Integration With Third Party SIEM Solutions

NetIQ® Secure Configuration Manager™

October 2016

Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see http://www.netiq.com/company/legal/.

Copyright © 2016 NetIQ Corporation. All Rights reserved.

For information about NetIQ trademarks, see http://www.netiq.com/company/legal/. All third-party trademarks are the property of their respective owners.

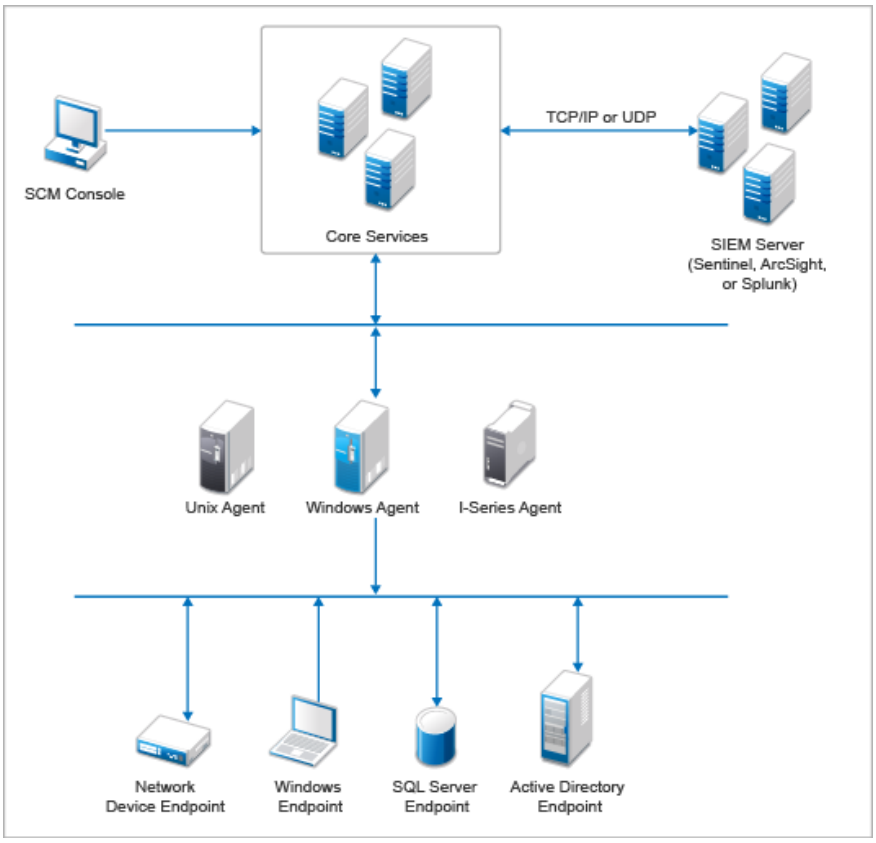
Contents

1. Introduction

NetIQ Secure Configuration Manager helps you to proactively enforce security configuration policy across critical systems in evolving IT environments. It helps in reducing the risk of security breaches, failed audits, or costly downtime. Security Information and Event Management (SIEM) is an approach that provides a holistic view of an organization's Information Technology (IT) security. However, you cannot determine compliance to configuration policy through a SIEM system at present. Determining compliance to configuration policy through SIEM solution will help in recording configuration compliance in line with system activity. It will inform the enterprise administrator about the compliance to configuration in times of anomalous activity.

This white paper describes how Secure Configuration Manager sends configuration compliance information as an event to SIEM solutions, such as Splunk and ArcSight. In this process, Secure Configuration Manager compliance information will be available in Splunk and ArcSight Dashboard for Enterprise administrator reference. Enterprise administrator can generate various reports on configuration compliance, and can also trigger alerts and actions such as sending emails for anomalous activity.

Secure Configuration Manager sends compliance data to the SIEM solution in common event format (CEF), through TCP or UDP connection. You can configure to send compliance data in TCP or UDP connection, based on the configuration of the SIEM solution. The following graphic depicts the overview.

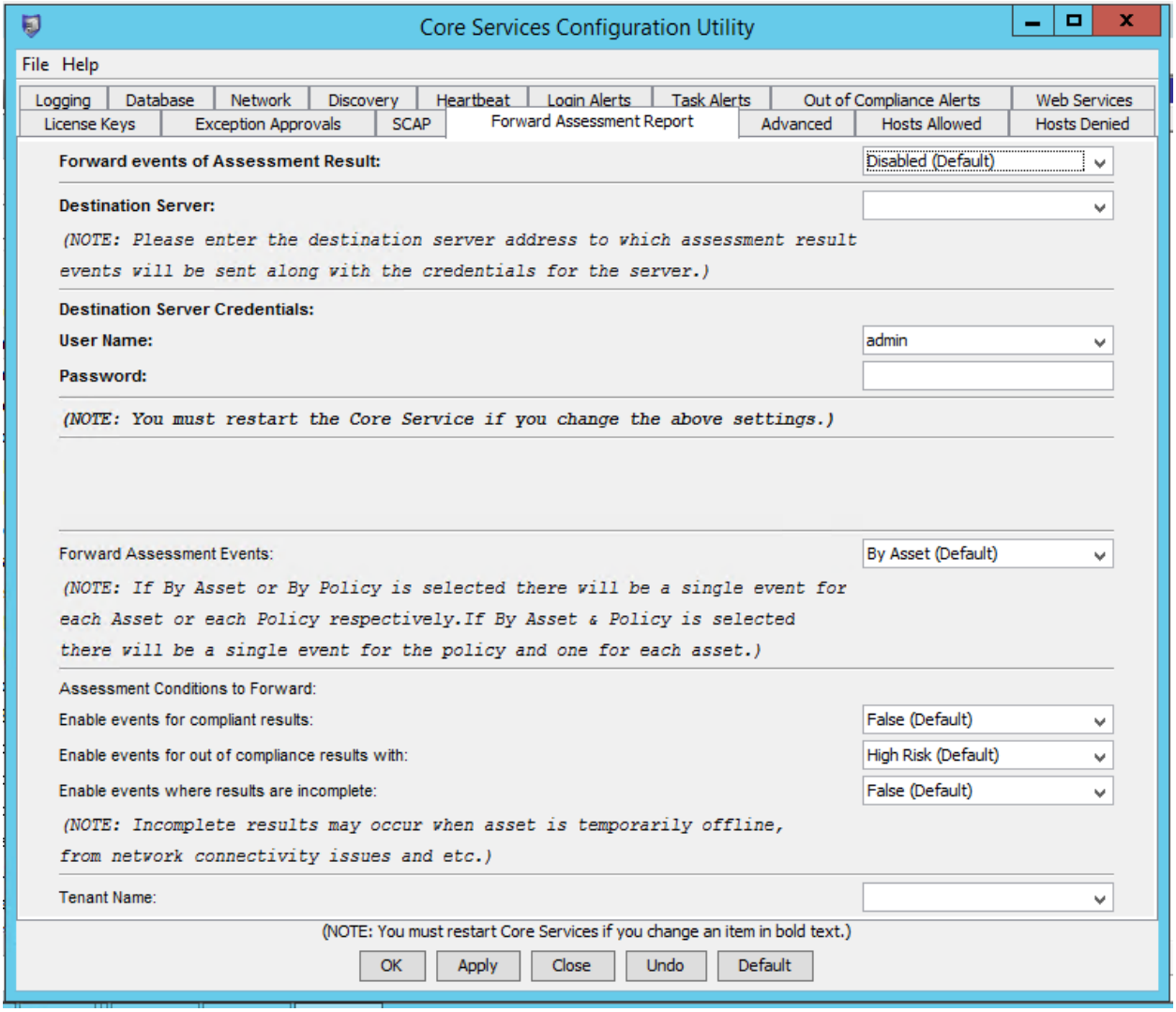


As shown in the above graphic, Secure Configuration Manager Core Services component connects to the data receiver component of the SIEM solution, and sends the compliance data in CEF.

2. Configuring Secure Configuration Manager for the Integration

Perform the following configuration in Secure Configuration Manager to enable it to send compliance data to SIEM solutions:

1. Open Core Services Configuration Utility in your Secure Configuration Manager system and go to the Forward Assessment Report tab.
2. Set the required values in the fields in the Forward Assessment Report tab, or leave them as default values.

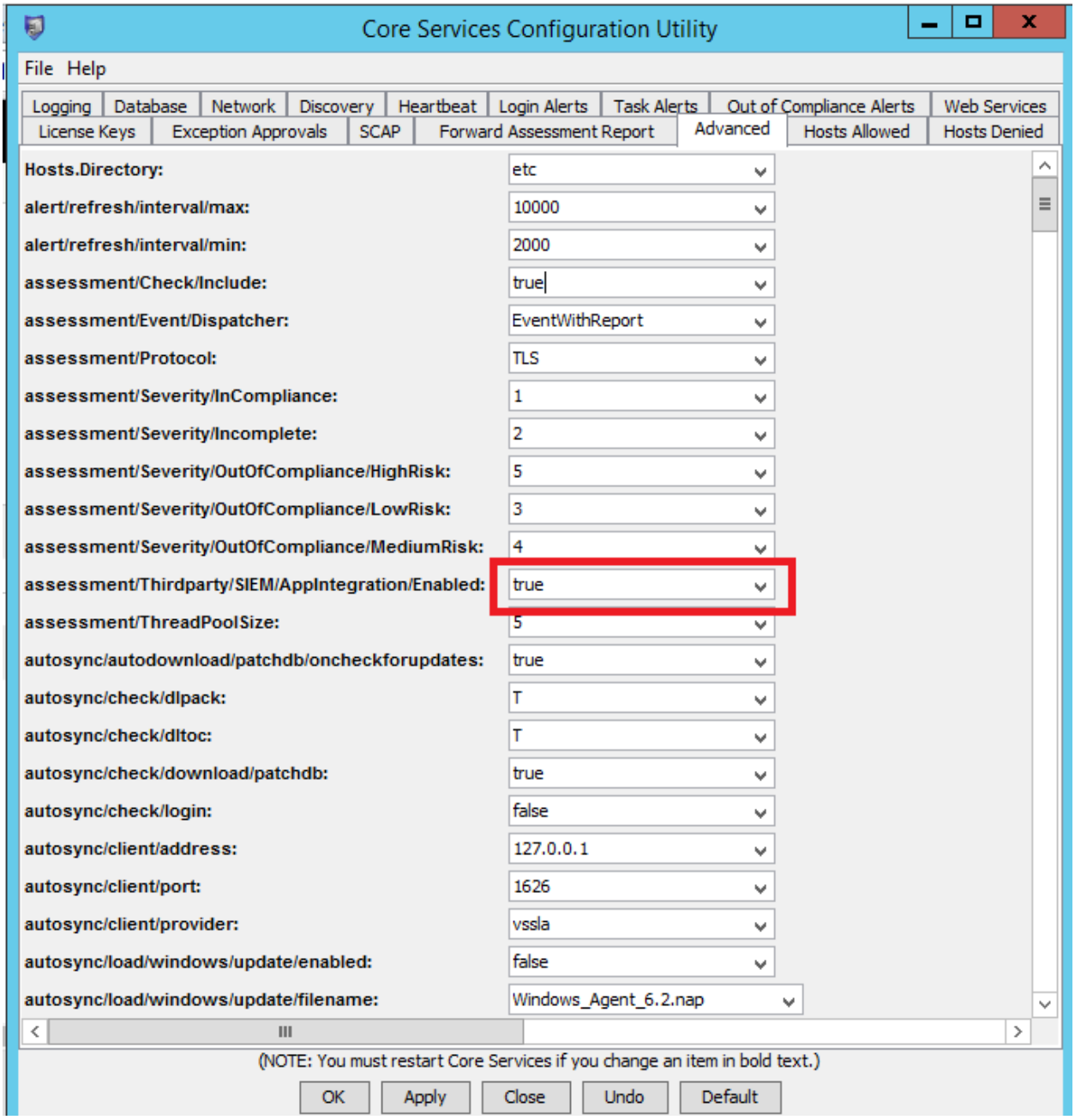


Note: Set the **Forward Assessment Events** field to `By Asset (Default)` to enable Secure Configuration Manager to send reports to the SIEM solutions for policy template runs.

3. Go to the Advanced tab.

   Note: To access the **Advanced** tab in the Core Services Configuration Utility, perform the following steps:
   - Close the Core Services Configuration Utility if it is open.
   - Run the config.bat program in the <Installation Directory>\Core Services\bin folder.
   - Reopen the Core Services Configuration Utility, and you will see the **Advanced** tab.

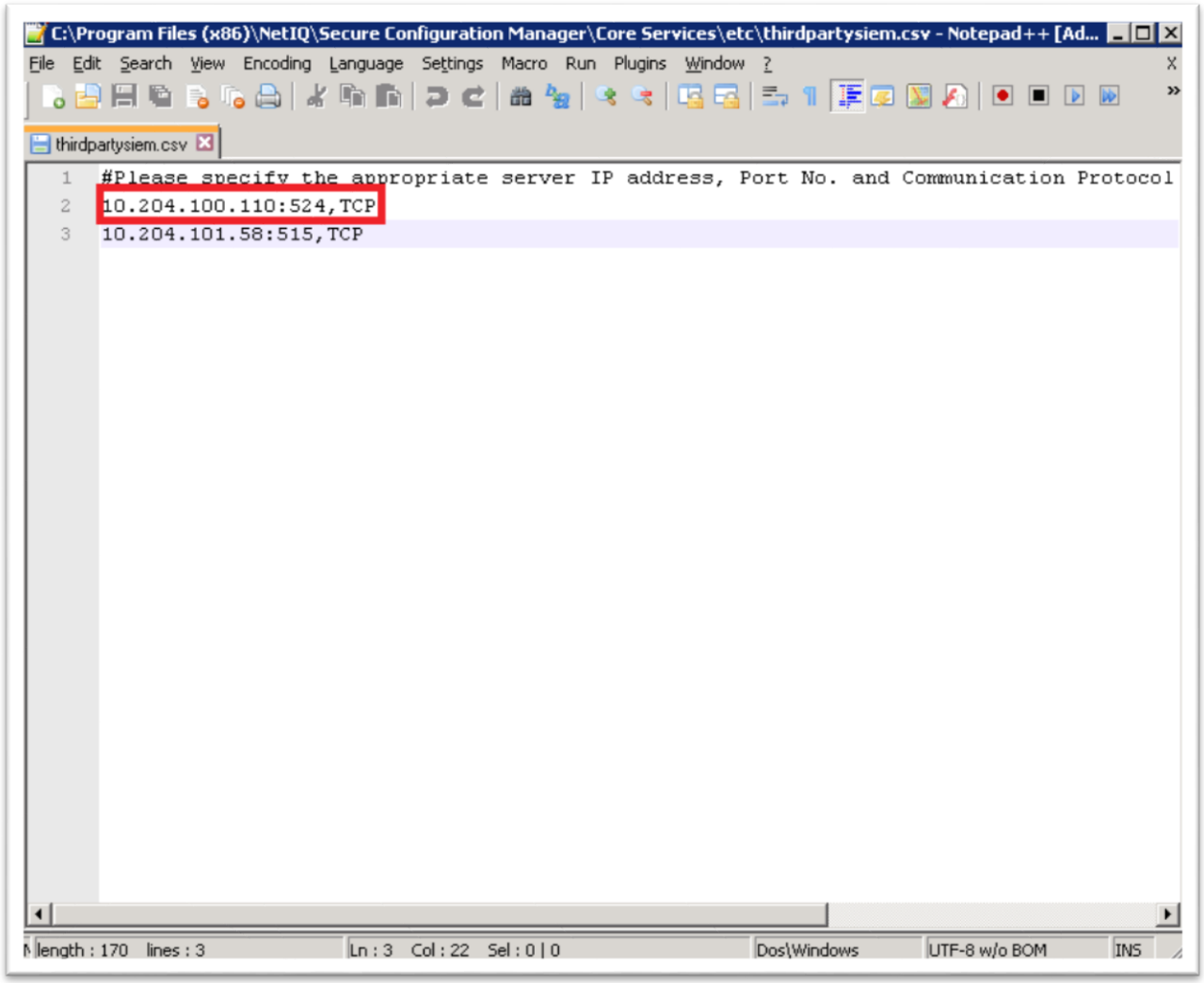
4. In the Advanced tab:
   - **assessment/Thirdparty/SIEM/AppIntegration/Enabled:** Set this field to `true`.
   - **assessment/Check/Include:**
     - Set this field to `true` to send a report to the SIEM solution for each check that is run as part of a template.
     - Set this field to `false` to send a consolidated report to the SIEM solution for each template you run.



5. Configure the SIEM solution server IP address, port, and protocol for sending data:
   a. Open the `\NetIQ\Secure Configuration Manager\Core Services\etc\thirdpartysiem.csv` file.
   b. Update this file with new entries, specifying the server configuration for each SIEM solution that you want to send compliance data. For example:

```
10.204.100.110:524, TCP
```

Where 10.204.100.110 is the IP address of the SIEM solution, 524 is the port number, and TCP is the protocol to be used to send compliance data.



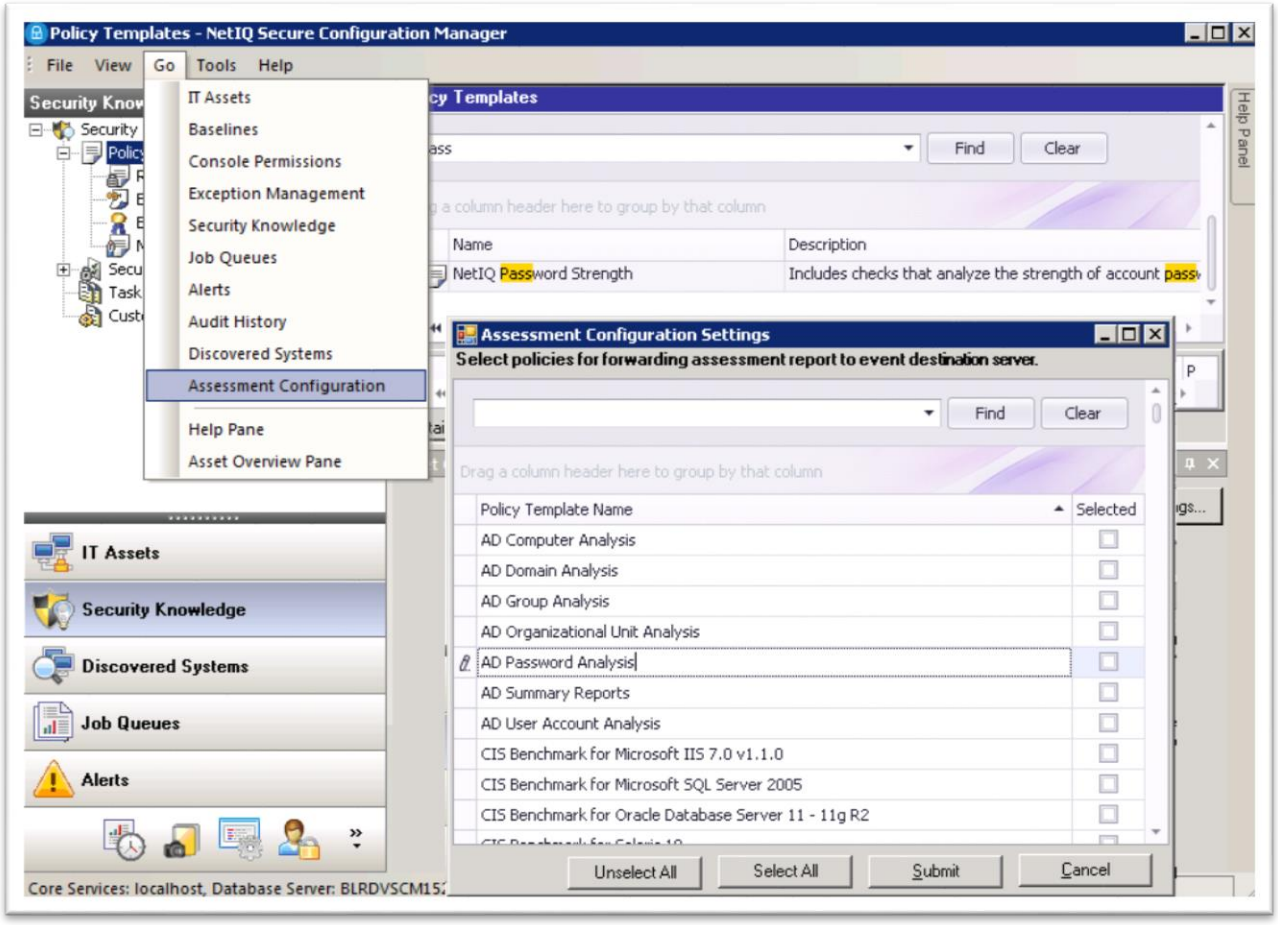
For more information about configuring advanced options, see the *Secure Configuration Manager User Guide*.

3. Sending Events to SIEM Solutions

After you have configured Secure Configuration Manager to send compliance events to SIEM solutions as specified in **Configuring Secure Configuration Manager for the Integration**, you can send the compliance data to SIEM servers as events. You can choose to send events to SIEM servers while running policy templates in the following two ways.

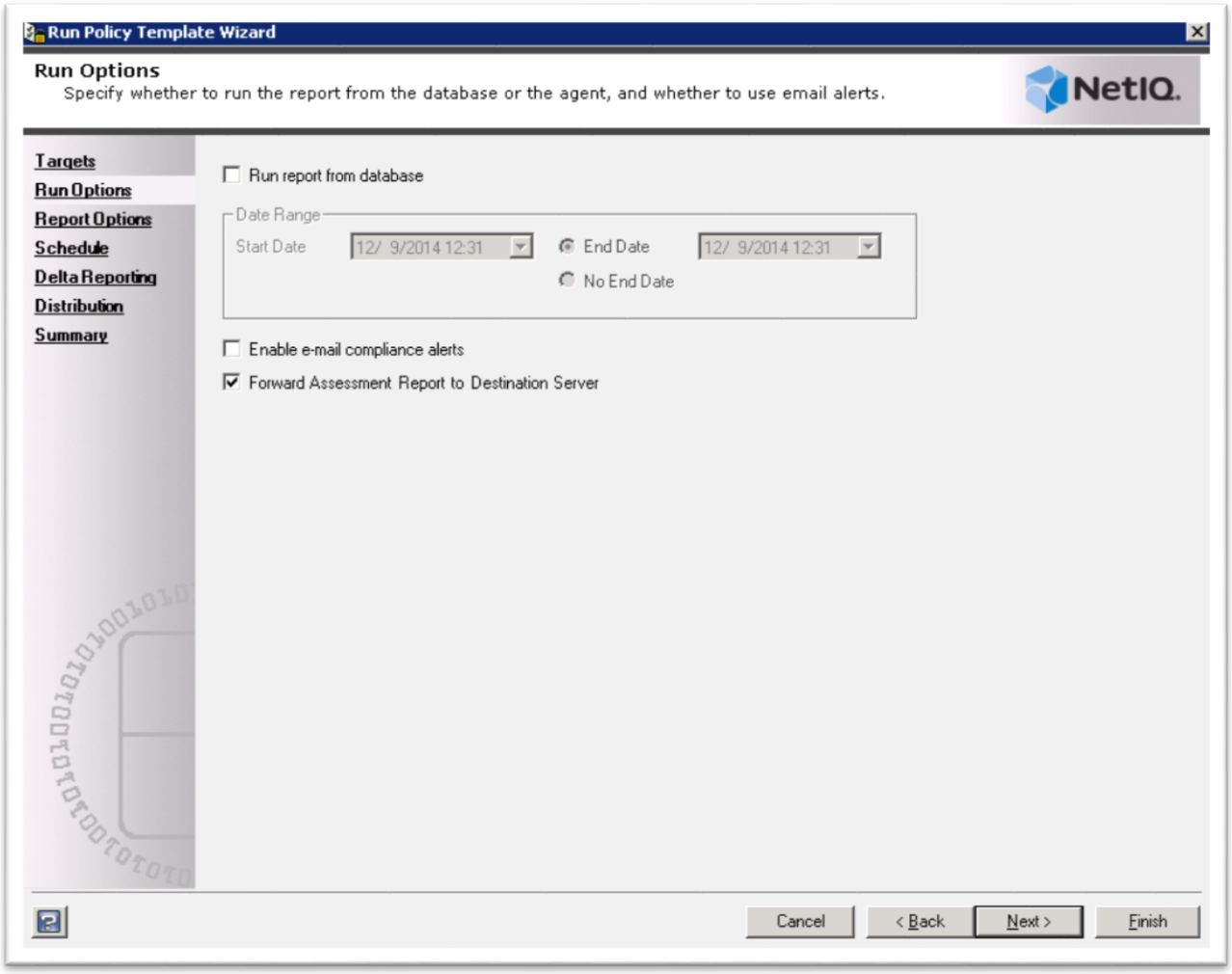
Selecting Policy Templates to Send Events:

In the Secure Configuration Manager Console, click **Go** > **Assessment Configuration**. In the **Assessment Configuration Settings** window, select the policy templates for which events need to be sent to the SIEM server.



Selecting to Send Events While Executing the Policy Template:

When you run a policy template, select the **Forward Assessment Report to Destination Server** option in the **Run Policy Template Wizard** window.


Run Policy Template Wizard
Run Options
Specify whether to run the report from the database or the agent, and whether to use email alerts.
NetIQ.
Targets
Run Options
Report Options
Schedule
Delta Reporting
Distribution
Summary
Run report from database
Date Range
Start Date
12/ 9/2014 12:31
End Date
12/ 9/2014 12:31
No End Date
Enable e-mail compliance alerts
Forward Assessment Report to Destination Server
Cancel
< Back
Next >
Finish

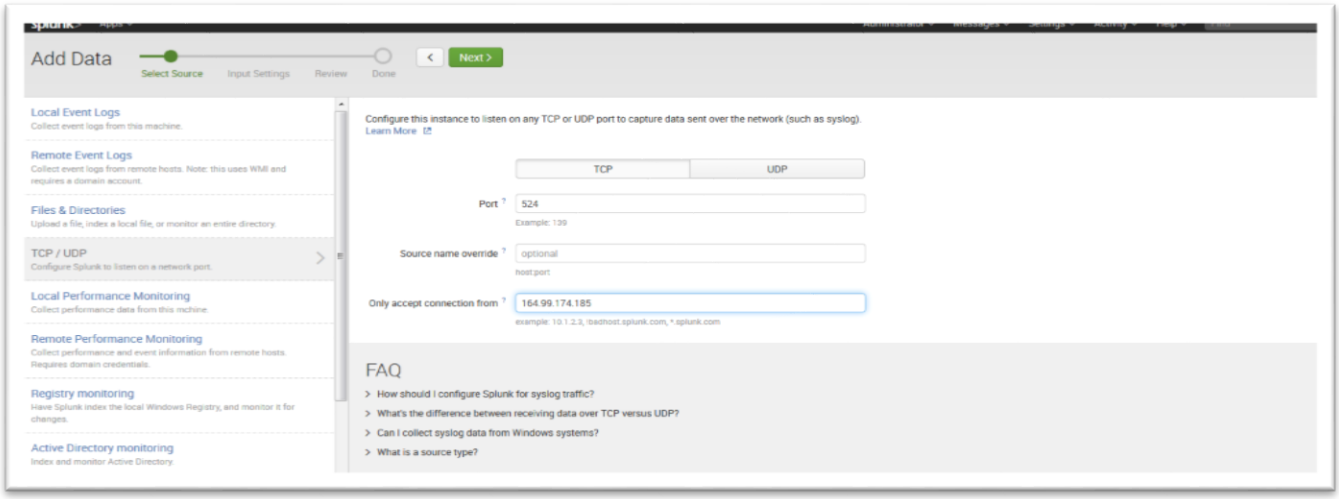
4. Integrating Secure Configuration Manager and Splunk Server

Integration of Secure Configuration Manager and Splunk server enables Secure Configuration Manager Server to send configuration compliance information as events to Splunk SIEM solution.

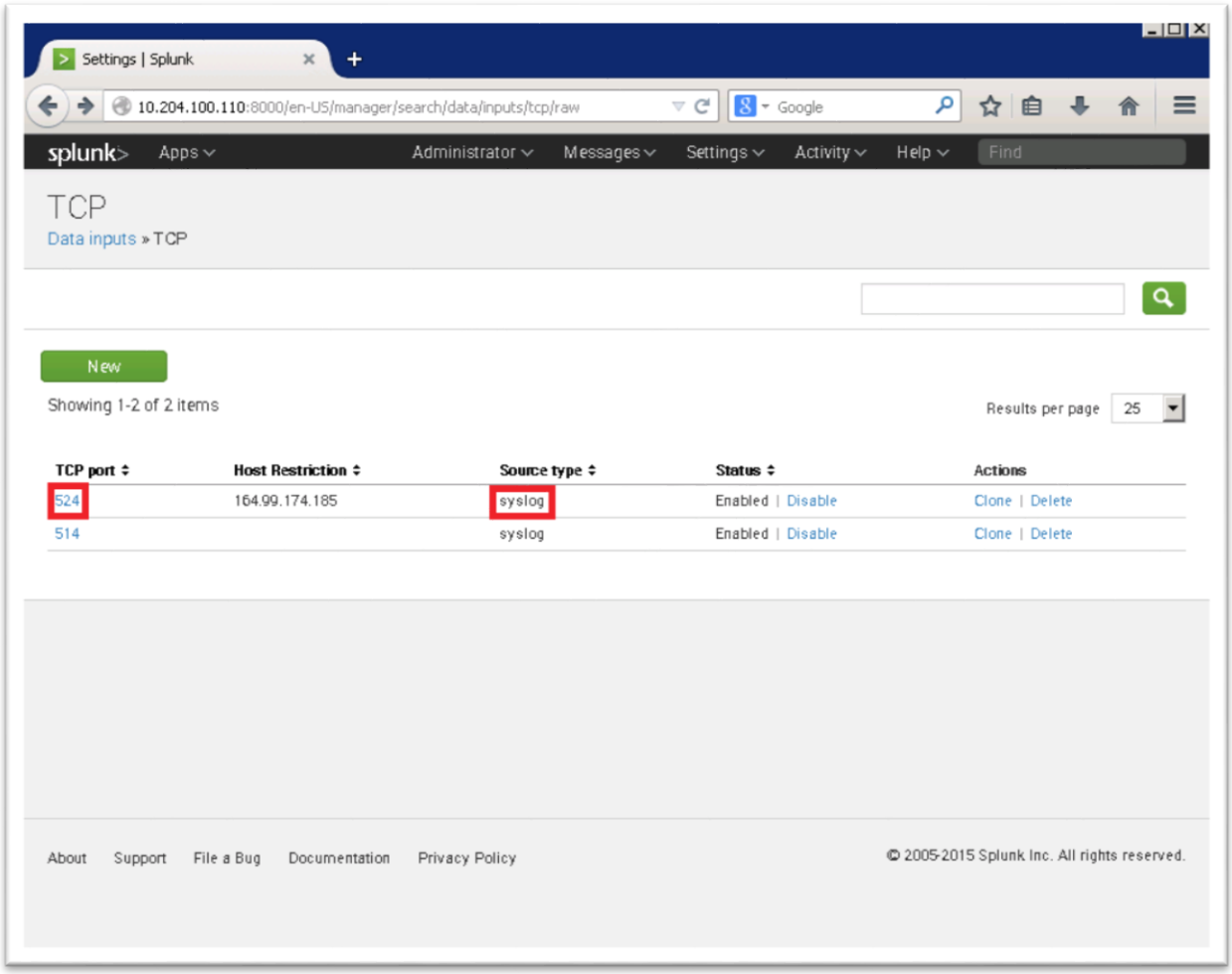
Configuring Splunk

Configure the Splunk Enterprise Server to listen on a network port for incoming data:

1. Configure a TCP/UDP data input listener with syslog source type, as shown in the following figure.



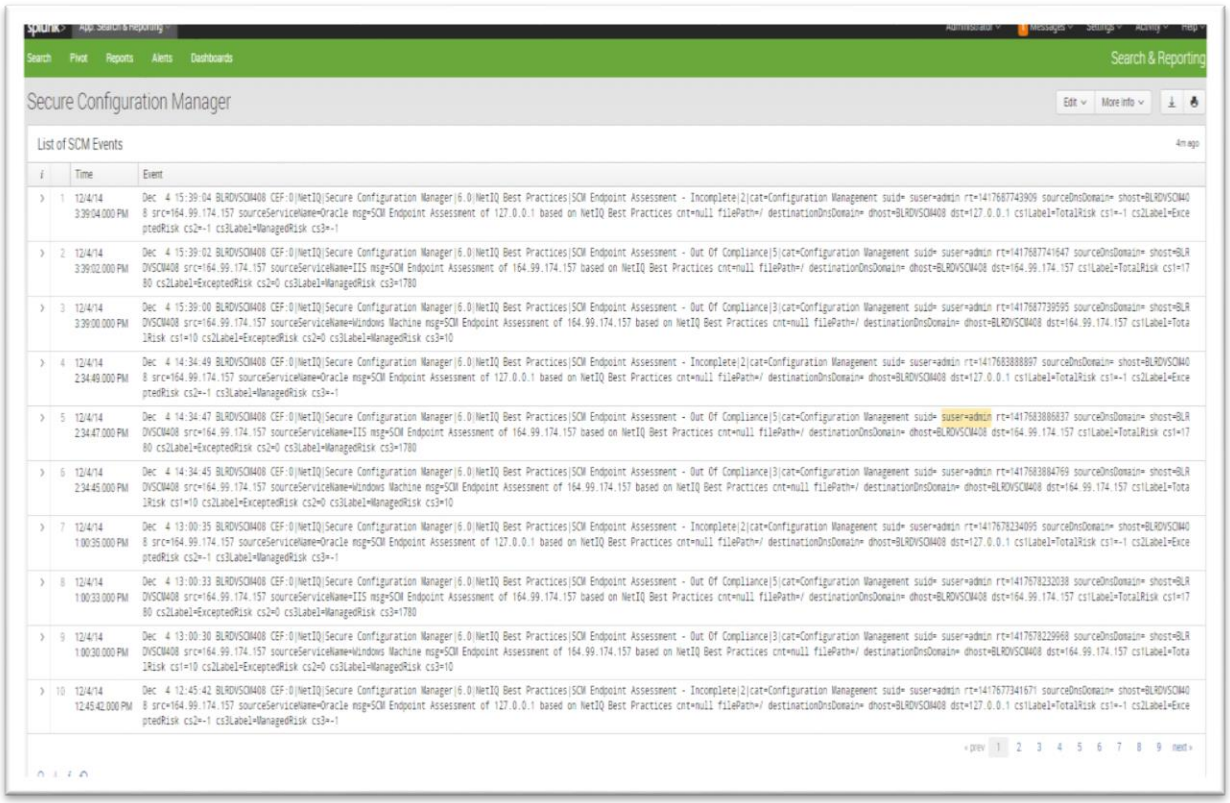
When the data input is configured, it will be added in the **TCP Data inputs** table, as shown in the following figure.



Viewing Raw Secure Configuration Manager Events in Splunk Server

After you configure Splunk to receive events from Secure Configuration Manager, whenever policy templates are executed in Secure Configuration Manager against selected endpoints, you can view the

events in Splunk server search panel.



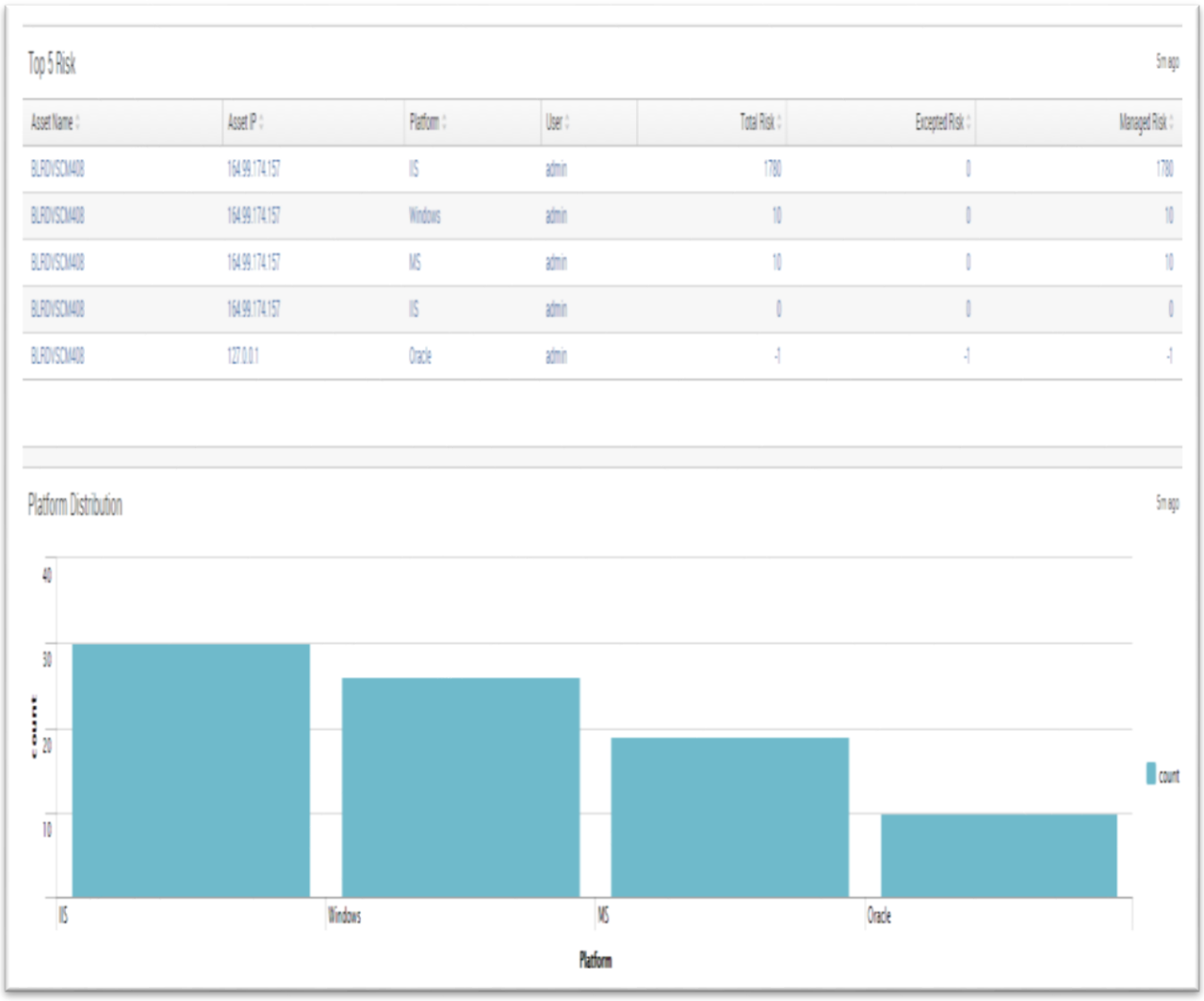
Viewing the Splunk Dashboard

You can generate reports in Splunk Dashboard using the Secure Configuration Manager events data.

For example, you can use the following search string to create a report of top assets by Risk:

```
<searchString>source="164.99.174.185"  | top 5
cs3,cs1,cs2,dst,dhost,sourceServiceName,suser showcount=false
showperc=false | table dhost,dst,sourceServiceName,suser,cs1,cs2,cs3|
sort -cs3 | rename cs3 as "Managed Risk" | rename cs2 as "Excepted
Risk" | rename suser as "User" | rename dhost as "Asset Name" | rename
dst as "Asset IP" | rename sourceServiceName as "Platform" | rename
cs1 as "Total Risk"</searchString>
```

Similarly, you can create a number of reports in various panels of Splunk Dashboard, using the attributes of event sent by Secure Configuration Manager.

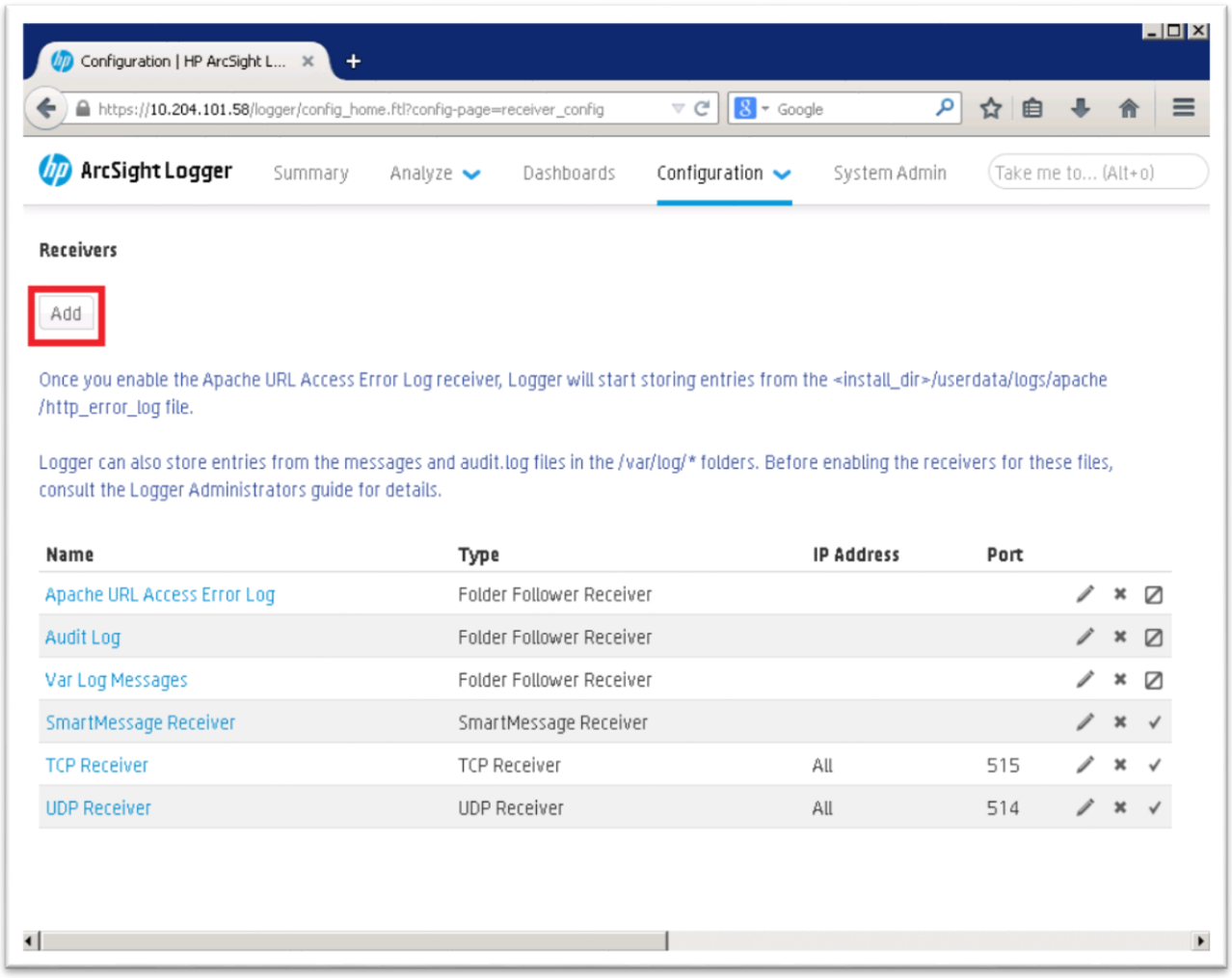


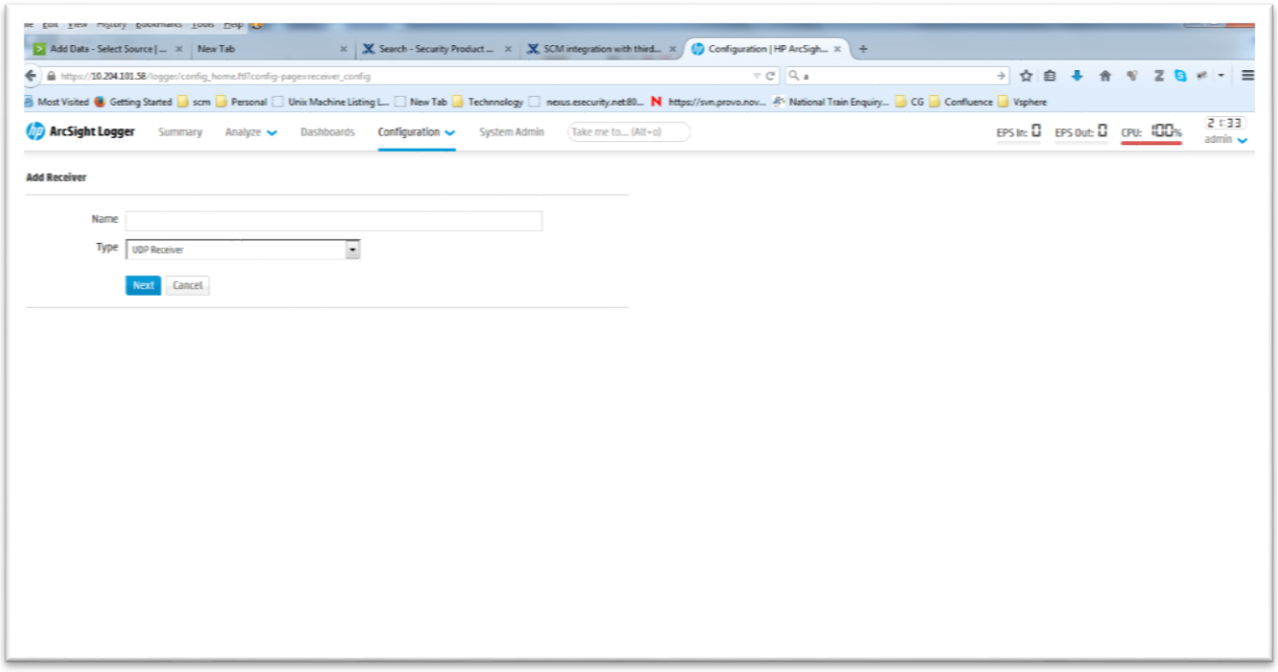
Generating Alerts on Secure Configuration Manager Events

You can generate alerts for Secure Configuration Manager events on Splunk Server. Splunk Server has a provision to trigger alerts on a specific saved search condition. There are options for performing actions such as sending emails and running scripts. See the Splunk Server documentation to configure saved searches, alert action, and other configurations.

5. Integrating Secure Configuration Manager and ArcSight Server

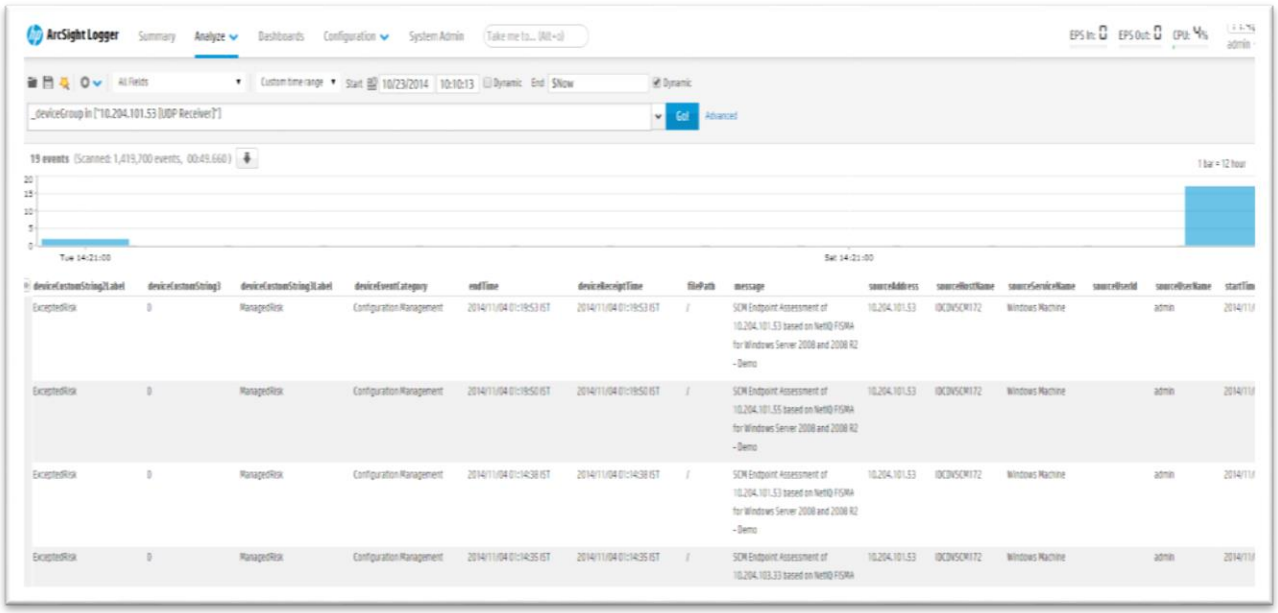
Configure a receiver in ArcSight to accept events from Secure Configuration Manager server, as shown in the following figures.





Viewing Raw Secure Configuration Manager Events in ArcSight Server

After configuring ArcSight to receive events from Secure Configuration Manager, you can view Secure Configuration Manager events in the ArcSght search panel. Whenever policy templates are executed in Secure Configuration Manager, events will be forwarded to ArcSight sever.



Viewing the ArcSight Dashboard

You can generate a number of reports in the ArcSight Dashboard using various saved searches such as top policies and compliance distribution. The following figure shows examples of reports.

Generating Alerts on Secure Configuration Manager Events

You can generate alerts on Secure Configuration Manager events based on saved searches, with various actions such as email and syslog event source. See the ArcSight documentation to configure alert generation for saved searches.