LogTime	Computer	System Name	Workstation Name	User Name	Account Domain	Source IP Address	Source Port Number	Reason For Failure	Logon ID
10/29/2018 04:59:56 PM	R1S5-VM30(AZURE01)	AzS-Sql01.azurestack.local	WIN-R9H529RIO4Y	AzS-Was-RmSAS	AZURESTACK	10.42.42.201	53176	Unknown user name or bad password.	0x119C822
10/29/2018 05:00:06 PM	R1S5-VM30(AZURE01)	AzS-Sql01.azurestack.local	WIN-R9H529RIO4Y	John	AZURESTACK	10.42.42.201	53176	Unknown user name or bad password.	0x119C823

Figure 1

- **Azure Stack - User Logon and Logoff:** This report provides information about the user logon and logoff.

LogTime	Computer	System Name	User Name	Account Domain	Workstation Name	Source Network Address	Action	Logon Type	Logon ID
10/31/2018 04:02:34 PM	R1S5-VM30\AZUREEE	AzS-ERCS01.azurestack.local	0x4D39317	AZURESTACK.LOCAL	-	-	Logon	3	0x4D39317

Figure 2

- **Azure Stack - User Account Locked Out:** This report provides information about user account locked out.

LogTime	Computer	System Name	User Name	Account Domain	Caller Computer Name	Logon ID
10/31/2018 12:34:53 PM	R1S5-VM30\AZURE001	AzS-Sql01.azurestack.local	John	AZURESTACK	WIN-R9H529RIO4Y	0x119C822
10/31/2018 12:36:12 PM	R1S5-VM30\AZURE001	AzS-Sql01.azurestack.local	Jim	AZURESTACK	WIN-R9H529RIO4Y	0x119C823

Figure 3

- **Azure Stack - Audit Logs Cleared:** This report provides information about the audit logs cleared.

LogTime	Computer	System Name	User Name	Domain Name	Message	Logon ID
10/31/2018 12:34:53 PM	R1S5-VM30\AZURE001	AzS-Sql01.azurestack.local	Administrator	AZURESTACK	The audit log was cleared.	0x119C822
10/31/2018 12:36:12 PM	R1S5-VM30\AZURE001	AzS-Sql01.azurestack.local	ETAdmin	AZURESTACK	The audit log was cleared.	0x119C823

Figure 4

- **Azure Stack - Administration Activities:** This report provides information about the administrative activities.

LogTime	Computer	System Name	Action	Object Changes	Permissions Change	Process Information	Subject Information
10/31/2018 12:46:49 PM	R1SS-VM30\AZURE001	AzS-ADFS01.azurestack.local	Permissions on an object were changed.	Object Server:Security\nObject Type:File\nObject Name: C:\Users\Administrator\restfolder\New Text Document.txt\nHandle ID:0x3E7	Original Security Descriptor:0x8c0\nProcess Name: C:\Windows\explorer.exe\nMasEventID=4670	Process ID:D:PAI(A;;FA;;;LA)(A;;FA;;;SY) (A;;FA;;;BA)\nNew Security Descriptor:D:PARAI(A;;FA;;;SY)(A;;FA;;;BA)	Security ID:S-1-5-18\nAccount Name:AZS-ADFS01\$\nAccount Name: AZURESTACK\nLogon ID:0x3E7

Figure 5

- **Azure Stack - Registry Changed:** This report provides information about the registry changes.

LogTime	Computer	System Name	User Name	Account Domain	Operation Type	Object Name	Object Value Name	Old Value Type	Old Value	New Value Type	New Value	Process Name
10/31/2018 01:06:37 PM	R1SS-VM30\AZURE001	AzS-ADFS01.azurestack.local	AZS-ADFS01\$	AZURESTACK	New registry value created	\REGISTRY\MACHINE\SOFTWARE\MTG	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	-	-	-	-	C:\Windows\egedit.exe

Figure 6

Alerts

- **Azure stack - *Security: User account unlocked** - This alert will be generated when a user account is unlocked.
- **Azure stack - Active Directory: Group policy changed** - This alert will be generated when a group policy is changed.
- **Azure stack - Admin Interactive/Remote Interactive login failure** - This alert will be generated when admin Interactive/Remote Interactive login failure occurs.
- **Azure stack - Admin Interactive/Remote Interactive login success** - This alert will be generated when admin Interactive/Remote Interactive login is successful.
- **Azure stack - Administrative logon failure** - This alert will be generated when an administrative logon failure occurs.
- **Azure stack - Administrative logon success** - This alert will be generated when administrative logon is successful.
- **Azure stack - Audit event records discarded** - This alert will be generated when audit event records are discarded.
- **Azure stack - Audit log cleared** - This alert will be generated when audit logs are cleared.
- **Azure stack - Directory permission change**- This alert will be generated when directory permissions are changed.
- **Azure stack - Domain policy changes** - This alert will be generated when domain policies are changed.
- **Azure stack - Excessive access failures by a user** - This alert will be generated when failure for excessive access occurs by a user.
- **Azure stack - Excessive access failures in your organization** - This alert will be generated when failure for excessive access occurs in your organization.
- **Azure stack - Excessive access failures on a specific computer** - This alert will be generated when failure for excessive access occurs on a specific computer.

- **Azure stack - Excessive file deletes on a computer** - This alert will be generated when excessive file is deleted on a computer.
- **Azure stack - Excessive logon attempts from a IP address** - This alert will be generated when excessive login attempts from a IP address.
- **Azure stack - Excessive logon failures due to bad password/username** - This alert will be generated when an excessive logon failure occurs due to bad password.
- **Azure stack - Excessive logon failures in your enterprise** - This alert will be generated when excessive logon failures occurs in your enterprise.
- **Azure stack - Excessive logon failures in your enterprise due to user account locked** - This alert will be generated when excessive logon failures occurs in your enterprise due to user account locked.
- **Azure stack - Excessive user lockout in your enterprise** - This alert will be generated when excessive user lockout occurs in your enterprise.
- **Azure stack - File replication service staging area full** - This alert will be generated when the file replication service staging area is full.
- **Azure stack - Group policy processing error**- This alert will be generated when an error occurs while processing a group policy.
- **Azure stack - Possible malware lateral movement** - This alert will be generated when a possible malware lateral movement is suspected.
- **Azure stack - Security: User account locked out** - This alert will be generated when a user account is locked out.
- **Azure stack - Security: Users added to Domain Admin or local Admin group** - This alert will be generated when user is added to domain admin or local admin group.
- **Azure stack - Security: Users password set to never expire** - This alert will be generated when user password is set to never expire.
- **Azure stack - System shutdown** - This alert will be generated when the system is shutdown.

Import Azure Stack knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Alerts
 - Token Templates
 - Flex Reports
1. Launch **EventTracker Control Panel**.
 2. Double click **Export Import Utility**.

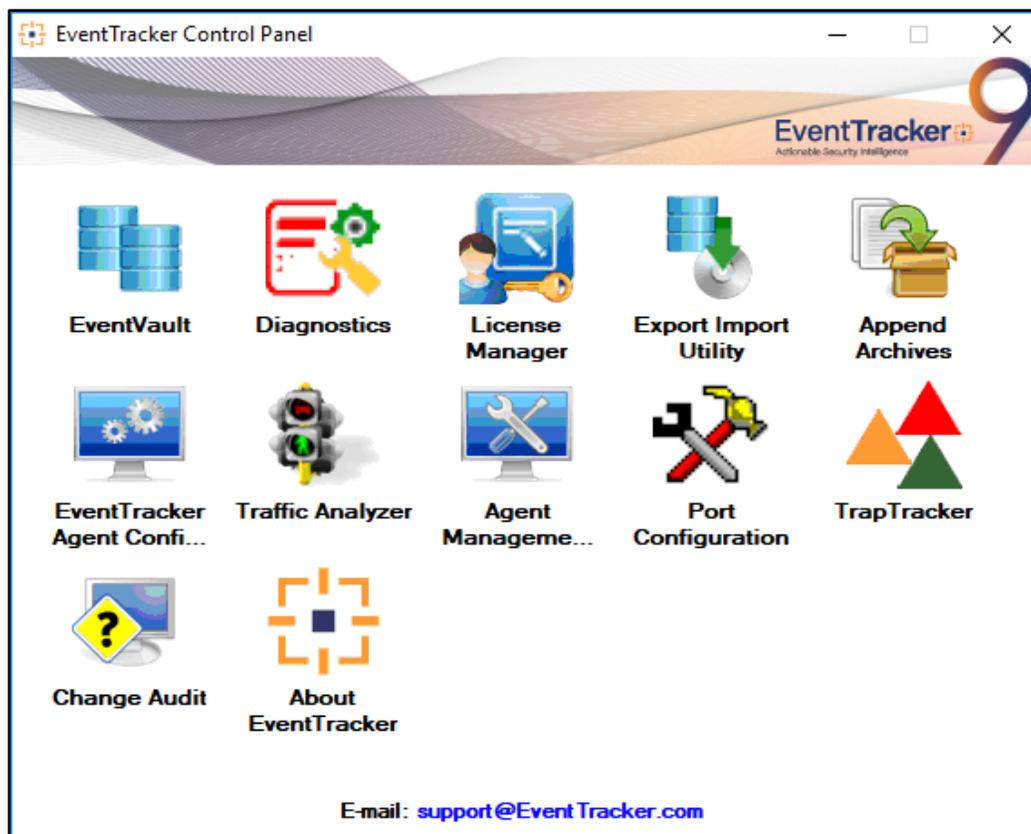


Figure 7

3. Click the **Import** tab.

Alerts

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

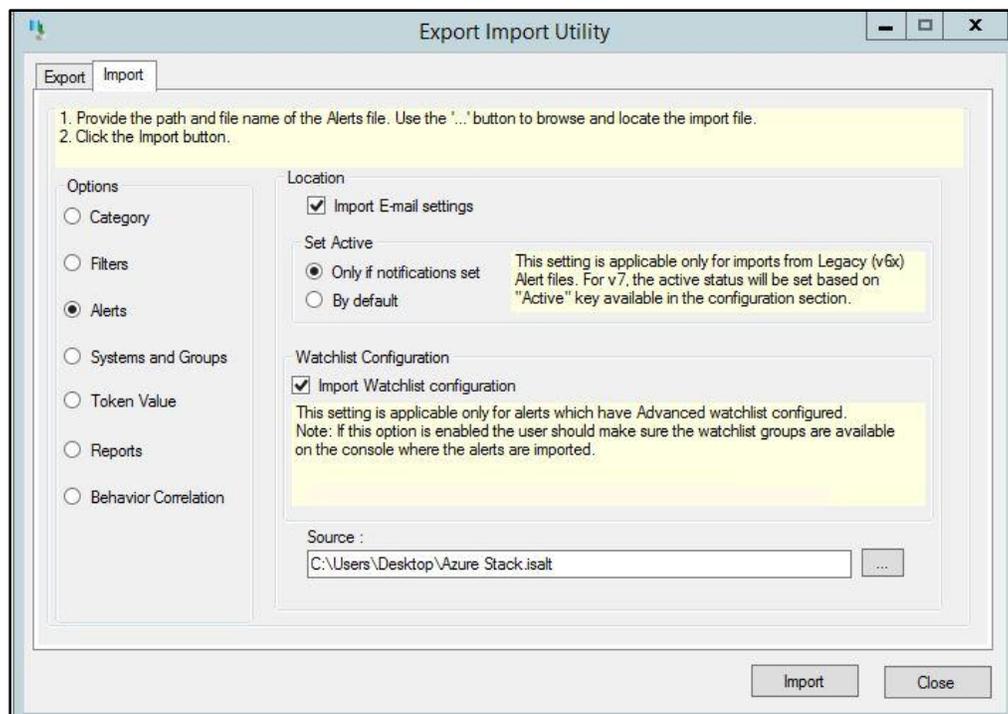


Figure 8

2. Locate **Alert_Azure Stack.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.



Figure 9

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_Azure Stack.ettd**.

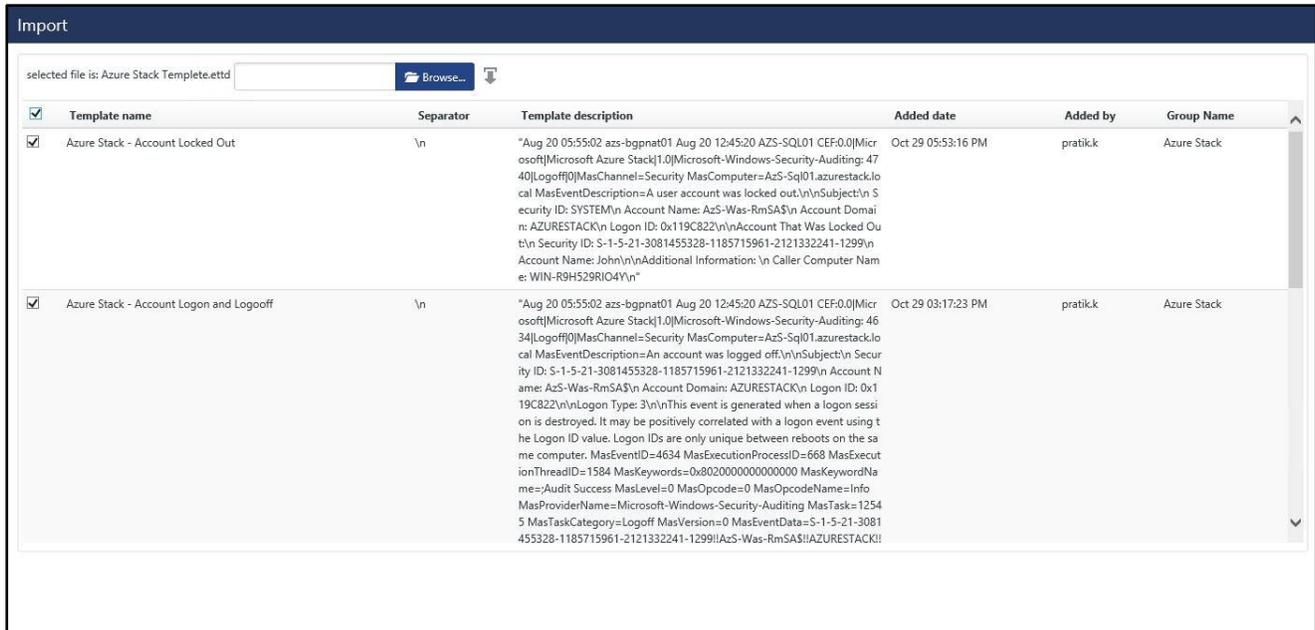


Figure 10

- Now select all the check box and then click on  Import option.

Flex Reports

On EventTracker Control Panel,

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

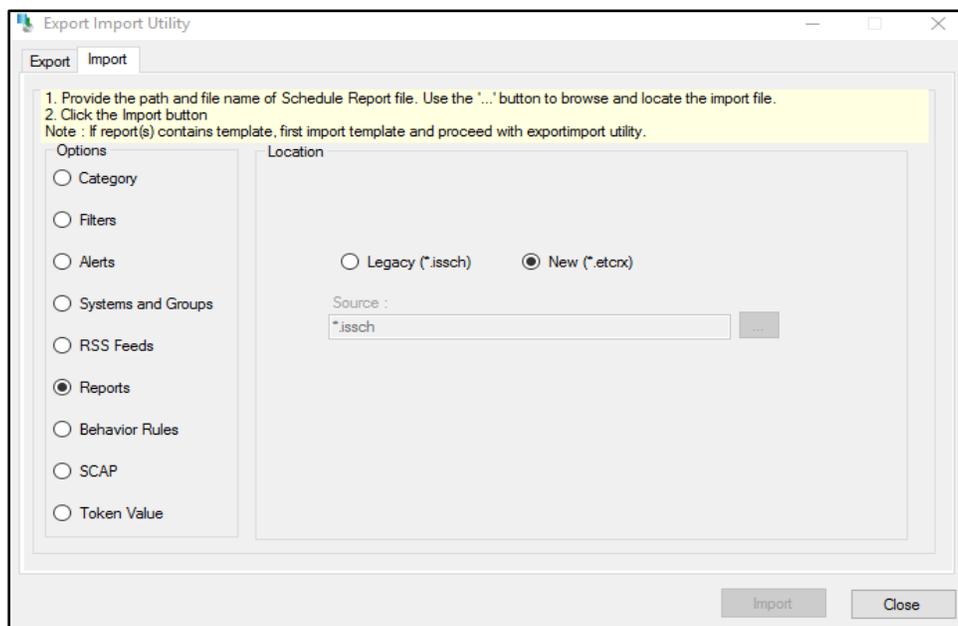


Figure 11

2. Locate the **Reports_Azure Stack.etcrx** file and select all the check box.

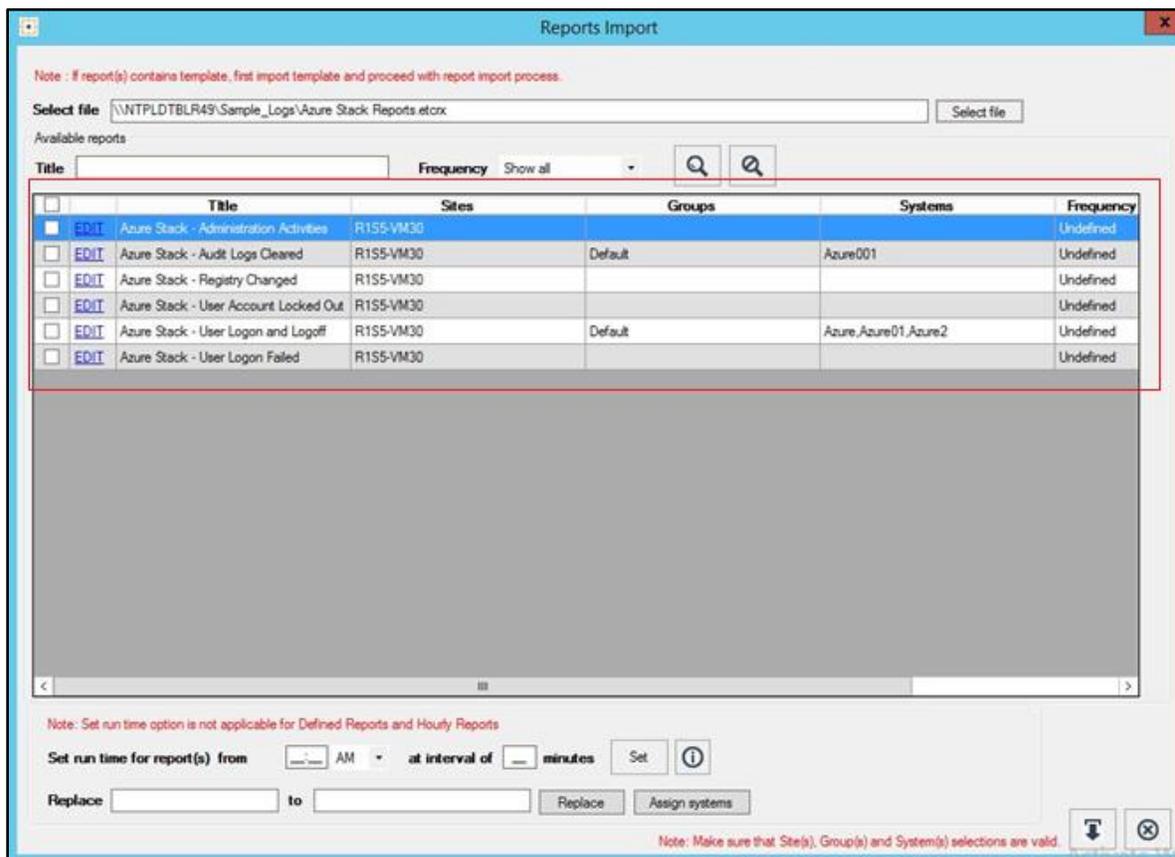


Figure 12

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

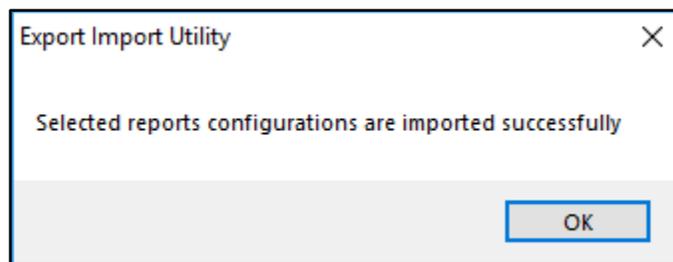


Figure 13

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

Verify Azure Stack knowledge pack in EventTracker

Alerts

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

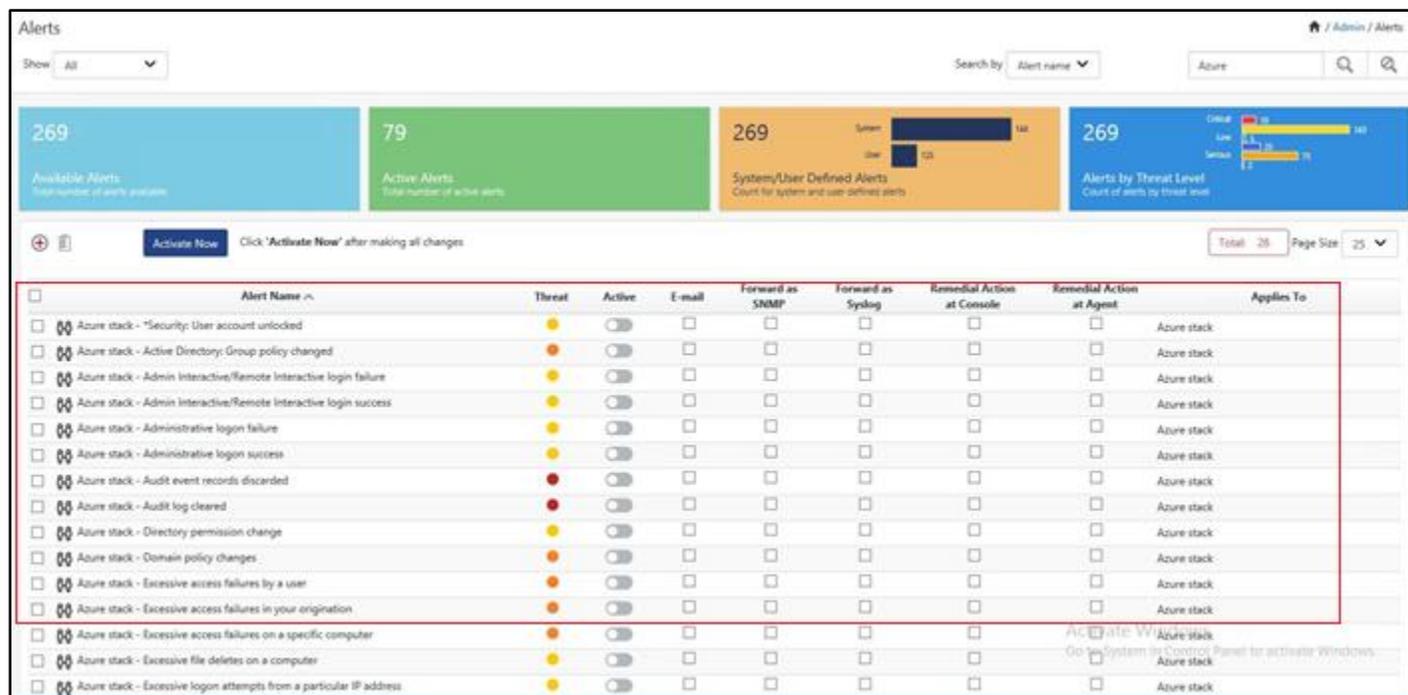


Figure 14

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 **Azure Stack group** folder to view the imported Token Values.

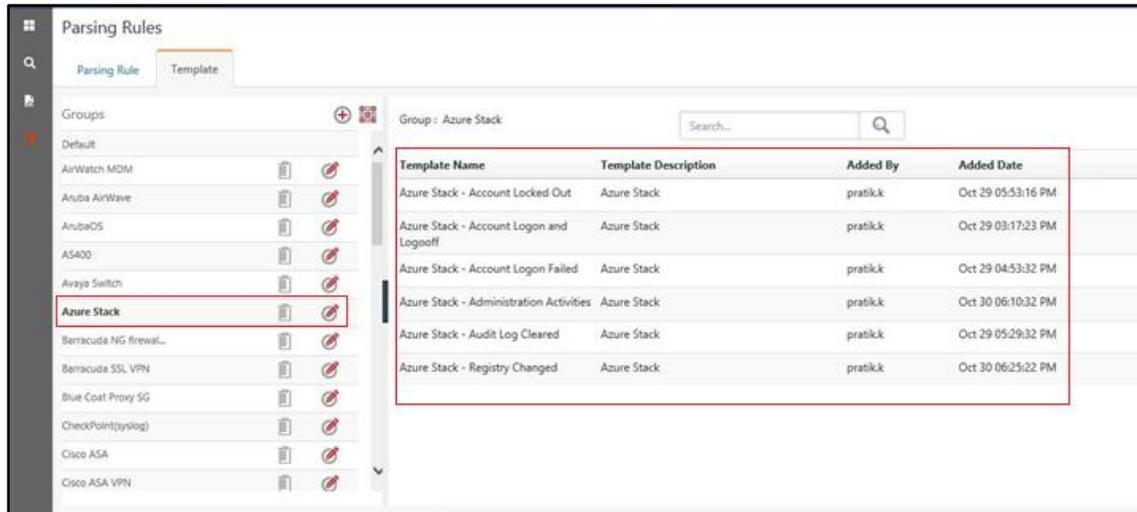


Figure 15

Flex Reports

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



Figure 16

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

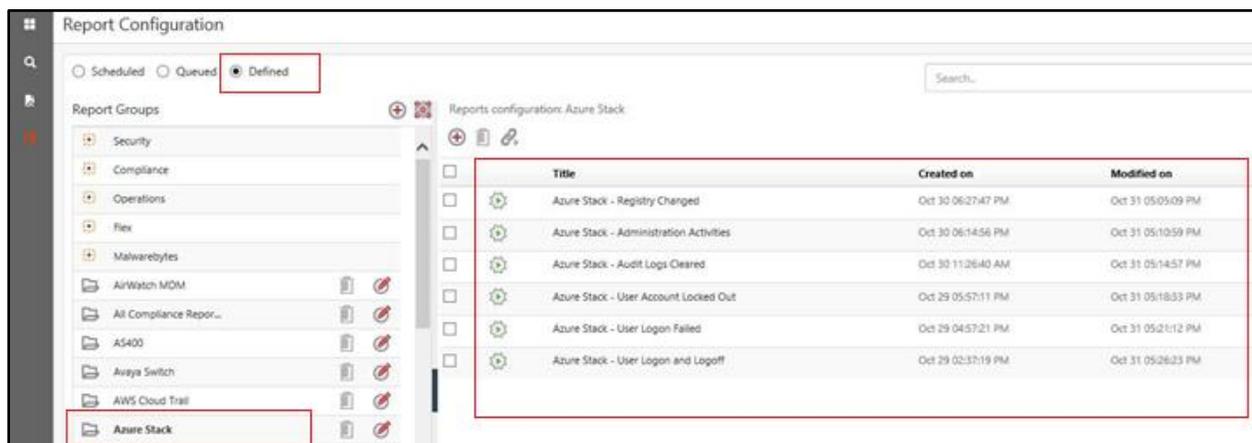


Figure 17