Integration With Third Party SIEM Solutions

Secure® Configuration Manager™

February 2015

Legal Notice

NetIQ Secure Configuration Manager is protected by United States Patent No(s): 5829001, 7707183.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2015 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

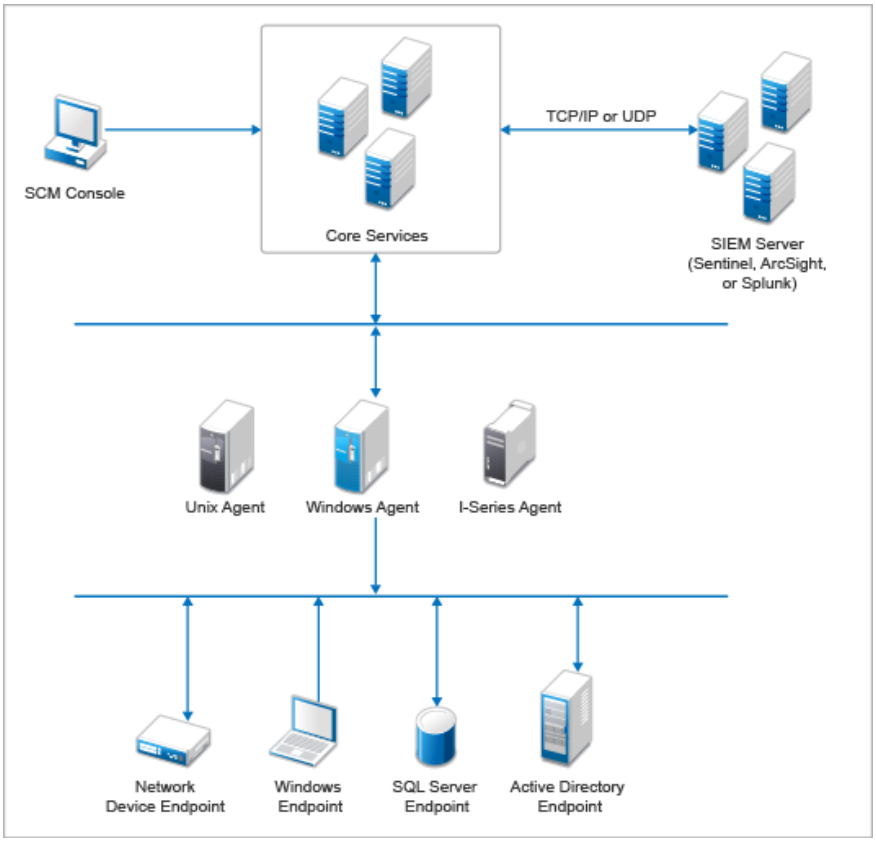
Contents

1. Introduction

NetIQ Secure Configuration Manager (SCM) 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 NetIQ Secure Configuration Manager (SCM) sends configuration compliance information as an event to SIEM solutions, such as Splunk and ArcSight. In this process, SCM 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.

SCM 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.

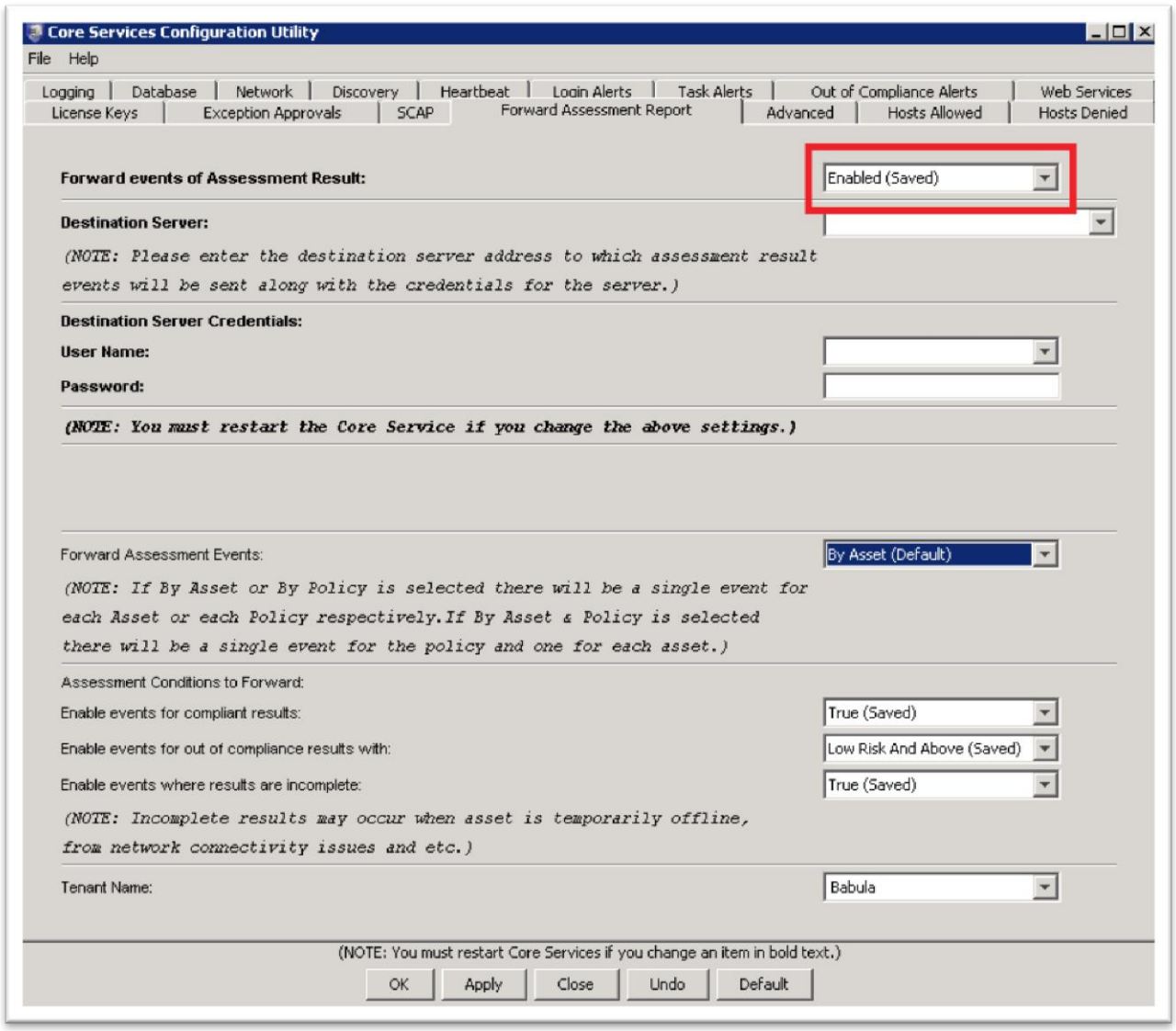


As shown in the above graphic, SCM Core Services component connects to the data receiver component of the SIEM solution, and sends the compliance data in CEF.

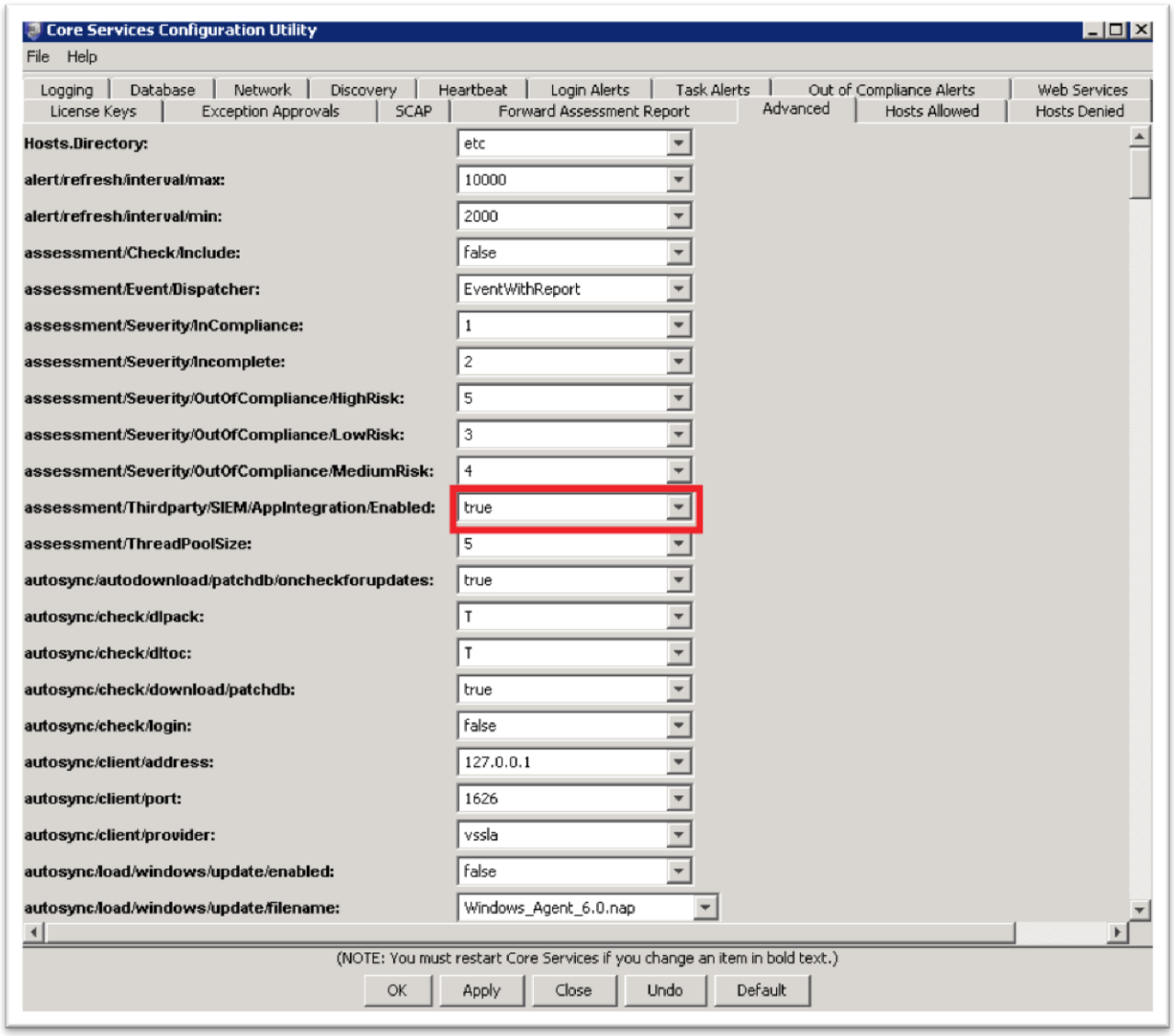
2. Configuring SCM for the Integration

Perform the following configuration in SCM to enable it to send compliance data to SIEM solutions:

1. Open Core Services Configuration Utility in your SCM system and go to the Forward Assessment Report tab.
2. Set the **Forward events of Assessment Result** field to **Enabled (Saved)**.



3. Set the **assessment/Thirdparty/SIEM/AppIntegration/Enabled** field to **true**.



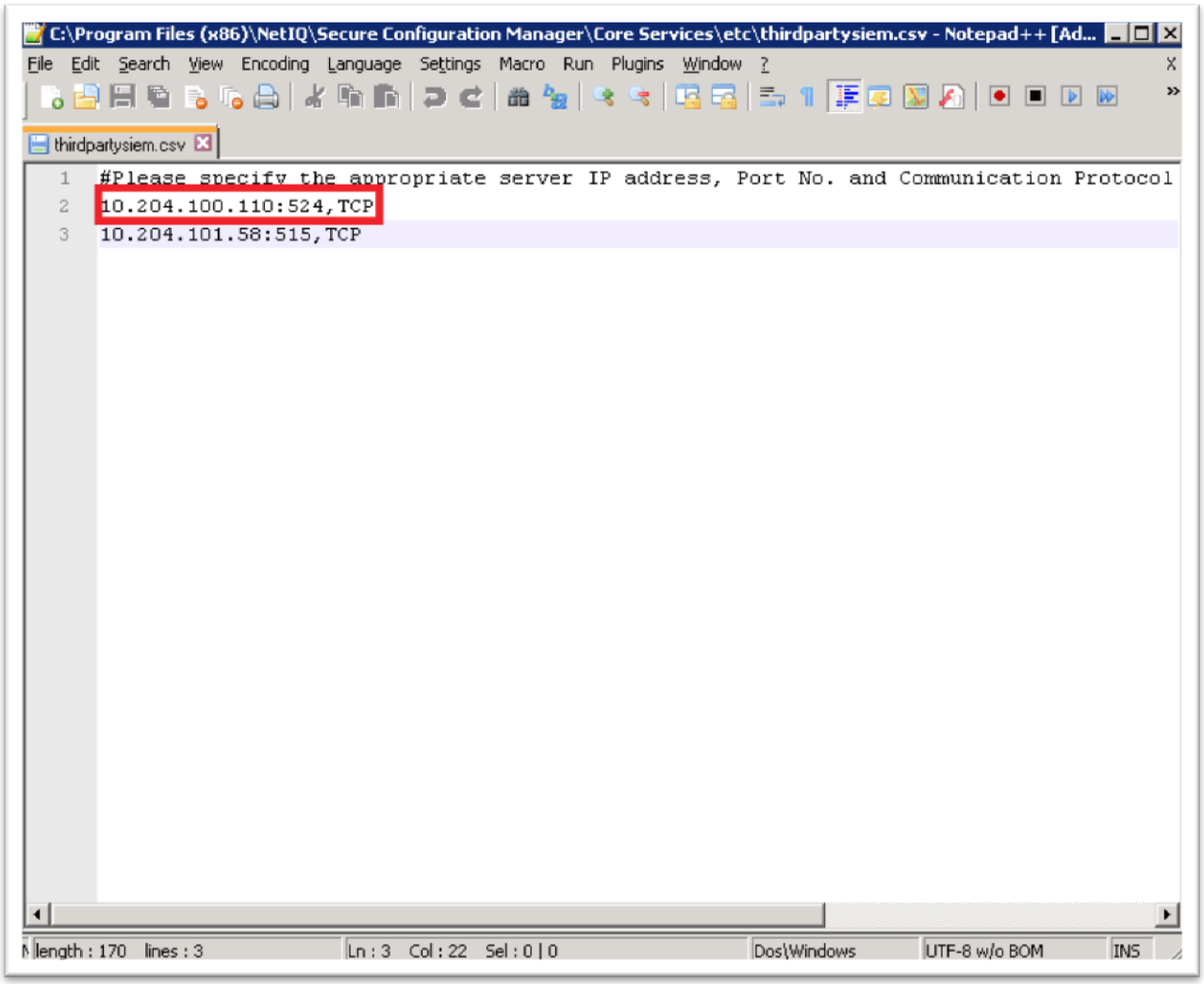
Note: To access the **Advanced** tab in the Core Services Configuration Utility, perform the following steps:

1. Close the Core Services Configuration Utility if it is open.
2. Run the `config.bat` program in the `<Installation Directory>\Core Services\bin` folder.
3. Reopen the Core Services Configuration Utility, and you will see the **Advanced** tab.

4. 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.



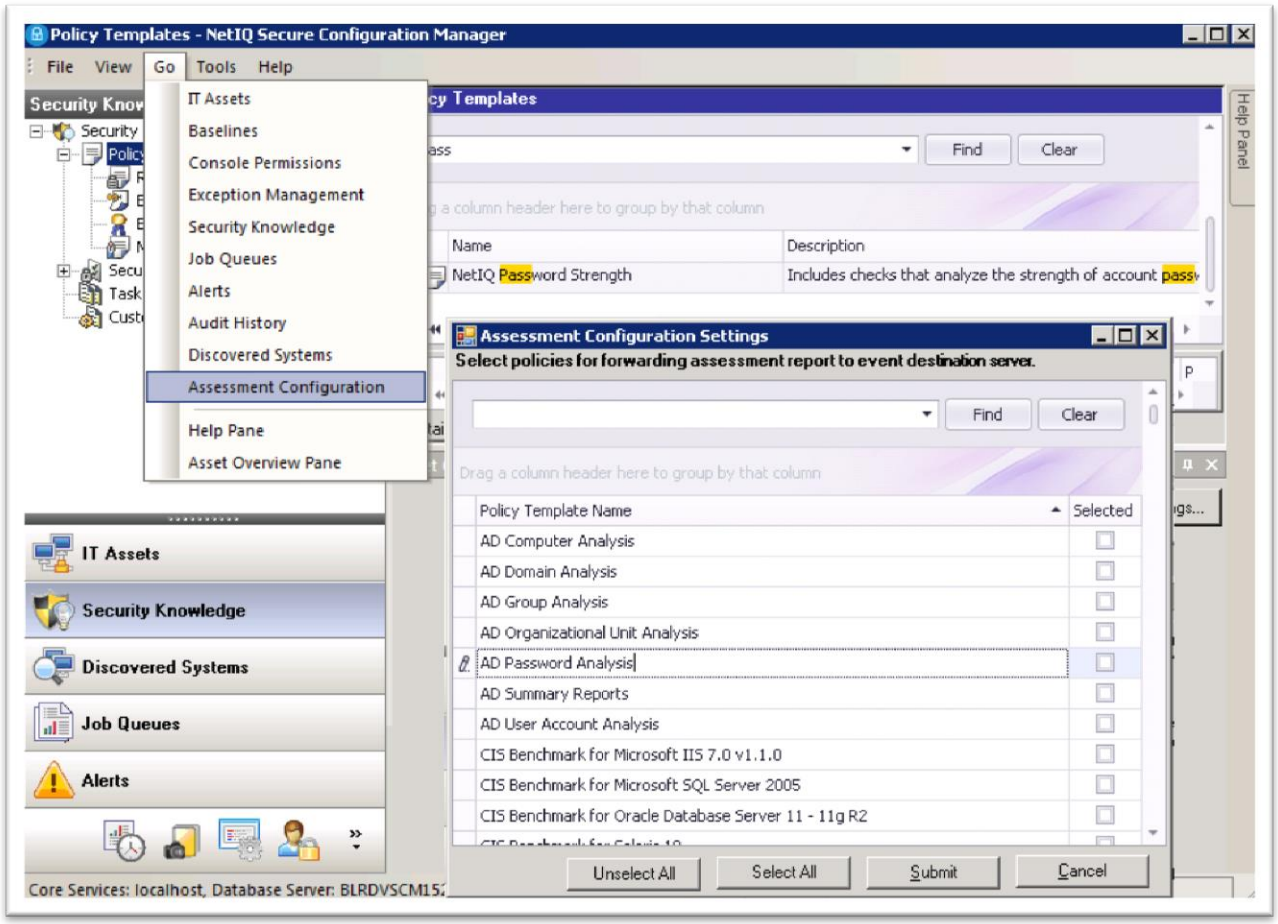
For more information about configuring advanced options, see the *Secure Configuration Manager User Guide*.

3. Sending Events to SIEM Solutions

After you have configured SCM to send compliance events to SIEM solutions as specified in **IntroductionConfiguring SCM 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.

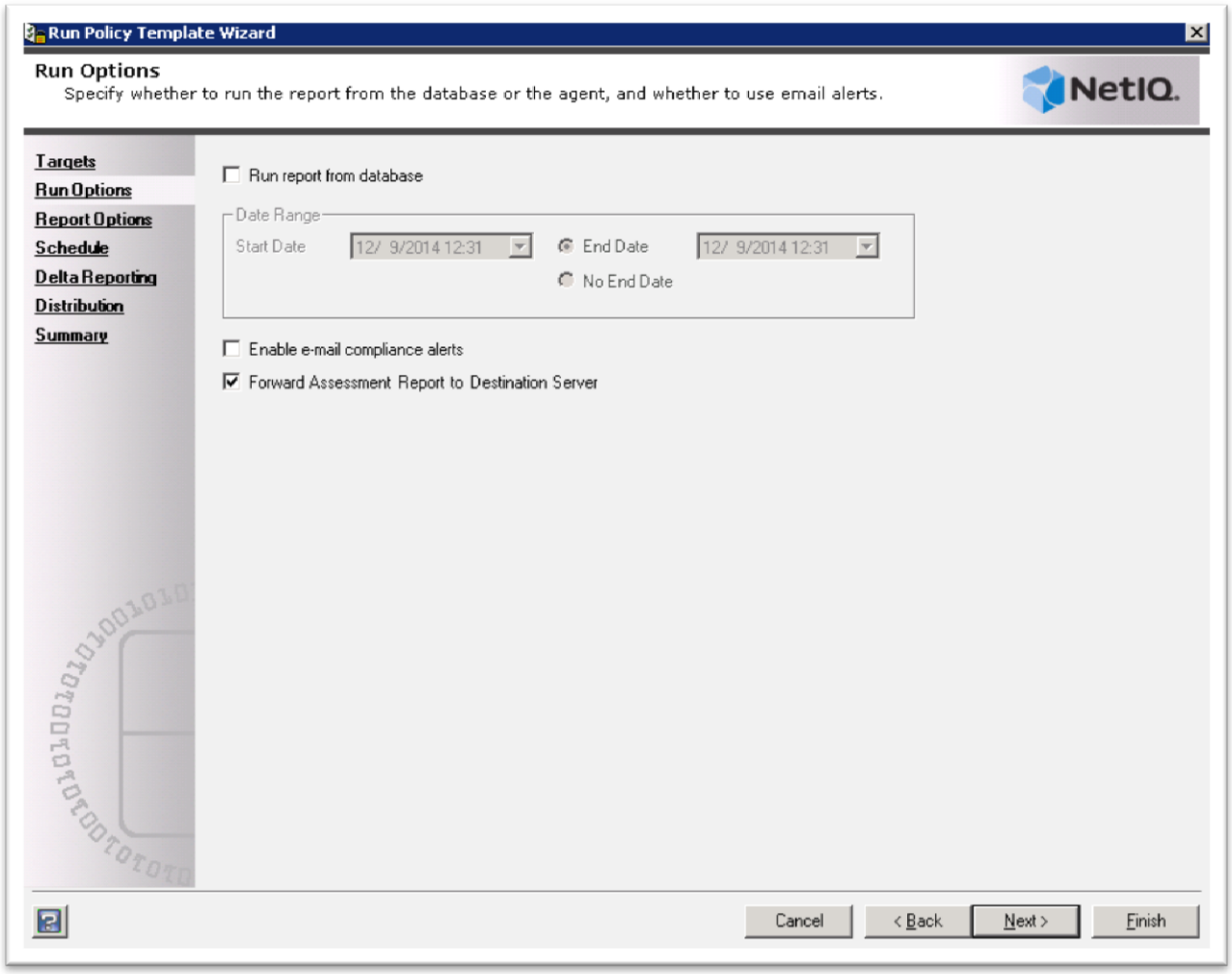
Selecting Policy Templates to Send Events:

In the SCM 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

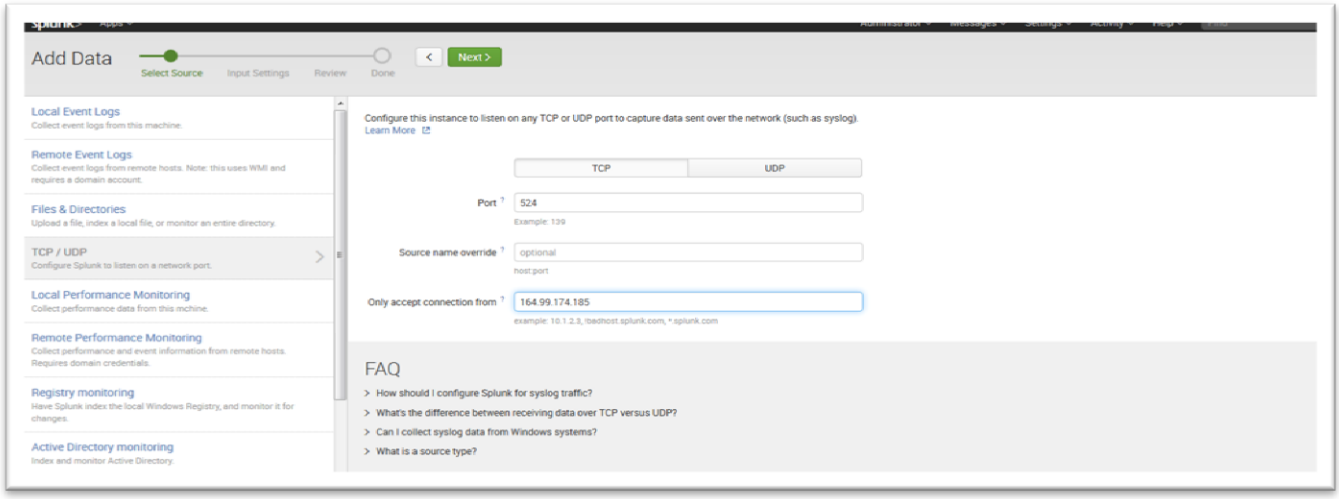
4. Integrating SCM and Splunk Server

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

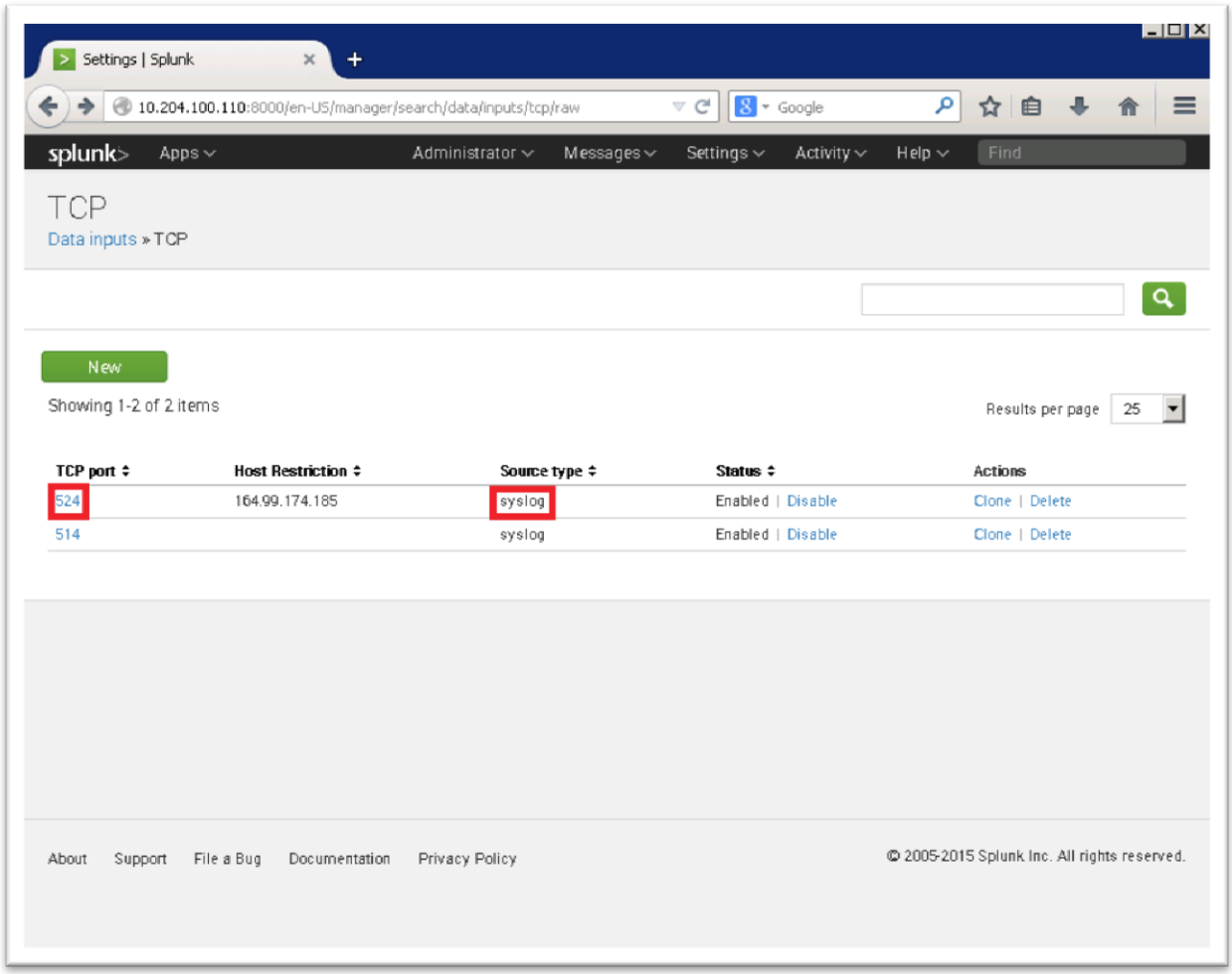
Configuring Splunk

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.

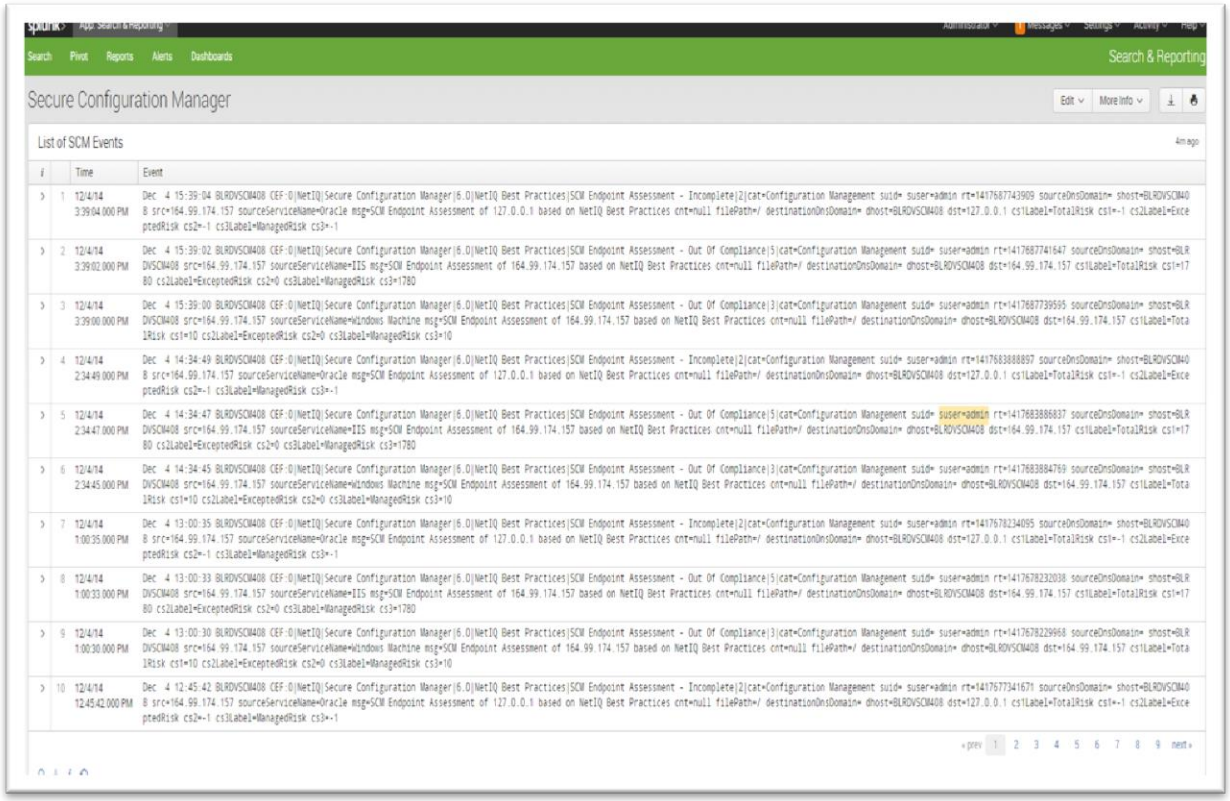


When the data input is configured, it will be added in the **TCP Data inputs** table, as shown in the following figure.


Settings | Splunk
10.204.100.110:8000/en-US/manager/search/data/inputs/tcp/raw
Google
splunk>
Apps
Administrator
Messages
Settings
Activity
Help
Find
TCP
Data inputs » TCP
New
Showing 1-2 of 2 items
Results per page
25
TCP port
Host Restriction
Source type
Status
Actions
524
164.99.174.185
syslog
Enabled | Disable
Clone | Delete
514
syslog
Enabled | Disable
Clone | Delete
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2015 Splunk Inc. All rights reserved.

Viewing Raw SCM Events in Splunk Server

After you configure Splunk to receive events from SCM, whenever policy templates are executed in SCM against selected endpoints, you can view the events in Splunk server search panel.



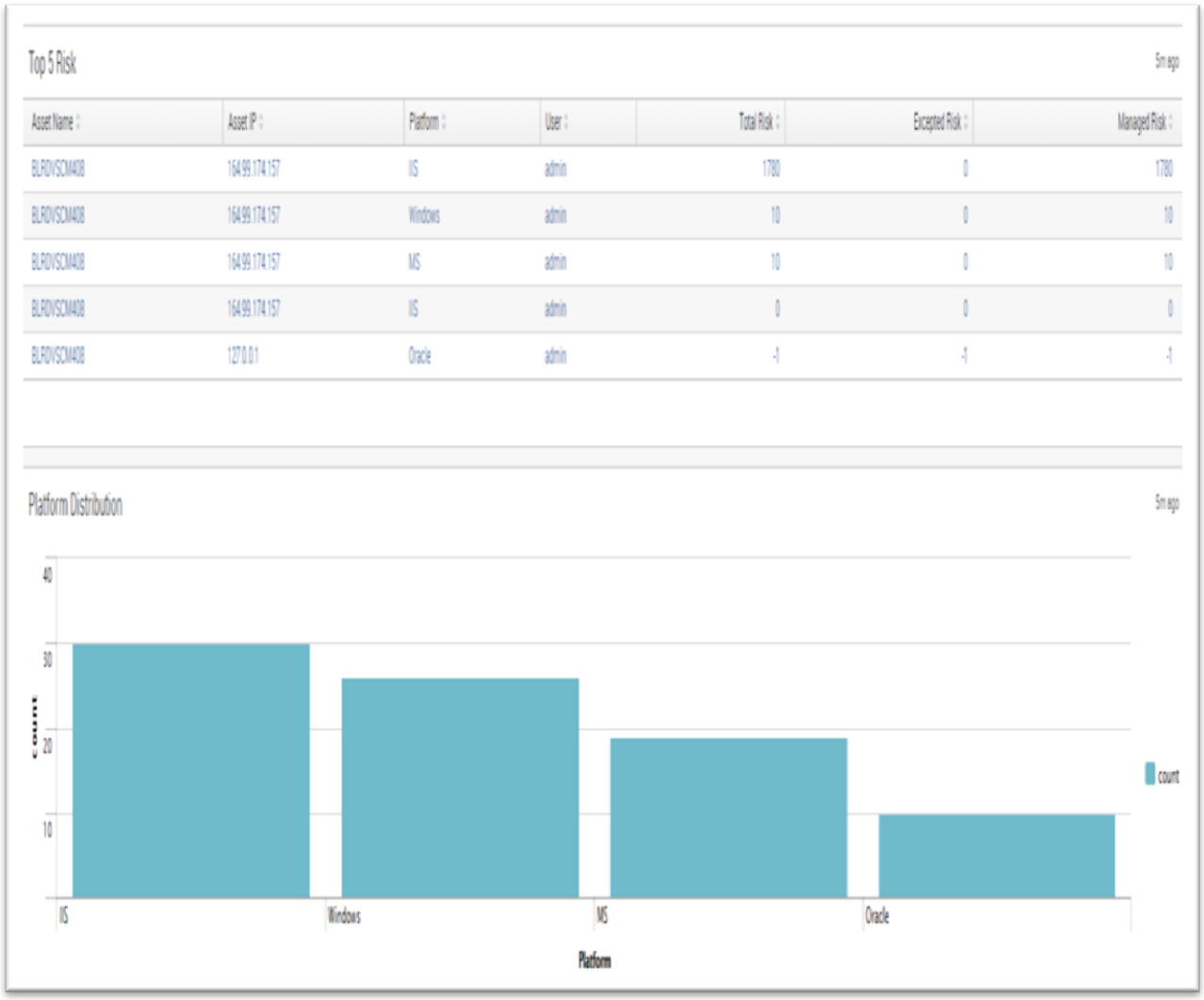
Viewing the Splunk Dashboard

You can generate reports in Splunk Dashboard using the SCM 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 SCM.

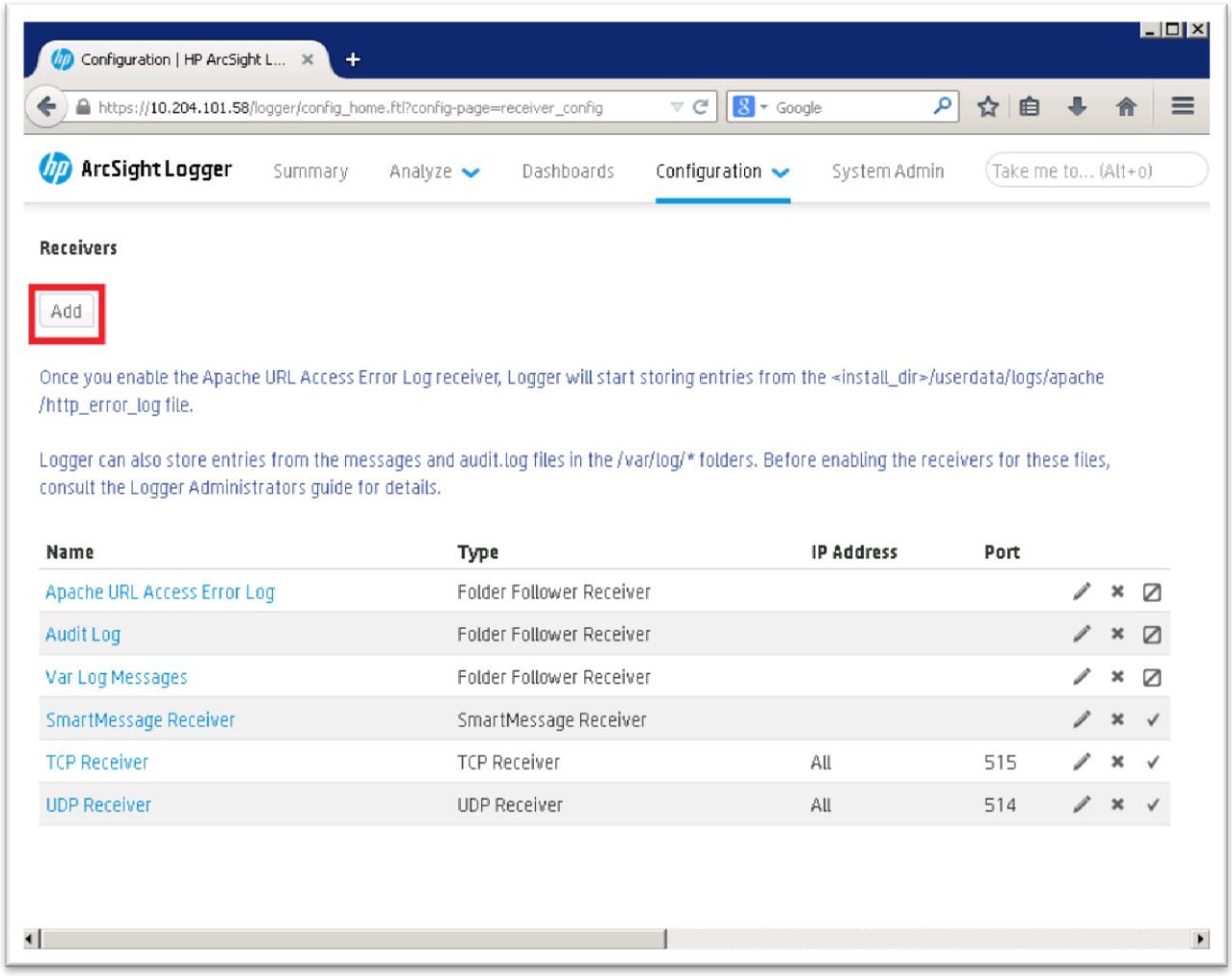


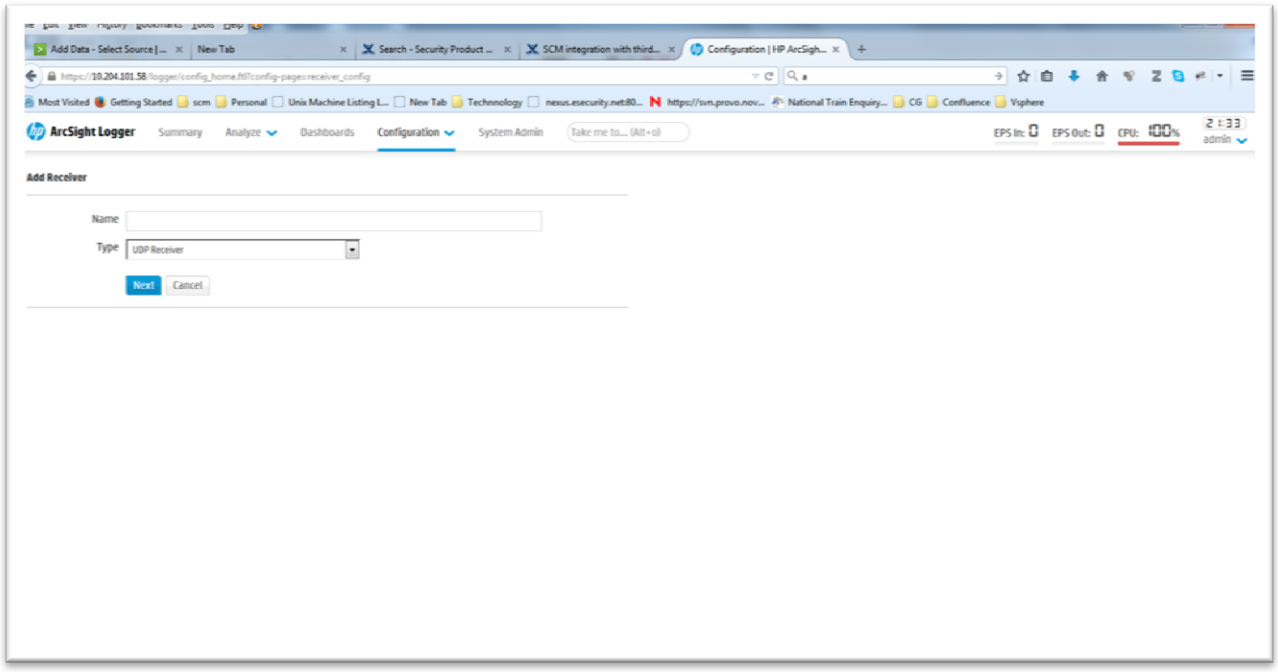
Generating Alerts on SCM Events

You can generate alerts for SCM 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 SCM and ArcSight Server

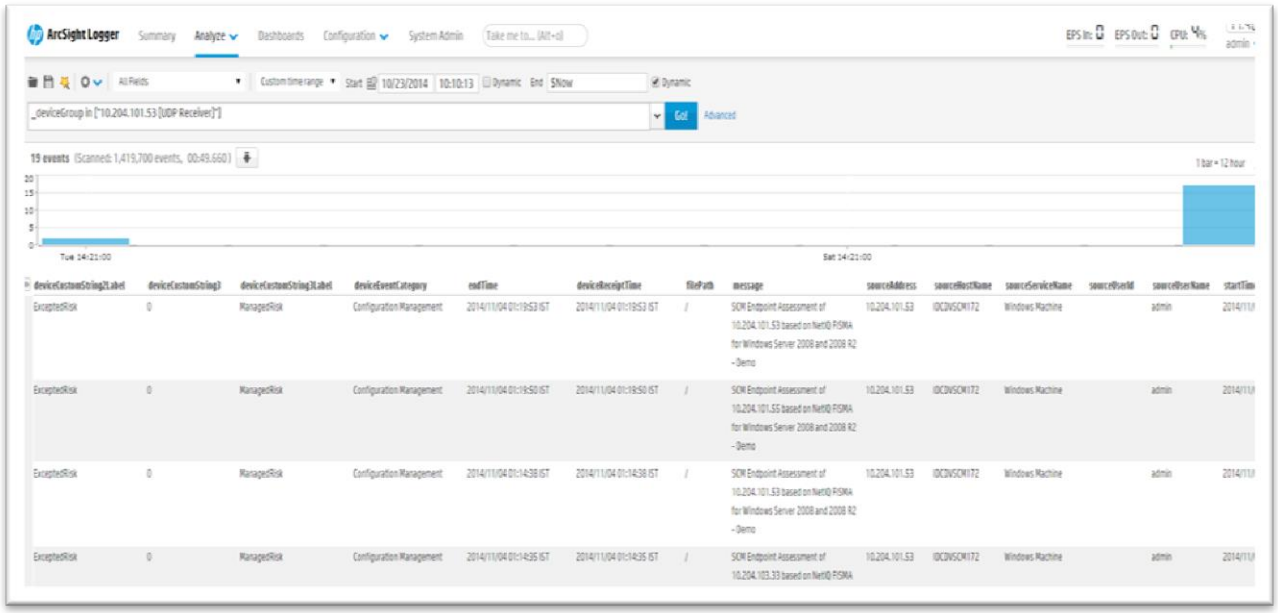
Configure a receiver in ArcSight to accept events from SCM server, as shown in the following figures.





Viewing Raw SCM Events in ArcSight Server

After configuring ArcSight to receive events from SCM, you can view SCM events in the ArcSght search panel. Whenever policy templates are executed in SCM, 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 SCM Events

You can generate alerts on SCM 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.