

Cerberus SFTP Server

EventTracker v9.x or 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 pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

With EventTracker, you can monitor your servers running on SFTP Server from a single view. EventTracker checks the status and availability of SFTP Servers, critical server processes, and it centrally consolidates all the event logs. Through consolidated logging, you can monitor the performance, availability, and security of your servers running on SFTP Server, alerting you to events that have a direct impact on server availability while filtering out events that require no action. Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a catastrophic failure occurs. EventTracker also includes reports that allow you to summarize server availability.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, Cerberus SFTP 10.0.9.

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
Overview.....	3
Cerberus SFTP Server Integration	3
Create New Rule.....	3
Enable Syslog Logging.....	12
Cerberus SFTP Server Knowledge Pack:	15
Alerts	15
Flex Reports	15
Dashboards.....	19
Import Cerberus SFTP Server knowledge pack into EventTracker.....	24
Alerts	24
Flex Reports	25
Knowledge Objects.....	27
Dashboards.....	27
Verify Cerberus SFTP Server knowledge pack in EventTracker.....	30
Knowledge Object	30
Flex Reports	30
Alerts	31

Overview

Cerberus FTP Server is a Windows-based FTP server with support for encrypted FTP sessions via FTPS and SFTP as well as web client support via HTTP and HTTPS. The server exposes files using a virtual file system and supports user authentication via built-in users and groups, Active Directory, LDAP and public key authentication.

EventTracker's built-in knowledge base enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems. With EventTracker, you can monitor all of your servers running Cerberus SFTP Server from a single view.

EventTracker helps to monitor events from **Cerberus SFTP Server**. EventTracker's **Flex Reports, Alerts, and Dashboards** will help you to analyze all the security related events. Through alerts, knowledge base solutions, and reports, EventTracker helps you correct problems long before a catastrophic failure occurs.

Prerequisites

- **EventTracker v9.x** or above should be installed.
- **Cerberus Enterprise 10.0.8.0 Administration Console.**
- **Windows PowerShell.**

Cerberus SFTP Server Integration

Create New Rule

A rule is defined by the type of event that triggers it. Each rule has a single event type associated with it. When that event occurs, any rules associated with that event type are triggered to EventTracker.

1. For creating a New Rule, we must create an **Event Target**.
2. Log-in on **Cerberus Enterprise 10.0.8.0 Administration Console**.
3. Go to **Events** or **Event Manager** and click on **Event Targets**.

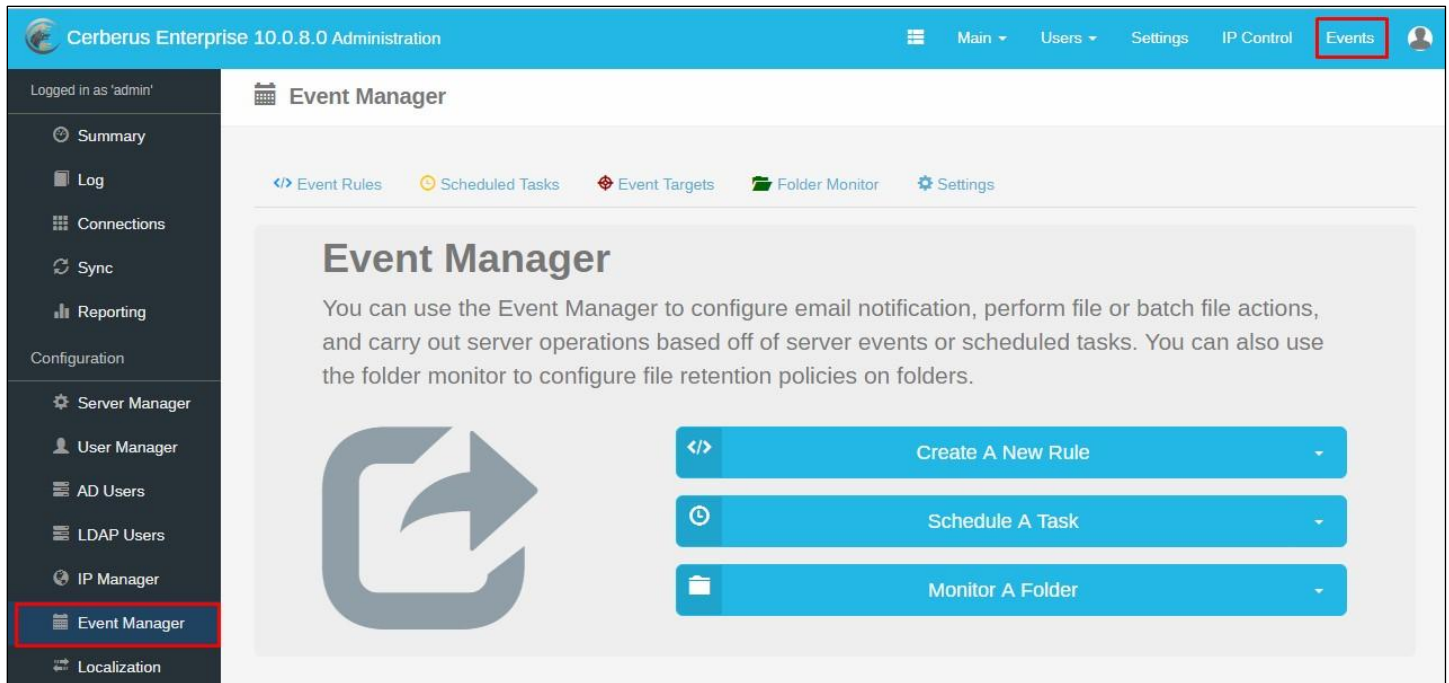


Figure 1

4. Click on Event Targets and then go to **External Process Configuration**. Click on  and then select **External path: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe**

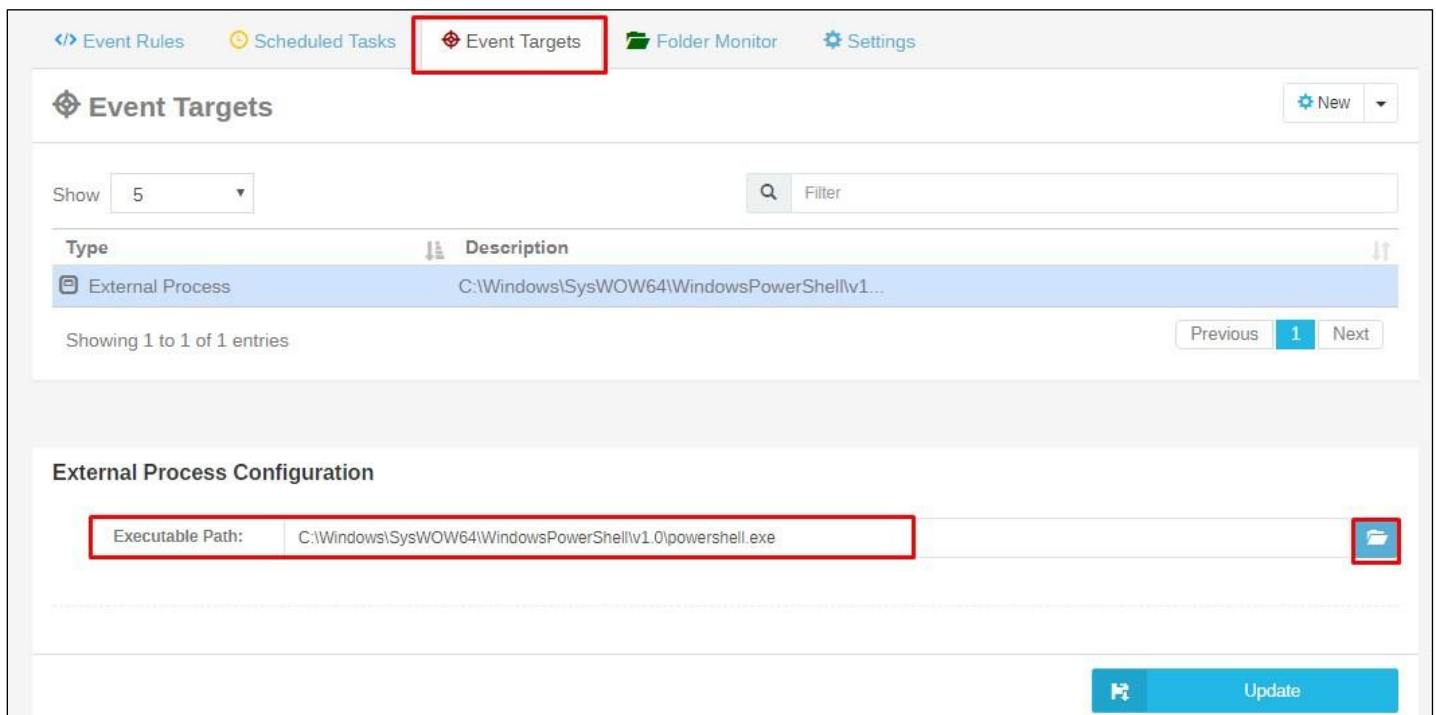


Figure 2

5. Click on **Update** and it displays a success message.

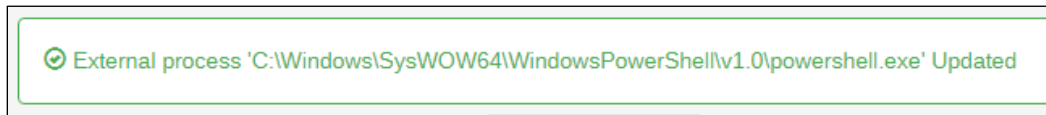


Figure 3

6. Go to **Events** or **Event Manager** and click on **Event Rule** and select **New** to create a new Rule.

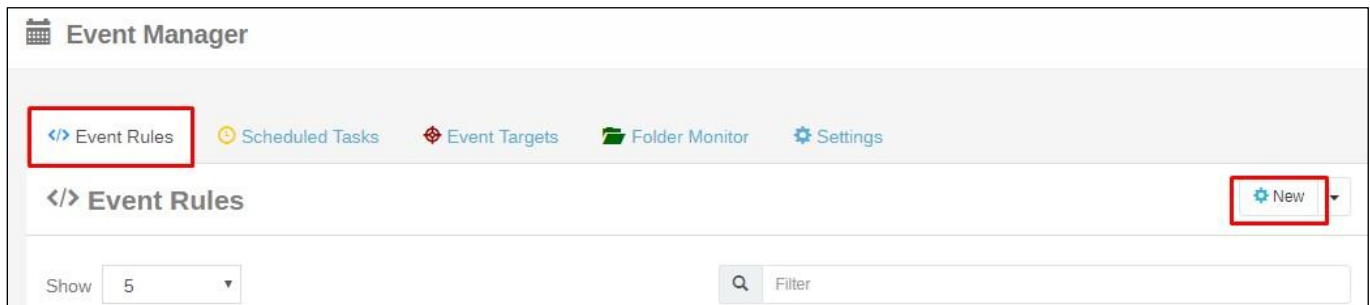


Figure 4

7. Select the **Type of event rule** you would like to add.

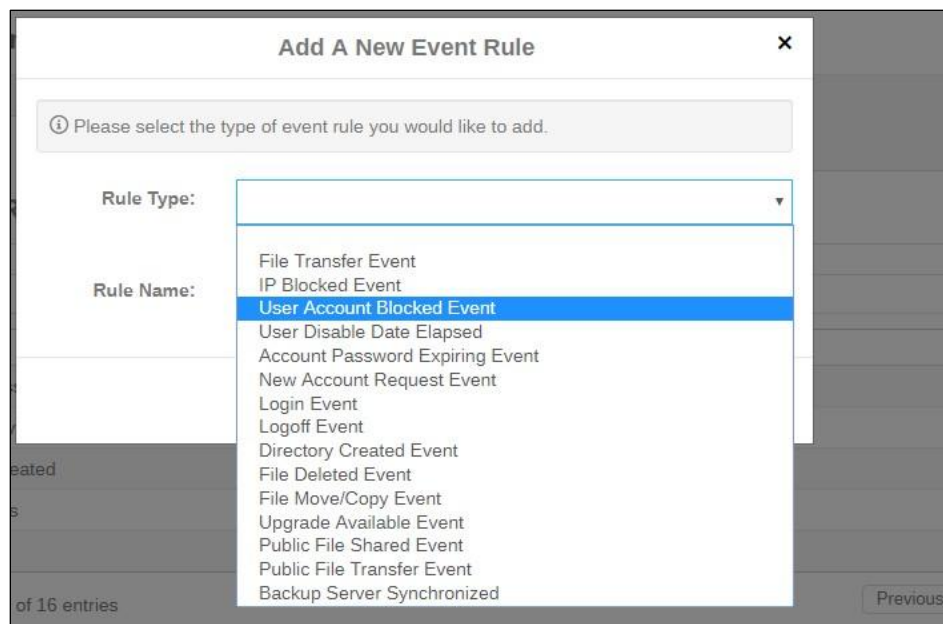
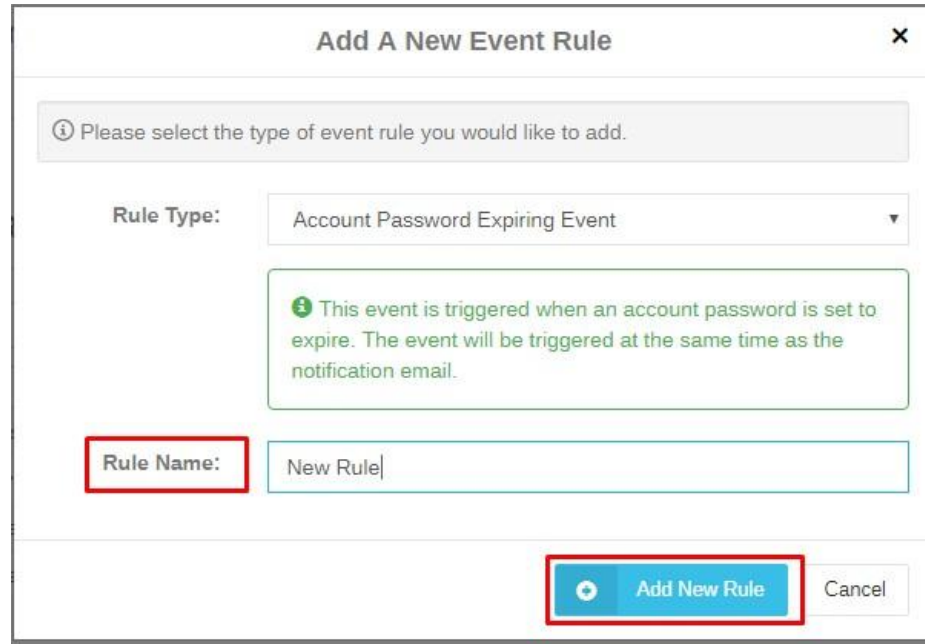


Figure 5

8. Provide the Rule Name and **Add the Rule**.



Add A New Event Rule [X]

Please select the type of event rule you would like to add.

Rule Type: Account Password Expiring Event

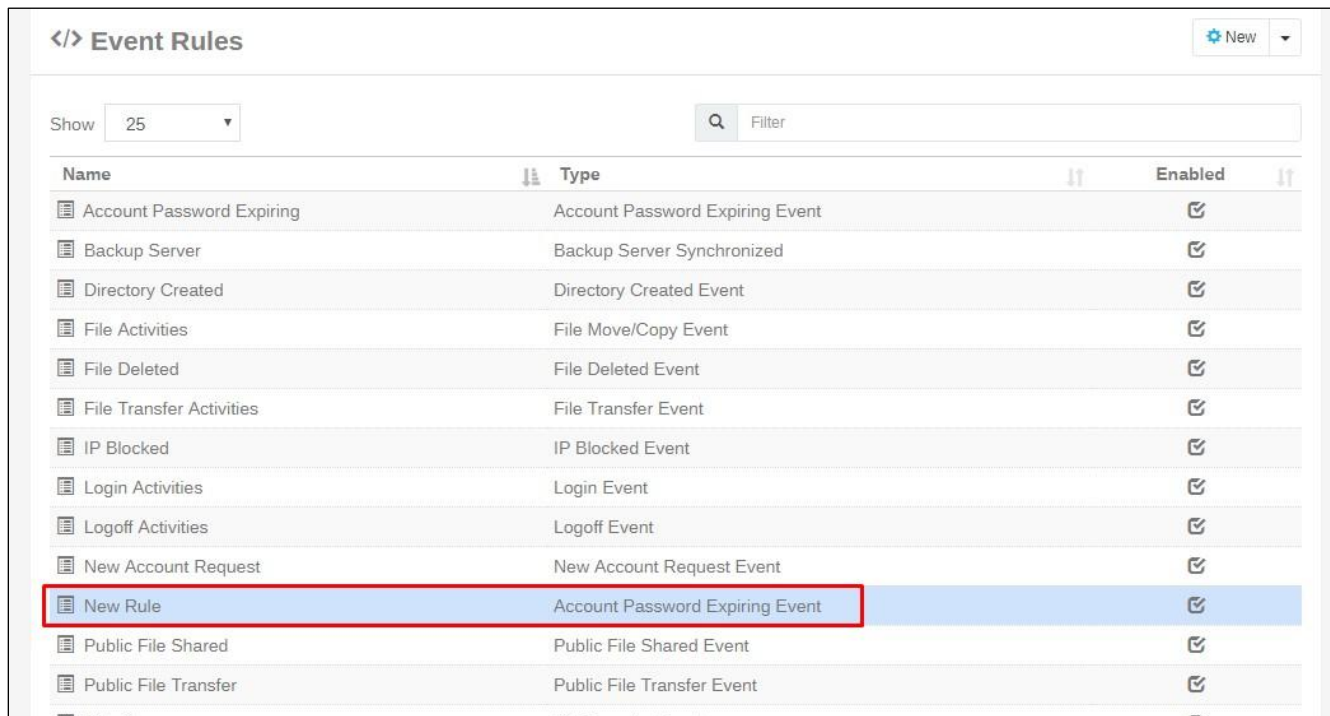
This event is triggered when an account password is set to expire. The event will be triggered at the same time as the notification email.

Rule Name: New Rule

[+ Add New Rule] [Cancel]

Figure 6

9. Now the Rule will be added in the **Events Rules** list.



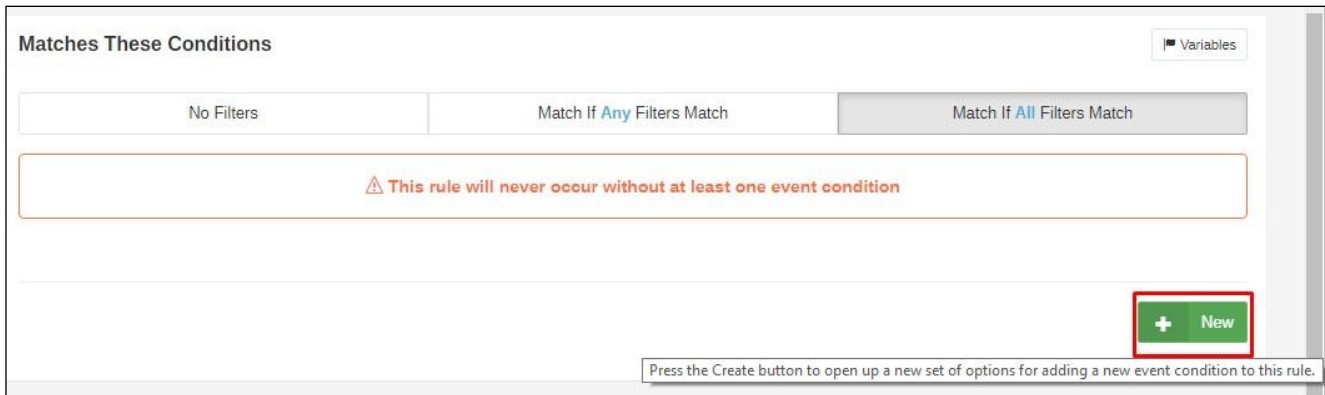
</> Event Rules [New]

Show 25 [Filter]

Name	Type	Enabled
Account Password Expiring	Account Password Expiring Event	<input checked="" type="checkbox"/>
Backup Server	Backup Server Synchronized	<input checked="" type="checkbox"/>
Directory Created	Directory Created Event	<input checked="" type="checkbox"/>
File Activities	File Move/Copy Event	<input checked="" type="checkbox"/>
File Deleted	File Deleted Event	<input checked="" type="checkbox"/>
File Transfer Activities	File Transfer Event	<input checked="" type="checkbox"/>
IP Blocked	IP Blocked Event	<input checked="" type="checkbox"/>
Login Activities	Login Event	<input checked="" type="checkbox"/>
Logoff Activities	Logoff Event	<input checked="" type="checkbox"/>
New Account Request	New Account Request Event	<input checked="" type="checkbox"/>
New Rule	Account Password Expiring Event	<input checked="" type="checkbox"/>
Public File Shared	Public File Shared Event	<input checked="" type="checkbox"/>
Public File Transfer	Public File Transfer Event	<input checked="" type="checkbox"/>

Figure 7

10. Now select the created Rule and for matching the condition, click on **New**  option.



Matches These Conditions

No Filters Match If Any Filters Match Match If All Filters Match

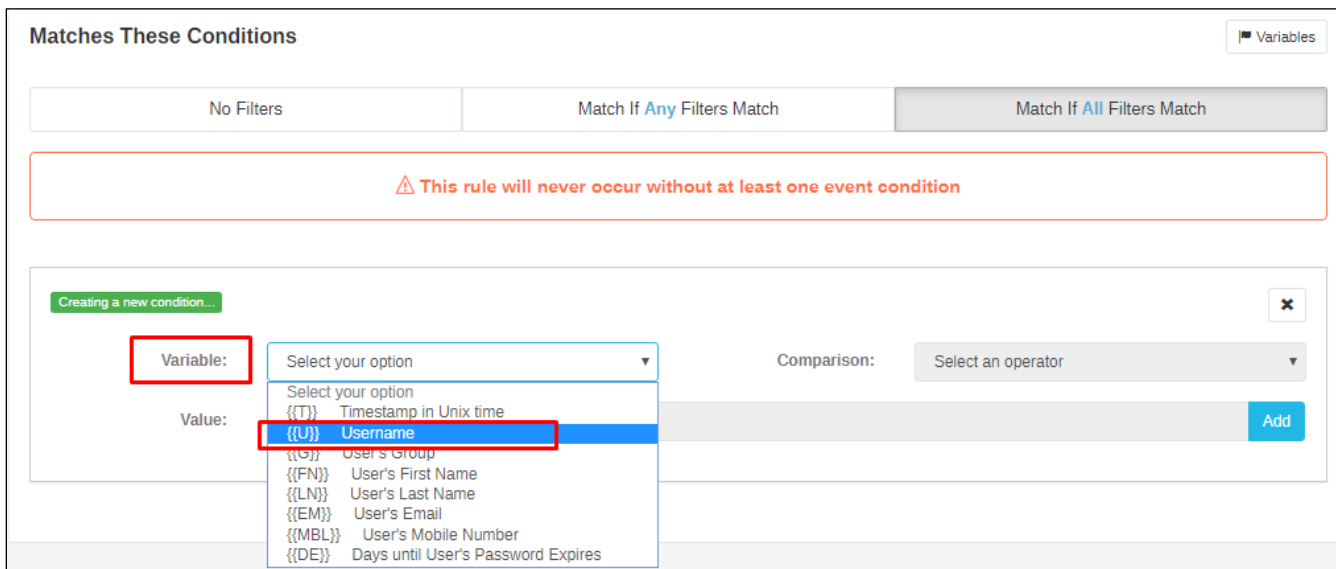
⚠ This rule will never occur without at least one event condition

+ New

Press the Create button to open up a new set of options for adding a new event condition to this rule.

Figure 8

11. For creating a new condition, select a **variable** from available option.



Matches These Conditions

No Filters Match If Any Filters Match Match If All Filters Match

⚠ This rule will never occur without at least one event condition

Creating a new condition...

Variable: Select your option

Value: Select your option

Comparison: Select an operator

Username

User's Group

User's First Name

User's Last Name

User's Email

User's Mobile Number

Days until User's Password Expires

Add

Figure 9

12. After selecting the Variable, click on **Comparison** and select **Regular Expression Match**.

Matches These Conditions Variables

No Filters | Match If **Any** Filters Match | Match If **All** Filters Match

⚠ This rule will never occur without at least one event condition

Creating a new condition...

Variable: Comparison:

Value:

Regular Expression Match

Perform These Actions

Figure 10

13. In value section, add a Matching Regular expression and click on **Add**.

Matches These Conditions Variables

No Filters | Match If **Any** Filters Match | Match If **All** Filters Match

⚠ This rule will never occur without at least one event condition

Creating a new condition...

Variable: Comparison:

Value:

Add

Add condition

Figure 11

14. For matching the condition, click on **Variables** and find the **Variable name**, **Type** and **Description**.

Matches These Conditions Variables

Variable Name	Type	Description
T	Date and Time	Timestamp in Unix time
U	String	Username
G	String	User's Group
FN	String	User's First Name
LN	String	User's Last Name
EM	String	User's Email
MBL	String	User's Mobile Number
DE	Integer	Days until User's Password Expires

IF DE matches *

-

Figure 12

15. Now click on **New** to create **Perform These Actions**.

Perform These Actions

+ New

Figure 13

16. Select an **Action** type.

Perform These Actions

Creating a new action...

Action: Perform this action

- Perform this action
- Email Event Notification
- Launch an Executable
- Launch File Operation
- Launch Server Operation
- Send HTTP POST

Using: Select additional options ☐ Stop on Failure

Figure 14

17. Select **Using path** (Event Target).

Perform These Actions

Creating a new action...

Action: Launch an Executable

You may need to add an SMTP server or executable target on the [Event Targets](#) page first

Using: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Command Line: Command Line - use double brackets to delimit variables e.g.

Wait timeout: 60

☐ Stop on Failure

Add

Figure 15

18. In Command Line enter **Script File path, Commands** and click on **Add**.

Perform These Actions

Creating a new action...

Action: Launch an Executable

You may need to add an SMTP server or executable target on the [Event Targets](#) page first

Using: C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Command Line: executionpolicy unrestricted -file "Location of LogTransfer.ps1" "Type: Account Password Expiring, Timestamp: {{T}}, Username: {{U}}, Use

Wait timeout: 60

☐ Stop on Failure

Add

Figure 16

NOTE: For Executable script File, please contact the Support Team.

19. Now we can see the Rule description in **Perform These Actions** section.



Figure 17

For Event Rule Type and Command Line, please Refer the Following Table-

Event Rule Type	Command Line
Account Password Expiring Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: Account Password Expiring, Timestamp: {{T}}, Username: {{U}}, UserGroup: {{G}}, User's FirstName: {{FN}}, User's LastName: {{LN}}, User's Email: {{EM}}, User's MobileNumber: {{MBL}}, User's Password Expires: {{DE}}"
Backup Server Synchronized	-executionpolicy unrestricted -file "Location of LogTransfer.ps1" "Type: Backup Server, Timestamp: {{T}}, Backup ServerHost: {{H}}, Synchronization Message: {{MSG}}, Successful: {{S}}"
Directory Created Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: Directory Created, Timestamp: {{T}}, Username: {{U}}, User's Group: {{G}}, Protocol Type: {{P}}, User's Connection ID: {{ID}}, User's IP Address: {{IP}}, User's FirstName: {{FN}}, User's LastName: {{LN}}, User's Email: {{EM}}, User's MobileNumber: {{MBL}}, DirectoryName: {{LFN}}, Local DirectoryPath: {{LP}}, Remote DirectoryPath: {{RP}}, Successful Operation: {{S}}"
File Deleted Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: File Deleted, Timestamp: {{T}}, Username: {{U}}, User's Group: {{G}}, Protocol Type: {{P}}, User's ConnectionID: {{ID}}, User's IP Address: {{IP}}, User's FirstName: {{FN}}, User's LastName: {{LN}}, User's Email: {{EM}}, User's MobileNumber: {{MBL}}, File Name: {{LFN}}, Local FilePath: {{LP}}, Remote FilePath: {{RP}}, Successful Operation: {{S}}, Directory: {{DIR}}"
File Move/Copy Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: File Activities, Timestamp: {{T}}, Username: {{U}}, User's Group: {{G}}, Protocol Type: {{P}}, User's ConnectionID: {{ID}}, User's IP Address: {{IP}}, User's FirstName: {{FN}}, User's LastName: {{LN}}, User's Email: {{EM}}, User's MobileNumber: {{MBL}}, File Name From: {{LFNF}}, File Name To: {{LFNT}}, Local FilePath From: {{LPF}}, Remote FilePath From: {{RPF}}, Local FilePath To: {{LPT}}, Remote FilePath To: {{RPT}}, Move Operation: {{M}}, Copy Operation: {{C}}, Successful Operation: {{S}}"
File Transfer Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: File Transfer, Timestamp: {{T}}, Username: {{U}}, User's Group: {{G}}, Protocol Type: {{P}}, User's ConnectionID: {{ID}}, User's IP Address: {{IP}}, User's FirstName: {{FN}}, User's LastName: {{LN}}, User's Email: {{EM}}, User's MobileNumber: {{MBL}}, File Name: {{LFN}}, Local FilePath: {{LP}}, Remote FilePath: {{RP}}, Download: {{D}}, Successful Transfer: {{S}}, File Size: {{SZ}}, Bytes Transferred: {{TRX}}, Byte Range Request: {{R}}, Byte Range Transferred: {{RNG}}"
IP Blocked Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: IP Blocked, Timestamp: {{T}}, Blocked IP: {{IP}}"

Login Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: Login Activities, Timestamp: {{T}}, Username: {{U}}, User's Group: {{G}}, Protocol Type: {{P}}, User's ConnectionID: {{ID}}, User's IP Address: {{IP}}, User's FirstName: {{FN}}, User's LastName: {{LN}}, User's Email: {{EM}}, User's MobileNumber: {{MBL}}"
Logoff Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: Logoff Activities, Timestamp: {{T}}, Username: {{U}}, User's Group: {{G}}, Protocol Type: {{P}}, User's ConnectionID: {{ID}}, User's IP Address: {{IP}}, User's FirstName: {{FN}}, User's LastName: {{LN}}, User's Email: {{EM}}, User's MobileNumber: {{MBL}}"
New Account Request Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: New Account Request, Timestamp: {{T}}, Requested Username: {{U}}, First Name: {{F}}, Last Name: {{L}}, Email Address: {{E}}, Telephone Number: {{TEL}}, Justification: {{J}}"
Public File Shared Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: Public File Shared, Timestamp: {{T}}, Username: {{U}}, File Name: {{LFN}}, Local FilePath: {{LFP}}, Remote FilePath {{REP}}, Shared Until: {{SU}}, Recipient Email List: {{RL}}, Public File ID: {{PID}}, Public File URL: {{URL}}"
Public File Transfer Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: Public File Transfer, Timestamp: {{T}}, IP Address: {{IP}}, Protocol Type: {{P}}, User's Connection ID: {{ID}}, File Name: {{LFN}}, Local FilePath: {{LFP}}, Remote FilePath {{REP}}, Download: {{D}}, Successful Transfer: {{S}}, File Size: {{SZ}}, Public File ID: {{PID}}"
Upgrade Available Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: Upgrade Available, Timestamp: {{T}}, Version: {{V}}"
User Disable Date Elapsed	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: User Account Blocked, Timestamp: {{T}}, Blocked Username: {{U}}"
User Account Blocked Event	-executionpolicy unrestricted -file " Location of LogTransfer.ps1 " "Type: User Disable, Timestamp: {{T}}, Disabled Username: {{U}}, User's Group: {{G}}, User's FirstName: {{FN}}, User's LastName: {{LN}}, User's Email: {{EM}}"

Enable Syslog Logging

1. Log-in to **Cerberus SFTP Enterprise** console.
2. Click on **Setting** or **Server Manger**.

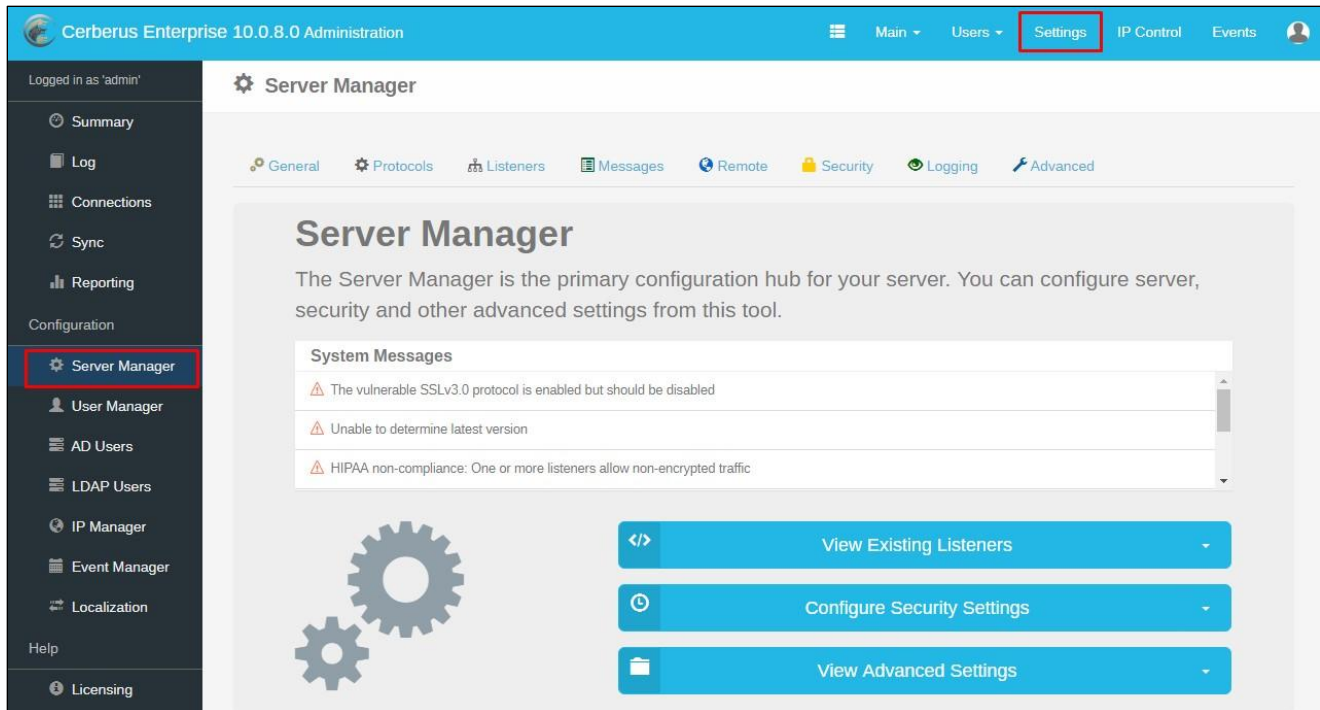


Figure 18

3. Click on **Logging** and in **Syslog** section **Enable Syslog Logging**.

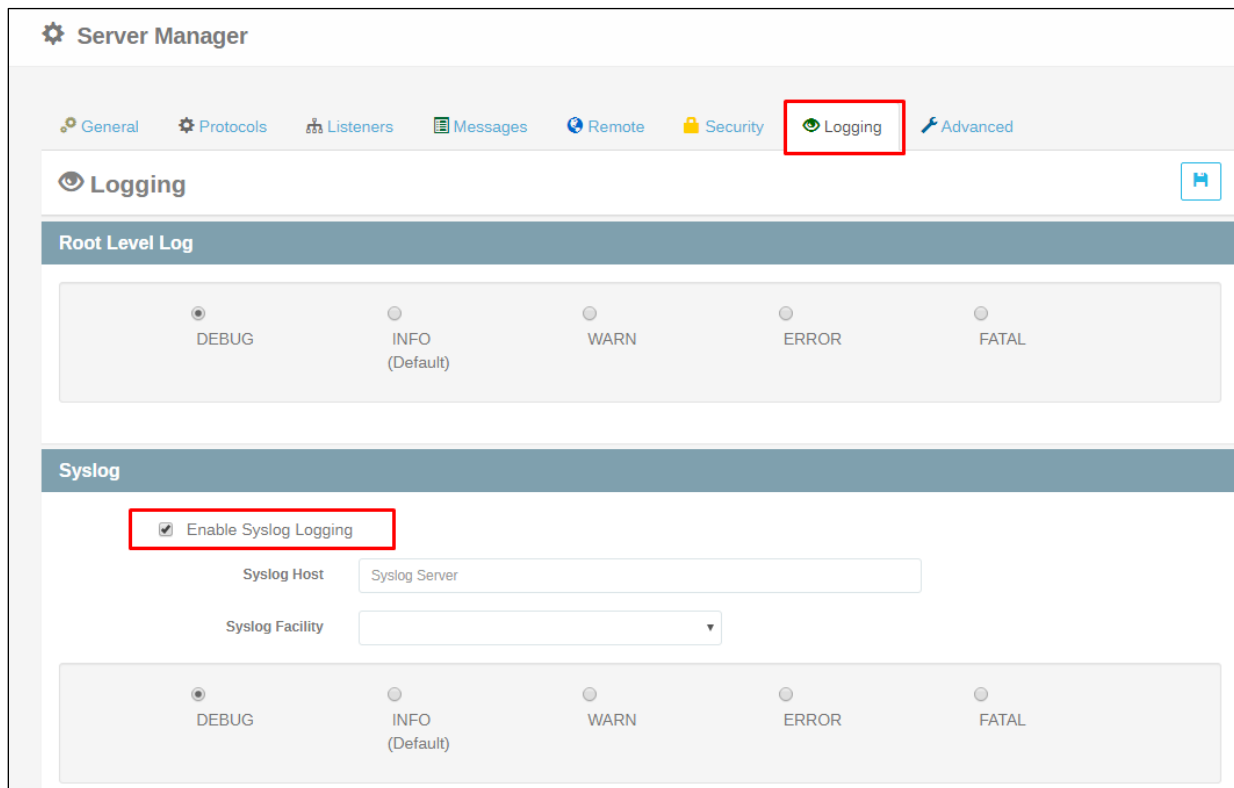
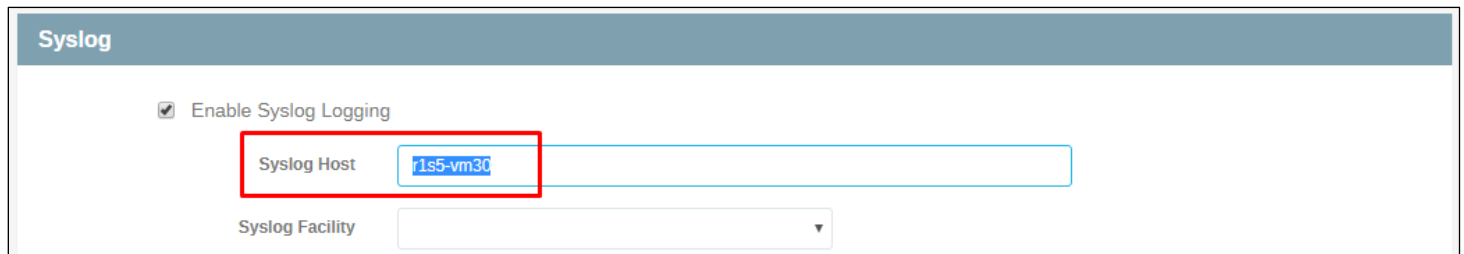


Figure 19

4. Provide the Syslog Host name.



Syslog

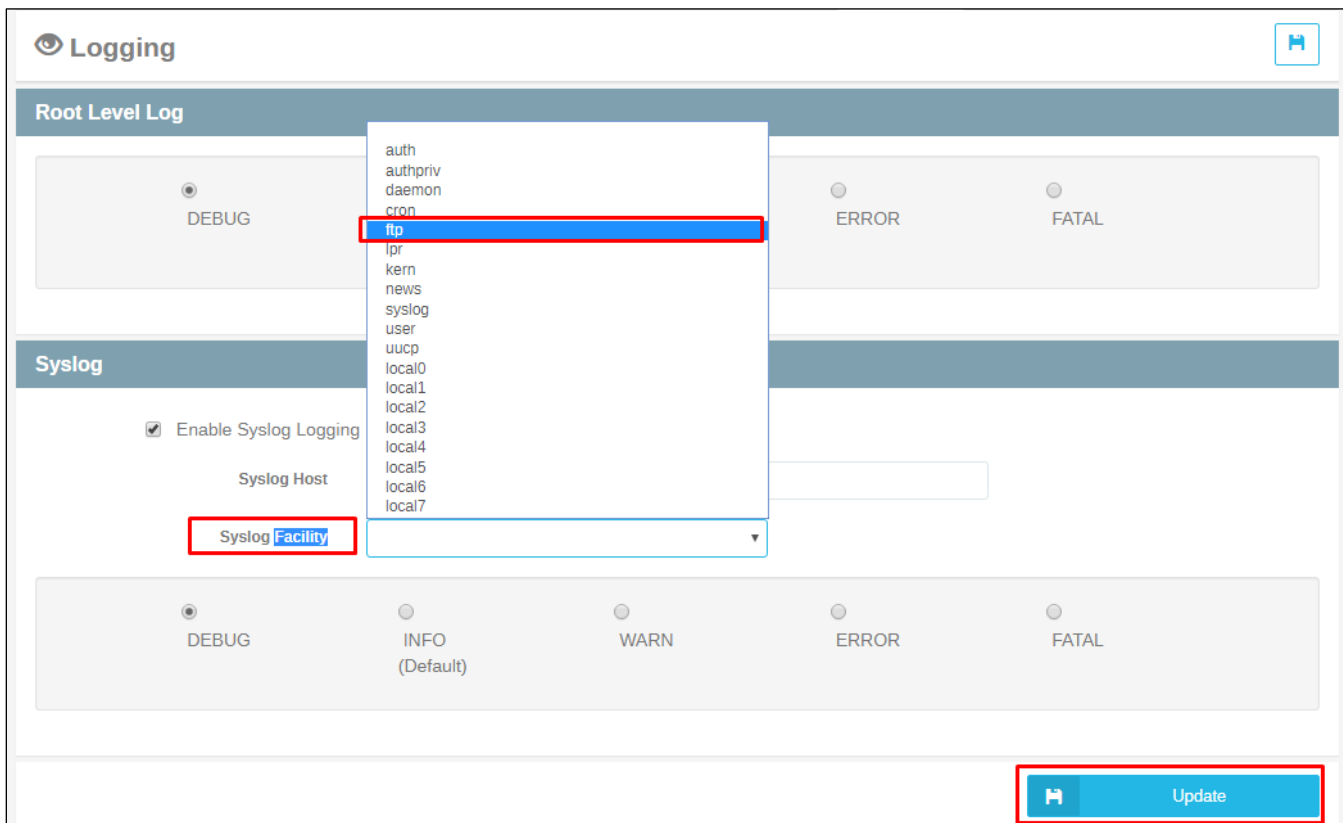
☒ Enable Syslog Logging

Syslog Host

Syslog Facility

Figure 20

5. Select the **syslog Facility** from option and **Update**.



Logging

Root Level Log

☒ DEBUG ☐ ERROR ☐ FATAL

Syslog

☒ Enable Syslog Logging

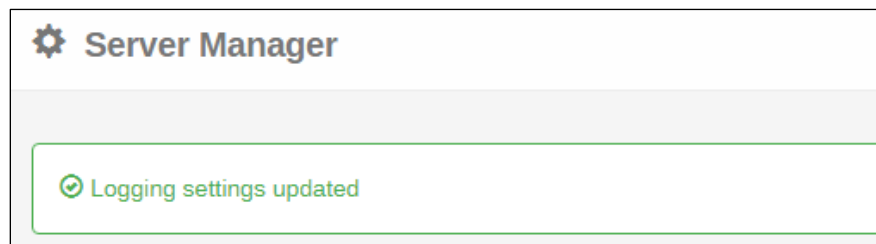
Syslog Host

Syslog Facility

☐ DEBUG ☐ INFO (Default) ☐ WARN ☐ ERROR ☐ FATAL

Figure 21

6. It will display message showing **Logging settings updated**.



Server Manager

✔ Logging settings updated

Figure 22

Cerberus SFTP Server Knowledge Pack:

Alerts

- **Cerberus SFTP Server- File Deleted:** This Alert provides information related to File deleted by user.
- **Cerberus SFTP Server- IP Blocked:** This Alert provides information related to Blocked IP.
- **Cerberus SFTP Server- User Account Blocked:** This Alert provides Information related to blocked user accounts in SFTP Server.
- **Cerberus SFTP Server- User Disable:** This Alert provides Information related to Disabled user accounts in SFTP Server.
- **Cerberus SFTP Server: User's Password Expire:** This Alert provides Information related to User's accounts Password Expire.

Flex Reports

- **Cerberus SFTP Server File Operations:** This report provides information related to File operations (File Deleted, Public File Shared, File Transfer, File Activities, Directory Created etc.)

EventId	Type	User Name	DirectoryName	File	File Name	File Size	IP Address	Local Directory	Local FilePath	Protocol	Remote DirectoryPath	Remote FilePath
3230	File Transfer	Matt		LFN22		500KB	172.55.66.33		LP55	UDP		RP88
3230	Public File Shared	clark		file10					contoso/file10			SharedUnit
3230	Directory Created	Tom	contoso/file1				172.23.55.44	contoso/shared		UDP	contoso/Remote	
3230	File Activities	Brenden		file123	file123		172.11.55.88		contoso/shared	TCP		Remote/contoso
3230	File Deleted	Joeb		LFN123			172.54.66.33		LP123	TCP		RP111
3230	File Transfer	Matt		LFN22		500KB	172.55.66.33		LP55	UDP		RP88
3230	File Deleted	Joeb		LFN123			172.54.66.33		LP123	TCP		RP111
3230	File Activities	Brenden		file123	file123		172.11.55.88		contoso/shared	TCP		Remote/contoso
3230	Directory Created	Tom	contoso/file1				172.23.55.44	contoso/shared		UDP	contoso/Remote	
3230	Public File Shared	clark		file10					contoso/file10			SharedUnit
3230	Public File Shared	clark		file10					contoso/file10			SharedUnit
3230	File Transfer	Matt		LFN22		500KB	172.55.66.33		LP55	UDP		RP88
3230	File Activities	Brenden		file123	file123		172.11.55.88		contoso/shared	TCP		Remote/contoso
3230	File Deleted	Joeb		LFN123			172.54.66.33		LP123	TCP		RP111
3230	Directory Created	Tom	contoso/file1				172.23.55.44	contoso/shared		UDP	contoso/Remote	
3230	Directory Created	Tom	contoso/file1				172.23.55.44	contoso/shared		UDP	contoso/Remote	
3230	Directory Created	Tom	contoso/file1				172.23.55.44	contoso/shared		UDP	contoso/Remote	
3230	File Activities	Brenden		file123	file123		172.11.55.88		contoso/shared	TCP		Remote/contoso
3230	File Deleted	Joeb		LFN123			172.54.66.33		LP123	TCP		RP111
3230	Public File Shared	clark		file10					contoso/file10			SharedUnit
3230	File Activities	Brenden		file123	file123		172.11.55.88		contoso/shared	TCP		Remote/contoso
3230	File Deleted	Joeb		LFN123			172.54.66.33		LP123	TCP		RP111
3230	File Transfer	Matt		LFN22		500KB	172.55.66.33		LP55	UDP		RP88
3230	File Transfer	Matt		LFN22		500KB	172.55.66.33		LP55	UDP		RP88

Figure 23

Sample Log:

Type: Directory Created, Timestamp: 2016-07-04 11:43:19, Username: Tom, User's Group: contoso, Protocol Type: UDP, User's Connection ID: 1114, User's IP Address: 172.23.55.44, User's FirstName: Tom, User's LastName: KP, User's Email: Tom.KP@contoso.com, User's MobileNumber: MBL, DirectoryName: contoso/file1, Local DirectoryPath: contoso/shared, Remote DirectoryPath: contoso/Remote, Successful Operation: Success"", max wait 60 seconds

Type: File Activities, Timestamp: 2016-08-04 11:43:19, Username: Brenden, User's Group: contoso, Protocol Type: TCP, User's ConnectionID: 44554, User's IP Address: 172.11.55.88, User's FirstName: Brenden, User's LastName: N, User's Email: Brenden.N@contoso.com, User's MobileNumber: MBL, File Name From: file123, File Name To: fileOld, Local FilePath From: contoso/shared, Remote FilePath From: Remote/contoso, Local FilePath To: Local/contoso, Remote FilePath To: file99, Move Operation: move, Copy Operation: copy, Successful Operation: successfully"", max wait 60 seconds

Type: File Deleted, Timestamp: 2016-09-04 11:43:19, Username: Joeb, User's Group: contoso, Protocol Type: TCP, User's ConnectionID: 7777, User's IP Address: 172.54.66.33, User's FirstName: Joeb, User's LastName: M, User's Email: Joeb.M@contoso.com, User's MobileNumber: MBL, File Name: LFN123, Local FilePath: LP123, Remote FilePath: RP111, Successful Operation: SO123. Directorv: DIR/contoso"". max wait 60 seconds

- **Cerberus SFTP Server IP Blocked:** This Report will provide information about blocked IP or range of IP addresses, which is in Blacklist IP Address List.

LogTime	EventId	EventSource	Type	Blocked IP	Timestamp
04/10/2019 06:55:38 PM	3230	Cerberus	IP Blocked	192.168.33.55""	2016-11-04 11:43:19
04/10/2019 06:55:40 PM	3230	Cerberus	IP Blocked	192.168.33.55""	2016-11-04 11:43:19
04/10/2019 06:55:41 PM	3230	Cerberus	IP Blocked	192.168.33.55""	2016-11-04 11:43:19
04/10/2019 06:55:42 PM	3230	Cerberus	IP Blocked	192.168.33.55""	2016-11-04 11:43:19
04/10/2019 07:21:39 PM	3230	Cerberus	IP Blocked	192.168.33.55	2016-11-04 11:43:19
04/10/2019 07:21:40 PM	3230	Cerberus	IP Blocked	192.168.33.55	2016-11-04 11:43:19
04/10/2019 07:21:41 PM	3230	Cerberus	IP Blocked	192.168.33.55	2016-11-04 11:43:19
04/10/2019 07:21:42 PM	3230	Cerberus	IP Blocked	192.168.33.55	2016-11-04 11:43:19
04/10/2019 07:21:43 PM	3230	Cerberus	IP Blocked	192.168.33.55	2016-11-04 11:43:19
04/11/2019 04:22:56 PM	3230	Cerberus	IP Blocked	192.10.22.44	2016-11-04 11:43:19
04/11/2019 04:22:56 PM	3230	Cerberus	IP Blocked	192.168.33.55	2016-11-04 11:43:19
04/11/2019 04:22:56 PM	3230	Cerberus	IP Blocked	192.168.22.99	2016-11-04 11:43:19
04/11/2019 04:22:58 PM	3230	Cerberus	IP Blocked	192.168.33.55	2016-11-04 11:43:19
04/11/2019 04:22:58 PM	3230	Cerberus	IP Blocked	192.168.22.99	2016-11-04 11:43:19

Figure 24

Sample Log:

Type: IP Blocked, Timestamp: 2016-11-04 11:43:19, Blocked IP: 192.168.33.55"", max wait 60 seconds

- **Cerberus SFTP Server Login Activities:** This Report provides Information related to Cerberus SFTP server login-logout activity.

LogTime	EventId	EventSource	Type	Timestamp	User Name	IP Address	Protocol Type
04/10/2019 02:58:00 PM	3230	Cerberus	Logout Activities	2016-13-04 11:43:19	Joe	172.55.66.44	TCP
04/10/2019 02:58:00 PM	3230	Cerberus	Login Activities	2016-12-04 11:43:19	Karen	172.22.5.60	UDP
04/10/2019 02:58:01 PM	3230	Cerberus	Logout Activities	2016-13-04 11:43:19	Joe	172.55.66.44	TCP
04/10/2019 02:58:01 PM	3230	Cerberus	Login Activities	2016-12-04 11:43:19	Karen	172.22.5.60	UDP
04/10/2019 02:58:02 PM	3230	Cerberus	Login Activities	2016-12-04 11:43:19	Karen	172.22.5.60	UDP
04/10/2019 02:58:02 PM	3230	Cerberus	Logout Activities	2016-13-04 11:43:19	Joe	172.55.66.44	TCP
04/10/2019 02:58:03 PM	3230	Cerberus	Login Activities	2016-12-04 11:43:19	Karen	172.22.5.60	UDP
04/10/2019 02:58:03 PM	3230	Cerberus	Logout Activities	2016-13-04 11:43:19	Joe	172.55.66.44	TCP
04/10/2019 02:58:04 PM	3230	Cerberus	Login Activities	2016-12-04 11:43:19	Karen	172.22.5.60	UDP
04/10/2019 02:58:04 PM	3230	Cerberus	Logout Activities	2016-13-04 11:43:19	Joe	172.55.66.44	TCP
04/10/2019 02:58:04 PM	3230	Cerberus	Login Activities	2016-12-04 11:43:19	Karen	172.22.5.60	UDP
04/10/2019 02:58:04 PM	3230	Cerberus	Logout Activities	2016-13-04 11:43:19	Joe	172.55.66.44	TCP
04/10/2019 02:58:05 PM	3230	Cerberus	Logout Activities	2016-13-04 11:43:19	Joe	172.55.66.44	TCP
04/10/2019 02:58:05 PM	3230	Cerberus	Login Activities	2016-12-04 11:43:19	Karen	172.22.5.60	UDP
04/10/2019 02:58:06 PM	3230	Cerberus	Logout Activities	2016-13-04 11:43:19	Joe	172.55.66.44	TCP
04/10/2019 02:58:06 PM	3230	Cerberus	Login Activities	2016-12-04 11:43:19	Karen	172.22.5.60	UDP
04/10/2019 02:58:43 PM	3230	Cerberus	Logout Activities	2016-13-04 11:43:19	Joe	172.55.66.44	TCP
04/10/2019 02:58:43 PM	3230	Cerberus	Login Activities	2016-12-04 11:43:19	Karen	172.22.5.60	UDP
04/10/2019 02:58:45 PM	3230	Cerberus	Login Activities	2016-12-04 11:43:19	Karen	172.22.5.60	UDP
04/10/2019 02:58:45 PM	3230	Cerberus	Logout Activities	2016-13-04 11:43:19	Joe	172.55.66.44	TCP
04/10/2019 02:58:46 PM	3230	Cerberus	Logout Activities	2016-13-04 11:43:19	Joe	172.55.66.44	TCP

Figure 25

Sample Log:

Type: Login Activities, Timestamp: 2016-12-04 11:43:19, Username: Karen, User's Group: contoso, Protocol Type: UDP, User's ConnectionID: 5588, User's IP Address: 172.22.5.60, User's FirstName: Karen, User's LastName: L, User's Email: Karen.L@contoso.com, User's MobileNumber: MBL"", max wait 60 seconds

Type: Logout Activities, Timestamp: 2016-13-04 11:43:19, Username: Joe, User's Group: contoso, Protocol Type: TCP, User's ConnectionID: 4488, User's IP Address: 172.55.66.44, User's FirstName: Joe, User's LastName: T, User's Email: Joe.T@contoso.com, User's MobileNumber: MBL"", max wait 60 seconds

- **Cerberus SFTP Server User Account Activities:** This report provides information related to User's Account activities (User Account Blocked, User Disabled, New Account Request, Account Password Expiring etc.)

LogTime	EventId	Type	Blocked User	Disabled User	Password Expires	Requested User	Timestamp	User Group	User Name
04/10/2019 02:58:04 PM	3230	User Account Blocked	Mary™				2016-18-04 11:43:19		Mary™
04/10/2019 02:58:04 PM	3230	User Disable		Albert			2016-19-04 11:43:19		Albert
04/10/2019 02:58:04 PM	3230	User Account Blocked	Mary™				2016-18-04 11:43:19		Mary™
04/10/2019 02:58:05 PM	3230	User Account Blocked	Mary™				2016-18-04 11:43:19		Mary™
04/10/2019 02:58:05 PM	3230	New Account Request				Peter	2016-14-04 11:43:19		Peter
04/10/2019 02:58:05 PM	3230	User Disable		Albert			2016-19-04 11:43:19		Albert
04/10/2019 02:58:05 PM	3230	Account Password Expiring			April 20™		2019-05-04 11:43:19	contoso	Gary
04/10/2019 02:58:06 PM	3230	User Disable		Albert			2016-19-04 11:43:19		Albert
04/10/2019 02:58:06 PM	3230	Account Password Expiring			April 20™		2019-05-04 11:43:19	contoso	Gary
04/10/2019 02:58:06 PM	3230	New Account Request				Peter	2016-14-04 11:43:19		Peter
04/10/2019 02:58:06 PM	3230	User Account Blocked	Mary™				2016-18-04 11:43:19		Mary™
04/10/2019 02:58:43 PM	3230	New Account Request				Peter	2016-14-04 11:43:19		Peter
04/10/2019 02:58:43 PM	3230	Account Password Expiring			April 20™		2019-05-04 11:43:19	contoso	Gary
04/10/2019 02:58:43 PM	3230	User Account Blocked	Mary™				2016-18-04 11:43:19		Mary™
04/10/2019 02:58:43 PM	3230	User Disable		Albert			2016-19-04 11:43:19		Albert
04/10/2019 02:58:44 PM	3230	Account Password Expiring			April 20™		2019-05-04 11:43:19	contoso	Gary
04/10/2019 02:58:45 PM	3230	User Account Blocked	Mary™				2016-18-04 11:43:19		Mary™
04/10/2019 02:58:45 PM	3230	User Disable		Albert			2016-19-04 11:43:19		Albert
04/10/2019 02:58:45 PM	3230	New Account Request				Peter	2016-14-04 11:43:19		Peter
04/10/2019 02:58:45 PM	3230	Account Password Expiring			April 20™		2019-05-04 11:43:19	contoso	Gary
04/10/2019 02:58:46 PM	3230	New Account Request				Peter	2016-14-04 11:43:19		Peter
04/10/2019 02:58:46 PM	3230	User Account Blocked	Mary™				2016-18-04 11:43:19		Mary™
04/10/2019 02:58:46 PM	3230	User Disable		Albert			2016-19-04 11:43:19		Albert

Figure 26

Sample Log:

Type: User Account Blocked, Timestamp: 2016-18-04 11:43:19, Blocked Username: Mary™, max wait 60 seconds
 Type: User Disable, Timestamp: 2016-19-04 11:43:19, Disabled Username: Albert, User's Group: contoso, User's FirstName: Albert, User's LastName: X, User's Email: Albert.X@contoso.com™, max wait 60 seconds
 Type: Account Password Expiring, Timestamp: 2019-05-04 11:43:19, Username: Gary, UserGroup: contoso, User's FirstName: Gary, User's LastName: LM, User's Email: Gary.LM@contoso.com, User's MobileNumber: MBL, User's Password Expires: April 20™,
 Type: New Account Request, Timestamp: 2016-14-04 11:43:19, Requested Username: Peter, First Name: Peter, Last Name: L. Email Address: Peter.L@contoso.com. Telephone Number: 022-558866. Justification: J™. max wait 60 seconds

Dashboards

- Cerberus SFTP Server - All Activities:**

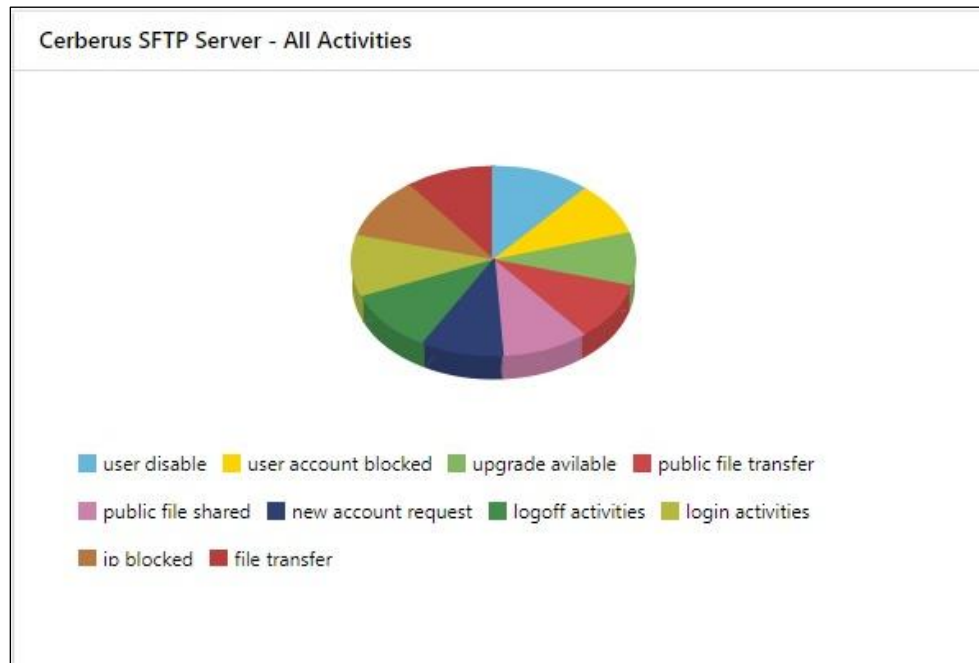


Figure 27

- Cerberus SFTP Server - File and Folder Activities:**

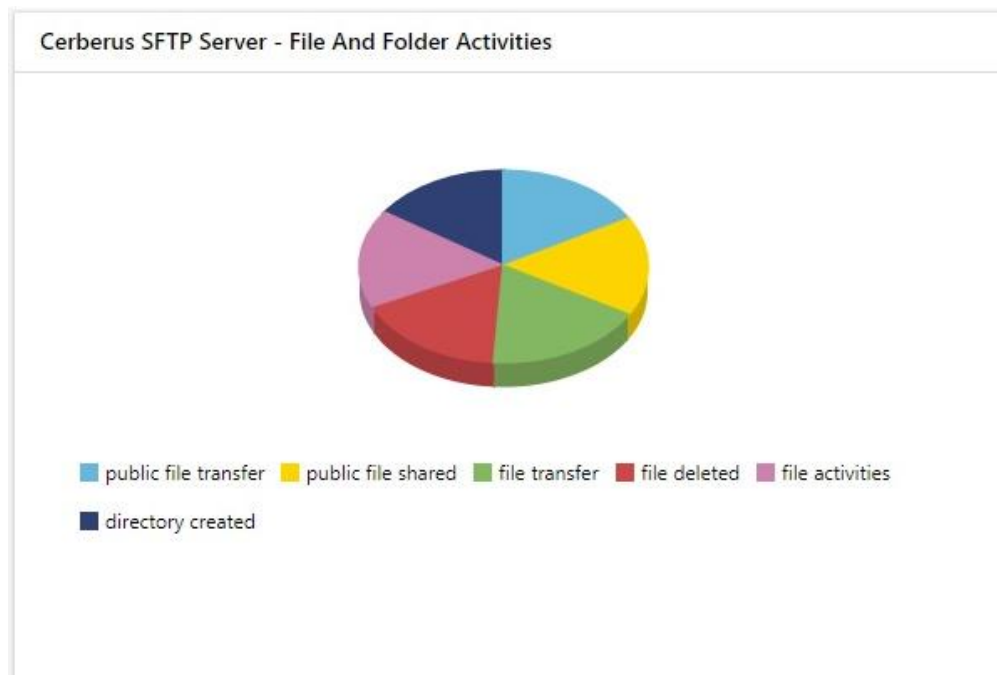


Figure 28

- Cerberus SFTP Server - File Deleted by User

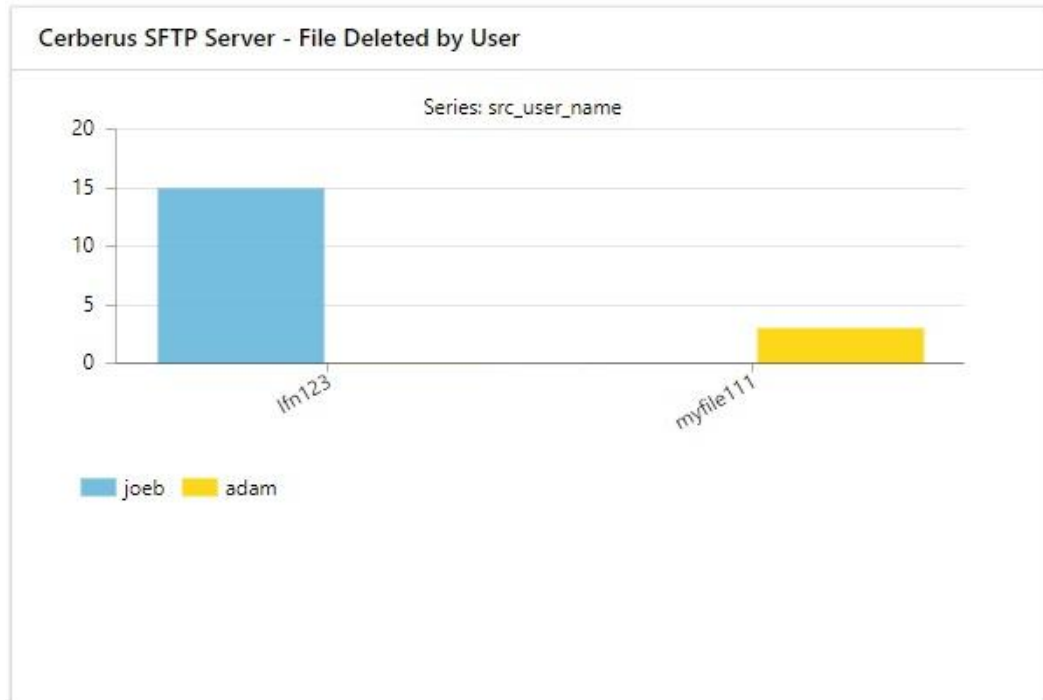


Figure 29

- Cerberus SFTP Server - IP Blocked

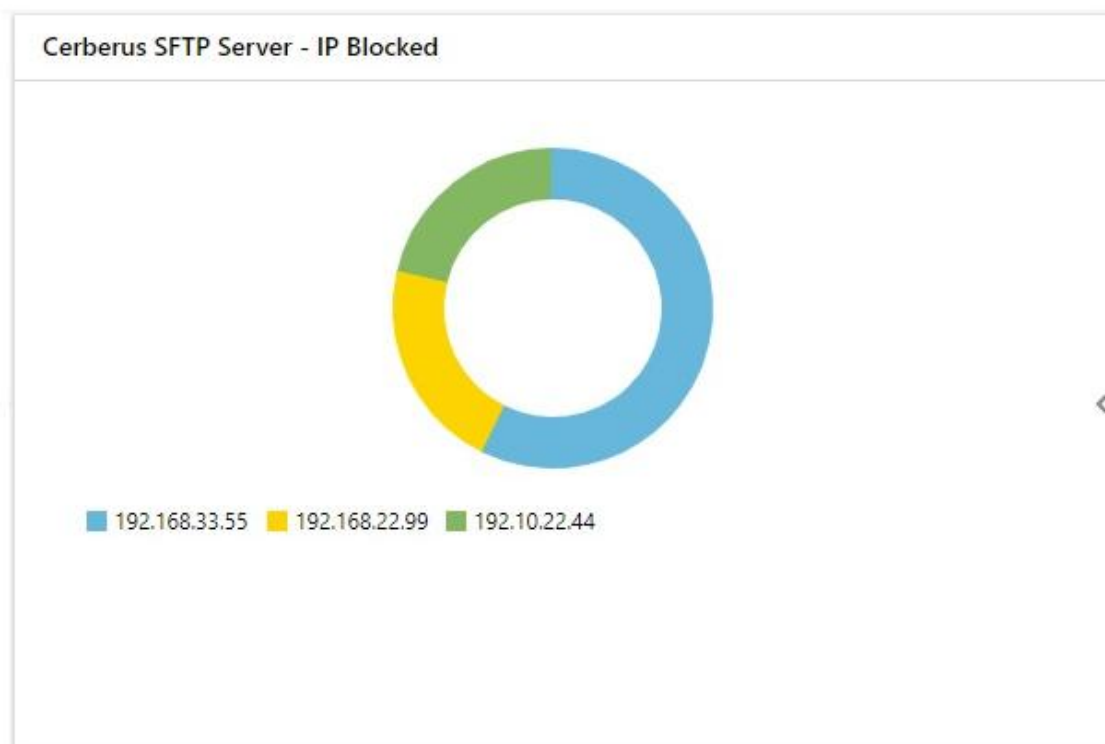


Figure 30

- **Cerberus SFTP Server - Login-Logoff activities:**

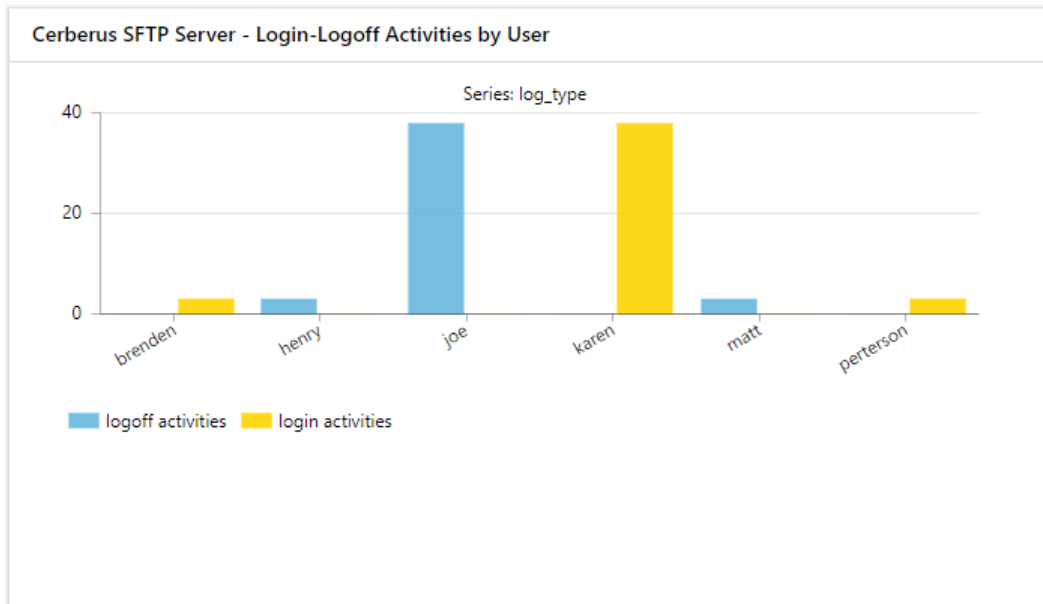


Figure 31

- **Cerberus SFTP Server - Password Expiring:**

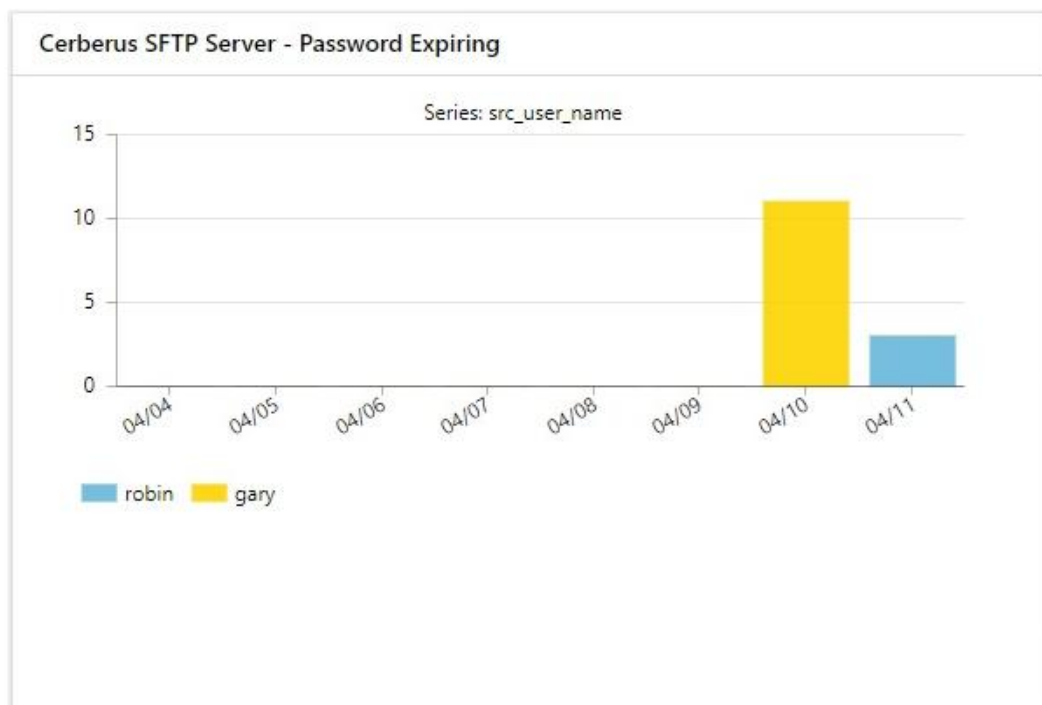


Figure 32

- **Cerberus SFTP Server - Public File shared by User:**

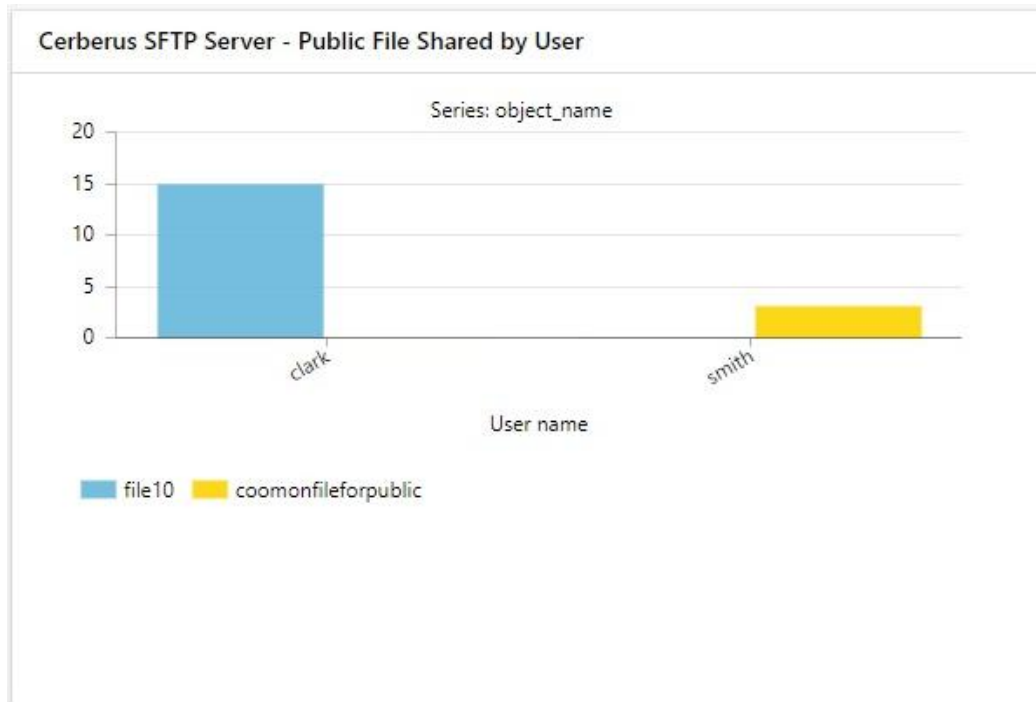


Figure 33

- **Cerberus SFTP Server - Public File Transferred by Source IP:**



Figure 34

- **Cerberus SFTP Server - User Disabled**

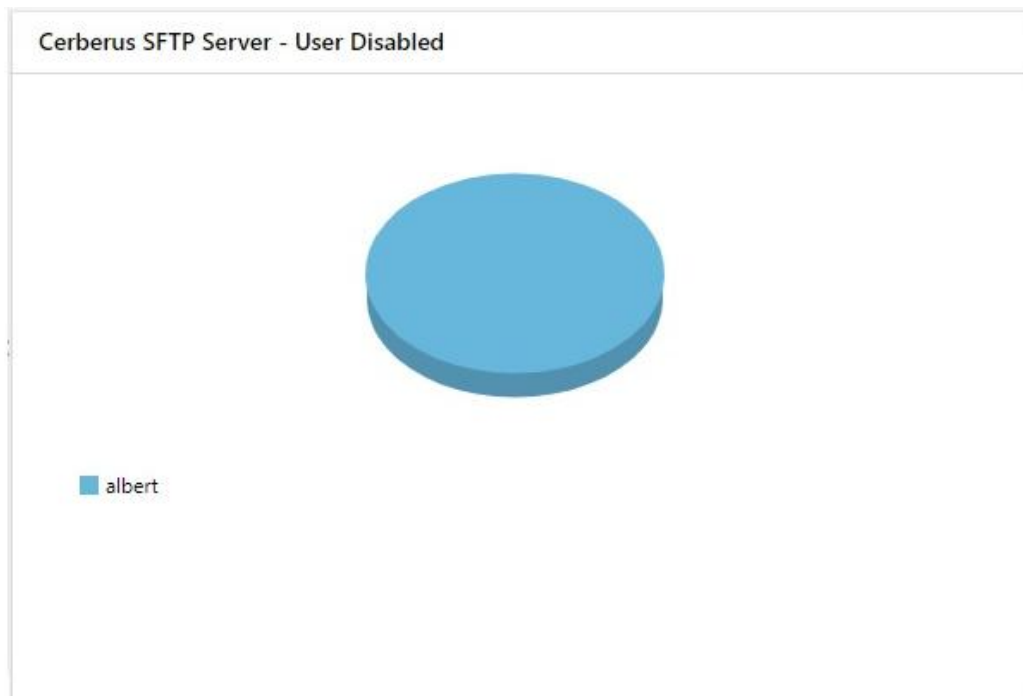


Figure 35

- **Cerberus SFTP Server - Username Blocked**

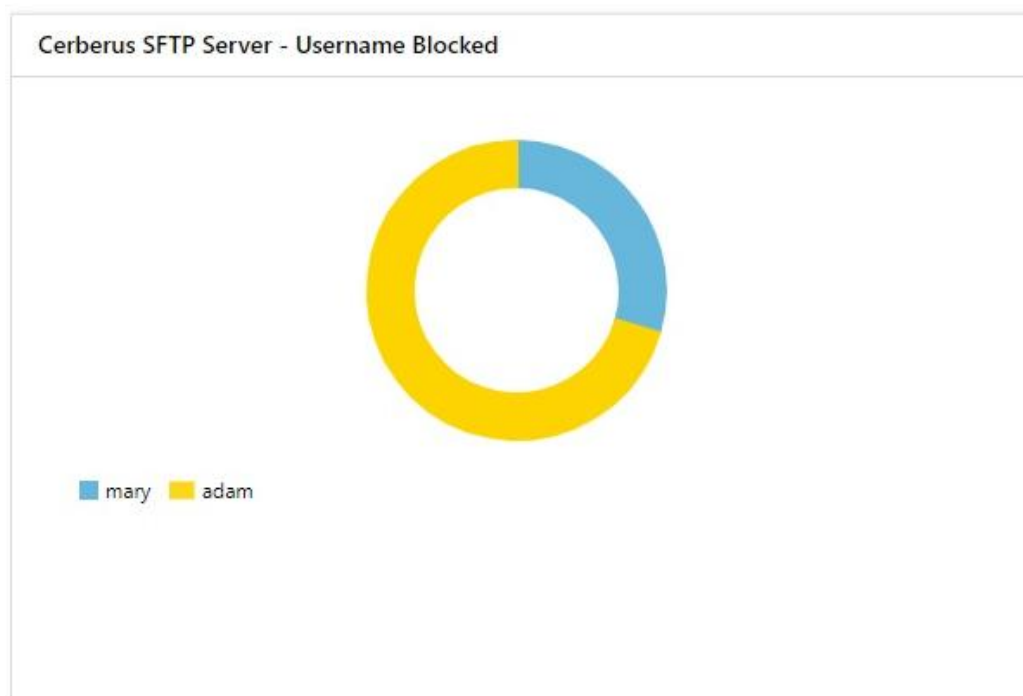


Figure 36

Import Cerberus SFTP Server knowledge pack into EventTracker

- Alerts
- Flex Reports
- Knowledge Objects
- Dashlets

Alerts

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

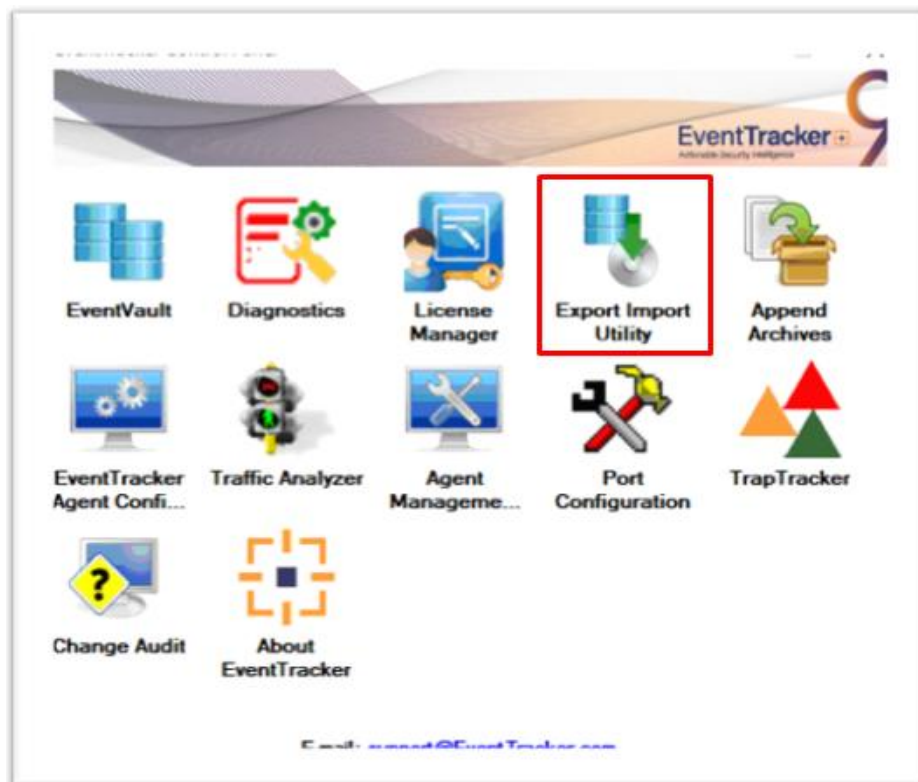


Figure 37

3. Click the **Import** tab.
4. Select **Alert** option.
5. Click on **Browse** button and select **file path**.
6. Click on **Import**.

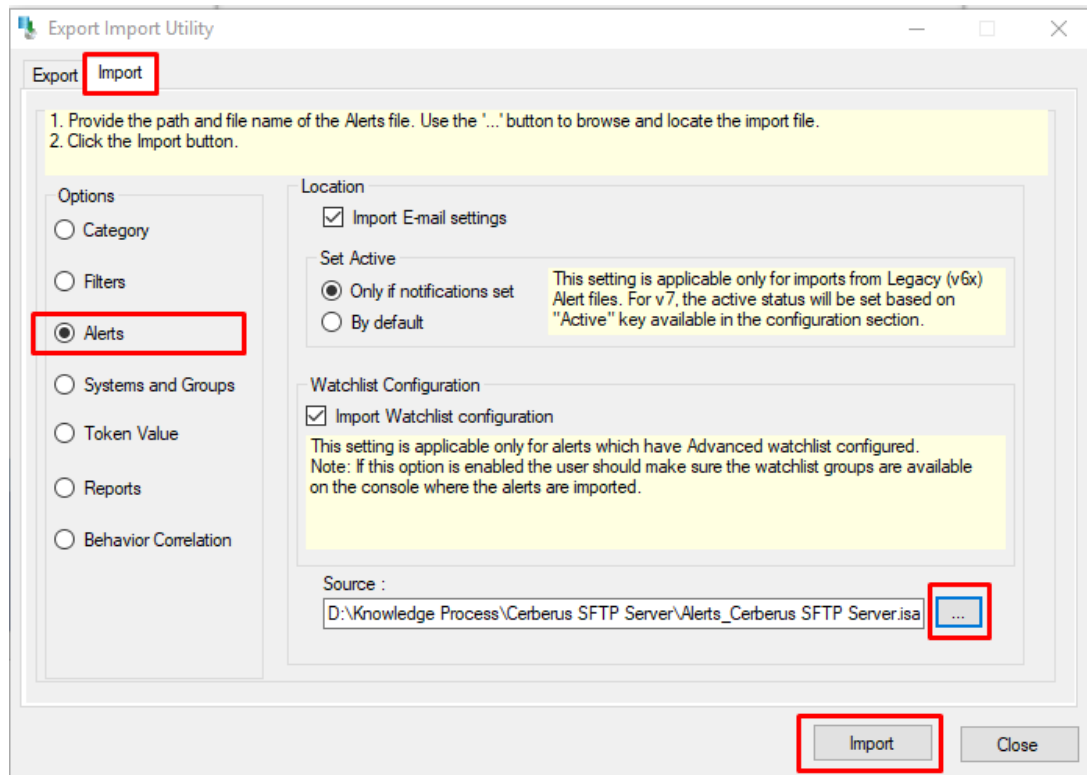


Figure 38

7. Alerts are now imported successfully.

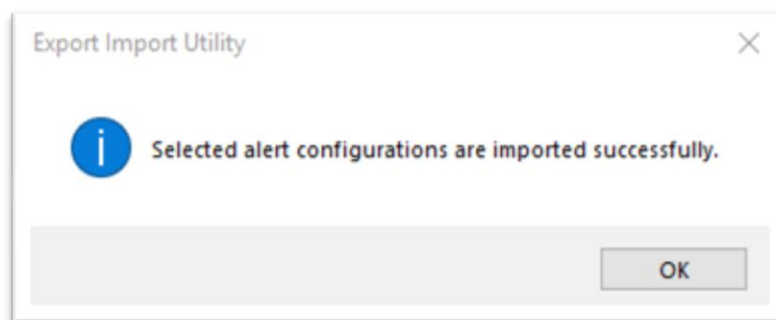


Figure 39

Flex Reports

On EventTracker **Control Panel**,

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

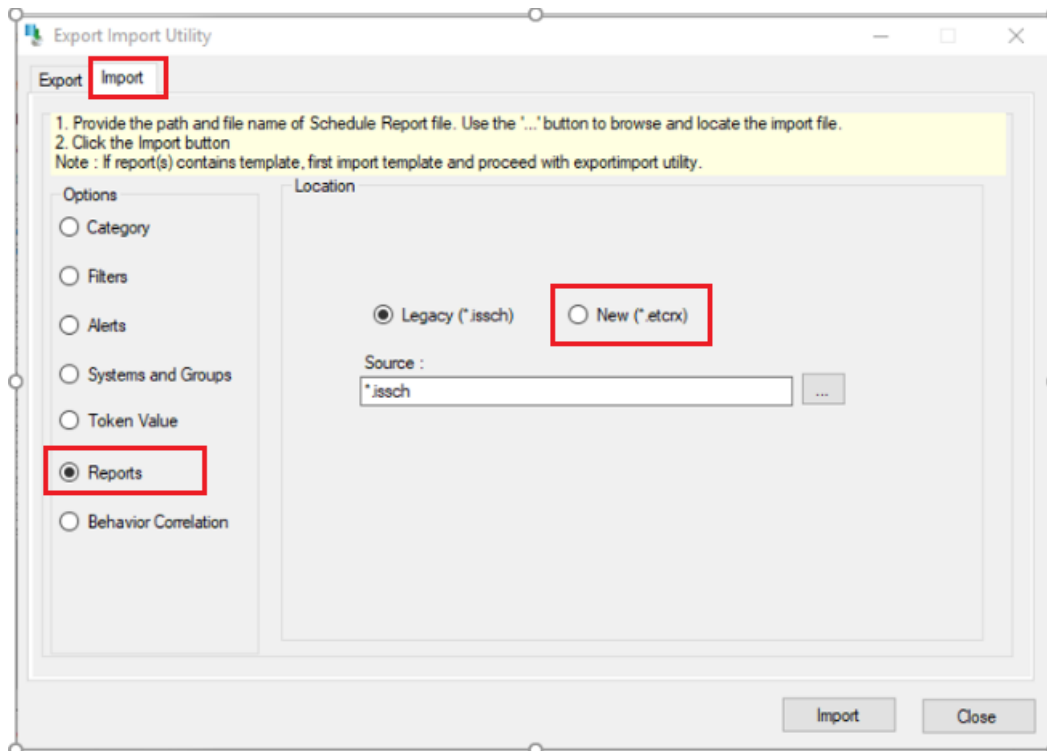


Figure 40

2. Locate the file named **Reports_Cerberus SFTP Server.etcrx** and select all the checkbox.

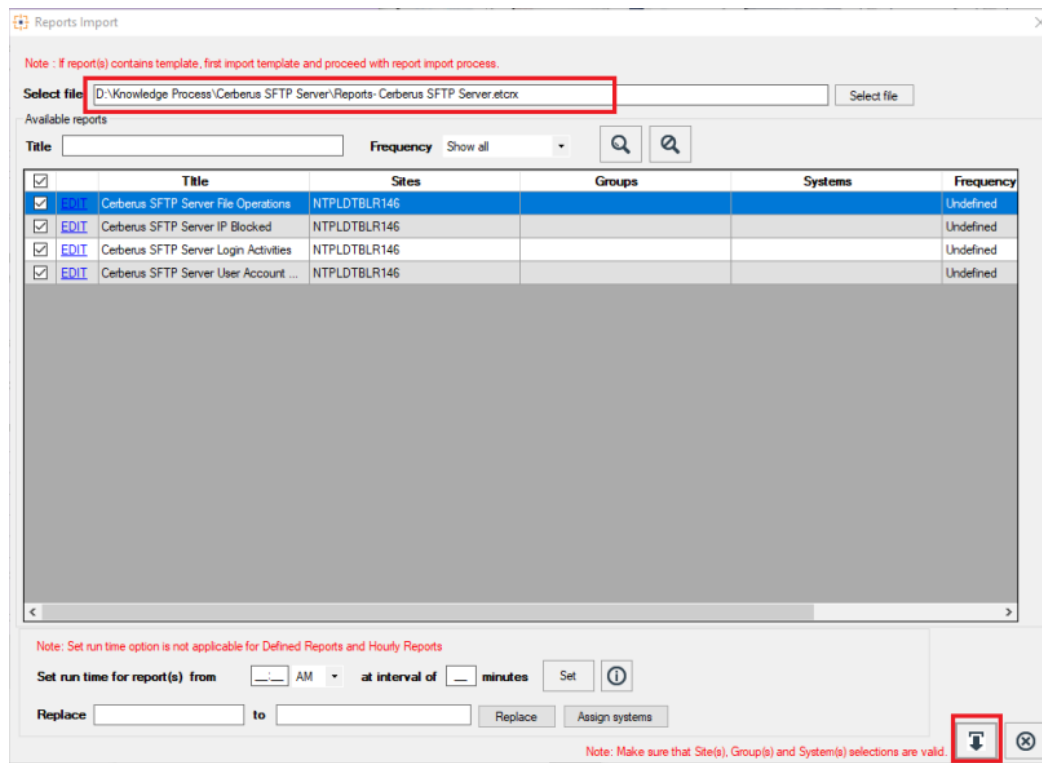


Figure 41

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

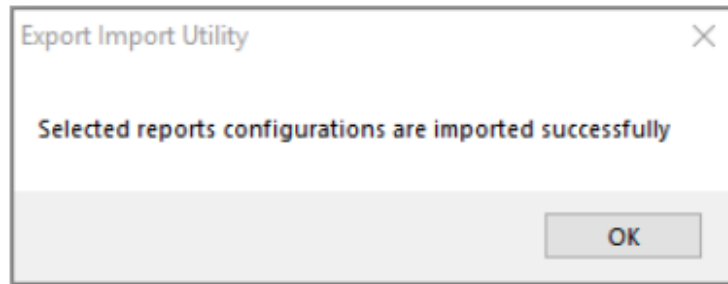


Figure 42

Knowledge Objects

- Login to EventTracker console
- Click **Knowledge objects** under Admin option in the **EventTracker manager** page.
- Locate the file named **KO_Cerberus SFTP Server.etko**



Figure 43

- Now select all the checkbox and then click on '**Upload**' option.
- Knowledge objects are now imported successfully.

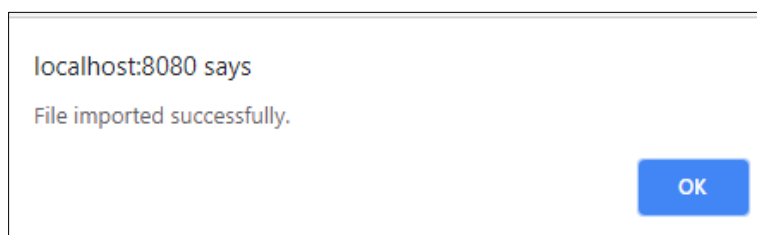


Figure 44

Dashboards

- Open **EventTracker Enterprise** in the browser and log in.

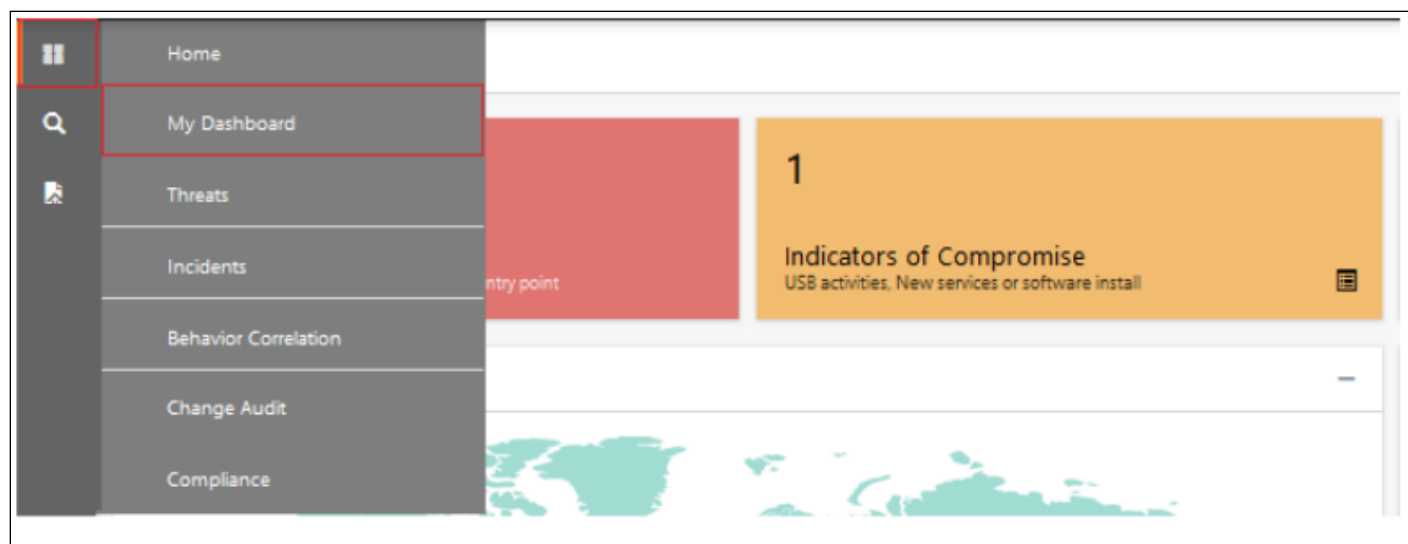


Figure 45

2. Navigate to **My Dashboard**.
3. Click on **Import Configuration** icon on the top right corner.
4. In the popup window browse the file named **Dashboard_Cerberus SFTP Server.etwd**

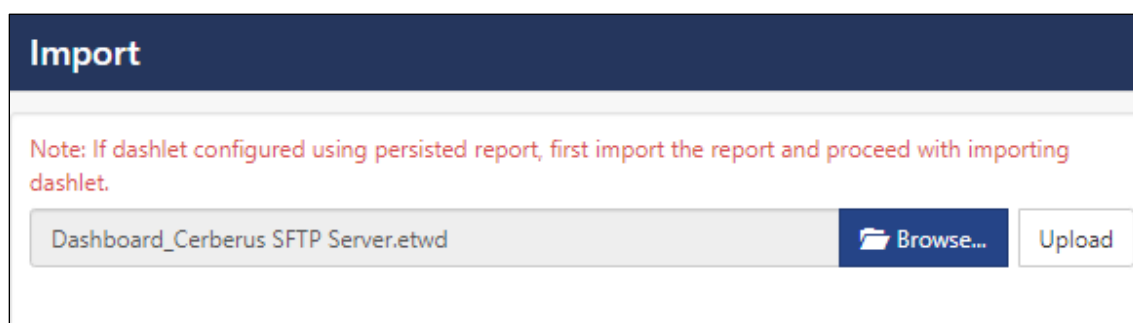


Figure 46

1. Now select all the checkbox and then click on **Import** option.

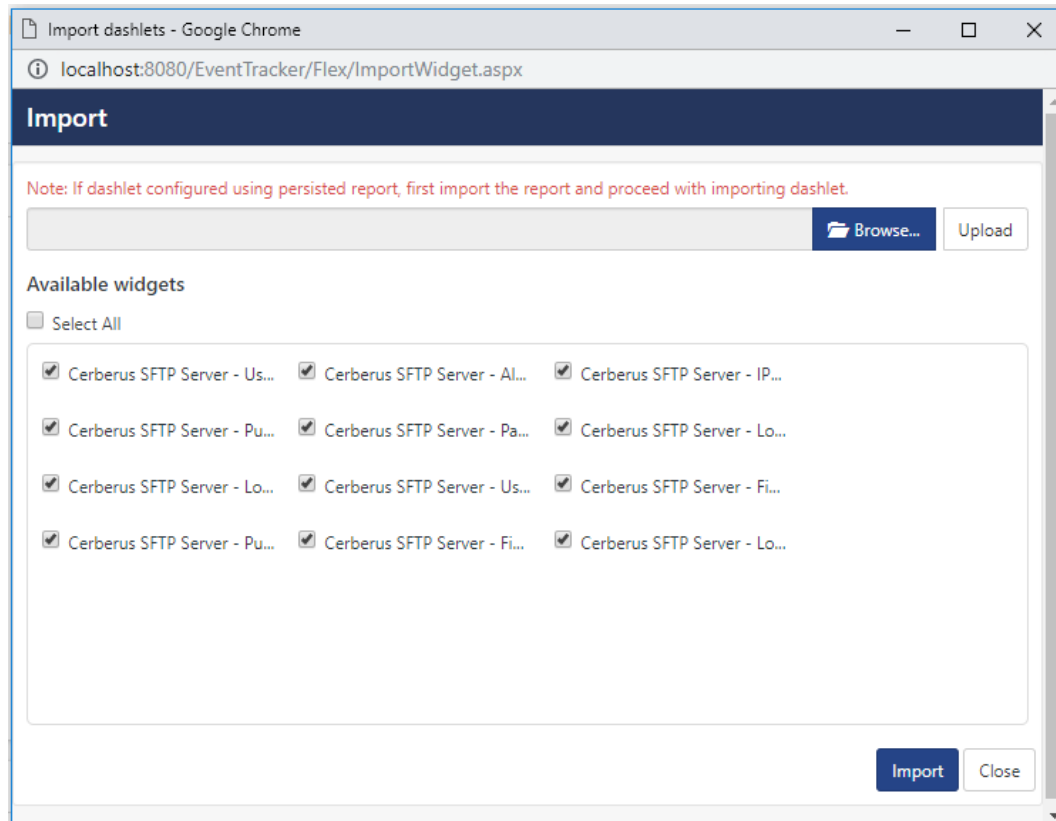



Figure 47

2. Click 'customize'  to locate and choose the created dashlets.
3. Click **Add** to add Dashlets to the dashboard.

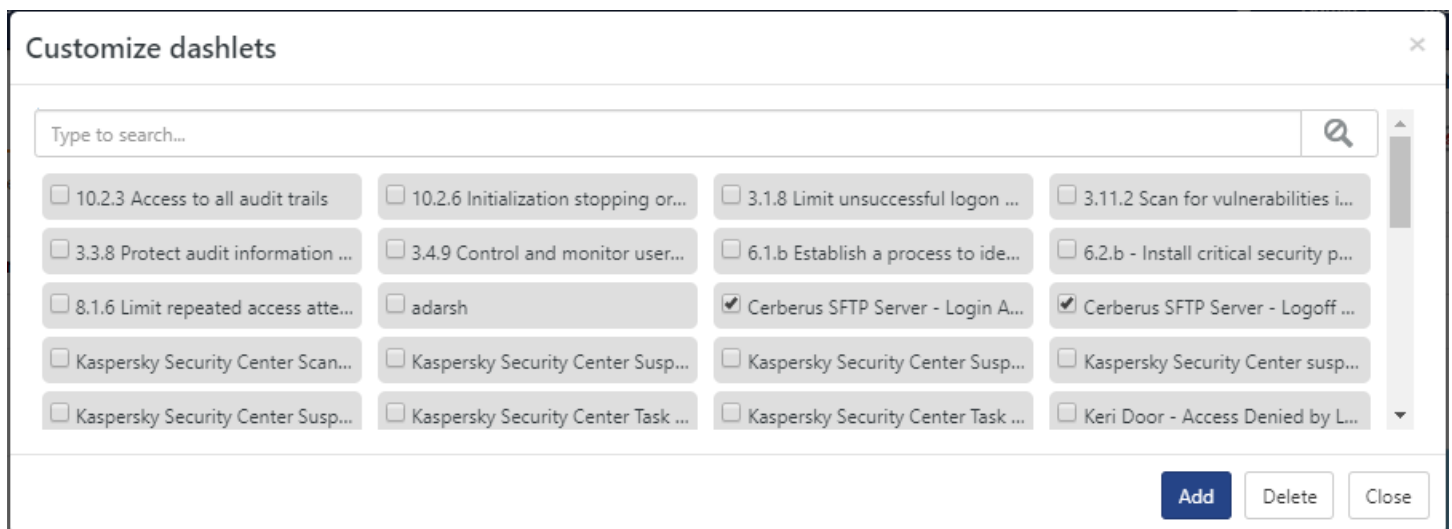


Figure 48

Verify Cerberus SFTP Server knowledge pack in EventTracker

Knowledge Object

1. In the **EventTracker Enterprise** web interface, click the **Admin** drop-down, and then click **Knowledge Objects**.
2. In the **Knowledge Object tree**, expand **Cerberus SFTP Server** group folder to view the imported Knowledge objects.

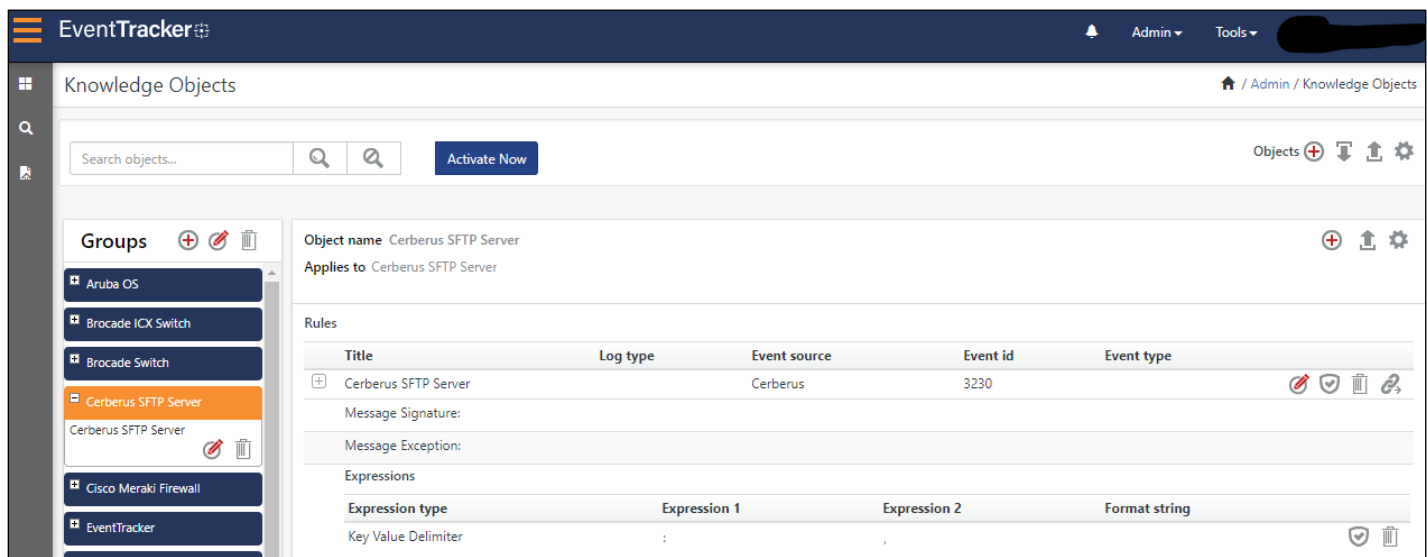


Figure 49

Flex Reports

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

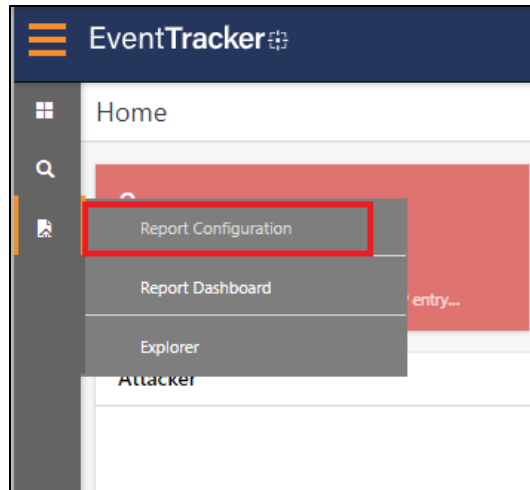


Figure 50

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

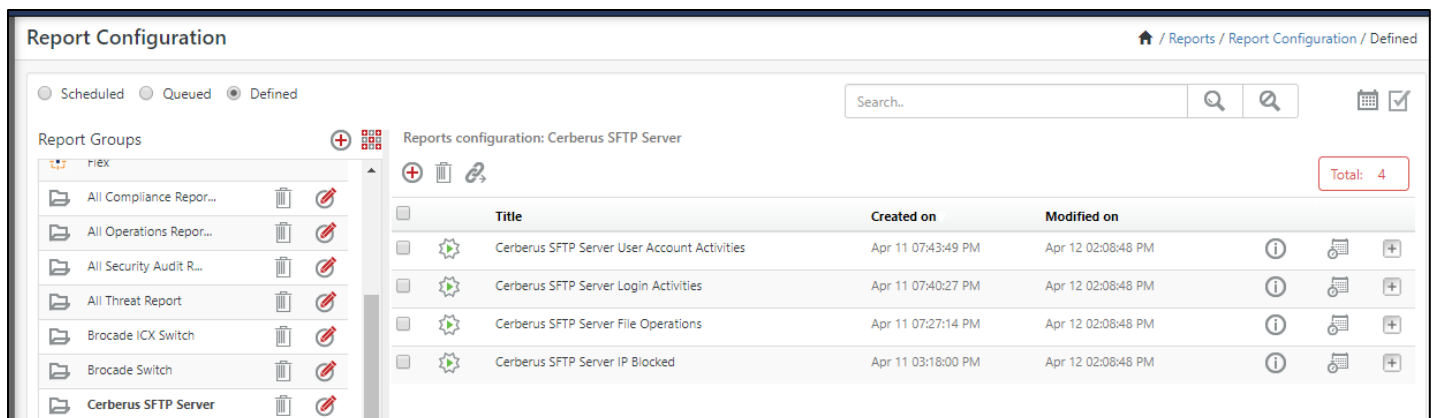


Figure 51

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** icon, and then select **Alerts**.

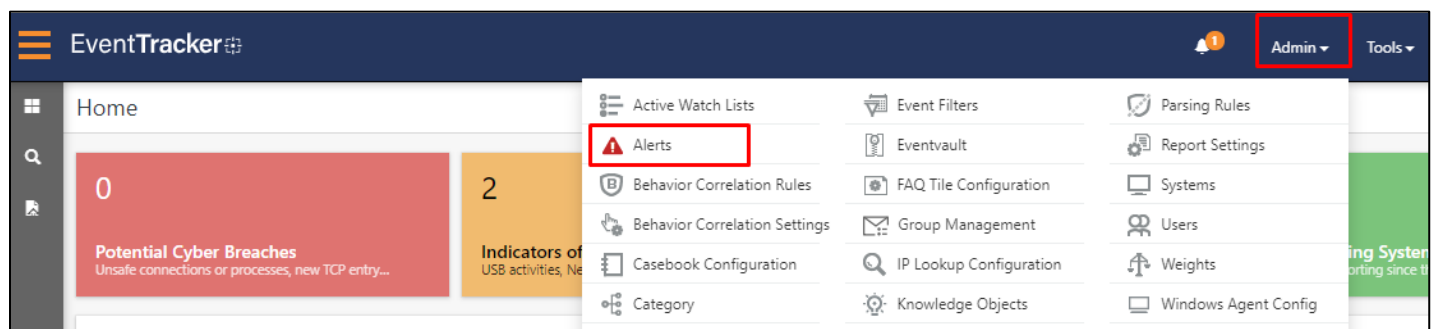


Figure 52

2. In the Alert search bar we can search the alert name and view the imported **Cerberus SFTP Server Alerts**.

Alerts Admin / Alerts

Show All Search by Alert name cerberus

143
Available Alerts
Total number of alerts available

20
Active Alerts
Total number of active alerts

143
System/User Defined Alerts
Count for system and user defined alerts
System 110
User 33

143
Alerts by Threat Level
Count of alerts by threat level
Critical 10
Low 14
Serious 23
6

Activate Now Click 'Activate Now' after making all changes Total: 5 Page Size 25

<input type="checkbox"/>	Alert Name ^	Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
<input type="checkbox"/>	Cerberus SFTP Server: File Deleted	●	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cerberus SFTP Server
<input type="checkbox"/>	Cerberus SFTP Server: IP Blocked	●	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cerberus SFTP Server
<input type="checkbox"/>	Cerberus SFTP Server: User Account Blocked	●	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cerberus SFTP Server
<input type="checkbox"/>	Cerberus SFTP Server: User Disable	●	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cerberus SFTP Server
<input type="checkbox"/>	Cerberus SFTP Server: User's Password Expire	●	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cerberus SFTP Server

Figure 53