# Microsoft Exchange

## Logpoint Log Sources Configuration Guide

LogPoint

# Table of Contents

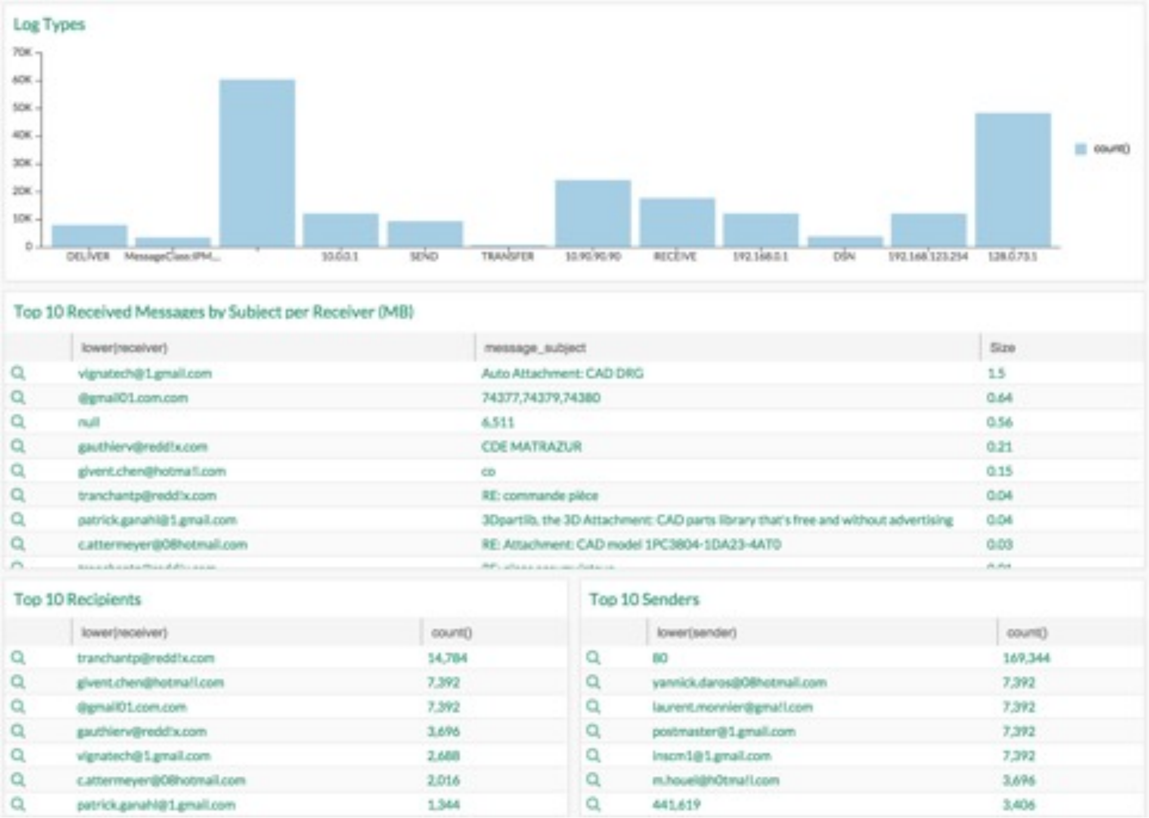
## General Description

With this integration, LogPoint can fully extract and correlate the Microsoft Exchange events while combining the results with observations from other systems. Administrators of the Microsoft Exchange can use LogPoint to get real-time alerts and provide long-term analytics.

## Functional Description

Key analytical components of the integration are: Ability to normalize data from the specified source and view statistics for Microsoft Exchange.

## Screenshots



Top 10 Received Messages by Subject per Receiver (MB)

| | lower(receiver) | message_subject | Size |
|---|---|---|---|
| 🔍 | vignatech@1.gmail.com | Auto Attachment: CAD DRG | 1.5 |
| 🔍 | @gmail01.com.com | 74377,74379,74380 | 0.64 |
| 🔍 | null | 6.511 | 0.56 |
| 🔍 | gauthierv@redd!x.com | CDE MATRAZUR | 0.21 |
| 🔍 | givent.chen@hotma!l.com | co | 0.15 |
| 🔍 | tranchantp@redd!x.com | RE: commande pièce | 0.04 |
| 🔍 | patrick.ganahl@1.gmail.com | 3Dpartlib, the 3D Attachment: CAD parts library that's free and without advertising | 0.04 |
| 🔍 | c.attermeyer@08hotmail.com | RE: Attachment: CAD model 1PC3804-1DA23-4AT0 | 0.03 |

Top 10 Recipients

| | lower(receiver) | count() |
|---|---|---|
| 🔍 | tranchantp@redd!x.com | 14,784 |
| 🔍 | givent.chen@hotma!l.com | 7,392 |
| 🔍 | @gmail01.com.com | 7,392 |
| 🔍 | gauthierv@redd!x.com | 3,696 |
| 🔍 | vignatech@1.gmail.com | 2,688 |
| 🔍 | c.attermeyer@08hotmail.com | 2,016 |
| 🔍 | patrick.ganahl@1.gmail.com | 1,344 |

Top 10 Senders

| | lower(sender) | count() |
|---|---|---|
| 🔍 | 80 | 169,344 |
| 🔍 | yannick.daros@08hotmail.com | 7,392 |
| 🔍 | laurent.monnier@gma!l.com | 7,392 |
| 🔍 | postmaster@1.gmail.com | 7,392 |
| 🔍 | inscm1@1.gmail.com | 7,392 |
| 🔍 | m.houel@h0tma!l.com | 3,696 |
| 🔍 | 441,619 | 3,406 |

## Supported Devices

The supported versions of Microsoft Exchange with LogPoint in this configuration are:

- Microsoft Exchange Message Tracking 2010, 2013 - space delimited or comma delimited.
- Microsoft Exchange 2003, 2010, 2013.

## Configure Microsoft Exchange

Microsoft provides multiple methods for Auditing Exchange Server. To forward the Microsoft Exchange logs to LogPoint, we need to configure Microsoft Exchange using LogBinder whereas to forward Microsoft Exchange Message Tracking logs to LogPoint, we need to install and configure LogPoint Agent in the server, where the Microsoft Exchange is present.

This document will show the steps to configure Microsoft Exchange using LogPoint Agent and LogBinder.

## LogPoint Agent:

LogPoint Agent is used to forward the logs of MS Exchange Message Tracking (MT). It requires events collected from Microsoft Exchange Message Tracking in a comma-separated format. It should be installed on the server, where MS Exchange is present. To install and configure the LogPoint Agent, please refer to: https://servicedesk.logpoint.com/hc/en-us/articles/207555339-LogPoint-Agent-v4-1-0

## LogBinder:

The following configuration steps apply for Microsoft Exchange 2013. LogBinder does not currently support Microsoft Exchange 2016

Mailbox Auditing is disabled by default. Hence to enable mail audit for already created user do as follows:

$UserMailboxes = Get-mailbox -Filter {(RecipientTypeDetails -eq 'UserMailbox')}

$UserMailboxes | ForEach {Set-Mailbox $_.Identity -AuditEnabled $true}

To enable automatic auditing of a user while creating mailbox via Exchange Admin Center and Exchange Management Shell is by using CmdletExtensionsAgent. This cmdlet will help to execute automated tasks.<**Get-CmdletExtensionAgent**> will list all the Extension available. For Automated tasks "Scripting Agent" is used. This Extension will enable automatic execution of command after execution of cmdlets in exchange.

To enabled Agent Enter the follow the below steps.

i. Script will be located at the following location: <Installation Folder>\Microsoft\Exchange Server\V15\Bin\CmdletExtensionAgents\.

ii. The script will not be functional until file extension is changed to the *.xml or a new file is created with **"ScriptingAgentConfig.**XML**"** name.

Sample Script which will help to enable auditing after creation or enabling of user in Exchange Server.

```
<?xml version="1.0" encoding="utf-8" ?>
<Configuration version="1.0">
<!--
In order to enable Scripting Agent:
- rename this file to ScriptingAgentConfig.xml
- edit it appropriately
- run the task: enable-CmdletExtensionAgent "Scripting Agent"

In order to include into your scriptlet characters prohibited in XML,
use escape sequences, e.g.
```

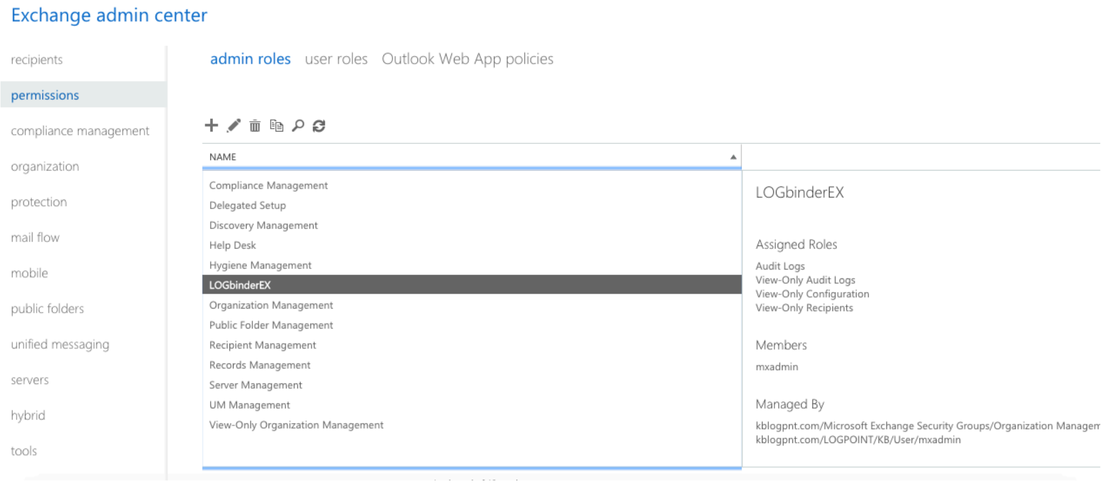
```
"&lt;","&gt;","&amp;" for "less than", greater than" and "ampersand
respectively.

-->

    <Feature Name="MailboxProvisioning" Cmdlets="new-mailbox,enable-
    mailbox">
    <ApiCall Name="OnComplete">
    If ($succeeded)
    {
    $Alias=$provisioningHandler.UserSpecifiedParameters["Alias"]
    $mailbox= Get-Mailbox $Alias
    Set-Mailbox $mailbox -AuditEnabled $true
    }
    </ApiCall>
    </Feature>

</Configuration>
```

After creating new file in the above folder with name "ScriptingAgentConfig.xml". Enter the following command to enable the agent
**Enable-CmdletExtensionAgent -Identity "Scripting Agent"**

### Installation and Configuration of LogBinderEX

Following are the prerequisite of LogBinderEX Installation

- Login using User with a privilege of a local administrator in exchange server.  It is recommended to run the Logbinder Application with Administrator Privilege.
- Create a group in the exchange with the following roles to ensure successful auditing of Exchange via Logbinder which will be used as service account for the application.
    - View-Only Audit Logs
    - View-Only Configuration
    - View-Only Recipients
    - Audit Logs (This option is only needed if using the LOGbinder’s Mailbox Audit Policy management wizard)



NAME
Compliance Management
Delegated Setup
Discovery Management
Help Desk
Hygiene Management
LOGbinderEX
Organization Management
Public Folder Management
Recipient Management
Records Management
Server Management
UM Management
View-Only Organization Management

LOGbinderEX

Assigned Roles
Audit Logs
View-Only Audit Logs
View-Only Configuration
View-Only Recipients

Members
mxadmin

Managed By
kblogpnt.com/Microsoft Exchange Security Groups/Organization Managem
kblogpnt.com/LOGPOINT/KB/User/mxadmin

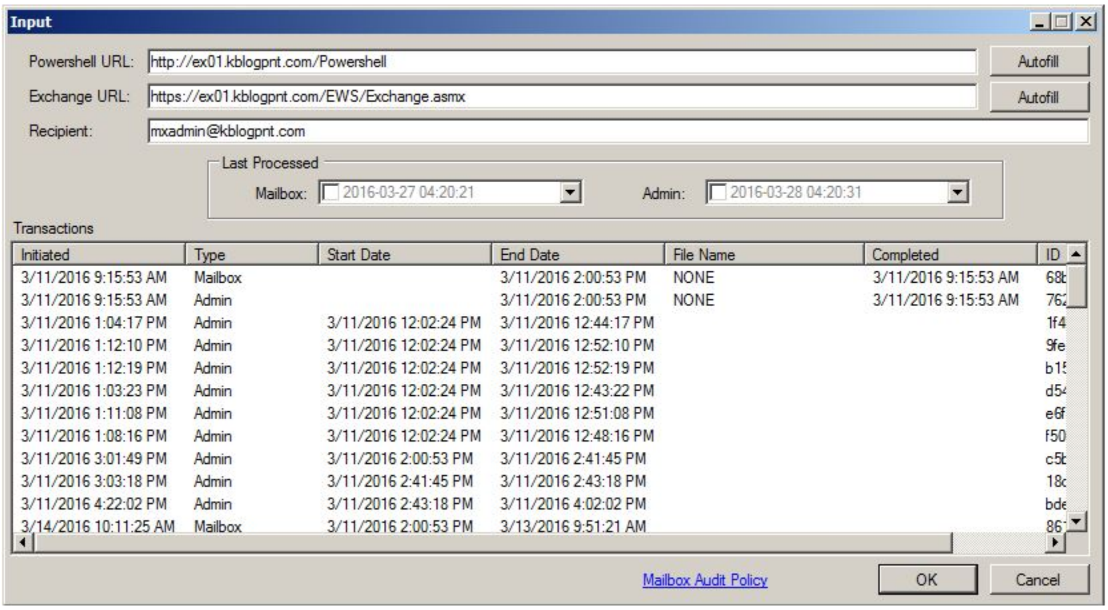
- Install the Following hotfix and restart the server before performing below options. http://hotfixv4.microsoft.com/Windows%207/Windows%20Server2008%20R2%20SP1/sp2/Fix348351/7600/free/425402_intl_x64_zip.exe

Configure as shown below in the table:

| Local Security Policy (secpol.msc) settings summary | | | | Windows Server 2003 | Windows Server 2008/2012 | |
|---|---|---|---|---|---|---|
| Security Settings | Local Policies | User Rights Assignment | *Log on as a service* | add service account | add service account | **This always needs to be set** |
| | | | *Generate security audits* | add service account | add service account | **These need to be set if outputting to Windows Security log** |
| | | Audit Policy | *Audit object access* | set Success | N/A | |
| | | Security Options | *Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings* | N/A | set Enabled | |
| | Advanced Audit Policy Configuration | Object Access | *Audit Application Generated* | N/A | set Success | |

After configuration of prerequisite, follow the below steps to complete installation and configuration of LogBinderEX:

Click on the New Input and Click on the Autofill Button, which will automatically configure Powershell URL, Exchange URL, manually insert recipient email address hence mail will sent every time log search is executed.



Powershell URL: http://ex01.kblogpnt.com/Powershell

Exchange URL: https://ex01.kblogpnt.com/EWS/Exchange.asmx

Recipient: mxadmin@kblogpnt.com

Last Processed

Mailbox: □ 2016-03-27 04:20:21

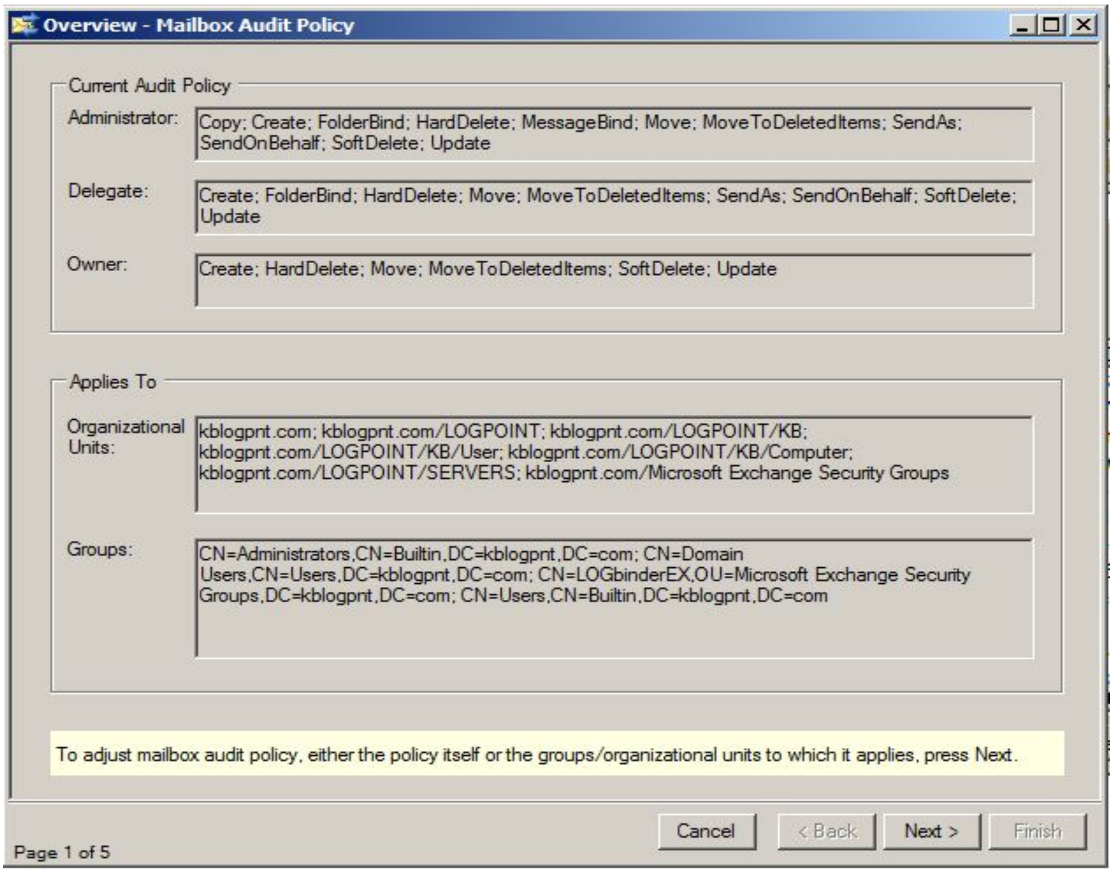
Admin: □ 2016-03-28 04:20:31

Transactions

| Initiated | Type | Start Date | End Date | File Name | Completed | ID |
|---|---|---|---|---|---|---|
| 3/11/2016 9:15:53 AM | Mailbox | | 3/11/2016 2:00:53 PM | NONE | 3/11/2016 9:15:53 AM | 68 |
| 3/11/2016 9:15:53 AM | Admin | | 3/11/2016 2:00:53 PM | NONE | 3/11/2016 9:15:53 AM | 76 |
| 3/11/2016 1:04:17 PM | Admin | 3/11/2016 12:02:24 PM | 3/11/2016 12:44:17 PM | | | 1f4 |
| 3/11/2016 1:12:10 PM | Admin | 3/11/2016 12:02:24 PM | 3/11/2016 12:52:10 PM | | | 9fe |
| 3/11/2016 1:12:19 PM | Admin | 3/11/2016 12:02:24 PM | 3/11/2016 12:52:19 PM | | | b1 |
| 3/11/2016 1:03:23 PM | Admin | 3/11/2016 12:02:24 PM | 3/11/2016 12:43:22 PM | | | d5 |
| 3/11/2016 1:11:08 PM | Admin | 3/11/2016 12:02:24 PM | 3/11/2016 12:51:08 PM | | | e6f |
| 3/11/2016 1:08:16 PM | Admin | 3/11/2016 12:02:24 PM | 3/11/2016 12:48:16 PM | | | f50 |
| 3/11/2016 3:01:49 PM | Admin | 3/11/2016 2:00:53 PM | 3/11/2016 2:41:45 PM | | | c5 |
| 3/11/2016 3:03:18 PM | Admin | 3/11/2016 2:41:45 PM | 3/11/2016 2:43:18 PM | | | 18 |
| 3/11/2016 4:22:02 PM | Admin | 3/11/2016 2:43:18 PM | 3/11/2016 4:02:02 PM | | | bd |
| 3/14/2016 10:11:25 AM | Mailbox | 3/11/2016 2:00:53 PM | 3/13/2016 9:51:21 AM | | | 86 |

Mailbox Audit Policy

Click on the Mailbox Audit Policy to configure log regarding Mailbox logging.



Current Audit Policy

Administrator: Copy; Create; FolderBind; HardDelete; MessageBind; Move; MoveToDeletedItems; SendAs; SendOnBehalf; SoftDelete; Update

Delegate: Create; FolderBind; HardDelete; Move; MoveToDeletedItems; SendAs; SendOnBehalf; SoftDelete; Update

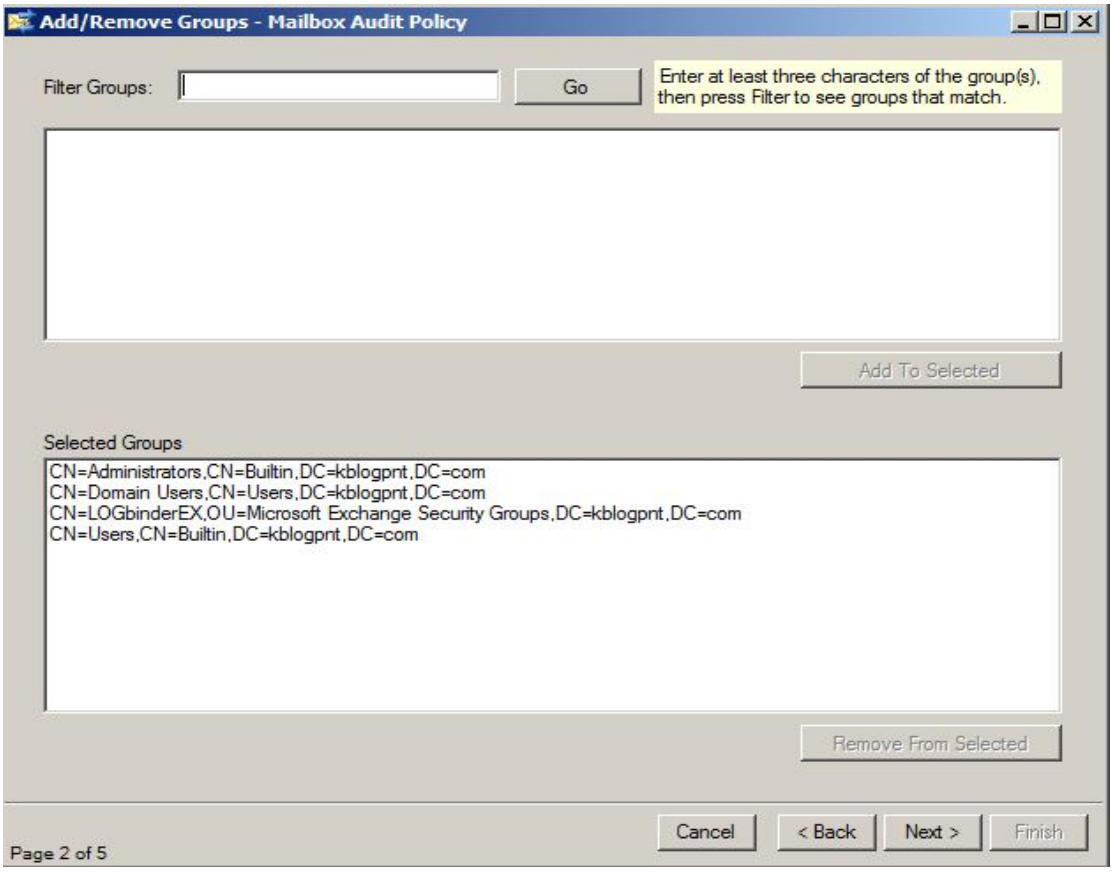
Owner: Create; HardDelete; Move; MoveToDeletedItems; SoftDelete; Update

Applies To

Organizational Units: kblogpnt.com; kblogpnt.com/LOGPOINT; kblogpnt.com/LOGPOINT/KB; kblogpnt.com/LOGPOINT/KB/User; kblogpnt.com/LOGPOINT/KB/Computer; kblogpnt.com/LOGPOINT/SERVERS; kblogpnt.com/Microsoft Exchange Security Groups

Groups: CN=Administrators,CN=Builtin,DC=kblogpnt,DC=com; CN=Domain Users,CN=Users,DC=kblogpnt,DC=com; CN=LOGbinderEX,OU=Microsoft Exchange Security Groups,DC=kblogpnt,DC=com; CN=Users,CN=Builtin,DC=kblogpnt,DC=com

To adjust mailbox audit policy, either the policy itself or the groups/organizational units to which it applies, press Next.



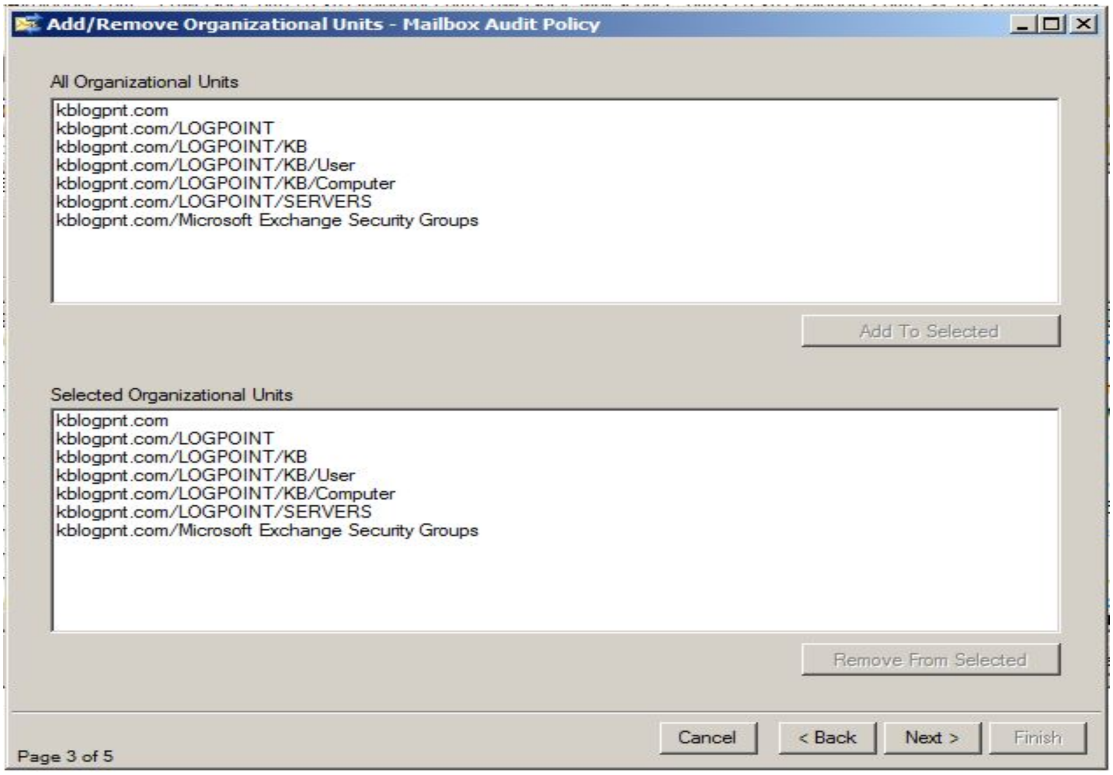
Add/Remove Groups - Mailbox Audit Policy

Enter at least three characters of the group(s), then press Filter to see groups that match.

Selected Groups

```
CN=Administrators,CN=Builtin,DC=kblogpnt,DC=com
CN=Domain Users,CN=Users,DC=kblogpnt,DC=com
CN=LOGbinderEX,OU=Microsoft Exchange Security Groups,DC=kblogpnt,DC=com
CN=Users,CN=Builtin,DC=kblogpnt,DC=com
```

Page 2 of 5



Add/Remove Organizational Units - Mailbox Audit Policy

All Organizational Units

```
kblogpnt.com
kblogpnt.com/LOGPOINT
kblogpnt.com/LOGPOINT/KB
kblogpnt.com/LOGPOINT/KB/User
kblogpnt.com/LOGPOINT/KB/Computer
kblogpnt.com/LOGPOINT/SERVERS
kblogpnt.com/Microsoft Exchange Security Groups
```

Selected Organizational Units

```
kblogpnt.com
kblogpnt.com/LOGPOINT
kblogpnt.com/LOGPOINT/KB
kblogpnt.com/LOGPOINT/KB/User
kblogpnt.com/LOGPOINT/KB/Computer
kblogpnt.com/LOGPOINT/SERVERS
kblogpnt.com/Microsoft Exchange Security Groups
```

Page 3 of 5

## Sample log

```
371 <13>1 2014-04-09T12:48:59+01:00 Z40467.logpoint.com MSWinEventLog
1 Application 66138 Wed - - - Apr 09 12:48:58 2014 1016
      MSExchangeIS Mailbox Store    N/A   N/A   Success Audit
      Z40467.lp.com     Logons      Windows User NT AUTHORITY\SYSTEM
logged on to SystemMailbox{e0dc1c29-89c3-4034-b678-
e6c29d823ed9}@pokharelprabhat.com.np mailbox, and is not the primary
Windows account on this mailbox. 72552
```

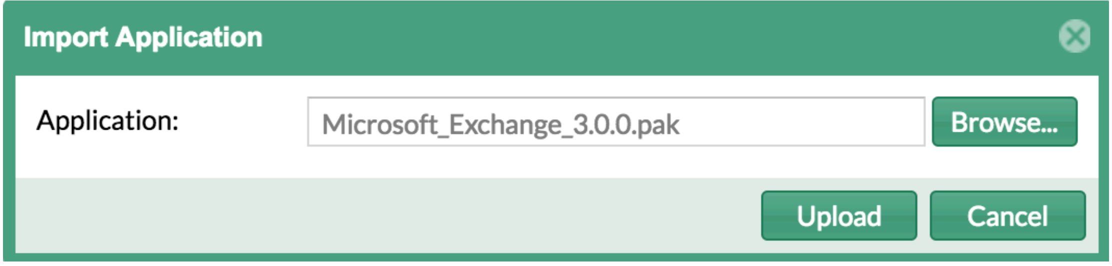
## Configuration in LogPoint

Now login to the LogPoint installation and run through the following steps to finalize.

### Importing Application

To import the application follow the following steps:

1. Go to Settings >> System >> Application.
2. Click Import.
3. Choose the relevant application and click upload.



Import Application

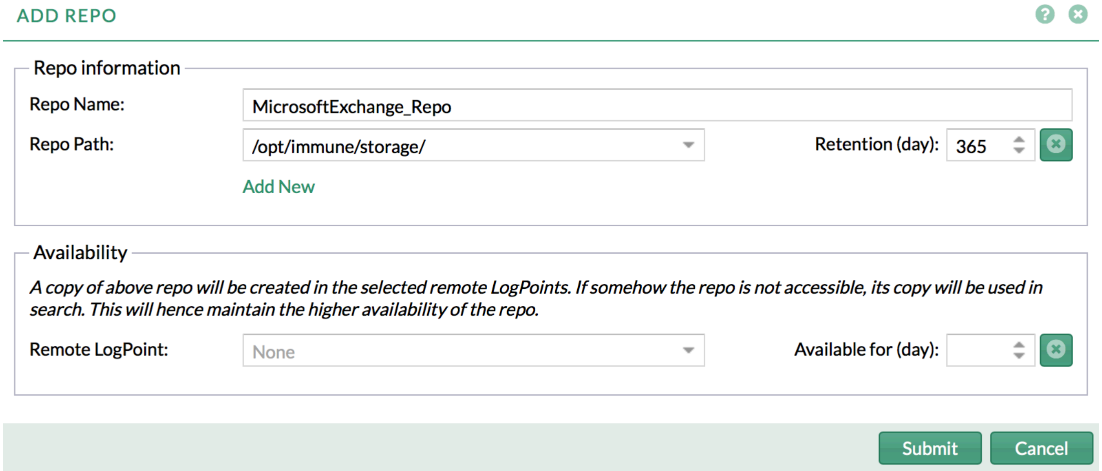
Application: Microsoft_Exchange_3.0.0.pak

### Adding Repos

To add repos, follow the following steps:

1. Go to Settings >> Configuration >> Repos.

2. Click **Add Repo**. A pop-up window appears for Repo Information and Availability.



ADD REPO

Repo information

Repo Name: MicrosoftExchange_Repo

Repo Path: /opt/immune/storage/

Retention (day): 365

Availability

*A copy of above repo will be created in the selected remote LogPoints. If somehow the repo is not accessible, its copy will be used in search. This will hence maintain the higher availability of the repo.*

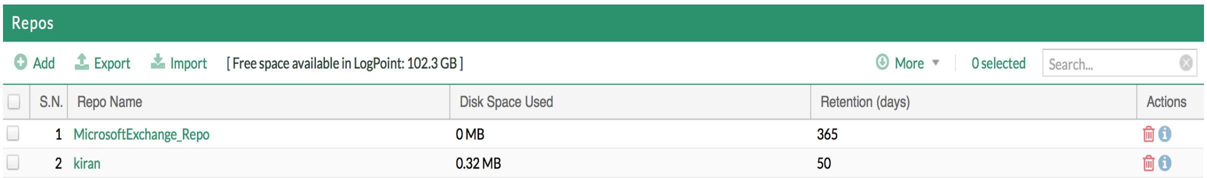
Remote LogPoint: None

Available for (day):

3. In the Repo Information section, provide a **Repo Name**. (The length of the Repo Name should not exceed 29 characters). Select a **Repo Path** and the preferred **Retention (day)** period.
4. Click Add New to add multiple storage locations for your repo.

5. Under the Availability section, select a **Remote LogPoint** and set up a time period for **Available for (day).**
6. Click **Submit**.

Once after a repo has been added, it will be populated in the Repos feed along with its repo name, disk space used and retention days like given below:



[ Free space available in LogPoint: 102.3 GB ]

| □ | S.N. | Repo Name | Disk Space Used | Retention (days) | Actions |
|---|---|---|---|---|---|
| □ | 1 | MicrosoftExchange_Repo | 0 MB | 365 | 🗑 ℹ |
| □ | 2 | kiran | 0.32 MB | 50 | 🗑 ℹ |

The number of days displayed under the **Retention (days)** column is the cumulative days of all the retention days associated with the different **Repo Path** for a repo.

## Configure Normalization Policy

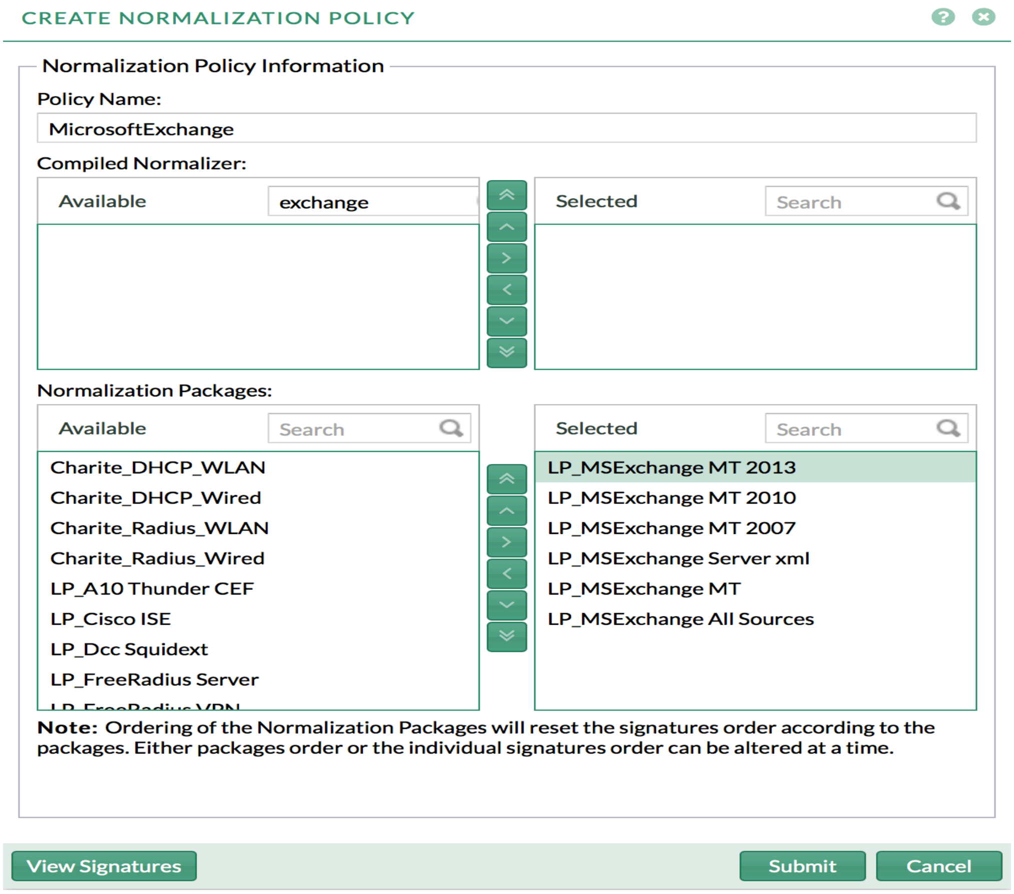
To configure the normalization policy, follow the following steps:

1. Go to Settings >> Configuration >> Normalization Policies.

2. Click **Add**.

3. Provide a **Policy Name**.

4. Drag and drop the available **Normalization Packages** and **Compiled Normalizer** to the right-side window pane. The selected normalization packages can now be reordered according to the requirement.



CREATE NORMALIZATION POLICY

Normalization Policy Information

Policy Name: MicrosoftExchange

Compiled Normalizer:

| Available: exchange | Selected: Search |
|---|---|

Normalization Packages:

| Available | Selected |
|---|---|
| Charite_DHCP_WLAN | LP_MSExchange MT 2013 |
| Charite_DHCP_Wired | LP_MSExchange MT 2010 |
| Charite_Radius_WLAN | LP_MSExchange MT 2007 |
| Charite_Radius_Wired | LP_MSExchange Server xml |
| LP_A10 Thunder CEF | LP_MSExchange MT |
| LP_Cisco ISE | LP_MSExchange All Sources |
| LP_Dcc Squidext | |
| LP_FreeRadius Server | |

**Note:** Ordering of the Normalization Packages will reset the signatures order according to the packages. Either packages order or the individual signatures order can be altered at a time.

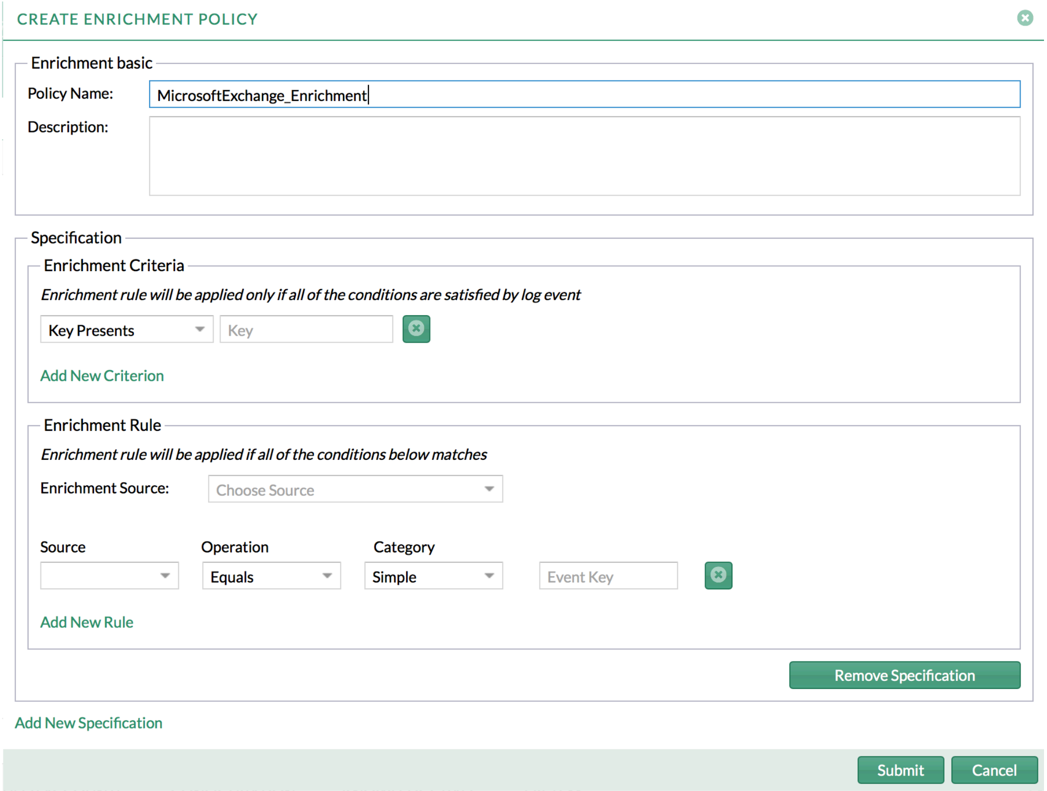
5. Click **View Signatures** to view signatures in the selected packages. You can deactivate signatures from your policy by deselecting them. You can deselect in three ways:

    - Double click the selected signatures
    - Drag and drop in the initial window pane.
    - Press < button from the arrow buttons.

6. Click **Submit**.

**Configure Enrichment Policy**

1. Go to Settings >> Configuration >> Enrichment Policies.
2. Click **Add**.



CREATE ENRICHMENT POLICY

Enrichment basic

Policy Name: MicrosoftExchange_Enrichment

Description:

Specification

Enrichment Criteria

*Enrichment rule will be applied only if all of the conditions are satisfied by log event*

Key Presents | Key

Enrichment Rule

*Enrichment rule will be applied if all of the conditions below matches*

Enrichment Source: Choose Source

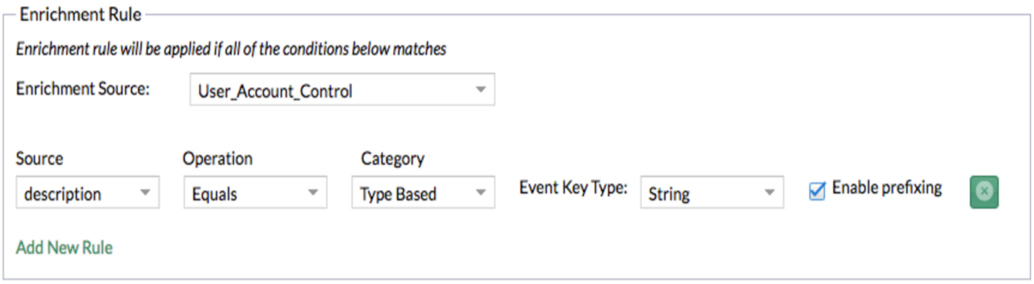
Source | Operation: Equals | Category: Simple | Event Key

3. Under Enrichment basic section, provide **Policy Name** and **Description**.
4. Under Specification section, provide **Enrichment Criteria** and **Enrichment Rule**.
5. Provide the key value after selecting the Enrichment Criterion from the dropdown menu. The key entered must be present in the log event, and the value of the key in the log event must match the value or Regular Expression specified.

**Note:** Clicking Add New Criterion will generate a new dropdown menu for Enrichment Criteria options.

6. Select the Enrichment Source from the dropdown menu. The information to be filled will be followed as per the selected Enrichment Source.

- Choose a Source from the dropdown menu.
- The type of Operation will be set to **Equals** by default.
- Choose a Category from the dropdown menu.
- If you select Simple, provide the Event Key suitable with the Source.
- If you select Type Based, choose an Event Key Type from the dropdown menu. In this case, all the fields of the selected type are eligible to be taken into consideration.



Enrichment Rule

*Enrichment rule will be applied if all of the conditions below matches*

Enrichment Source: User_Account_Control

| Source | Operation | Category | Event Key Type: | |
|---|---|---|---|---|
| description | Equals | Type Based | String | ☑ Enable prefixing |

- Select the checkbox Enable prefixing, if you want the results to be prefixed with the event key. Unselect the checkbox if you want to obtain a particular result. In such case, LogPoint will perform the lexicographic operation, where the result will be presented in alphabetical order of the event key.

Note: Clicking Add New Rule will generate a new dropdown menu for Enrichment Rule options.

7. Click Submit.

**Note**: If you have a distributed LogPoint setup you cannot administer the Enrichment Policies of the remote LogPoints from the **Distributed LogPoint** dropdown menu on the **Header Bar** inside the Settings menu.

**Warning**: Using enriched field as an Enrichment Criteria for Type based enrichment is now allowed if the enrichment has been performed once previously. For example, if the field **source_address** is an enriched field, then the user is not allowed to use that field as an enrichment criteria value.

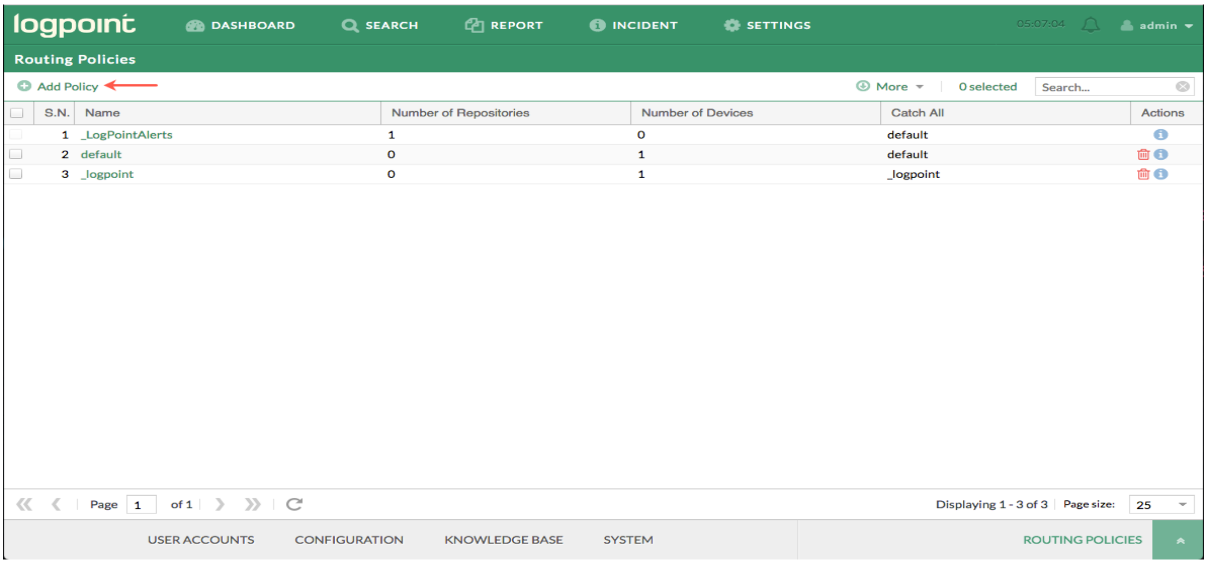
### Configure Routing policy

Routing Policy allows the users to selectively determine what incoming data gets forwarded to a particular repository and what gets dropped. Routing is performed on the basis of "key-value-match" or "key-present" criteria.

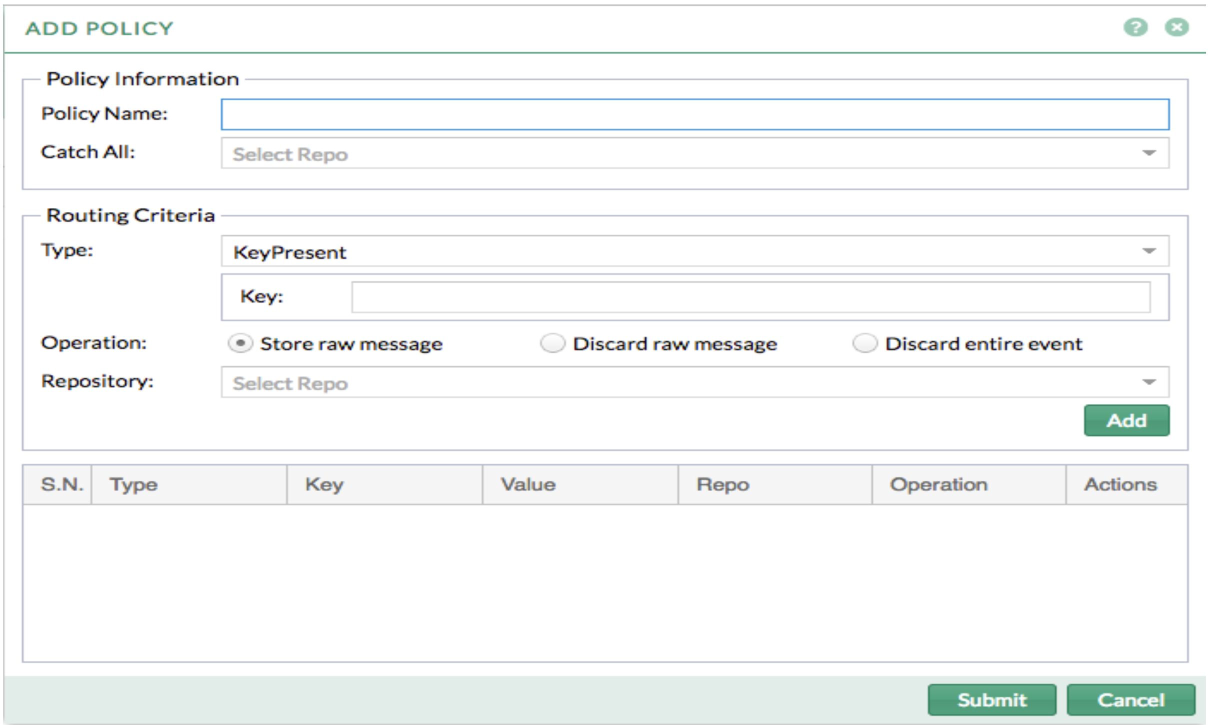
Steps to configure Routing Policy:

1. Go to Settings >> Configuration >> Routing Policies.

2. Click **Add Policy**.



| □ | S.N. | Name | Number of Repositories | Number of Devices | Catch All | Actions |
|---|---|---|---|---|---|---|
| □ | 1 | _LogPointAlerts | 1 | 0 | default | ⓘ |
| □ | 2 | default | 0 | 1 | default | 🗑 ⓘ |
| □ | 3 | _logpoint | 0 | 1 | _logpoint | 🗑 ⓘ |



Policy Name:

Catch All: Select Repo

Type: KeyPresent

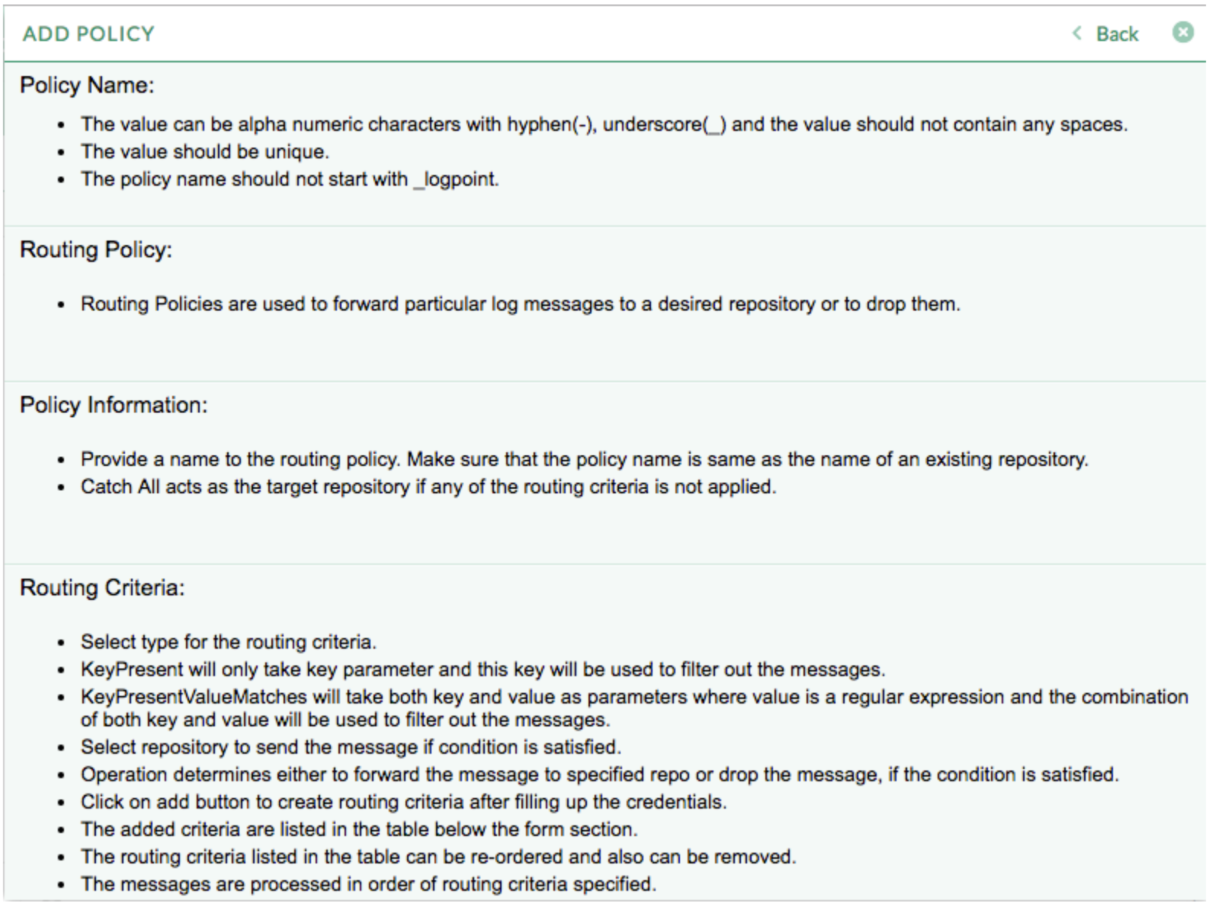
Key:

Operation: ● Store raw message ○ Discard raw message ○ Discard entire event

Repository: Select Repo

| S.N. | Type | Key | Value | Repo | Operation | Actions |
|---|---|---|---|---|---|---|

In the Add Policy panel, click ? to open the help section for routing policy. It lists all the points to be considered while creating a routing policy.



Policy Name:

- The value can be alpha numeric characters with hyphen(-), underscore(_) and the value should not contain any spaces.
- The value should be unique.
- The policy name should not start with _logpoint.

Routing Policy:

- Routing Policies are used to forward particular log messages to a desired repository or to drop them.

Policy Information:

- Provide a name to the routing policy. Make sure that the policy name is same as the name of an existing repository.
- Catch All acts as the target repository if any of the routing criteria is not applied.

Routing Criteria:

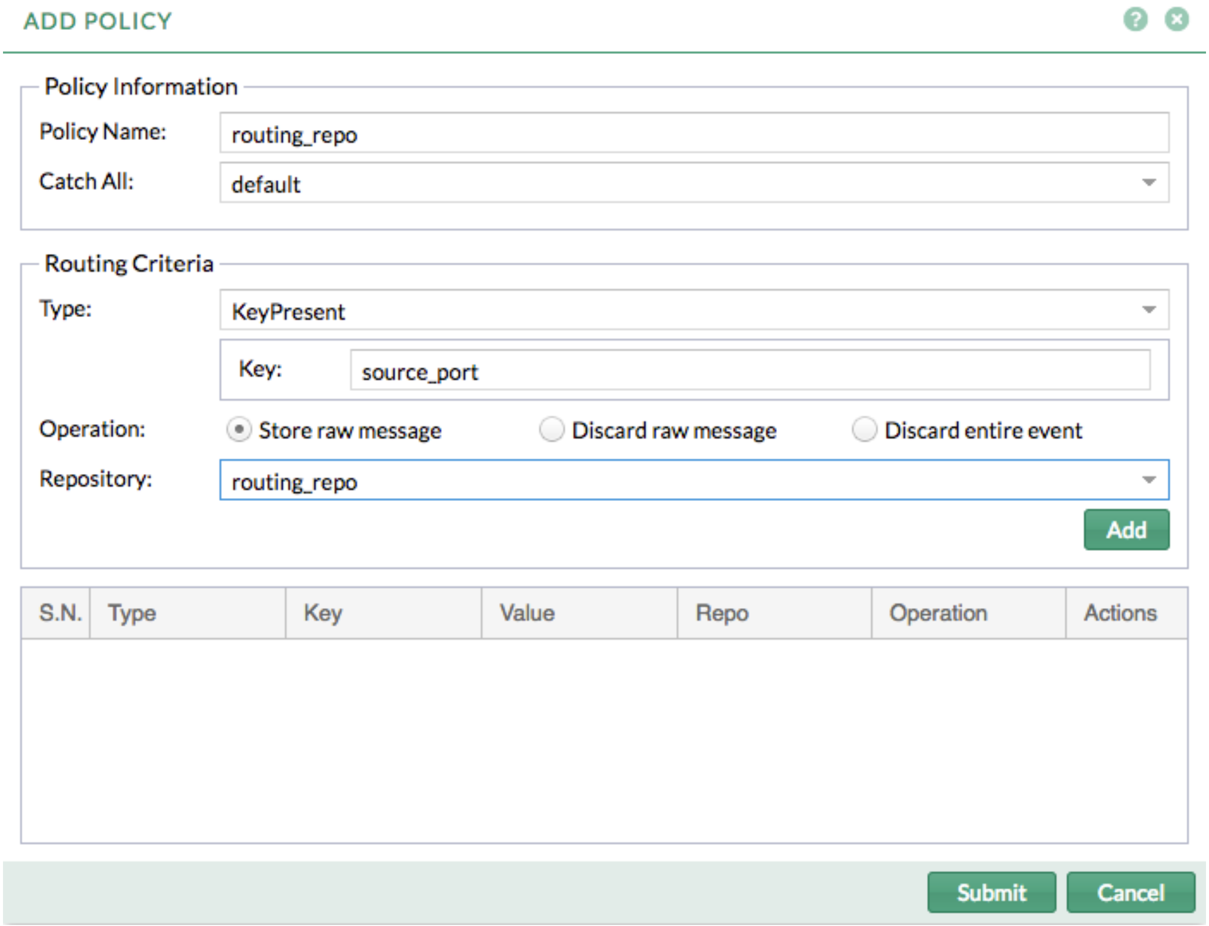
- Select type for the routing criteria.
- KeyPresent will only take key parameter and this key will be used to filter out the messages.
- KeyPresentValueMatches will take both key and value as parameters where value is a regular expression and the combination of both key and value will be used to filter out the messages.
- Select repository to send the message if condition is satisfied.
- Operation determines either to forward the message to specified repo or drop the message, if the condition is satisfied.
- Click on add button to create routing criteria after filling up the credentials.
- The added criteria are listed in the table below the form section.
- The routing criteria listed in the table can be re-ordered and also can be removed.
- The messages are processed in order of routing criteria specified.

- In *Policy Information* section of the panel, provide **Policy Name** for the routing policy.

- In the same section, select a repository from the dropdown menu as **Catch All**. If any *Routing Criteria* does not match with the log messages, Catch All repository will act as the target repository.

5. In *Routing Criteria* section, select a **Type** for the routing criteria. The type may be either “KeyPresent" or “KeyPresentValueMatches".

  - If KeyPresent type is selected, provide a **Key**. The routing criteria will be applied to the log messages containing the provided key.



Policy Information

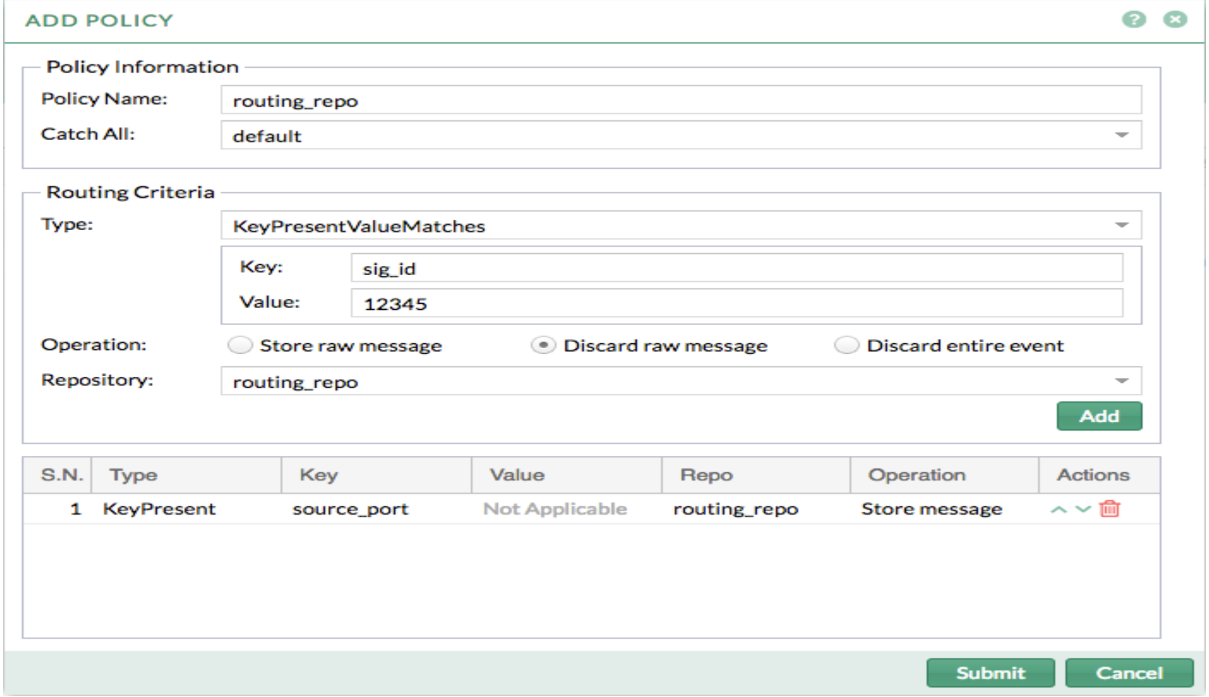
| | |
|---|---|
| Policy Name: | routing_repo |
| Catch All: | default |

Routing Criteria

| | |
|---|---|
| Type: | KeyPresent |
| Key: | source_port |
| Operation: | ● Store raw message ○ Discard raw message ○ Discard entire event |
| Repository: | routing_repo |

| S.N. | Type | Key | Value | Repo | Operation | Actions |
|---|---|---|---|---|---|---|

- If KeyPresentValueMatches is selected, provide a **Key** and its **Value**. The routing criteria will be applied to the log messages confirming the provided Key-Value match.



Policy Information

| | |
|---|---|
| Policy Name: | routing_repo |
| Catch All: | default |

Routing Criteria

| | |
|---|---|
| Type: | KeyPresentValueMatches |
| Key: | sig_id |
| Value: | 12345 |
| Operation: | ○ Store raw message ● Discard raw message ○ Discard entire event |
| Repository: | routing_repo |

| S.N. | Type | Key | Value | Repo | Operation | Actions |
|---|---|---|---|---|---|---|
| 1 | KeyPresent | source_port | Not Applicable | routing_repo | Store message | |

**Note:** The Key for both KeyPresent and KeyPresentValueMatches types must be a normalized field name of the log message.

6. Select the target **Repository** from the dropdown menu for the *Routing Criteria*.

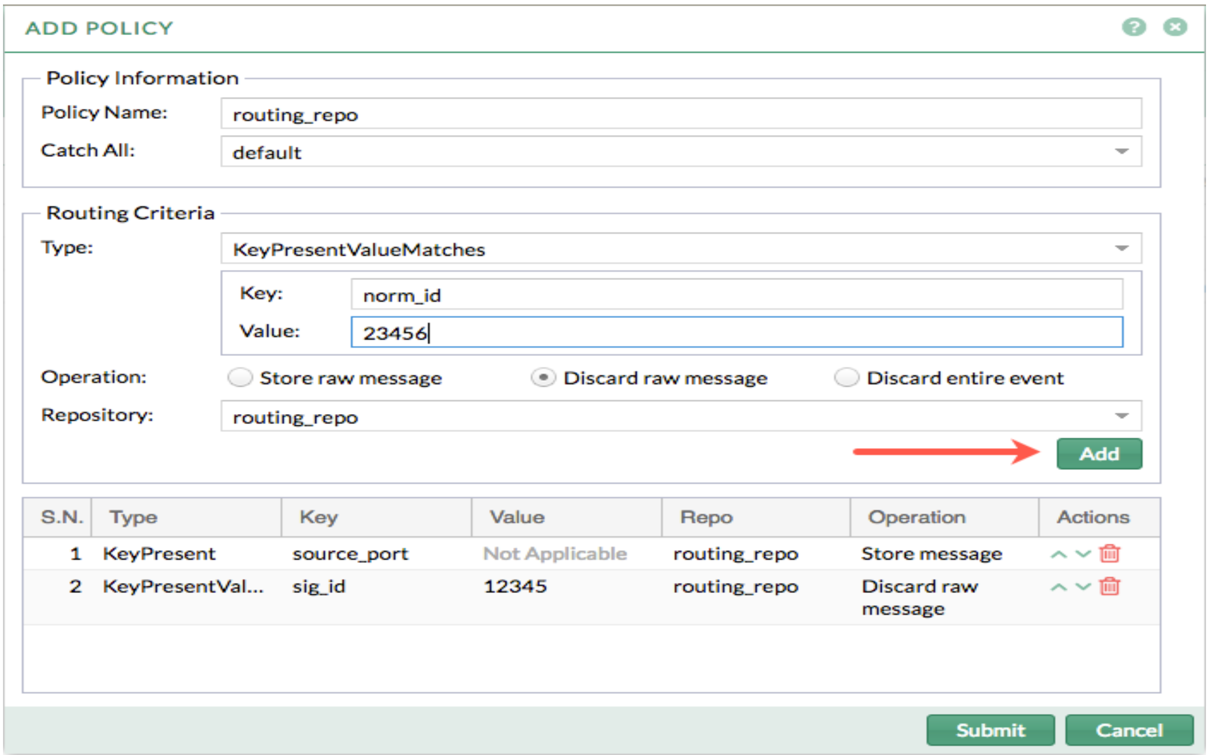
7. Choose an **Operation** to:

   - Store raw message: This will store both the raw message and the normalized data in the target repository.

   - Discard raw message: This will discard raw message and store the normalized data only.

   - Discard entire event: This will discard both raw message and the normalized data.

8. Click **Add**.



ADD POLICY

Policy Information

Policy Name: routing_repo

Catch All: default

Routing Criteria

Type: KeyPresentValueMatches

Key: norm_id

Value: 23456

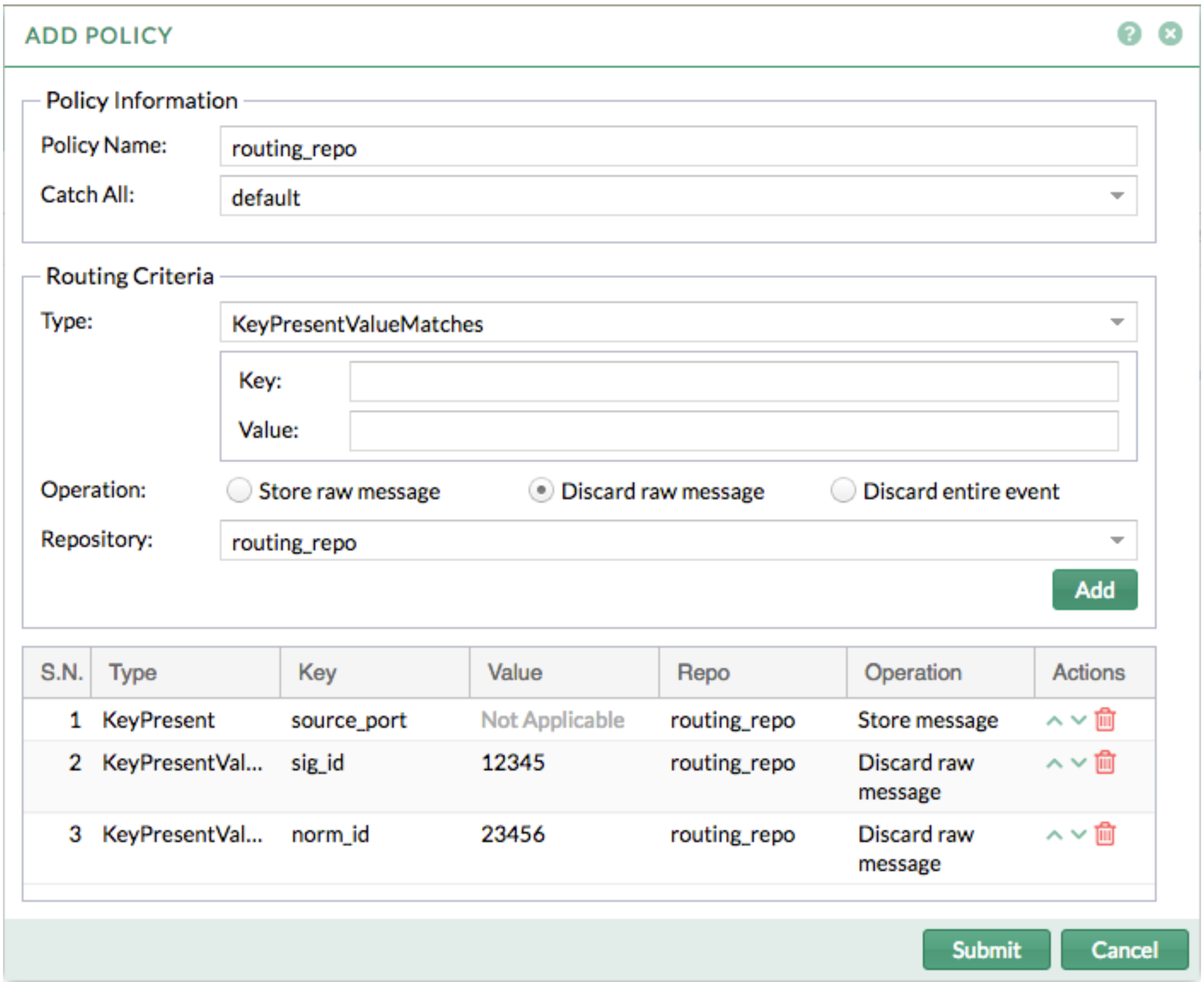
Operation: ○ Store raw message ● Discard raw message ○ Discard entire event

Repository: routing_repo

| S.N. | Type | Key | Value | Repo | Operation | Actions |
|---|---|---|---|---|---|---|
| 1 | KeyPresent | source_port | Not Applicable | routing_repo | Store message | ^ v 🗑 |
| 2 | KeyPresentVal... | sig_id | 12345 | routing_repo | Discard raw message | ^ v 🗑 |

All the added criteria are listed in the table below *Policy Information* section and prioritized according to their *S.N.* with serial number 1 being the highest priority criteria. Priority of routing criteria can be changed by clicking "up arrow" and "down arrow" in *Actions* column of the table.

9. Click **Submit** to save the routing policy, or **Cancel** to abort the process.



ADD POLICY

Policy Information

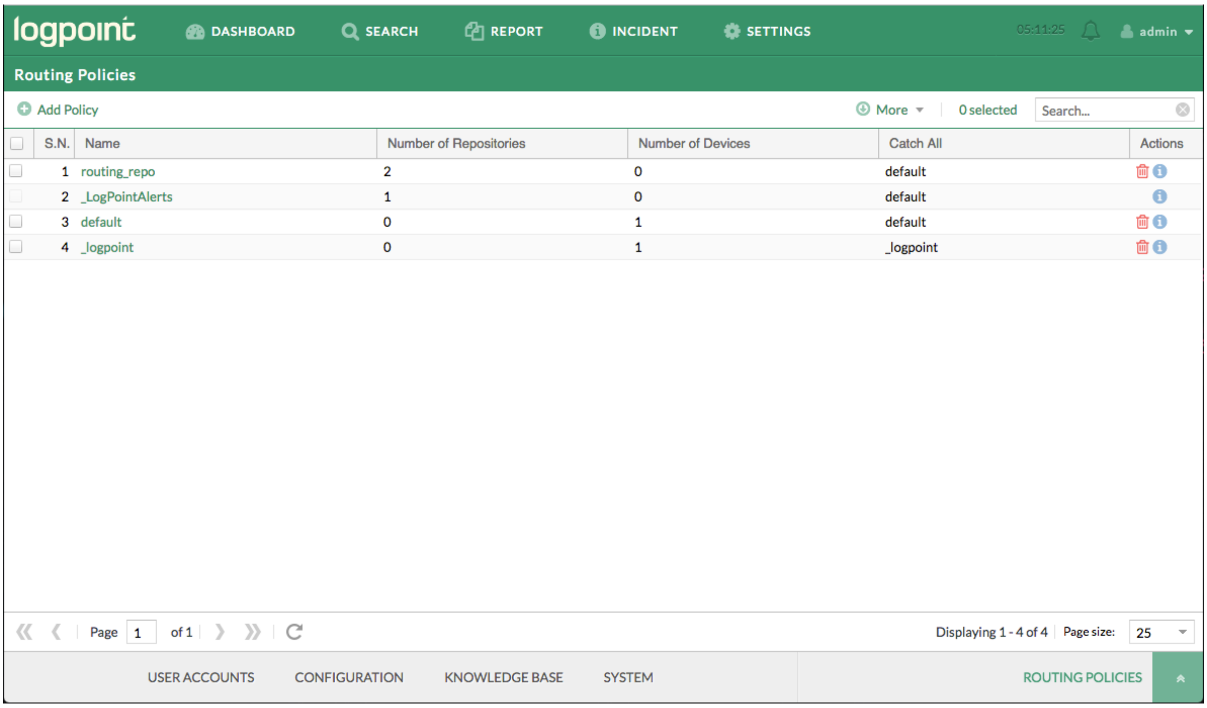
| | |
|---|---|
| Policy Name: | routing_repo |
| Catch All: | default |

Routing Criteria

| | |
|---|---|
| Type: | KeyPresentValueMatches |
| Key: | |
| Value: | |
| Operation: | ○ Store raw message ● Discard raw message ○ Discard entire event |
| Repository: | routing_repo |

| S.N. | Type | Key | Value | Repo | Operation | Actions |
|---|---|---|---|---|---|---|
| 1 | KeyPresent | source_port | Not Applicable | routing_repo | Store message | |
| 2 | KeyPresentVal... | sig_id | 12345 | routing_repo | Discard raw message | |
| 3 | KeyPresentVal... | norm_id | 23456 | routing_repo | Discard raw message | |

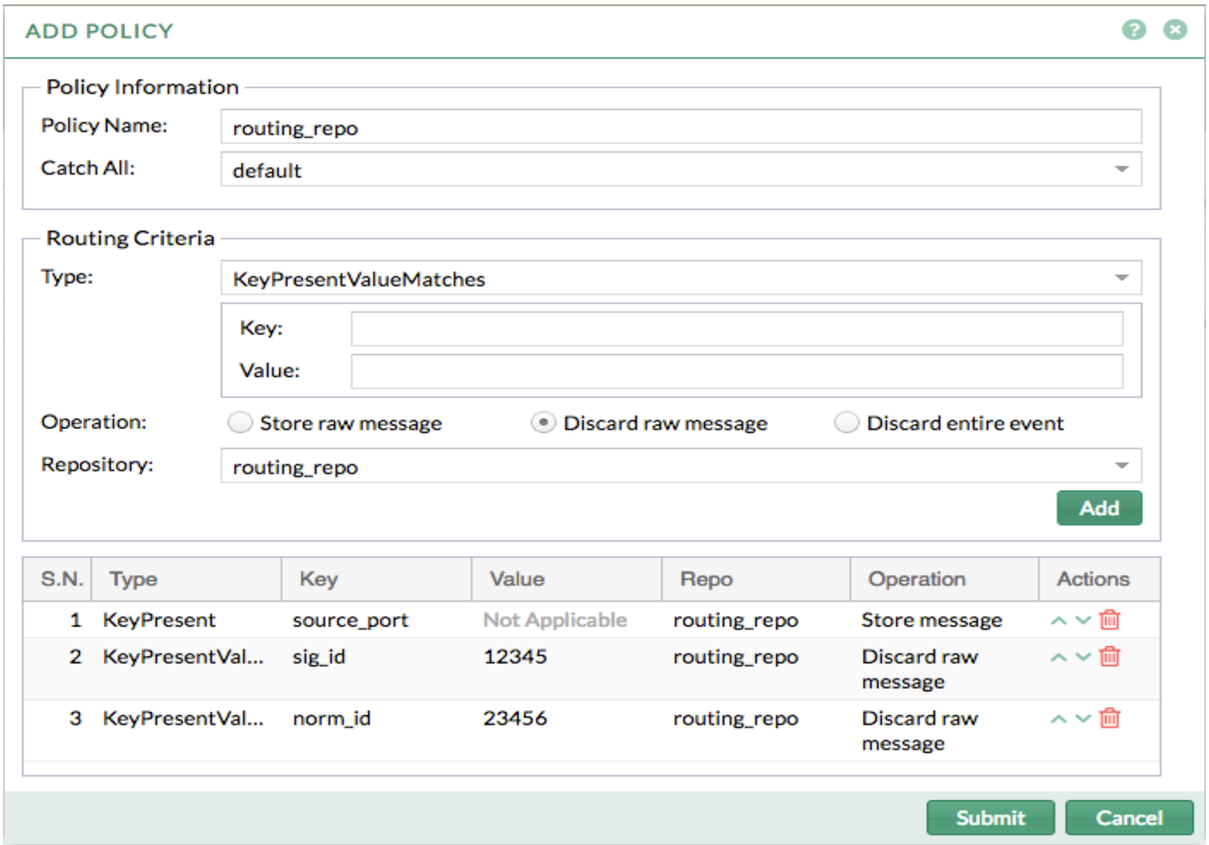
After submitting the policy, users will be redirected to the Routing Policy page where all the routing policies are listed in a table. The table also displays **Number of Repositories** that the policy is using and **Number of Devices** to which the policy is applied.



| □ | S.N. | Name | Number of Repositories | Number of Devices | Catch All | Actions |
|---|---|---|---|---|---|---|
| □ | 1 | routing_repo | 2 | 0 | default | |
| □ | 2 | _LogPointAlerts | 1 | 0 | default | |
| □ | 3 | default | 0 | 1 | default | |
| □ | 4 | _logpoint | 0 | 1 | _logpoint | |

Now, if any of the routing criteria configured in the policy is matched by an incoming log message, it will be either forwarded to the target repository or dropped as per the policy.

For example, let's configure a routing policy as shown in the figure below:



Policy Name: routing_repo

Catch All: default

Type: KeyPresentValueMatches

Key:

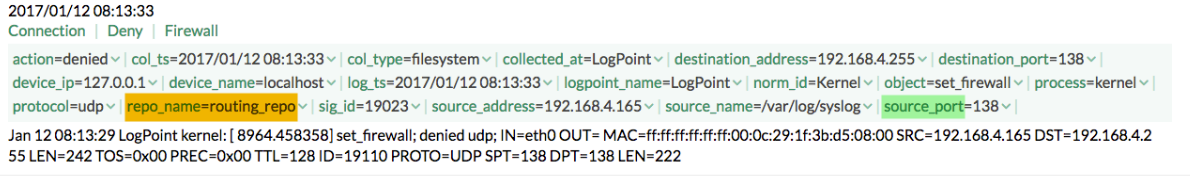
Value:

Operation: ○ Store raw message ● Discard raw message ○ Discard entire event

Repository: routing_repo

| S.N. | Type | Key | Value | Repo | Operation | Actions |
|---|---|---|---|---|---|---|
| 1 | KeyPresent | source_port | Not Applicable | routing_repo | Store message | |
| 2 | KeyPresentVal... | sig_id | 12345 | routing_repo | Discard raw message | |
| 3 | KeyPresentVal... | norm_id | 23456 | routing_repo | Discard raw message | |

So, the following log message which contains a field named **source_port** is forwarded to "routing_repo" repository as configured in the routing policy.



```
2017/01/12 08:13:33
Connection | Deny | Firewall
action=denied | col_ts=2017/01/12 08:13:33 | col_type=filesystem | collected_at=LogPoint | destination_address=192.168.4.255 | destination_port=138 |
device_ip=127.0.0.1 | device_name=localhost | log_ts=2017/01/12 08:13:33 | logpoint_name=LogPoint | norm_id=Kernel | object=set_firewall | process=kernel |
protocol=udp | repo_name=routing_repo | sig_id=19023 | source_address=192.168.4.165 | source_name=/var/log/syslog | source_port=138 |
Jan 12 08:13:29 LogPoint kernel: [ 8964.458358] set_firewall; denied udp; IN=eth0 OUT= MAC=ff:ff:ff:ff:ff:ff:00:0c:29:1f:3b:d5:08:00 SRC=192.168.4.165 DST=192.168.4.2
55 LEN=242 TOS=0x00 PREC=0x00 TTL=128 ID=19110 PROTO=UDP SPT=138 DPT=138 LEN=222
```

- It is not possible to specify routing specifications for the repo "_logpoint".

- "_LogPointAlerts" is the default routing policy bundled with LogPoint. For the log messages whose 'norm_id' field has 'LogPointAlerts' value, the policy routes those log messages to _LogPointAlerts repo. Otherwise, it forwards them to default repo.

### Configure Processing Policy

A **Processing Policy** integrates Normalization Policy, Enrichment Policy, and Routing Policy into a single policy. The main purpose of the Processing Policy is to aid in the data enrichment process.

1. Go to Settings >> Configuration >> Processing Policies.

2. Click **Add**.

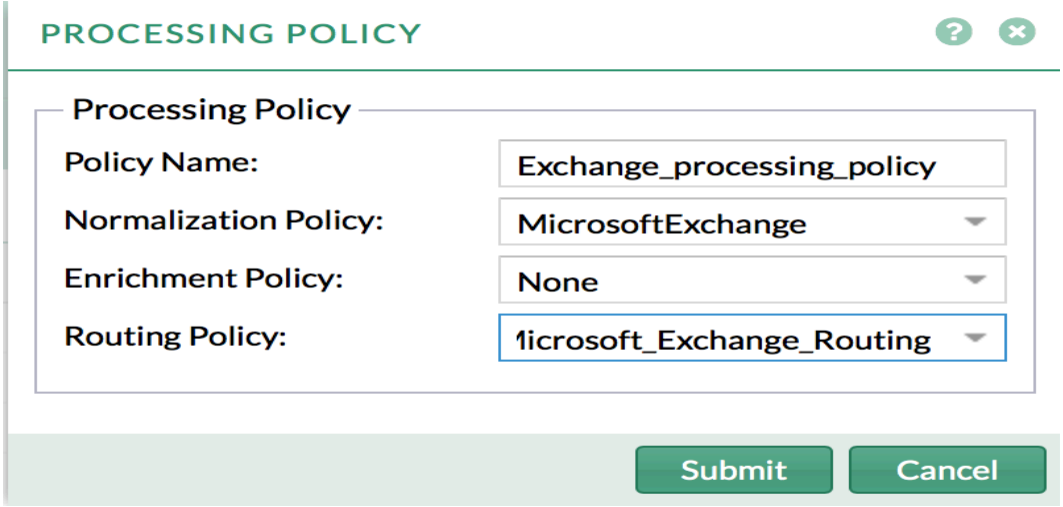
3. Provide **Policy Name**.

4. Select the required **Normalization Policy** from the dropdown menu.

5. Select the required **Enrichment Policy** from the dropdown menu. It is optional to add an **Enrichment Policy**.

6. Select the required **Routing Policy** from the dropdown menu.

7. Click **Submit**.



PROCESSING POLICY

Processing Policy

Policy Name: Exchange_processing_policy

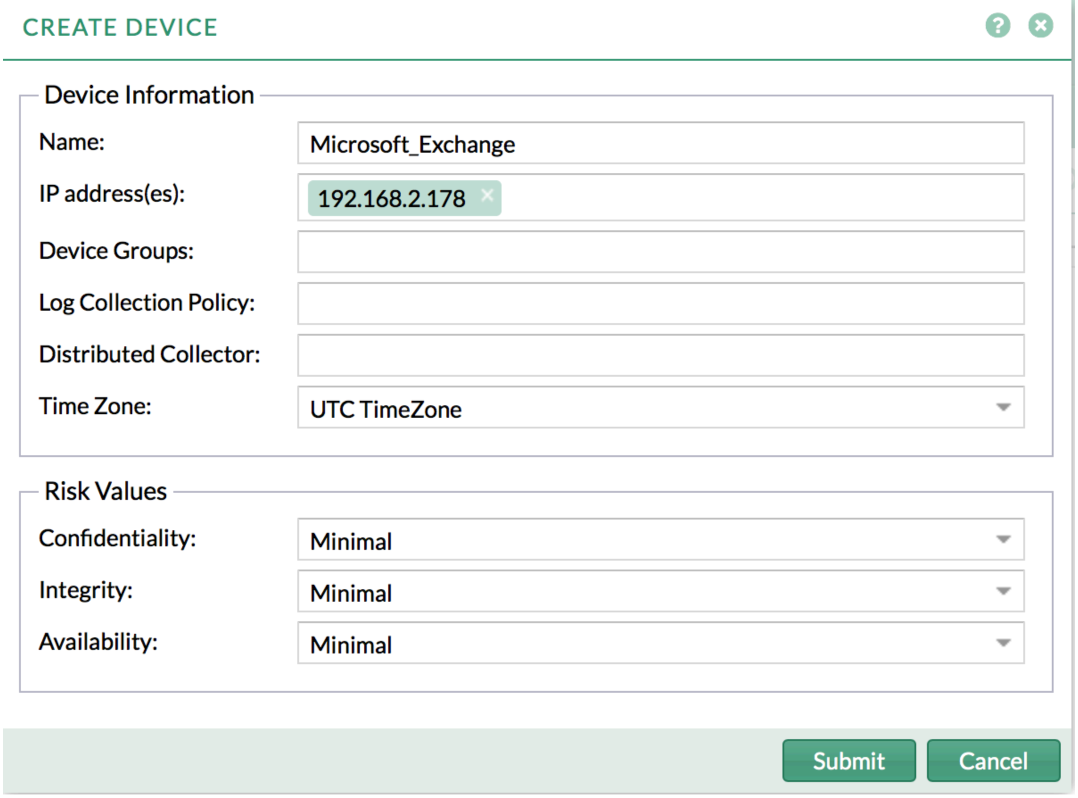
Normalization Policy: MicrosoftExchange

Enrichment Policy: None

Routing Policy: icrosoft_Exchange_Routing

**Configure Device**

1. Start by clicking through “Settings” > “Devices”
2. Click on the “Add” button, to add a new device, and fill out the fields
    a. “Name”: Name of the device
    b. “IP address(es)”: IP address of the device
    c. “Device Groups”: Device groups, that this device should be part of.



CREATE DEVICE

Device Information

Name: Microsoft_Exchange

IP address(es): 192.168.2.178

Device Groups:

Log Collection Policy:

Distributed Collector:

Time Zone: UTC TimeZone

Risk Values

Confidentiality: Minimal

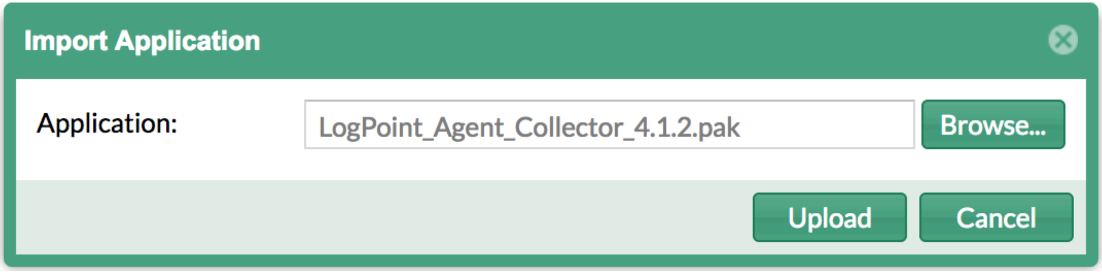
Integrity: Minimal

Availability: Minimal

**Configure LPA Agent Collector:**

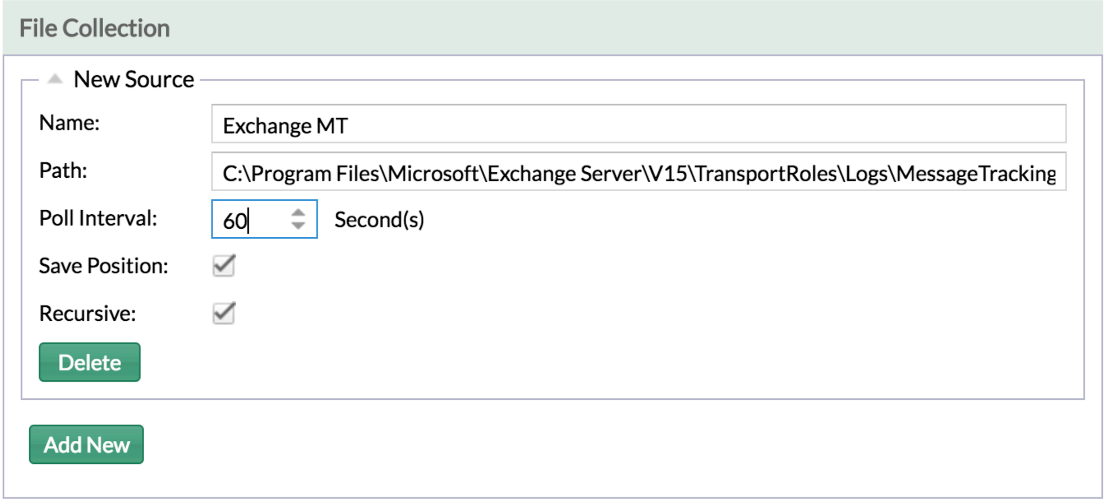
To forward the logs using LogPoint Agent, we need to install and configure LogPoint Agent Collector in LogPoint.

1. Goto “Settings” > “System” > “Applications”  > “Import” and import “LogPoint Agent Collector”



Application: LogPoint_Agent_Collector_4.1.2.pak

2. Goto “Settings” > “System” > “Plugins” > “LogPoint Agent Collector” > “Manage”
3. On Templates, click on Add button
4. Fill the template name and on the section “File Collection” fill in name and path of the source and the poll interval.



Name: Exchange MT

Path: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking

Poll Interval: 60 Second(s)

Save Position: ☑

Recursive: ☑

Now go to “Settings” > “Configuration” > “Devices” and click on the “+” button corresponding to your device. Click on LogPoint Agent Collector and configure it.

logpoint