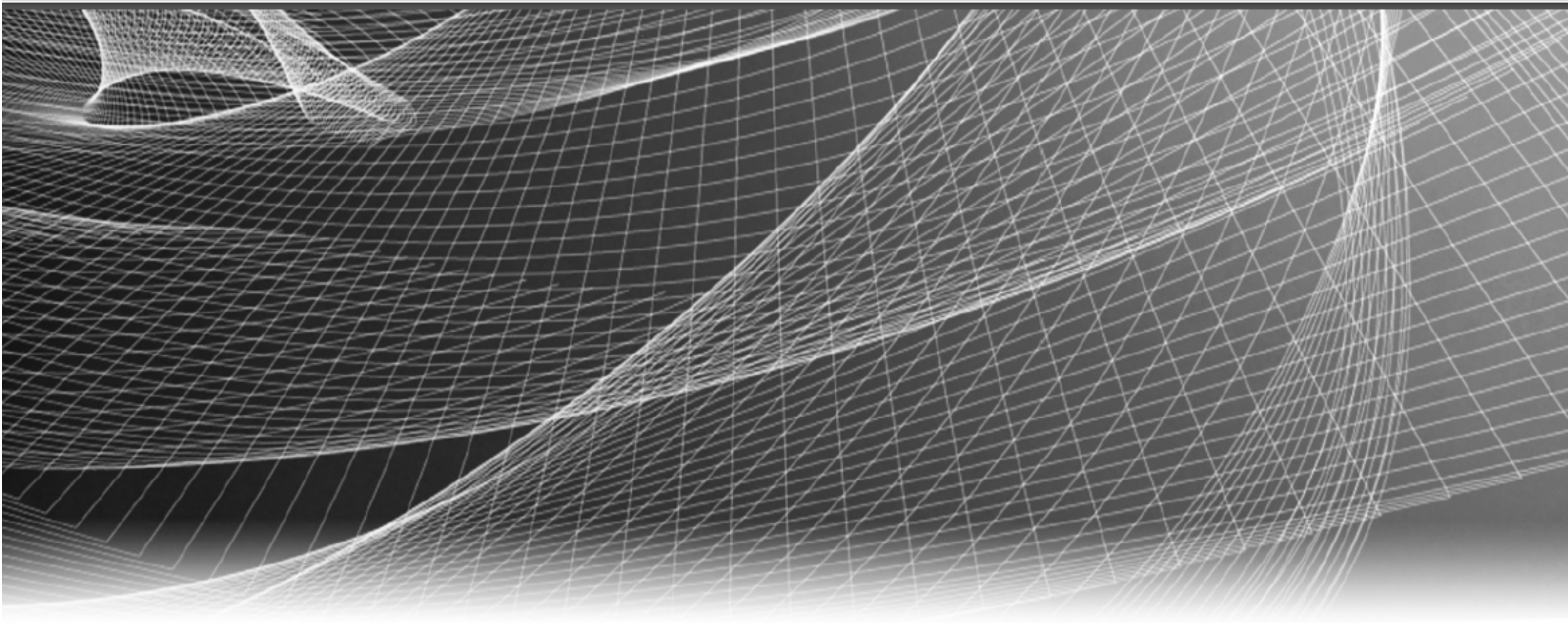


RSA Security Analytics

Log Collection

for Version 10.6.5

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

October 2017

Contents

Log Collection Getting Started Guide

This guide contains the basic tasks you need to complete to start collecting events through Log Collection.

This guide tells you:

- What Log Collection does, how it works from a high level, and provides high-level deployment diagrams.
- How to start collecting events.
- Where to find instructions to set up more complex deployments.
- How to start any collection protocol.
- What the structure of the Log Collection Configuration User Interface is.
- Which tools to use to troubleshoot Log Collection issues and lists global troubleshooting instructions.
- How to fine tune and customize Log Collection in your environment.

This guide does not tell you how to:

- Deploy Log Collection in multiple locations with high availability and load balancing. This information is in the Log Collection Deployment Guide.
- Configure Log Collection as a whole after deployment. This information is in the Log Collection Configuration Guide.
- Configure individual collection protocols. Instructions are in the individual Log Collection Guides:

- AWS (CloudTrail) Collection Configuration Guide
- Check Point Collection Configuration Guide
- File Collection Protocol Configuration Guide
- Netflow Collection Configuration Guide
- ODBC Collection Configuration Guide
- SDEE Collection Configuration Guide
- SNMP Collection Configuration Guide
- VMware Collection Configuration Guide
- Windows Collection Configuration Guide
- Windows Legacy and NetApp Collection Configuration Guide
- Configuration Guides for each supported event source.

  See the Event Source Configuration Guide space on RSA Link for these guides.

Log Collection Basics

This topic tells you how Log Collection works and how you deploy it; lists the supported collection protocols; describes the basic implementation; and illustrates how you configure and deploy Log Collection.

How Log Collection Works

The Log Collector service collects logs from event sources throughout the IT environment in an organization and forwards the logs to other Security Analytics components. The logs and the descriptive content are stored as meta data for use in investigations and reports.

Event sources are the assets on the network, such as servers, switches, routers, storage arrays, operating systems, and firewalls. In most cases, your Information Technology (IT) team configures event sources to send their logs to the Log Collector service and the Security Analytics administrator configures the Log Collector service to poll event sources and retrieve their logs. As a result, the Log Collector receives all logs in their original form.

What Collection Protocols Are Supported

The Log Collector service supports the following collection protocols:

Collection Protocol	Description
AWS	Collects events from Amazon Web Services (AWS) CloudTrail. Specifically CloudTrail records AWS API calls for an account. For more information, see The Basics in the *AWS (CloudTrail) Collection Configuration Guide*.
Check Point	Collects events from Check Point event sources using OPSEC LEA. OPSEC LEA is the Check Point Operations Security Log Export API that facilitates the extraction of logs. For more information, see The Basics in the *Check Point Collection Configuration Guide*.
File	Collects events from log files. Event sources generate log files that are transferred using a secure file transfer method to the Log Collector service. For more information, see The Basics in the *File Protocol Collection Configuration Guide*.
Netflow	Accepts events from Netflow v5 and Netflow v9. For more information, see The Basics in the *Netflow Collection Configuration Guide*.
ODBC	Collects events from event sources that store audit data in a database using the Open Database Connectivity (ODBC) software interface. For more information, see The Basics in the *ODBC Collection Configuration Guide*.
SDEE	Collects Intrusion Detection System (IDS) and Intrusion Prevention Service (IPS) messages. For more information, see The Basics in the *SDEE Collection Configuration Guide*.
SNMP Trap	Accepts SNMP traps. For more information, see The Basics in the *SNMP Collection Configuration Guide*.
Syslog	Accepts messages from event sources that issue syslog messages.
VMware	Collects events from a VMware virtual infrastructure. For more information, see The Basics in the *VMware Collection Configuration Guide*.

Collection Protocol	Description
Windows	Collects events from Windows machines that support the Microsoft Windows model. Windows 6.0 is an event logging and tracing framework included in the operating system beginning with Microsoft Windows Vista and Windows Server 2008. For more information, see The Basics in the *Windows Collection Configuration Guide*.
Windows Legacy	Collects events from: • Older Windows versions such as Windows 2000 and Window 2003 and collects from Windows event sources that are already configured for enVision collection without having to reconfigure them. • NetApp ONTAP appliance event source so that you can now collect and parse NetApp evt files. • For more information, see The Basics in the *Windows Legacy and NetApp Collection Configuration Guide*. **Note:** You install the Security Analytics Windows Legacy Collector on a physical or virtual Windows 2008 R2 SP1 64-Bit server using the **SALegacyWindowsCollector-*version-number.exe***. Please refer to the *Windows Collection Configuration Guide* for detailed instructions on how to deploy the Windows Legacy Collector.

This topic describes basic, required tasks you need to complete to start collecting events using Security Analytics Log Collector service. Please refer to the *Log Collection Deployment Guide* for instructions on how to set up more elaborate deployments.

Basic Implementation

To implement Log Collection, you must:

1. Set up a Log Collector locally on a Log Decoder (that is a Local Collector). You can also set up log collectors in as many remote locations (that is Remote Collectors) as you need for your enterprise.
2. Configure:
   - Security Analytics Log Collection to to collect events from event sources
   - Events sources to send events to Security Analytics Log Collection service.

Roles of Local and Remote Collectors

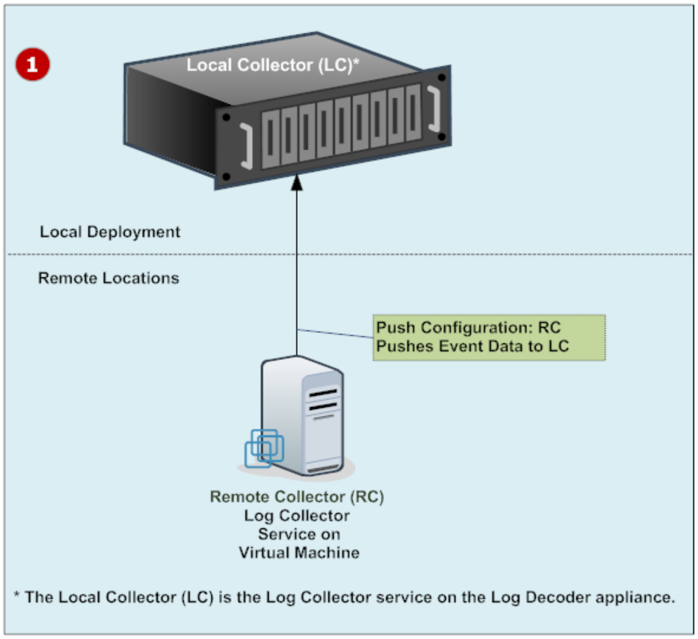
A Local Collector (LC) is a Log Collector service running on a Log Decoder host. In a local deployment scenario, the Log Collector service is deployed on a Log Decoder host, with the Log Decoder service. Log collection from various protocols like Windows, ODBC, and so on, is performed through the Log Collector service, and events are forwarded to the Log Decoder service. The Local Collector sends all collected event data to the Log Decoder service.

You must have at least one Local Collector to collect non-Syslog events.

A Remote Collector (RC), also referred to as a Virtual Log Collector (VLC), is a Log Collector service running on a stand-alone Virtual Machine. Remote Collectors are optional and they must send the events they collect to a Local Collector. Remote Collector deployment is ideal when you have to collect logs from remote locations. Remote Collectors compress and encrypt the logs before sending them to a Local Collector.

Deploying and Configuring Log Collection

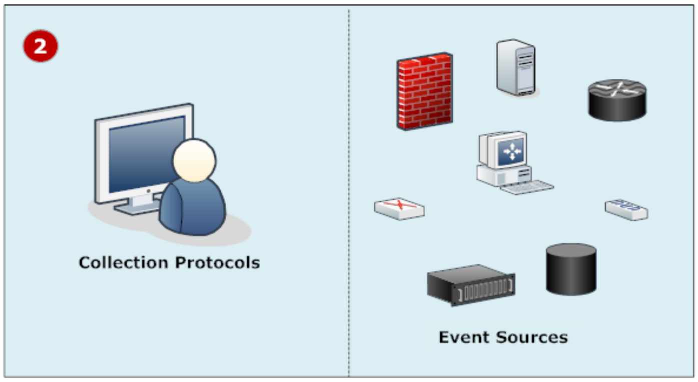
The following figure illustrates the basic tasks you must complete to deploy and configure Log Collection. To deploy Log Collection, you need to set up a Local Collector. You can also deploy one or more Remote Collectors. After you deploy Log Collection, you need to configure the events sources in Security Analytics and on the events sources themselves. The following diagram shows the Local Collector with one remote collector that pushes events to the Local Collector.


1
Local Collector (LC)*
Local Deployment
Remote Locations
Push Configuration: RC Pushes Event Data to LC
Remote Collector (RC) Log Collector Service on Virtual Machine
* The Local Collector (LC) is the Log Collector service on the Log Decoder appliance.

1 Set up Local and Remote Collectors.

The Local collector is the Log Collector service running on the Log Decoder host.

A Remote Collector is the Log Collector service running on a virtual machine or Windows server in a remote location.

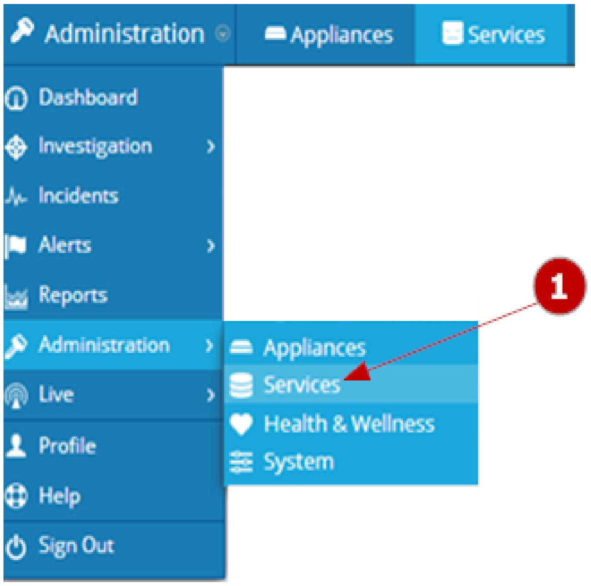


2 Configure event sources:

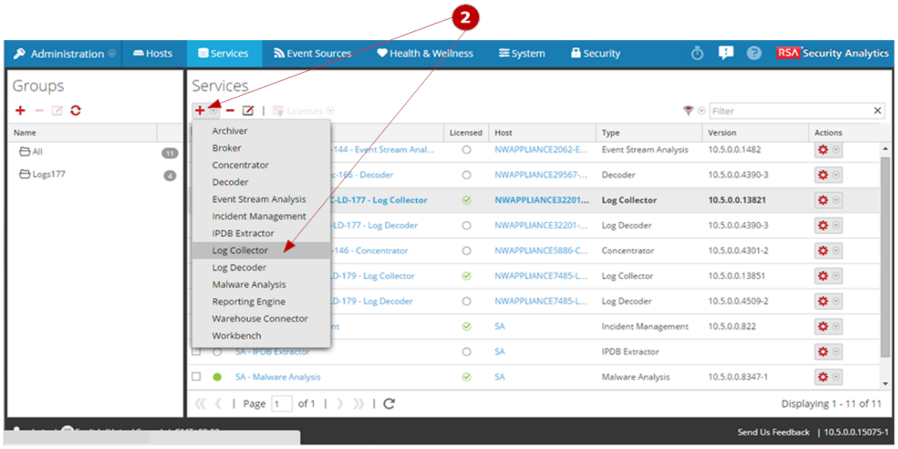
- Configure collection protocols in Security Analytics.
- Configure each event source to communicate with the Security Analytics Log Collector.

Adding Local Collector and Remote Collector to Security Analytics

The following figure shows how to add a Local Collector and Remote Collector to Security Analytics.

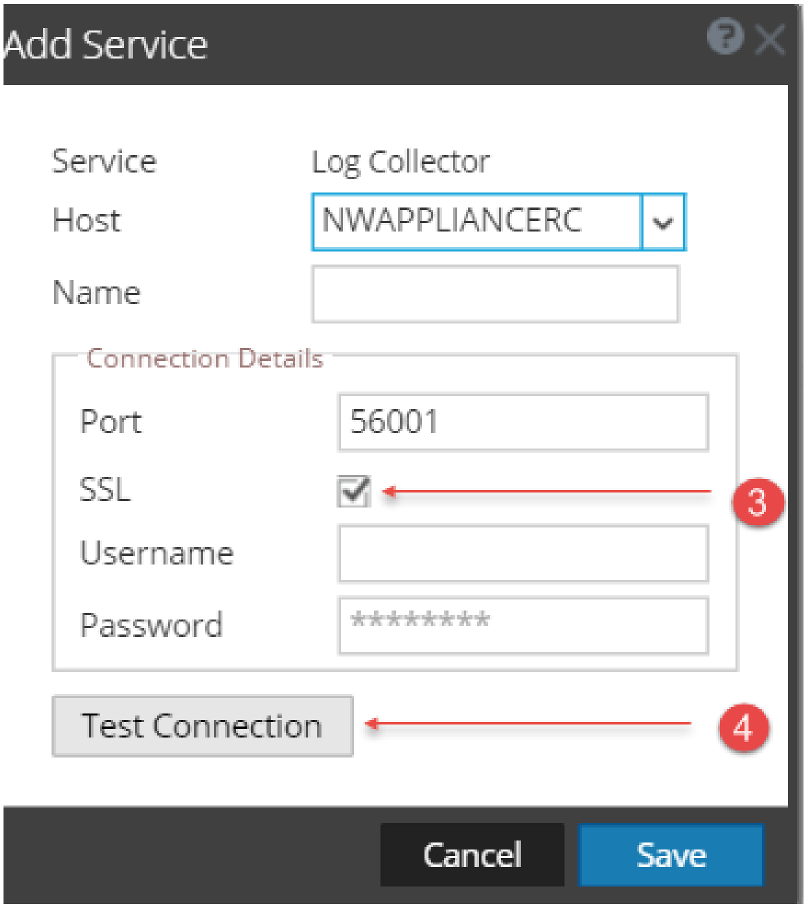


1 Access the **Services** view.



	Licensed	Host	Type	Version	Actions
-144 - Event Stream Anal...	○	NWAPPLIANCE2062-E...	Event Stream Analysis	10.5.0.0.1482	⚙
c-166 - Decoder	○	NWAPPLIANCE29567-...	Decoder	10.5.0.0.4390-3	⚙
C-LD-177 - Log Collector	✓	NWAPPLIANCE32201...	Log Collector	10.5.0.0.13821	⚙
LD-177 - Log Decoder	○	NWAPPLIANCE32201-...	Log Decoder	10.5.0.0.4390-3	⚙
-146 - Concentrator	○	NWAPPLIANCE5886-C...	Concentrator	10.5.0.0.4301-2	⚙
D-179 - Log Collector	✓	NWAPPLIANCE7485-L...	Log Collector	10.5.0.0.13851	⚙
D-179 - Log Decoder	○	NWAPPLIANCE7485-L...	Log Decoder	10.5.0.0.4509-2	⚙
nt	✓	SA	Incident Management	10.5.0.0.822	⚙
SA - IPDB Extractor	○	SA	IPDB Extractor		⚙
SA - Malware Analysis	✓	SA	Malware Analysis	10.5.0.0.8347-1	⚙

2 Open the **Add Service** dialog.



Service: Log Collector

Host: NWAPPLIANCERC

Name:

Connection Details

Port: 56001

SSL: ☑

Username:

Password: ********

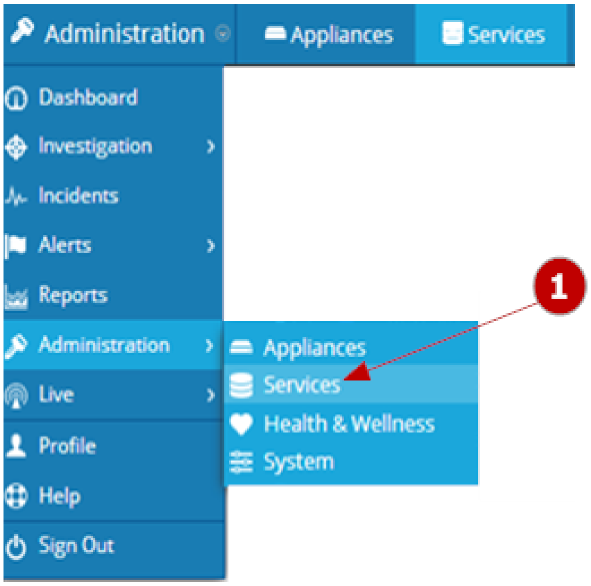
Test Connection

3 Define the details of the **Log Collection** service.

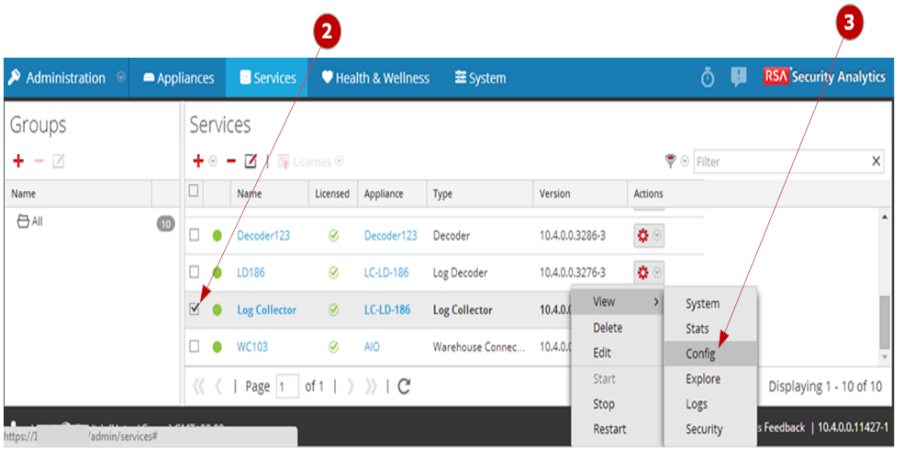
4 Select **Test Connection** to ensure that your Local or Remote Collector is added.

Configuring Log Collection

You choose the Log Collector, that is a Local Collector (LC) or Remote Collector (RC), for which you want to define parameters in the Services view. The following figure shows how to navigate to the Services view, select a log collector service, and display the configuration parameter interface for that service.



1 Access the **Services** view

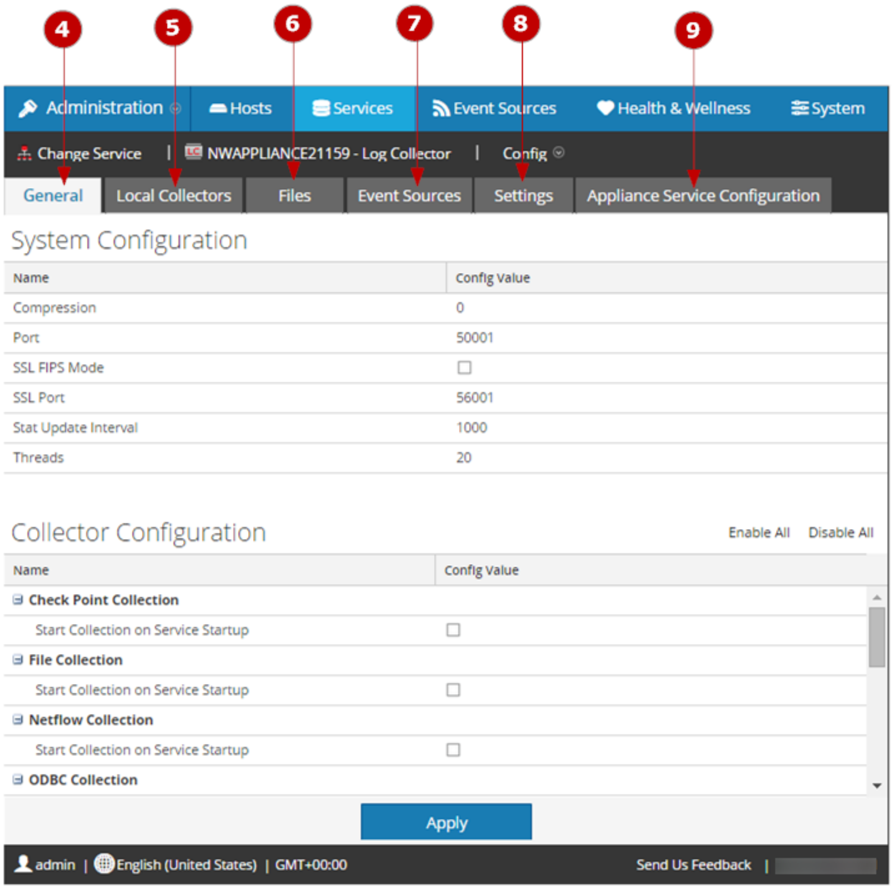


Services

☐		Name	Licensed	Appliance	Type	Version	Actions
☐	●	Decoder123	✓	Decoder123	Decoder	10.4.0.0.3286-3	⚙
☐	●	LD186	✓	LC-LD-186	Log Decoder	10.4.0.0.3276-3	⚙
☑	●	Log Collector	✓	LC-LD-186	Log Collector	10.4.0.	
☐	●	WC103	✓	AIO	Warehouse Connec...	10.4.0.	

2 Select a **Log Collection** service.

3 Click under **Actions** and select **View** > **Config** to display the Log Collection configuration parameter tabs.



System Configuration

Name	Config Value
Compression	0
Port	50001
SSL FIPS Mode	□
SSL Port	56001
Stat Update Interval	1000
Threads	20

Collector Configuration

Name	Config Value
⊟ **Check Point Collection**	
Start Collection on Service Startup	□
⊟ **File Collection**	
Start Collection on Service Startup	□
⊟ **Netflow Collection**	
Start Collection on Service Startup	□
⊟ **ODBC Collection**	

4 Define global Log Collection parameters in the **General** tab.

5 For a:

- Local Collector, Security Analytics displays the **Remote Collectors** tab. Select the Remote Collectors from which the Local Collector pulls events in this tab.
- Remote Collector, Security Analytics displays the **Local Collectors**. Select the Local Collectors to which the Remote Collector pushes events in this tab.

6 Edit configuration files as text files in the **Files** tab

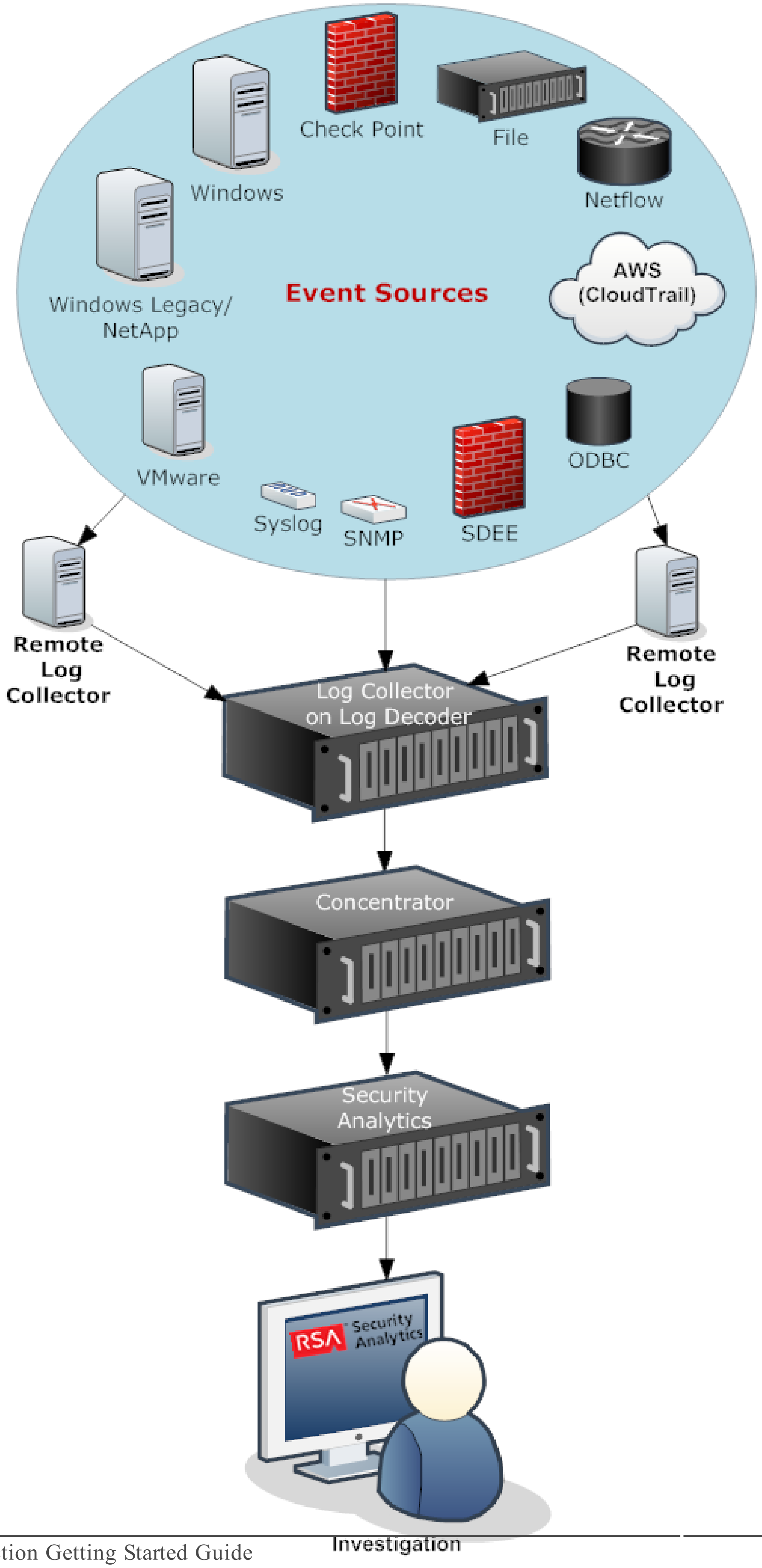
7 Define collection protocol parameters in the **Event Sources** tab.

8 Define the lockbox, encryption keys, and certificates in the Settings tab.

9 Define Appliance Service parameters in the **Appliance Service Configuration** tab.

Data Flow Diagram

You use the log data collected by the Log Collector service to monitor the health of your enterprise and to conduct investigations. The following figure shows you how data flows through Security Analytics Log Collection to Investigation.


Event Sources
Windows
Check Point
File
Netflow
Windows Legacy/ NetApp
AWS (CloudTrail)
VMware
ODBC
Syslog
SNMP
SDEE
Remote Log Collector
Remote Log Collector
Log Collector on Log Decoder
Concentrator
Security Analytics
RSA Security Analytics
Investigation

Procedures

This topic provides an overview of the end-to-end sequential steps you must complete to start collecting events.

High-Level Checklist

Note: The steps in this list are in the order in which you must complete them.

Step	Description
1	Add Local and Remote Collectors to Security Analytics.
2	Download latest content from LIVE.
3	Set up the Lockbox.
4	Configure collection protocols and event sources.
5	Start collection service for configured collection protocols.
6	Verify that Log Collection is working.

Step 1. Add Local and Remote Collectors

This topic tells how to perform the initial setup of Local Collectors and Remote Collectors so that you can configure them.

After completing this procedure, you will have ...

- Added a Local Collector service.
- Added a Remote Collector service

Verify That the Log Decoder Is Set Up

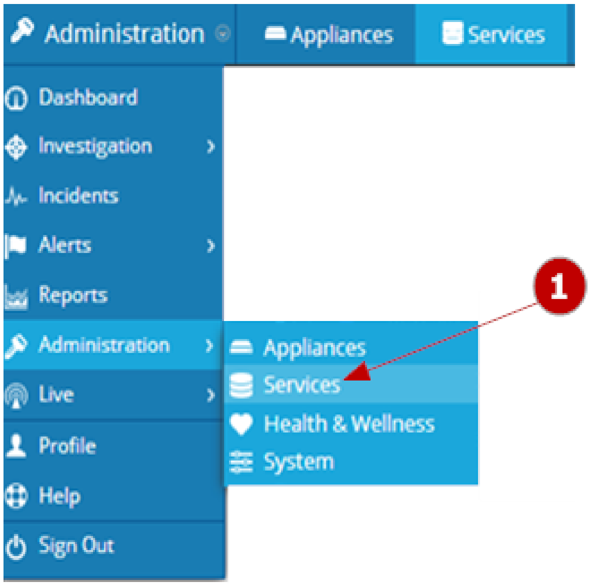
Verify that the Log Decoder:

- is capturing data.
- has the current content loaded.
- is properly licensed.

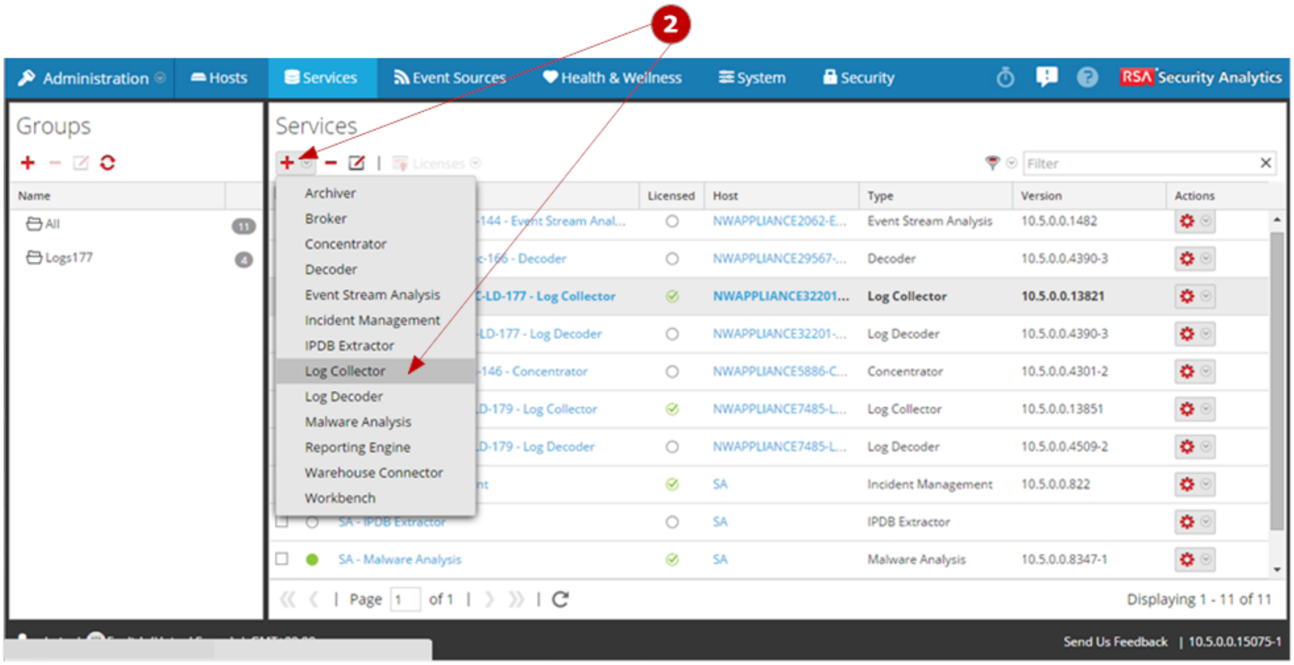
Please refer to the *Log Decoder Configuration Guide* for instructions on how to configure the Log Decoder.

Add a Local Collector

You add a Local Collector by adding the Log Collector service to a Log Decoder host in Security Analytics as shown in the following figure.



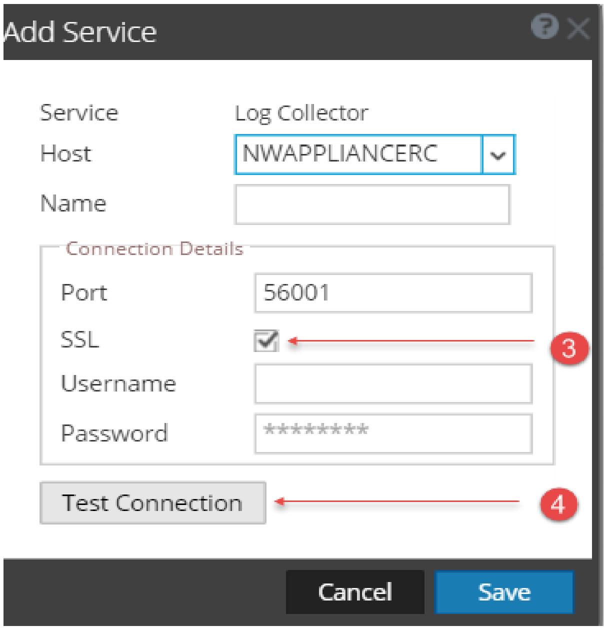
1 Access the **Services** view.



	Licensed	Host	Type	Version	Actions
-144 - Event Stream Anal...	○	NWAPPLIANCE2062-E...	Event Stream Analysis	10.5.0.0.1482	
c-166 - Decoder	○	NWAPPLIANCE29567-...	Decoder	10.5.0.0.4390-3	
C-LD-177 - Log Collector	✓	NWAPPLIANCE32201...	Log Collector	10.5.0.0.13821	
LD-177 - Log Decoder	○	NWAPPLIANCE32201-...	Log Decoder	10.5.0.0.4390-3	
-146 - Concentrator	○	NWAPPLIANCE5886-C...	Concentrator	10.5.0.0.4301-2	
D-179 - Log Collector	✓	NWAPPLIANCE7485-L...	Log Collector	10.5.0.0.13851	
D-179 - Log Decoder	○	NWAPPLIANCE7485-L...	Log Decoder	10.5.0.0.4509-2	
nt	✓	SA	Incident Management	10.5.0.0.822	
□ ○ SA - IPDB Extractor	○	SA	IPDB Extractor		
□ ● SA - Malware Analysis	✓	SA	Malware Analysis	10.5.0.0.8347-1	

Displaying 1 - 11 of 11

2 Open the **Add Service** dialog.



Add Service

Service Log Collector

Host NWAPPLIANCERC

Name

Connection Details

Port 56001

SSL ☑

Username

Password ********

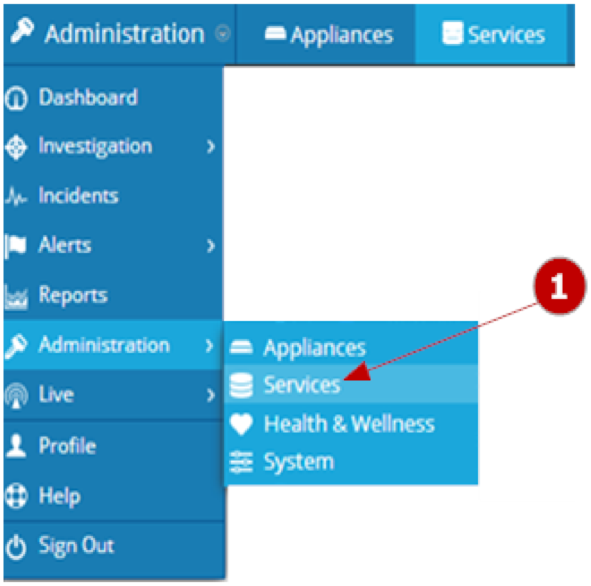
3 Define the connection details of the Log Collection service on a Local Collector.

4 Click **Test Connection**. If the connection is valid you will see Test connection successful. If the connection fails you will see Fail. If it failed, make sure that the Log Decoder host is running and that you have entered the correct information on the **Add Service** dialog and click **Save**.

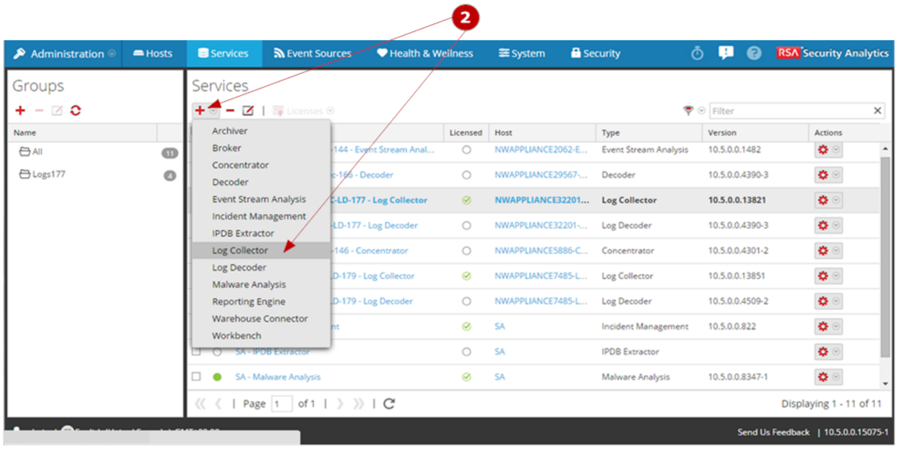
Add a Remote Collector (Optional)

You add a Remote Collector by adding the Log Collector service to a remote host as shown in the following figure.

Note: Before you add a Legacy Windows Remote Collector, you must install the Security Analytics Legacy Windows Collector on a physical or virtual Windows 2008 SP1 64-bit server using the **SALegacyWindowsCollector-*version-number.exe***. You download the **SALegacyWindowsCollector-*version-number.exe*** from SCOL (please refer to the *Microsoft Windows Legacy Windows Eventing Configuration Guide* for instructions.)



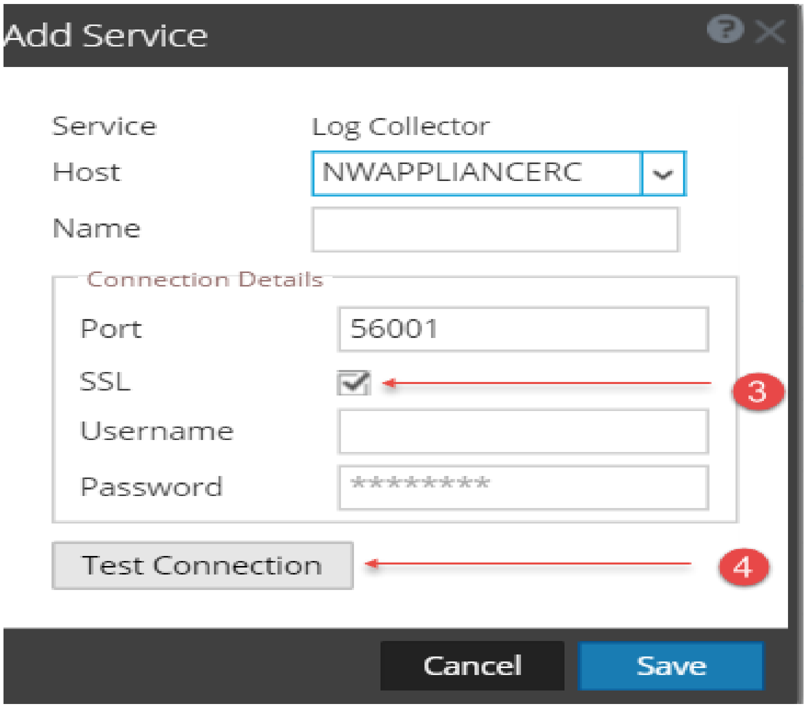
1 Access the **Services** view.



Name	Licensed	Host	Type	Version	Actions
-144 - Event Stream Anal...	○	NWAPPLIANCE2062-E...	Event Stream Analysis	10.5.0.0.1482	
c-166 - Decoder	○	NWAPPLIANCE29567-...	Decoder	10.5.0.0.4390-3	
C-LD-177 - Log Collector	✓	**NWAPPLIANCE32201...**	**Log Collector**	**10.5.0.0.13821**	
LD-177 - Log Decoder	○	NWAPPLIANCE32201-...	Log Decoder	10.5.0.0.4390-3	
-146 - Concentrator	○	NWAPPLIANCE5886-C...	Concentrator	10.5.0.0.4301-2	
D-179 - Log Collector	✓	NWAPPLIANCE7485-L...	Log Collector	10.5.0.0.13851	
D-179 - Log Decoder	○	NWAPPLIANCE7485-L...	Log Decoder	10.5.0.0.4509-2	
nt	✓	SA	Incident Management	10.5.0.0.822	
□ ○ SA - IPDB Extractor	○	SA	IPDB Extractor		
□ ● SA - Malware Analysis	✓	SA	Malware Analysis	10.5.0.0.8347-1	

Displaying 1 - 11 of 11

2 Open the **Add Service** dialog.



Add Service

Service: Log Collector

Host: NWAPPLIANCERC

Name:

Connection Details

Port: 56001

SSL: ☑

Username:

Password: *********

3 Define the connection details of the Log Collection service on a Remote Collector and click **Save**.

4 Click **Test Connection**. If the connection is valid you will see Test connection successful. If the connection fails you will see Fail. If it failed, make sure that the Log Decoder host is running and that you have entered the correct information on the **Add Service** dialog and click **Save** again.

Step 2. Download Latest Content from LIVE

This topic sends you to the RSA Content and Resources documentation in which you will find the instructions for retrieving Log Collection content.

Return to Procedures

LIVE is Security Analytics' Content Management System from which you download the latest content. The two resource types you use to download Log Collection content are:

- **RSA Log Collector** - content enabling the collection of event source types.
- **RSA Log Device** - the latest supported event source parsers. **See Adding or Updating Supported Event Source Log Parsers** in the *RSA Content and Resources Guide* for instructions on how to download log parsers from LIVE.

Step 3. Set Up a Lockbox

This topic tells you how to configure Lockbox Security Settings.

What Is a Lockbox

A lockbox is an encrypted file that you use to store confidential information about an application. The Security Analytics Lockbox stores an encryption key for the Log Collector.

The encryption key is used to encrypt all event source passwords and the event broker password.

When you create the Lockbox, you need to define a password for the Lockbox.

The Log Collector operates the Lockbox in a mode during data collection that does not require you to specify the password (the Log Collector uses the host system fingerprint instead).

These are the lockbox security settings.

Feature	Description
Old Lockbox Password	When you set up a Lockbox for the first time, this field is blank. Security Analytics populates this field after you enter a New Lockbox Password and click Apply.
New Lockbox Password	Initial or new lockbox password. To maximize lockbox security, specify a password that is eight or more characters in length with at least one numeric character, uppercase character, and non-alphanumeric character such as # or !
Apply	Click **Apply** to save the changes to the lockbox password.

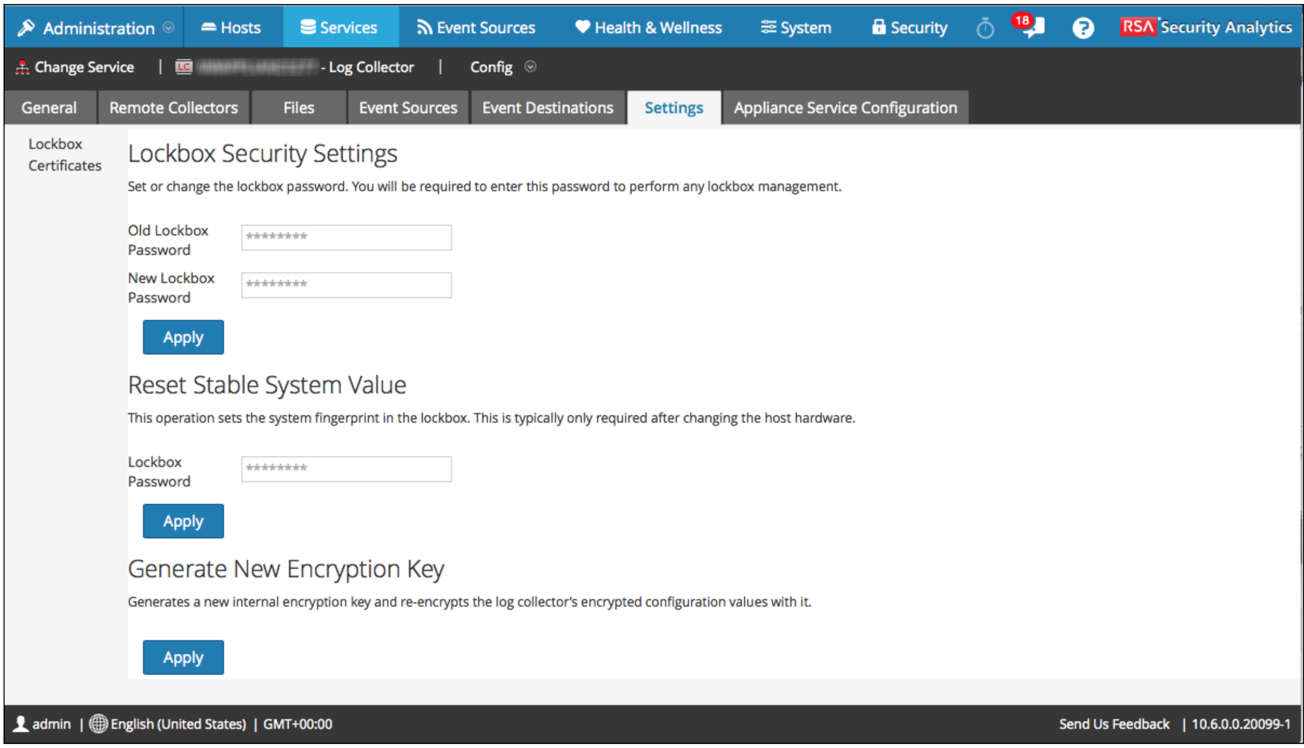
Set Up a Lockbox

To set up a lockbox you need to set a password, as follows:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In **Services**, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.

   The Service Config view is displayed with the **Log Collector General** tab open.

4. Click the **Settings** tab.



Lockbox Security Settings

Set or change the lockbox password. You will be required to enter this password to perform any lockbox management.

Old Lockbox Password ********

New Lockbox Password ********

Reset Stable System Value

This operation sets the system fingerprint in the lockbox. This is typically only required after changing the host hardware.

Lockbox Password ********

Generate New Encryption Key

Generates a new internal encryption key and re-encrypts the log collector's encrypted configuration values with it.

5. In the options panel, select **Lockbox** to configure Lockbox settings.

6. Under **Lockbox Security Settings**, enter a password in the **New Lockbox Password** field and click **Apply**.

Step 4. Configure Collection Protocols and Event Sources

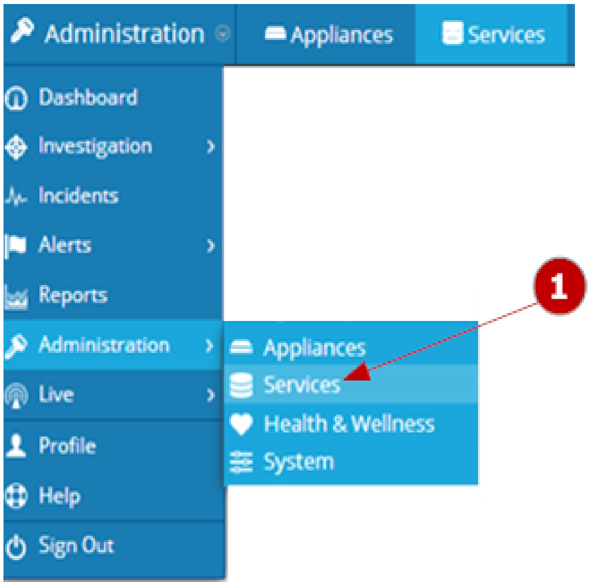
This topic tells you how to configure collection protocols and the event sources using those protocols.

You configure the Log Collector to collect event data from your event sources in the Event Sources tab of the Log Collection parameter view.

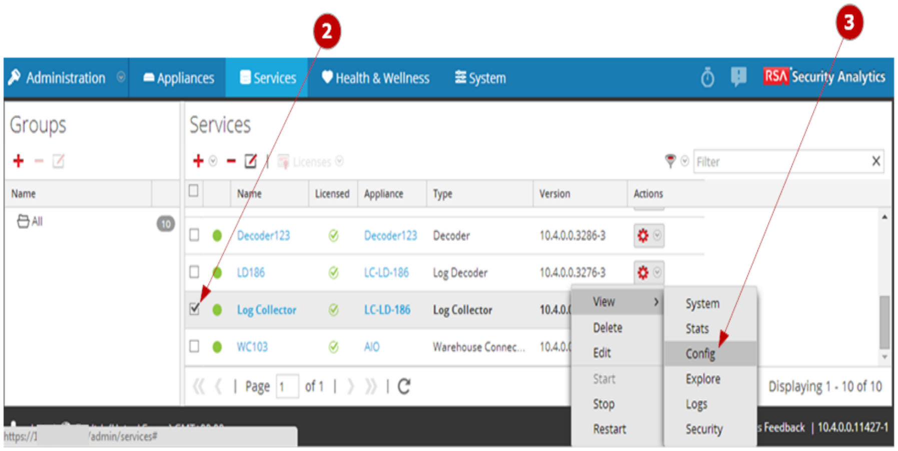
Procedures

Configure a Collection Protocol

The following figure shows the basic workflow for configuring an event source in Security Analytics. Each event source has different parameters so you must to refer to guides for the event source you are configuring for all the instructions.



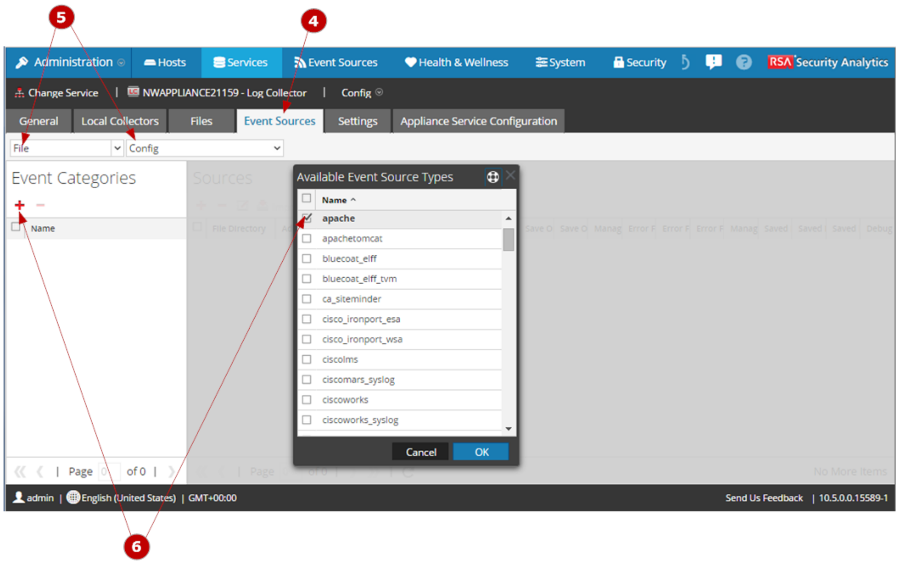
1 Access the Services view.



☐		Name	Licensed	Appliance	Type	Version	Actions
☐	●	Decoder123	✓	Decoder123	Decoder	10.4.0.0.3286-3	⚙
☐	●	LD186	✓	LC-LD-186	Log Decoder	10.4.0.0.3276-3	⚙
☑	●	Log Collector	✓	LC-LD-186	Log Collector	10.4.0.(	
☐	●	WC103	✓	AIO	Warehouse Connec...	10.4.0.(	

2 Select a Log Collection service.

3 Click ⌄ under **Actions**and select **View** > **Config**to display the Log Collection configuration parameter tabs.

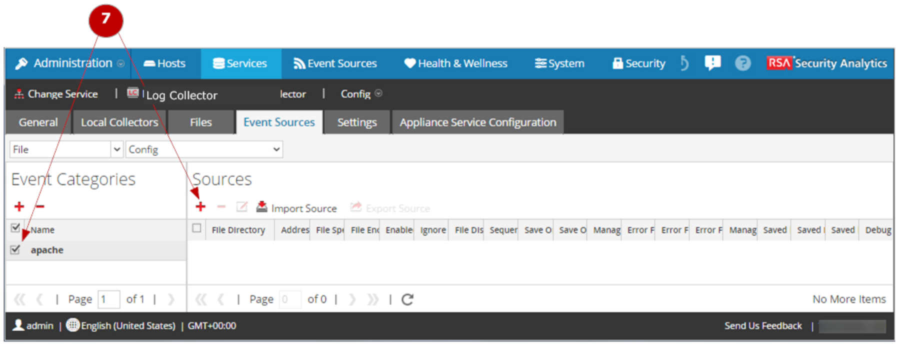


4 Click the **Event Sources** tab.

5 Select a collection protocol (for example, **File**) and select **Config**.

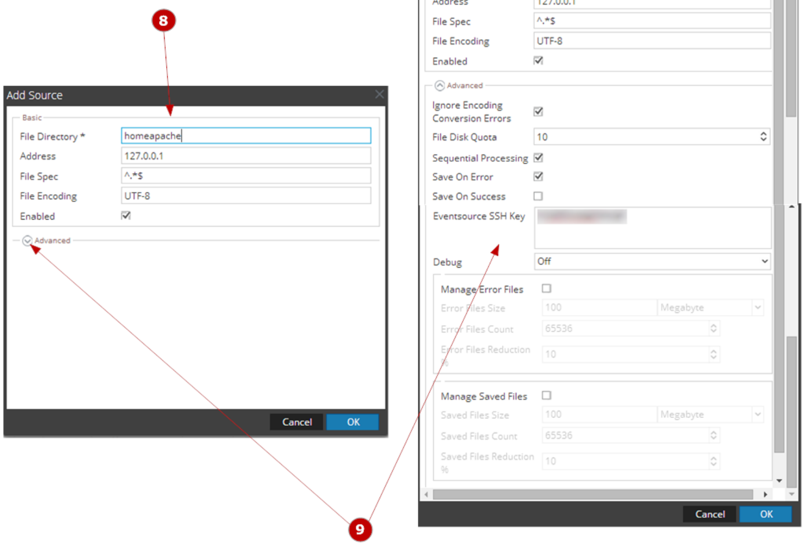
6 Click + and select an event source category (for example, **apache**).

The event source category is part of the content you downloaded from LIVE.



7 Select the newly added category (for example, **apache**).

Click + .



Add Source

Basic

File Directory * homeapache
Address 127.0.0.1
File Spec ^.*$
File Encoding UTF-8
Enabled ☑

Advanced

Add Source

Basic

File Directory * homeapache
Address 127.0.0.1
File Spec ^.*$
File Encoding UTF-8
Enabled ☑

Advanced

Ignore Encoding Conversion Errors ☑
File Disk Quota 10
Sequential Processing ☑
Save On Error ☑
Save On Success ☐
Eventsource SSH Key [redacted]
Debug Off

Manage Error Files ☐
Error Files Size 100 Megabyte
Error Files Count 65536
Error Files Reduction % 10

Manage Saved Files ☐
Saved Files Size 100 Megabyte
Saved Files Count 65536
Saved Files Reduction % 10

8 Specify the basic parameters required for the event source.

9 Click ⌄ and specify additional parameters that enhance how the protocol handles event collection for the event source.

Individual Collection Protocol Guides

The following guides provide detailed instructions on how to configure the collection protocols and their associated event sources in Security Analytics. Each guide includes an index to configuration instructions for the event sources supported for that collection protocol.

Configure individual collection protocols. Instructions are in the individual Log Collection Guides:

- AWS (CloudTrail) Collection Configuration Guide
- Check Point Collection Configuration Guide
- File Collection Protocol Configuration Guide
- Netflow Collection Configuration Guide
- ODBC Collection Configuration Guide
- SDEE Collection Configuration Guide
- SNMP Collection Configuration Guide
- VMware Collection Configuration Guide
- Windows Collection Configuration Guide
- Windows Legacy and NetApp Collection Configuration Guide
- Configuration Guides for each supported event source.

  See the Event Source Configuration Guide space on RSA Link for these guides.

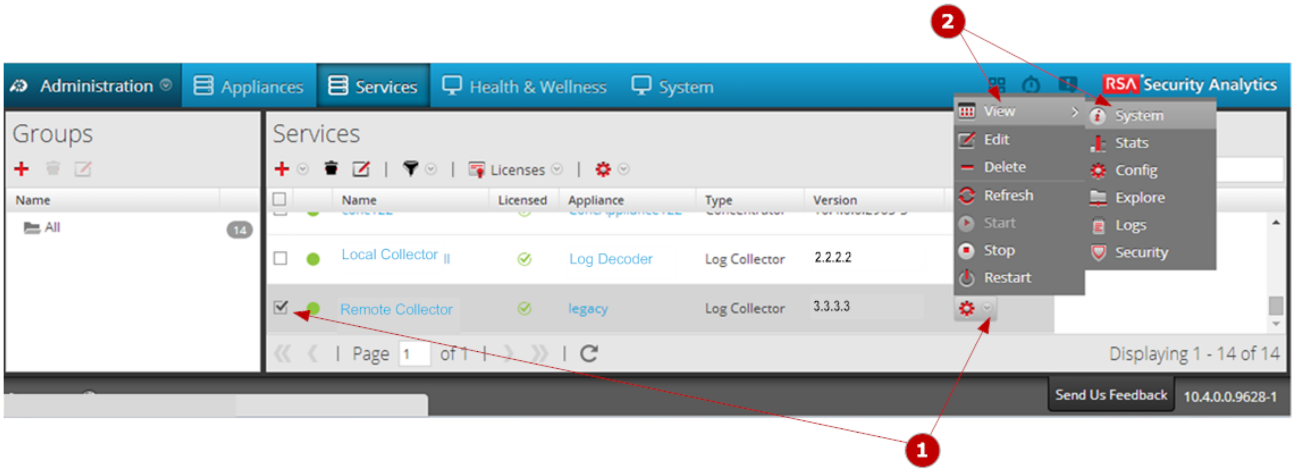
Step 5. Start Collection Services and Enable Automatic Start

If a collection service stops, you may need to start it again. You can also enable the automatic start of collection services.

Start a Collection Service

Return to Procedures

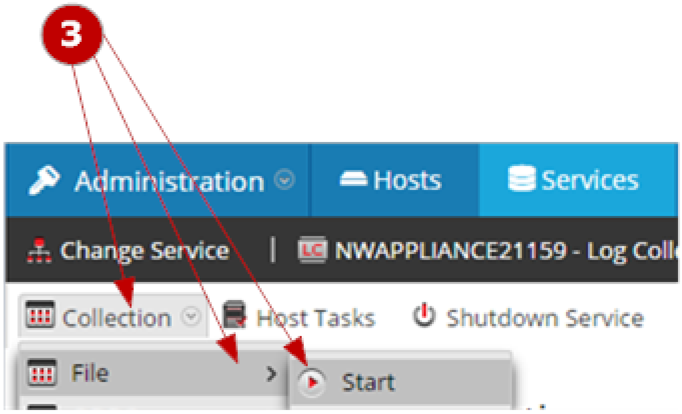
The following figure shows you how to start a collection service.



Name	Licensed	Appliance	Type	Version
Local Collector	✓	Log Decoder	Log Collector	2.2.2.2
Remote Collector	✓	legacy	Log Collector	3.3.3.3

1 Select a Log Collector service and click ⌄ under Actions.

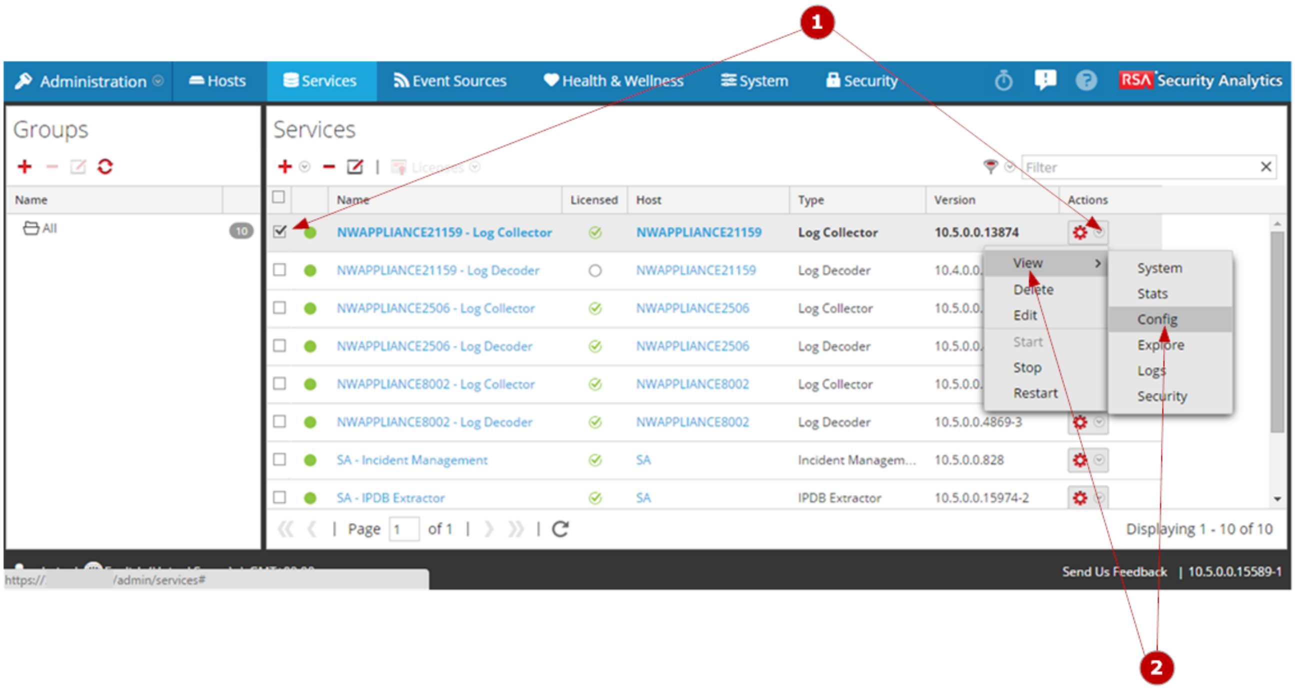
2 Click **View > System**.



3 Click **Collection** > ***service*** (for example, **File**) and click **Start**.

Enable Automatic Start of Collection Services

The following figure shows you how to enable the automatic start of a collection service.

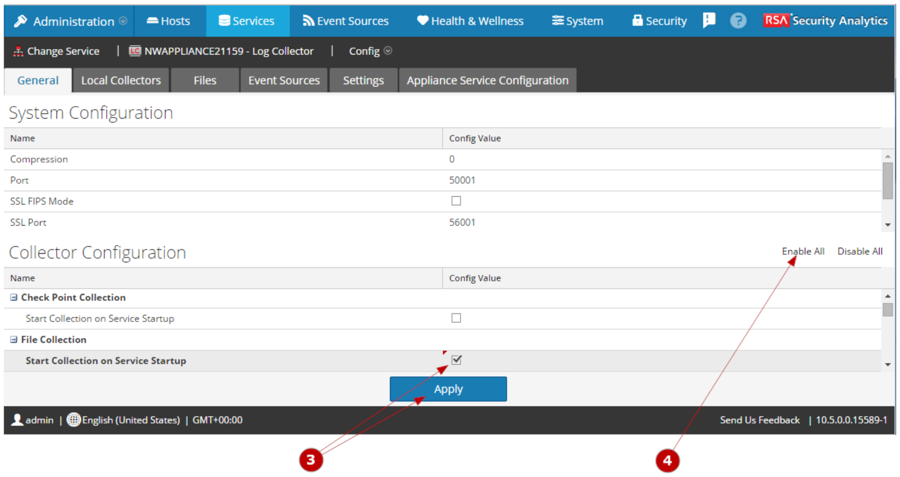


Name	
All	10

☐		Name	Licensed	Host	Type	Version	Actions
☑	●	NWAPPLIANCE21159 - Log Collector	✓	NWAPPLIANCE21159	Log Collector	10.5.0.0.13874	
☐	●	NWAPPLIANCE21159 - Log Decoder	○	NWAPPLIANCE21159	Log Decoder	10.4.0.0.	
☐	●	NWAPPLIANCE2506 - Log Collector	✓	NWAPPLIANCE2506	Log Collector	10.5.0.0.	
☐	●	NWAPPLIANCE2506 - Log Decoder	✓	NWAPPLIANCE2506	Log Decoder	10.5.0.0.	
☐	●	NWAPPLIANCE8002 - Log Collector	✓	NWAPPLIANCE8002	Log Collector	10.5.0.0.	
☐	●	NWAPPLIANCE8002 - Log Decoder	✓	NWAPPLIANCE8002	Log Decoder	10.5.0.0.4869-3	
☐	●	SA - Incident Management	✓	SA	Incident Managem...	10.5.0.0.828	
☐	●	SA - IPDB Extractor	✓	SA	IPDB Extractor	10.5.0.0.15974-2	

1 Select a Log Collector service and click ⌄ under Actions.

2 Click **View > Config**.



System Configuration

Name	Config Value
Compression	0
Port	50001
SSL FIPS Mode	☐
SSL Port	56001

Collector Configuration

Name	Config Value
Check Point Collection	
Start Collection on Service Startup	☐
File Collection	
Start Collection on Service Startup	☑

3 Select the **Start Collection on Service Startup** checkbox for a collection service (for example, **File**) and click **Apply**.

4 (Optional) You can click Enable All and click Apply to select every collection service to start upon the startup of the Log Collector service.

Step 6. Verify That Log Collection Is Working

This topic tells you how to verify that you have set up Log Collection correctly.

You need to verify that Log Collection has been configured correctly, otherwise it might not work.

The following methods verify that Log Collection is working.

- Verify that there is event activity the Event Source Monitoring tab of the **Administration > Health & Wellness** view.
- Verify that there are parsers in the **device.type** field in the **Details** column in the **Investigation > Events** view for the collection protocol you configured.

Please refer to the *Log Collection Configuration Guide* for each Collection Protocol for steps on how to verify that protocol is set up correctly.

Reference - Configuration Parameters Interface

Reference topics for the Log Collection configuration parameter and system command user interface:

- Log Collector Configuration Parameters Interface:The Log Collector Config Service view is the view on which you maintain all the Log Collector configuration parameters.
- Log Collection Service System View Interface: The Log Collector Systems view is the view on which you execute all the Log Collector system commands and review the status of the service.

Log Collector Configuration Parameters Interface

This topic points you to the reference documentation for the Log Collection parameter user interface.

The Log Collector Config Service view is the view on which you maintain all the Log Collector parameters. The following diagrams show you where to find the documentation for each tab on the Parameters view.

Tab	Description	Described in this Guide
General	High-level parameters that govern the operation of the Log Collector service and each collection protocol.	Log Collection Configuration Guide

Tab	Description	Described in this Guide
Remote/Local Collectors	For Local Collector, the **Remote Collectors** tab defines which Remote Collectors (RCs) the Local Collector pulls events from. For Remote Collector, **Local Collectors** tab defines which Local Collectors (LCs) the Remote Collector pushes events to.	Log Collection Deployment Guide
Event Sources	Supported collection protocols.	AWS (CloudTrail) Collection Configuration Guide Check Point Collection Configuration Guide File Collection Protocol Configuration Guide Netflow Collection Configuration Guide ODBC Collection Configuration Guide SDEE Collection Configuration Guide SNMP Collection Configuration Guide VMware Collection Configuration Guide Windows Collection Configuration Guide Windows Legacy and NetApp Collection Configuration Guide
Settings	Lockbox, Encryption Key, and Certificates	Log Collection Configuration Guide

Log Collection Service System View Interface

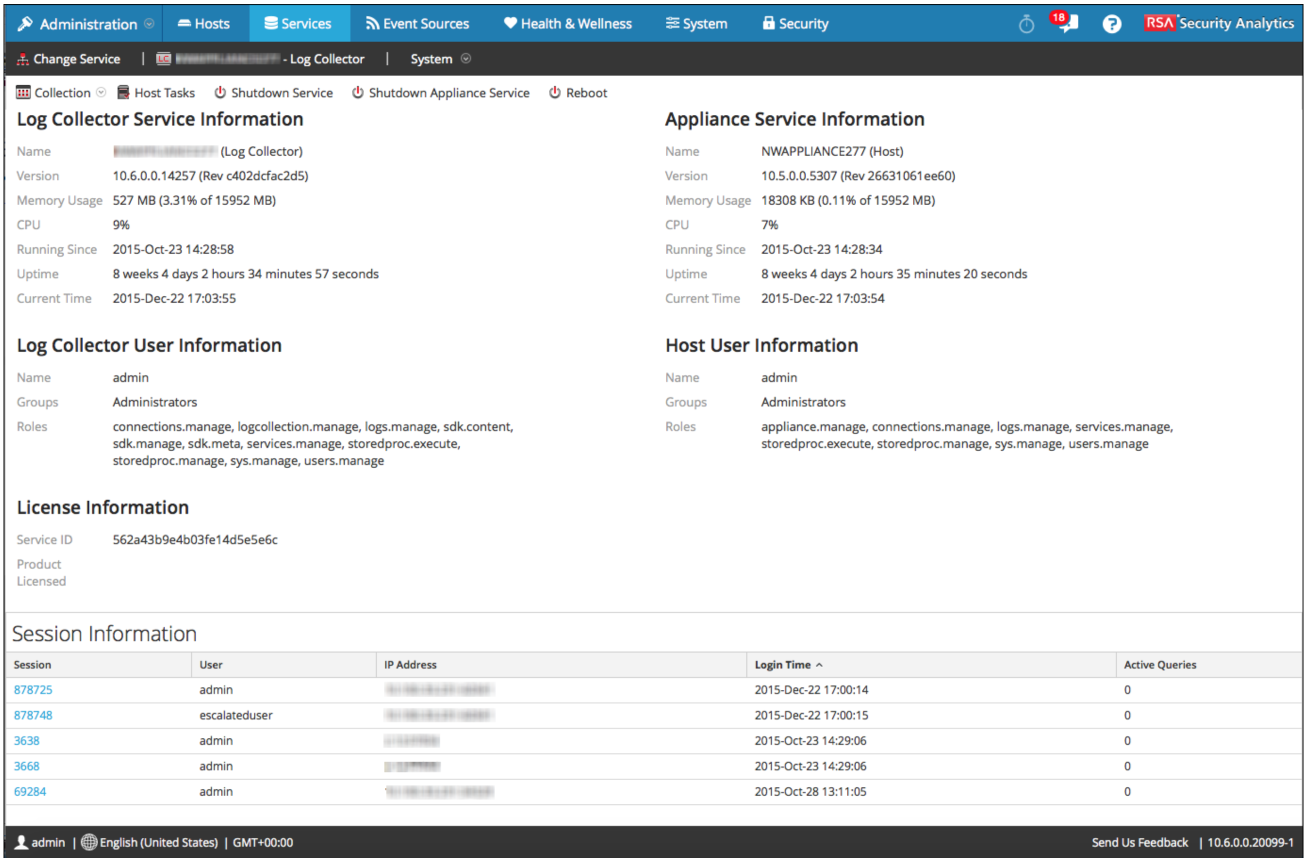
This topic introduces features in the System view that pertain specifically to Log Collection.

A Log Collector is a service that runs on a Log Decoder host (referred to as a Local Collector) or sends events from a Remote Collector to a Local Collector, and is configured and managed in a similar way to a Log Decoder. Therefore, most of the information in this section refers to Decoders in general. Differences for Log Collectors are noted. To display this view:

1. In the **Security Analytics** menu, select **Administration** > **Services**.

   The Administration services view is displayed.

2. Click the checkbox next to a Log Collector, and select **View** > **System**.



Log Collector Service Information

Name	[redacted] (Log Collector)
Version	10.6.0.0.14257 (Rev c402dcfac2d5)
Memory Usage	527 MB (3.31% of 15952 MB)
CPU	9%
Running Since	2015-Oct-23 14:28:58
Uptime	8 weeks 4 days 2 hours 34 minutes 57 seconds
Current Time	2015-Dec-22 17:03:55

Appliance Service Information

Name	NWAPPLIANCE277 (Host)
Version	10.5.0.0.5307 (Rev 26631061ee60)
Memory Usage	18308 KB (0.11% of 15952 MB)
CPU	7%
Running Since	2015-Oct-23 14:28:34
Uptime	8 weeks 4 days 2 hours 35 minutes 20 seconds
Current Time	2015-Dec-22 17:03:54

Log Collector User Information

Name	admin
Groups	Administrators
Roles	connections.manage, logcollection.manage, logs.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Host User Information

Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

License Information

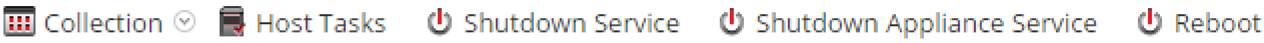
Service ID	562a43b9e4b03fe14d5e5e6c
Product Licensed	

Session Information

Session	User	IP Address	Login Time ^	Active Queries
878725	admin	[redacted]	2015-Dec-22 17:00:14	0
878748	escalateduser	[redacted]	2015-Dec-22 17:00:15	0
3638	admin	[redacted]	2015-Oct-23 14:29:06	0
3668	admin	[redacted]	2015-Oct-23 14:29:06	0
69284	admin	[redacted]	2015-Oct-28 13:11:05	0

admin | English (United States) | GMT+00:00 Send Us Feedback | 10.6.0.0.20099-1

Service Info Toolbar



The Service Info toolbar shares many options with the Service System view toolbar. The following table describes the options which are unique to the Service Info toolbar.

Action	Description
Collection	Displays a list of the collection protocols and gives you the options: • **Start** - start collecting event data from a stopped protocol. • **Stop** - stop collecting event data from a started protocol. • **Pause** - pause the collection of event data from a started protocol. Please refer to the Step 5. Start Collection Services and Enable Automatic Start

Troubleshoot Log Collection

This topic describes the format and content of Log Collection Troubleshooting. Security Analytics informs you of Log Collector problems or potential problems in the following two ways.

- Log files.
- Health and Wellness Monitoring views.

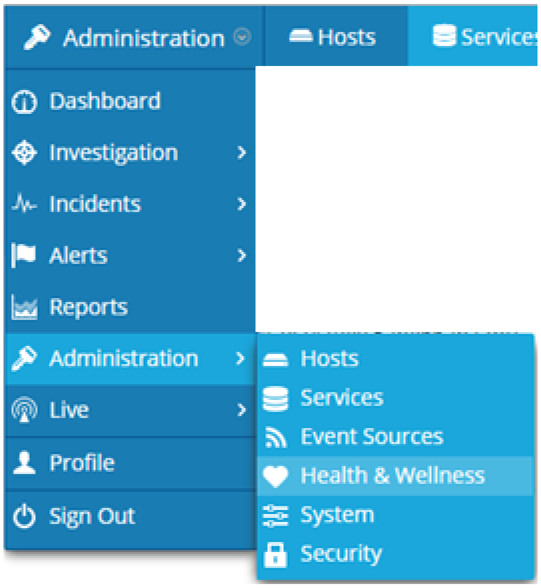
Log Files

If you have an issue with a particular event source collection protocol, you can review debug logs to investigate this issue. Each event source has a Debug parameter that you can enable (set parameter to On or Verbose) to capture these logs.

Caution: Only enable debugging if you have a problem with this event source and you need to investigate this problem. If you have Debug enabled all the time it will adversely affect the performance of the Log Collector.

Health and Wellness Monitoring

Health and Wellness monitoring makes you aware of potential hardware and software problems in a timely manner so that you can avoid to outages. RSA recommends that you monitor the Log Collector statistical fields to make sure that the service is operating efficiently and is not at or near the maximum values you have configured. You can monitor the following statistics (Stats) described in the **Administration > Health & Wellness** view.



Sample Troubleshooting Format

Security Analytics returns the following types of error messages in the log files for.

Log Messages	`timestamp failure (LogCollection) Message-Broker Statistics: ...`
	`timestamp failure (AMQPClientBaseLogCollection): ...`
	`timestamp failure (MessageBrokerLogReceiver): ...`

Possible Cause	The Log Collector cannot reach the Message Broker because the Message Broker: • stopped running. • has erroneous connection settings.

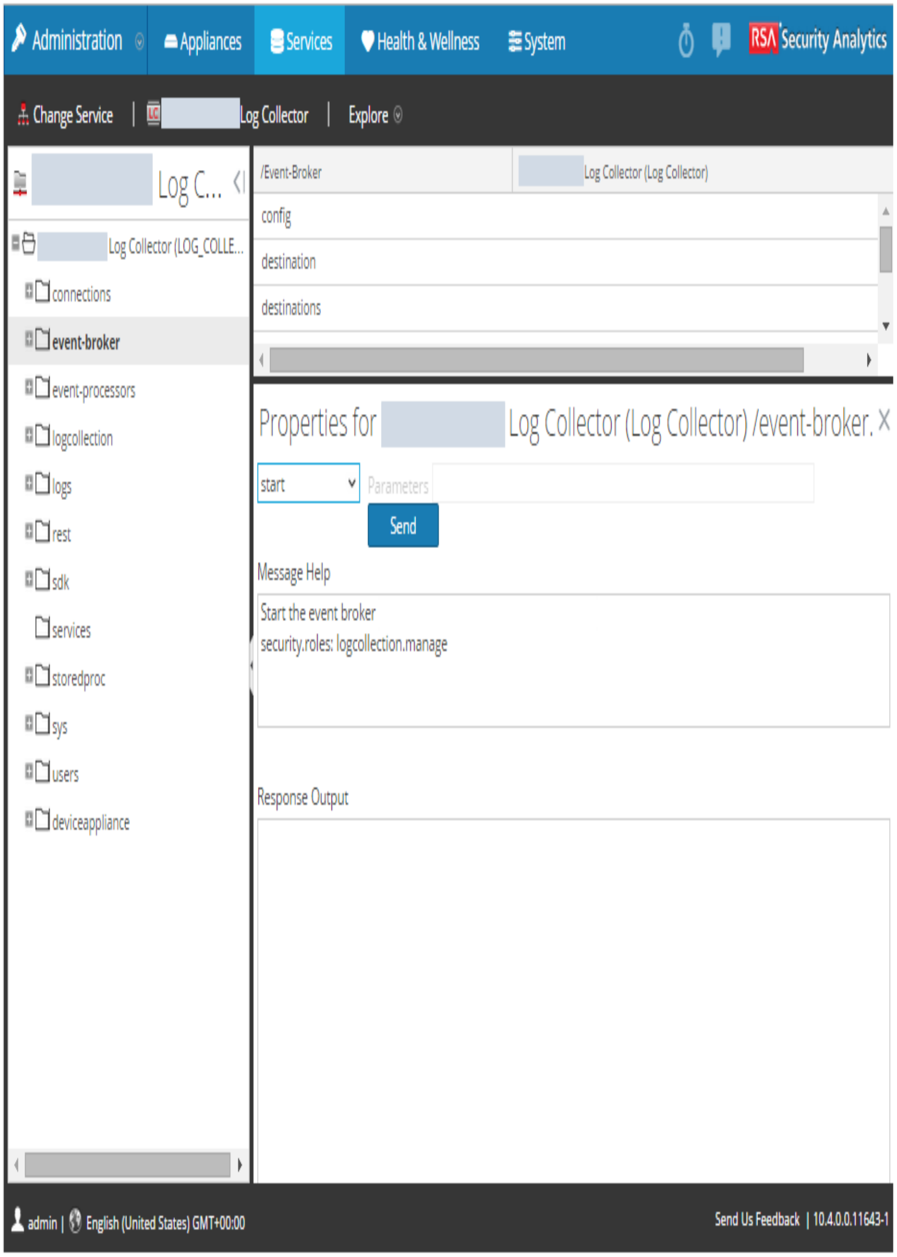
Solutions

1. `<use the="the" initctl="initctl" command="command" on="on" console="console" to="to" check="check" status="status" of="of" message="message" broker="broker" shell="shell" console.="console.">returns the following if the message broker is not running:</use>`

```
prompt$ status rabbitmq


rabbitmq start/running, process 10916
```

2. Start the RabbitMQ Message Broker on event-broker node in the Explore view:



Properties for [redacted] Log Collector (Log Collector) /event-broker.

start
Parameters
Send

Message Help

Start the event broker
security.roles: logcollection.manage

Response Output

Log Collection Deployment Guide

This guide tells you how to deploy Log Collection in your Security Analytics domain. It provides detailed deployment instructions (that is, how to set up Local and Remote Collectors). It does not contain any global Log Collection or individual collection protocol information.

This guide tells you how to set up the Log Collection deployments currently available in Security Analytics.

This guide does not tell you how to:

- Get started by creating the basic, minimum deployment and configuration. This information is in the Log Collection Getting Started Guide.
- Configure Log Collection as a whole after deployment. This information is in the Log Collection Configuration Guide.
- Configure individual collection protocols. Instructions are in the individual Log Collection Guides:
  - AWS (CloudTrail) Collection Configuration Guide
  - Check Point Collection Configuration Guide
  - File Collection Protocol Configuration Guide
  - Netflow Collection Configuration Guide
  - ODBC Collection Configuration Guide
  - SDEE Collection Configuration Guide
  - SNMP Collection Configuration Guide
  - VMware Collection Configuration Guide
  - Windows Collection Configuration Guide
  - Windows Legacy and NetApp Collection Configuration Guide
  - Configuration Guides for each supported event source guide.

    See the Event Source Configuration Guide space on RSA Link for these guides.

The Basics

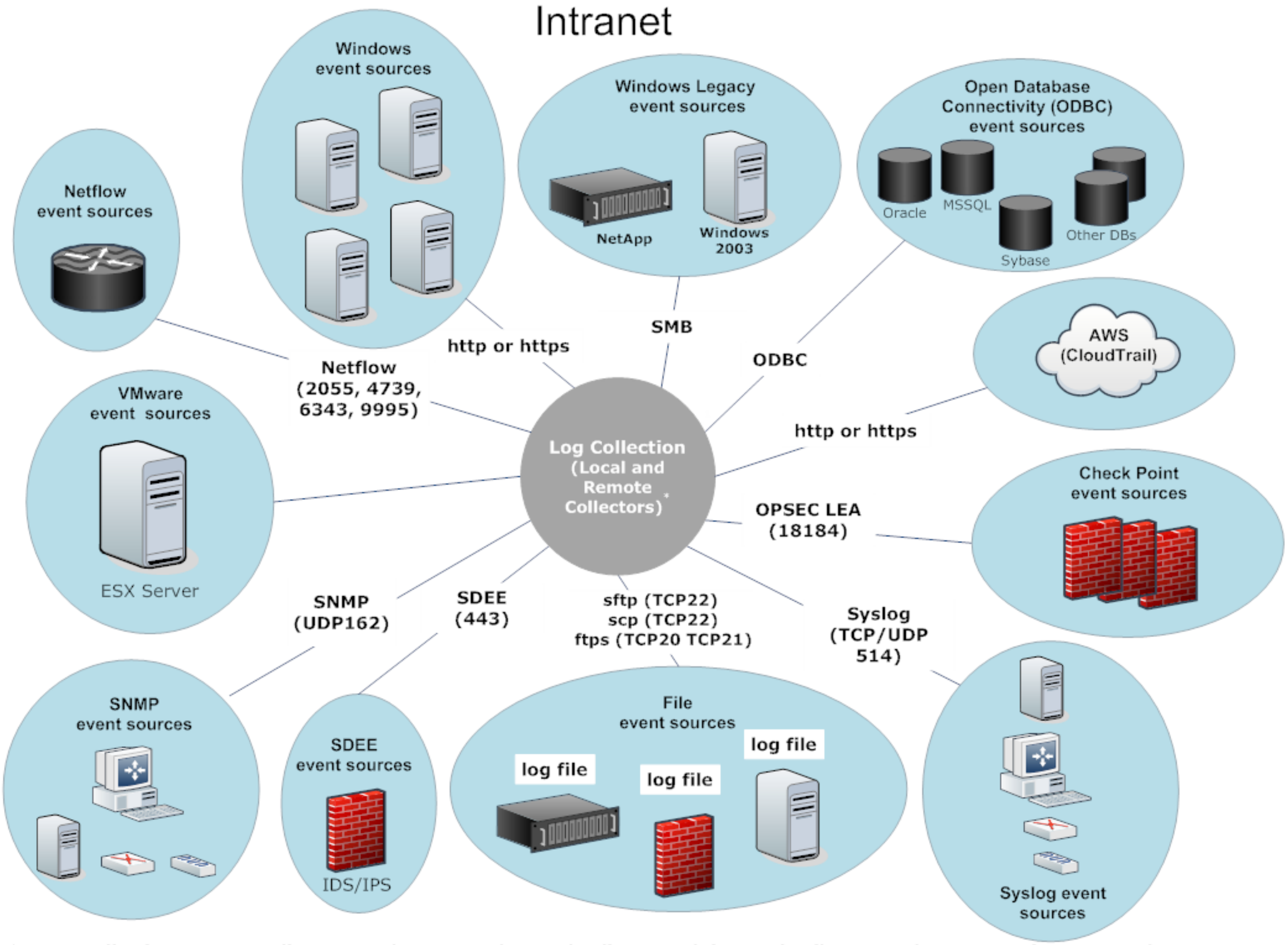
This topic outlines the basic procedures you complete to deploy Log Collection to meet the needs of your enterprise

How You Deploy Log Collection

You can deploy Log Collection according to needs and preferences of your enterprise. This includes deploying Log Collection across multiple locations and collect data from varying sets of event sources. You do this by setting up a Local Collector with one or many Remote Collectors.

Components of Log Collection

The following figure shows all the components involved in event collection through the Security Analytics Log Collector.



*In Log Collection, Remote Collectors send events to the Local Collector and the Local Collector sends events to the Log Decoder.

For more information on Log Collector Event Source content, see the topic **Configure Event Sources to Send Events to Security Analytics** in the *Log Collection Configuration Guide*.

Local and Remote Collectors

The following figure illustrates how the Local and Remote Collectors interact to collect events from all of your locations.

In this scenario, log collection from various protocols like Windows, ODBC, and so on, is performed through both the Remote Collector and Log Collector service. If the log collection is done by the Local Collector, it is forwarded to the Log Decoder service, just like the local deployment scenario. If the log collection is done by a Remote Collector, there are two methods in which these are transferred to the Local Collector:

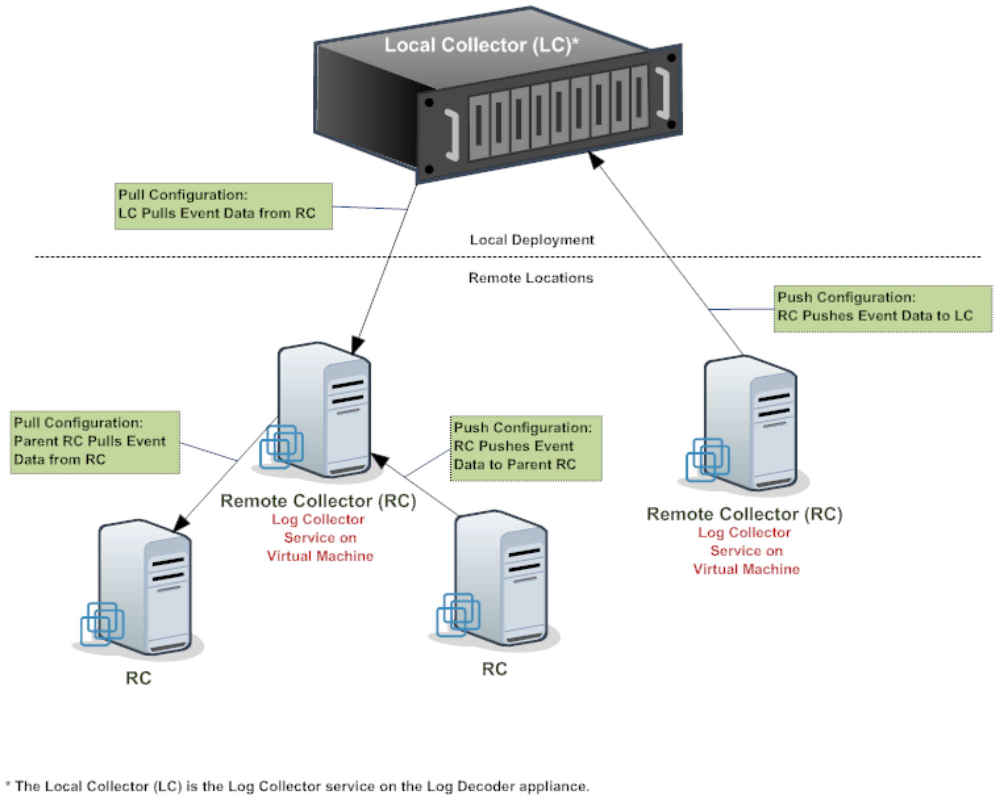
- **Pull Configuration -** From a Local Collector, you select the Remote Collectors from which you want to pull events.
- **Push Configuration -** From a Remote Collector, you select the Local Collector to which you want to push events.

You can configure one or more Remote Collectors to push event data to a Local Collector, or you can configure a Local Collector to pull event data from one or more Remote Collectors.

For 10.4 Remote Collector and later releases, you can set up a chain of Remote Collectors for which you can configure:

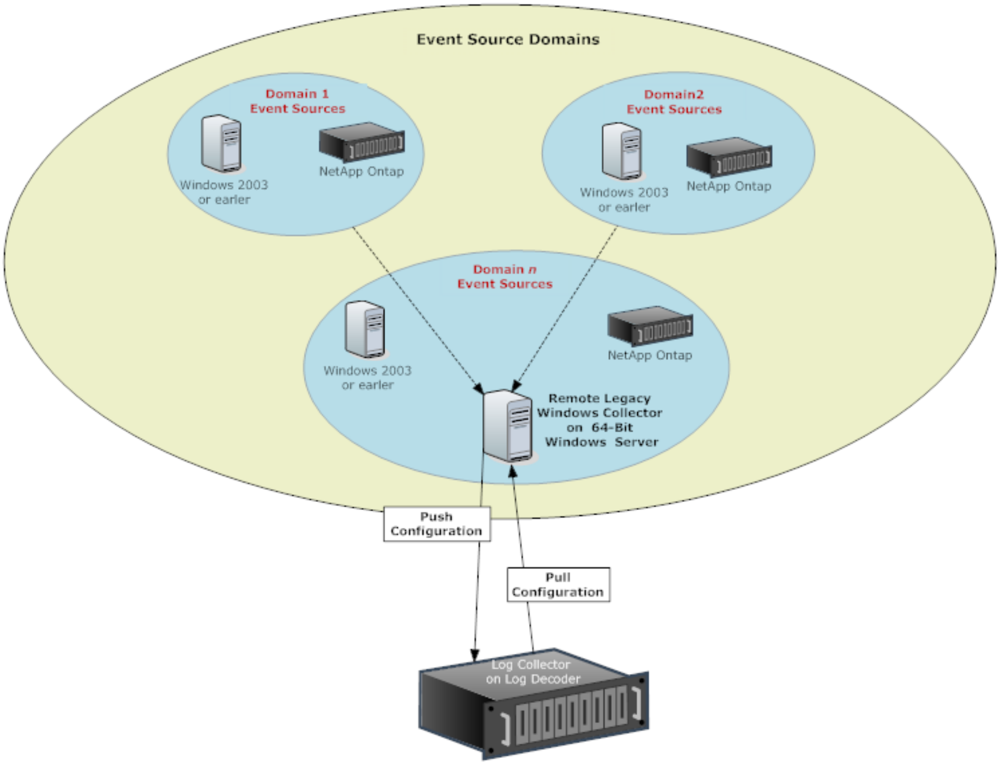
- One or more Remote Collectors to push event data to a Remote Collector.
- A Remote Collector to pull event data from one or more Remote Collectors.

Note: For Remote Collector chaining, you can only:
Push data from a 10.4 or later Remote Collector to other 10.4 or later Remote Collectors or 10.4 or later Local Collectors.
Use a 10.4 or later Remote Collector to pull data from one or more 10.4 or later Remote Collectors.



Windows Legacy Remote Collector

The following figure illustrates the deployment required to collect events from Windows Legacy (Windows 2003/2000 and NetApp) event sources).



Procedures

This topic introduces the high-level steps that you need to complete to deploy and configure Log Collection

Deployment Checklist

Before you deploy Log Collection, make sure that the Log Decoder:

- is capturing data. Refer to the *Decoder and Log Decoder Configuration Guide* for more information explaining how data is captured.
- has the Log Decoder content loaded.
- is properly licensed. Refer to the *Licensing Guide* for more information on the licensing process.

Step Description	√
Access Local and Remote Collectors	

Step Description	√
Configure Local and Remote Collectors. • Pull Events from Remote Collectors. • Push Events to Local Collectors.	
Configure a Chain of Remote Collectors.	
Throttle Remote Collector to Local Collector Bandwidth.	

Access Local Collectors and Remote Collectors

This topic tells how to access Local Collectors and Remote Collectors so that you can configure them. You can access a Local Collector or Remote Collector by selecting the service that you want in the **Administration > Services** view. If you do not see a Local Collector or Remote Collector in the Services view, you need to add it.

After completing this procedure, you will have:

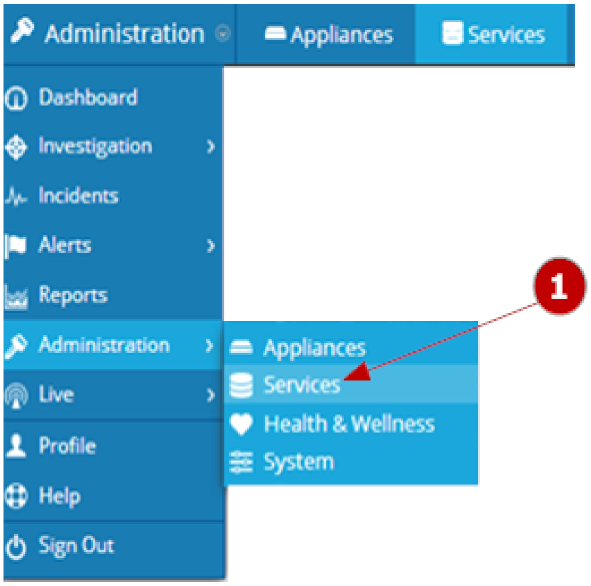
- Added a Local Collector/Remote Collector service.
- Added a Legacy Windows Remote service

Procedures

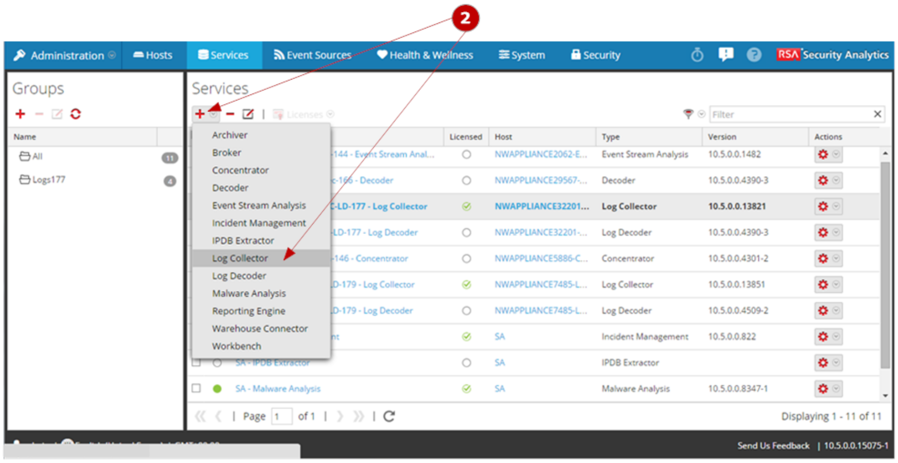
Add a Local Collector/Remote Collector

You add a Local Collector by adding the Log Collector service to a Log Decoder host in Security Analytics.
You add a Remote Collector by adding the Log Collector service to a host in Security Analytics.

Note: The dialog boxes are identical for Local Collectors, Remote Collectors, and Legacy Windows Collectors.



1 Access the **Services** view.

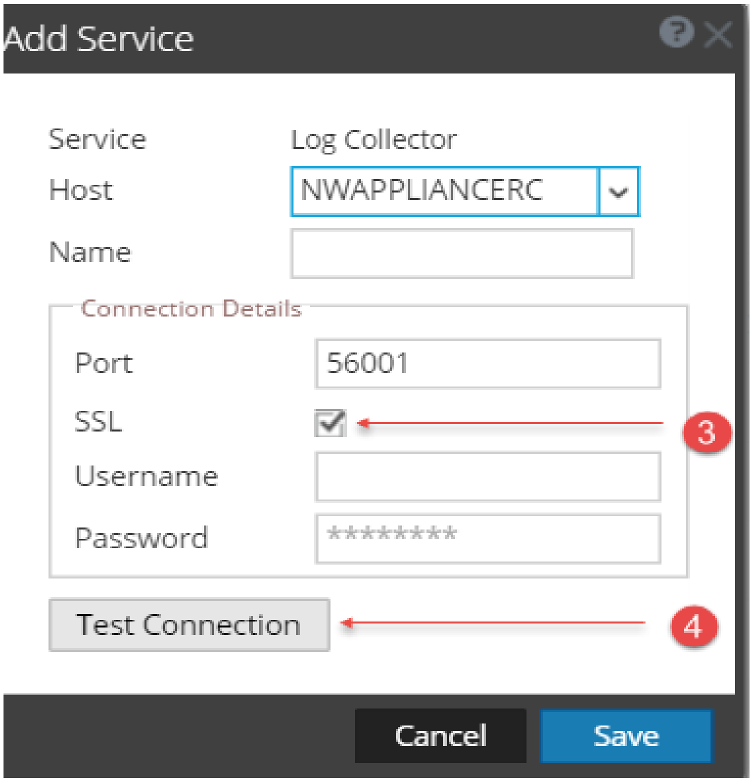


	Licensed	Host	Type	Version	Actions
-144 - Event Stream Anal...	○	NWAPPLIANCE2062-E...	Event Stream Analysis	10.5.0.0.1482	⚙
c-166 - Decoder	○	NWAPPLIANCE29567-...	Decoder	10.5.0.0.4390-3	⚙
C-LD-177 - Log Collector	✓	NWAPPLIANCE32201...	Log Collector	10.5.0.0.13821	⚙
LD-177 - Log Decoder	○	NWAPPLIANCE32201-...	Log Decoder	10.5.0.0.4390-3	⚙
-146 - Concentrator	○	NWAPPLIANCE5886-C...	Concentrator	10.5.0.0.4301-2	⚙
D-179 - Log Collector	✓	NWAPPLIANCE7485-L...	Log Collector	10.5.0.0.13851	⚙
D-179 - Log Decoder	○	NWAPPLIANCE7485-L...	Log Decoder	10.5.0.0.4509-2	⚙
nt	✓	SA	Incident Management	10.5.0.0.822	⚙
SA - IPDB Extractor	○	SA	IPDB Extractor		⚙
SA - Malware Analysis	✓	SA	Malware Analysis	10.5.0.0.8347-1	⚙

Page 1 of 1

Displaying 1 - 11 of 11

2 Click + to open the **Add Service** dialog and select **Log Collector**.



Add Service

Service: Log Collector

Host: NWAPPLIANCERC

Name:

Connection Details

Port: 56001

SSL: ☑

Username:

Password: *********

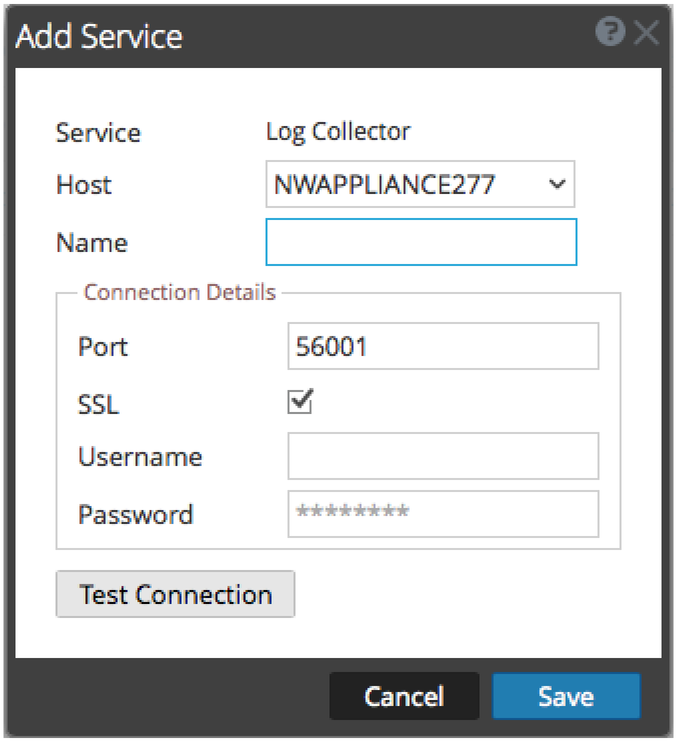
3 Define the connection details of the Log Collector service on a Local Collector.

4 Click **Test Connection**. If the connection is valid you will see **Test connection successful**. If the connection fails you will see **Fail**. If it failed, make sure that the Log Decoder host is running and that you have entered the correct information on the **Add Service** dialog and click **Save** again.

To add a Local Collector or Remote Collector:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** view, select + in the toolbar.

   The **Add Service** dialog is displayed.



Add Service

Service: Log Collector

Host: NWAPPLIANCE277

Name:

Connection Details

Port: 56001

SSL: ☑

Username:

Password: *********

3. In the **Add Service** dialog, provide the following information.

Field	Description
Service	Select Log Collector as the service type.
Name	Type name you want to assign to the service.
Host	Select the log collector host that you added to the Hosts view where the corresponding log collector service resides.
Port	Default port is 50001 for clear text and 56001 for SSL encrypted.
SSL	Select SSL if you want Security Analytics to communicate with the host using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates.
(Optional)Username	Type the username of the Local Collector.
(Optional) Password	Type the password of the Local Collector.

4. Click **Test Connection** to determine if Security Analytics connects to the service.

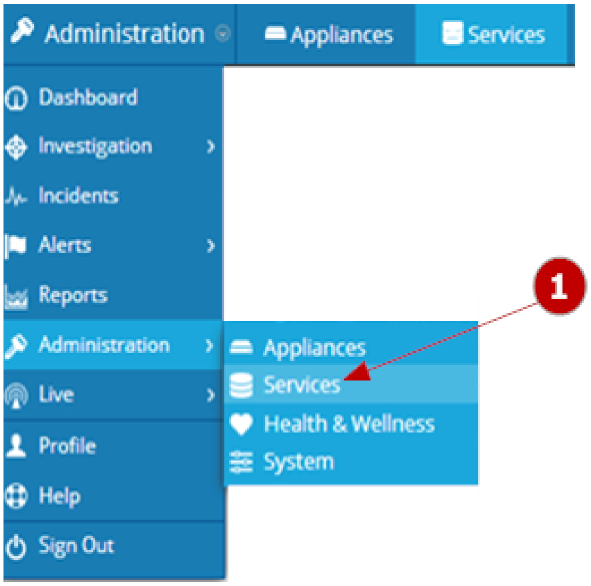
5. When the result is successful, click **Save**.

   If the test is unsuccessful, edit the service information and retry.

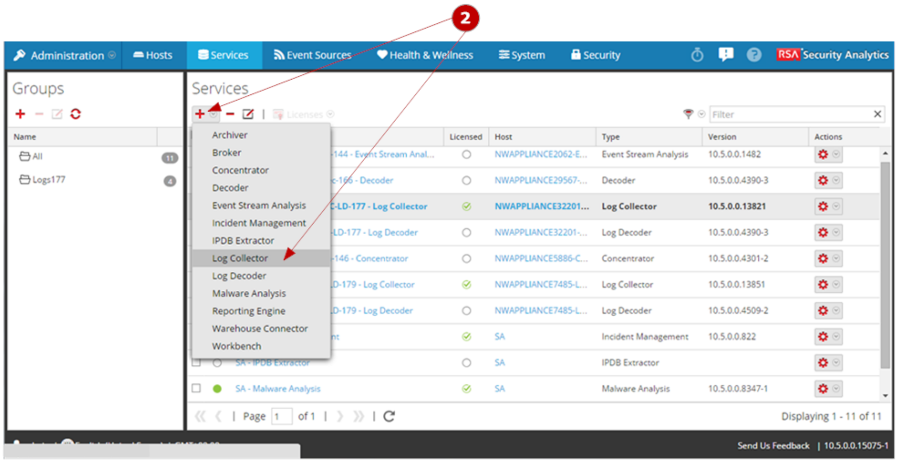
Add a Legacy Windows Remote Collector

You add a Remote Collector by adding the Log Collector service to a remote host.

> **Note:** Before you add a Legacy Windows Remote Collector, you must install the Security Analytics Legacy Windows Collector on a physical or virtual Windows 2008 SP1 64-bit server using the **SALegacyWindowsCollector-*version-number.exe***. You download the **SALegacyWindowsCollector-*version-number.exe*** from Download Central (please refer to the SA-v10.6 Legacy Windows Update and Installation Instructions.)



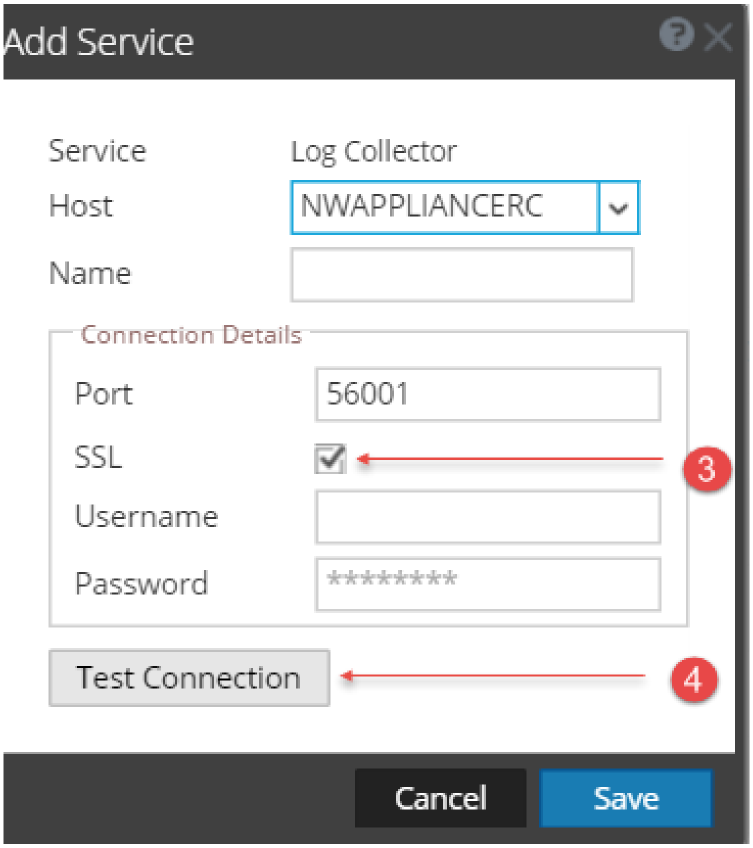
1 Access the **Services** view.



	Licensed	Host	Type	Version	Actions
-144 - Event Stream Anal...	○	NWAPPLIANCE2062-E...	Event Stream Analysis	10.5.0.0.1482	
c-166 - Decoder	○	NWAPPLIANCE29567-...	Decoder	10.5.0.0.4390-3	
C-LD-177 - Log Collector	✓	NWAPPLIANCE32201...	Log Collector	10.5.0.0.13821	
LD-177 - Log Decoder	○	NWAPPLIANCE32201-...	Log Decoder	10.5.0.0.4390-3	
-146 - Concentrator	○	NWAPPLIANCE5886-C...	Concentrator	10.5.0.0.4301-2	
D-179 - Log Collector	✓	NWAPPLIANCE7485-L...	Log Collector	10.5.0.0.13851	
D-179 - Log Decoder	○	NWAPPLIANCE7485-L...	Log Decoder	10.5.0.0.4509-2	
nt	✓	SA	Incident Management	10.5.0.0.822	
SA - IPDB Extractor	○	SA	IPDB Extractor		
SA - Malware Analysis	✓	SA	Malware Analysis	10.5.0.0.8347-1	

Page 1 of 1 Displaying 1 - 11 of 11

2 Click + to open the **Add Service** dialog and select **Log Collector**.



Service Log Collector

Host NWAPPLIANCERC

Name

Connection Details

Port 56001

SSL ☑

Username

Password ********

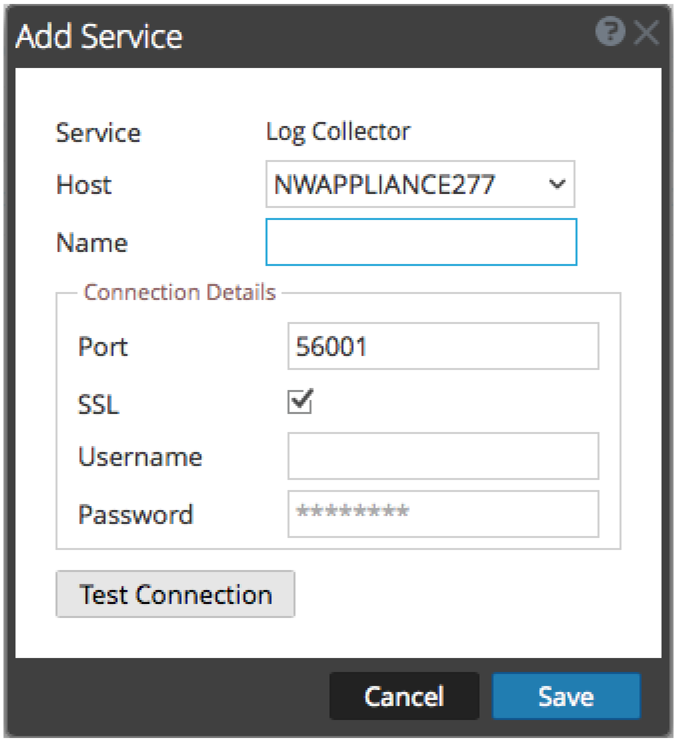
3 Define the details of the Log Collection service on a Remote Collector.

4 Click **Test Connection**. If the connection is valid you will see **Test connection successful**. If the connection fails you will see **Fail**.If it failed, make sure that the Log Decoder host is running and that you have entered the correct information on the **Add Service** dialog and click **Save** again.

To add a Remote Collector:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** view, select + in the toolbar.

   The **Add Service** dialog is displayed.



Service: Log Collector

Host: NWAPPLIANCE277

Name:

Port: 56001

SSL: ☑

Username:

Password: *********

3. In the **Add Service** dialog, provide the following information.

Field	Description
Service	Select Log Collector as the service type.
Name	Type the service name.
Host	Select a remote host.
Port	Default port is 50001 for clear text and 56001 for SSL encrypted.
SSL	Select **SSL** if you want Security Analytics to communicate with the host using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates.
(Optional) Username	Type the username of the Remote Collector.
(Optional) Password	Type the password of the Remote Collector.

4. Click **Test Connection** to determine if Security Analytics connects to the service.

5. When the result is successful, click **Save**.

   If the test is unsuccessful, edit the service information and retry.

Provisioning Local Collectors and Remote Collectors

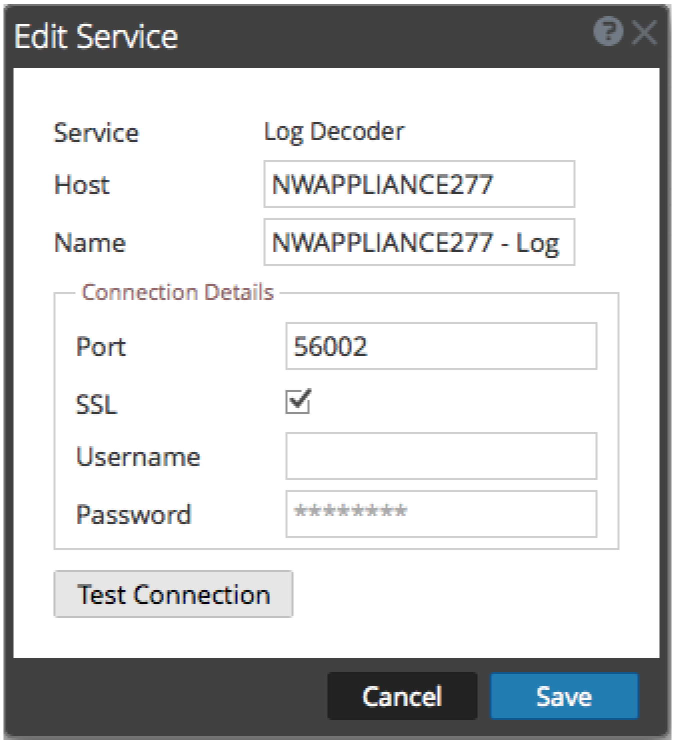
The Security Analytics server verifies if an appliance has a Log Decoder service. If there is a Log Decoder service, it becomes a Local Collector. If a Log Decoder service is missing, it becomes a Remote Collector. A local Log Collector has an Event Destination and by default goes to the Local Log Decoder service. A Remote Collector does not have an Event Destination. The Security Analytics server identifies a Legacy Windows Collector as a Remote Collector.

> **Note:** Remote Collector checkbox has been removed from the Edit Service dialog box. Security Analytics dynamically determines whether it is a Local or Remote Collector.

To edit a Local Collector or Remote Collector:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** view, select ✎ in the toolbar.

   The **Edit Service** dialog is displayed.



Edit Service

Service Log Decoder

Host NWAPPLIANCE277

Name NWAPPLIANCE277 - Log

Connection Details

Port 56002

SSL ☑

Username

Password ********

3. In the **Edit Service** dialog, provide the following information.

Field	Description
Service	Select Log Collector as the service type.
Host	Select a Log Decoder host.

Field	Description
Name	Type name you want to assign to the service.
Port	Default port is 50001 for clear text and 56001 for SSL encrypted.
SSL	Select **SSL** if you want Security Analytics to communicate with the host using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates.
(Optional) Username	Type the username of the Local Collector.
(Optional) Password	Type the password of the Local Collector.

4. Click **Test Connection** to determine if Security Analytics connects to the service.
5. When the result is successful, click **Save**.
   If the test is unsuccessful, edit the service information and retry.

Configure Local and Remote Collectors

This topic tells you how to configure Local and Remote Collectors.

When you deploy Log Collection, you must configure the Log Collectors to collect the log events from various event sources, and to deliver these events reliably and securely to the Log Decoder host, where the events are parsed and stored for subsequent analysis.

You can configure one or more Remote Collectors to push event data to a Local Collector, or you can configure a Local Collector to pull event data from one or more Remote Collectors.

Return to Procedures

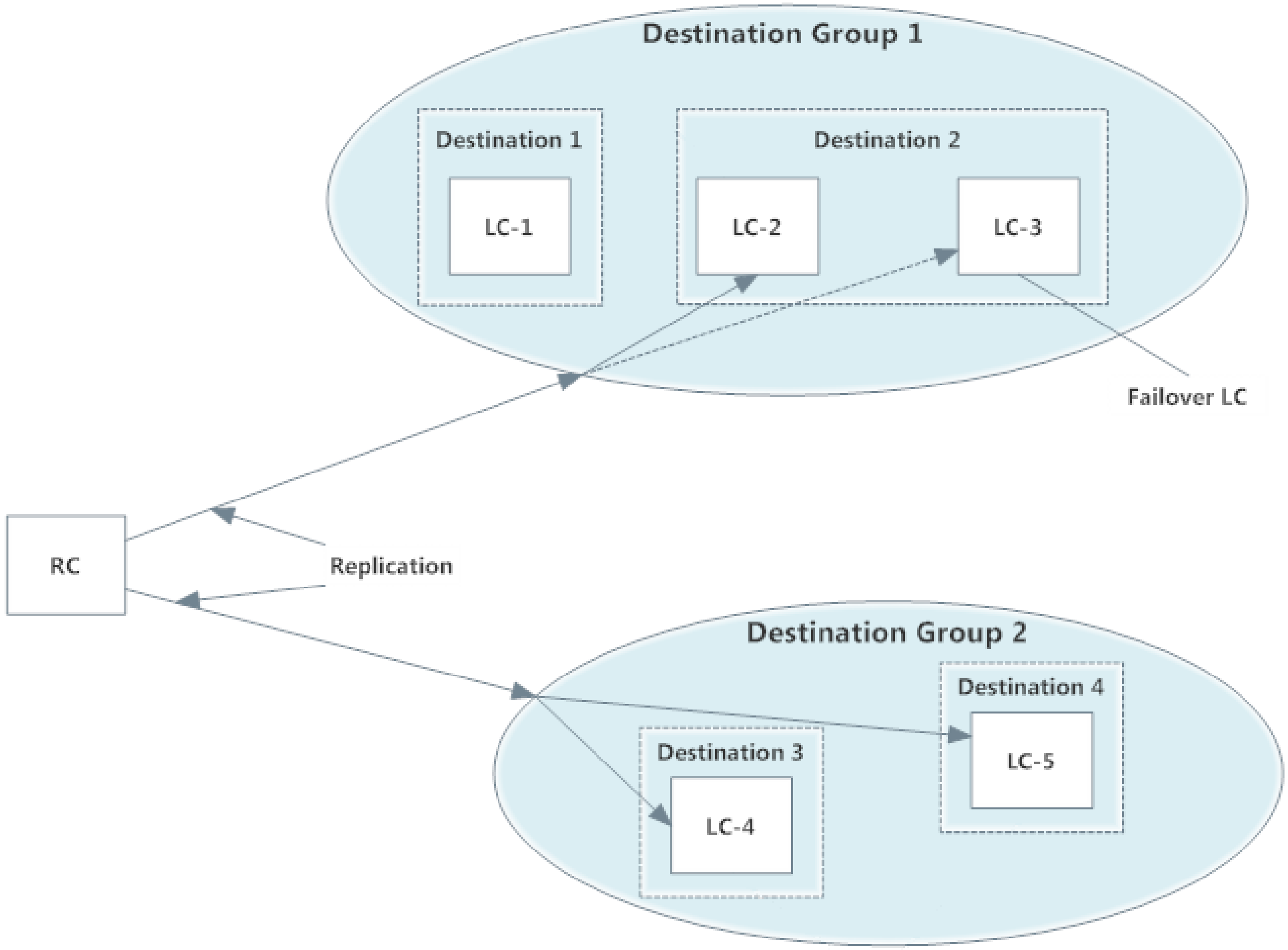
This topic tells you how to:

- Configure Local Collector to Pull Events from Remote Collector
  If you want a Local Collector to pull events from Remote Collector, you set this up in the Remote Collectors tab of the Local Collector's Configuration view.
- Configure Remote Collector to Push Events to Local Collectors
  If you want a Remote Collector to push events to a Local Collector, you set this up in the Local Collector tab of the Remote Collector's Configuration view. In the Push configuration, you can also:

  - Configure Failover Local Collector for Remote Collector
    You set up a destination made up of local collectors. When the primary Local Collector is unreachable, the Remote Collector attempts to connect to each local collector in this destination until it makes a successful connection.
  - Configure Replication
    You set up multiple destination groups so that Security Analytics replicates the event data in each group. If the connection to one of the destination groups fails, you can recover the required data because it is replicated in the other destination group.
  - Configure Log Routing for Specific Protocols
    You set up multiple destinations in a destination group to direct event data to specific locations according to protocol type.
- Configure Chain of Remote Collectors
  You can set up a chain of Remote Collectors to push event data to a Local Collector, or you can configure a Local Collector to pull event data from a chain of Remote Collectors.
  - One or more Remote Collectors to push event data to a Remote Collector.
  - A Remote Collector to pull event data from one or more Remote Collectors.

Failover and Replication

The following figure illustrates a Remote Collector configured for failover and replication.



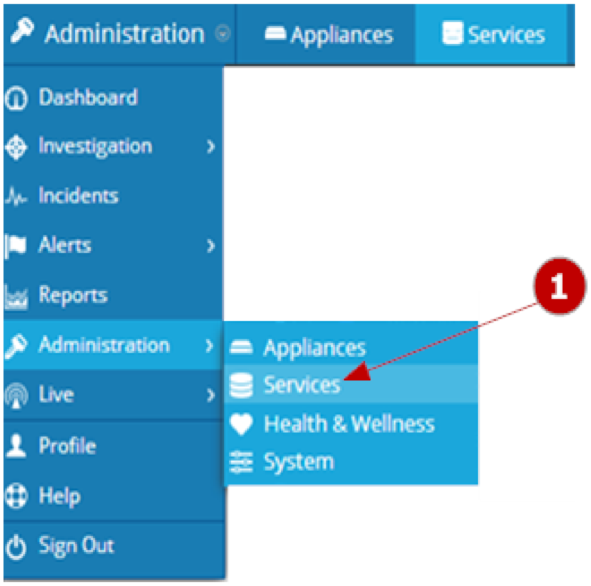
In Destination Group 1, LC-2 and LC-3 are the failover local collectors configured for LC-1. If the Remote Collector cannot connect to LC1 for some reason, the Remote Collector attempts to connect to LC-2 or LC-3 until it makes a successful connection.

Destination Group 1 and Destination Group 2 are configured for replication. If Local Collector in Destination Group 1 fails, you can use the data replicated in the Local Collector in the destination Group 2.

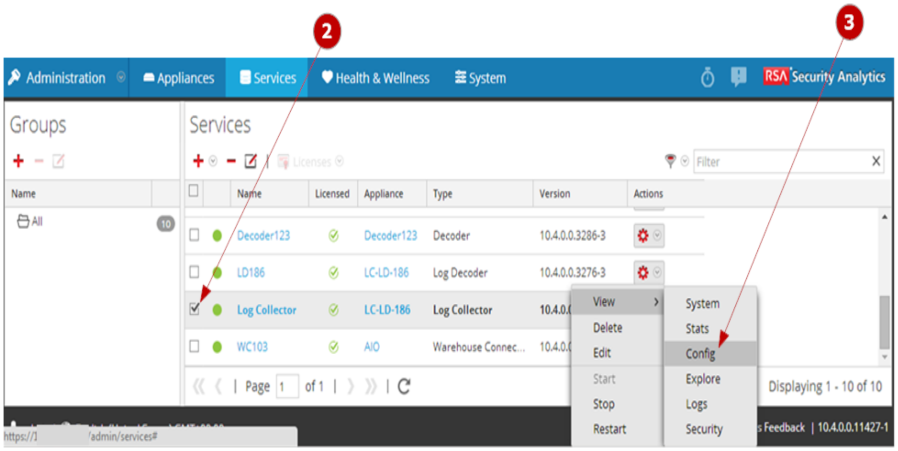
Note: You can also set up log routing so that event data for specific protocols is sent to specific destinations.

Procedure

You choose the Log Collector, that is a Local Collector (LC) or Remote Collector (RC), for which you want to define deployment parameters in the Services view. The following procedure shows you how to navigate to the Services view, select a Local or Remote Collector, and display the deployment parameter interface for that service.



1 Access the **Services** view.



Name	
All	10

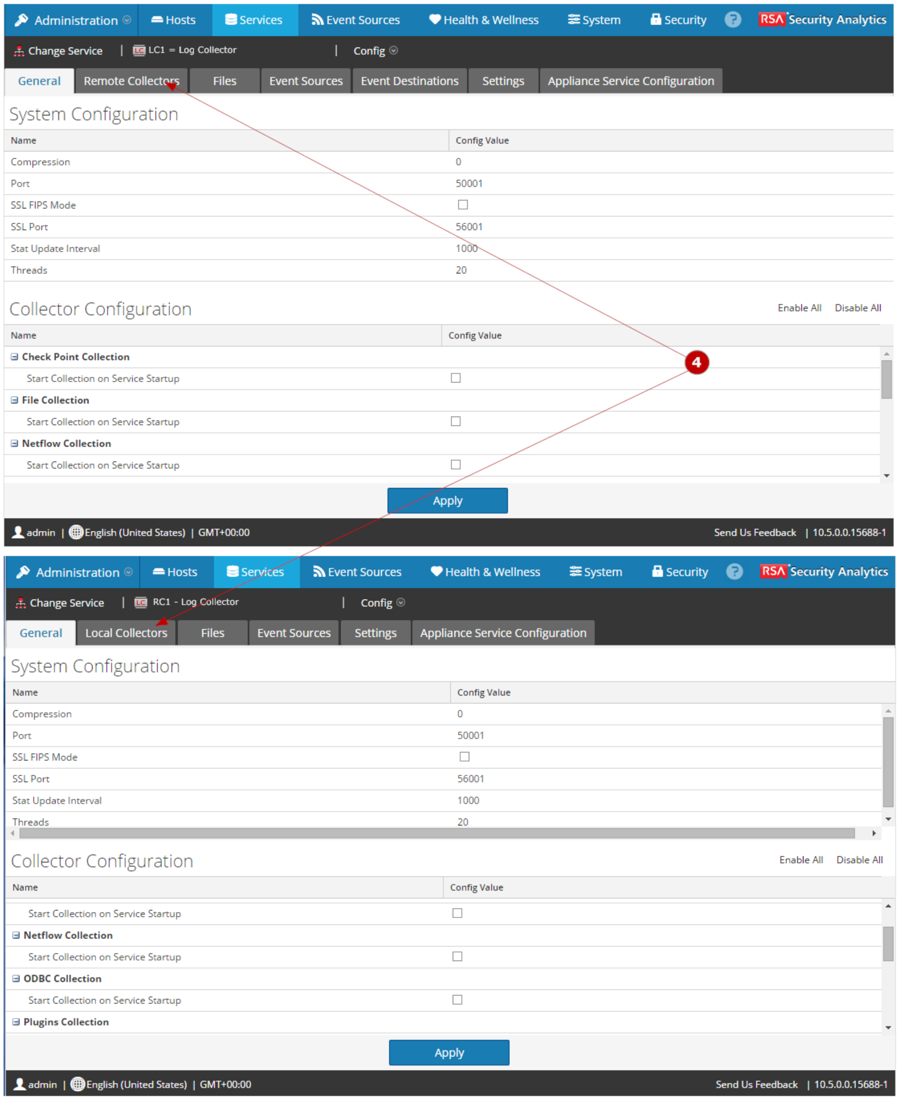
☐		Name	Licensed	Appliance	Type	Version
☐	●	Decoder123	✓	Decoder123	Decoder	10.4.0.0.3286-3
☐	●	LD186	✓	LC-LD-186	Log Decoder	10.4.0.0.3276-3
☑	●	Log Collector	✓	LC-LD-186	Log Collector	10.4.0.
☐	●	WC103	✓	AIO	Warehouse Connec...	10.4.0.

Page 1 of 1

Displaying 1 - 10 of 10

2 Select a log collector service.

3 Click ⌄ under **Actions** and select **View** > **Config** to display the Log Collection configuration parameter tabs.



System Configuration

Name	Config Value
Compression	0
Port	50001
SSL FIPS Mode	□
SSL Port	56001
Stat Update Interval	1000
Threads	20

Collector Configuration

Name	Config Value
⊟ **Check Point Collection**	
Start Collection on Service Startup	□
⊟ **File Collection**	
Start Collection on Service Startup	□
⊟ **Netflow Collection**	
Start Collection on Service Startup	□

System Configuration

Name	Config Value
Compression	0
Port	50001
SSL FIPS Mode	□
SSL Port	56001
Stat Update Interval	1000
Threads	20

Collector Configuration

Name	Config Value
Start Collection on Service Startup	□
⊟ **Netflow Collection**	
Start Collection on Service Startup	□
⊟ **ODBC Collection**	
Start Collection on Service Startup	□
⊟ **Plugins Collection**	

4 In step 2, if you selected a log collector service for a:

- Local Collector, the **Remote Collectors** tab is displayed. Select the Remote Collectors from which the Local Collector pulls events in this tab.

- Remote Collector, the **Local Collectors** are displayed. Select the Local Collectors to which the Remote Collector pushes events in this tab.

Parameters

Reference - Remote/Local Collectors Configuration Parameters Interface

Pull Events from Remote Collector

This topic tell

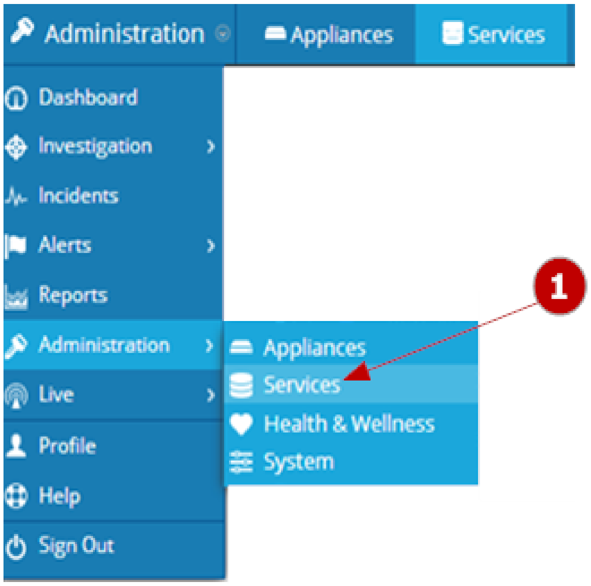
s you how to configure a Local Collector to pull Events from a Remote Collector.

After completing this procedure, you will have configured a Local Collector to pull Events from a Remote Collector.

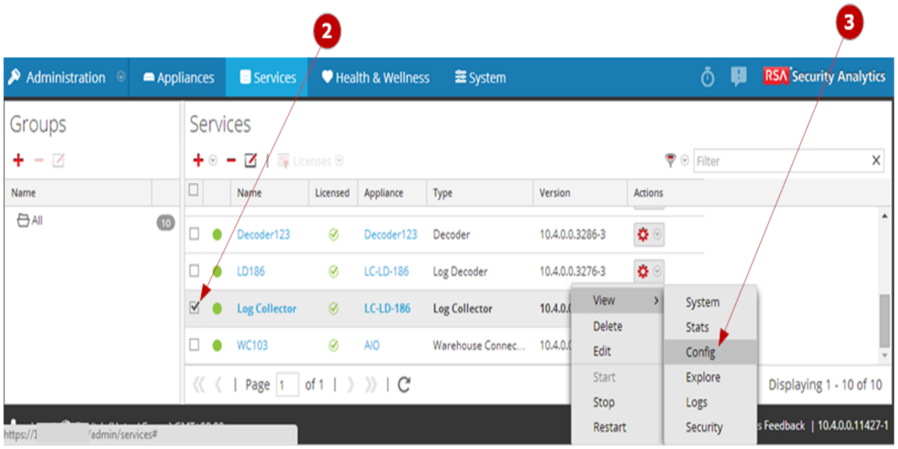
Configure Local Collector to Pull Events from Remote Collector

You can configure a Local Collector to pull event data from one or more Remote Collectors.

The following figures shows you how to configure a Local Collector to pull events from a Remote Collector.



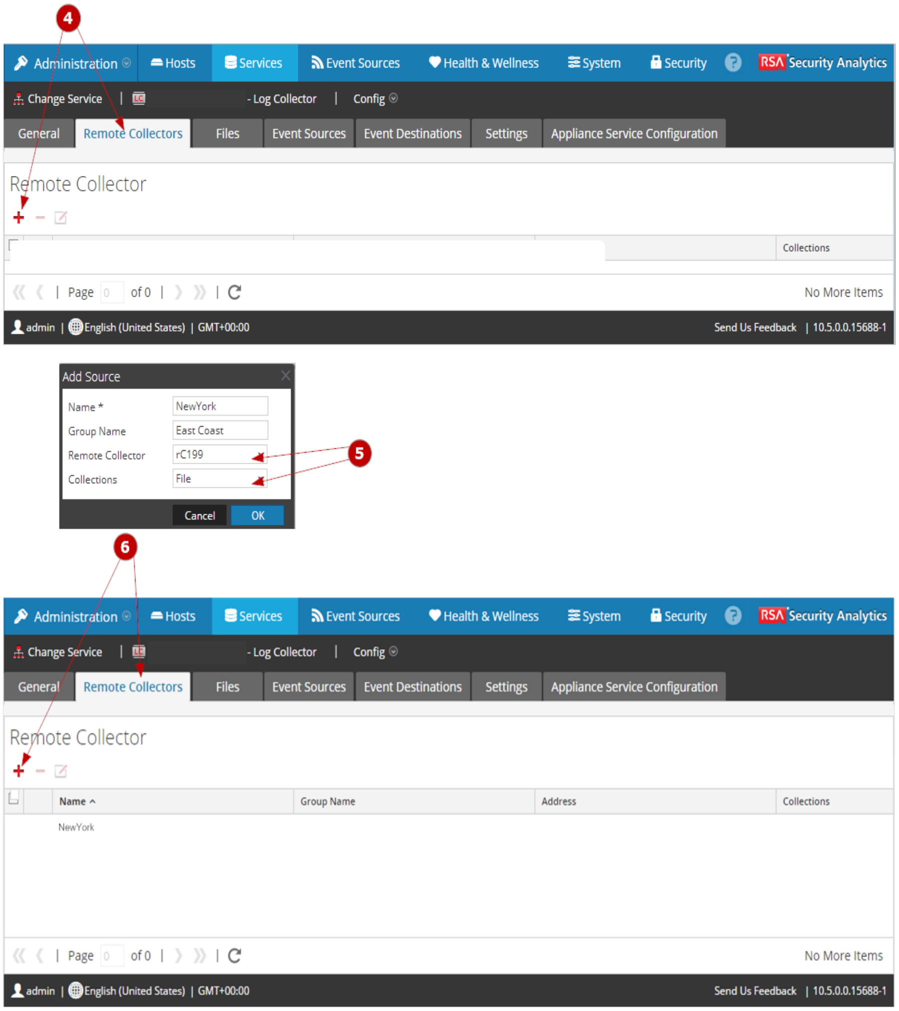
1 Access the **Services** view.



□		Name	Licensed	Appliance	Type	Version	Actions
□	●	Decoder123	✓	Decoder123	Decoder	10.4.0.0.3286-3	⚙
□	●	LD186	✓	LC-LD-186	Log Decoder	10.4.0.0.3276-3	⚙
☑	●	Log Collector	✓	LC-LD-186	Log Collector	10.4.0.(	
□	●	WC103	✓	AIO	Warehouse Connec...	10.4.0.(	

2 Select a Log Collector service.

3 Click ⌄ under **Actions** and select **View** > **Config** to display the Log Collection configuration parameter tabs.



Add Source

Name * NewYork

Group Name East Coast

Remote Collector rC199

Collections File

4 Select the **Remote Collectors** tab and click + to display to display the **Add Source** dialog.

5 Specify a Remote Collector from which the Local Collector pulls events. Specify the Collection protocols to pull.

6 Newly added Remote Collector displays in the **Remote Collector** tab.

Configure the Selected Local Collector to Pull Events from Specified Remote Collector

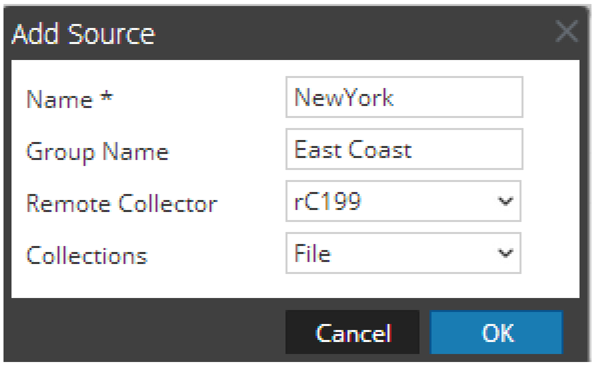
1. In the **Security Analytics** menu, select **Administration > Services**.
2. In **Services**, select a **Local Collector**.
3. Click ⌄ under Actions and select View > Config.

   The **Service Config** view is displayed with the **Log Collector General** tab open.
4. Click the **Settings** tab.
5. Select the **Remote Collectors** tab.
6. Click **+**.

   The **Add Source** dialog displays.
7. In the **Add Source** dialog:

   a. Select a Remote Collector from the drop-down list.

   b. Select one or more collection protocols.



Name * NewYork

Group Name East Coast

Remote Collector rC199

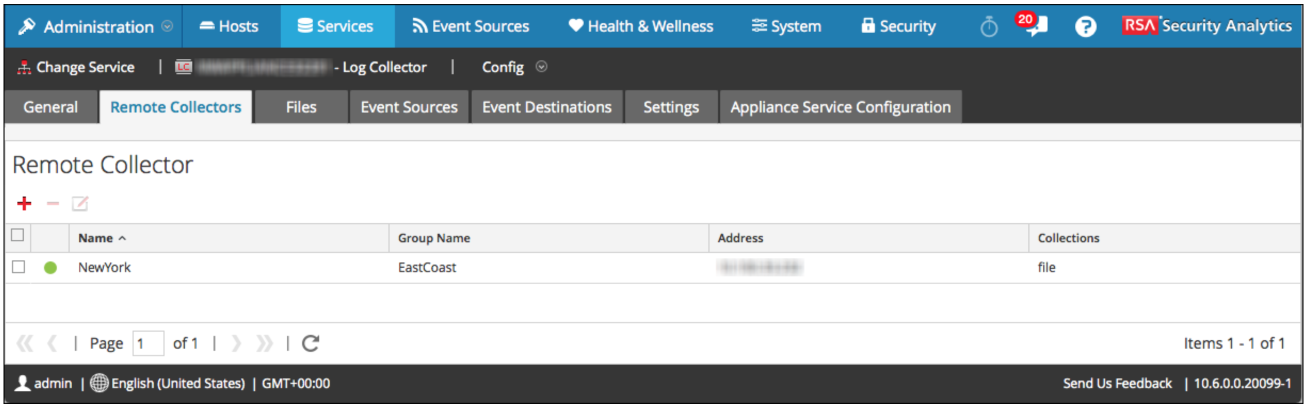
Collections File

> **Note:** If you do not select a collection protocol, the Local Collector pulls all collection protocols from the Remote Collector.

   c. Click **OK**.

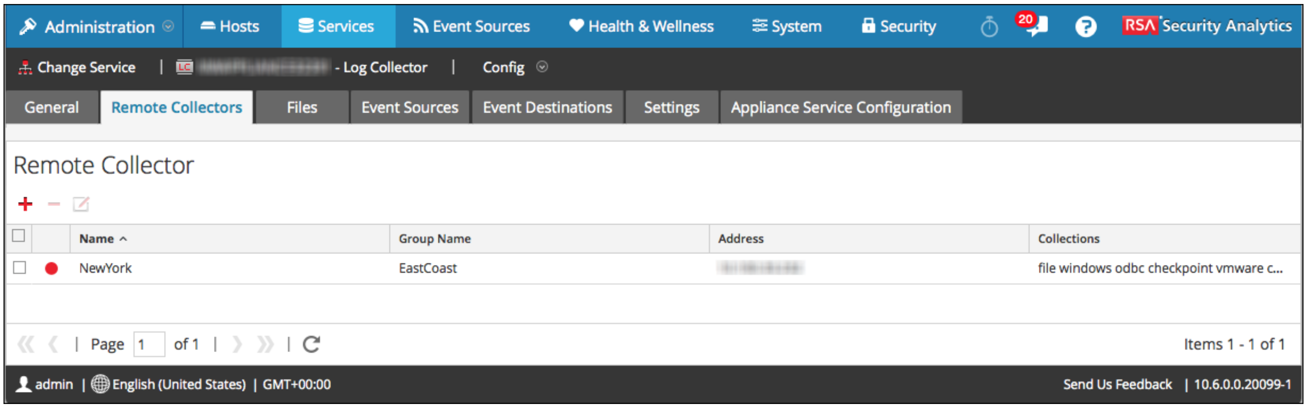
The Remote Collector is added to the Remote Collector section. When the Log Collector starts collecting data, it pulls event data from this Remote Collector.

The following tab shows **File** as the only protocol selected.



		Name ^	Group Name	Address	Collections
□	●	NewYork	EastCoast	[redacted]	file

The following tab shows all protocols selected. Security Analytics select all protocols if you leave the Collections field blank.



		Name ^	Group Name	Address	Collections
□	●	NewYork	EastCoast	[redacted]	file windows odbc checkpoint vmware c...

Note: The RabbitMQ may drop events between a Remote Collector and Local Collector due to low bandwidth as it utilizes high memory, thus setting off memory_alarm. For more information on the RabbitMQ behaviour, refer to https://www.rabbitmq.com/blog/2012/05/11/some-queuing-theory-throughput-latency-and-bandwidth/.

Parameters

Reference - Remote/Local Collectors Configuration Parameters Interface

Push Events to Local Collectors

This topic tells you how to configure a Remote Collector to push events to a Local Collector.

After completing this procedure, you will have configured a Remote Collector to push events to Local Collectors.

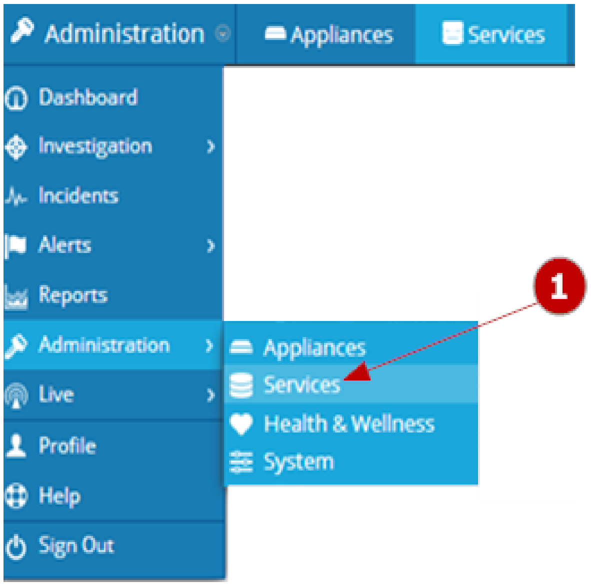
Return to Procedures

Procedures

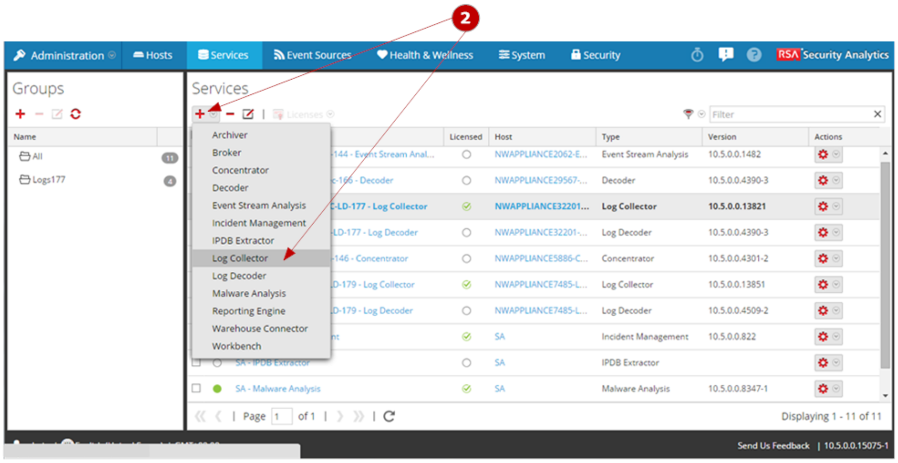
Configure Remote Collector to Push Events to Log Collectors

You can configure a Remote Collector to push event data to one or more Local Collectors.

The following figure shows you how to configure a Remote Collector to push events to a Local Collector.



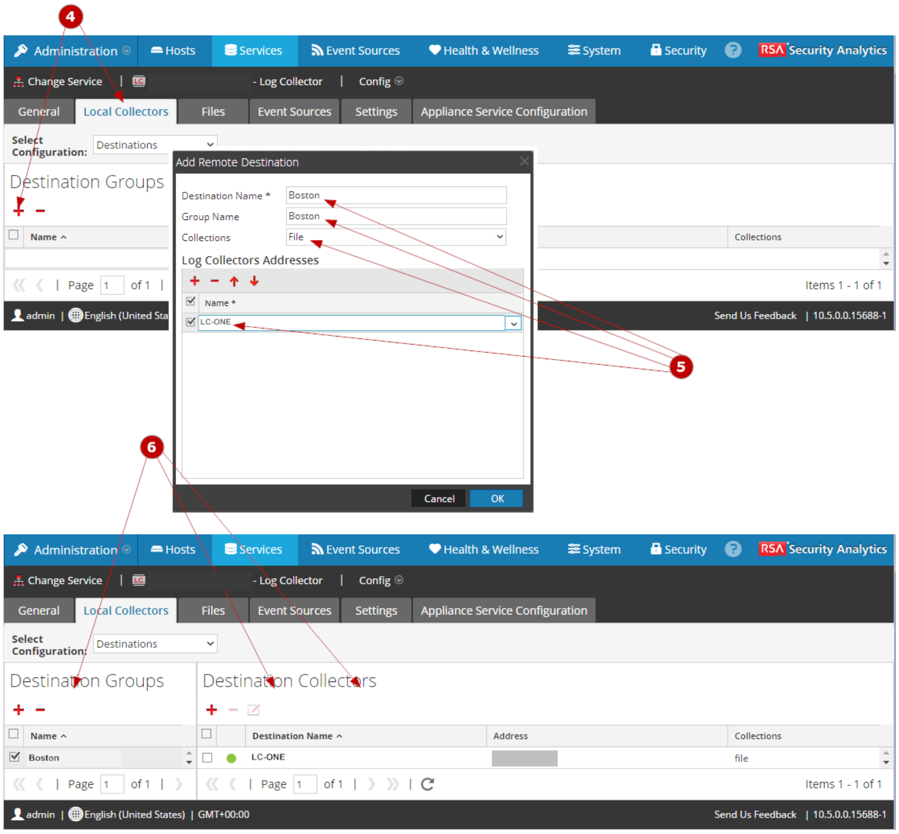
1 Access the **Services** view.



Name	Licensed	Host	Type	Version	Actions
-144 - Event Stream Anal...	○	NWAPPLIANCE2062-E...	Event Stream Analysis	10.5.0.0.1482	
c-166 - Decoder	○	NWAPPLIANCE29567-...	Decoder	10.5.0.0.4390-3	
C-LD-177 - Log Collector	✓	NWAPPLIANCE32201...	Log Collector	10.5.0.0.13821	
LD-177 - Log Decoder	○	NWAPPLIANCE32201-...	Log Decoder	10.5.0.0.4390-3	
-146 - Concentrator	○	NWAPPLIANCE5886-C...	Concentrator	10.5.0.0.4301-2	
D-179 - Log Collector	✓	NWAPPLIANCE7485-L...	Log Collector	10.5.0.0.13851	
D-179 - Log Decoder	○	NWAPPLIANCE7485-L...	Log Decoder	10.5.0.0.4509-2	
nt	✓	SA	Incident Management	10.5.0.0.822	
SA - IPDB Extractor	○	SA	IPDB Extractor		
SA - Malware Analysis	✓	SA	Malware Analysis	10.5.0.0.8347-1	

2 Select a remote collector.

3 Click ⌄ under **Actions** and select **View** > **Config** to display the Log Collection configuration parameter tabs.



Select Configuration: Destinations

Destination Name * Boston

Group Name Boston

Collections File

☑ Name *

☑ LC-ONE

	Destination Name ^	Address	Collections
□ ●	LC-ONE		file

4 Select the **Local Collectors** tab, select **Destinations** in the **Select Configuration** drop-down menu, and click + to display in **Destination Groups** to display the **Add Remote Destinations** dialog.

5 Specify a Local Collector to which the Remote Collector pushes events. Specify the Collection protocols to pull.

6 Newly added Local Collector is displayed in the **Local Collector** tab.

Configure the Selected Remote Collector to Push Events to Specified Log Collectors

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In **Services**, select a **Remote Collector**.
3. Click ⌄ under Actions and select **View** > **Config**.

   The **Service Config** view is displayed with the **Log Collector General** tab open.
4. Select the **Local Collectors** tab.

5. In the Destination Groups panel section, click ✚.

   The **Add Remote Destination** dialog displays.

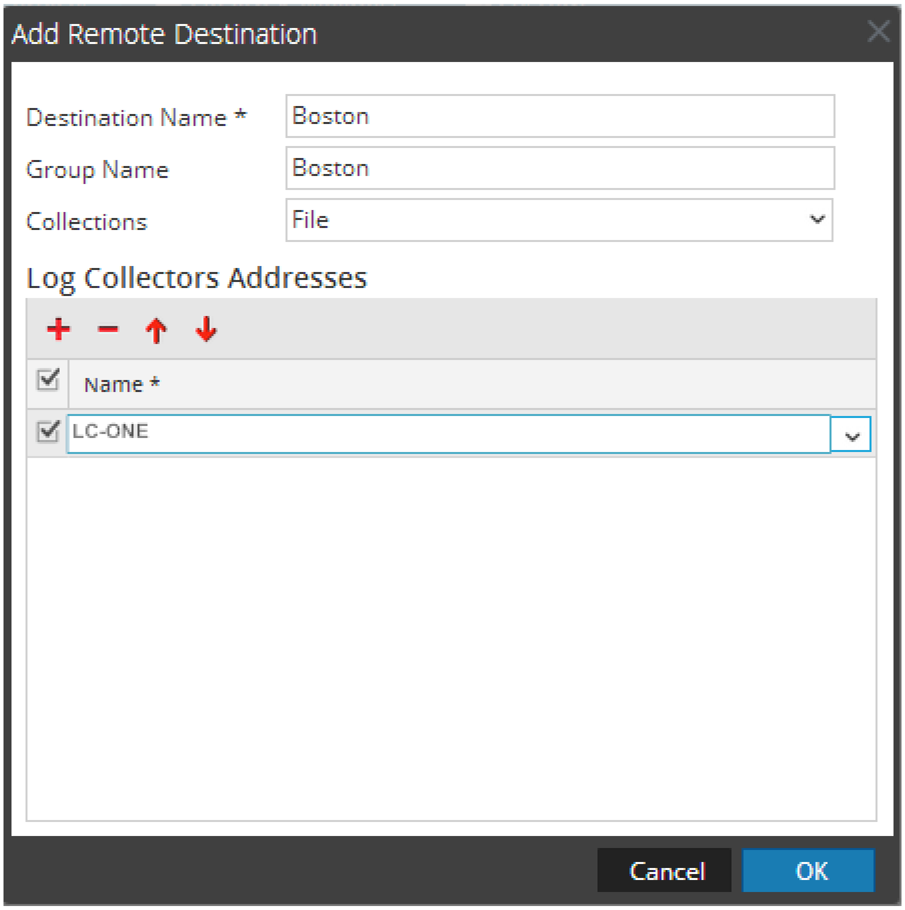
6. Set up a Destination Group:

   a. Enter a **Destination Name**.

   b. (Optional) Enter a Group Name. If you leave Group Name blank, Security Analytics sets it to the value that you specified in Destination Name.

   c. Select one or more collection protocols in the **Collections** drop-down list.

   d. Under **Log Collectors Addresses**, click ✚ to select a Local Collector.



Add Remote Destination

Destination Name * Boston

Group Name Boston

Collections File

Log Collectors Addresses

☑	Name *
☑	LC-ONE

Note: If you do not select a collection protocol, the Remote Collector pushes all collection protocols to the Local Collectors .

Note: The RabbitMQ may drop events between a Remote Collector and Local Collector due to low bandwidth as it utilizes high memory, thus setting off memory_alarm. For more information on the RabbitMQ behaviour, refer to https://www.rabbitmq.com/blog/2012/05/11/some-queuing-theory-throughput-latency-and-bandwidth/.

Parameters

Reference - Remote/Local Collectors Configuration Parameters Interface

Configure Failover Local Collector

This topic tells you how to set up a Failover Local Collector for a Remote Collector.

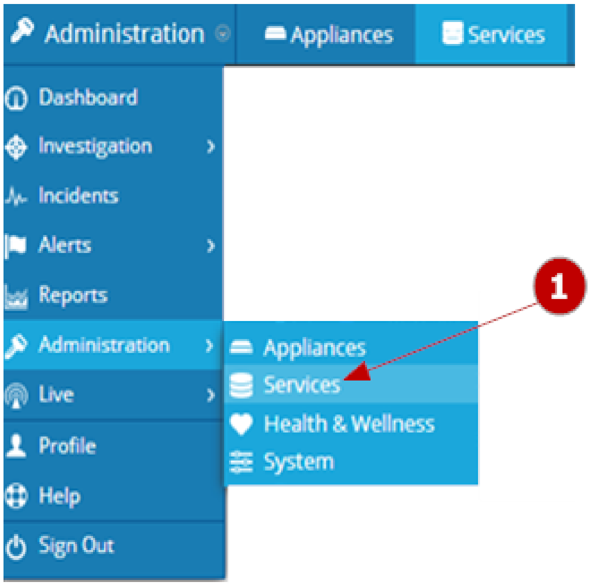
After completing this procedure, you will have set up a destination made up of local collectors such that when the primary Local Collector is unreachable, the Remote Collector attempts to connect to each local collector in this destination until it makes a successful connection.

Return to Procedures

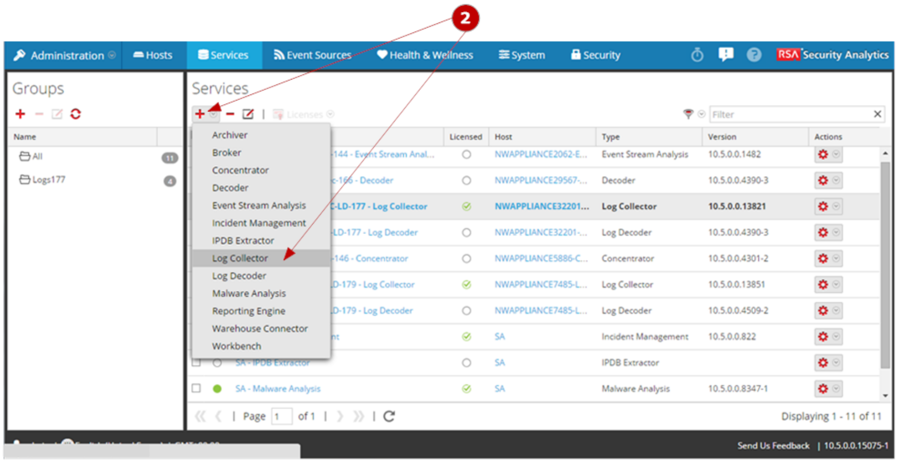
Configure a Failover Local Collector

You can set up a Failover Local Collector that Security Analytics will fail over to if your primary Local Collector stops operating for any reason.

The following figures shows you how to set up a failover Local Collector.



1 Access the **Services** view.



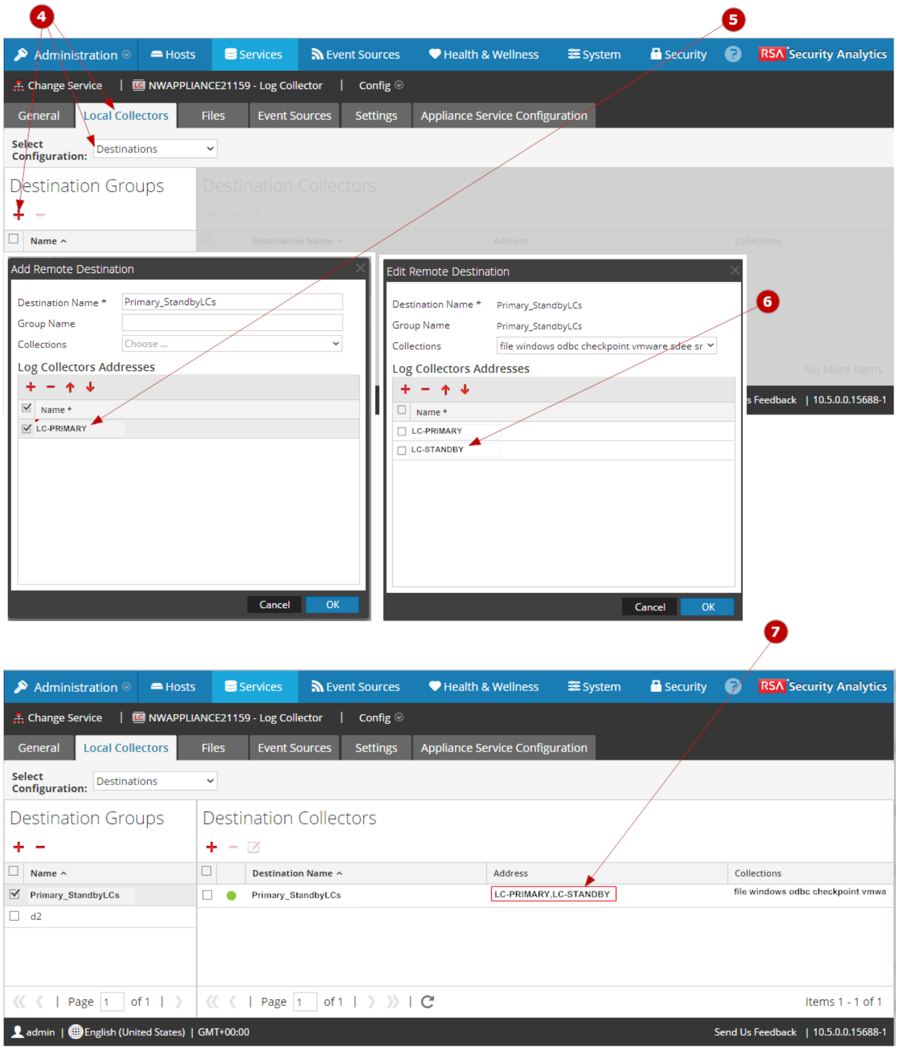
Name	Licensed	Host	Type	Version	Actions
-144 - Event Stream Anal...	○	NWAPPLIANCE2062-E...	Event Stream Analysis	10.5.0.0.1482	
c-166 - Decoder	○	NWAPPLIANCE29567-...	Decoder	10.5.0.0.4390-3	
C-LD-177 - Log Collector	✓	**NWAPPLIANCE32201...**	**Log Collector**	**10.5.0.0.13821**	
LD-177 - Log Decoder	○	NWAPPLIANCE32201-...	Log Decoder	10.5.0.0.4390-3	
-146 - Concentrator	○	NWAPPLIANCE5886-C...	Concentrator	10.5.0.0.4301-2	
D-179 - Log Collector	✓	NWAPPLIANCE7485-L...	Log Collector	10.5.0.0.13851	
D-179 - Log Decoder	○	NWAPPLIANCE7485-L...	Log Decoder	10.5.0.0.4509-2	
nt	✓	SA	Incident Management	10.5.0.0.822	
SA - IPDB Extractor	○	SA	IPDB Extractor		
SA - Malware Analysis	✓	SA	Malware Analysis	10.5.0.0.8347-1	

Page 1 of 1

Displaying 1 - 11 of 11

2 Select a remote collector.

3 Click under **Actions** and select **View** > **Config** to display the Log Collection configuration parameter tabs.



Select Configuration: Destinations

Destination Groups

Destination Collectors

Add Remote Destination

Destination Name * Primary_StandbyLCs

Group Name

Collections Choose ...

Log Collectors Addresses

	Name *
☑	LC-PRIMARY

Edit Remote Destination

Destination Name * Primary_StandbyLCs

Group Name Primary_StandbyLCs

Collections file windows odbc checkpoint vmware sdee sr

Log Collectors Addresses

	Name *
□	LC-PRIMARY
□	LC-STANDBY

Destination Groups

	Name ^
☑	Primary_StandbyLCs
□	d2

Destination Collectors

		Destination Name ^	Address	Collections
□	●	Primary_StandbyLCs	LC-PRIMARY,LC-STANDBY	file windows odbc checkpoint vmwa

4 Select the **Local Collectors** tab, select **Destinations** in **Select Configuration** drop-down menu, and click + to display in **Destination Groups** to display the **Add Remote Destinations** dialog.

5 Add a primary Local Collector.

6 Edit the Remote Destination and add a standby Local Collector.

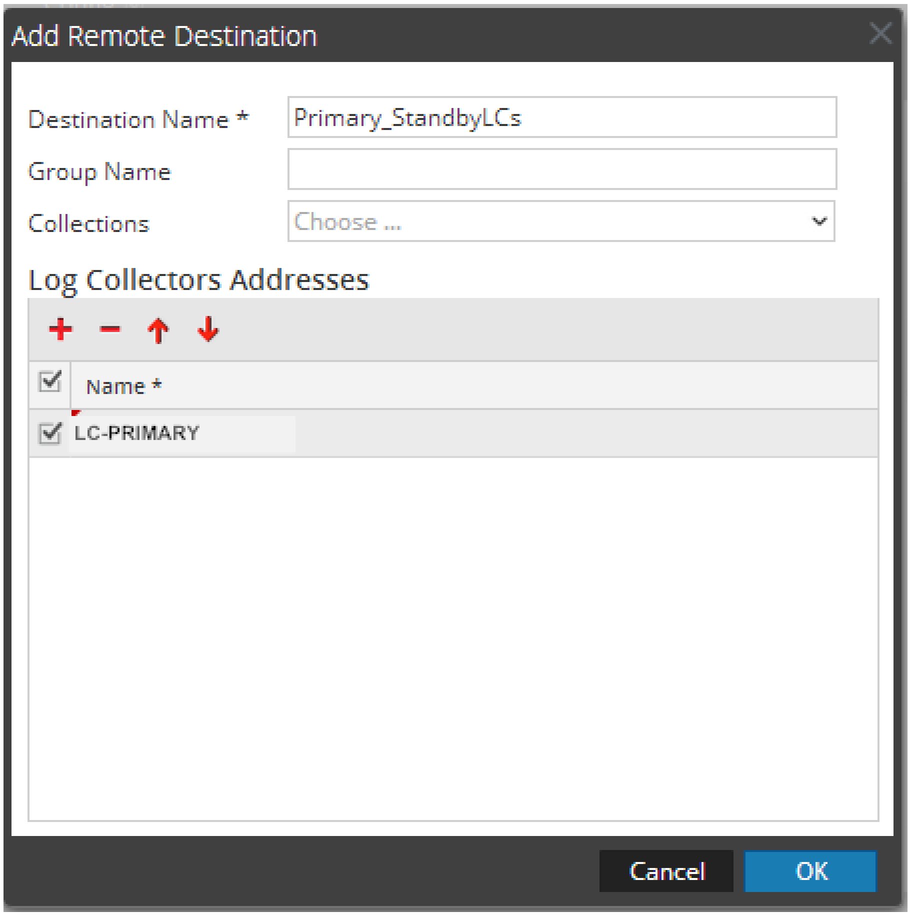
7 Newly added primary and standby Local Collectors are displayed in the **Local Collector** tab.

Set Up a Failover Local Collector

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In **Services**, select a Remote Collector.
3. Click ⌄ under **Actions** and select **View** > **Config**.

   The Service Config view is displayed with the Log Collector General tab open.
4. Select the **Local Collectors** tab.
5. In the **Destination Groups** panel section, select +.

   The Add Remote Destination dialog displays.
6. Set up a Destination Group and select a primary Local Collector (for example, **LC-PRIMARY**).



Add Remote Destination

Destination Name *	Primary_StandbyLCs
Group Name	
Collections	Choose ...

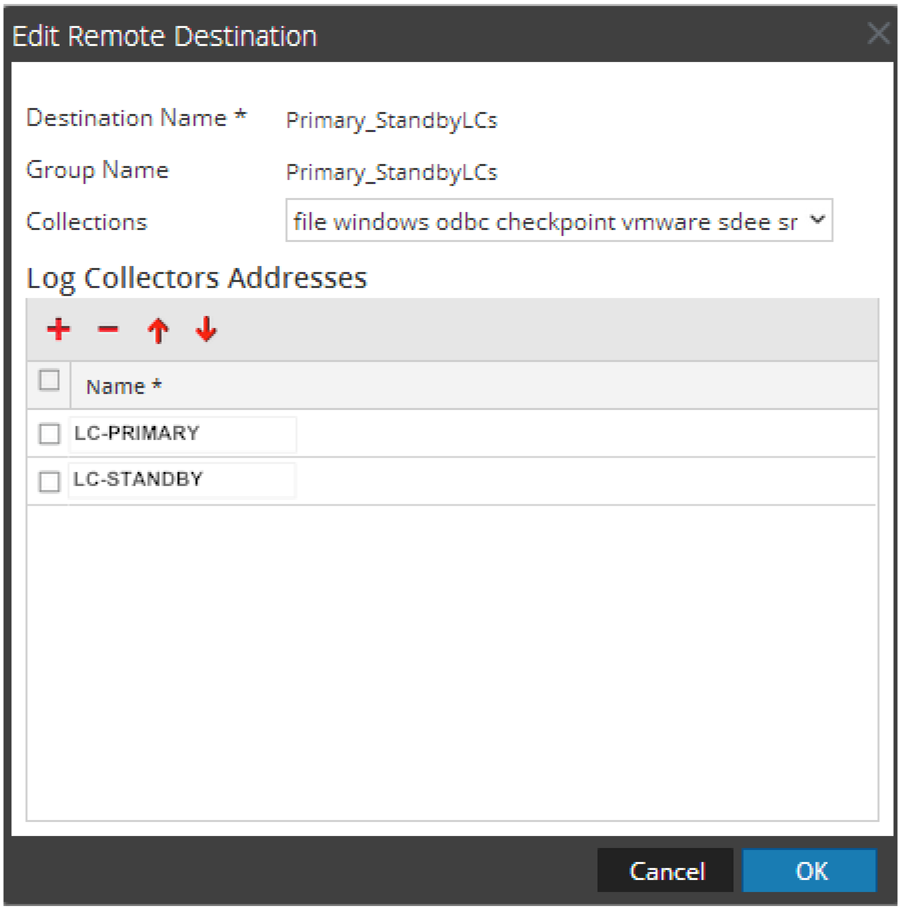
Log Collectors Addresses

☑	Name *
☑	LC-PRIMARY

7. Select the Group (for example, **Primary_Standby_LCs**) in the Destination Groups panel and click ✎.

   The Group you selected is displayed in the Local Collectors panel.

8. Add the Failover Local Collector (for example, **LC-STANDBY**).



Destination Name * Primary_StandbyLCs

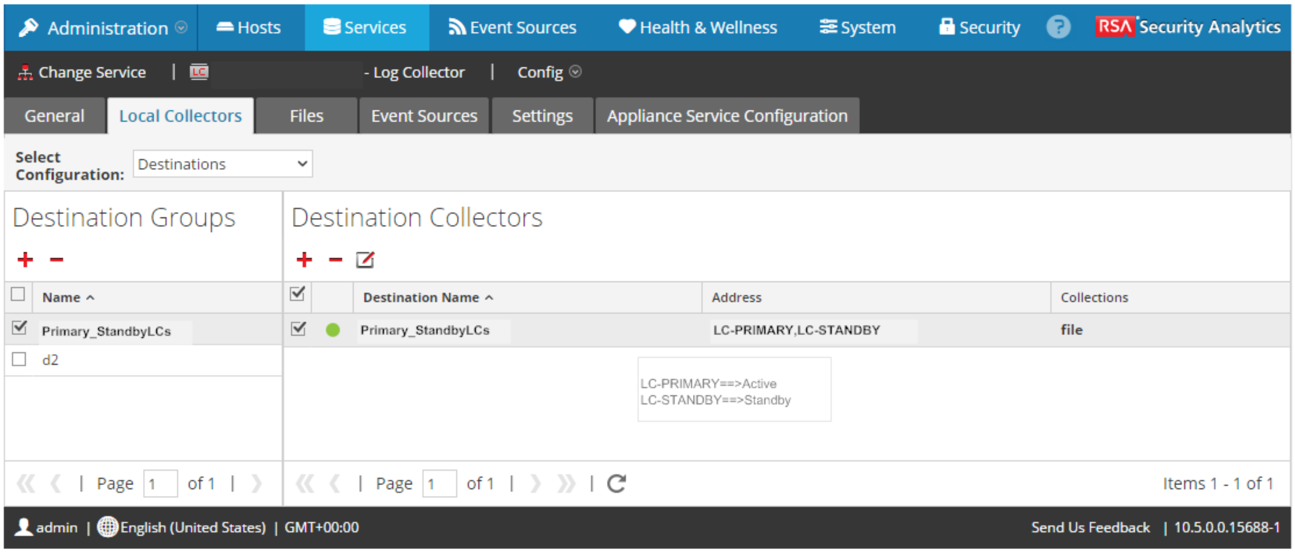
Group Name Primary_StandbyLCs

Collections file windows odbc checkpoint vmware sdee sr

Log Collectors Addresses

□	Name *
□	LC-PRIMARY
□	LC-STANDBY

The following examples show the newly added primary and failover Local Collectors showing the primary Local Collector as **Active** and the Failover Local Collector as **Standby**. The active Local Collector is highlighted (for example, **LC-PRIMARY**).



☐	Name ^
☑	Primary_StandbyLCs
☐	d2

☑		Destination Name ^	Address	Collections
☑	●	Primary_StandbyLCs	LC-PRIMARY,LC-STANDBY	file

LC-PRIMARY==>Active
LC-STANDBY==>Standby

9. (Optional) Add, delete, and change the order of Local Collectors to each Remote Destination.

   a. Click + to add a Log Collector as a failover Remote Destination.

   b. When connecting to a Remote Destination, the Remote Collector will attempt to connect to each Local Collector in this list in order, until it makes a successful connection.

   c. Select a Local Collector and use the ↑ ↓ (up and down arrow buttons) to change the order of connection.

   d. Select one or more Local Collectors and click − to remove them from the list.

   The selected Local Collectors are added to the Log Collector section. When the Remote Collector starts collecting data, it pushes data to these Log Collectors.

Parameters

Reference - Remote/Local Collectors Configuration Parameters Interface

Configure Failover Remote Collector

This topic tells you how to set up a Failover Remote Collector for a Remote Collector.

After completing this procedure, you will have set up a destination made up of Remote Collectors such that when the primary Remote Collector is unreachable, the Remote Collector attempts to connect to each Remote Collector in this destination until it makes a successful connection.

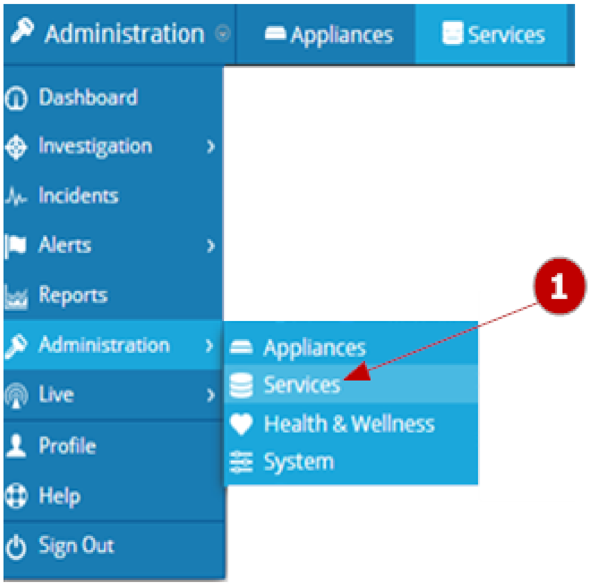
Return to Procedures

Procedures

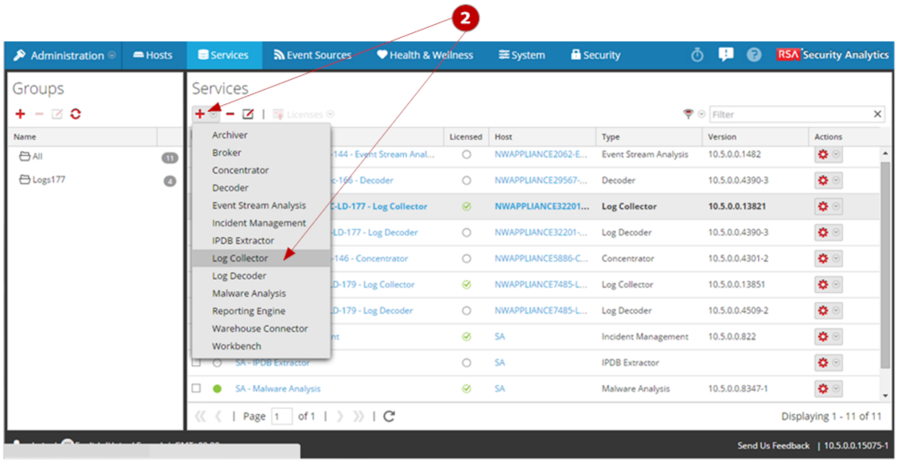
Configure a Failover Remote Collector

You can set up a Failover Remote Collector that Security Analytics will fail over to if your primary Remote Collector stops operating for any reason.

The following figure shows you how to set up a failover Remote Collector.



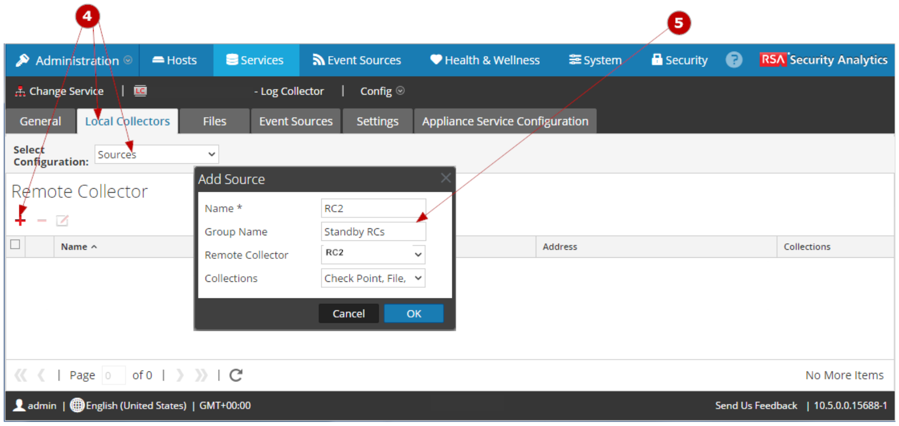
1 Access the **Services** view.



	Licensed	Host	Type	Version	Actions
-144 - Event Stream Anal...	○	NWAPPLIANCE2062-E...	Event Stream Analysis	10.5.0.0.1482	
c-166 - Decoder	○	NWAPPLIANCE29567-...	Decoder	10.5.0.0.4390-3	
C-LD-177 - Log Collector	✓	NWAPPLIANCE32201...	Log Collector	10.5.0.0.13821	
-LD-177 - Log Decoder	○	NWAPPLIANCE32201-...	Log Decoder	10.5.0.0.4390-3	
-146 - Concentrator	○	NWAPPLIANCE5886-C...	Concentrator	10.5.0.0.4301-2	
D-179 - Log Collector	✓	NWAPPLIANCE7485-L...	Log Collector	10.5.0.0.13851	
D-179 - Log Decoder	○	NWAPPLIANCE7485-L...	Log Decoder	10.5.0.0.4509-2	
nt	✓	SA	Incident Management	10.5.0.0.822	
SA - IPDB Extractor	○	SA	IPDB Extractor		
SA - Malware Analysis	✓	SA	Malware Analysis	10.5.0.0.8347-1	

2 Select a Remote Collector.

3 Click ⌄ under **Actions** and select **View** > **Config** to display the Log Collection configuration parameter tabs.

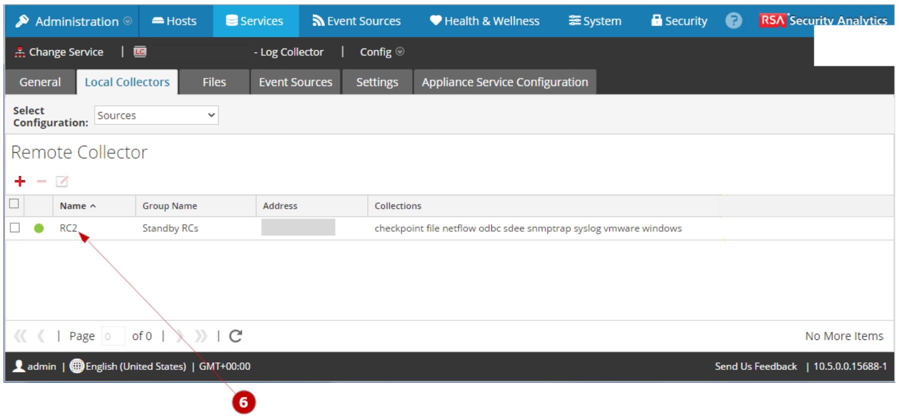


Select Configuration: Sources

Add Source

Name *	RC2
Group Name	Standby RCs
Remote Collector	RC2
Collections	Check Point, File,

Cancel OK



Select Configuration: Sources

Remote Collector

		Name ^	Group Name	Address	Collections
□	●	RC2	Standby RCs		checkpoint file netflow odbc sdee snmptrap syslog vmware windows

4 Select the **Local Collectors** tab, select **Sources** in **Select Configuration** drop-down menu, and click + to display in **Add Source** dialog.

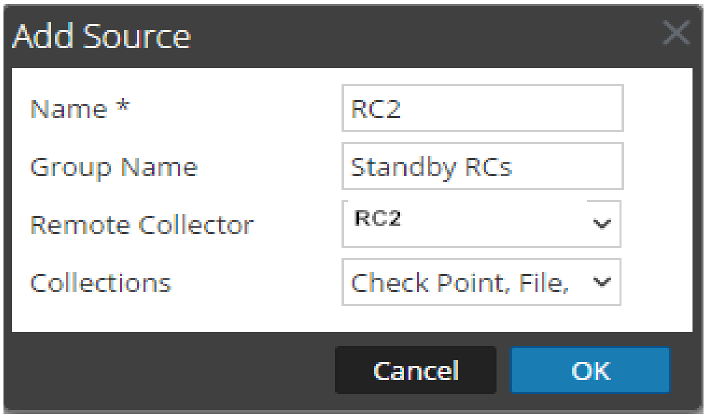
5 Add a standby Remote Collector.

6 Newly added standby Remote Collector is displayed in the **Local Collector** tab.

Set Up a Failover Remote Collector:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In **Services**, select a **Remote Collector**.
3. Click ⌄ under **Actions** and select **View** > **Config**.

   The **Service Config** view is displayed with the **Log Collector General** tab open.
4. Select the **Local Collectors** tab.
5. Select **Sources** in **Select Configuration** drop-down menu.
6. Click + to display in **Add Source** dialog.
7. Define the failover Remote Collector and click **OK**.



Add Source

Name *	RC2
Group Name	Standby RCs
Remote Collector	RC2
Collections	Check Point, File,

Parameters

Reference - Remote/Local Collectors Configuration Parameters Interface

Configure Replication

This topic tells you how to replicate event data sent by a Remote Collector.

After completing this procedure, you will have configured Security Analytics so that it replicates a Remote Collector's event data in multiple local collector destination groups.

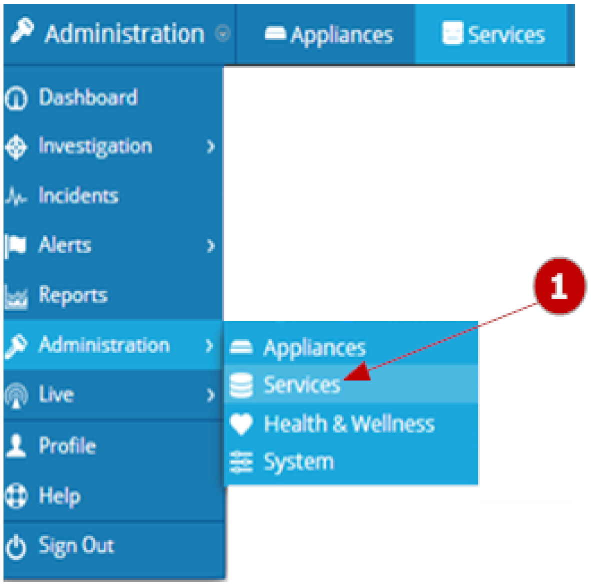
Return to Procedures.

Procedures

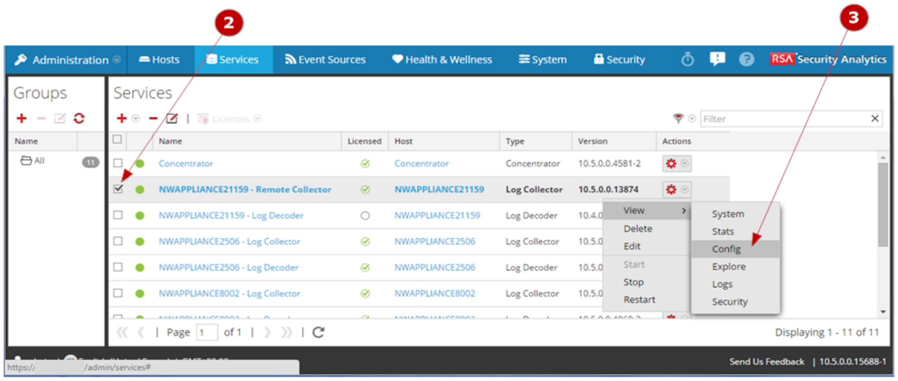
Replicate Event Messages

You can specify multiple Destination Groups so that the event data is replicated to each group.

The following figure shows you how to replicate event data to multiple Local Collectors.



1 Access the **Services** view.

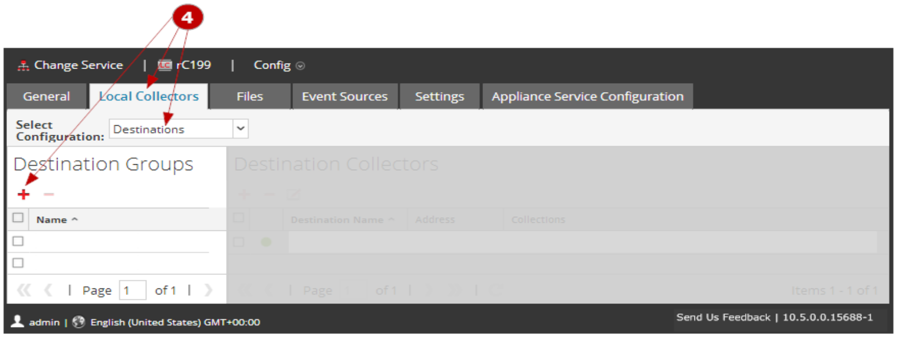


	Name	Licensed	Host	Type	Version	Actions
□	Concentrator	✓	Concentrator	Concentrator	10.5.0.0.4581-2	
☑	NWAPPLIANCE21159 - Remote Collector	✓	NWAPPLIANCE21159	Log Collector	10.5.0.0.13874	
□	NWAPPLIANCE21159 - Log Decoder	○	NWAPPLIANCE21159	Log Decoder	10.4.0	
□	NWAPPLIANCE2506 - Log Collector	✓	NWAPPLIANCE2506	Log Collector	10.5.0	
□	NWAPPLIANCE2506 - Log Decoder	✓	NWAPPLIANCE2506	Log Decoder	10.5.0	
□	NWAPPLIANCE8002 - Log Collector	✓	NWAPPLIANCE8002	Log Collector	10.5.0	

Displaying 1 - 11 of 11

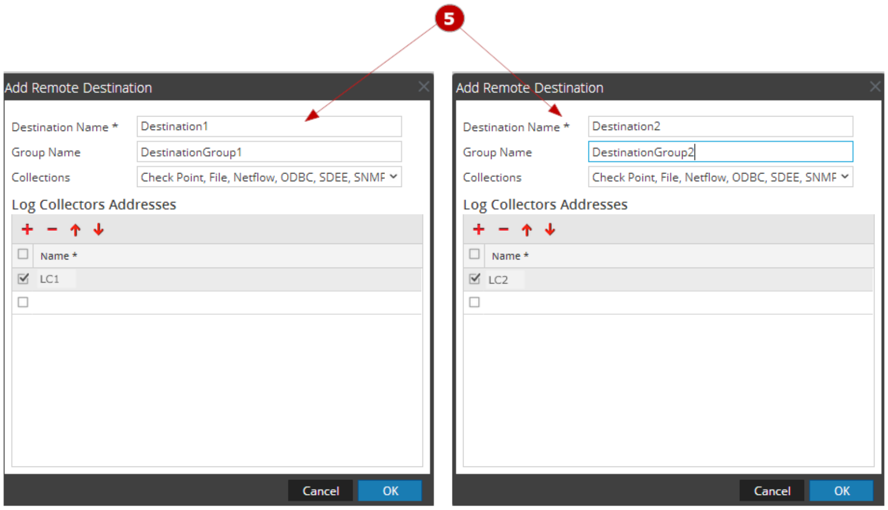
2 Select a Remote Collector.

3 Click ⌄ under **Actions** and select **View** > **Config** to display the Log Collection configuration parameter tabs.



Select Configuration: Destinations

4 Select the **Local Collectors** tab, select **Destinations** in **Select Configuration** drop-down menu, and click + in **Destination Groups** to display the **Add Remote Destinations** dialog.



Add Remote Destination

Destination Name * Destination1

Group Name DestinationGroup1

Collections Check Point, File, Netflow, ODBC, SDEE, SNMF

Log Collectors Addresses: ☑ LC1

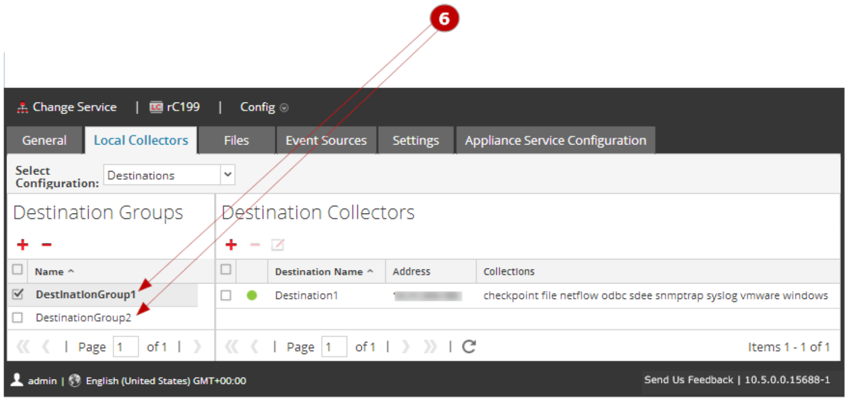
Add Remote Destination

Destination Name * Destination2

Group Name DestinationGroup2

Collections Check Point, File, Netflow, ODBC, SDEE, SNMF

Log Collectors Addresses: ☑ LC2


6
Change Service | rC199 | Config
General
Local Collectors
Files
Event Sources
Settings
Appliance Service Configuration
Destination Groups
Destination Collectors
Page 1 of 1
Items 1 - 1 of 1
admin | English (United States) GMT+00:00
Send Us Feedback | 10.5.0.0.15688-1

Select Configuration: Destinations

	Name ^
☑	DestinationGroup1
□	DestinationGroup2

		Destination Name ^	Address	Collections
□	●	Destination1	[redacted]	checkpoint file netflow odbc sdee snmptrap syslog vmware windows

5 Set up the **Destination Groups** to facilitate replication.

6 Newly added replication Destination Groups display in the **Local Collector** tab.

Replicate Event Data to Multiple Local Collectors

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In **Services**, select a **Remote Collector**.
3. Click ⌄ under **Actions** and select **View > Config**.

   The **Service Config** view is displayed with the **Log Collector General** tab open.
4. Select the **Local Collectors** tab.
5. In the **Destination Groups** panel section, click +.

   The **Add Remote Destination** dialog is displayed.
6. Set up a separate Destination for each Local Collector and designate the protocols for which you want to push event messages to that Local Collector. The following examples shows the addition of two Destination Local Collectors (**Destination1** and **Destination2**) for the **Check Point**, **File**, **Netflow**, **ODBC**, **SDEE**, **SNMP**, **Syslog**, and **Windows** collection protocols:

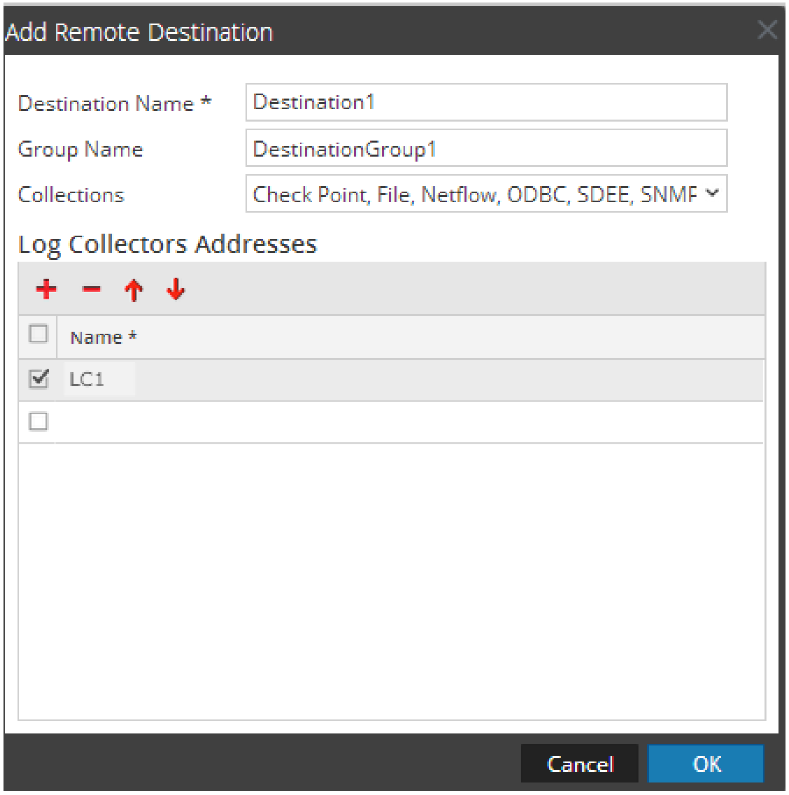
   a. Type the **Destination Name**.

   b. Type the **Group Name**. If you do not type a Group Name, the Destination Name is taken as the Group Name.

   c. Select the collection protocols in the drop-down list.

   d. Select a Local Collector (for example, **LC1**).

   e. Click **OK**.



Add Remote Destination

Destination Name * Destination1

Group Name DestinationGroup1

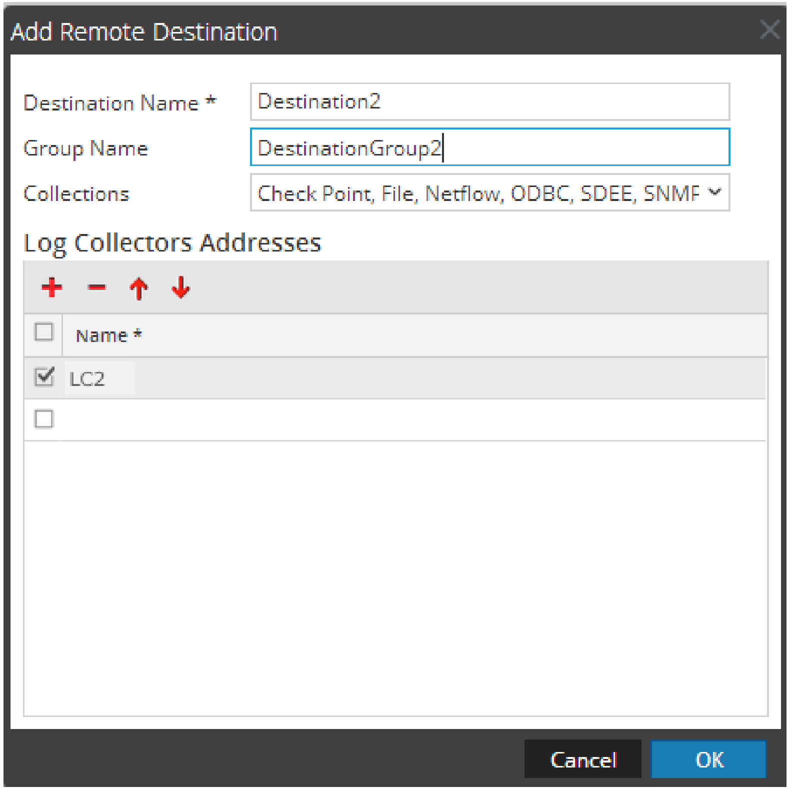
Collections Check Point, File, Netflow, ODBC, SDEE, SNMF

Log Collectors Addresses

□	Name *
☑	LC1
□	

f. Select the new group (for example, **DestinationGroup2**) group in the **Destination Groups** panel and click + in the **Local Collector** panel.

g. In the **Local Collector** panel, click + and complete the **Add Remote Destination** dialog as illustrated in the following figure.



Add Remote Destination

Destination Name * Destination2

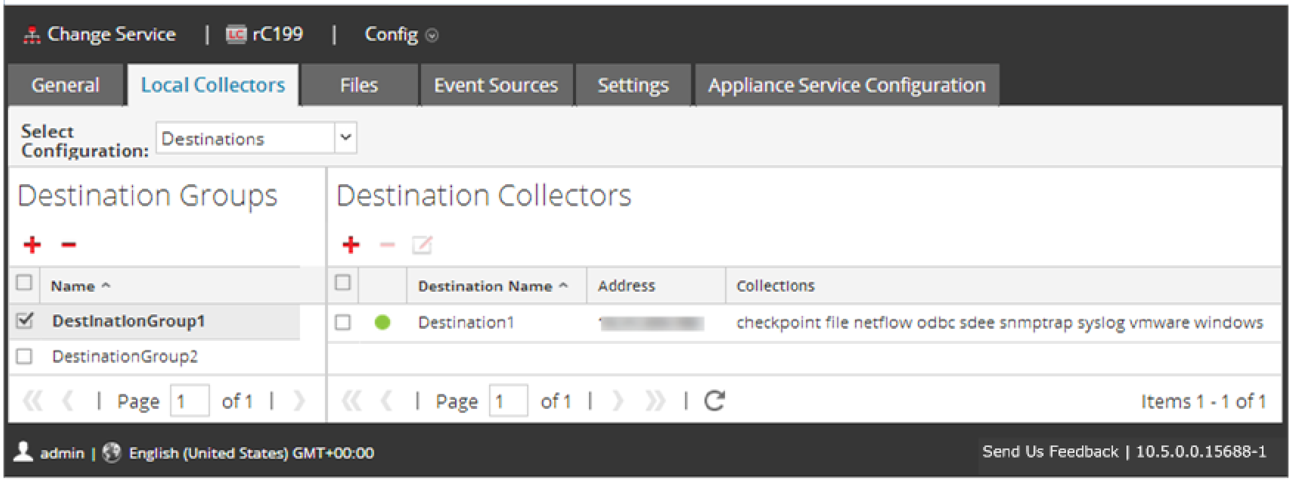
Group Name DestinationGroup2

Collections Check Point, File, Netflow, ODBC, SDEE, SNMF

Log Collectors Addresses

□	Name *
☑	LC2
□	

The **Check Point**, **File**, **Netflow**, **ODBC**, **SDEE**, **SNMP**, **Syslog**, and **Windows** collection protocols are sent to two Local Collectors (**LC1** and **LC2**). Both Local Collectors are active and collecting event data.



Change Service | rC199 | Config
General
Local Collectors
Files
Event Sources
Settings
Appliance Service Configuration

Select Configuration: Destinations

Destination Groups

□	Name ^
☑	DestinationGroup1
□	DestinationGroup2

Destination Collectors

□		Destination Name ^	Address	Collections
□	●	Destination1	[redacted]	checkpoint file netflow odbc sdee snmptrap syslog vmware windows

Page 1 of 1

Items 1 - 1 of 1

admin | English (United States) GMT+00:00
Send Us Feedback | 10.5.0.0.15688-1

Parameters

Reference - Remote/Local Collectors Configuration Parameters Interface

Configure Log Routing for Specific Protocols

This topic tells you how to define where specific protocol event messages are routed by configuring multiple Local Collectors in a destination group. This can help you to direct event data to specific locations according to protocol type.

After completing this procedure, you will have set up multiple destinations, in a destination group, to which Security Analytics distributes protocol event data.

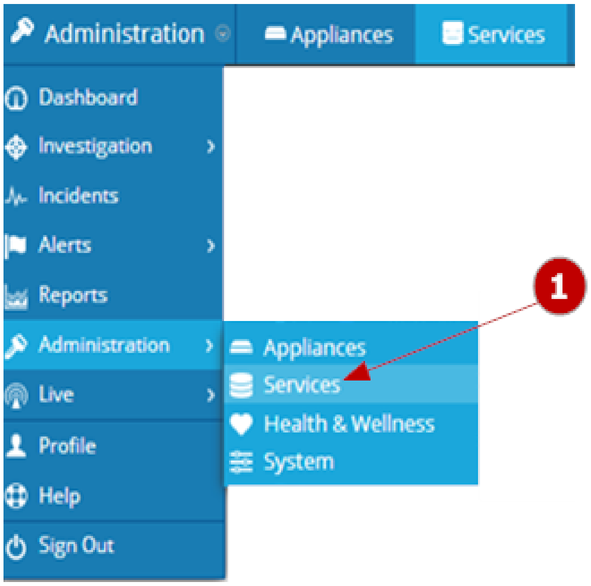
Return to Procedures

Procedure

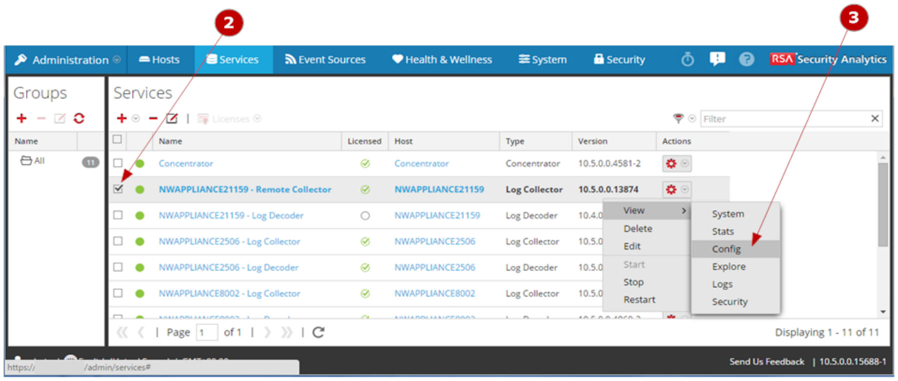
Define Routing of Protocol Event Data

When pushing to more than one Local Collector, you can choose to route specific protocol event data to multiple Local Collectors by specifying multiple destinations within a Destination Group. A Destination Group is a collection of Local Collectors, such that event data can be distributed to all members of the group.

The following figure shows you how to route event messages from a collection protocol.



1 Access the **Services** view.



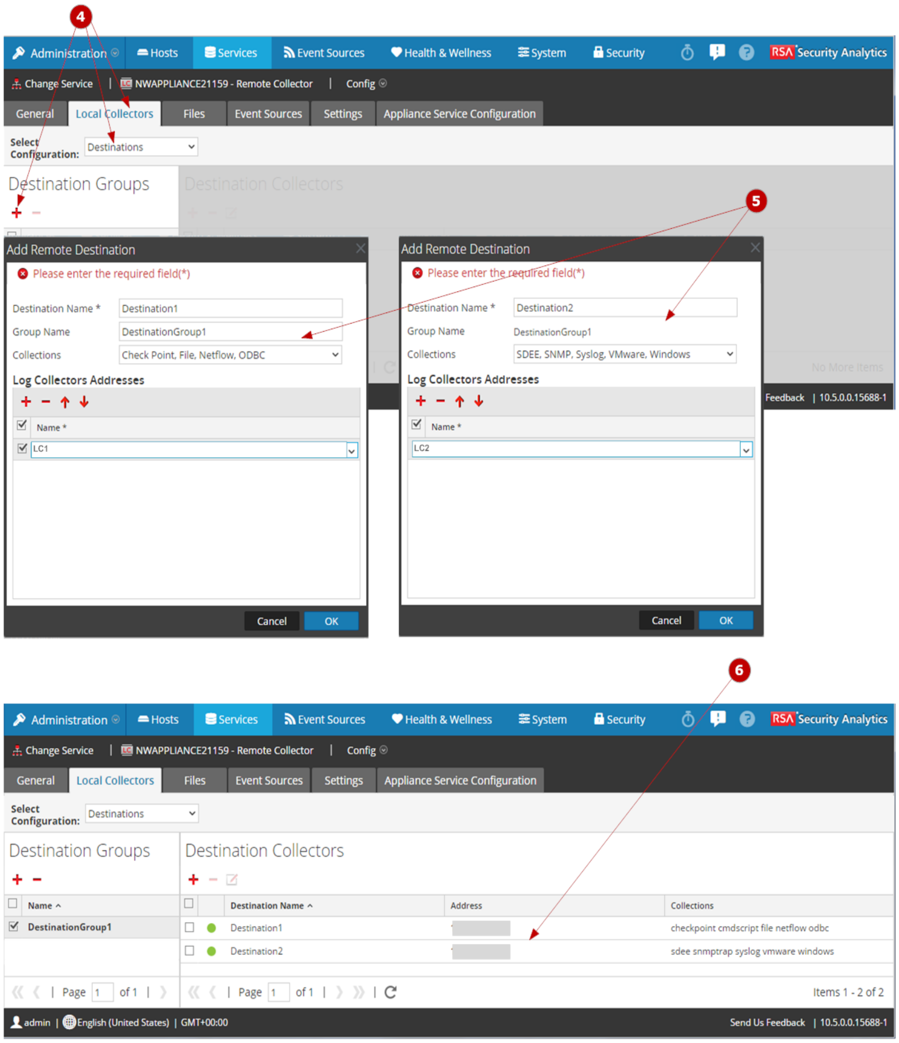
□		Name	Licensed	Host	Type	Version	Actions
□	●	Concentrator	✓	Concentrator	Concentrator	10.5.0.0.4581-2	⚙ ⌄
☑	●	NWAPPLIANCE21159 - Remote Collector	✓	NWAPPLIANCE21159	Log Collector	10.5.0.0.13874	⚙ ⌄
□	●	NWAPPLIANCE21159 - Log Decoder	○	NWAPPLIANCE21159	Log Decoder	10.4.0	
□	●	NWAPPLIANCE2506 - Log Collector	✓	NWAPPLIANCE2506	Log Collector	10.5.0	
□	●	NWAPPLIANCE2506 - Log Decoder	✓	NWAPPLIANCE2506	Log Decoder	10.5.0	
□	●	NWAPPLIANCE8002 - Log Collector	✓	NWAPPLIANCE8002	Log Collector	10.5.0	

Page 1 of 1

Displaying 1 - 11 of 11

2 Select a remote collector.

3 Click ⌄ under **Actions** and select **View** > **Config** to display the Log Collection configuration parameter tabs.



Select Configuration: Destinations

Add Remote Destination

Please enter the required field(*)

Destination Name * Destination1
Group Name DestinationGroup1
Collections Check Point, File, Netflow, ODBC

Log Collectors Addresses

☑ Name *
☑ LC1

Add Remote Destination

Please enter the required field(*)

Destination Name * Destination2
Group Name DestinationGroup1
Collections SDEE, SNMP, Syslog, VMware, Windows

Log Collectors Addresses

☑ Name *
LC2

Destination Groups

□	Name ^
☑	DestinationGroup1

Page 1 of 1

Destination Collectors

□		Destination Name ^	Address	Collections
□	●	Destination1	[redacted]	checkpoint cmdscript file netflow odbc
□	●	Destination2	[redacted]	sdee snmptrap syslog vmware windows

Page 1 of 1 Items 1 - 2 of 2

4 Select the **Local Collectors** tab, select **Destinations** in **Select Configuration** drop-down menu, and click + to display in **Destination Groups** to display the **Add Remote Destinations** dialog.

5 Set up a separate Destination for each Local Collector and designate the protocols for which you want to push event messages to that Local Collector.

6 Newly added primary and load-balanced Local Collector configuration is displayed in the **Local Collector** tab.

Configure Event Message Routing from a Collection Protocol

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In **Services**, select a **Remote Collector**.
3. Click ⌄ under **Actions** and select **View** > **Config**.

   The **Service Config** view is displayed with the **Log Collector General** tab open.
4. Select the **Local Collectors** tab.
5. In the **Destination Groups** panel, click +.

   The **Add Remote Destination** dialog displays.
6. Set up a separate Destination for each Local Collector and designate the protocols for which you want to push event messages to that Local Collector. The following examples shows the addition of two Destination Local Collectors (**Destination1** and **Destination2**). This configuration sends:

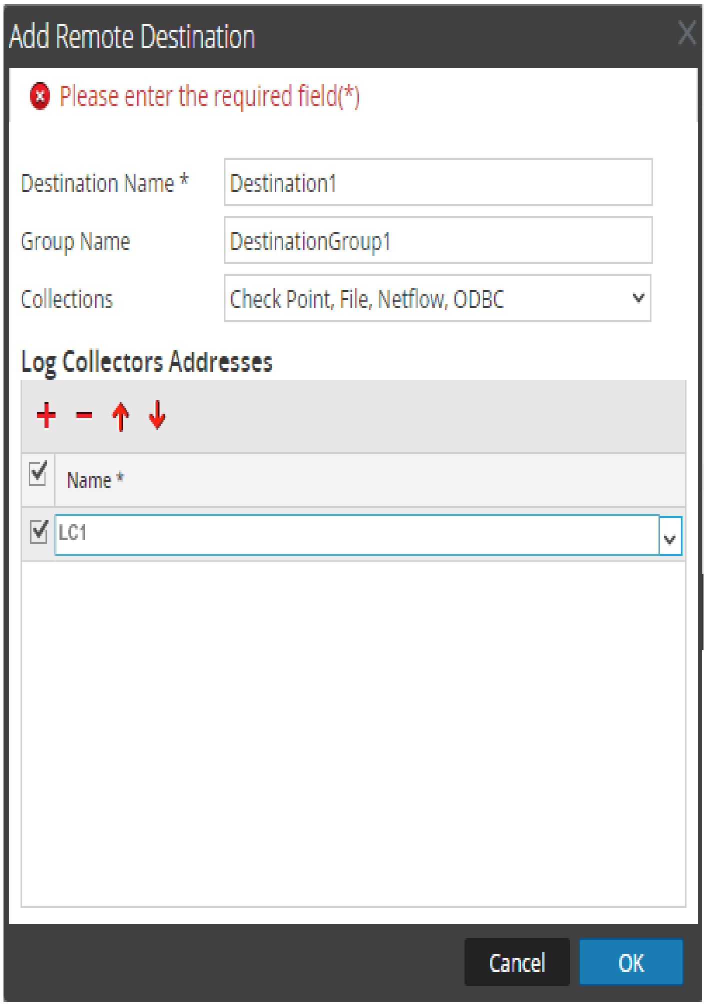
   - **Check Point**, **File**, and **ODBC** event data to **Destination1**.
   - **Syslog** and **Windows** event data to **Destination2**.

   a. Type the **Destination Name**.

   b. Type the **Group Name**. If you do not type a Group Name, the Destination Name is taken as the Group Name.

   c. Select the collection protocol from the drop-down list.

   d. Select a Local Collector (for example, **LC1**)



Add Remote Destination

Please enter the required field(*)

Destination Name * Destination1

Group Name DestinationGroup1

Collections Check Point, File, Netflow, ODBC

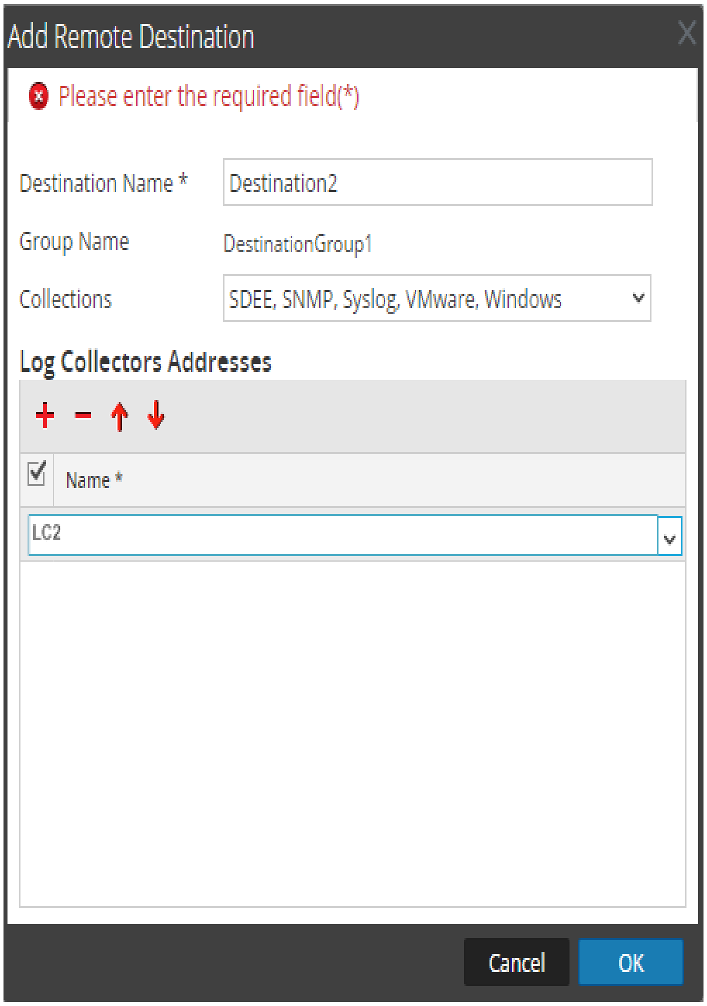
Log Collectors Addresses

☑	Name *
☑	LC1

e. Click **OK**. **Destination1** is created and displayed in the **Destination Groups** panel.

f. Select the new group (for example, **Destination1**) in the **Destination Groups** panel, and click + in the **Local Collector** panel.

g. In the **Local Collector** panel, click + and complete the **Add Remote Destination** dialog as illustrated in the following figure.



Add Remote Destination

Please enter the required field(*)

Destination Name * Destination2

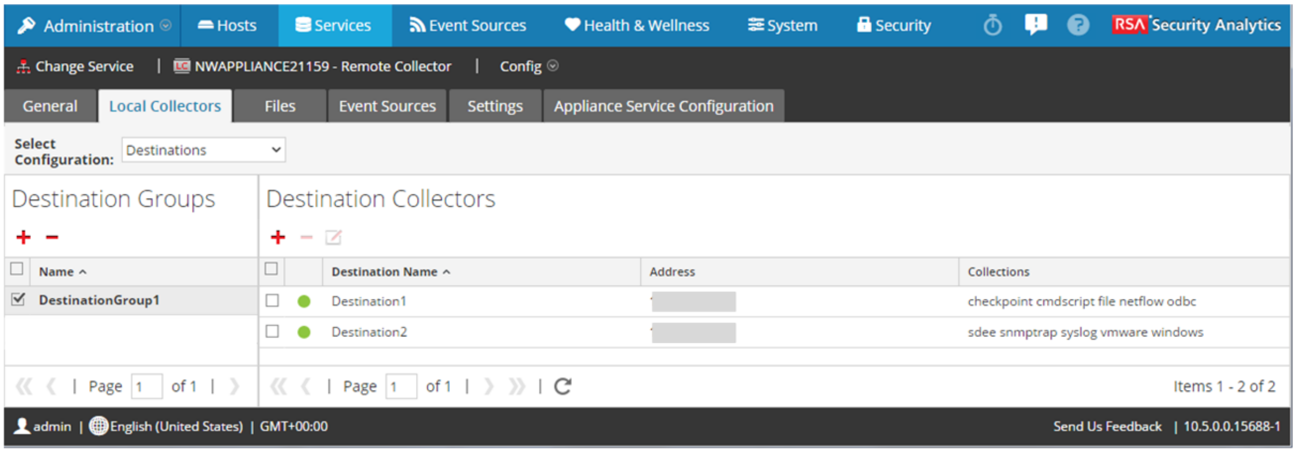
Group Name DestinationGroup1

Collections SDEE, SNMP, Syslog, VMware, Windows

Log Collectors Addresses

☑	Name *
	LC2

The **Check Point**, **File**, **ODBC**, **Syslog**, and **Windows** collection protocols are being load balanced between two Local Collectors (LC1 and LC2). Both Local Collectors are active and collecting event data.



Select Configuration: Destinations

Destination Groups

☐	Name ^
☑	DestinationGroup1

Page 1 of 1

Destination Collectors

☐		Destination Name ^	Address	Collections
☐	●	Destination1	[redacted]	checkpoint cmdscript file netflow odbc
☐	●	Destination2	[redacted]	sdee snmptrap syslog vmware windows

Page 1 of 1 Items 1 - 2 of 2

admin | English (United States) | GMT+00:00 Send Us Feedback | 10.5.0.0.15688-1

Parameters

Reference - Remote/Local Collectors Configuration Parameters Interface

Configure Chain of Remote Collectors

This topic describes how to chain Remote Collectors (also referred to as VLCs).

You can set up a chain of Remote Collectors to push event data to a Remote Collector, or you can configure a Remote Collector to pull event data from a chain of Remote Collectors.

- Remote Collectors to push event data to a Remote Collector.
- A Remote Collector to pull event data from one or more Remote Collectors.

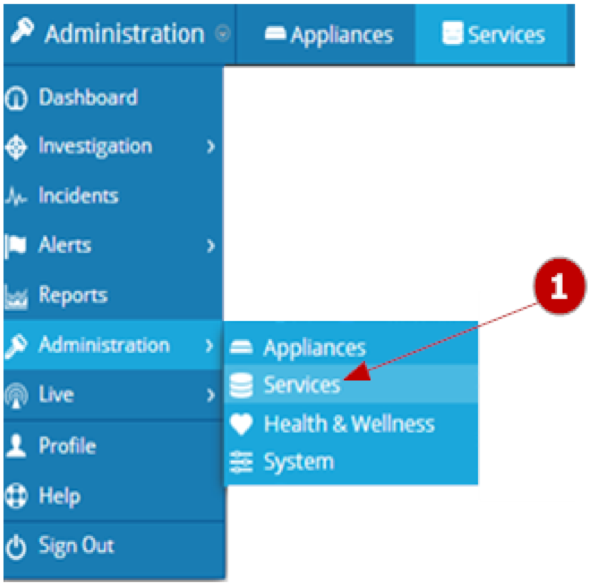
Note: For Remote Collector chaining, you can only:
Push data from a 10.4 or later Remote Collector to other 10.4 or later Remote Collectors or 10.4 or later Local Collectors.
Use a 10.4 or later Remote Collector to pull data from one or more 10.4 or later Remote Collectors.

Procedures

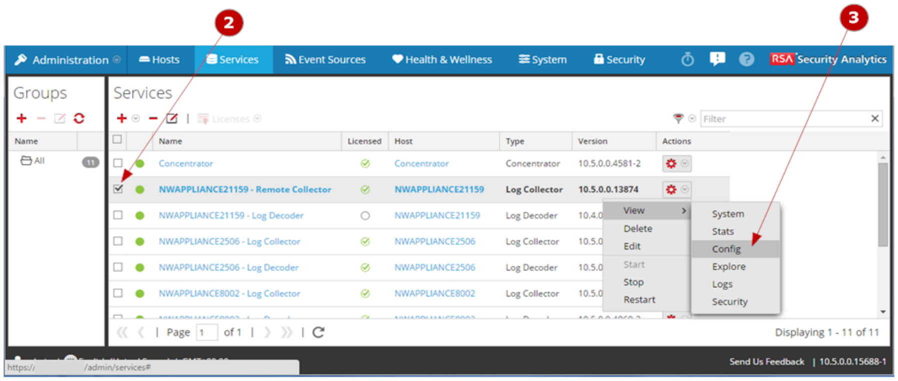
Configure Remote Collector to Push Event Data to Remote Collector

You can configure a Remote Collector to push event data to a Remote Collector.

The following figure shows you how to configure a Remote Collector to push event data to a Remote Collector.



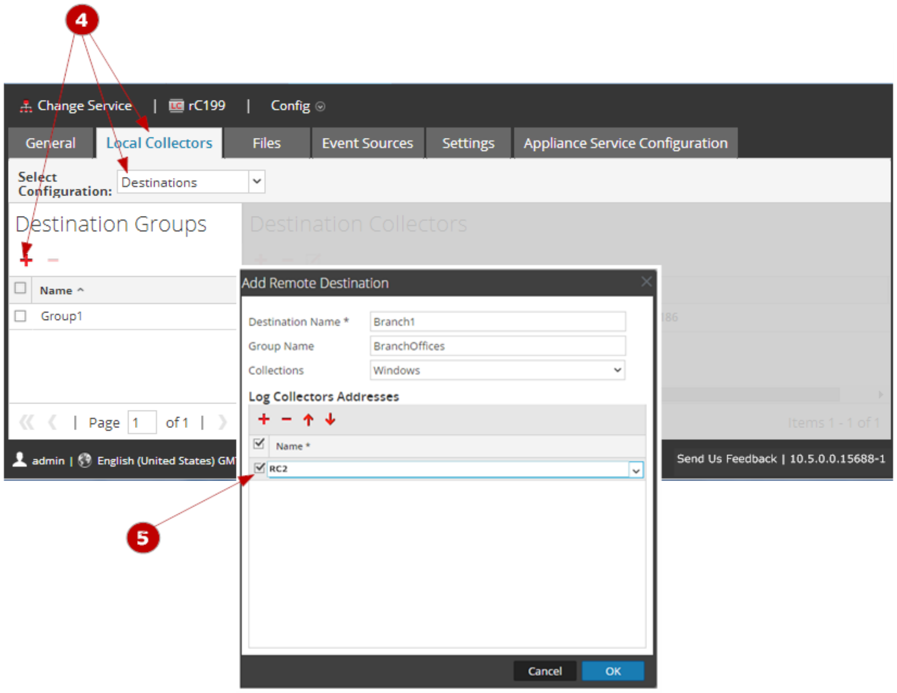
1 Access the **Services** view.



☐	Name	Licensed	Host	Type	Version	Actions
☐	Concentrator	✓	Concentrator	Concentrator	10.5.0.0.4581-2	
☑	NWAPPLIANCE21159 - Remote Collector	✓	NWAPPLIANCE21159	Log Collector	10.5.0.0.13874	
☐	NWAPPLIANCE21159 - Log Decoder	○	NWAPPLIANCE21159	Log Decoder	10.4.0	
☐	NWAPPLIANCE2506 - Log Collector	✓	NWAPPLIANCE2506	Log Collector	10.5.0	
☐	NWAPPLIANCE2506 - Log Decoder	✓	NWAPPLIANCE2506	Log Decoder	10.5.0	
☐	NWAPPLIANCE8002 - Log Collector	✓	NWAPPLIANCE8002	Log Collector	10.5.0	

2 Select a Remote Collector.

3 Click ⌄ under **Actions** and select **View** > **Config**to display the Log Collection configuration parameter tabs.



Select Configuration: Destinations

Destination Name * Branch1

Group Name BranchOffices

Collections Windows

Log Collectors Addresses

☑ Name *

☑ RC2

4 Select the **Local Collectors** tab, select **Destinations** in **Select Configuration** drop-down menu, and click + in **Destination Groups** to display the **Add Remote Destinations** dialog.

5 Set up the Destination Groups.

Configure the Selected Remote Collector to Push Events to Specified Remote Collector

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In **Services**, select a **Remote Collector**.
3. Click ⌄ under **Actions** and select **View** > **Config**.

   The **Log Collector Service Config** view is displayed with the **Log Collector General** tab open.
4. Select the **Local Collectors** tab.
5. Select **Destinations** in the **Select Configurations** drop-down menu.
6. In the **Destination Groups** panel section, select +.

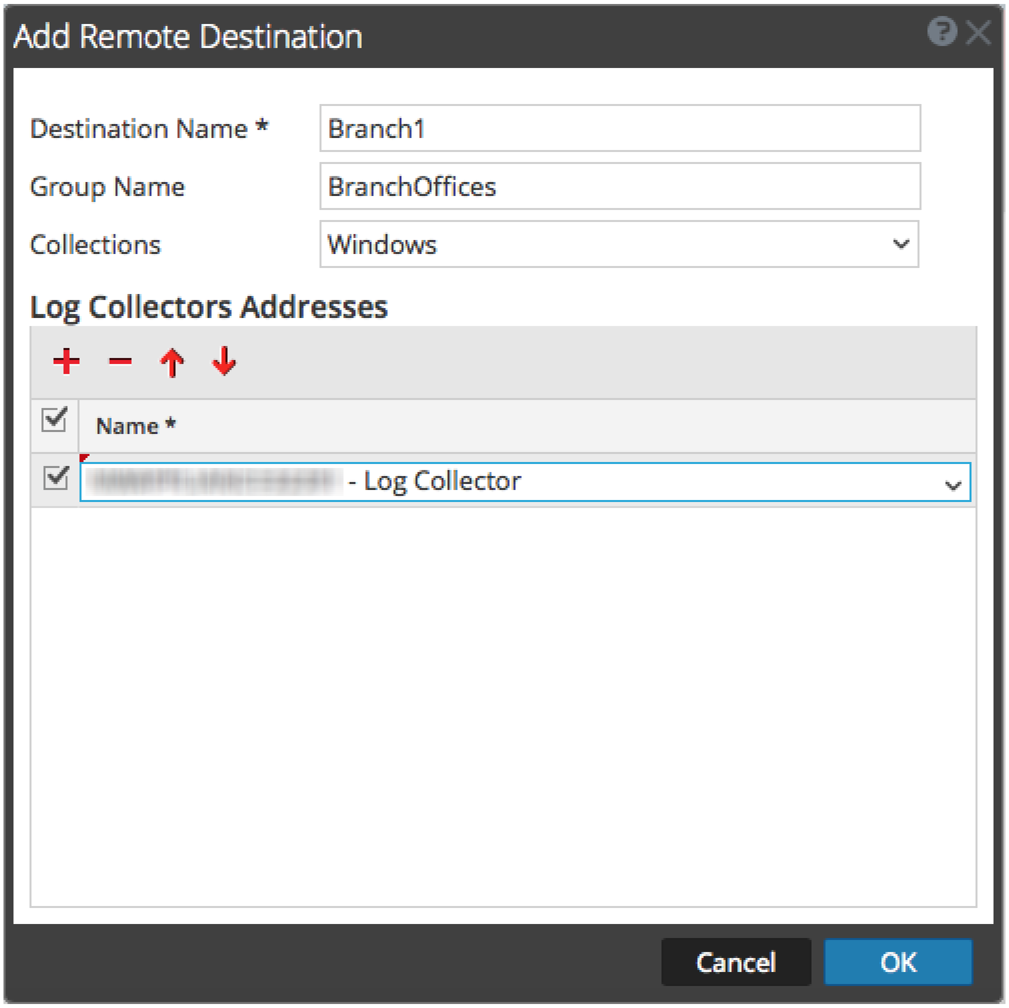
   The **Add Remote Destination** dialog is displayed.
7. Set up a **Destination Group**:

   a. Enter a **Destination Name**.

   b. (Optional) **Enter a Group Name**. If you leave Group Name blank, Security Analytics sets it to the value that you specified in Destination Name.

   c. Select one or more collection protocols in the **Collections** drop-down list.

   d. Under **Log Collectors Addresses**, click + to select a Remote Collector.



Add Remote Destination

Destination Name * Branch1

Group Name BranchOffices

Collections Windows

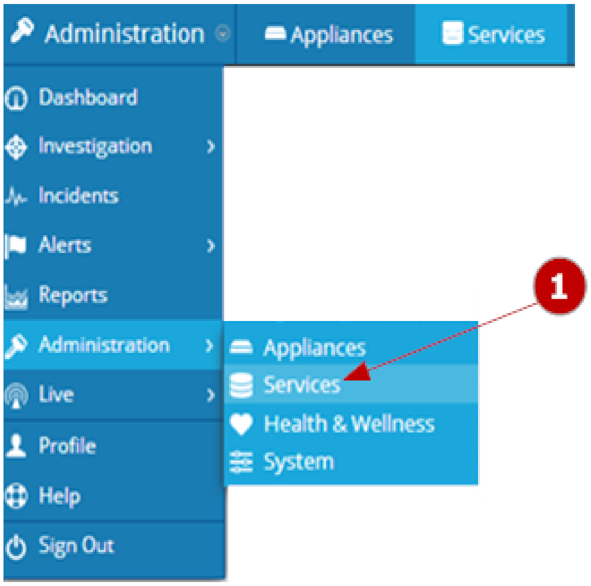
Log Collectors Addresses

☑	Name *
☑	[redacted] - Log Collector

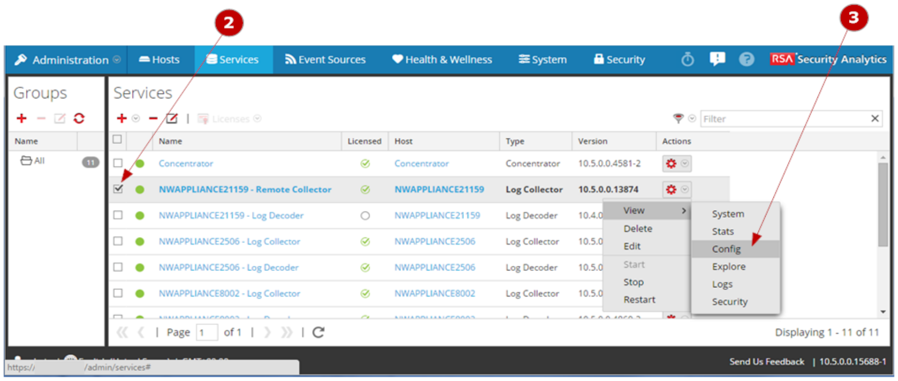
Note: If you do not select a collection protocol, the Remote Collector pushes all collection protocols to the Remote Collectors.

Configure Remote Collector to Pull Event Data from a Remote Collector

The following figure shows you how to configure a Remote Collector to pull events from specified Remote Collector.



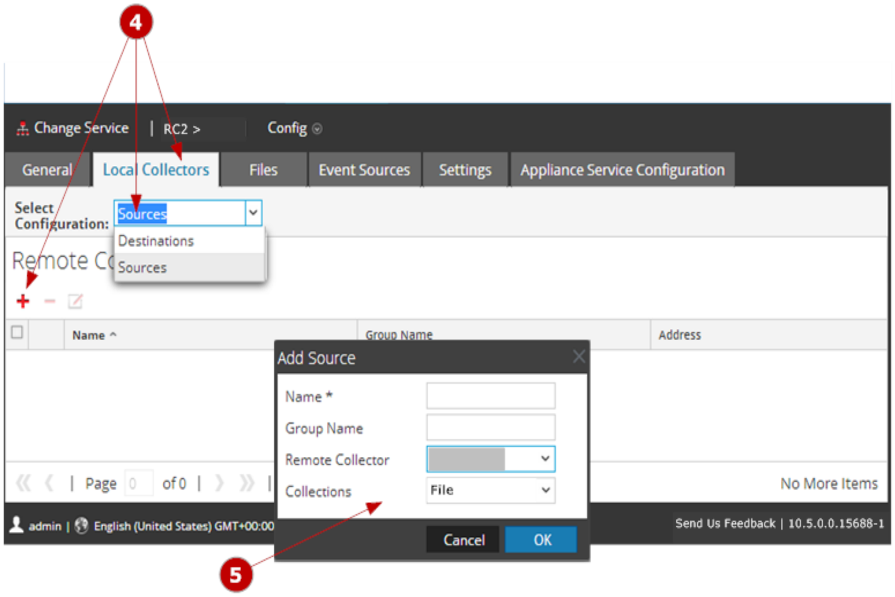
1 Access the **Services** view.



☐		Name	Licensed	Host	Type	Version	Actions
☐	●	Concentrator	✓	Concentrator	Concentrator	10.5.0.0.4581-2	⚙ ⌄
☑	●	NWAPPLIANCE21159 - Remote Collector	✓	NWAPPLIANCE21159	Log Collector	10.5.0.0.13874	⚙ ⌄
☐	●	NWAPPLIANCE21159 - Log Decoder	○	NWAPPLIANCE21159	Log Decoder	10.4.0	
☐	●	NWAPPLIANCE2506 - Log Collector	✓	NWAPPLIANCE2506	Log Collector	10.5.0	
☐	●	NWAPPLIANCE2506 - Log Decoder	✓	NWAPPLIANCE2506	Log Decoder	10.5.0	
☐	●	NWAPPLIANCE8002 - Log Collector	✓	NWAPPLIANCE8002	Log Collector	10.5.0	

2 Select a Remote Collector.

3 Click ⌄ under **Actions** and select **View** > **Config** to display the Log Collection configuration parameter tabs.



Select Configuration: Sources

Collections: File

4 Select the **Local Collectors** tab, select **Sources**in **Select Configurations** drop-down menu, and click + in **Remote Collectors** to display the **Add Source**dialog.

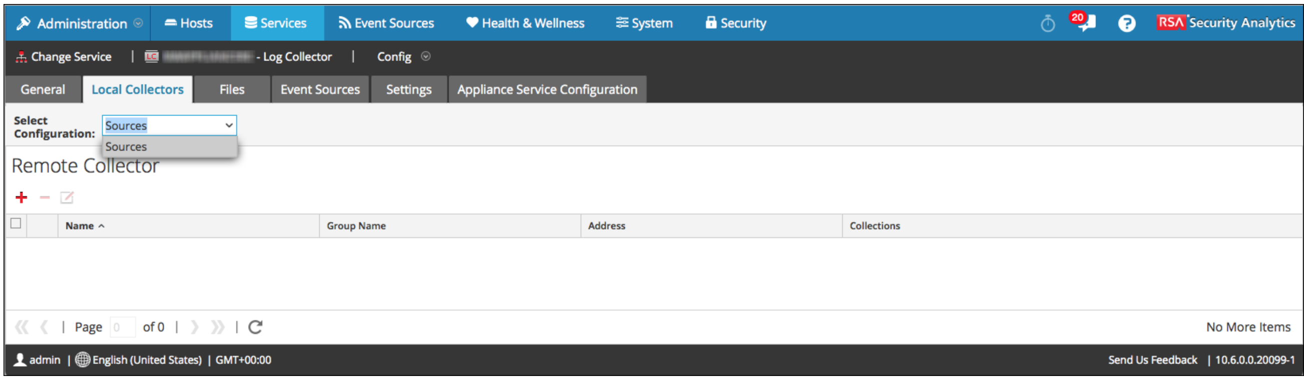
5 In the **Add Source** dialog, select the Remote Collector from which you want to pull events.

Configure the Selected Remote Collector to Pull Events from Specified Remote Collector

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In **Services**, select a **Remote Collector**.
3. Click ⌄ under **Actions** and select **View** > **Config**.

   The **Service Config** view is displayed with the **Log Collector General** tab open.
4. Select the **Local Collectors** tab.

5. Select **Sources** in the **Select Configurations** drop-down menu.



Select Configuration: Sources

6. In the **Remote Collectors** panel, select +.

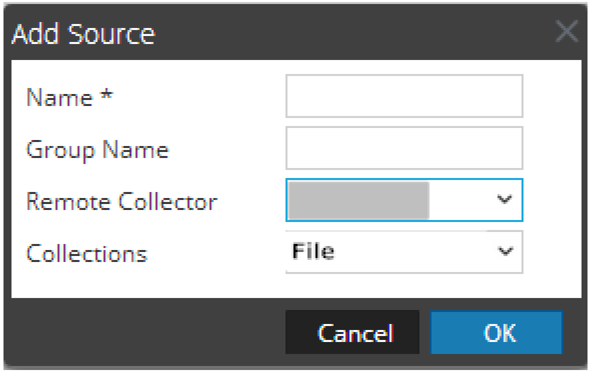
   The **Add Source** dialog is displayed.

7. In the **Add Source** dialog:

   a. Select one or more collection protocols.

      If you do not select a collection protocol, the Remote Collector pulls all collection protocols from the Remote Collector.

   b. Click **OK**.



Name *:

Group Name:

Remote Collector: [redacted]

Collections: File

The Remote Collector is added to the Remote Collector section. When the Log Collector starts collecting data, it pulls event data from this Remote Collector.

Parameters

[Reference - Remote/Local Collectors Configuration Parameters Interface]

Throttle Remote Collector to Local Collector Bandwidth

To improve performance, you can throttle the bandwidth to control the rate that the Remote Collector sends event data to Local Collector or between Message Brokers. To do this, you configure the Linux kernel's filtering and IpTable functionality.

This works for both push and pull Remote Collector configurations. The **set-shovel-transfer-limit.sh** shell script located on the **/opt/netwitness/bin** automates the configuration of the kernel filter and iptables related to this port.

Context

After reading this topic, you know how to throttle Remote Collector to Local Collector bandwidth using the **set-shovel-transfer-limit.sh** shell script by reviewing:

- The **set-shovel-transfer-limit.sh** shell script command line help.

  > **Note:** The filter value that you need to set depends on the rate at which remote log collector is sending events to the Local Collector.

- An example that sets the Filter to 4096 kilobits per second.

Return to Procedures

set-shovel-transfer-limit.sh Command Line Help

Issue the `-h` command to display help for `set-shovel-transfer-limit.sh` shell script.

```
cd /opt/netwitness/bin
./set-shovel-transfer-limit.sh
```

```
Usage: set-shovel-transfer-limit.sh -s|-c|-d|[-i interface] [-r rate]
```

where:

-c = clear existing

-d = display filter

-s = set new values

-i = interface is the name of the network interface. default=eth0

-r = rate is the bandwidth rate. default=256kbps
Bandwidths or rates can be specified in:
nolimit = disables throttling
kbit = Kilobits per second
mbit = Megabits per second
kbps = Kilobytes per second
mbps = Megabytes per second
bps = Bytes per second

Set the Filter to 4096 Kilobits per Second

```
[root@<hostname> bin]# ./set-shovel-transfer-limit.sh -s -r 4096kbit
```

```
RATE=4096kbit
 PORTNUMBER=5671
 DEVICE_INTERACE=eth0
```

```
iptables: No chain/target/match by that name.
 iptables: No chain/target/match by that name.
 iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]
```

Current/new values...

```
iptables -t mangle -n -v -L
 Chain PREROUTING (policy ACCEPT 2 packets, 161 bytes)
 pkts bytes target  prot opt in  out  source
destination
 Chain INPUT (policy ACCEPT 2 packets, 161 bytes)
 pkts bytes target prot opt in out   source          destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target prot opt in out   source          destination

Chain OUTPUT (policy ACCEPT 2 packets, 248 bytes)
 pkts bytes target prot opt in out   source          destination
     0    0 MARK   tcp -- *    eth0     0.0.0.0/0     0.0.0.0/0
multiport dports 5671 MARK set 0xa
     0    0 MARK   tcp -- *    eth0     0.0.0.0/0    0.0.0.0/0
multiport sports 5671 MARK set 0xa

Chain POSTROUTING (policy ACCEPT 2 packets, 248 bytes)
 pkts bytes target prot opt in out   source          destination

tc -s -d class show dev eth0
 class htb 1:1 root rate 10000Kbit ceil 10000Kbit burst 1600b/8
mpu 0b overhead 0b cburst 1600b/8 mpu 0b overhead 0b level 7
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 20000 ctokens: 20000

class htb 1:2 parent 1:1 prio 0 quantum 51200 rate 4096Kbit ceil
4096Kbit burst 1599b/8 mpu 0b overhead 0b cburst 1599b/8 mpu 0b
overhead 0b level 0
 Sent 0 bytes 0 pkt (dropped 0, overlimits 0 requeues 0)
 rate 0bit 0pps backlog 0b 0p requeues 0
 lended: 0 borrowed: 0 giants: 0
 tokens: 48828 ctokens: 48828
```

Reference - Remote/Local Collectors Configuration Parameters Interface

This topic introduces the user interface for configuring the Log Collection deployment parameters

The Services Config view is the view on which you maintain all the Log Collection parameters. The tab in which you maintain the deployment parameters referred to in this guide is the **Remote/Local** Collectors tab:

- If you are configuring a Local Collector, Security Analytics displays the **Remote Collectors** tab so that you can configure the Local Collector to pull events from Remote Collectors.
- If you are configuring a Remote Collector, Security Analytics displays the **Local Collectors** tab so that you can configure the Remote Collector to push events to a Local Collector.

This topic introduces features of the **Services Config view** > **Remote Collectors/Local Collectors** tab

Remote/Local Collectors Tab

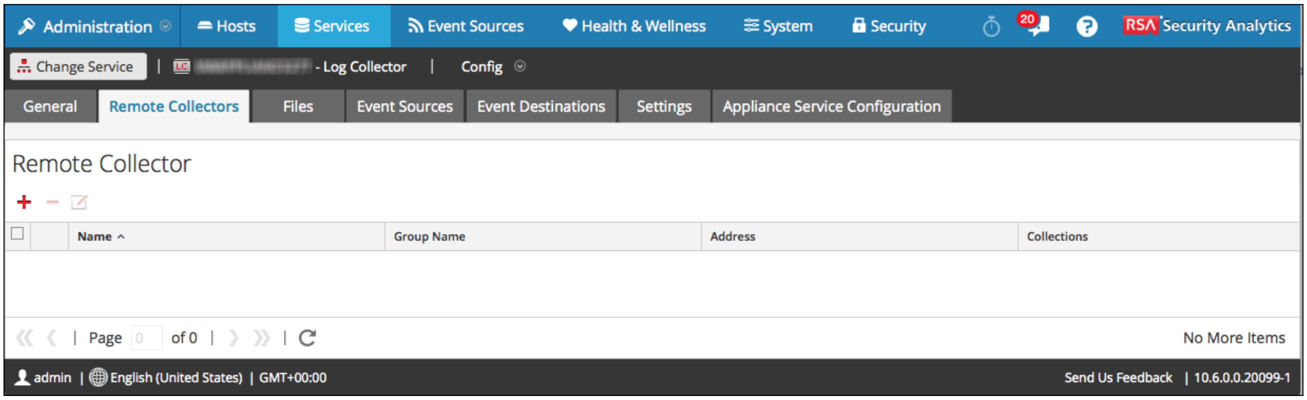
If you deploy Remote Collectors, the RSA Security Analytics administrator must configure the method of sending events collected by Remote Collectors to the Local Collector.

To access this tab:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In **Services**, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.

   The **Service Config** view is displayed with the **Log Collector General** tab open.
4. Select the **Remote Collectors** tab.

The following figure depicts the **Remote Collectors** tab for a Local Collector that is configured to pull events from a Remote Collector. Security Analytics displays this tab when you have selected a Local Collector in **Administration** > **Services**.



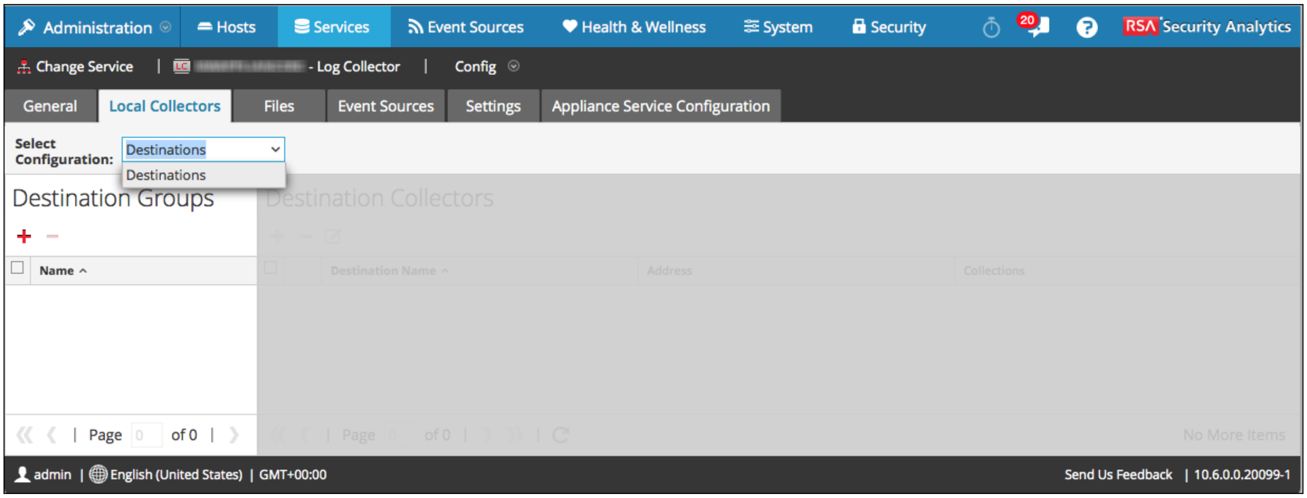
Local Collectors Tab for a Remote Collector

To access this tab:

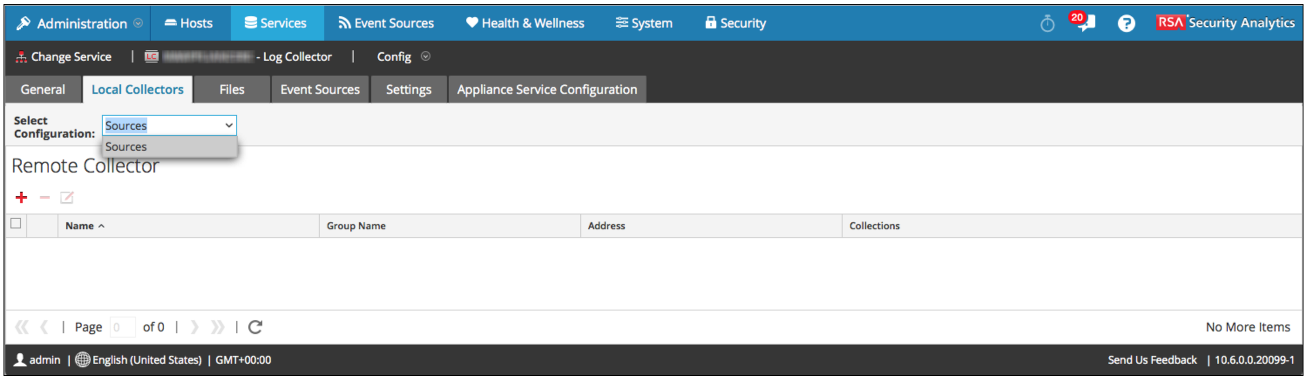
1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In **Services**, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.

   The **Service Config** view is displayed with the **Log Collector General** tab open.
4. Select the **Local Collectors** tab.

The following figure depicts a **Local Collectors** tab for a Remote Collector that is configured to push events to a Local Collector or another Remote Collector.



The following figure depicts the Local Collectors tab for a Remote Collector that is configured to pull events from a Remote Collector. Security Analytics displays this tab when you have selected a Remote Collector in **Administration** > **Services**.



Remote Collectors Tab

On a Local Collector, the Remote Collectors panel provides a way to add or delete Remote Collectors from which the Local Collector pulls events.

Remote Collector Panel

Column	Description
+	Displays the **Add Source** dialog in which you select the Remote Collectors from which you want the Local Collector to pull events.
−	Deletes the Remote Collector from the Local Collector Remote Collectors panel.
✎	Displays the **Edit Source** dialog for the selected Remote Collector.
□	Selects Remote Collectors.
Name	Names of the Remote Collectors from which the Local Collector currently pulls events.
Address	IP Addresses of the Remote Collectors from which the Local Collector currently pulls events.

Column	Description
Collections	Choose which collection protocols that the Remote Collector pushes to a Local Collector: **Check Point** **File** **Netflow** **ODBC** **Plugins** **SDEE** **SNMP** **VMware** **Windows** **Windows Legacy** You can select any combination of protocols. If you do not select a protocol, Security Analytics selects all protocols.

Local Collector Tab

On a Remote Collector, the Local Collector panel provides a way to add or delete the Local Collectors to which you want to the Remote Collector to push events.

Select the **Destination** or **Source** in the **Select Configuration** drop-down menu.

- **Destination** displays the **Add Remote Destination** dialog.
- Source displays the **Add Source** dialog.

The following table describes the Add Source dialog.

Column	Description
+	Displays the **Add Source** dialog in which you select the Remote Collectors from which you want the Local Collector to pull events.
−	Deletes the Remote Collector from the Local Collector Remote Collectors panel.
✎	Displays the **Edit Source** dialog for the selected Remote Collector.

Column	Description
□	Selects Remote Collectors.
Name	Names of the Remote Collectors from which the Local Collector currently pulls events.
Address	IP Addresses of the Remote Collectors from which the Local Collector currently pulls events.

The following table describes the Local Collectors Panel.

Column	Description
+	Displays the **Add Remote Destination** dialog for the Group that you selected. You add destination Local Collectors for this group to which you want the Remote Collector to push events.
−	Deletes the destination Log Collector from the group.
	Displays the **Edit Remote Destination** dialog for the selected destination Local Collector.
□	Selects a destination Local Collector.
Destination Name	Displays the name of the destination Local Collector.
Address	Displays the IP address of the destination Local Collector.

Column	Description
Collections	Choose which collection protocols that the Local Collector pulls from a Remote Collector: **Check Point** **File** **Netflow** **ODBC** **Plugins** **SDEE** **SNMP** **VMware** **Windows** **Windows Legacy** You can select any combination of protocols. If you do not select a protocol, Security Analytics selects all protocols.

Tasks

Configure Local and Remote Collectors

Troubleshoot Log Collection Deployment

This topic suggests how to resolve problems you may encounter during deployment

Security Analytics informs you of Log Collector problems or potential problems in the following two ways:

- Log files.
- Health and Wellness Monitoring view

Log Files

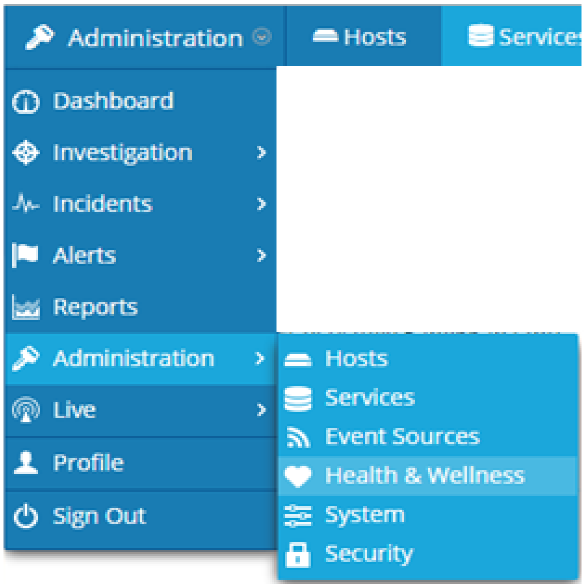
If you have an issue with a particular event source collection protocol, you can review debug logs to investigate this issue. Each event source has a Debug parameter that you can enable (set parameter to On or Verbose) to capture these logs.

Only enable debugging if you have a problem with this event source and you need to investigate this problem. If you have Debug enabled all the time it will adversely affect the performance of the Log Collector.

Security Analytics has a set of error messages associated with Log Collection that it includes in log files.

Health and Wellness Monitoring

Health and Wellness monitoring makes you aware of potential hardware and software problems in a timely manner so that you can avoid to outages. RSA recommends that you monitor the Log Collector statistical fields to make sure that the service is operating efficiently and is not at or near the maximum values you have configured. You can monitor the statistics described in the **Administration** > **Health & Wellness** view.



Log Collection Configuration Guide

This guide tells you how to configure Log Collection after you have deployed it (that is, after you set up Local and Remote Collectors).

This guide tells you:

- What Log Collection does, how it works from a high level, and provides high-level deployment diagrams.
- How to start collecting events.
- Where to find instructions to set up more complex deployments.
- How to start, pause, and stop any collection protocol.
- What the structure of the Log Collection Configuration User Interface is.
- Which tools to use to troubleshoot Log Collection issues and lists global troubleshooting instructions.
- How to fine tune and customize Log Collection in your environment.

This guide does not tell you how to:

- Get started by creating the basic, minimum deployment and configuration. This information is in the Log Collection Getting Started Guide.
- Deploy Log Collection in multiple locations with high availability and load balancing. This information is in the Log Collection Deployment Guide.
- Configure individual collection protocols. Instructions are in the individual Log Collection Guides:

- AWS (CloudTrail) Collection Configuration Guide
- Check Point Collection Configuration Guide
- File Collection Protocol Configuration Guide
- Netflow Collection Configuration Guide
- ODBC Collection Configuration Guide
- SDEE Collection Configuration Guide
- SNMP Collection Configuration Guide
- VMware Collection Configuration Guide
- Windows Collection Configuration Guide
- Windows Legacy and NetApp Collection Configuration Guide
- Configuration Guides for each supported event source.

  See the Event Source Configuration Guide space on RSA Link for these guides.

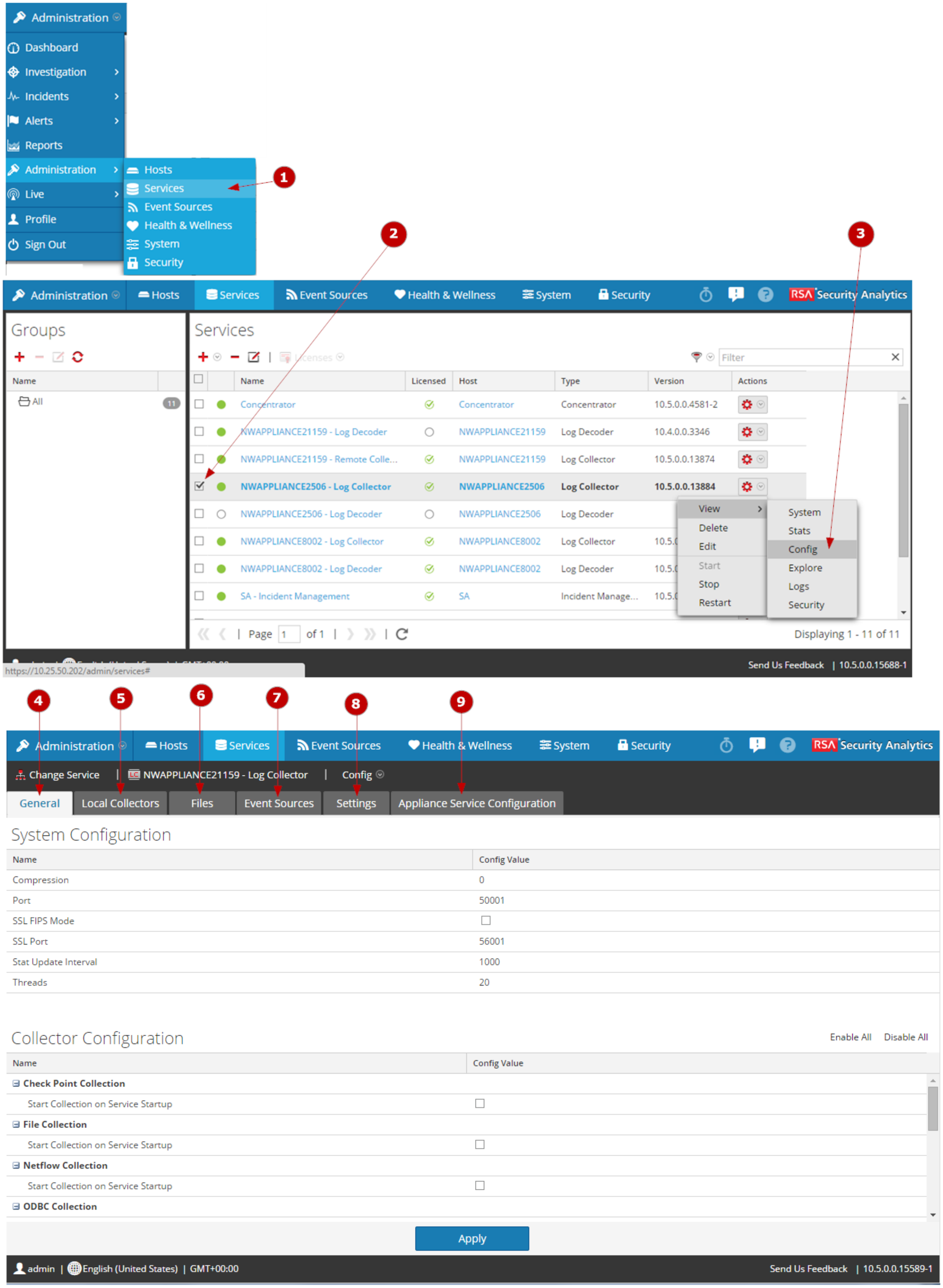
The Basics

This topics describes the configuration process and illustrates how to perform this configuration using the Security Analytics user Interface.

Log Collection Configuration

After you deploy Log Collection, you must configure the parameters for each log collector service running locally or remotely. You perform this configuration in the Log Collection Configuration views for service.

Configuration Parameter Interface



Services

☐		Name	Licensed	Host	Type	Version	Actions
☐	●	Concentrator	✓	Concentrator	Concentrator	10.5.0.0.4581-2	⚙
☐	●	NWAPPLIANCE21159 - Log Decoder	○	NWAPPLIANCE21159	Log Decoder	10.4.0.0.3346	⚙
☐	●	NWAPPLIANCE21159 - Remote Colle...	✓	NWAPPLIANCE21159	Log Collector	10.5.0.0.13874	⚙
☑	●	NWAPPLIANCE2506 - Log Collector	✓	NWAPPLIANCE2506	Log Collector	10.5.0.0.13884	⚙
☐	○	NWAPPLIANCE2506 - Log Decoder	○	NWAPPLIANCE2506	Log Decoder		
☐	●	NWAPPLIANCE8002 - Log Collector	✓	NWAPPLIANCE8002	Log Collector	10.5.(	
☐	●	NWAPPLIANCE8002 - Log Decoder	✓	NWAPPLIANCE8002	Log Decoder	10.5.(	
☐	●	SA - Incident Management	✓	SA	Incident Manage...	10.5.(	

System Configuration

Name	Config Value
Compression	0
Port	50001
SSL FIPS Mode	☐
SSL Port	56001
Stat Update Interval	1000
Threads	20

Collector Configuration

Name	Config Value
Check Point Collection	
Start Collection on Service Startup	☐
File Collection	
Start Collection on Service Startup	☐
Netflow Collection	
Start Collection on Service Startup	☐
ODBC Collection	

1. In the **Security Analytics** menu, select **Administration** > **Services**.

2. In the **Services** grid, select the log collector service you want to configure.

3. In the toolbar, select **View** > **Config**.

4. Click the **General** tab to review the high-level system parameters and enable or disable the automatic start of collection protocols.

5. Click the **Remote Collectors/Local Collectors** tab to configure the method of sending events collected by Remote Collectors to the Local Collector.

6. Click the **Files** tab to edit service configuration files for the Log Decoder as text files.

7. Click the **Event Sources** tab to configure parameters for supported collection protocols.

8. Click the **Settings** tab to configure the lockbox and manage certificates.

9. Click the **Appliance Service Configuration** tab to review the statistics for the Log Decoder host.

Procedures

This topic provides an overview of the end-to-end sequential configuration procedure for Log Collection with links to each of the configuration steps.

Configuration steps for Log Collector must occur in the specific sequence listed in the table below. When these steps are complete, the Log Collector is operational, and the only additional configuration required would be due to updates to your system or software.

Configuration Checklist

Note: The steps in this list are in the order in which you must complete them.

Description	√
Step 1. Download Latest Content from LIVE	
Step 2. Configure Settings (Lockbox Security Settings and Certificates)	
Step 3. Configure Event Sources in Security Analytics	
Step 4. Configure the Event Sources to Send Events to Security Analytics	
Step 5. Start and Stop Services for Configured Protocols	
Step 6. Verify That Log Collection Is Working	

Step 1. Download Latest Content from LIVE

Overview

This topic sends you to the RSA Content and Resources documentation in which you will find the instructions for retrieving Log Collection content.

Context

LIVE is Security Analytics's Content Management System from which you download the latest content. The two resource types you use to download Log Collection content are:

- **RSA Log Collector** - content enabling the collection of event source types.
- **RSA Log Device** - the latest supported event source parsers. See **Adding or Updating Supported Event Source Log Parsers** in the *RSA Content and Resources Guide*.

Identity Feed Prerequisites

In order to create an identity feed, you need to have:

- A Log Collector service with Windows Collection configured and enabled
- Created and configured an identity feed in LIVE. See **Create an Identity Feed** in the *Live Resource Management Guide* for instructions on how to create an identity feed in the LIVE Content Management System.

Step 2. Configure Settings

Overview

This topic introduces the settings that you can configure for Log Collection.

Context

After completing this procedure, you will have selected the Log Collector settings that you want to configure.

Procedure

To select the Log Collector settings that you want to configure:

1. Select a Log Collector service in the **Event Sources** tab of the **Administration > Services > View > Config** view.

   The **Log Collector Configuration Parameters** view is displayed.

2. Click the **Settings tab Event Source** tab and choose one of the two following options:

   - Lockbox
   - Certificates

Parameters:

Log Collection Settings Tab

Configure Lockbox Security Settings

This topic tells you how to configure Lockbox Security Settings. A new Lockbox stat corresponds to an Out-of-the-Box Alarm notification that monitors the status of the lockbox.

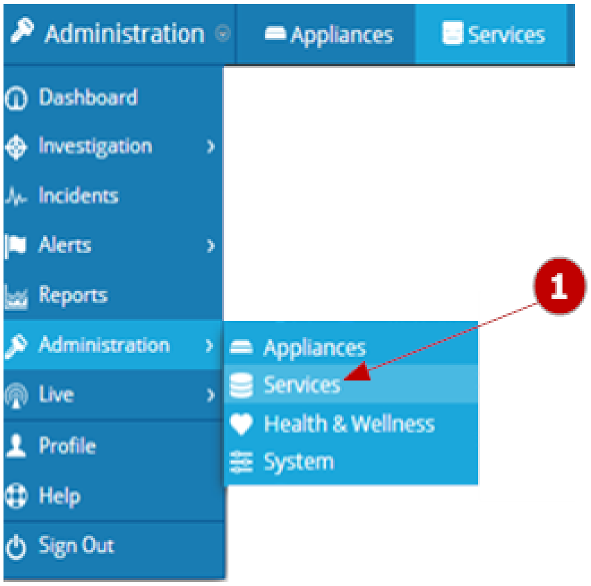
After completing this procedure, you will have:

- Set the Lockbox password
- Changed the Lockbox password
- Reset the Stable System value
- Generated a new encryption key
- Displayed a Lockbox stat

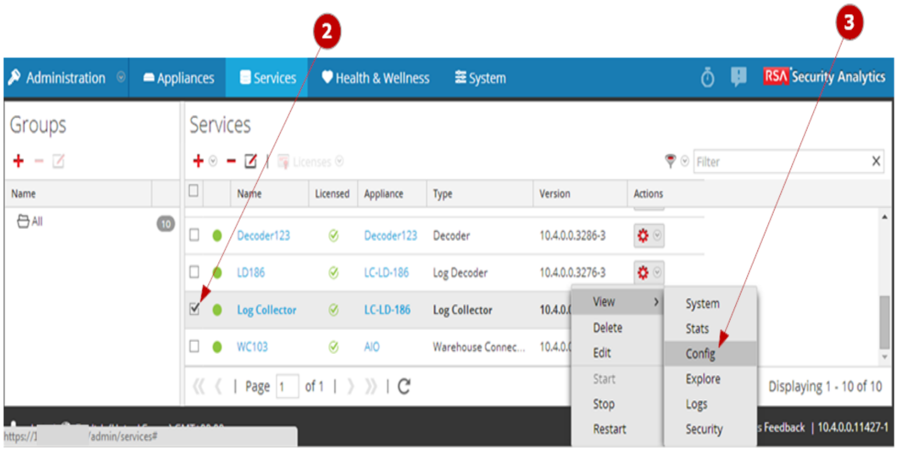
Note: You can configure Health & Wellness to notify when there is an issue during Lockbox configuration.

Return to Procedures

The following figure shows you how to configure Lockbox Security Settings.



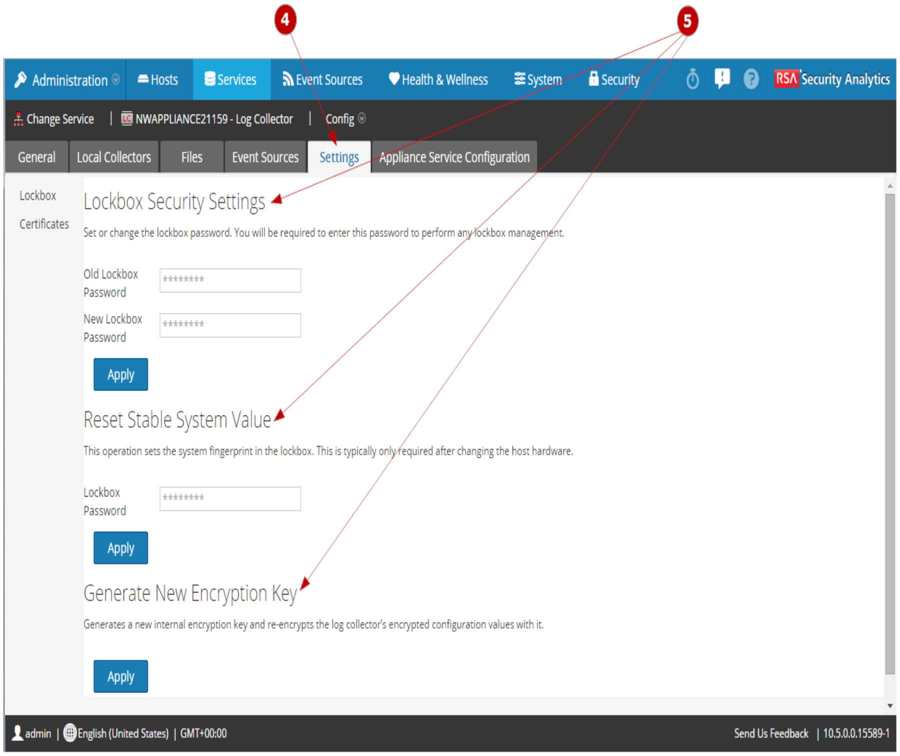
1 Access the **Services** view.



☐		Name	Licensed	Appliance	Type	Version	Actions
☐	●	Decoder123	✓	Decoder123	Decoder	10.4.0.0.3286-3	
☐	●	LD186	✓	LC-LD-186	Log Decoder	10.4.0.0.3276-3	
☑	●	Log Collector	✓	LC-LD-186	Log Collector	10.4.0.	
☐	●	WC103	✓	AIO	Warehouse Connec...	10.4.0.	

2 Select a **Log Collection** service.

3 Click ⌄ under **Actions** and select **View > Config** to display the Log Collection configuration parameter tabs.



Lockbox Security Settings

Set or change the lockbox password. You will be required to enter this password to perform any lockbox management.

Old Lockbox Password ********

New Lockbox Password ********

Apply

Reset Stable System Value

This operation sets the system fingerprint in the lockbox. This is typically only required after changing the host hardware.

Lockbox Password ********

Apply

Generate New Encryption Key

Generates a new internal encryption key and re-encrypts the log collector's encrypted configuration values with it.

Apply

4 Select the **Settings** tab.

5 Modify the **Lockbox** parameters.

Procedures

Set the Lockbox Password

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. Click the **Settings** tab.
5. In the options panel, select **Lockbox** to maintain Lockbox settings.
6. Under **Lockbox Security Settings**, enter a password in the **New Lockbox Password** field and click **Apply**.

Change the Lockbox Password

In the **Security Analytics** menu, select **Administration** > **Services**.

1. In the **Services** grid, select a **Log Collector** service.
2. Click ⌄ under **Actions** and select **View** > **Config**.
3. Click the **Settings** tab.
4. In the options panel, select **Lockbox** to maintain Lockbox settings.
5. Enter the current password in the **Old Lockbox Password** field.
6. Enter a new password in the **New Lockbox Password** field.
7. Click **Apply**.
   Security Analytics changes the old password to the new password.

Create a New Lockbox

Caution: If you forgot the current password, you cannot retrieve it from the Lockbox. This means that you must recreate the lockbox. If you recreate the lockbox, you have a new encryption key which means that passwords for any existing event sources will no longer be able to be decrypted. You must then reset the password for each event source.

You may need to create a new lockbox if you forget your password, or if a catastrophic event occurs.

To create a new lockbox:

1. On the Log Collector appliance, remove all the files in the directory **/etc/netwitness/ng/vault**.
2. In the **Security Analytics** menu, select **Administration** > **Services**.
3. In the **Services** grid, select a **Log Collector** service.
4. Click ⌄ under **Actions** and select **View** > **Config**.
5. Click the **Settings** tab.
6. In the options panel, select **Lockbox** to maintain Lockbox settings.
7. Enter a new password in the **New Lockbox Password** field.

Note: Your password is not required in order to create a new lockbox.

8. Click **Apply**.

Reset the Stable System Value

> **Caution:** If several stable system values change due to system upgrades, you must update the host system fingerprint. If you do not update the host system fingerprint, the Log Collector cannot open the Lockbox and this will affect log collection

To reset the Lockbox password for new appliance hardware (set the system fingerprint on the new hardware):

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. Click the **Settings** tab.
5. Under **Reset Stable System Value**, enter a password in the **Lockbox Password** field and click **Apply**.

Generate New Encryption Key

If you generate a new encryption key, passwords for any existing event sources can no longer be decrypted so you must reset the password for each event source.

To generate a new encryption key that is applied to your event source password parameters:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. Click the **Settings** tab.
5. Under **Generate New Encryption Key**, click **Apply**.

Display Lockbox Stat

The Lockbox stat reflects the state of the lockbox and whether there are any event sources that use the lockbox. There is an alarm associated with the Lockbox stat that monitors the status of the lockbox. An alarm condition occurs when the Lockbox is in either a Not Found or Error Message state.

The Lockbox stat can be one of the following values:

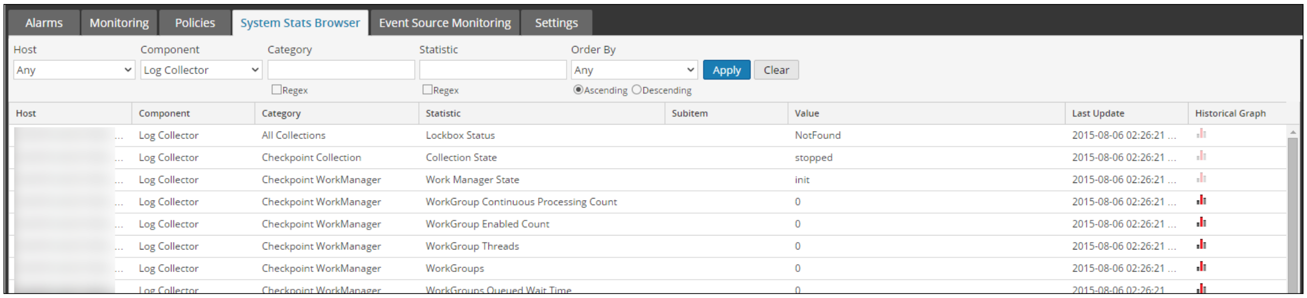
- *OK*
- *Not Required*

- *Not Found*
- *Error Message*

To display the Lockbox stat:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. Click the **System Stats Browser** tab.

The following figure displays a Lockbox status that is in a **Not Found** state that triggers an alarm condition.



Host: Any
Component: Log Collector
Category: □Regex
Statistic: □Regex
Order By: Any ● Ascending ○ Descending

Host	Component	Category	Statistic	Subitem	Value	Last Update	Historical Graph
[redacted]...	Log Collector	All Collections	Lockbox Status		NotFound	2015-08-06 02:26:21 ...	📊
[redacted]...	Log Collector	Checkpoint Collection	Collection State		stopped	2015-08-06 02:26:21 ...	📊
[redacted]...	Log Collector	Checkpoint WorkManager	Work Manager State		init	2015-08-06 02:26:21 ...	📊
[redacted]...	Log Collector	Checkpoint WorkManager	WorkGroup Continuous Processing Count		0	2015-08-06 02:26:21 ...	📊
[redacted]...	Log Collector	Checkpoint WorkManager	WorkGroup Enabled Count		0	2015-08-06 02:26:21 ...	📊
[redacted]...	Log Collector	Checkpoint WorkManager	WorkGroup Threads		0	2015-08-06 02:26:21 ...	📊
[redacted]...	Log Collector	Checkpoint WorkManager	WorkGroups		0	2015-08-06 02:26:21 ...	📊
[redacted]	Log Collector	Checkpoint WorkManager	WorkGroups Queued Wait Time		0	2015-08-06 02:26:21	📊

Parameters:

Lockbox Configuration Parameters

Configure Certificates

This topic tells you how to add certificates.

After completing this procedure, you will have added a certificate.

Return to Procedures

Procedure

To add a certificate:

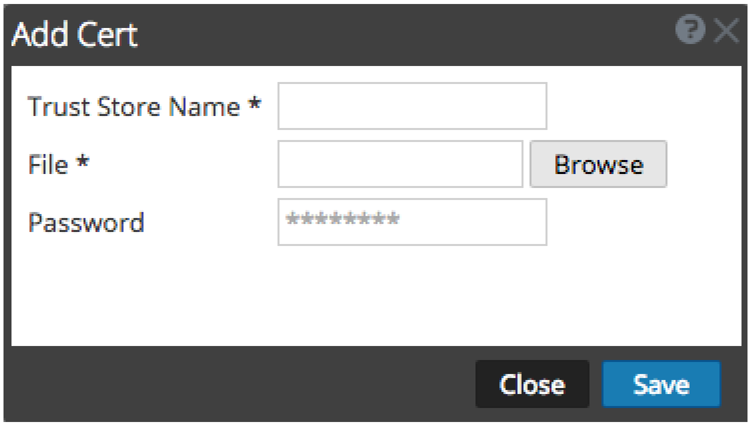
1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. Click the **Settings** tab.
5. In the options panel, select **Certificates**.

6. Click ✚ in the **Certificates** tool bar.

   The **Add Cert** dialog is displayed.

7. Click **Browse** and select a certificate (***.PEM**) from your network.

8. Specify a password (if required).



Add Cert

Trust Store Name *

File *

Password: *********

9. Click **Save**.

Parameters

Certificates Configuration Parameters

Step 3. Configure Event Sources in Security Analytics

Collection Protocol Configuration Guides

Return to Procedures

Use these guides to configure the collection protocols for the event sources you have in your enterprise network.

- *AWS (CloudTrail) Collection Configuration Guide*
- *Check Point Collection Configuration Guide*
- *File Configuration Guide*
- *Netflow Collection Configuration Guide*
- *ODBC Collection Configuration Guide*
- *SDEE Collection Configuration Guide*
- *SNMP Collection Configuration Guide*
- *Configure Syslog Event Sources for the Remote Collector*

- *Configure Syslog Event Filters for the Remote Collector*
- *VMware Collection Configuration Guide*
- *Windows Collection Configuration Guide*
- *Windows Legacy and NetApp Configuration Guide*
- *Supported Event Sources*

Add Certificates and Passwords

This topic tells you how to add certificates.

After completing this procedure, you will have added a certificate.

Return to Procedures

Procedure

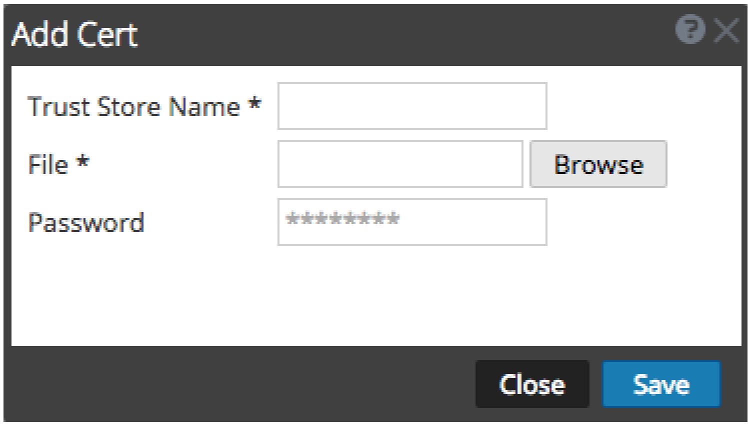
To add a certificate:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.
4. Click the **Settings** tab.
5. In the options panel, select **Certificates**.
6. Click + in the **Certificates** tool bar.

   The **Add Cert** dialog is displayed.

   > **Note:** Make sure that the certificate you add is a valid certificate.

7. Click **Browse** and select a certificate (***.PEM**) from your network.
8. Specify a password (if required).



9. Click **Save**.

Parameters

Certificates Configuration Parameters

Import, Export, and Edit Event Sources in Bulk

This topic tells you how to import, export, and edit event sources in bulk.

You can use the bulk export option to export the event source details of your current set up and store it. This data can be imported in bulk when you face a problem with your current set up and require the event source data you had.

You can use the bulk edit feature when you have multiple event sources that need a specific modification. You can select all the sources and apply the edit option across them at a time and avoid applying the change one by one.

After completing this procedure, you will have...

- Imported event sources in bulk.
- Exported event sources in bulk.
- Edited event sources in bulk.

Return to Procedures

See Also

Similar procedures are available from the **Event Sources** module (Administration > Event Sources). For details, see the following topics in the *Event Source Management Guide*:

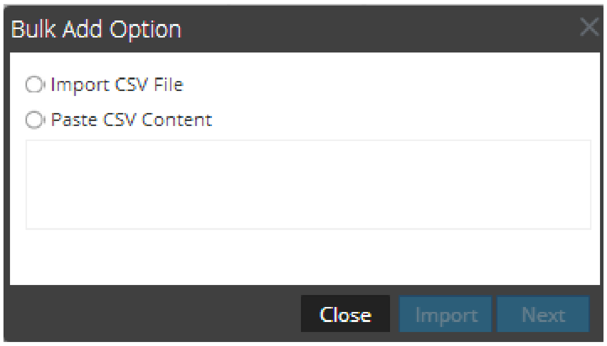
- **Import Event Sources**
- **Export Event Sources**
- **Bulk Edit Event Source Attributes**

Import Event Sources in Bulk

Warning: When using a spreadsheet program to edit an exported event source CSV file, some data fields like numbers and dates can be re-formatted into the spreadsheet program's native field types. This can cause issues when re-importing this information, as some data fields may be garbled or formatted incorrectly. This can be avoided by importing the CSV file into the spreadsheet program, and specifying all data fields as text values.

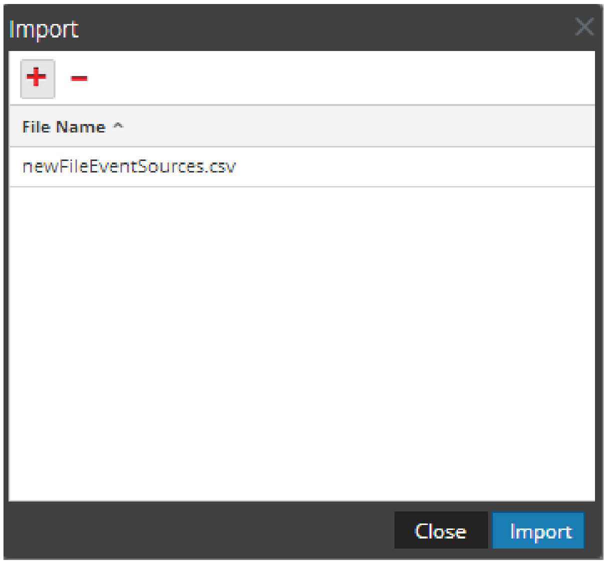
To import multiple event sources at once:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.
4. Select the **Event Sources** tab, select **AWS (CloudTrail)**, **Check Point**, **File**, **Netflow**, **ODBC**, **SDEE**, **(Syslog for Remote Collectors) only**, **VMware**, **Windows**, and **Windows Legacy** (SNMP does not have an Import function.).
5. In the **Sources** panel toolbar, click **Import Source**.
   The **Bulk Add Option** dialog is displayed.



6. Select either **Import CSV File** or **Paste CSV Content**. If you select:
   - Import CSV File:
     a. Click **Next**.
        The **Import dialog** is displayed.

b. Click **Add** and select a **.csv** file from your network.



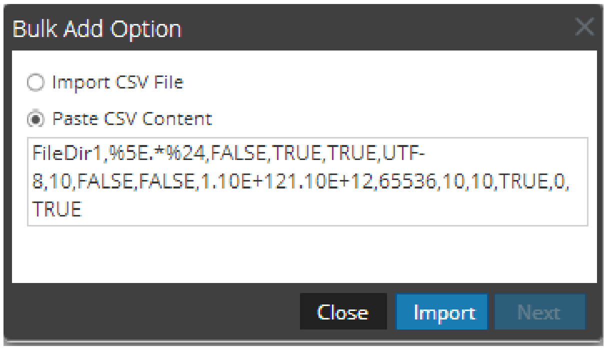
newFileEventSources.csv

c. Click **Import**.

The event sources are added to the **Event Source** list.

- Paste CSV Content:

a. Copy the contents of the **.csv** file and paste it into the dialog.



```
FileDir1,%5E.*%24,FALSE,TRUE,TRUE,UTF-
8,10,FALSE,FALSE,1.10E+121.10E+12,65536,10,10,TRUE,0,
TRUE
```

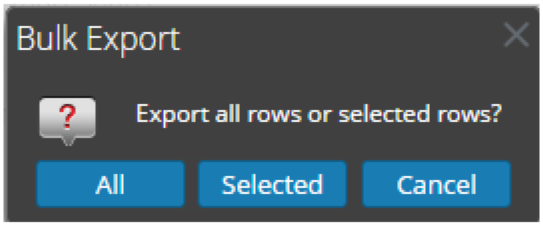
b. Click **Import**.

The event sources are added to **Event Source List**.

Export Event Sources in Bulk

Warning: When using a spreadsheet program to edit an exported event source CSV file, some data fields like numbers and dates can be re-formatted into the spreadsheet program's native field types. This can cause issues when re-importing this information, as some data fields may be garbled or formatted incorrectly. This can be avoided by importing the CSV file into the spreadsheet program, and specifying all data fields as text values.

- In the **Security Analytics** menu, select **Administration** > **Services**.
- In the **Services** grid, select a **Log Collector** service.
- Click ⌄ under **Actions** and select **View** > **Config**.
- Select **Event Sources** tab, select **AWS (CloudTrail)**, **Check Point**, **File**, **Netflow**, **ODBC**, **SDEE**, **VMware**, **Windows**, and **Windows Legacy** (SNMP does not have an Export function.).
- In the **Sources** panel, select one or multiple event sources and click **Export Source**.
  The **Bulk Export** dialog is displayed.

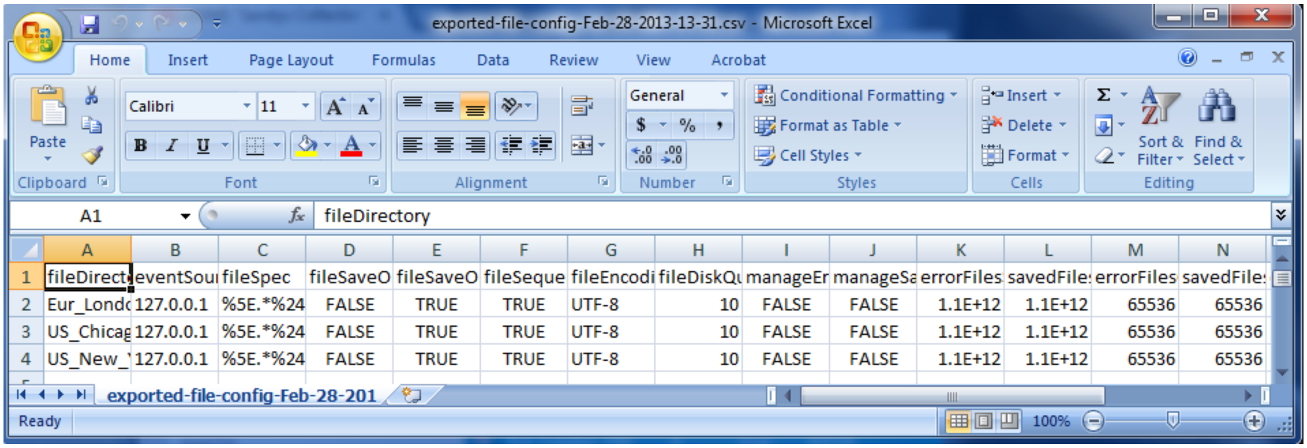


Bulk Export

Export all rows or selected rows?

- If you select:
  - **All**, Security Analytics exports all event sources to a time-stamped CSV file.
  - **Selected**, Security Analytics exports the event source or sources you selected to a time-stamped CSV file.
  - **Cancel**, Security Analytics cancels the export.

  The time-stamped CSV file (for example, **exported-file-config-Feb-28-2013-13-31.csv**) with the event sources that you selected from the list.



exported-file-config-Feb-28-2013-13-31.csv - Microsoft Excel

A1 fileDirectory

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	fileDirect	eventSou	fileSpec	fileSaveO	fileSaveO	fileSeque	fileEncodi	fileDiskQu	manageEr	manageSa	errorFiles	savedFile:	errorFiles	savedFile:
2	Eur_Londo	127.0.0.1	%5E.*%24	FALSE	TRUE	TRUE	UTF-8	10	FALSE	FALSE	1.1E+12	1.1E+12	65536	65536
3	US_Chicag	127.0.0.1	%5E.*%24	FALSE	TRUE	TRUE	UTF-8	10	FALSE	FALSE	1.1E+12	1.1E+12	65536	65536
4	US_New_`	127.0.0.1	%5E.*%24	FALSE	TRUE	TRUE	UTF-8	10	FALSE	FALSE	1.1E+12	1.1E+12	65536	65536

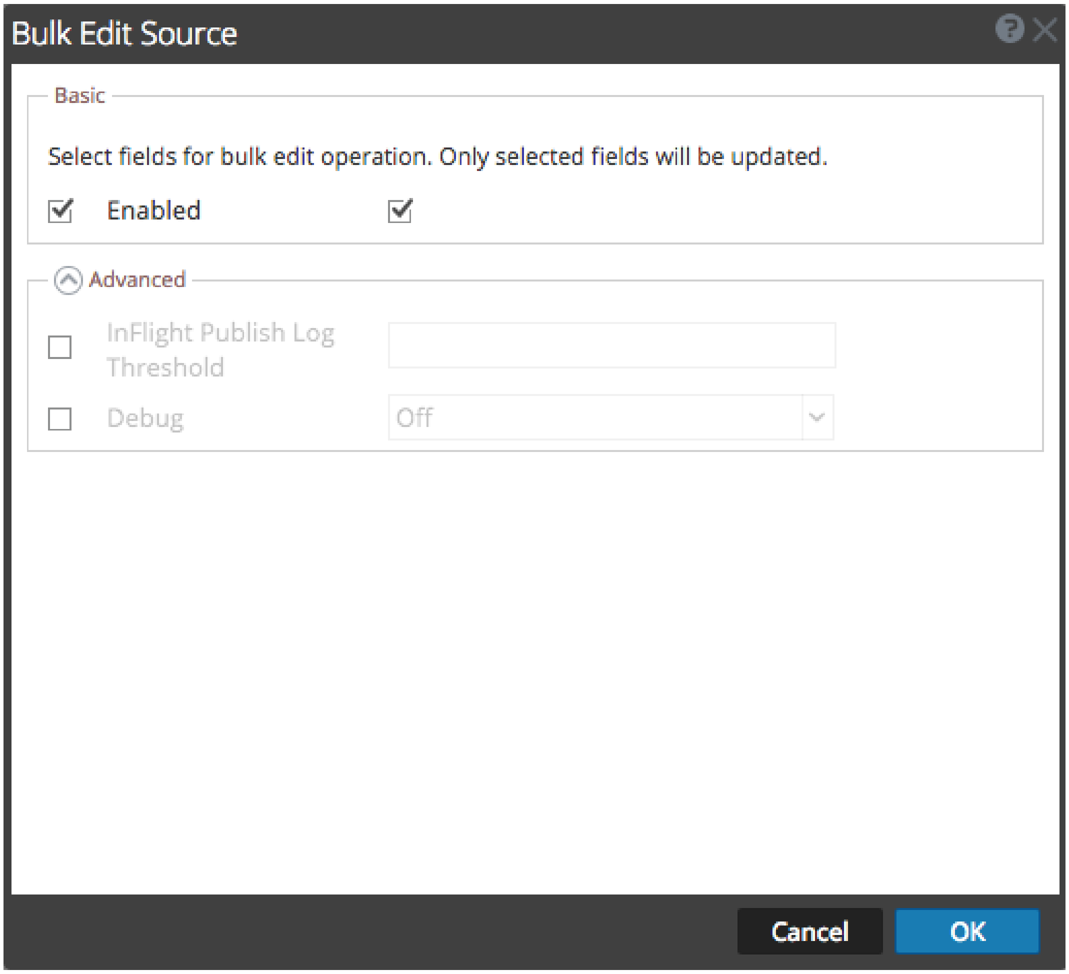
Edit Event Sources in Bulk

To edit multiple event sources at once:

1. On the **Log Collector Event Sources** tab, select **AWS (CloudTrail)**, **Check Point**, **File**, **Netflow**, **ODBC**, **SDEE**, **Syslog**, **VMware**, **Windows**, or **Windows Legacy** (SNMP does not have an Edit function.).

2. In the **Sources** panel, select multiple event sources and click (edit icon).

   The appropriate **Bulk Edit** dialog for the selected event source is displayed. The following figure is an example of **Bulk Edit Source** dialog for File event source parameters.



Bulk Edit Source

Basic

Select fields for bulk edit operation. Only selected fields will be updated.

☑ Enabled ☑

Advanced

□ InFlight Publish Log Threshold

□ Debug Off

3. Select the checkbox to the left of the fields that you want to modify (for example, **Debug**).

4. Modify the selected parameters (for example, change Debug from **Off** to **On**).

5. Click **OK**.

   Security Analytics applies the same parameter value change to all of the selected event sources

Parameters

AWS (CloudTrail)
Check Point
File Event Source
Netflow
Open Database Connectivity (ODBC)
SDCC
Syslog
VMware
Windows

Test Event Source Connections in Bulk

This topic tells you how to import, export, and edit event sources in bulk.

You can use the bulk export option to export the event source details of your current set up and store it. This data can be imported in bulk when you face a problem with your current set up and require the event source data you had.

You can use the bulk edit feature when you have multiple event sources that need a specific modification. You can select all the sources and apply the edit option across them at a time and avoid applying the change one by one.

After completing this procedure, you will have...

- Imported event sources in bulk.
- Exported event sources in bulk.
- Edited event sources in bulk.

Return to Procedures

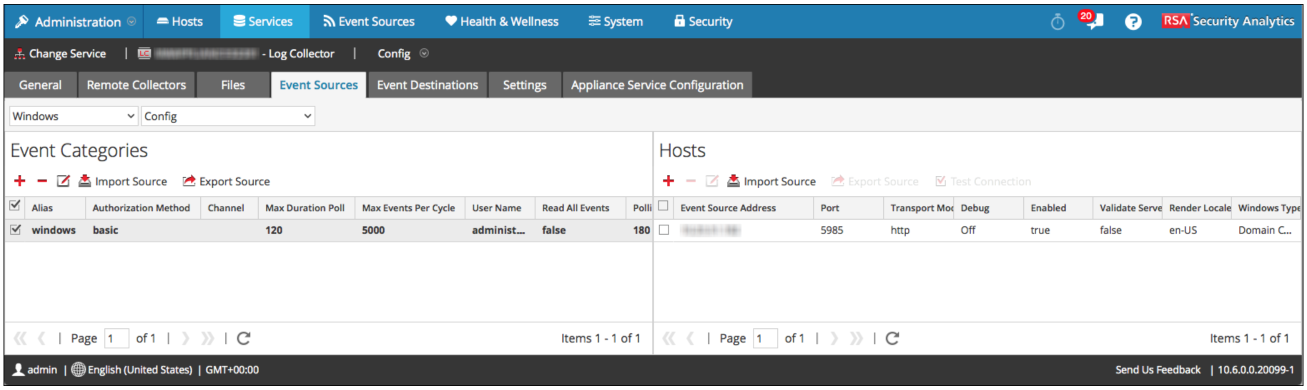
Procedure

To test multiple event source connections at once:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.
4. Select the **Event Sources** tab, select **Plugins**, **ODBC**, and **Windows** (the other protocols do not have a bulk test connection function).
5. Select one or more:

- sources from the **Sources** panel for **Plugins** or **ODBC**
- hosts from **Hosts** panel for **Windows**

  The **Test Connection** button is enabled.



☑	Alias	Authorization Method	Channel	Max Duration Poll	Max Events Per Cycle	User Name	Read All Events	Polli
☑	windows	basic		120	5000	administ...	false	180

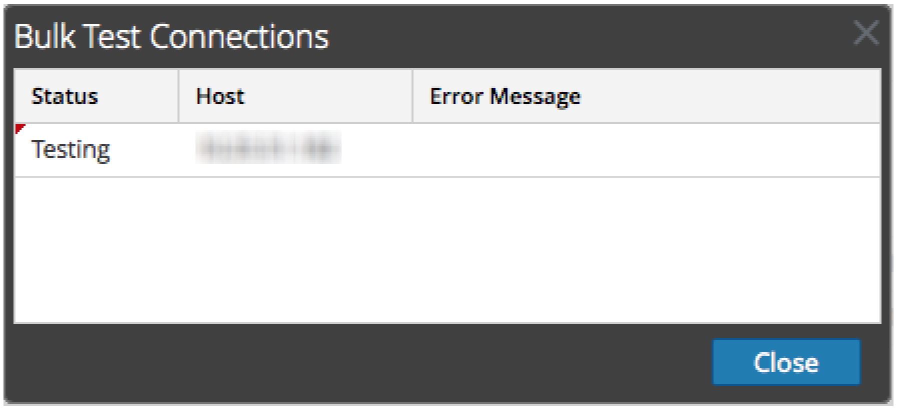
□	Event Source Address	Port	Transport Moc	Debug	Enabled	Validate Serve	Render Locale	Windows Type
□	[redacted]	5985	http	Off	true	false	en-US	Domain C...

6. Click ☑ Test Connection.

   The **Bulk Test Connections** dialog is displayed showing the current status of the test for each source. The status can be waiting, testing, passed or failed.

   If you choose to close the testing before it is completed, the testing stops and the **Bulk Test Connections** dialog closes.

   After the testing is complete, the results are displayed in the **Bulk Test Connections** dialog.



Status	Host	Error Message
Testing	[redacted]	

Parameters

AWS (CloudTrail)
Open Database Connectivity (ODBC)
Windows

Configure Syslog Event Sources for Remote Collector

This topic tells you how to configure Syslog event sources for the Log Collector.

After completing this how-to you will have:

- Configured a Syslog Event Source
- Modified a Syslog Event Source

> **Caution:** Do not configure Syslog Collection for Local Log Collectors. You only need to configure Syslog Collection for Remote Collectors.

Return to Procedures

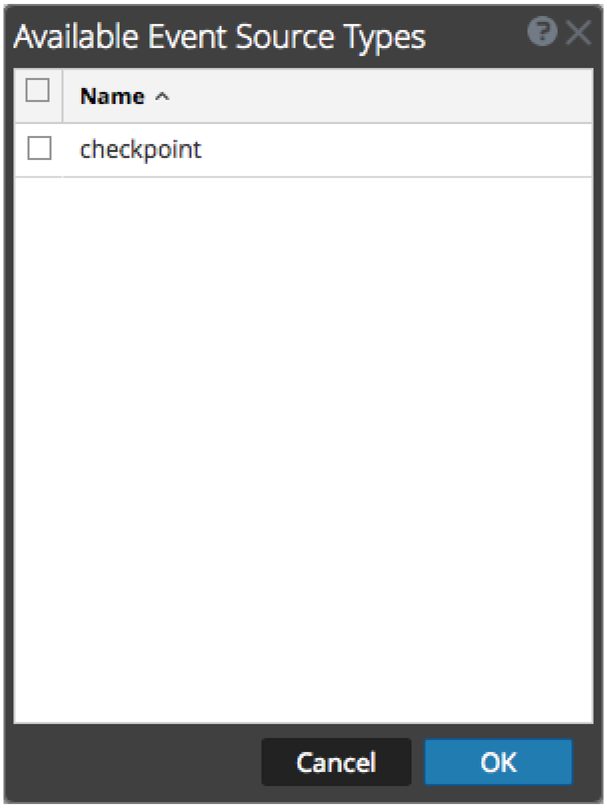
Procedures

Configure a Syslog Event Source

> **Note:** The Log Decoder collects Syslog messages directly from local site's event sources. This means that you only need to complete the following procedures if you are collecting Syslog messages from a remote site through a Remote Collector.

To configure a Syslog event source:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.
4. In the **Log Collector Event Sources** tab, select **Syslog/Config** from the drop-down menu.
   The **Event Categories** panel displays the Syslog event sources that are configured, if any.
5. In the **Event Categories** panel toolbar, click ✚.
   The **Available Event Source Types** dialog is displayed.



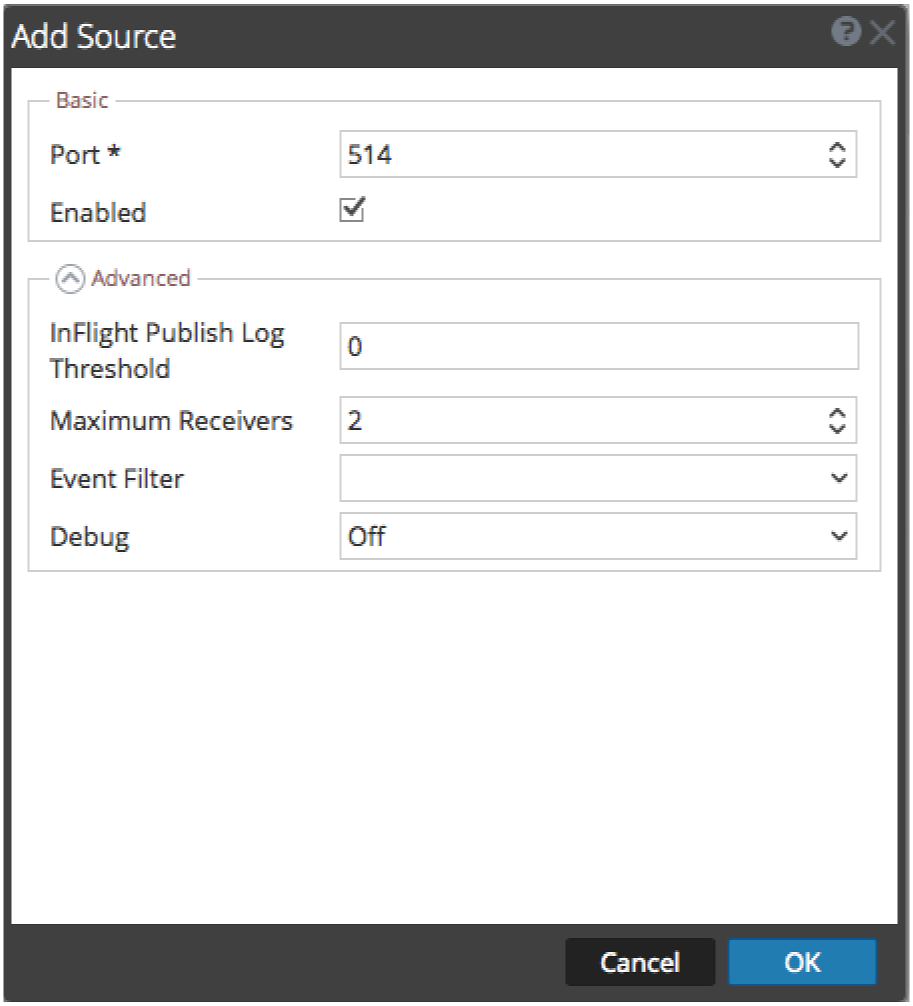
□	Name ^
□	checkpoint

6. Select an event source type (for example, **syslog-tcp**) and click **OK**.

   The newly added event source type is displayed in the **Event Categories** panel.

7. Select the new type in the **Event Categories** panel and click + in the **Sources** panel toolbar.

   The **Add Source** dialog is displayed.



Add Source

Basic

Port * 514

Enabled ☑

Advanced

InFlight Publish Log Threshold 0

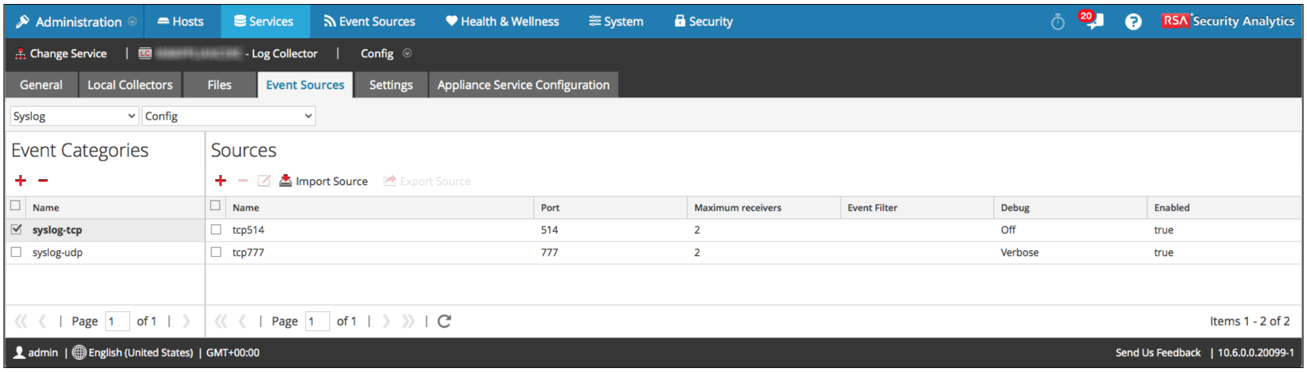
Maximum Receivers 2

Event Filter

Debug Off

8. Modify any of the parameter settings and click **OK**.

   The Syslog event source is added to the **Sources** panel.



[redacted] - Log Collector | Config

Syslog | Config

Event Categories

	Name
☑	**syslog-tcp**
□	syslog-udp

Sources

□	Name	Port	Maximum receivers	Event Filter	Debug	Enabled
□	tcp514	514	2		Off	true
□	tcp777	777	2		Verbose	true

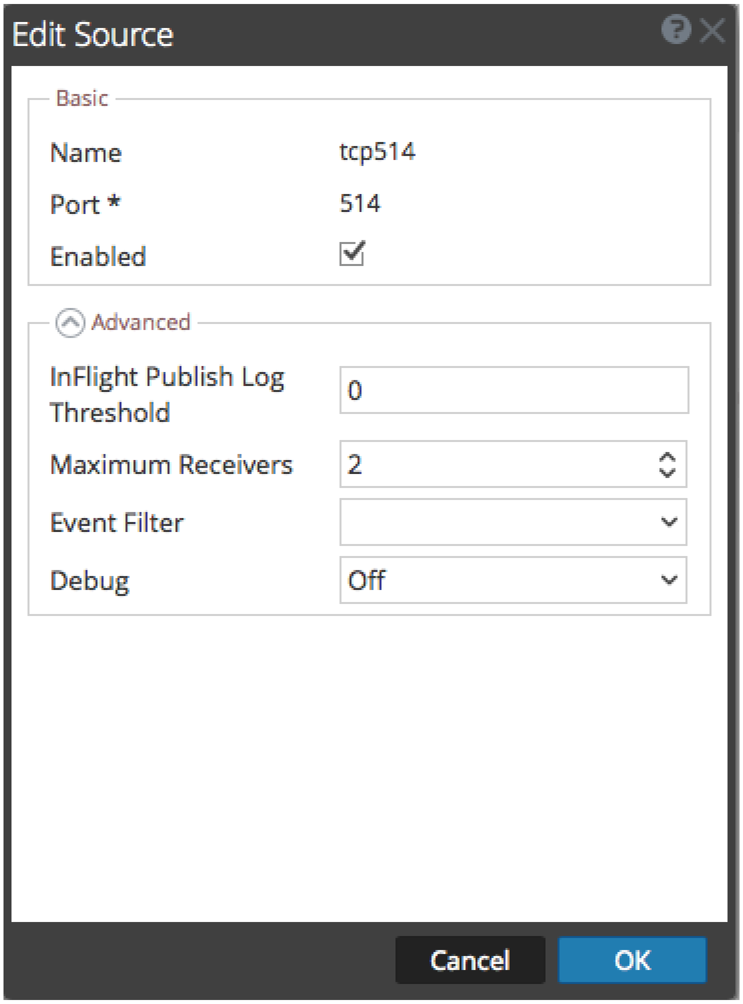
Page 1 of 1
Items 1 - 2 of 2
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.6.0.0.20099-1

Modify a Syslog Event Source

To modify an event source:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Log Collector Event Sources** tab, select **Syslog/Config** from the drop-down menu.
5. Select an event source type (for example, **syslog-tcp**) and click **OK**.
6. In the **Source** panel, select an event source (for example, **tcp514**) and click ✎.

   The **Edit Source** dialog is displayed.



Edit Source

Basic

Name	tcp514
Port *	514
Enabled	☑

Advanced

InFlight Publish Log Threshold	0
Maximum Receivers	2
Event Filter	
Debug	Off

5. Modify the parameters that require changes and click **OK**.

   Security Analytics applies the parameter changes to the selected event source

Parameters

Syslog Event Source Configuration Parameters for Remote Collector

Configure Event Filters for a Collector

This topics tells you how to create and maintain Event filters across all collection protocols.

After completing this how-to, you will have:

- Configured an Event Filter
- Modified Event Filter Rules.

> **Note:** You cannot configure Syslog Collection for Local Log Collectors. You only need to configure Syslog Collection for Remote Collectors. See Access Local Collectors and Remote Collectors for additional configuration information.

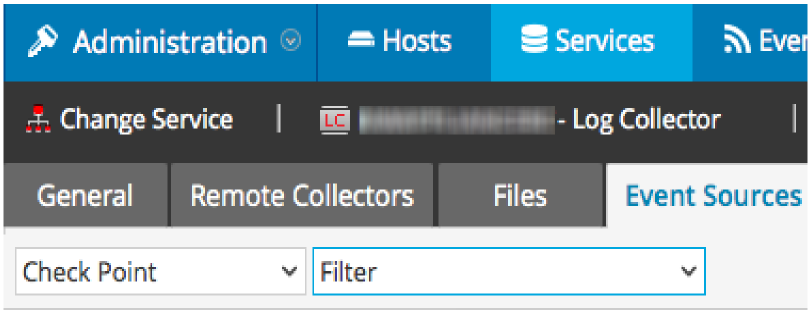
Return to Procedures

Configure an Event Filter

To configure an event source:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.
4. In the **Event Sources** tab, select any collection method / **Filters** from the drop-down menus.

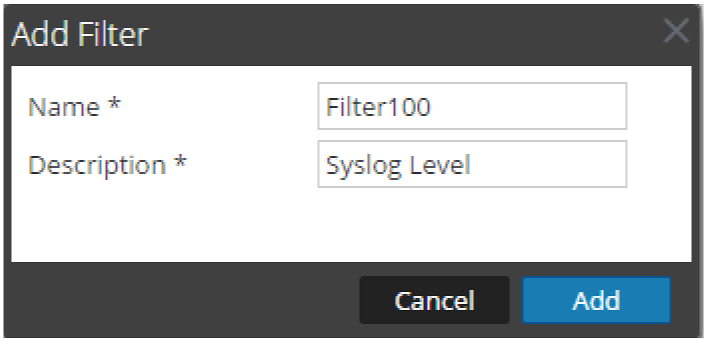
   The following screenshot shows **Check Point** selected.

   The **Filters** view displays the filters that are configured for the selected collection method, if any.

5. In the **Filters** panel toolbar, click +.

   The **Add Filter** dialog displays.

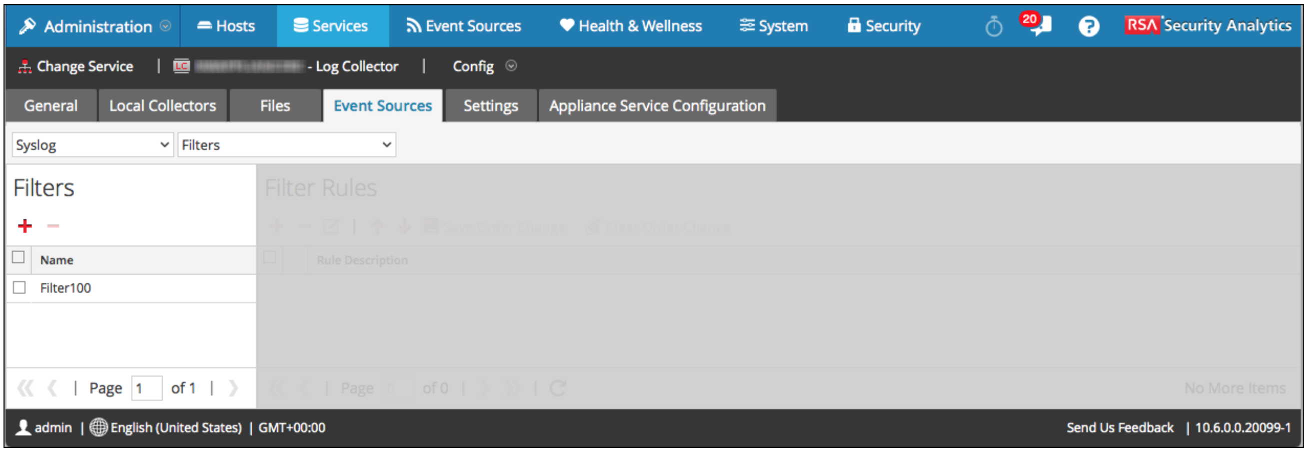


Add Filter

Name *	Filter100
Description *	Syslog Level

6. Enter a name and description for the new filter and click **Add**.

   The new filter displays in the **Filter** panel.



Syslog | Filters

Filters

□	Name
□	Filter100

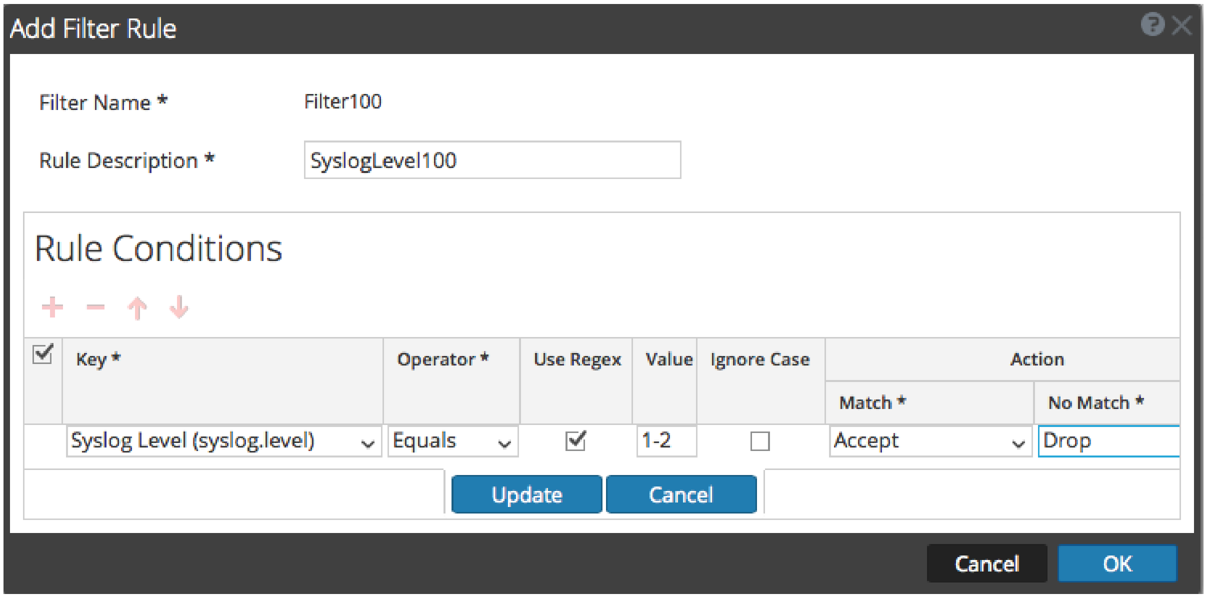
Page 1 of 1

7. Select the new filter in the **Filters** panel and click + in the **Filter Rules** panel toolbar.

   The **Add Filter Rule** dialog is displayed.

8. Click + under **Rule Conditions**.

9. Add the parameters for this rule and click **Update** > **OK**.



Add Filter Rule

Filter Name * Filter100

Rule Description * SyslogLevel100

Rule Conditions

☑	Key *	Operator *	Use Regex	Value	Ignore Case	Action	
						Match *	No Match *
	Syslog Level (syslog.level)	Equals	☑	1-2	□	Accept	Drop

Security Analytics updates the filter with the rule that you defined.

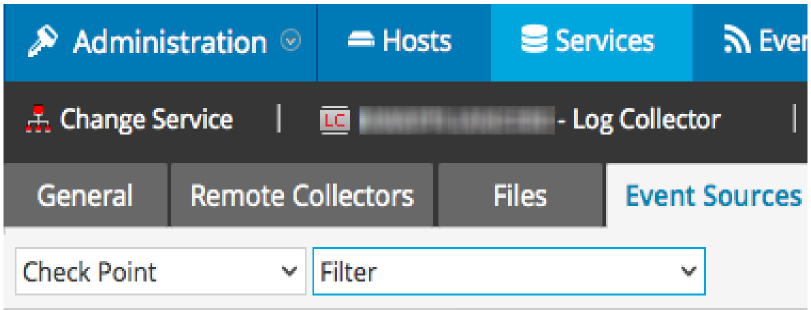
Field	Description
Key	Valid values are: • For Syslog: • Syslog level • Source IP • Raw Event • For other collection methods: Event ID (EventID)
Operator	Valid values are: • Contains • Equal
Use Regex	Optional. You can select this if you want to use regex.
Value	Value depends on the key value you selected. For example if you choose **Syslog level** for Key, the value will be a number that denotes the syslog level.
Ignore case	Optional. Select this to ignore the case sensitivity.

Field	Description
Action	If there is a match you can choose an action to accept, drop, next condition or next rule. If there is no match, you can choose an action to accept, drop, next condition or next rule.

Modify Filter Rules

To modify an event source:

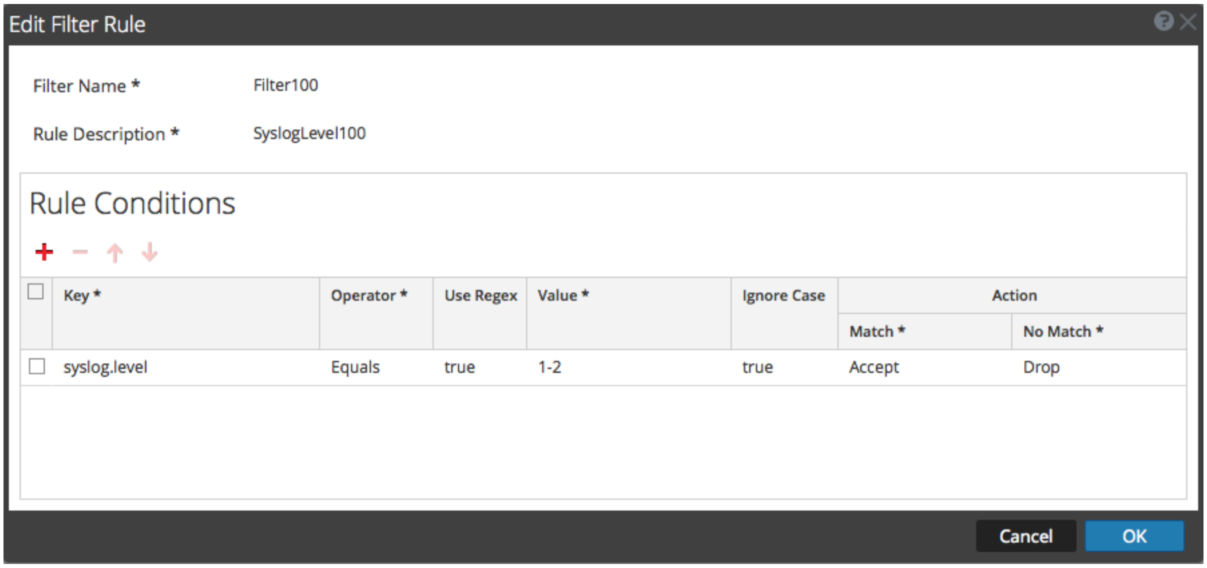
1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.
4. In the **Event Sources** tab, select any collection method / **Filters** from the drop-down menus.



The **Filters** view displays the filters that are configured for the selected collection method, if any.

5. In the **Filter Rules** list, select a rule and click ✎.

The **Edit Filter Rule** dialog is displayed.



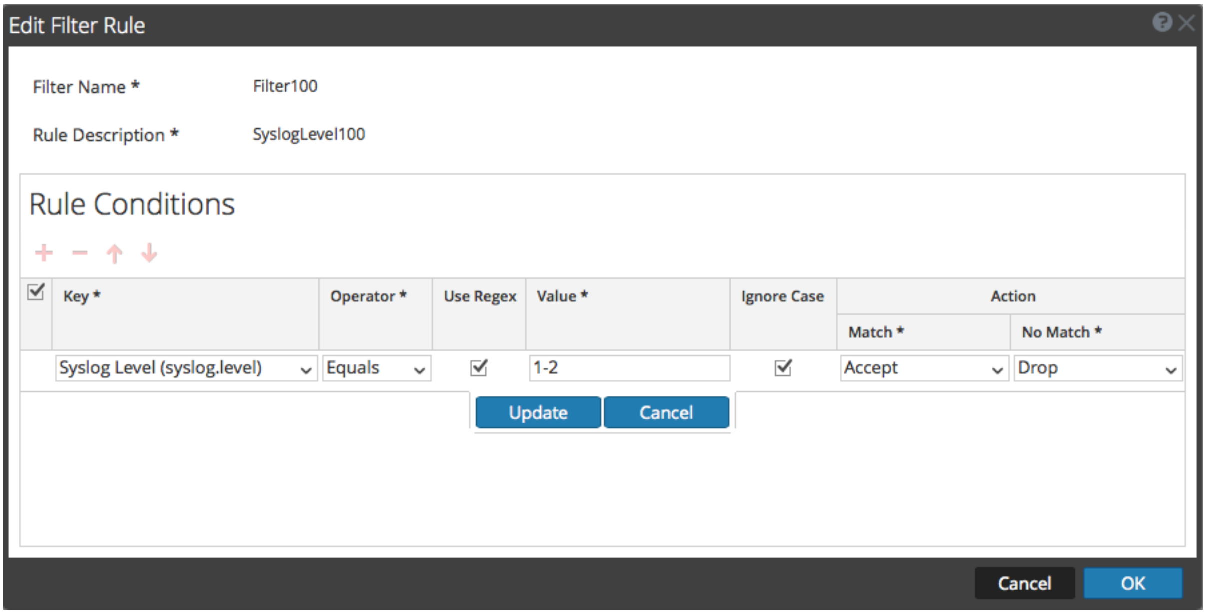
Filter Name * Filter100

Rule Description * SyslogLevel100

Rule Conditions

□	Key *	Operator *	Use Regex	Value *	Ignore Case	Action	
						Match *	No Match *
□	syslog.level	Equals	true	1-2	true	Accept	Drop

6. Select the rule condition that you want to modify.



Filter Name * Filter100

Rule Description * SyslogLevel100

Rule Conditions

☑	Key *	Operator *	Use Regex	Value *	Ignore Case	Action	
						Match *	No Match *
	Syslog Level (syslog.level)	Equals	☑	1-2	☑	Accept	Drop

7. Modify the condition parameters that require changes and click **Update** > **OK**.

Security Analytics applies the condition parameter changes to the selected filter rule.

Step 4. Configure the Event Sources to Send Events to Security Analytics

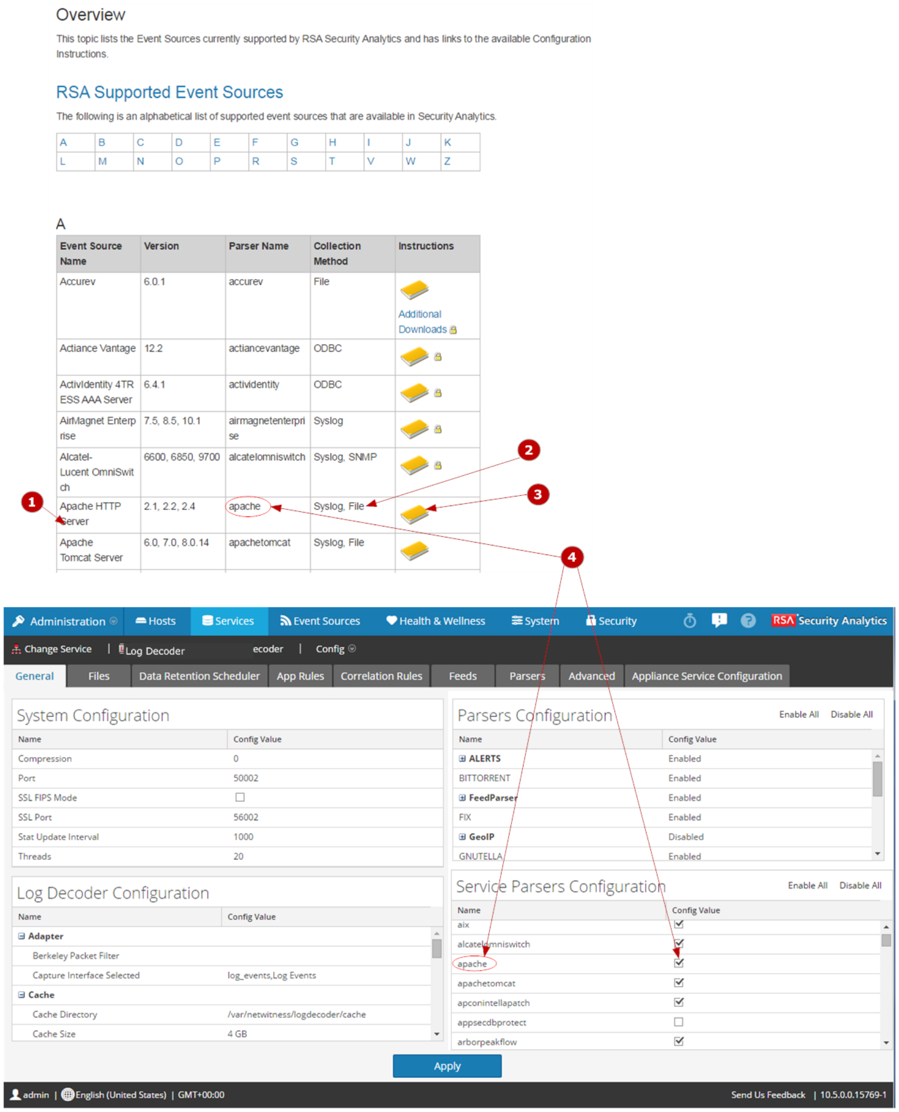
Overview

This topic contain a table that with links to the configuration instructions for every event source supported by Security Analytics.

RSA Security Analytics Supported Event Sources

Return to Procedures

The following illustration shows you the first section of the table that will be part of the Content inserted into this guide.



Overview

This topic lists the Event Sources currently supported by RSA Security Analytics and has links to the available Configuration Instructions.

RSA Supported Event Sources

The following is an alphabetical list of supported event sources that are available in Security Analytics.

A	B	C	D	E	F	G	H	I	J	K
L	M	N	O	P	R	S	T	V	W	Z

A

Event Source Name	Version	Parser Name	Collection Method	Instructions
Accurev	6.0.1	accurev	File	Additional Downloads
Actiance Vantage	12.2	actiancevantage	ODBC	
ActivIdentity 4TR ESS AAA Server	6.4.1	actividentity	ODBC	
AirMagnet Enterprise	7.5, 8.5, 10.1	airmagnetenterprise	Syslog	
Alcatel-Lucent OmniSwitch	6600, 6850, 9700	alcatelomniswitch	Syslog, SNMP	
Apache HTTP Server	2.1, 2.2, 2.4	apache	Syslog, File	
Apache Tomcat Server	6.0, 7.0, 8.0.14	apachetomcat	Syslog, File	

System Configuration

Name	Config Value
Compression	0
Port	50002
SSL FIPS Mode	□
SSL Port	56002
Stat Update Interval	1000
Threads	20

Parsers Configuration

Name	Config Value
⊞ ALERTS	Enabled
BITTORRENT	Enabled
⊞ FeedParser	Enabled
FIX	Enabled
⊞ GeoIP	Disabled
GNUTELLA	Enabled

Log Decoder Configuration

Name	Config Value
⊟ Adapter	
Berkeley Packet Filter	
Capture Interface Selected	log_events,Log Events
⊟ Cache	
Cache Directory	/var/netwitness/logdecoder/cache
Cache Size	4 GB

Service Parsers Configuration

Name	Config Value
aix	☑
alcatelomniswitch	☑
apache	☑
apachetomcat	☑
apconintellapatch	☑
appsecdbprotect	□
arborpeakflow	☑

1 Find the name of the event source (for example, **Apache HTTP Server**).

2 Verify that it is supported by the Collection Protocol (for example, the **File Collection Protocol**).

3 Click on to display the configuration instructions for the event source.

4 Verify that you downloaded the correct parser (for example, apache) from LIVE to the Log Decoder and enabled it.

Step 5. Start and Stop Services for Configured Protocols

This topic tells you how to start a collection service and enable the automatic start of a collection service.

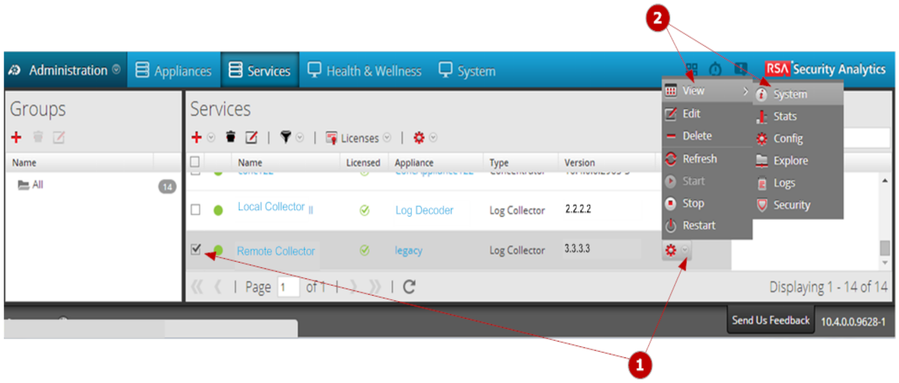
Context

If a collection service stops, you may need to start again, or you may want to enable the automatic start of a collection service.

Start a Collection Service

Return to Procedures

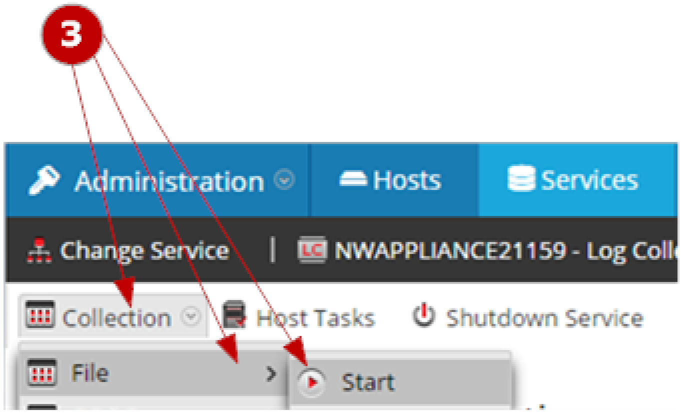
The following figure shows you how to start a collection service.



□	Name	Licensed	Appliance	Type	Version
□	Local Collector	✓	Log Decoder	Log Collector	2.2.2.2
☑	Remote Collector	✓	legacy	Log Collector	3.3.3.3

1 Select a Log Collector service and click under **Actions**.

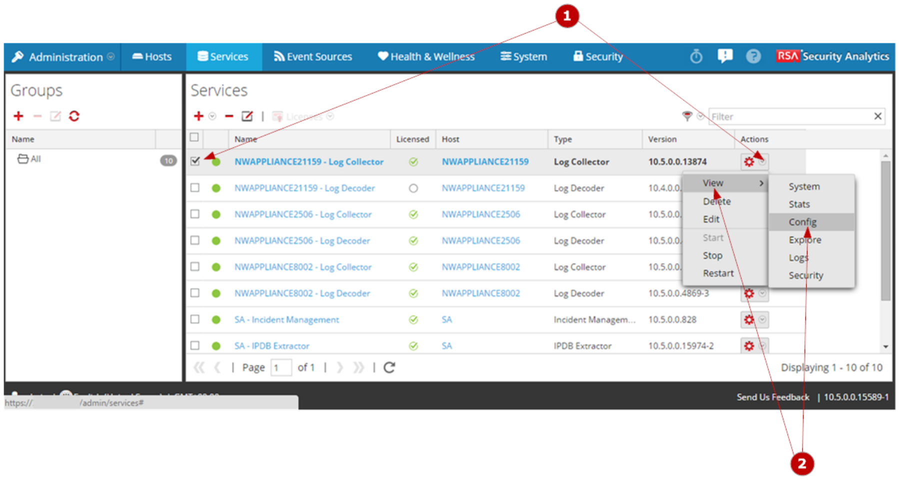
2 Click **View > System**.



Click **Collection** > ***service*** (for example, **Windows Legacy**) and click **Start**.

Enable Automatic Start of Individual Services

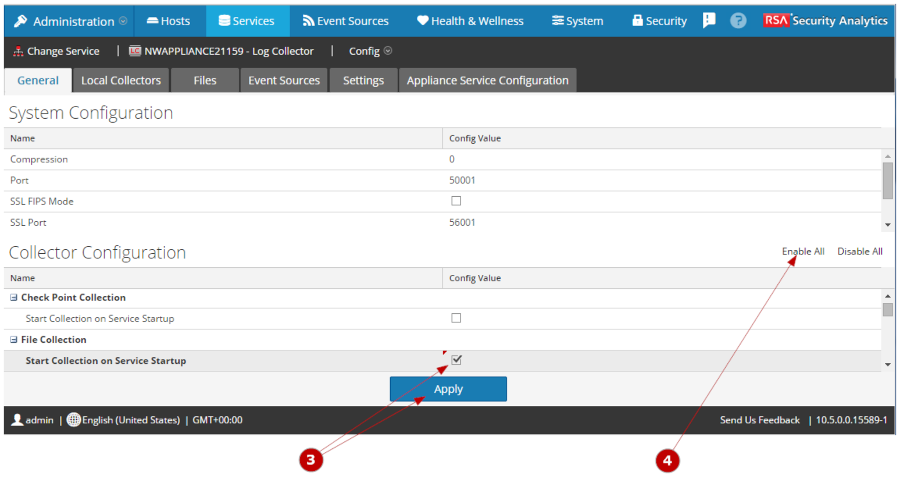
The following figure shows you how to enable the automatic start of a collection service.



☐		Name	Licensed	Host	Type	Version	Actions
☑	●	NWAPPLIANCE21159 - Log Collector	✓	NWAPPLIANCE21159	Log Collector	10.5.0.0.13874	⚙ ⌄
☐	●	NWAPPLIANCE21159 - Log Decoder	○	NWAPPLIANCE21159	Log Decoder	10.4.0.0.	
☐	●	NWAPPLIANCE2506 - Log Collector	✓	NWAPPLIANCE2506	Log Collector	10.5.0.0.	
☐	●	NWAPPLIANCE2506 - Log Decoder	✓	NWAPPLIANCE2506	Log Decoder	10.5.0.0.	
☐	●	NWAPPLIANCE8002 - Log Collector	✓	NWAPPLIANCE8002	Log Collector	10.5.0.0.	
☐	●	NWAPPLIANCE8002 - Log Decoder	✓	NWAPPLIANCE8002	Log Decoder	10.5.0.0.4869-3	⚙ ⌄
☐	●	SA - Incident Management	✓	SA	Incident Managem...	10.5.0.0.828	⚙ ⌄
☐	●	SA - IPDB Extractor	✓	SA	IPDB Extractor	10.5.0.0.15974-2	⚙ ⌄

1 Select a Log Collector service and click ⌄ under **Actions**.

2 Click **View** > **Config**.



System Configuration

Name	Config Value
Compression	0
Port	50001
SSL FIPS Mode	□
SSL Port	56001

Collector Configuration

Name	Config Value
Check Point Collection	
Start Collection on Service Startup	□
File Collection	
Start Collection on Service Startup	☑

3 Select the **Start Collection on Service Startup** checkbox for a collection service (for example, **Windows Legacy**) and click **Apply**.

4 (Optional) You can click **Enable All** and click **Apply** to select every collection service to start upon the startup of the Log Collector service.

Step 6. Verify That Log Collection Is Working

This topic tells you how to verify that you have set up Log Collection correctly.

You need to verify that Log Collection is configured correctly, otherwise it might not work

Procedure

Return to Procedures

The following methods verify that Log Collection is working.

- Verify that there is event activity the **Event Source Monitoring** tab of the **Administration > Health & Wellness** view.
- Verify that there are parsers in the **device.type** field in the **Details** column in the **Investigation > Events** view for the collection protocol you configured.

Please refer to the Configuration Guide for each Collection Protocol for steps on how to verify that protocol is set up correctly.

Reference - Configuration Parameters Interface

The **Log Collector Config Service** view is the view on which you maintain all the Log Collector parameters.

General tab = High-level parameters that govern the operation of the Log Collector service and each collection protocol.

Event Sources = Supported event sources (Check Point, File, ODBC, Netflow, Plugins, SDEE, SNMP, Syslog, VMware, Windows, and Windows Legacy)

Settings tab = Lockbox security setup, and certificate management.

Please refer to the **Files** tab and the **Appliance Service Configuration** tab in the *Host and Services Configuration Guide* for information on the configuration parameters on these tabs.

Log Collection General Tab

This topic introduces features of the service Config view > General tab that relate specifically to Log Collector.

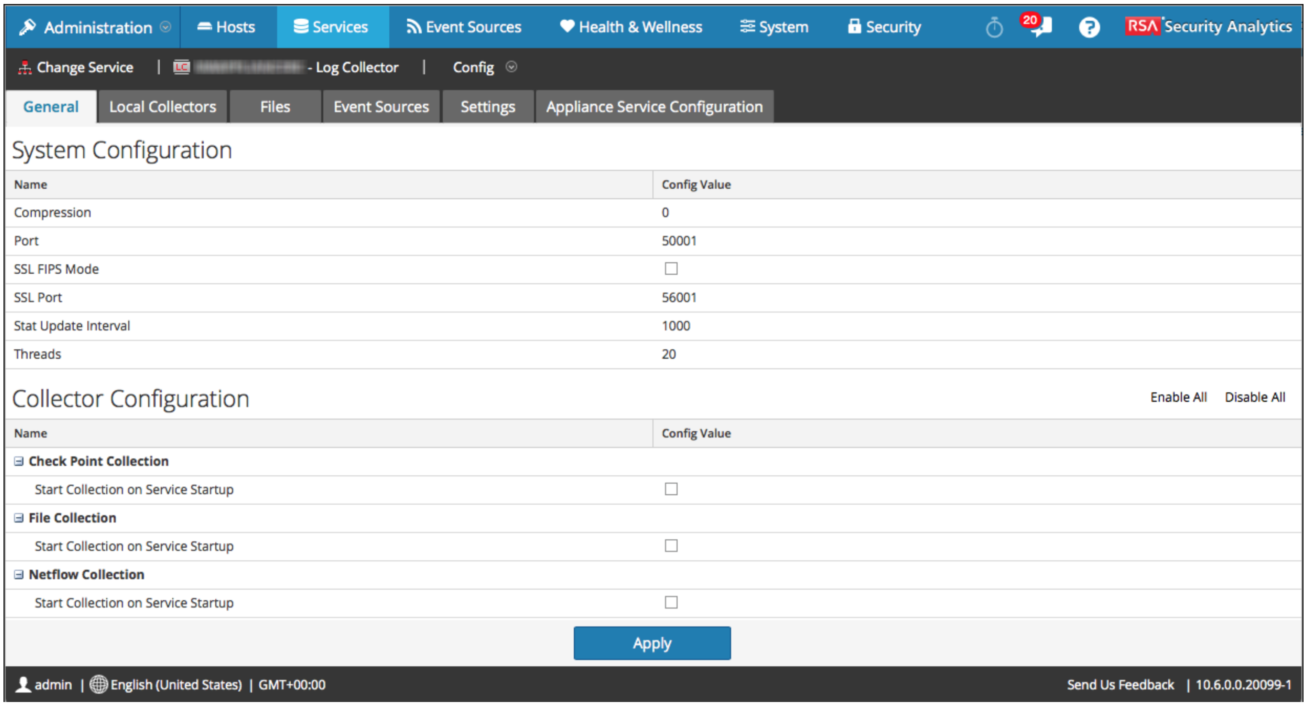
The RSA Security Analytics administrator must configure event sources to send logs to the collectors. When event sources are configured they poll event sources, retrieve logs, and send the event data to Security Analytics). In the service Config view > General tab, you can perform these actions:

- Adjust the system configuration parameters if required in the System Configuration panel.
- Configure automatic start of log collection by event source type in the Log Collector Configuration panel:
  - Check Point
  - File
  - Netflow
  - ODBC
  - Plugins (AWS CloudTrail)
  - SDEE
  - SNMP
  - VMware
  - Windows
  - Windows Legacy

To access the Log Collection General tab:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In **Services**, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.

The **Service Config** view is displayed with the Log Collector **General** tab open.



System Configuration

Name	Config Value
Compression	0
Port	50001
SSL FIPS Mode	□
SSL Port	56001
Stat Update Interval	1000
Threads	20

Collector Configuration

Name	Config Value
⊟ **Check Point Collection**	
Start Collection on Service Startup	□
⊟ **File Collection**	
Start Collection on Service Startup	□
⊟ **Netflow Collection**	
Start Collection on Service Startup	□

System Configuration Panel

The System Configuration panel manages service configuration for a Security Analytics service. When a service is first added, default values are in effect. You can edit these values to tune performance. Refer to the **General** tab for a description of these parameters.

The System Configuration section has these parameters.

Parameter	Description
Compression	The minimum number of bytes that must be transmitted per response before compression. A setting of 0 disables compression. The default value is **0**. A change in value is effective immediately for all subsequent connections.
Port	The port on which the service listens. The ports are: • 50001 for Log Collectors • 50002 for Log Decoders • 50003 for Brokers • 50004 for Decoders • 50005 for Concentrators • 50007 for other services

Parameter	Description
SSL FIPS Mode	When enabled (**on**), the security of data transmission is managed by encrypting information and providing authentication with SSL certificates. The default value is **off**.
SSL Port	The Security Analytics Core SSL port on which the service service listens. The ports are: • 56001 for Log Collectors • 56002 for Log Decoders • 56003 for Brokers • 56004 for Decoders • 56005 for Concentrators • 56007 for other services
Stat Update Interval	The number of milliseconds between statistic updates on the system. Lower numbers cause more frequent updates and can slow down other processes. The default value is **1000**. A change in value is effective immediately.
Threads	The number of threads in the thread pool to handle incoming requests. A setting of 0 lets the system decide. The default value is 15. A change takes effect on service restart.

Collector Configuration Panel

The Collector Configuration panel provides a way to enable automatic start of log collection by event source type: Check Point, File, ODBC, SDEE, SNMP, Syslog, VMware, and Windows.

Name	Configuration Value
Enable All Disable All	Enables or disables the automatic collection for all event types. • **Enable All** = start receiving events and collecting logs for all event types when the Log Collector service starts. • **Disable All** = (default) do not receive event data for all event types until you explicitly start collection.

Name	Configuration Value
Start Collection on Service Startup	Enables automatic start, per event source type, of log collection when the Log Collector service starts. Valid values are: • Selected = start collecting logs when the Log Collector service starts. • Not selected = (default) do not collect event data until you explicitly start collection.
Apply	Click Apply to save the changes to the parameter values.

Tasks

See the *Log Collection Getting Started Guide* for more information about enabling or disabling an automatic start of the collection or starting and stopping log collection protocols.

Log Collection Event Destinations Tab

Use the Event Destinations tab of the Log Collection service Config view to configure the destination of event data collected by the Log Collector:

- Log Decoders
- Identity Feed

Prerequisites

You must implement the following configuration to create an identity feed.

- A Log Collector service with an Identity Feed Event Processor
- A Log Collector service with Windows Collection configured and enabled

> **Note:** See the Create an Identity Feed topic in the Live Resource Management Guide for more information on how to create and investigate on an identity feed.

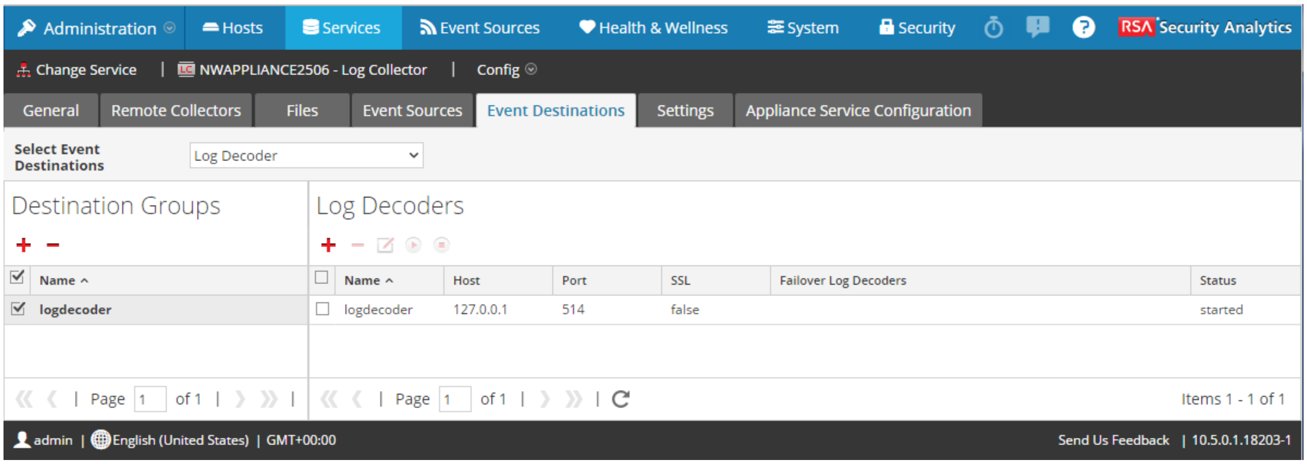
The required permission to access this view is Manage Services.

1. In the **Security Analytics** menu, select **Administration >Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.
4. Click the **Event Destinations** tab.
5. In the **Select Event Destinations** drop-down menu:

- Select **Log Decoder** to configure Log Decoder destinations for event data collected by the Log Collector.

> **Note:** You must select a Log Decoder service from the Add Log Decoder Destination dialog, but the remainder of the configuration is done automatically.

- Select **Identity Feed** to configure an identity feed destination for event data collected by the Log Collector.



Select Event Destinations: Log Decoder

Destination Groups

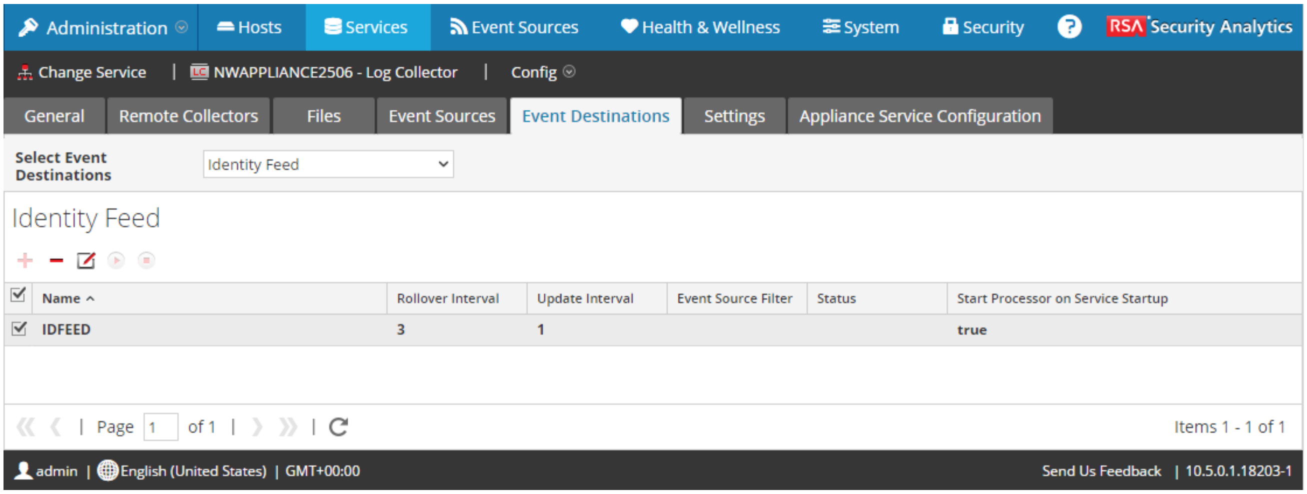
☑	Name ^
☑	logdecoder

Page 1 of 1

Log Decoders

□	Name ^	Host	Port	SSL	Failover Log Decoders	Status
□	logdecoder	127.0.0.1	514	false		started

Page 1 of 1 | Items 1 - 1 of 1



Select Event Destinations: Identity Feed

Identity Feed

☑	Name ^	Rollover Interval	Update Interval	Event Source Filter	Status	Start Processor on Service Startup
☑	IDFEED	3	1			true

Page 1 of 1 | Items 1 - 1 of 1

Log Collection Parameters

The Log Collection Config View is the view on which you maintain all the Log Collection parameters.

Log Collection Event Sources Tab

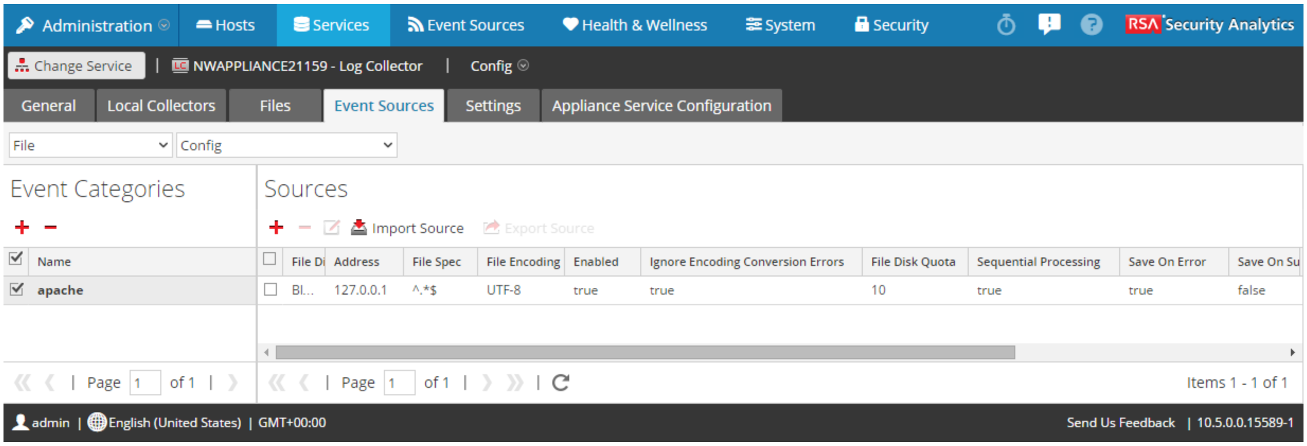
This topic introduces the service configuration parameters available on the Event Sources tab of the Log Collection service Config view.

Use the Event Sources tab of the Log Collector service Config view to configure the AWS (CloudTrail), Check Point, File, ODBC, SDEE, SNMP, Syslog, SNMP, VMware, Windows, and Windows Legacy event sources.

To access the Log Collection Event Sources Tab:

1. In the **Security Analytics** menu, select **Administration** >**Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ ⌄ under **Actions** and select **View** > **Config**.

   The **Service Config** view is displayed with the Log Collector **General** tab open.
4. Click **Event Sources** tab.



☑	Name
☑	apache

□	File Di	Address	File Spec	File Encoding	Enabled	Ignore Encoding Conversion Errors	File Disk Quota	Sequential Processing	Save On Error	Save On Su
□	Bl...	127.0.0.1	^.*$	UTF-8	true	true	10	true	true	false

Features

The File/Config view in the Event sources tab has two panels: Event Categories and Sources.

Event Source Types Menu

The Log Collector Event Sources tab has a two-box, drop-down menu in which you select the collection protocol and any supporting parameters for that protocol.

In the left box, you select one of the following protocols: Check Point, File, ODBC, Plugins, SDEE, SNMP, SNMP, VMware, Windows, and Windows Legacy.

In the right box, you select:

- Config to configure the generic event source parameters for the type you selected in the left drop-down. All generic Config panels have a toolbar with these options:
  - Add, Edit, and Delete
  - Import (also Import Source, Import DSN)

  - Export (also Export Source, Export DSN)
- For ODBC, SNMP, and Windows only:
  - For ODBC, DSNs to configure
  - For SNMP, SNMP v3 User Manager
  - For Windows, Kerberos Realm Configuration
- For Syslog on Remote Collectors only, Syslog, Filters

Selecting an option displays a configuration panel where you configure the collection parameters for the event source. The configuration panels are slightly different for different event sources and are described separately.

The following drop-down menu has the configuration parameters selected for Check Point.

Tasks

Step 3. Configure Event Sources in Security Analytics

Syslog Event Filters View for Remote Collector

This topic describes the parameters in the Syslog Filters view.

To access the Syslog Filters view:

1. In the **Security Analytics** menu, select **Administration >Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ ⌄ under **Actions** and select **View > Config**.
4. In the **Log Collector Event Sources** tab, select **Syslog/Filters** from the drop-down menus.
   The **Filters** view displays the **Syslog** filters that are configured, if any.

Features

The following table describes the Syslog Filters view parameters.

Field	Description
Key	Valid values are: • Syslog level • Source IP • Raw Event
Operator	Valid values are: • Contains • Equals
Use Regex	Optional. You can select this if you want to use regex.
Value	Value depends on the key value you selected. For example if you choose Syslog level for Key, the value will be a number that denotes the syslog level.
Ignore case	Optional. Select this to ignore the case sensitivity.
Action	If there is a match you can choose an action to accept, drop, next condition or next rule. If there is no match you can choose an action to accept, drop, next condition or next rule.

Tasks

Procedures

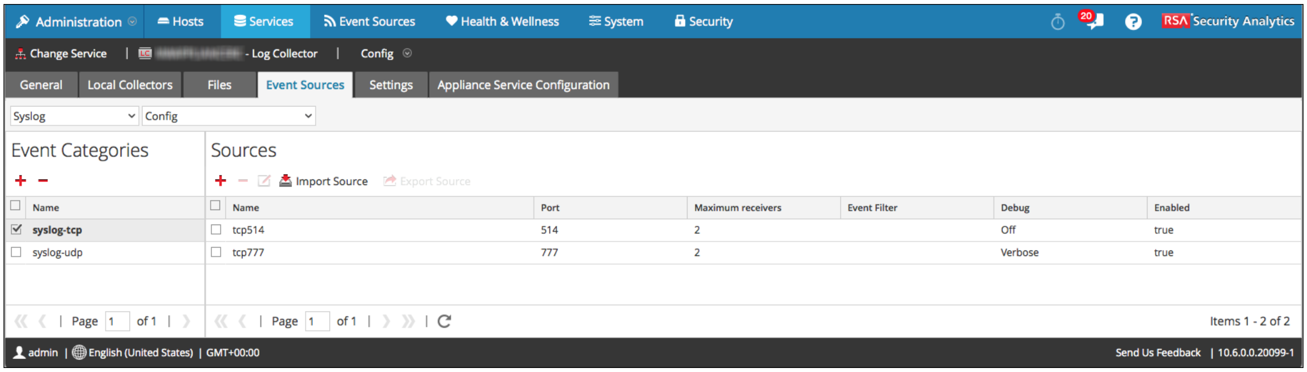
Syslog Event Source Configuration Parameters for Remote Collector

This topic describes the parameters in the Syslog Event Sources view.

Caution: Do not configure Syslog Collection for Local Log Collectors. You only need to configure Syslog Collection for Remote Collectors.

To access the Event Sources Tab for a remote log collector:

1. In the **Security Analytics** menu, select **Administration** >**Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Log Collector Event Sources** tab, select **Syslog/Config** from the drop-down menu.



Syslog | Config

Event Categories

☐	Name
☑	**syslog-tcp**
☐	syslog-udp

Page 1 of 1

Sources

☐	Name	Port	Maximum receivers	Event Filter	Debug	Enabled
☐	tcp514	514	2		Off	true
☐	tcp777	777	2		Verbose	true

Page 1 of 1

Items 1 - 2 of 2

The **Syslog/Config** view in the **Event Sources** tab has two panels: Event Categories and Sources.

Event Categories Panel

In the Event Categories panel, you can add or delete the appropriate event source types.

Feature	Description
+	Displays the Available Event Source Types dialog from which you select the event source type for which you want to define parameters.
−	Deletes the selected event source types from the Event Categories panel.
☐	Selects event source types.
Name	Displays the name of the event source types that you have added.

Available Event Sources Types Dialog

The Available Event Source Types dialog displays the list of supported event source types.

Feature	Description
☐	Selects the event source type that you want to add.

Feature	Description
Type	Display the event source types that are available to add.
Cancel	Closes the dialog without adding an event source type.
OK	Adds the selected event source type to the Event Categories panel.

Sources Panel

Use this panel to review, add, modify, and delete event sources and their parameters for the event source type you selected in the Event categories panel.

Toolbar

The following table provides descriptions of the toolbar options.

Feature	Description
+	Displays the Add Source dialog in which you define the parameters for a Firewall host.
−	Deletes the host that you selected.
✎	Opens the Edit Source dialog, in which you edit the parameters for the selected event source. Select multiple event sources and click ✎ to open the Bulk Edit Source dialog in which you can edit the parameters values for the selected event sources. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.
Import Source	Opens the Bulk Add Option dialog in which you can import hosts in bulk from a comma-separated values (CSV) file. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.
Export Source	Creates a .csv file that contains the parameters for the selected hosts. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.

Add or Modify Sources Dialog

In this dialog, you add or modify an event source for the selected event source type.

Feature	Description
Source Parameters	Lists the parameters populated with the default values. Enter or modify the appropriate values.
Cancel	Closes the dialog without adding an event source or saving the parameter values for the selected event source.
OK	In the Add Sources dialog, adds the event source and its parameters. In the Edit Source dialog, applies the parameter value changes for the selected event source.

Source Parameters

The following table provides descriptions of the source parameters.

Name	Description
	Basic
Port*	Default port is **514**.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
Advanced	
Maximum Receivers	Maximum number of receiver resources used to process collected syslog events. The default value is **2**.
Inflight Publish Log Threshold	Establishes a threshold that, when reached, Security Analytics generates a log message to help you resolve event flow issues. The Threshold is the size of the syslog event messages currently flowing from the event source to Security Analytics. Valid values are: • **0** (default) - disables the log message • **100-100000000 -** generates log message when the syslog event messages currently flowing from the event source to Security Analytics are within the 100 to 100000000 byte range.

Name	Description
Event Filter	Select a filter. Please refer to Configure an Event Filter for instructions on how to define filters.
Debug	**Caution:** Only enable debugging (set this parameter to "On" or "Verbose") if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables/disables debug logging for the event source. Valid values are: - **Off** = (default) disabled - **On** = enabled - **Verbose** = enabled in verbose mode -adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
Cancel	Closes the dialog without making adding an event source type.
OK	Adds the parameters for the event source.

Tasks

Procedures

Configure an Event Filter

Log Collection Settings Tab

This topic describes the service configuration parameters available in the Settings tab of the Log Collector service Config view.

You use the Settings tab to:

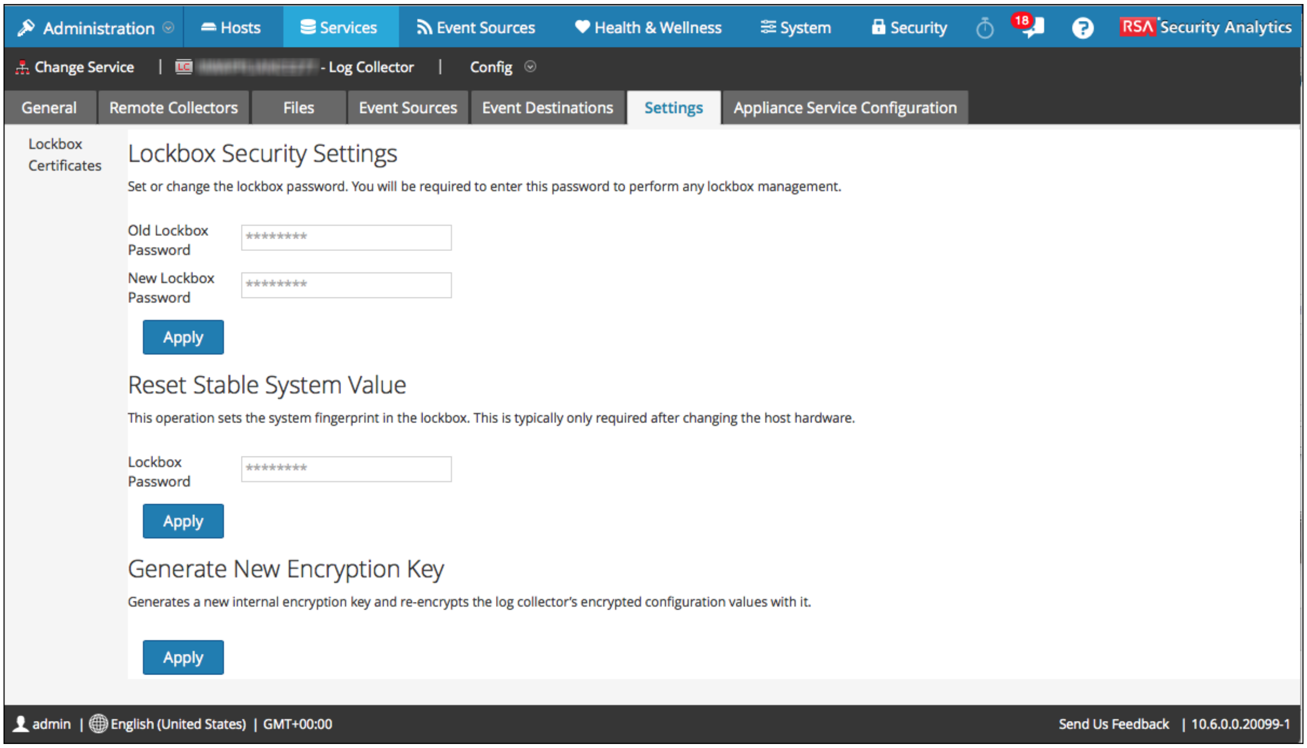
- Set up a lockbox
- Reset Stable System value

> **Caution:** If the host name on which the Log Collector is installed is changed after installation, the Log Collector will fail to collect events from event sources. You must reset stable system values if the hostname changes.

- Manage certificates.

To access the Log Collection Settings Tab:

1. In the **Security Analytics** menu, select **Administration >Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ under **Actions** and select **View > Config**.
4. In the options panel, select:
   - Lockbox to maintain Lockbox settings.
   - Certificates to add or delete certificates.



Lockbox Security Settings

Set or change the lockbox password. You will be required to enter this password to perform any lockbox management.

Old Lockbox Password: ********

New Lockbox Password: ********

Apply

Reset Stable System Value

This operation sets the system fingerprint in the lockbox. This is typically only required after changing the host hardware.

Lockbox Password: ********

Apply

Generate New Encryption Key

Generates a new internal encryption key and re-encrypts the log collector's encrypted configuration values with it.

Apply

Lockbox Configuration Parameters

This topic describes the Lockbox Security Settings.

A lockbox is an encrypted file that you use to store confidential information about an application. The Security Analytics Lockbox stores an encryption key for the Log Collector.

The encryption key encrypts all event source passwords and the event broker password, but the actual event source passwords are not stored in the Lockbox.

When you create the Lockbox, you need to:

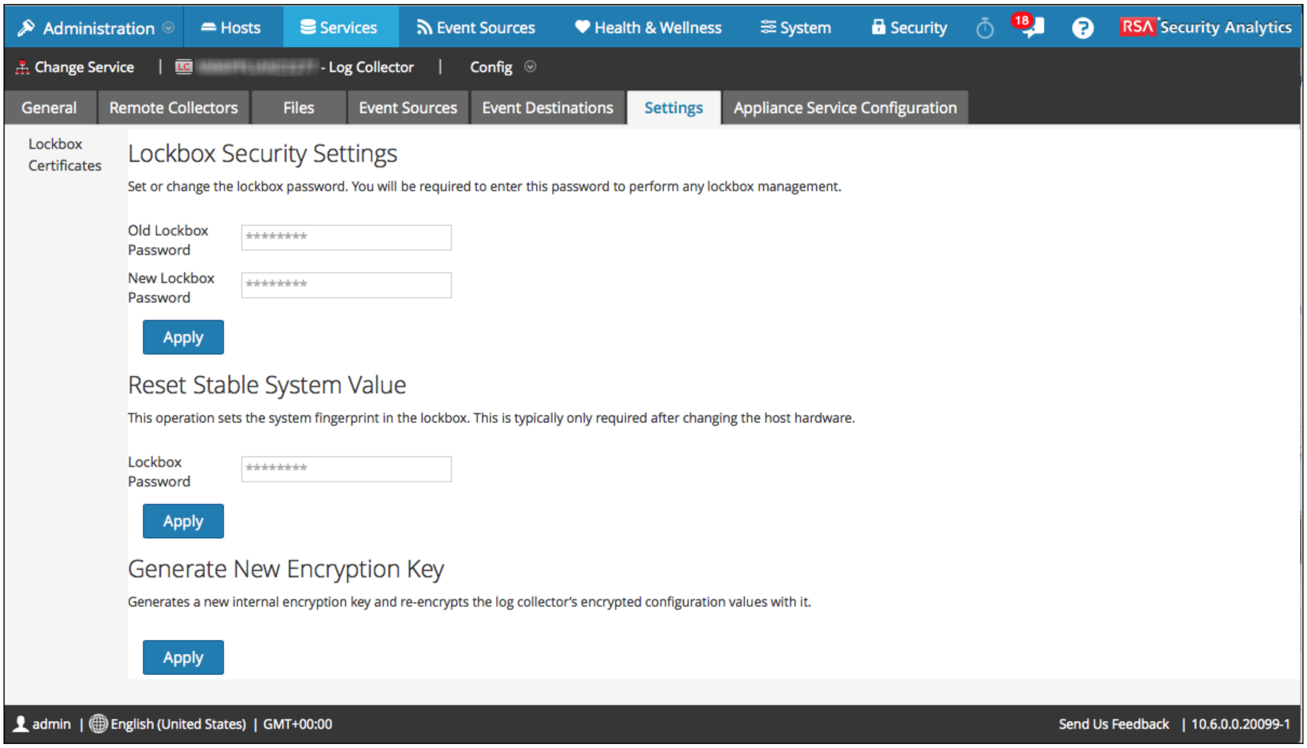
1. Define a password for the Lockbox.
2. Set a host system fingerprint based on stable system values.

The Log Collector operates the Lockbox in a mode during data collection that does not require you to specify the password (the Log Collector uses the host system fingerprint instead). You do need to use the Lockbox password to:

- Change the Lockbox password.
- Reset stable system values.
- Generate a new encryption key.

To access the Lockbox Configuration Parameters:

1. In the **Security Analytics** menu, select **Administration >Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ ⌄ under **Actions** and select **View > Config**.
4. Click the **Settings** tab.
5. In the options panel, select **Lockbox** to maintain Lockbox settings.



Lockbox Security Settings

Set or change the lockbox password. You will be required to enter this password to perform any lockbox management.

Old Lockbox Password: ********

New Lockbox Password: ********

Apply

Reset Stable System Value

This operation sets the system fingerprint in the lockbox. This is typically only required after changing the host hardware.

Lockbox Password: ********

Apply

Generate New Encryption Key

Generates a new internal encryption key and re-encrypts the log collector's encrypted configuration values with it.

Apply

admin | English (United States) | GMT+00:00
Send Us Feedback | 10.6.0.0.20099-1

Features

The Lockbox view in the Settings tab has three sections: Lockbox Security Settings, Reset Stable System Value, and Generate New Encryption Key.

Lockbox Security Settings

Before you configure event sources for the Log Collector, you need to set up a lockbox. General guidelines for lockbox setup are:

- You only need to set a lockbox password once.
- Set the password before you configure event sources.
- After you set the password, the lockbox is set up for any event source that you add.

These are the lockbox security settings.

Feature	Description
Old Lockbox Password	When you set up a Lockbox for the first time, this field is blank. Security Analytics populates this field after you enter a New Lockbox Password and click Apply.
New Lockbox Password	Initial or new lockbox password. **Note:** To maximize lockbox security, specify a password that is eight or more characters in length with at least one numeric character, uppercase character, and non-alphanumeric character such as # or !
Apply	Click Apply to save the changes to the lockbox password.

Reset Stable System Value

These are the Reset Stable System Value settings.

Feature	Description
Lockbox Password	When you set up a Lockbox for the first time, this field is blank. Specify the same Lockbox password that you entered under Lockbox Security Settings. Typically, you only need to reset this password if you change the host hardware.
Apply	Click Apply to set the system fingerprint in the lockbox.

Generate New Encryption Key

This option generates a new internal encryption key and re-encrypts the Log Collector encrypted configuration parameter values (usually passwords). Clicking Apply activates the option.

Tasks

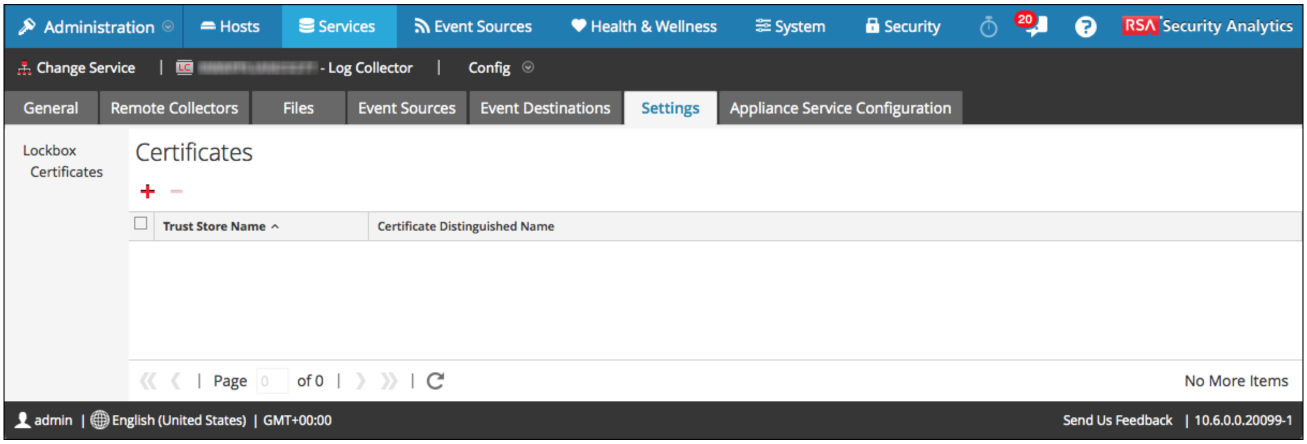
Procedures

Certificates Configuration Parameters

This topic describes the Certificates configuration parameters.

To access the Certificates configuration parameters:

1. In the **Security Analytics** menu, select **Administration >Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ under **Actions** and select **View > Config**.
4. Click the **Settings** tab.
5. In the options panel, select **Certificates** to add or delete certificates.



Features

The Certificates view in the Settings tab has one section: Certificates.

Certificates

You manage certificates by creating trust stores on the Log Collector. The Log Collector refers to these trust stores to determine whether or not the event sources are trusted.

Field	Description
+	Opens the Add Cert dialog in which you can add a certificate and password.
✎	Deletes the selected certificates.
□	Selects certificates.
Trust Store Name	Displays the name of the trust store.
Certificate Distinguished Name	For Check Point event source only, displays the distinguished name for the certificate.
Certificate Password Name	For Check Point event source only, displays the password name for the certificate.

Add Cert Dialog

These are the fields in the Add Cert dialog.

Field	Description
Trust Store Name	Enter a trust store name.
File	Click Browse to select a certificate (*.PEM file) file from your network
Password	Specify the password for this certificate.
Close	Closes the dialog without adding a certificate.
Saves	Adds the certificate.

Tasks

Procedure

Troubleshoot Log Collection Configuration

This topic highlights possible problems that you may encounter when you configure Log Collection and suggested solutions to these problems.

Troubleshoot Remote Collector Configuration Issues

The log messages in the following table are sent to:

- For Push configuration - **C:\NetWitness\ng\logcollector\rabbitmq\log\logcollector@localhost.log** on the Windows Legacy Collector server.
- For Pull configuration - **/var/log/rabbitmq/sa@localhost.log** on Log Decoder host server on which the Local Collector is running.

Log Messages	Log message with "certificate expired' as part of the message. For example:
	`Any =ERROR REPORT==== 7-Apr-2015::11:02:07 ===`
	`SSL: cipher: tls_connection.erl:375:Fatal error: certificate expired`
	`=ERROR REPORT==== 7-Apr-2015::11:02:07 ===`
	`Shovel failed to connect to Host: "10.31.204.240" Port: 5671 VirtualHost: <<"logcollection">>: error: {badmatch,{error,`
	`{tls_alert,`
	`"certificate expired"}}}`

Possible Causes	The high-level cause of a certificate expired log message is that the SA service host clock (date/time) and one or more hosts running the log collector service clocks are not synchronized. The following scenarios can cause this error. The SA service host and the Local Collector host clocks are synchronized, but the Windows Legacy Collector (WLC) clock is: • Cause 1 - Ahead (in the future) of the Local Collector host and the SA host. • Cause 2 - Behind (in the past) of the Local Collector host and the SA host. Having the WLC clock in the past works if the WLC is configured to Push events to the Local Collector. However, if the Local Collector is configured to Pull events from the WLC, the WLC reads the Local Collector certificate as invalid because it has a date ahead (in the future) of the WLC.

Solutions	For either cause, make sure that the clocks for SA host and all Remote and Local Collector hosts are synchronized. • Cause 1 - For a Legacy Windows Remote Collector, you may need to do a "rekey" if the certificate was created at a time that is "in the future" as compared to the Local Collector and Security Analytics. To do this: a. Select the **Log Collector** service for the **Legacy Windows Remote Collector** from the **Services** view. b. Click **View** > **Explore**. c. Right-click **/event-broker/ssl** and click **Properties**. The **Properties** dialog is displayed. d. Regenerate the certificate with the **rekey** command in the **Properties** dialog. e. Exchange the new certificate with Security Analytics by removing and re-adding the windows Legacy Windows logcollector service in Security Analytics. • Cause 2 -Synchronize the WLC with the LC.

Troubleshoot Collection Issues

Please refer to the troubleshooting instructions for each collection protocol for issues related to those protocols.

Exporting Event Source Issues

This topic describes how to address problems you may encounter when exporting event source information.

Issue

When using a spreadsheet program to edit an exported event source CSV file, some data fields like numbers and dates can be re-formatted into the spreadsheet program’s native field types. This can cause issues when re-importing this information, as some data fields may be garbled or formatted incorrectly.

Guidelines

To work around this problem, the best thing is to not open the file directly into the spreadsheet program, but rather import the text file (CSV) data into the spreadsheet program while it is already open. During the import of text data, your spreadsheet program will give you the option to have the spreadsheet program format the data as **text** so that mathematical formatting is not used on your CSV file's numbers.

Process

The exact steps differ depending on the spreadsheet program being used but the basic process is as follows:

1. Export your CSV file from Security Analytics.

   You will have a CSV file on your computer. Most CSV files will open up directly into your computer's installed Spreadsheet program. However, do **not** double-click the file to open it. Instead, proceed with the following steps.

2. Open up your spreadsheet program independently.
3. Create a new workbook or blank spreadsheet in the program.
4. Look for your spreadsheet program's import functions.

Import Options

The exact method of importing into your spreadsheet is dependent upon which spreadsheet you are using. Some versions of Microsoft Excel will have an **Import Wizard** located in the **Data** menu. Other versions will have the import functions located directly in the program's main screen. Please refer to your spreadsheet program's documentation for information on importing data into the spreadsheet.

When importing the data you may be given the option to select the data type. If so, select **comma separated**. Furthermore, as part of the import you should be given the option to select the formatting that will be used for the display of the imported data.

Tip

Before selecting the format type, be sure to select all of the columns in the file, then proceed:

1. Select **text** for the format that the data will be displayed in.
2. Complete your import.

Your spreadsheet file will now be formatted in text only and preserve your numerical data as it was generated by the store.

AWS (CloudTrail) Collection Configuration Guide

The Amazon Web Service (AWS) CloudTrail collection protocol collects events from Amazon Web Services (AWS) CloudTrail. CloudTrail records AWS API calls for an account. The events contain the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. The AWS API call history provided by CloudTrail events enables security analysis, resource change tracking, and compliance auditing. CloudTrail uses Amazon S3 for log file storage and delivery. Security Analytics copies the log files from the cloud (S3 bucket), and sends the events contained in the files to the Log Collector.

You must deploy Log Collection before you can configure the AWS collection protocol.

The Basics

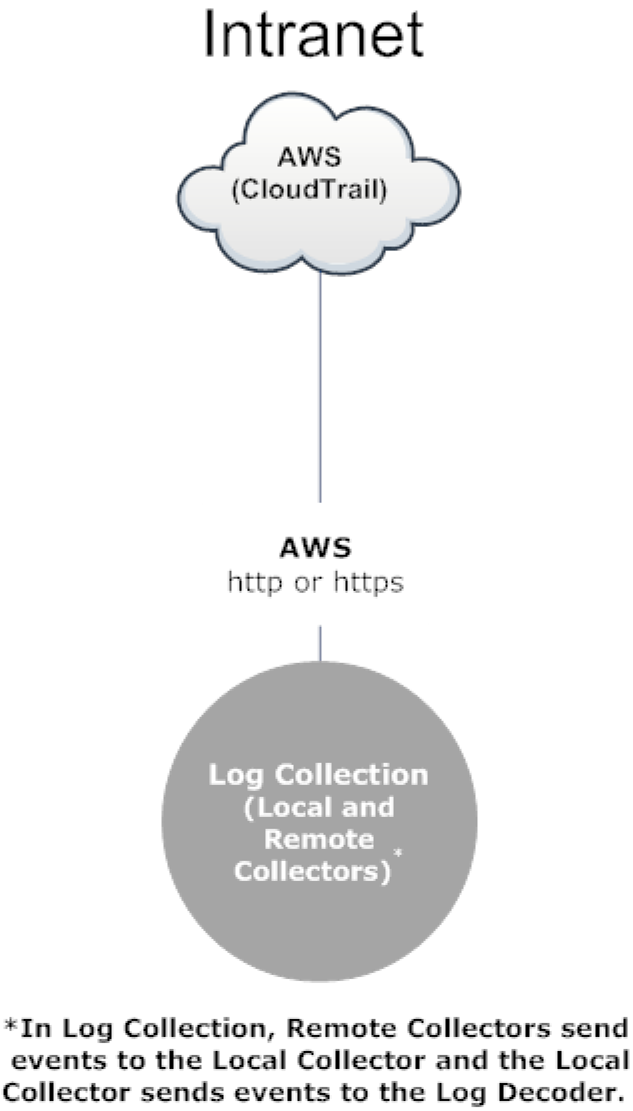
This guide tells you how to configure AWS (CloudTrail) collection protocol which collects events from Amazon Web Services (AWS) CloudTrail.

How AWS Collection Works

The Log Collector service collects events from Amazon Web Services (AWS) CloudTrail. CloudTrail records AWS API calls for an account. The events contain the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. The AWS API call history provided by CloudTrail events enables security analysis, resource change tracking, and compliance auditing. CloudTrail uses Amazon S3 for log file storage and delivery. Security Analytics copies the log files from the cloud (S3 bucket), and sends the events contained in the files to the Log Collector.

Deployment Scenario

The following figure illustrates how you deploy the AWS (CloudTrail) Collection Protocol in Security Analytics.


Intranet
AWS (CloudTrail)
AWS
http or https
Log Collection (Local and Remote Collectors)*
*In Log Collection, Remote Collectors send events to the Local Collector and the Local Collector sends events to the Log Decoder.

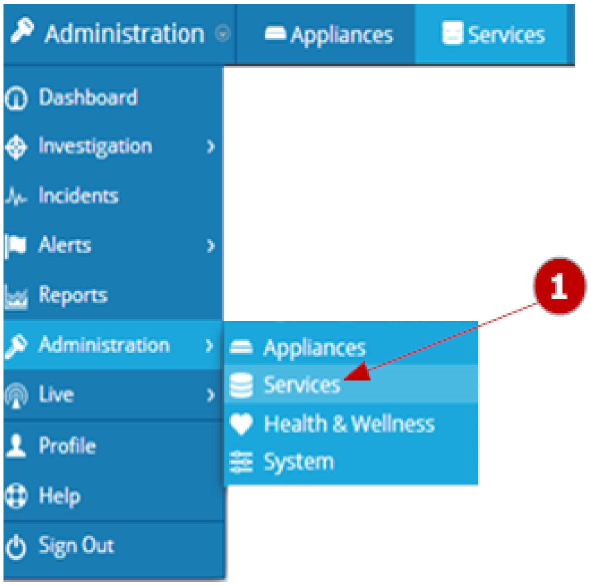
Procedures

Configure AWS (CloudTrail) Collection Protocol in Security Analytics

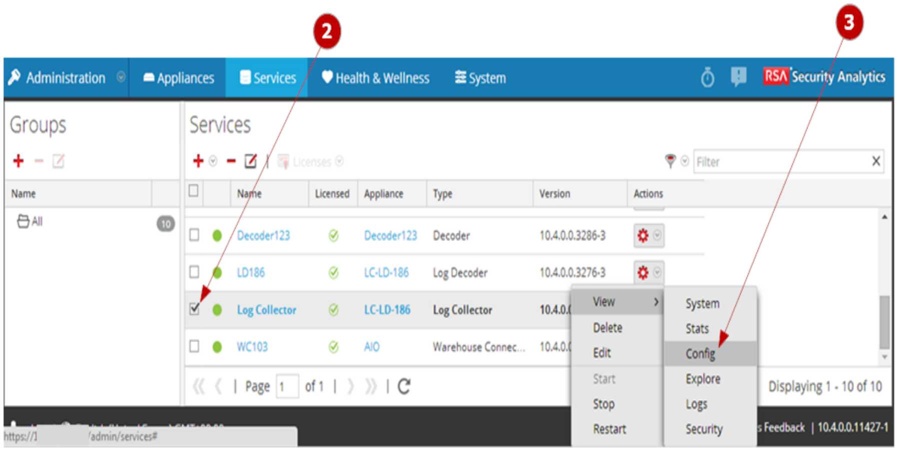
You configure the Log Collector to use AWS (CloudTrail) collection for an event source in the event Source tab of the Log Collector parameter view. The following figure the basic workflow for configuring an event source for AWS (CloudTrail) Collection in Security Analytics. Please refer to:

- Step 1. Configure AWS (CloudTrail) Event Sources in Security Analytics for step-by-step instructions on how to configure events sources in Security Analytics that use the AWS Collection protocol.

- References - AWS (CloudTrail) Collection Configuration Parameters for a detailed description of each AWS (CloudTrail) Collection Protocol parameter.



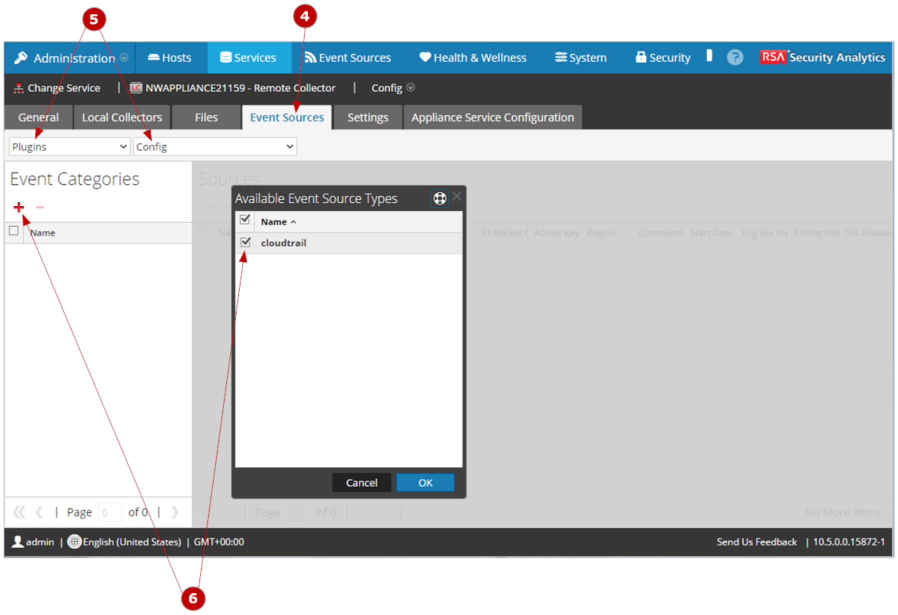
1 In the **Security Analytics** menu, select **Administration > Services**.



☐		Name	Licensed	Appliance	Type	Version	Actions
☐	●	Decoder123	✓	Decoder123	Decoder	10.4.0.0.3286-3	
☐	●	LD186	✓	LC-LD-186	Log Decoder	10.4.0.0.3276-3	
☑	●	Log Collector	✓	LC-LD-186	Log Collector	10.4.0.(	
☐	●	WC103	✓	AIO	Warehouse Connec...	10.4.0.(	

2 Select a **Log Collection** service.

3 Click under **Actions** and select **View > Config** to display the Log Collection configuration parameter tabs.

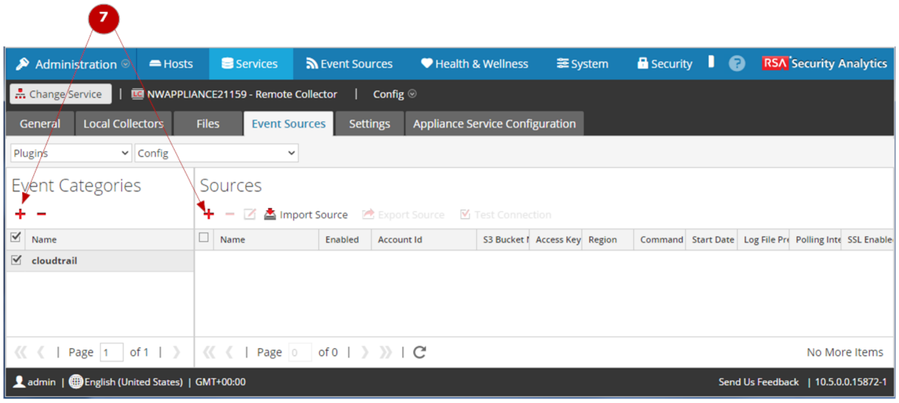


4 Click the **Event Sources** tab.

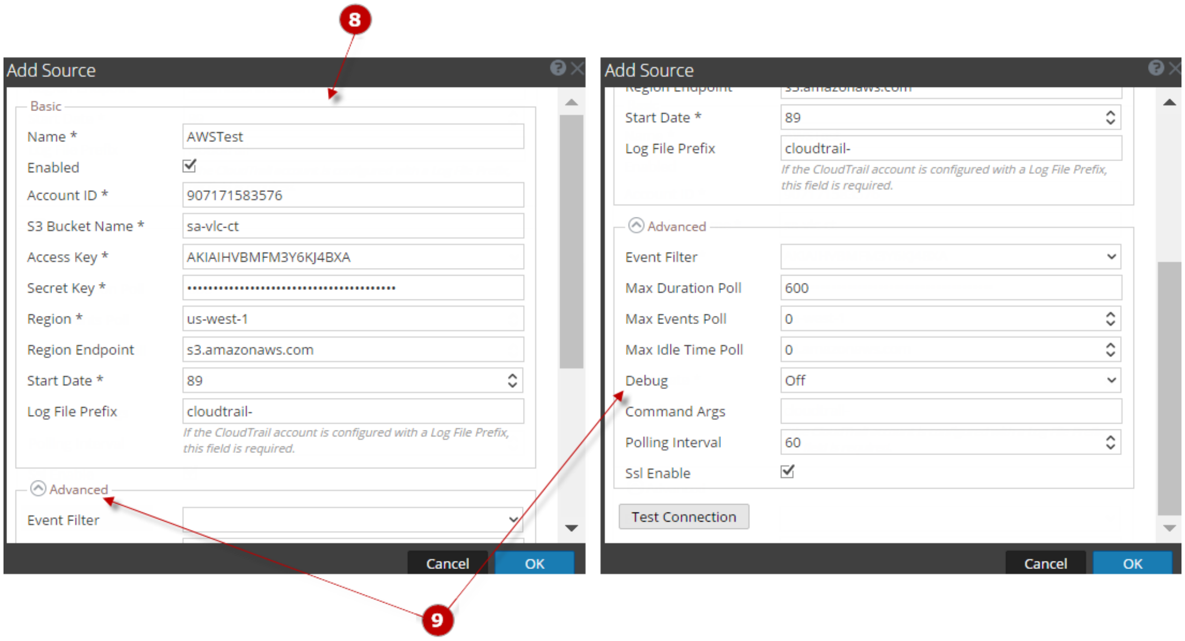
5 Select **Plugins** as the collection protocol and select **Config**.

6 Click + and select **cloudtrail** as the event source category.

The event source category is part of the content you downloaded from LIVE.



7 Select the **AWS (CloudTrail)** category and click +.



Add Source

Basic

Name *	AWSTest
Enabled	☑
Account ID *	907171583576
S3 Bucket Name *	sa-vlc-ct
Access Key *	AKIAIHVBMFM3Y6KJ4BXA
Secret Key *	••
Region *	us-west-1
Region Endpoint	s3.amazonaws.com
Start Date *	89
Log File Prefix	cloudtrail- *If the CloudTrail account is configured with a Log File Prefix, this field is required.*

Advanced

Event Filter	

Add Source

Start Date *	89
Log File Prefix	cloudtrail- *If the CloudTrail account is configured with a Log File Prefix, this field is required.*

Advanced

Event Filter	
Max Duration Poll	600
Max Events Poll	0
Max Idle Time Poll	0
Debug	Off
Command Args	
Polling Interval	60
Ssl Enable	☑

8 Specify the basic parameters required for the AWS (CloudTrail) event source.

9 Click ⌄ and specify additional parameters that enhance how the AWS (CloudTrail) protocol handles event collection for the event source.

Configure Event Sources to Use AWS (CloudTrail) Collection Protocol

You need to configure each event source that uses the AWS (CloudTrail) Collection protocol to communicate with Security Analytics (see Step 2. Configure AWS (CloudTrail) Event Sources to Send Events to Security Analytics).

Procedures

This topic provides an overview of the end-to-end sequential configuration procedure for the AWS (CloudTrail) Collection protocol with a checklist that contains each configuration step.

Configuration steps for the AWS (CloudTrail) collection protocol must occur in the specific sequence listed in the table below.

AWS (CloudTrail) Configuration Checklist

Note: The steps in this list are in the order in which you must complete them.

Step	Description
1	Configure AWS (CloudTrail) Event Sources in Security Analytics.
2	Configure AWS (CloudTrail) Event Sources to Send Events to Security Analytics.
3	Start service for configured AWS (CloudTrail) collection protocol.
4	Verify that AWS (CloudTrail) Collection is working.

Step 1. Configure AWS (CloudTrail) Event Sources in Security Analytics

This topic tells you how to configure AWS (CloudTrail) event sources for the Log Collector.

After completing this procedure, you will have...

- Configured an AWS (CloudTrail) event source.
- Modified an AWS (CloudTrail) event source.
- Pulled a Certificate for a AWS (CloudTrail) event source.

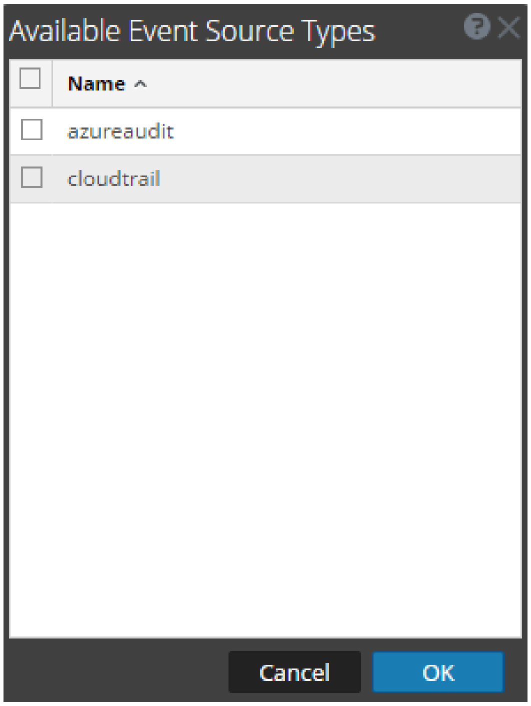
Return to Procedures

Procedures

Configure an AWS (CloudTrail) Event Source

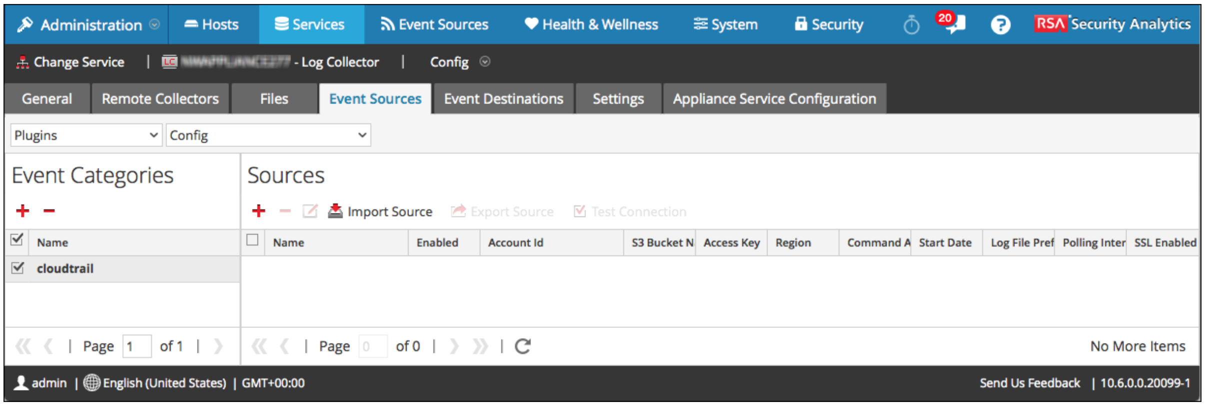
1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.
5. In the **Event Categories** panel toolbar, click ＋.
   The **Available Event Source Types** dialog is displayed.

6. Select an event source type (for example, **cloudtrail**) and click **OK**.



□	Name ^
□	azureaudit
□	cloudtrail

The newly added event source type is displayed in the **Event Categories** panel.



Event Categories

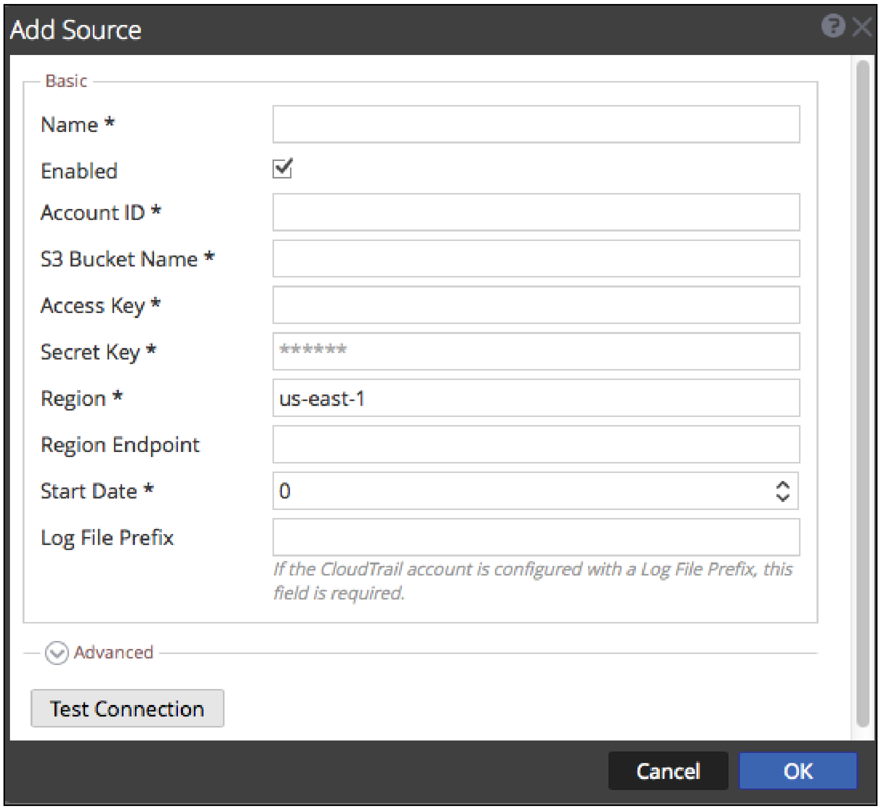
☑	Name
☑	cloudtrail

Sources

□	Name	Enabled	Account Id	S3 Bucket N	Access Key	Region	Command A	Start Date	Log File Pref	Polling Inter	SSL Enabled

7. Select the new type in the **Event Categories** panel and click + in the **Sources** toolbar.

   The **Add Source** dialog is displayed.



Add Source

Basic

Name *	
Enabled	☑
Account ID *	
S3 Bucket Name *	
Access Key *	
Secret Key *	******
Region *	us-east-1
Region Endpoint	
Start Date *	0
Log File Prefix	

If the CloudTrail account is configured with a Log File Prefix, this field is required.

Advanced

8. Define parameter values (See References - AWS (CloudTrail) Collection Configuration Parameters for definitions of each parameter).

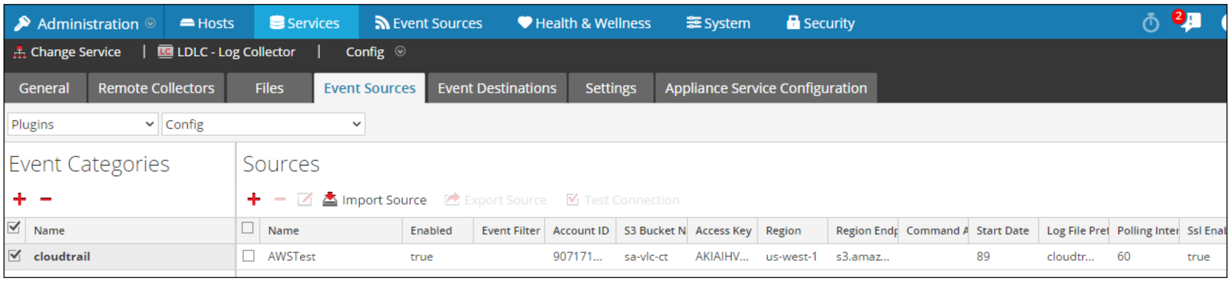
9. Click **Test Connection**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

   Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and the Security Analytics displays an error message.

10. If the test is successful, click **OK**.

    The new event source is displayed in the **Sources** panel.



Event Categories

☑	Name
☑	cloudtrail

Sources

□	Name	Enabled	Event Filter	Account ID	S3 Bucket N	Access Key	Region	Region Endp	Command A	Start Date	Log File Pre	Polling Inter	Ssl Enal
□	AWSTest	true		907171...	sa-vlc-ct	AKIAIHV...	us-west-1	s3.amaz...		89	cloudtr...	60	true

Modify an AWS (CloudTrail) Event Source

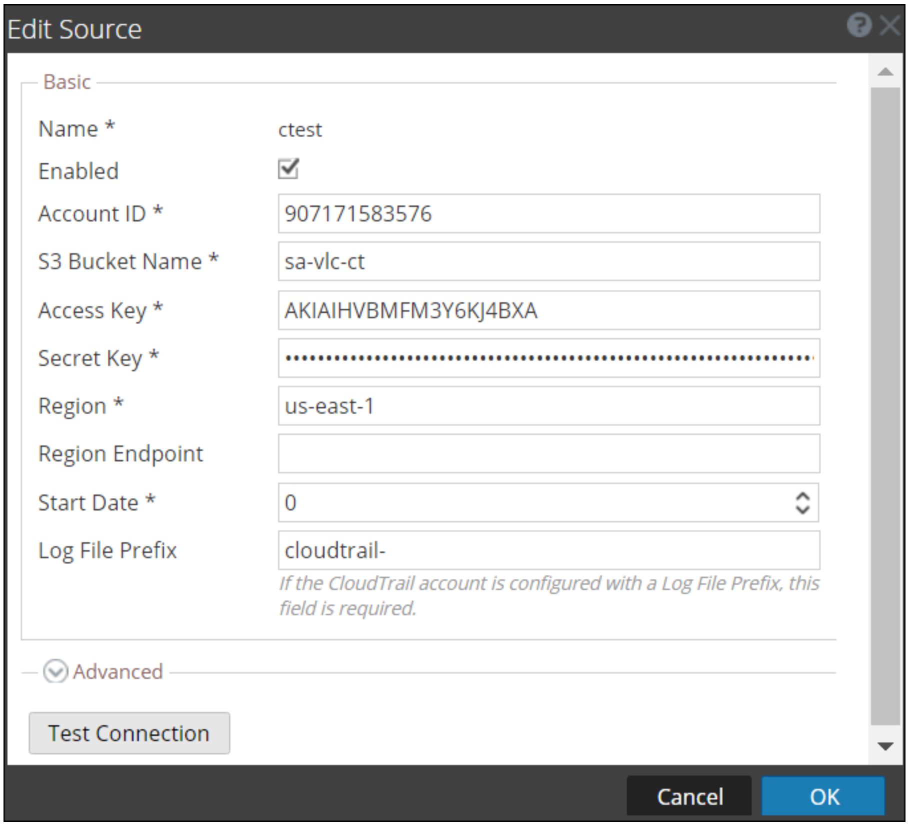
To modify an event source:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

   The **Event Categories** panel is displayed with the event sources that are configured, if any.
5. Select an event source type in the **Event Categories** panel.

   The event sources for this type are displayed in the **Sources** panel.
6. Select a source and click ✎ in the toolbar.

   The **Edit Source** dialog is displayed.
7. Modify the parameters that require changes.



Edit Source

Basic

Name *	ctest
Enabled	☑
Account ID *	907171583576
S3 Bucket Name *	sa-vlc-ct
Access Key *	AKIAIHVBMFM3Y6KJ4BXA
Secret Key *	••
Region *	us-east-1
Region Endpoint	
Start Date *	0
Log File Prefix	cloudtrail- *If the CloudTrail account is configured with a Log File Prefix, this field is required.*

8. Click **Test Connection**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device and service information and retry.

Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and the Security Analytics displays an error message.

9. If the test is successful, click **OK**.
   Security Analytics applies the parameter changes to the selected event source.

Parameters

References - AWS (CloudTrail) Collection Configuration Parameters

Step 2. Configure AWS (CloudTrail) Event Sources to Send Events to Security Analytics

This topic tells you where to find the event sources currently supported for AWS (CloudTrail) collection and the available configuration instructions for each event source

Return to Procedures

Please refer to Step 1. Configure AWS (CloudTrail) Event Sources in Security Analyticsfor instructions on how to configure a CloudTrail Event Source.

Step 3. Start Service for Configured AWS (CloudTrail) Collection Protocol

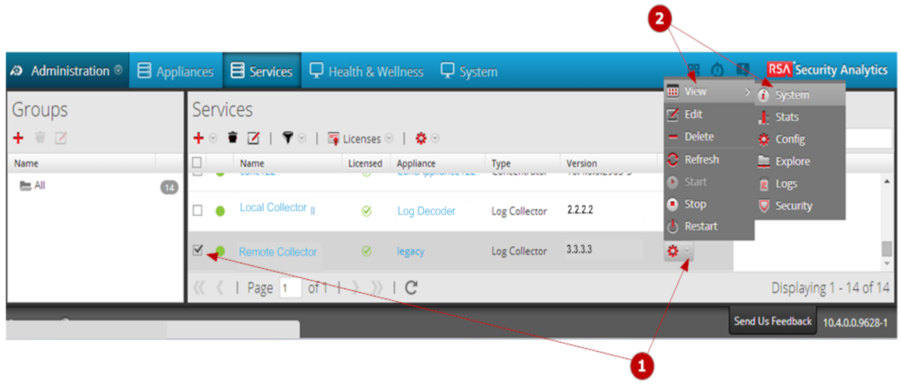
This topic tells you how to start a stopped Plugins collection service.

Return to Procedures

If the Plugins collection service stops, you will need to start it again in order to make it work. You can also refer to the Enable Automatic Start of Individual Services topic in the Log Collection Configuration Guide if you want the service to start automatically.

Procedure

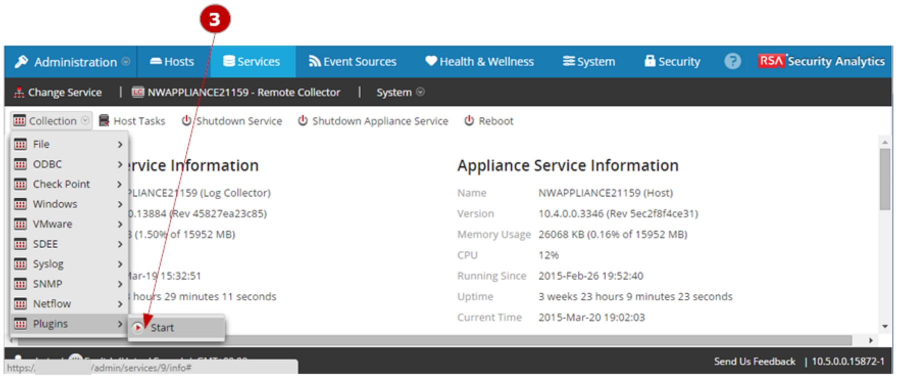
The following figure shows you how to start a collection service.



		Name	Licensed	Appliance	Type	Version
□	●	Local Collector	✓	Log Decoder	Log Collector	2.2.2.2
☑	●	Remote Collector	✓	legacy	Log Collector	3.3.3.3

1 In the **Security Analytics** menu, select **Administration** > **Services**.

2 Select a **Log Collector** service and click ⌄ under **Actions**. Click **View** > **System**.



rvice Information

PLIANCE21159 (Log Collector)
0.13884 (Rev 45827ea23c85)
3 (1.50% of 15952 MB)
lar-19 15:32:51
hours 29 minutes 11 seconds

Appliance Service Information

Name	NWAPPLIANCE21159 (Host)
Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)
Memory Usage	26068 KB (0.16% of 15952 MB)
CPU	12%
Running Since	2015-Feb-26 19:52:40
Uptime	3 weeks 23 hours 9 minutes 23 seconds
Current Time	2015-Mar-20 19:02:03

https:/[redacted]/admin/services/9/info#

3 Click **Collection** > **Plugins** and click **Start**.

Step 4. Verify That AWS (CloudTrail) Collection Is Working

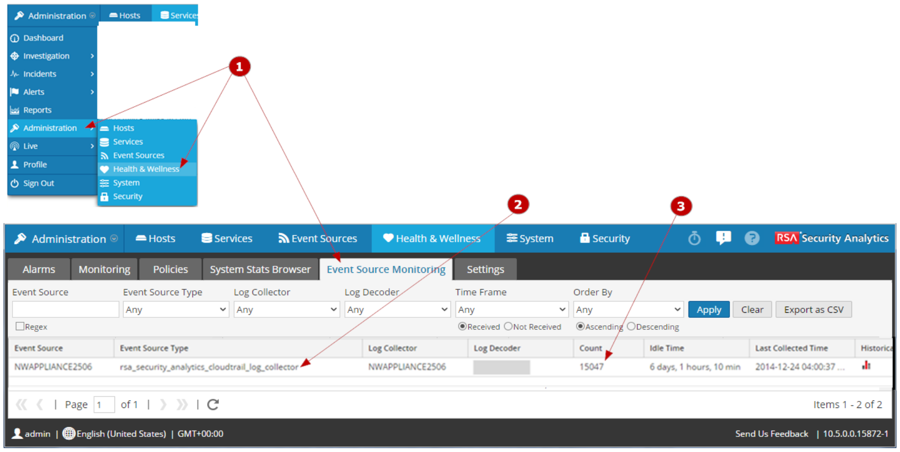
This topic tells you what to check in Security Analytics to verify that you have configured AWS (CloudTrail) Collection correctly.

Return to Procedures

If the AWS Collection is not configured correctly, it will not work. In order to ensure the collection working, you can verify it in the **Health & Wellness** view.

Procedure

The following figure illustrates how you can verify that AWS (CloudTrail) collection is working from the **Administration** > **Health & Wellness** > **Event Source Monitoring** tab.



Event Source: (blank) □Regex | Event Source Type: Any | Log Collector: Any | Log Decoder: Any | Time Frame: Any ●Received ○Not Received | Order By: Any ●Ascending ○Descending

Event Source	Event Source Type	Log Collector	Log Decoder	Count	Idle Time	Last Collected Time	Historica
NWAPPLIANCE2506	rsa_security_analytics_cloudtrail_log_collector	NWAPPLIANCE2506	[redacted]	15047	6 days, 1 hours, 10 min	2014-12-24 04:00:37 ...	

1 Access the **Event Source Monitoring** tab from the **Administration > Health & Wellness** view.

2 Find **rsa_security_analytics_aws_log_collector** in the **Event Source Type** column.

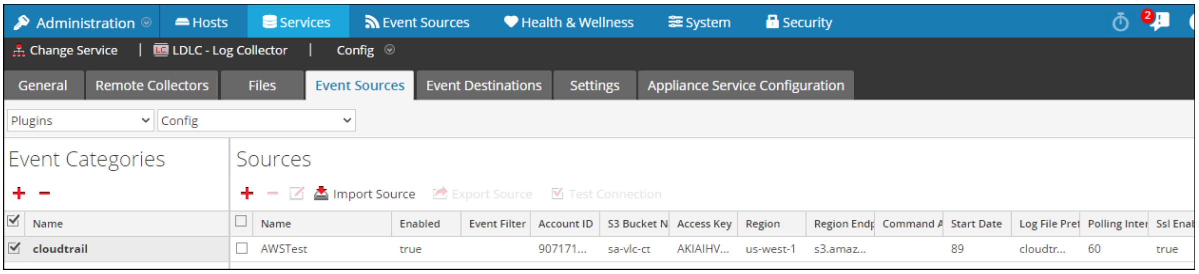
3 Look for activity in the **Count** column to verify that AWS (CloudTrail) collection is accepting events.

References - AWS (CloudTrail) Collection Configuration Parameters

This topic describes the AWS (CloudTrail) event source configuration parameters.

To access the AWS Collection Configuration Parameters:

1. In the **Security Analytics** menu, select **Administration > Services**
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.
4. In the **Log Collector Event Sources** tab, select **Plugins/Config** from the drop-down menu.



☑	Name
☑	cloudtrail

☐	Name	Enabled	Event Filter	Account ID	S3 Bucket N	Access Key	Region	Region Endp	Command A	Start Date	Log File Pre	Polling Inter	Ssl Enal
☐	AWSTest	true		907171...	sa-vlc-ct	AKIAIHV...	us-west-1	s3.amaz...		89	cloudtr...	60	true

The Plugins/Config view in the Event Sources tab has two panels: Event Categories and Sources.

Event Categories Panel

In the Event Categories panel, you can add or delete the appropriate event source types.

Feature	Description
+	Displays the Available Event Source Types dialog from which you select the event source type for which you want to define parameters.

Feature	Description
−	Deletes the selected event source types from the Event Categories panel.
□	Selects event source types.
Name	Displays the name of the event source types that you have added.

Available Event Sources Types Dialog

The Available Event Source Types dialog displays the list of supported event source types.

Feature	Description
□	Selects the event source type that you want to add.
Type	Display the event source types that are available to add.
Cancel	Closes the dialog without adding an event source type.
OK	Adds the selected event source type to the Event Categories panel.

Sources Panel

The AWS (CloudTrail) Sources panel displays a list of existing AWS (CloudTrail) firewall event sources. Use this section to add or delete event sources and associated communication parameters.

Toolbar

The following table provides descriptions of the toolbar options.

Feature	Description
+	Displays the Add Source dialog in which you define the parameters for a AWS (CloudTrail) Firewall host.
−	Deletes the host that you selected.

Feature	Description
✎	Opens the Edit Source dialog in which you edit the parameters for the selected AWS (CloudTrail) event source. Select multiple event sources and click ✎ to open the Bulk Edit Source dialog in which you can edit the parameters values for the selected event sources. Refer to the *Log Collection Configuration Guide* for detailed steps on how to import, export, and edit event sources in bulk.
Import Source	Opens the Bulk Add Option dialog in which you can import AWS (CloudTrail) hosts in bulk from a comma-separated values (CSV) file. Refer to the *Log Collection Configuration Guide* for detailed steps on how to import, export, and edit event sources in bulk.
Export Source	Creates a **.csv** file that contains the parameters for the selected AWS (CloudTrail) hosts. Refer to the *Log Collection Configuration Guide* for detailed steps on how to import, export, and edit event sources in bulk.
☑ Test Connection	Validates the configuration parameters for the selected AWS (CloudTrail) Firewall hosts. *Refer to the Log Collection Configuration Guide* for detailed steps on how to test event source connections in bulk.

Add or Edit Source Dialog

The Add Source dialog and the Edit Source dialog contain the same information.

Validates the connection to Event Source Address.

Parameter	Description
Parameter	**Description**
Basic	
Name *	Name of the event source.

Parameter	Description
Enabled □	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
Account Id *	Account Identification code of the S3 Bucket
S3 Bucket Name *	Name of the AWS (CloudTrail) S3 bucket. Amazon S3 bucket names are globally unique, regardless of the AWS (CloudTrail) region in which you create the bucket. You specify the name at the time you create the bucket. Bucket names should comply with DNS naming conventions. The rules for DNS-compliant bucket names are: • Bucket names must be at least three and no more than 63 characters long. • Bucket names must be a series of one or more labels. Adjacent labels are separated by a single period “.”. Bucket names can contain lowercase letters, numbers, and hyphens. Each label must start and end with a lowercase letter or a number. • Bucket names must not be formatted as an IP address (for example, 192.168.5.4). The following examples are **valid** bucket names: • **myawsbucket** • **my.aws.bucket** • **myawsbucket.1** The following examples are **invalid** bucket names: • **.myawsbucket** - Do not start a Bucket Name with a period ".". • **myawsbucket.** - Do not end a Bucket Name with a period ".". • **my..examplebucket** - Only use one period between labels.
Access Key *	Key used to access the S3 bucket. Access Keys are used to make seure REST or Query protocol requests to any AWS service API. Please refer to Manage User Credentials on the Amazon Web Services support site for more information on Access Keys.

Parameter	Description
Secret Key *	Secret key used to access the S3 bucket.
Region *	Region of the S3 bucket. **us-east-1** is the default value.
Region Endpoint	Specifies the AWS cloudtrail hostname. For example, for an AWS public cloud for us-east region, the Region Endpoint would be s3.amazonaws.com. More information can be found at http://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region. This parameter is necessary to collect CloudTrail logs from AWS Government or Private clouds.
Start Date *	Starts AWS (CloudTrail) collection from the specified number of days in the past, measured from the current timestamp. The default value is 0, which starts from today. The range is 0–89 days.
Log File Prefix	Prefix of the files to be processed. **Note:** If you set a prefix when you set up your CloudTrail service, make sure to enter the same prefix in this parameter.
Advanced	

Parameter	Description
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables/disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
Command Args	Arguments added to the script.
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is 60. For example, if you specify 60, the collector schedules a polling of the event source every 60 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 60 seconds for the polling to start because the threads are busy.
SSL Enabled ☐	Select the check box to communicate using SSL. The security of data transmission is managed by encrypting information and providing authentication with SSL certificates. The check box is selected by default.

Parameter	Description
Test Connection	Validates the configuration parameters specified in this dialog are correct. For example, this test validates that: • Security Analytics can connect with the S3 Bucket in AWS using the credentials specified in this dialog. • Security Analytics can download a log file from the bucket (test connection would fail if there were no log files for the entire bucket, but this would be extremely unlikely).
Cancel	Closes the dialog without adding the AWS (CloudTrail).
OK	Adds the current parameter values as a new AWS (CloudTrail).

Tasks

Step 1. Configure AWS (CloudTrail) Event Sources in Security Analytics

Troubleshoot AWS (CloudTrail) Collection

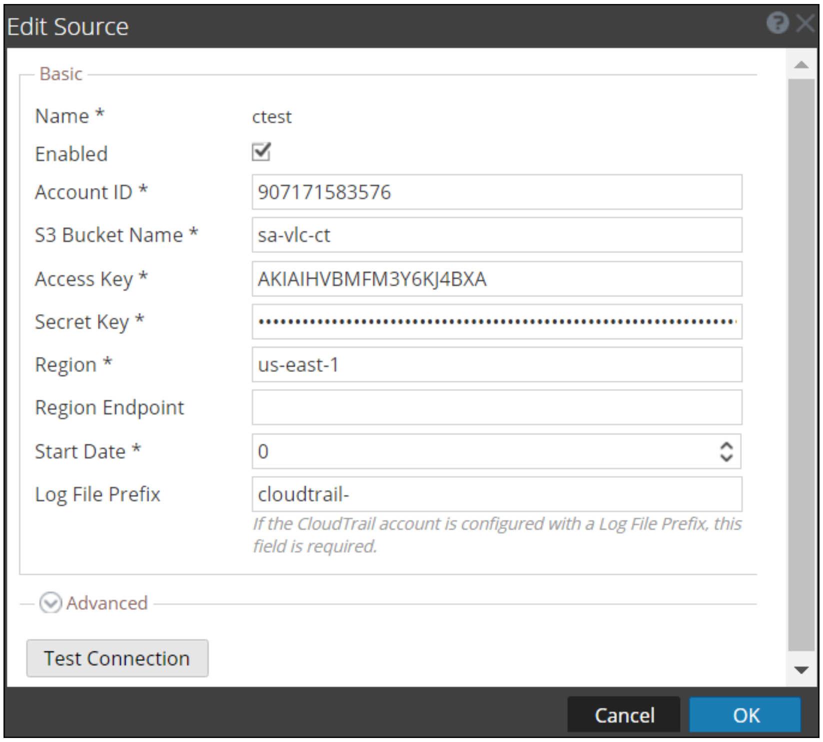
This topic highlights possible problems that you may encounter with AWS (CloudTrail) Collection and suggested solutions to these problems.

Note: In general, you receive more robust log messages by disabling SSL.

Log Message/ Problem	No bucket key found under 'arn:aws:s3:::bucket-name/AWSLogs/account-id/CloudTrail/region/'. Determine if the 'S3 Bucket Name' for CloudTrail is configured and that 'Account Id' and 'Region' are correct. Also determine if the CloudTrail account is configured with a 'Log File Prefix' and if so, it is also defined correctly for this event source.
Possible Cause	The S3 Bucket Name parameter and its associated parameters are not configured correctly.
Solution	For the event source that returned this message: 1. Make sure that you specified an S3 Bucket Name. 2. Make sure that you specified the correct Account Id and correct Region. 3. If the CloudTrail account has a Log File Prefix, make sure that you

specified it correctly.

For example:



Edit Source

Basic

Name * ctest

Enabled ☑

Account ID * 907171583576

S3 Bucket Name * sa-vlc-ct

Access Key * AKIAIHVBMFM3Y6KJ4BXA

Secret Key * ••

Region * us-east-1

Region Endpoint

Start Date * 0

Log File Prefix cloudtrail-

If the CloudTrail account is configured with a Log File Prefix, this field is required.

Check Point Collection Configuration Guide

This protocol collects events from Check Point event sources using OPSEC LEA. OPSEC LEA is the Check Point Operations Security Log Export API that facilitates the extraction of logs.

You must deploy Log Collection before you can configure the Check Point collection protocol.

For deployment instructions, see Log Collection Deployment Guide.

The Basics

Overview

This guide tells you how to configure Check Point collection protocol which collects events from a Check Point event source such as a firewall or Check Point Log Manager.

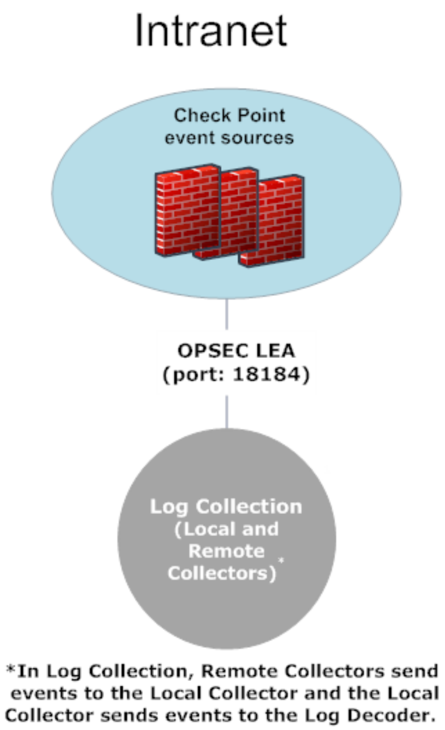
How Check Point Collection Works

The Log Collector service collects events from Check Point event sources using OPSEC LEA. OPSEC LEA is the Check Point Operations Security Log Export API that facilitates the extraction of logs.

Note: OPSEC LEA (Log Export API) supports extraction of logs from Check Point event sources configured with SHA-256 or SHA-1 certificate.

Deployment Scenario

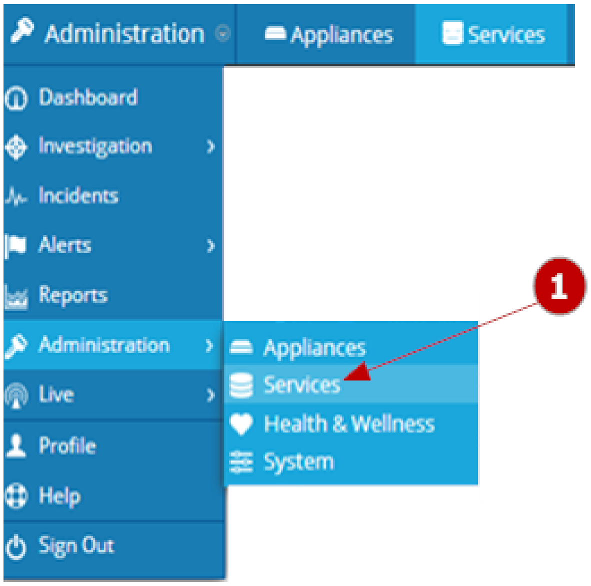
The following figure illustrates how you deploy the Check Point Collection Protocol in Security Analytics.


Intranet
Check Point event sources
OPSEC LEA (port: 18184)
Log Collection (Local and Remote Collectors)*
*In Log Collection, Remote Collectors send events to the Local Collector and the Local Collector sends events to the Log Decoder.

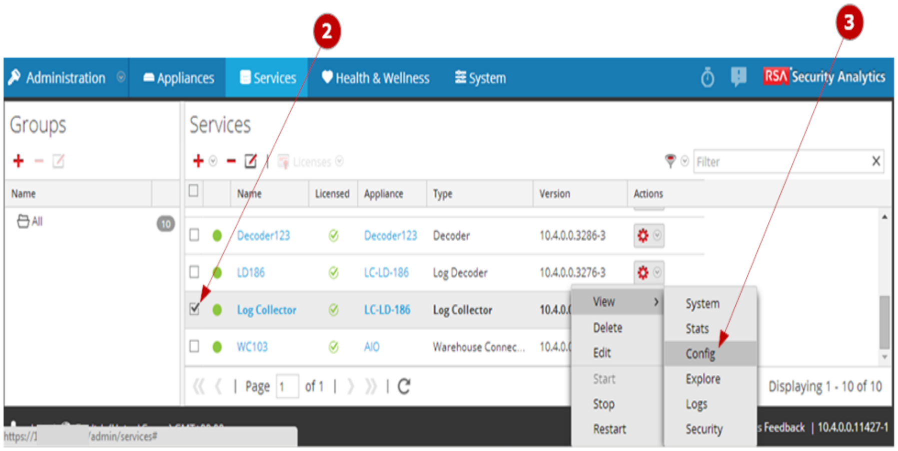
Configure Check Point Collection Protocol in Security Analytics

You configure to the Log Collector to use Check Point collection for an event source in the event Source tab of the Log Collector parameter view. The following figure the basic workflow for configuring an event source for Check Point Collection in Security Analytics. Please refer to:

- Step 2. Configure Check Point Event Sources in Security Analyticsfor step-by-step instructions on how to configure events sources in Security Analytics tht use the Check Point Collection protocol.
- Check Point Collection: Configuration Parametersfor a detailed description of each Check Point Collection Protocol parameter.



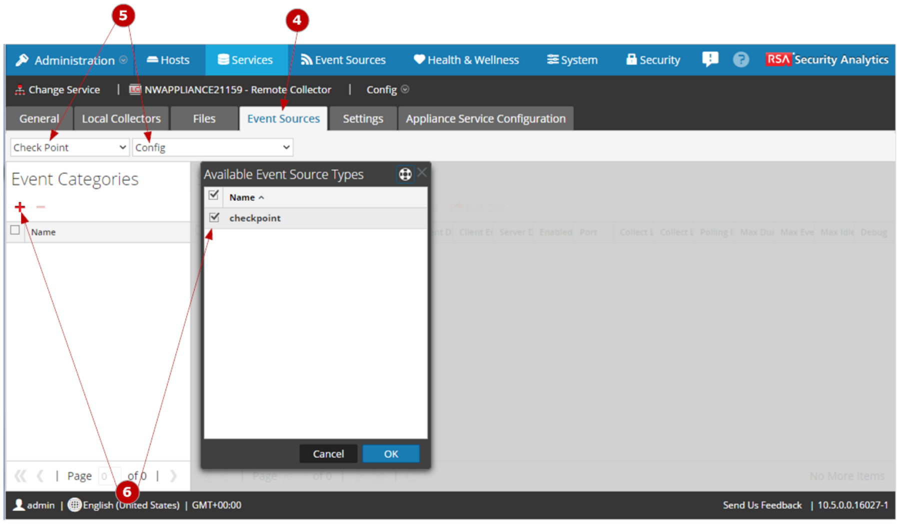
1 Access the **Services** view.



☐		Name	Licensed	Appliance	Type	Version	Actions
☐	●	Decoder123	✓	Decoder123	Decoder	10.4.0.0.3286-3	⚙
☐	●	LD186	✓	LC-LD-186	Log Decoder	10.4.0.0.3276-3	⚙
☑	●	Log Collector	✓	LC-LD-186	Log Collector	10.4.0.(	
☐	●	WC103	✓	AIO	Warehouse Connec...	10.4.0.(	

2 Select a **Log Collection** service.

3 Click ⌄ under **Actions** and select **View > Config** to display the Log Collection configuration parameter tabs.

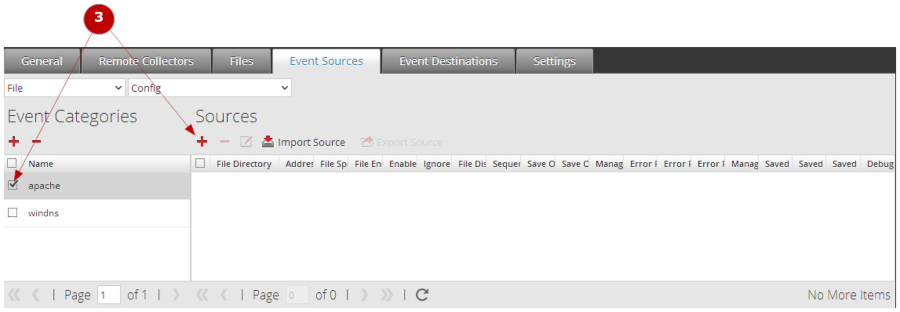


4 Click the **Event Sources** tab.

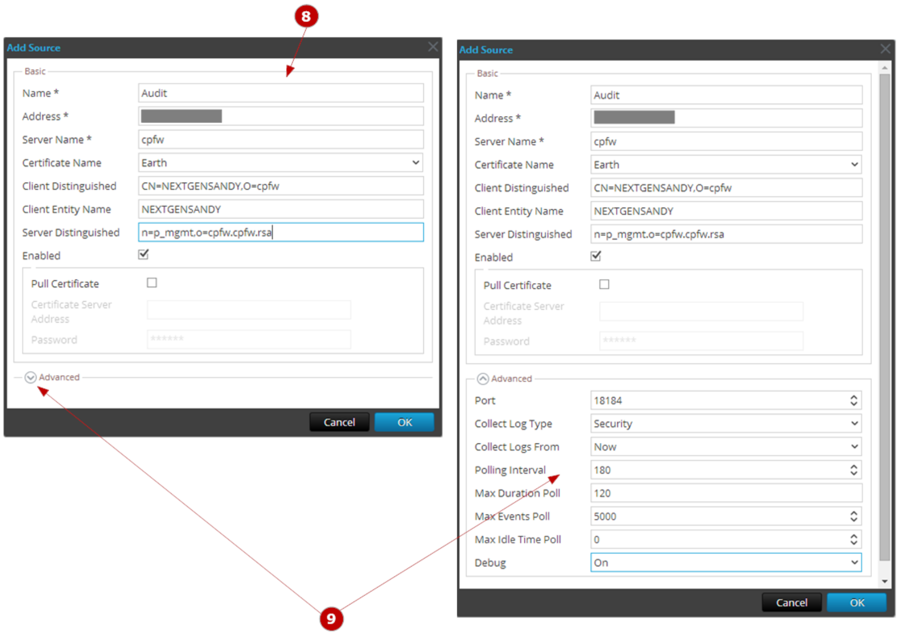
5 Select **Check Point** as the collection protocol and select **Config**.

6 Click + and select **Check Point** as the event source category.

The event source category is part of the content you downloaded from LIVE.



7 Select the **Check Point** category and click + .



Name *	Audit
Address *	[redacted]
Server Name *	cpfw
Certificate Name	Earth
Client Distinguished	CN=NEXTGENSANDY,O=cpfw
Client Entity Name	NEXTGENSANDY
Server Distinguished	n=p_mgmt.o=cpfw.cpfw.rsa
Enabled	☑
Pull Certificate	□
Certificate Server Address	
Password	******

Name *	Audit
Address *	[redacted]
Server Name *	cpfw
Certificate Name	Earth
Client Distinguished	CN=NEXTGENSANDY,O=cpfw
Client Entity Name	NEXTGENSANDY
Server Distinguished	n=p_mgmt.o=cpfw.cpfw.rsa
Enabled	☑
Pull Certificate	□
Certificate Server Address	
Password	******
Port	18184
Collect Log Type	Security
Collect Logs From	Now
Polling Interval	180
Max Duration Poll	120
Max Events Poll	5000
Max Idle Time Poll	0
Debug	On

8 Specify the basic parameters required for the **Check Point** event source.

9 Click ⌄ and specify additional parameters that enhance how the **Check Point** protocol handles event collection for the event source.

Configure Event Sources to Use Check Point Collection Protocol

You need to configure each event source that uses the Check Point Collection protocol to communicate with Security Analytics (see Step 1. Configure Check Point Event Sources to Send Events to Security Analytics).

Procedures

This topic provides an overview of the end-to-end sequential configuration procedure for the Check Point Collection protocol with a checklist that contains each configuration step.

Context

Configuration steps for the Check Point collection protocol must occur in the specific sequence listed in the table below.

Check Point Configuration Checklist

Note: The steps in this list are in the order in which you must complete them.

Step	Description	√
1	Configure Check Point Event Sources to Send Events to Security Analytics.	
2	Configure Check Point Event Sources in Security Analytics.	
3	Start service for configured Check Point collection protocol.	
4	Verify that Check Point Collection is working.	

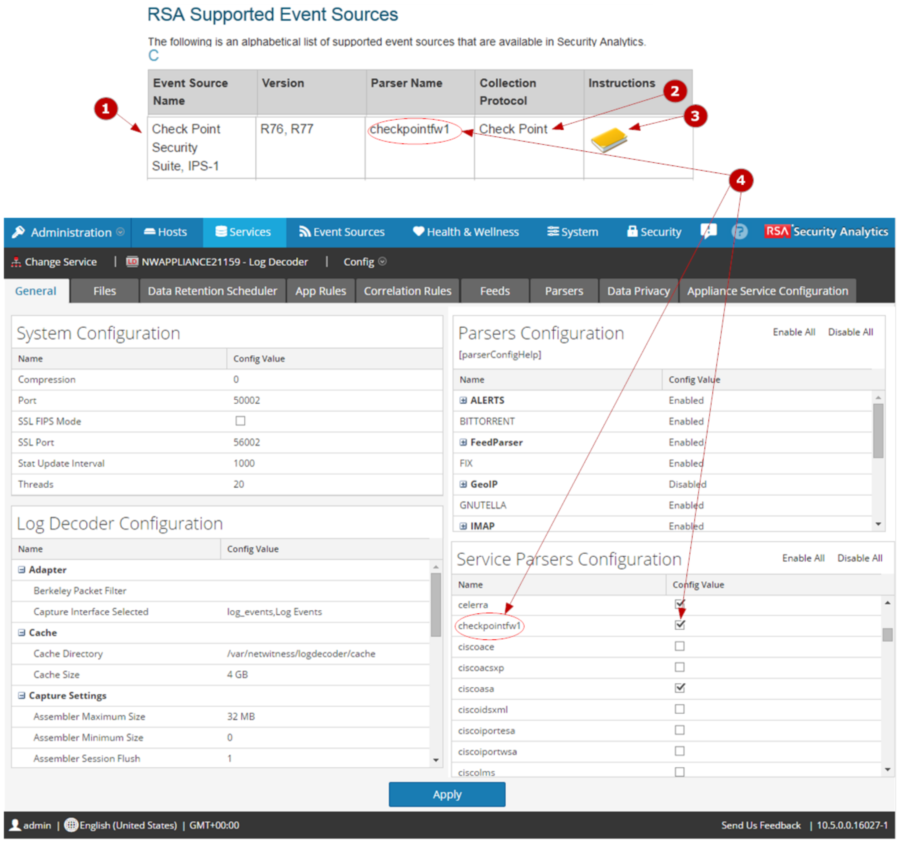
Step 1. Configure Check Point Event Sources to Send Events to Security Analytics

This topic tells you where to find the event sources currently supported for Check Point collection and the available configuration instructions for each event source.

Supported Event Sources List

Return to Procedures

The list of RSA Supported Event Sources is an alphabetized of all the event sources currently supported by Security Analytics that identifies which event sources you can use with Check Point Collection.



RSA Supported Event Sources

The following is an alphabetical list of supported event sources that are available in Security Analytics.

C

Event Source Name	Version	Parser Name	Collection Protocol	Instructions
Check Point Security Suite, IPS-1	R76, R77	checkpointfw1	Check Point	

System Configuration

Name	Config Value
Compression	0
Port	50002
SSL FIPS Mode	□
SSL Port	56002
Stat Update Interval	1000
Threads	20

Log Decoder Configuration

Name	Config Value
⊟ Adapter	
Berkeley Packet Filter	
Capture Interface Selected	log_events,Log Events
⊟ Cache	
Cache Directory	/var/netwitness/logdecoder/cache
Cache Size	4 GB
⊟ Capture Settings	
Assembler Maximum Size	32 MB
Assembler Minimum Size	0
Assembler Session Flush	1

Parsers Configuration

Enable All Disable All

[parserConfigHelp]

Name	Config Value
⊞ ALERTS	Enabled
BITTORRENT	Enabled
⊞ FeedParser	Enabled
FIX	Enabled
⊞ GeoIP	Disabled
GNUTELLA	Enabled
⊞ IMAP	Enabled

Service Parsers Configuration

Enable All Disable All

Name	Config Value
celerra	☑
checkpointfw1	☑
ciscoace	□
ciscoacsxp	□
ciscoasa	☑
ciscoidsxml	□
ciscoiportesa	□
ciscoiportwsa	□
ciscolms	□

Apply
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.5.0.0.16027-1

1 Find the name of the event source.

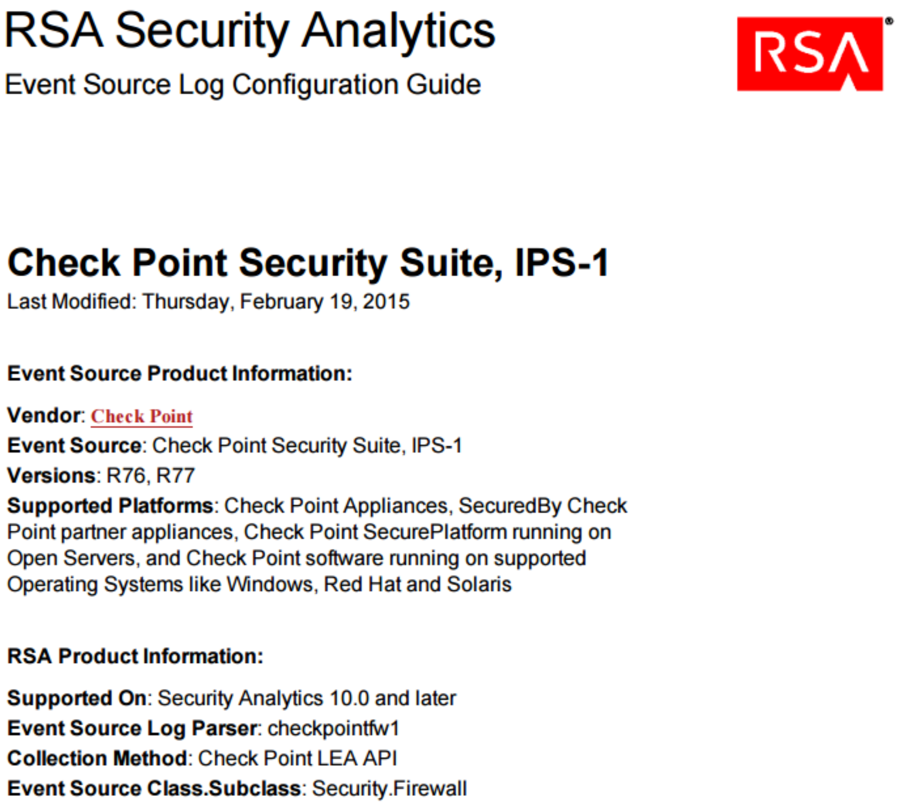
2 Verify that it is supported by the **Check Point Collection** Protocol.

3 Click on to display the configuration instructions for the event source.

4 Verify that you downloaded the correct event source parser (for example, **checkpointfw1**) from LIVE to the Log Decoder and enabled it.

Sample Configuration Instructions

The following illustration is taken from the Check Point Security Suite, IPS-1 configuration instructions.



RSA Security Analytics

Event Source Log Configuration Guide

Check Point Security Suite, IPS-1

Last Modified: Thursday, February 19, 2015

Event Source Product Information:

Vendor: Check Point
Event Source: Check Point Security Suite, IPS-1
Versions: R76, R77
Supported Platforms: Check Point Appliances, SecuredBy Check Point partner appliances, Check Point SecurePlatform running on Open Servers, and Check Point software running on supported Operating Systems like Windows, Red Hat and Solaris

RSA Product Information:

Supported On: Security Analytics 10.0 and later
Event Source Log Parser: checkpointfw1
Collection Method: Check Point LEA API
Event Source Class.Subclass: Security.Firewall

Step 2. Configure Check Point Event Sources in Security Analytics

This topic tells you how to configure Check Point event sources for the Log Collector.

After completing this procedure, you will have...

- Configured a Check Point event source.
- Modified a Check Point event source.
- Pulled a Certificate for a Check Point event source.

Return to Procedures

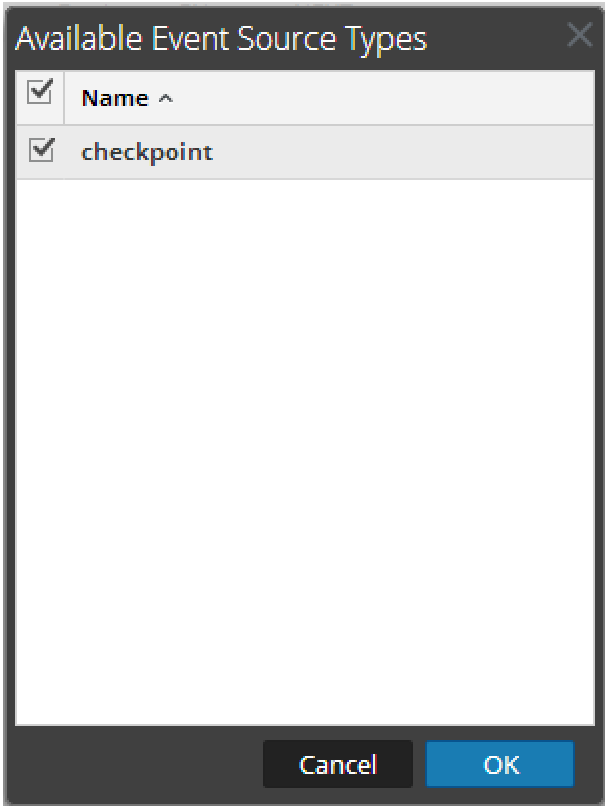
Procedures

Configure a Check Point Event Source

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.

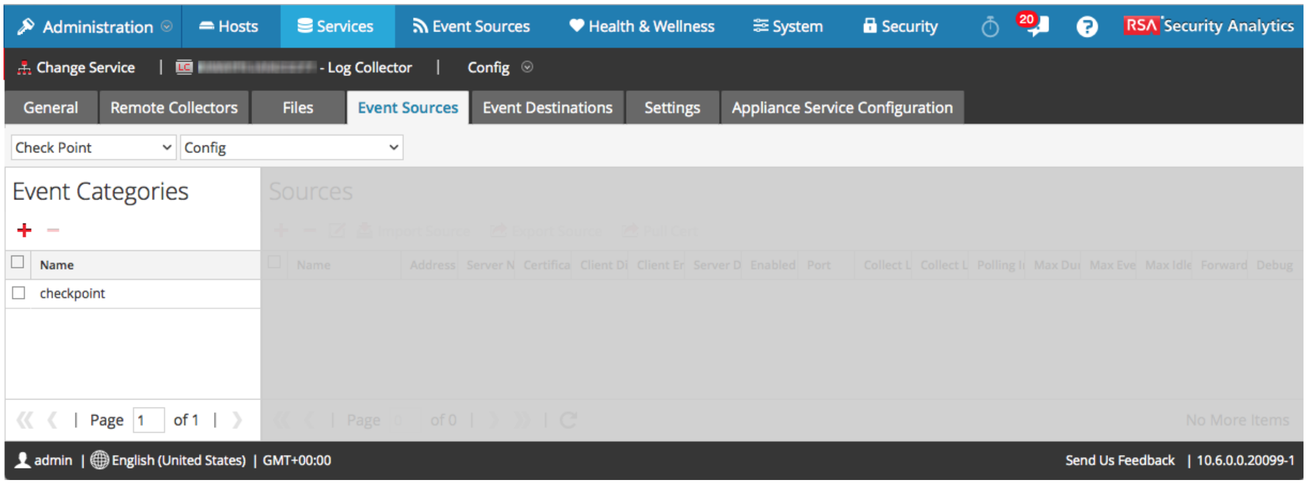
3. Click ⌄ under **Actions** and select **View > Config**.
4. In the **Event Sources** tab, select **Check Point/Config** from the drop-down menu.
5. In the **Event Categories** panel toolbar, click ➕.

   The **Available Event Source Types** dialog is displayed.
6. Select an event source type (for example, checkpoint) and click OK.



☑	Name ^
☑	checkpoint

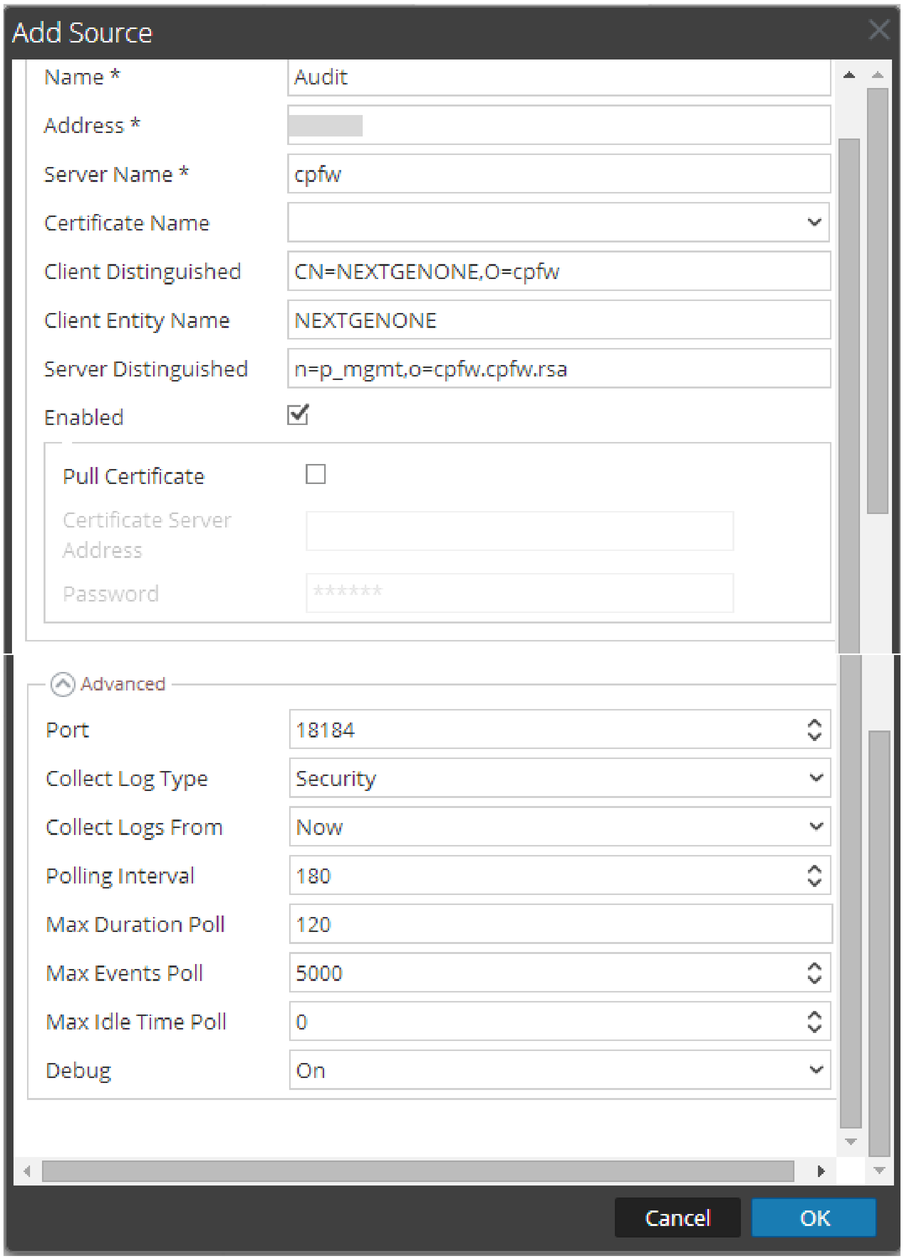
The newly added event source type is displayed in the **Event Categories** panel.



□	Name
□	checkpoint

7. Select the new type in the **Event Categories** panel and click ➕ in the **Sources** toolbar.
   The **Add Source** dialog is displayed.
8. Define parameter values (See Check Point Collection: Configuration Parametersfor definitions of each parameter).

> **Note:** You use less system resources when you set up a connection that only stays open for the time and event volume you specified or a transient connection. By default, the parameters are set up for a transient connection, as follows:
> **Max Events Poll** = 0
> **Polling Interval** = 0
> **Max Duration Poll** = 0
> **Polling Interval** = -1
> Specify the number of events and the length of time you want the connection to stay open in the **Max Events**, **Polling Interval**, **Max Duration Poll**, and **Polling Interval** parameters. For very active Check Point event sources, it is a good practice to set up a connection that stays open until you stop collection (persistent connection). This ensures that Check Point collection maintains the pace of the events generated by these active event sources. The persistent connection avoids restart and connection delays and prevents Check Point collection from lagging behind event generation. To establish a persistent connection for a Check Point event source, set the following parameters to the following values:
> **5000Polling Interval** = 180 (3 minutes)
> **Max Duration Poll** = 120 (2 minutes)
> **Max Events Poll** = 0



Add Source

Name *	Audit
Address *	[redacted]
Server Name *	cpfw
Certificate Name	
Client Distinguished	CN=NEXTGENONE,O=cpfw
Client Entity Name	NEXTGENONE
Server Distinguished	n=p_mgmt,o=cpfw.cpfw.rsa
Enabled	☑
Pull Certificate	□
Certificate Server Address	
Password	******

Advanced

Port	18184
Collect Log Type	Security
Collect Logs From	Now
Polling Interval	180
Max Duration Poll	120
Max Events Poll	5000
Max Idle Time Poll	0
Debug	On

9. Select **Pull Certificate** to pull a certificate for the first time. This makes the certificate available from the trust store.

10. Click **OK**.

The new event source is displayed in the **Sources** panel.

Pull Certificate

Complete the following procedure if you:

- did not pull a certificate when you configured a Check Point event source, or
- need to re-pull a certificate.

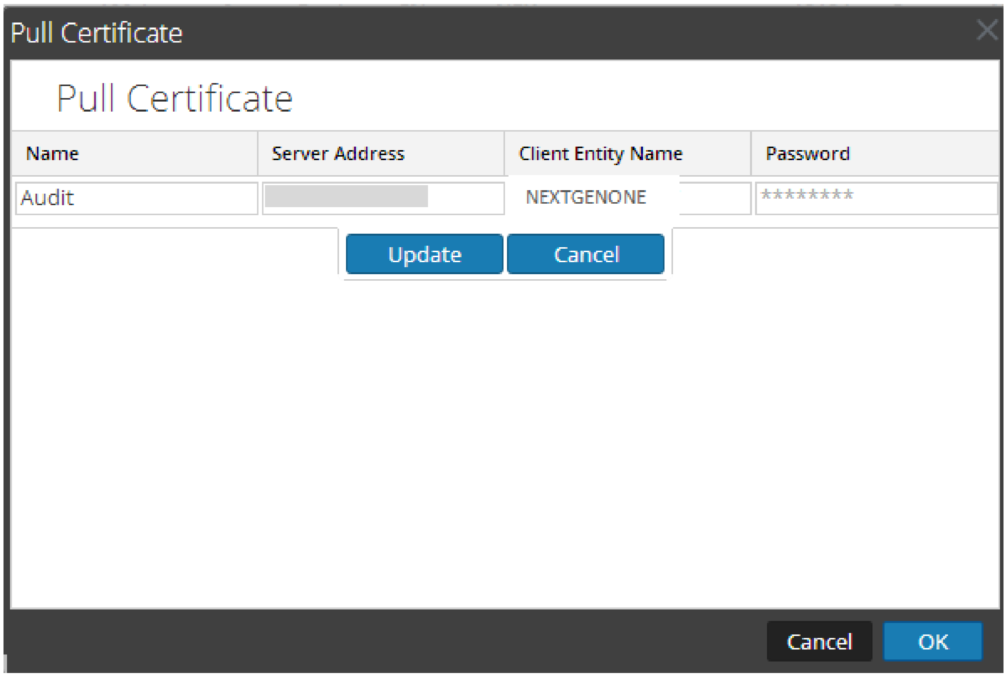
To pull a certificate:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Event Sources** tab, select **Check Point/Config** from the drop-down menu.
5. Select an event source type in the Event Categories panel.

   The sources for this type are displayed in the **Sources** panel.
6. Select a source, or multiple sources, and click Pull Cert.

   The settings of the Check Point server(s) from which you can pull certificates are displayed.
7. Click the text box under **Password**.

   All the fields become editable.



Name	Server Address	Client Entity Name	Password
Audit	[redacted]	NEXTGENONE	********

8. Enter a password, click **Update**, and click **OK.**

   > **Note:** You must specify a password. If you need to modify the other Check Point server certificate parameters (Audit, Server Address, and Client Entity Name) you have that option.

   Security Analytics pulls the certificate.

Modify a Check Point Event Source

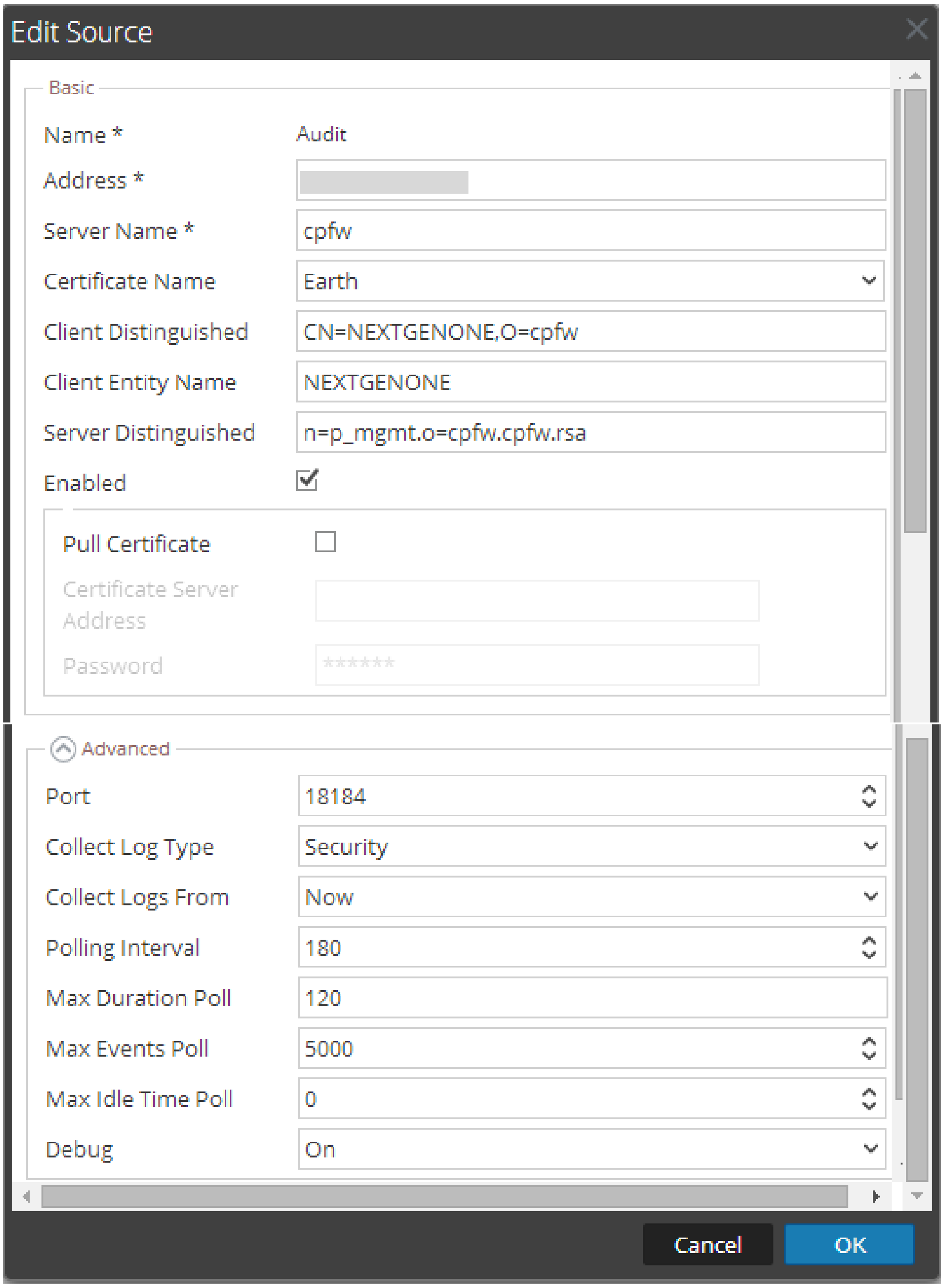
To modify an event source:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.
4. In the **Event Sources** tab, select **Check Point/Config** from the drop-down menu.

   The **Event Categories** panel is displayed with the event sources that are configured, if any.
5. Select an event source type in the **Event Categories** panel.

   The event sources for this type are displayed in the **Sources** panel.
6. Select a source and click ✎ in the toolbar.

   The **Edit Source** dialog is displayed.
7. Modify the parameters that require changes and click **Save**.


Edit Source

Basic

Name * Audit

Address * [redacted]

Server Name * cpfw

Certificate Name Earth

Client Distinguished CN=NEXTGENONE,O=cpfw

Client Entity Name NEXTGENONE

Server Distinguished n=p_mgmt.o=cpfw.cpfw.rsa

Enabled ☑

Pull Certificate □

Certificate Server Address

Password ******

Advanced

Port 18184

Collect Log Type Security

Collect Logs From Now

Polling Interval 180

Max Duration Poll 120

Max Events Poll 5000

Max Idle Time Poll 0

Debug On

Security Analytics applies the parameter changes to the selected event source.

Parameters

Check Point Collection: Configuration Parameters

Step 3. Start Service for Configured Check Point Collection Protocol

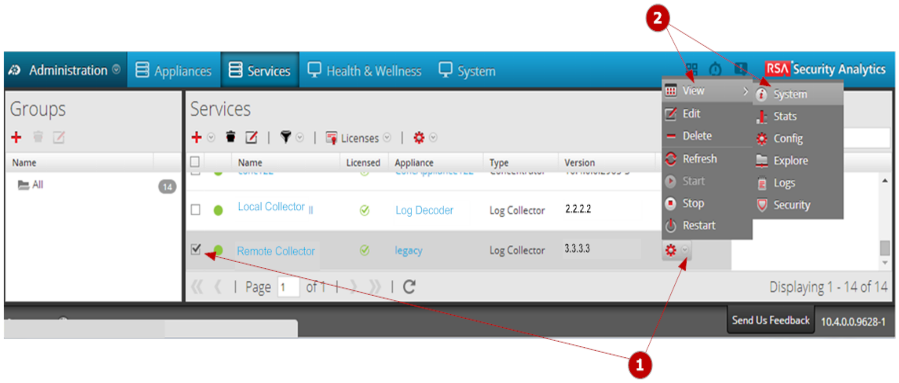
This topic tells you how to start a stopped Check Point collection service.

Return to Procedures

You may need to start a stopped collection service or enable the automatic start of an individual service.

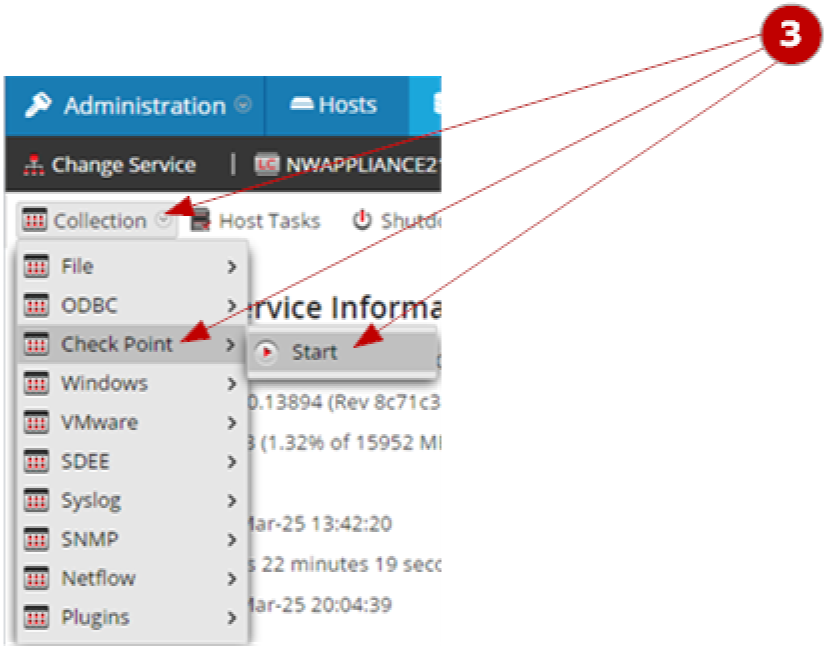
Procedure

The following figure shows you how to start a collection service. See the **Enable Automatic Start of Individual Services** topic in the *Log Collection Configuration Guide* if you want the service to start automatically.



1 Select a **Log Collector** service and click ⌄ under **Actions**.

2 Click **View** > **System**.



3 Click **Collection** > **Check Point** and click **Start**.

Step 4. Verify That Check Point Collection Is Working

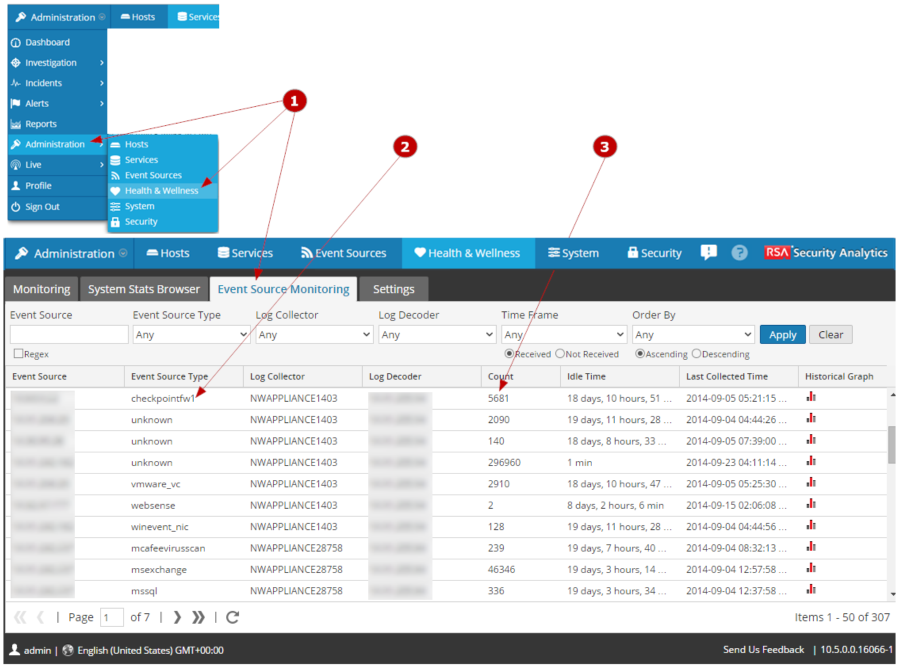
This topic tells you what to check in Security Analytics to verify that you have configured Check Point Collection correctly.

Return to Procedures

You may need to verify that Check Point Collection is configured correctly, otherwise it won't work.

Procedure

The following figure illustrates how you can verify that Check Point collection is working from the **Administration** > **Health & Wellness** > **Event Source Monitoring** tab.



Event Source: (empty) □ Regex | Event Source Type: Any | Log Collector: Any | Log Decoder: Any | Time Frame: Any ● Received ○ Not Received | Order By: Any ● Ascending ○ Descending

Event Source	Event Source Type	Log Collector	Log Decoder	Count	Idle Time	Last Collected Time	Historical Graph
[redacted]	checkpointfw1	NWAPPLIANCE1403	[redacted]	5681	18 days, 10 hours, 51 ...	2014-09-05 05:21:15 ...	
[redacted]	unknown	NWAPPLIANCE1403	[redacted]	2090	19 days, 11 hours, 28 ...	2014-09-04 04:44:26 ...	
[redacted]	unknown	NWAPPLIANCE1403	[redacted]	140	18 days, 8 hours, 33 ...	2014-09-05 07:39:00 ...	
[redacted]	unknown	NWAPPLIANCE1403	[redacted]	296960	1 min	2014-09-23 04:11:14 ...	
[redacted]	vmware_vc	NWAPPLIANCE1403	[redacted]	2910	18 days, 10 hours, 47 ...	2014-09-05 05:25:30 ...	
[redacted]	websense	NWAPPLIANCE1403	[redacted]	2	8 days, 2 hours, 6 min	2014-09-15 02:06:08 ...	
[redacted]	winevent_nic	NWAPPLIANCE1403	[redacted]	128	19 days, 11 hours, 28 ...	2014-09-04 04:44:56 ...	
[redacted]	mcafeevirusscan	NWAPPLIANCE28758	[redacted]	239	19 days, 7 hours, 40 ...	2014-09-04 08:32:13 ...	
[redacted]	msexchange	NWAPPLIANCE28758	[redacted]	46346	19 days, 3 hours, 14 ...	2014-09-04 12:57:58 ...	
[redacted]	mssql	NWAPPLIANCE28758	[redacted]	336	19 days, 3 hours, 34 ...	2014-09-04 12:37:58 ...	

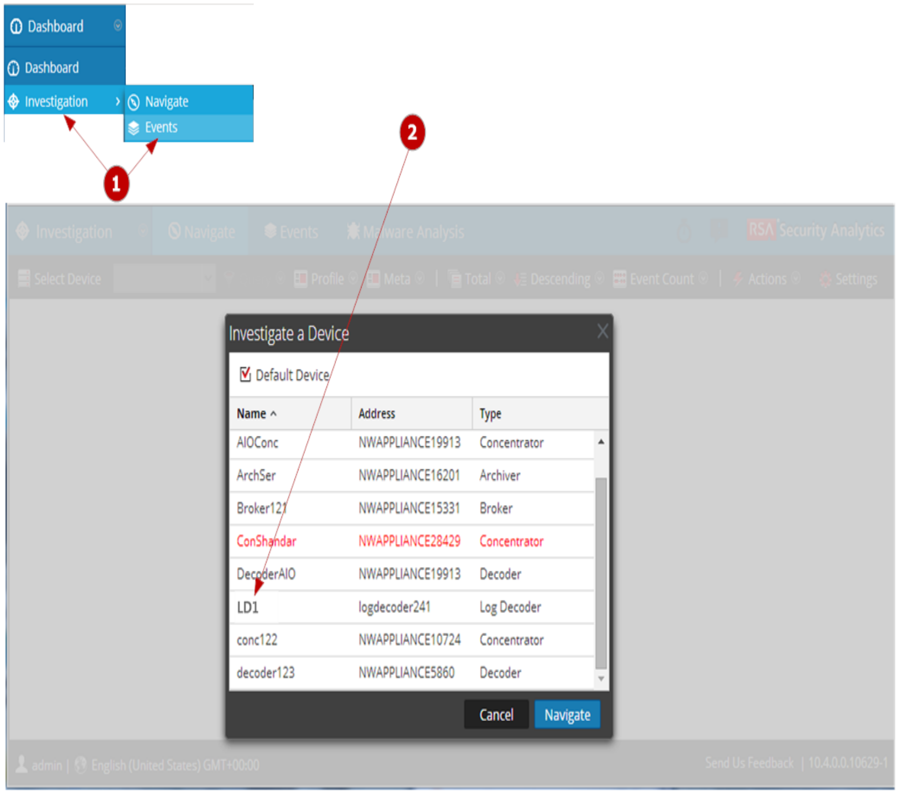
Page 1 of 7 | Items 1 - 50 of 307

1 Access the **Event Source Monitoring tab** from the **Administration** > **Health & Wellness** view.

2 Find **checkpointfw1** in the **Event Source Type** column.

3 Look for activity in the **Count** column to verify that Check Point collection is accepting events.

The following figure illustrates how you can verify that Check Point collection is working from the **Investigation** > **Events** view.



Investigate a Device

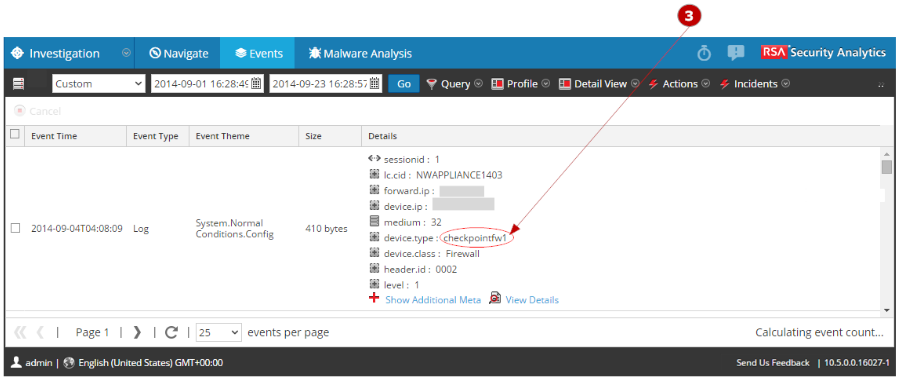
☑ Default Device

Name ^	Address	Type
AIOConc	NWAPPLIANCE19913	Concentrator
ArchSer	NWAPPLIANCE16201	Archiver
Broker121	NWAPPLIANCE15331	Broker
ConShandar	NWAPPLIANCE28429	Concentrator
DecoderAIO	NWAPPLIANCE19913	Decoder
LD1	logdecoder241	Log Decoder
conc122	NWAPPLIANCE10724	Concentrator
decoder123	NWAPPLIANCE5860	Decoder

Cancel Navigate

1 Access the **Investigation** > **Events** view.

2 Select the Log Decoder (for example, **LD1**) collecting Check Point events in the **Investigate a Device** dialog.



Custom 2014-09-01 16:28:49 2014-09-23 16:28:57

□	Event Time	Event Type	Event Theme	Size	Details
□	2014-09-04T04:08:09	Log	System.Normal Conditions.Config	410 bytes	sessionid : 1 lc.cid : NWAPPLIANCE1403 forward.ip : [redacted] device.ip : [redacted] medium : 32 device.type : checkpointfw1 device.class : Firewall header.id : 0002 level : 1

Page 1 | 25 events per page Calculating event count...

3 Look for a Check Point event source parser (for example, **checkpointfw1**)in the **device.type** field in the **Details** column to verify that Check Point collection is accepting events.

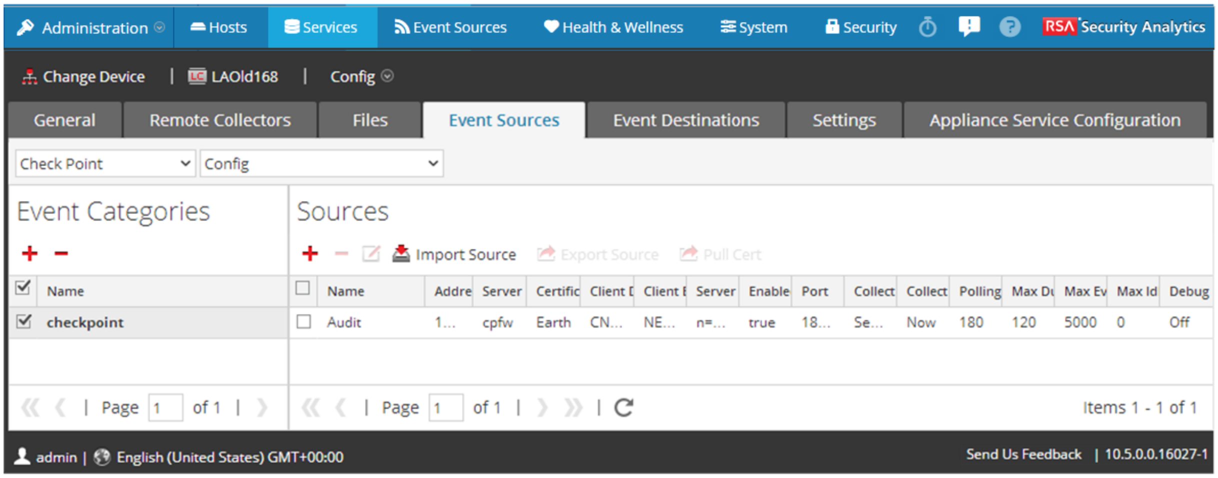
Note: If the logs from the VSX Checkpoint firewall server is collected by the Log Collector checkpoint service, to translate the VSX IP in the logs to ip.orig meta, you must add the VSX hostname and the VSX IP address to the `/etc/hosts` file in the Log Collector.

Check Point Collection: Configuration Parameters

This topic describes the Check Point event source configuration parameters

To access the Check Point Collection Configuration Parameters:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Log Collector Event Sources** tab, select **Check Point/Config** from the drop-down menu.



☑	Name
☑	checkpoint

□	Name	Addre	Server	Certific	Client [	Client E	Server	Enable	Port	Collect	Collect	Polling	Max Du	Max Ev	Max Id	Debug
□	Audit	1...	cpfw	Earth	CN...	NE...	n=...	true	18...	Se...	Now	180	120	5000	0	Off

The Check Point/Config view in the Event Sources tab has two panels: Event Categories and Sources.

Event Categories Panel

In the Event Categories panel, you can add or delete the appropriate event source types.

Feature	Description
+	Displays the Available Event Source Types dialog from which you select the event source type for which you want to define parameters.

Feature	Description
−	Deletes the selected event source types from the Event Categories panel.
☐	Selects event source types.
Name	Displays the name of the event source types that you have added.

Available Event Sources Types Dialog

The Available Event Source Types dialog displays the list of supported event source types.

Feature	Description
☐	Selects the event source type that you want to add.
Type	Display the event source types that are available to add.
Cancel	Closes the dialog without adding an event source type.
OK	Adds the selected event source type to the Event Categories panel.

Sources Panel

The Check Point Sources panel displays a list of existing Check Point firewall event sources. Use this section to add or delete event sources and associated communication parameters.

Toolbar

The following table provides descriptions of the toolbar options.

Feature	Description
+	Displays the Add Source dialog in which you define the parameters for a Check Point Firewall host.
−	Deletes the host that you selected.

Feature	Description
✎	Opens the Edit Source dialog, in which you edit the parameters for the selected Check Point event source. Select multiple event sources and click ✎ to open the Bulk Edit Source dialog in which you can edit the parameters values for the selected event sources. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.
Import Source	Opens the Bulk Add Option dialog in which you can import Check Point hosts in bulk from a comma-separated values (CSV) file. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.
Export Source	Creates a .csv file that contains the parameters for the selected Check Point hosts. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.
Pull Cert	Open the Pull Certificate dialog. Use this dialog to pull a certificate from the Check Point server for this host.

Add or Edit Source Dialog

The Add Source dialog and the Edit Source dialog the contain the same information.

Parameter	Description
Basic	
Name*	Name of the event source.
Server Address*	IP Address of the Check Point server.
Server Name*	Name of the Check Point server.

Parameter	Description
Certificate Name	Certificate name for secure connections to use when the transport mode is https. If set, the certificate must exist in the certificate trust store that you created using the Settings tab. Select a certificate from the drop-down list. The file naming convention for Check Point event source certificates is checkpoint_name-of-event-source.
Client Distinguished	Enter the Client Distinguished Name from the Check Point server.
Client Entity Name	Enter the Client Entity Name from the Check Point server.
Server Distinguished	Enter the Server Distinguished Name from the Check Point server.
Pull Certificate	Select the checkbox to pull a certificate for first time. Pulling a certificate makes it available from the trust store.
Certificate Server Address	IP Address of the server on which the certificate resides.
Password	Only active when you select the Pull Certificate checkbox for first time. Password required to pull the certificate. The password is the activation key created when adding an OPSEC application to Check Point on the Check Point server.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td colspan="2"><b>Advanced</b></td></tr>
<tr><td colspan="2"><b>Note:</b> You use less system resources when you configure a Check Point event source connection to stay open for a specific time and specific event volume (transient connection). Security Analytics defaults to the following connection parameters that establish a transient connection:

Polling Interval = 180 (3 minutes)
Max Duration Poll = 120 (2 minutes)
Max Events Poll = 5000 (5000 events per polling interval)
Max Idle Time Poll = 0

For very active Check Point event sources, it is a good practice to set up a connection that stays open until you stop collection (persistent connection). This ensures that Check Point collection maintains the pace of the events generated by these active event sources. The persistent connection avoids restart and connection delays and prevents Check Point collection from lagging behind event generation. To establish a persistent connection for a Check Point event source, set the following parameters to the following values:

Polling Interval = -1
Max Duration Poll = 0
Max Events Poll = 0
Max Idle Time Poll = 0</td></tr>
<tr><td>Port</td><td>Port on the Check Point server that Log Collector connects to.
Default value is 18184.</td></tr>
<tr><td>Collect Log Type</td><td>Type of logs that you want to collect: Valid values are:
• <b>Audit</b> - collects audit events.
• <b>Security</b> - collects security events.

If you want to collect both audit and security events, you must create a duplicate event source. For example, first you would create an event source with Audit selected pulling a certificate into the trust store for this event source. Next you would create another event source with the same values except that you would select Security for the Collect Log Type and you would select the same certificate in Certificate Name that you pulled when you set up the first set of parameters for this event source and you would make sure that Pull Certificate was not selected.</td></tr>
</table>

Parameter	Description
Collect Logs From	When you set up a Check Point event source, Security Analytics collects events from the current log file. Valid values are: • **Now** - Start collecting logs now (at this point in time in the current log file). • **Start of Log -** Collect logs from the beginning of the current log file. If you choose **Start of Log** for this parameter value, you may collect a very large amount of data depending on how long the current log file has been collecting events. And, this option is effective only for the first collection session.
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Duration Poll	The maximum duration of polling cycle (how long the cycle lasts) in seconds.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum idle time, in seconds, of a polling cycle. 0 indicates no limit.> **300** is the default value.
Forwarder	Enables or disables the Check Point server as a forwarder. By default it is disabled.
Log Type (Name Value Pair)	Logs from the event source in Name Value format. By default it is disabled.

Parameter	Description
Debug	**Caution:** Only enable debugging (set this parameter to "On" or "Verbose") if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables and disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
Cancel	Closes the dialog without adding the Check Point Firewall host.
OK	Adds the current parameter values as a new Check Point host.

Pull Certificate Dialog

The following table provides descriptions of the Pull Certificate dialog parameters.

Parameter	Description
Name	Displays the name of the event source
Server Address	Displays the IP Address of the Check Point server.
Client Entity Name	Displays the Client Entity Name that you acquire when you configure the Check Point event source for Security Analytics.

Parameter	Description
Password	Activation key created when adding an OPSEC application to Check Point. You need to reenter this password to pull the certificate from the Check Point server.
Update	(Only displays in edit mode - click on Password field) Applies edits that you make to the host parameters.
Cancel	(Only displays in edit mode - click on Password field) Closes edit mode with applying changes.
Cancel	Closes the dialog without pulling a certificate.
OK	Pulls the certificate.

Tasks

Step 2. Configure Check Point Event Sources in Security Analytics

Troubleshoot Check Point Collection

Overview

This topic highlights possible problems that you may encounter with Check Point Collection and suggested solutions to these problems.

Troubleshoot Check Point Collection Issues

In general, you receive more robust log messages by disabling SSL.

Log Message/ Problem	Check Point Collection is not keeping up with the pace at which a Check Point event source is sending events.
Possible Cause	You have not configured the parameters for this event source so that it have a persistent connection.

Solution	To establish a persistent connection for a Check Point server, set the following Event Source parameters to the following values: • **Polling Interval** = -1 • **Max Duration Poll** = 0 • **Max Events Poll** = 0 • **Max Idle Time Poll** = 0

File Collection Protocol Configuration Guide

This guide tells you how to configure the File collection protocol. This protocol collects events from log files.

You must deploy Log Collection before you can configure the File collection protocol.

For deployment instructions, see Log Collection Deployment Guide.

To set up the SFTP Agent Collector, download the following PDF guides from RSA Link:

- To set up the SFTP agent on Windows, download **Install and Update the SFTP Agent**: https://community.rsa.com/docs/DOC-53125
- To set up the SFTP agent on Linux, download Configure SFTP Shell Script File Transfer: https://community.rsa.com/docs/DOC-53124

The Basics

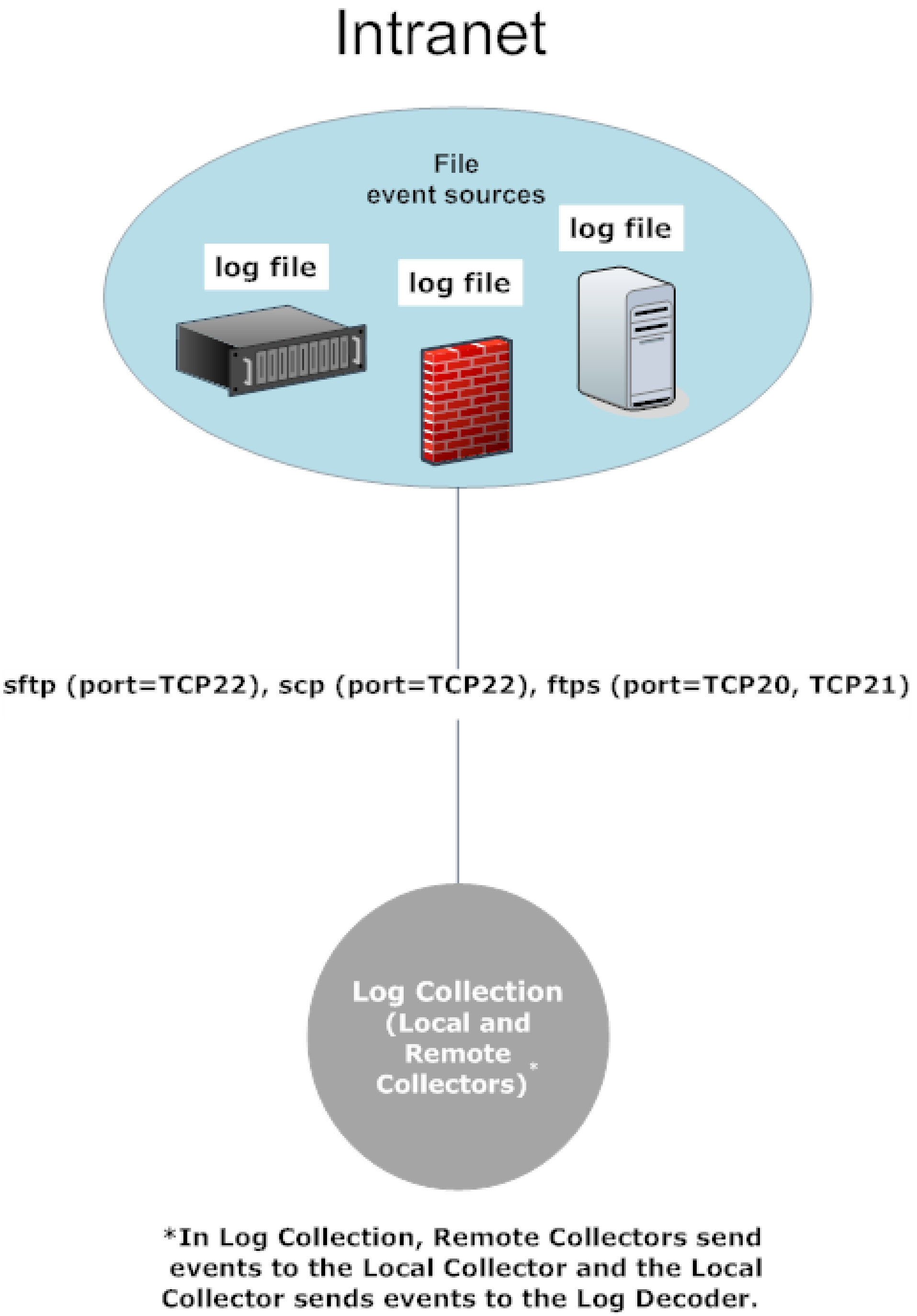
This guide tells you how to configure File collection protocol which collects events from log files. The Event sources for this protocol generate log files that are transferred using a secure file transfer method to the Log Collector service.

How File Collection Works

The Log Collector service collects events from log files. Event sources generate log files that are transferred using a secure file transfer method to the Log Decoder host running the Log Collector service.

Deployment Scenario

The File collection protocol collects event data from log files.

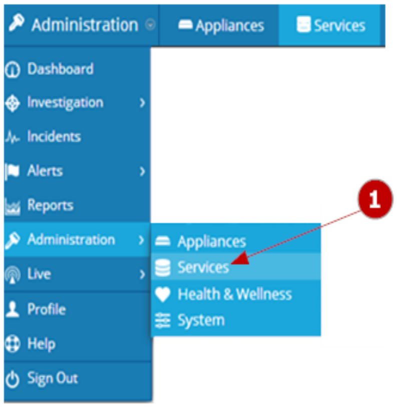

Intranet
File
event sources
log file
log file
log file
sftp (port=TCP22), scp (port=TCP22), ftps (port=TCP20, TCP21)
Log Collection
(Local and
Remote
Collectors)*
*In Log Collection, Remote Collectors send
events to the Local Collector and the Local
Collector sends events to the Log Decoder.

Procedures

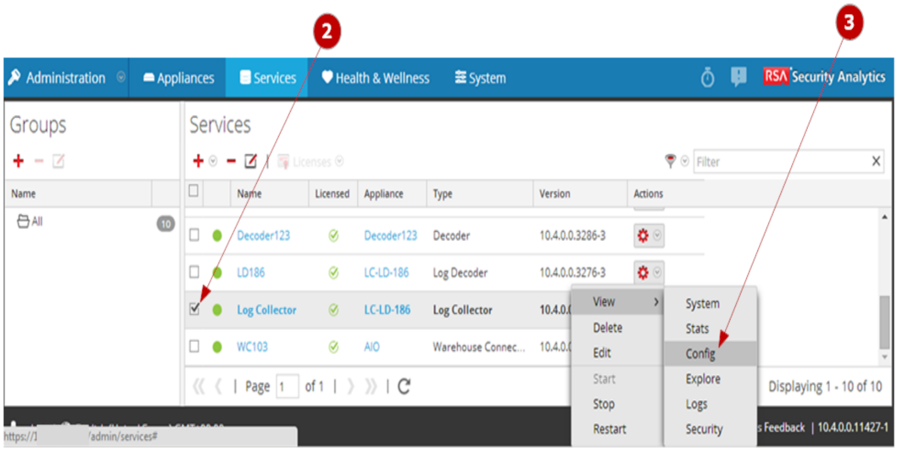
Configure File Collection Protocol in Security Analytics

You configure the Log Collector to use File collection for an event source in the Event Source tab of the Log Collector parameter view. The following figure depicts the basic workflow for configuring an event source for File Collection in Security Analytics. Please refer to:

- Step 1. Configure File Event Sources in Security Analytics for step-by-step instructions on how to configure events sources in Security Analytics that use the File Collection protocol.
- File Collection: Configuration Parameters for a detailed description of each File Collection Protocol parameter.



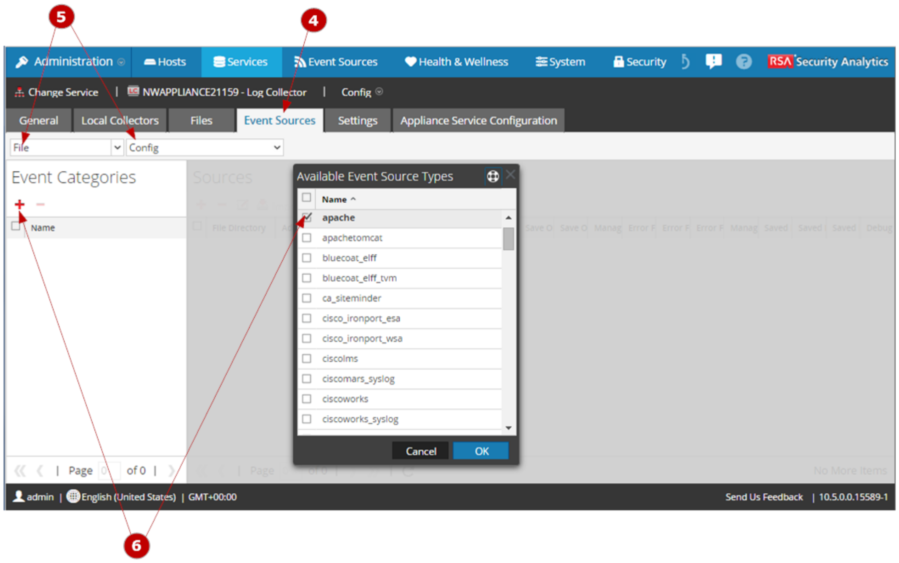
1. Access the **Services** view.



□	Name	Licensed	Appliance	Type	Version	Actions
□	Decoder123	✓	Decoder123	Decoder	10.4.0.0.3286-3	
□	LD186	✓	LC-LD-186	Log Decoder	10.4.0.0.3276-3	
☑	Log Collector	✓	LC-LD-186	Log Collector	10.4.0.	
□	WC103	✓	AIO	Warehouse Connec...	10.4.0.	

2. Select a Log Collection service.

3. Click ⚙ ⌄ under **Actions** and select **View** > **Config** to display the Log Collection configuration parameter tabs.



Available Event Source Types

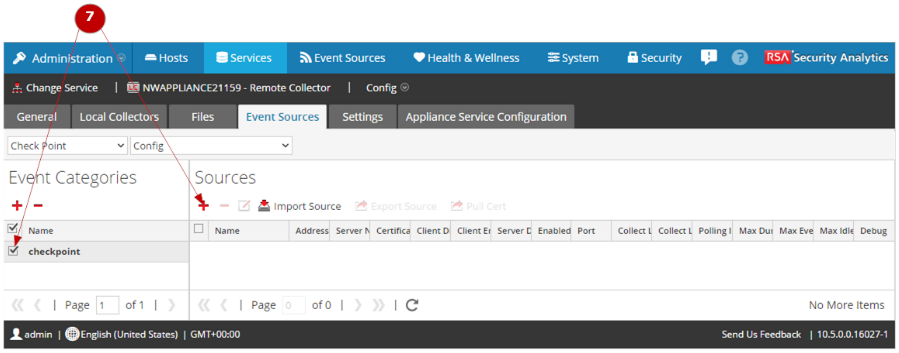
Name ^
☑ apache
☐ apachetomcat
☐ bluecoat_elff
☐ bluecoat_elff_tvm
☐ ca_siteminder
☐ cisco_ironport_esa
☐ cisco_ironport_wsa
☐ ciscolms
☐ ciscomars_syslog
☐ ciscoworks
☐ ciscoworks_syslog

4. Click the **Event Sources** tab.

5. Select **File**as the collection protocol and select **Config**.

6. Click ✚ and select and event source type (for example, **apache**) as the event source category.

The event source category is part of the content you downloaded from LIVE.

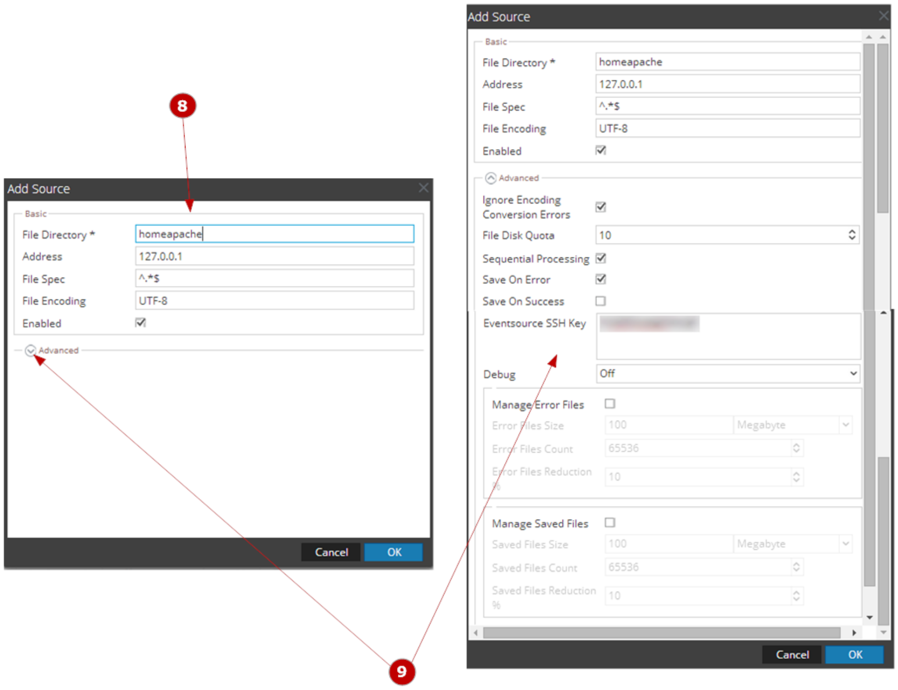


☑ Name
☑ checkpoint

☐	Name	Address	Server N	Certifica	Client D	Client Er	Server D	Enabled	Port	Collect L	Collect L	Polling I	Max Dur	Max Eve	Max Idle	Debug

7. Select the newly added category (for example, **apache**).

Click ✚.



File Directory * homeapache
Address 127.0.0.1
File Spec ^.*$
File Encoding UTF-8
Enabled ☑

File Directory * homeapache
Address 127.0.0.1
File Spec ^.*$
File Encoding UTF-8
Enabled ☑
Ignore Encoding Conversion Errors ☑
File Disk Quota 10
Sequential Processing ☑
Save On Error ☑
Save On Success ☐
Eventsource SSH Key [redacted]
Debug Off
Manage Error Files ☐
Error Files Size 100 Megabyte
Error Files Count 65536
Error Files Reduction % 10
Manage Saved Files ☐
Saved Files Size 100 Megabyte
Saved Files Count 65536
Saved Files Reduction % 10

8. Specify the basic parameters required for the event source.

9. Click and specify additional parameters that enhance how the protocol handles event collection for the event source.

Configure Event Sources to Use File Collection Protocol

You need to configure each event source that uses the File Collection protocol to communicate with Security Analytics (see Step 2. Configure File Event Sources to Send Events to Security Analytics).

Procedures

This topic provides an overview of the end-to-end sequential configuration procedure for the File Collection protocol with a checklist that contains each configuration step

Configuration steps for the File collection protocol must occur in the specific sequence listed in the table below.

File Collection Configuration Checklist

Note: The steps in this list are in the order in which you must complete them.

Step	Description	√
1	Configure File Event Sources in Security Analytics.	
2	Configure File Event Sources to Send Events to Security Analytics.	
3	Start service for configured File collection protocol.	
4	Verify that File Collection is working.	

Step 1. Configure File Event Sources in Security Analytics

This topic tells you how to configure File event sources in Security Analytics.

After completing this procedure, you will have...

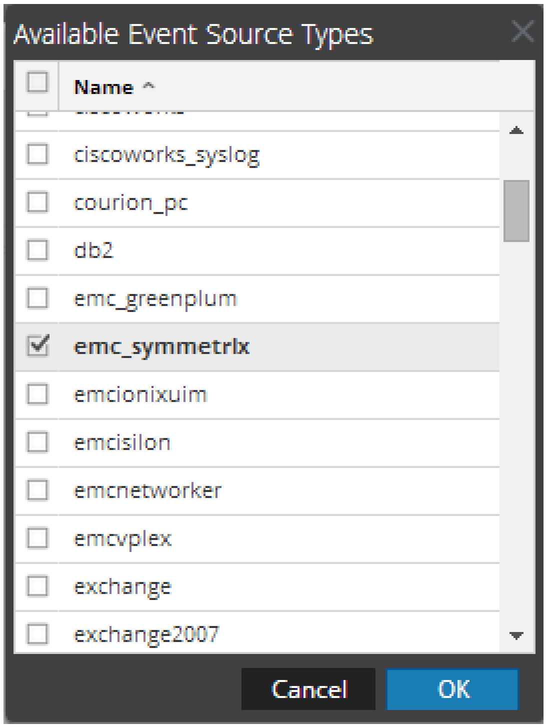
- Configured File collection for an event source in Security Analytics.
- Modified File collection for an event source in Security Analytics.
- Verified that the correct parser has been enabled on the Log Decoder to parse the log events from the new event source.

Return to Procedures

Procedures

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Log Collector Event Sources** tab, select **File/Config** from the drop-down menu.

5. In the **Event Categories** panel toolbar, click +.

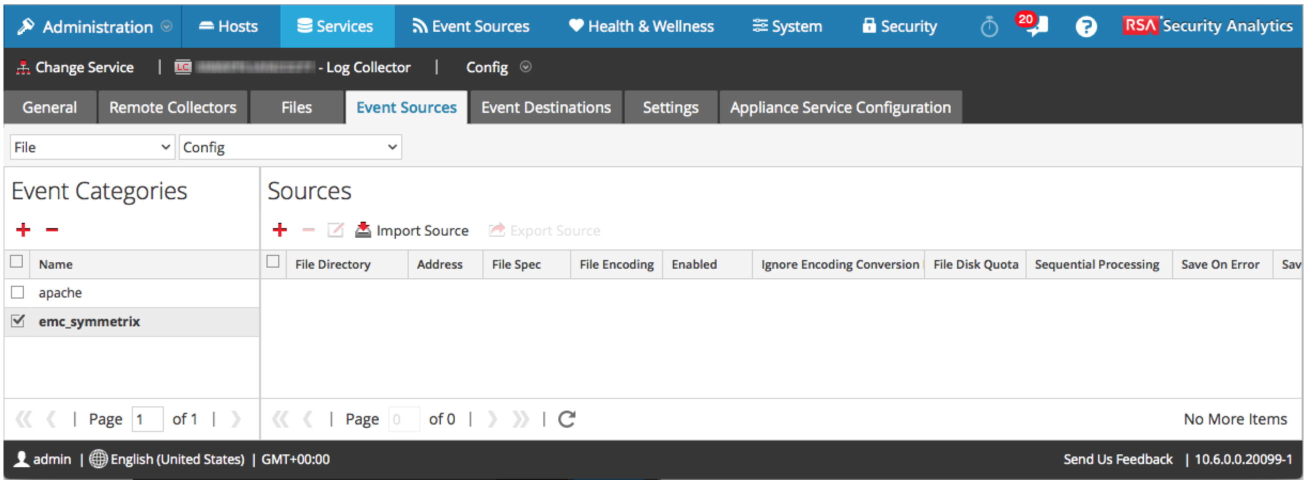


Available Event Source Types

☐	Name ^
☐	ciscoworks_syslog
☐	courion_pc
☐	db2
☐	emc_greenplum
☑	emc_symmetrix
☐	emcionixuim
☐	emcisilon
☐	emcnetworker
☐	emcvplex
☐	exchange
☐	exchange2007

6. Select an event source type (for example, **emc_symmetrix**) and click **OK**.

   The newly added event source type is displayed in the Event Categories panel.



Event Categories

☐	Name
☐	apache
☑	emc_symmetrix

Page 1 of 1

Sources

☐	File Directory	Address	File Spec	File Encoding	Enabled	Ignore Encoding Conversion	File Disk Quota	Sequential Processing	Save On Error	Sav

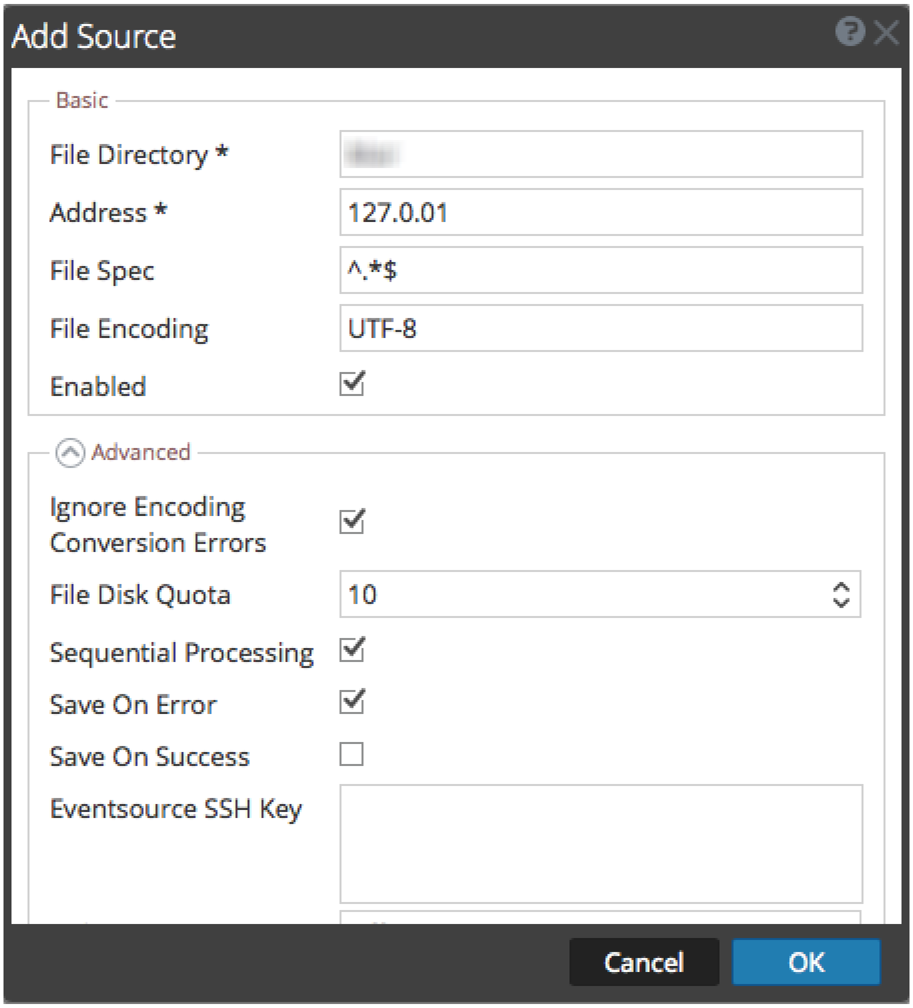
Page 0 of 0 | No More Items

admin | English (United States) | GMT+00:00 | Send Us Feedback | 10.6.0.0.20099-1

7. Select the new type in the **Event Categories** panel and click + in the Sources toolbar.

   The **Add Source** dialog is displayed.

8. Add a **File Directory** name and modify any other parameters that require changes.



Basic

File Directory * [redacted]

Address * 127.0.01

File Spec ^.*$

File Encoding UTF-8

Enabled ☑

Advanced

Ignore Encoding Conversion Errors ☑

File Disk Quota 10

Sequential Processing ☑

Save On Error ☑

Save On Success □

Eventsource SSH Key

9. To get the public key and enter it into the dialog box, do the following:
   a. Select and copy the public key from the Event Source by running: **cat ~/.ssh/id_rsa.pub**
   b. Paste the public key in the **Eventsource SSH Key** field.
10. Click **OK**.

You need to restart file collection for your changes to take effect.

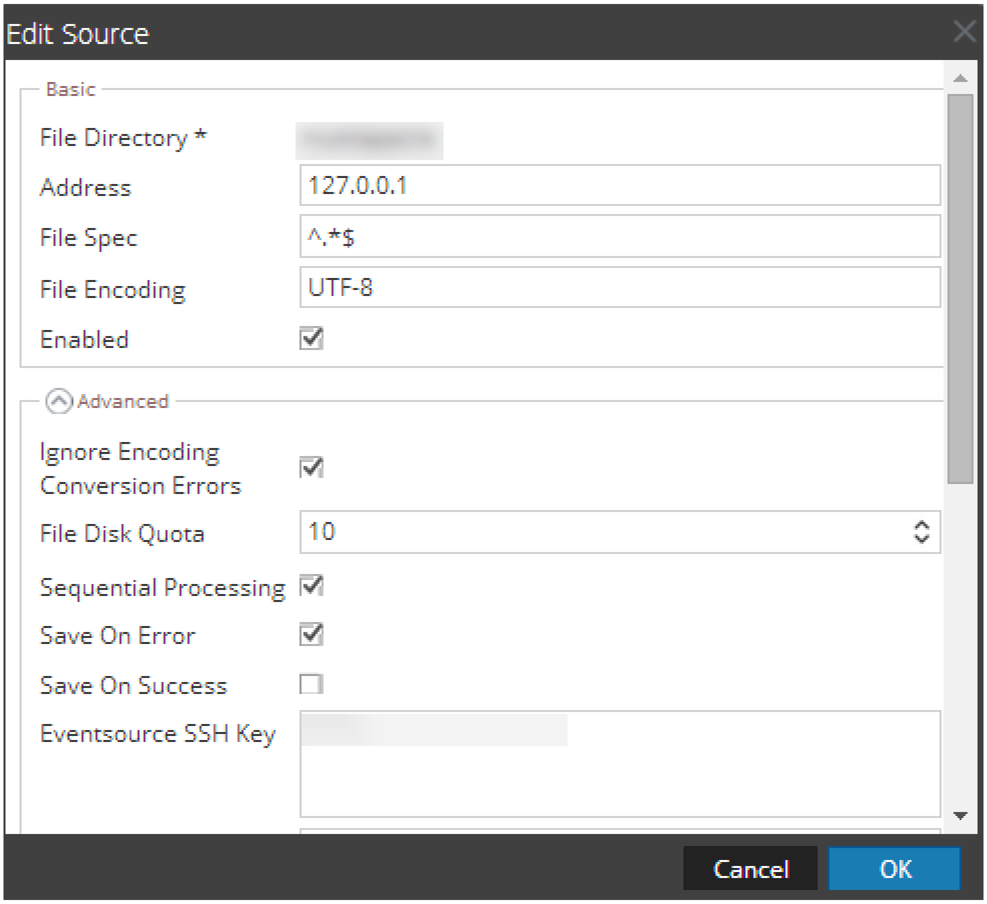
Stop and Restart File Collection

After you add a new event source that uses file collection, you must stop and restart the Security Analytics File Collection service. This is necessary to add the key to the new event source.

Modify File Collection for Event Source in Security Analytics

To modify an event source:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Log Collector Event Sources** tab, select **File/Config** from the drop-down menu.
5. Select an event source type (for example, **emc_symmetrix**) from the **Event Categories** panel and click **OK**.
6. In the **Sources** panel, select an event source and click ✎.
   The **Edit Source** dialog is displayed.
7. Modify the parameters that require changes and click **OK**.



Edit Source

Basic

File Directory *

Address: 127.0.0.1

File Spec: ^.*$

File Encoding: UTF-8

Enabled ☑

Advanced

Ignore Encoding Conversion Errors ☑

File Disk Quota: 10

Sequential Processing ☑

Save On Error ☑

Save On Success ☐

Eventsource SSH Key

8. Security Analytics applies the parameter changes to the selected event source.

Parameters

File Collection: Configuration Parameters

Create Custom Typespec for File Collection

This topic tells you how to create a custom typespec for the Log Collector. The topic includes:

- Create Custom typespec procedure
- File Collection typespec syntax
- Sample typespec files

Create Custom Typespec File

To create a custom typespec file:

1. Open an SFTP client (for example, WinSCP) and connect to a Log Collector or remote Log Collector.
2. Navigate to **/etc/netwitness/ng/logcollection/content/collection/file**, and copy an existing file, for example **apache.xml**.
3. Modify the file according to your requirements. See File Collection Typespec Syntax for details.
4. Rename and save the file to the same directory.
5. Restart the Log Collector.

> **Note:** You will not be able to see new Event Source type in Security Analytics until you restart the Log Collector.

File Collection Typespec Syntax

The following table describes the typespec parameters.

Parameter	Description
name	The display name of your File event source (for example, **apache**). Security Analytics displays this name in the **Sources** panel of the **View** > **Config** > **Events Sources** tab. Valid value is an alphanumeric string. You cannot use - (dashes), _(underscores), or spaces . The name must be unique across all typespec files in the folder.
type	Event source type: **file**. Do not modify this line.

Parameter	Description
prettyName	User-defined name for the event source. You can use the same value as name (for example, apache) or use a more descriptive name.
version	Version of this typespec file. Default value is 1.0.
author	Person who created the typespec file. Replace author-name with your name.
description	Formal description of the event source. Replace formal-description with your description of the event source.
	<device> Section
parser	**This *optional* parameter applies to Security Analytics 10.6.1 and newer.** This parameter contains the name of the log parser. This value forces the Log Decoder to use the specified log parser when parsing logs from this event source. **Note:** Please leave the field blank when unsure of the log parser to be used.
name	Name of your File event source (for example, apache).
	<collection><file> Section
parserId	Reserved for future use.
processorType	Examples of a processor-type are generic, xml, tagvalmap, and oracle. Processor types are similar to handlers in RSA enVision. **Note:** If the processorType is XML, the typespec file contains an <eventGroups> section, described below.
dataStartLine	The line number in the log file at which Security Analytics starts collecting events. Default value is 1.

Parameter	Description
fieldDelim	Specify the delimiter that separates the fields in the log file being parsed. Specify any of the following values: • || (piping) • ^ (caret) • **,** (comma) • **:** (colon) • **0x20** (to represent a space)
idField	Msg ID (message ID) field number. For example, specify 6 to identify the sixth field from the space-delimited event as the Msg ID.
lineDelim	Line delimiter that detects the end of an event. For example, specify **\n** to provide values for CR and LF.
File collection uses the following tags during event transformation.	
transformType	Transform type. Example of a transform-type is **ias**. The Internet Authentication Service (IAS) allows you to parse IAS logs when **transformType = ias** and **ProcessorType = generic**.
transformPrefixTag	Inserts the specified prefix in front of the transformed event. For example, if you specify APACHE, Security Analytics inserts %APACHE as the prefix.
transformReplaceFieldDelim	Specifies whether or not to replace the delimiter during transformation. Values: • **0** (default): do not replace • **1**: replace
	Specifies whether or not to add the prefix to the filename during transformation. Values: • **0** (default): do not add • **1**: add

Parameter	Description
transformMultipleDelimiterAsOne	Specifies whether or not to combine multiple sequential delimiters as one. Values: • **0** do not combine • **1** (default): combine
transformReplacementFieldDelim	Replace raw field delimiters with the given values with the specified values, if the **transformReplaceFieldDelim** flag = 1.

Entries in the `<eventGroups><eventGroup>` section:

- **globalInfo**: The globalInfo xpath. Reads parent node information and adds it to each level.
- **eventXPath**: xpath of events.

Sample File Collection Typespec Files

The following sample is the typespec file for the CA ACF2 event source.

```
<?xml version="1.0" encoding="UTF-8"?>
<typespec>

   <name>acf2tvm</name>
   <type>file</type>
   <prettyName>ibmacf2</prettyName>
   <version>1.0</version>
   <author>administrator</author>
   <description>File Collection specification for event source
      type "CA ACF2" using file handler type "ACF2TVM"
   </description>

   <device>
      <name>ibmacf2</name>
      <parser>ibmacf2</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <file>
         <parserId>file.acf2tvm</parserId>
         <processorType>generic</processorType>
         <dataStartLine>1</dataStartLine>
         <fieldDelim>|</fieldDelim>
         <idField></idField>
         <lineDelim>0x0a</lineDelim>
         <transformPrefixTag>ACF2TVM</transformPrefixTag>
         <transformReplaceFieldDelim>0</transformReplaceFieldDelim>
         <transformPrefixFilename>0</transformPrefixFilename>
         <transformMultipleDelimiterAsOne>0</transformMultipleDelimiterAsOne>
         <transformReplacementFieldDelim></transformReplacementFieldDelim>
      </file>
   </collection>
</typespec>
```

The following sample is the typespec file for the Tripwire Enterprise event source. Note that this file contains an `<eventGroups>` section (because the `<processorType>` value is XML).

```
<?xml version="1.0" encoding="UTF-8"?>
<typespec>
   <name>tripwire</name>
   <type>file</type>
   <prettyName>tripwire</prettyName>
   <version>1.0</version>
   <author>administrator</author>
   <description>FileCollection specification for eventsource type
   "Tripwire Enterprise" using file handler type "tripwire"
   </description>
   <device>
      <name>tripwire</name>
      <parser>tripwire</parser>
   </device>
   <configuration>
   </configuration>
   <collection>
      <file>
         <parserId>file.tripwire</parserId>
         <processorType>xml</processorType>
         <eventXPath></eventXPath>
         <eventGroups>
          <eventGroup>
          <globalInfo> //ReportHead/Report[@type!='systemlog_
rpt']/../../ReportBody/ReportSection/@name |
             //ReportHead/Report[@type!='systemlog_
rpt']/../../ReportBody/ReportSection/ReportSection/@name |
             //ReportHead/Report[@type!='systemlog_
rpt']/../../ReportBody/ReportSection/ReportSection/ReportSection/@name |
             //ReportHead/Report[@type!='systemlog_
rpt']/../../ReportBody/ReportSection/String |
             //ReportHead/Report[@type!='systemlog_
rpt']/../../ReportBody/ReportSection/ReportSection/String
          </globalInfo>
          <eventXPath>
         //ReportHead/Report[@type!='systemlog_
rpt']/../../ReportBody/ReportSection/ReportSection/ReportSection/ReportSection
          </eventXPath>
       </eventGroup>
       <eventGroup>
          <globalInfo></globalInfo>
          <eventXPath>
         //ReportHead/Report[@type='systemlog_
rpt']/../../ReportBody/ReportSection/ReportSection/*
          </eventXPath>
       </eventGroup>
        </eventGroups>
        <dataStartLine></dataStartLine>
        <fieldDelim></fieldDelim>
        <idField></idField>
        <lineDelim>\n</lineDelim>
        <transformPrefixTag></transformPrefixTag>
        <transformReplaceFieldDelim>0</transformReplaceFieldDelim>
        <transformPrefixFilename>0</transformPrefixFilename>
        <transformMultipleDelimiterAsOne>0</transformMultipleDelimiterAsOne>
        <transformReplacementFieldDelim></transformReplacementFieldDelim>
      </file>
   </collection>
</typespec>
```

Step 2. Configure File Event Sources to Send Events to Security Analytics

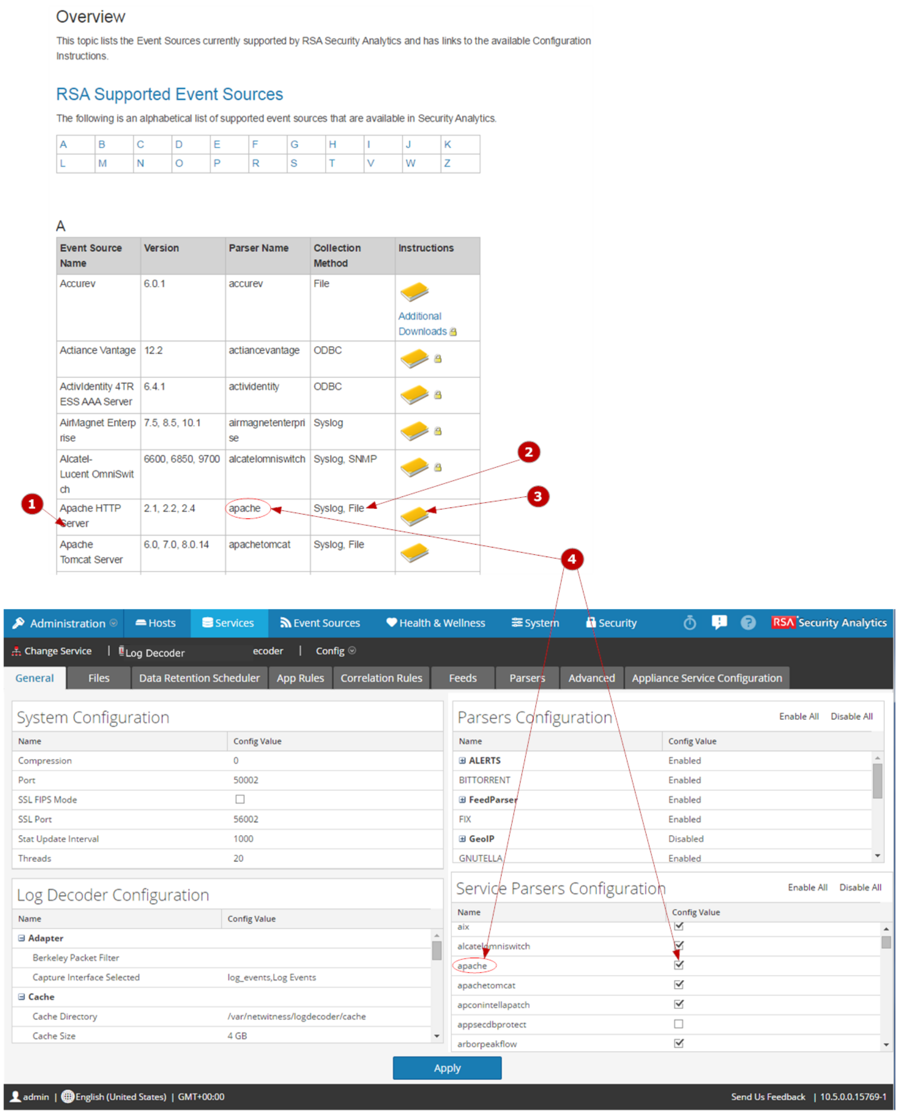
This topic tells you where to find the event sources currently supported for File collection and the available configuration instructions for each event source

The list of RSA Supported Event Sources is an alphabetized of all the event sources currently supported by Security Analytics that identifies which event sources you can use with File Collection.

Return to Procedures

Procedure

To verify that the event sources are correctly configured:



Overview

This topic lists the Event Sources currently supported by RSA Security Analytics and has links to the available Configuration Instructions.

RSA Supported Event Sources

The following is an alphabetical list of supported event sources that are available in Security Analytics.

A	B	C	D	E	F	G	H	I	J	K
L	M	N	O	P	R	S	T	V	W	Z

A

Event Source Name	Version	Parser Name	Collection Method	Instructions
Accurev	6.0.1	accurev	File	📒 Additional Downloads 🔒
Actiance Vantage	12.2	actiancevantage	ODBC	📒 🔒
ActivIdentity 4TR ESS AAA Server	6.4.1	actividentity	ODBC	📒 🔒
AirMagnet Enterprise	7.5, 8.5, 10.1	airmagnetenterprise	Syslog	📒 🔒
Alcatel-Lucent OmniSwitch	6600, 6850, 9700	alcatelomniswitch	Syslog, SNMP	📒 🔒
Apache HTTP Server	2.1, 2.2, 2.4	apache	Syslog, File	📒
Apache Tomcat Server	6.0, 7.0, 8.0.14	apachetomcat	Syslog, File	📒

System Configuration

Name	Config Value
Compression	0
Port	50002
SSL FIPS Mode	□
SSL Port	56002
Stat Update Interval	1000
Threads	20

Parsers Configuration

Name	Config Value
⊞ ALERTS	Enabled
BITTORRENT	Enabled
⊞ FeedParser	Enabled
FIX	Enabled
⊞ GeoIP	Disabled
GNUTELLA	Enabled

Log Decoder Configuration

Name	Config Value
⊟ Adapter	
Berkeley Packet Filter	
Capture Interface Selected	log_events,Log Events
⊟ Cache	
Cache Directory	/var/netwitness/logdecoder/cache
Cache Size	4 GB

Service Parsers Configuration

Name	Config Value
aix	☑
alcatelomniswitch	☑
apache	☑
apachetomcat	☑
apconintellapatch	☑
appsecdbprotect	□
arborpeakflow	☑

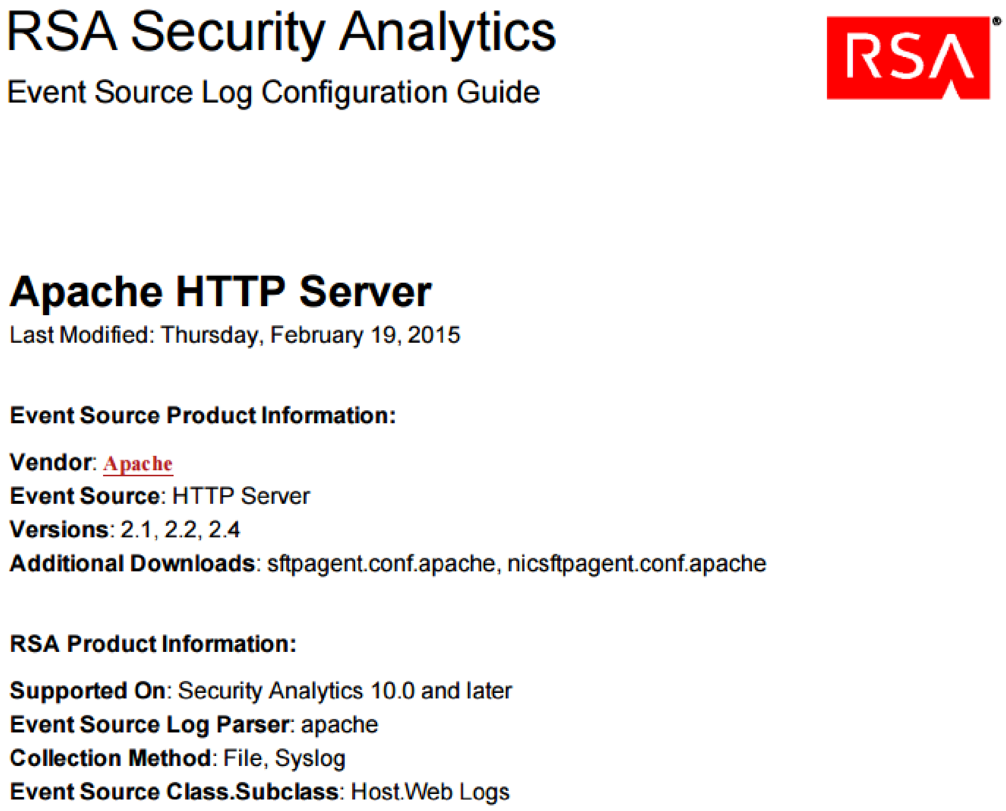
1 Find the name of the event source.

2 Verify that it is supported by **File Collection Protocol** 3 Click on 📒 to display the configuration instructions for the event source.

4 Verify that you downloaded the correct parser (for example, apache) from LIVE to the Log Decoder and enabled it.

Sample Configuration Instructions

The following illustration is taken from the Apache HTTP Server configuration instructions.



RSA Security Analytics

Event Source Log Configuration Guide

Apache HTTP Server

Last Modified: Thursday, February 19, 2015

Event Source Product Information:

Vendor: Apache
Event Source: HTTP Server
Versions: 2.1, 2.2, 2.4
Additional Downloads: sftpagent.conf.apache, nicsftpagent.conf.apache

RSA Product Information:

Supported On: Security Analytics 10.0 and later
Event Source Log Parser: apache
Collection Method: File, Syslog
Event Source Class.Subclass: Host.Web Logs

Step 3. Start Service for Configured File Collection Protocol

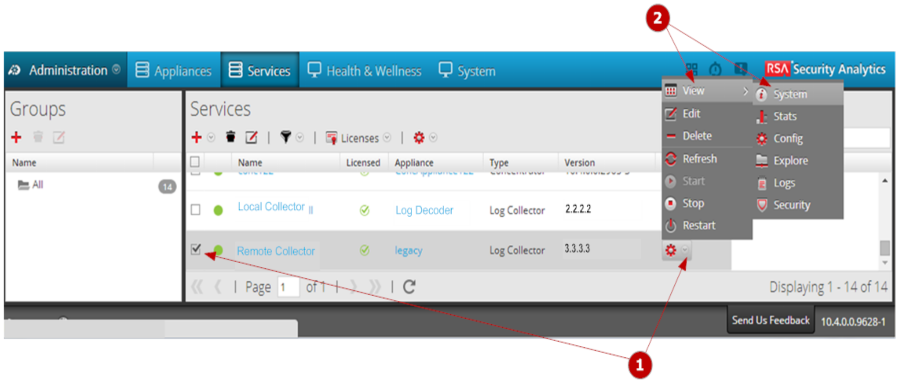
This topic tells you how to start a stopped File collection service.

If a File collection service has stopped, you may need to start it again.

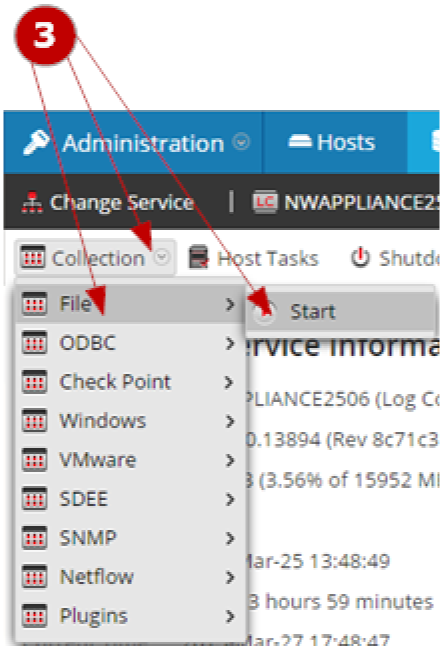
Return to Procedures

Procedure

The following figure shows you how to start a collection service. See the **Enable Automatic Start of Individual Services** topic in the *Log Collection Configuration Guide* if you want the service to start automatically.



Name	Licensed	Appliance	Type	Version
Local Collector	✓	Log Decoder	Log Collector	2.2.2.2
Remote Collector	✓	legacy	Log Collector	3.3.3.3



1 Select a Log Collector service and click ⚙ ⌄ under **Actions**.

2 Click **View** > **System**.

3 Click **Collection** > **File**, and click **Start**.

Step 4. Verify That File Collection Is Working

This topic tells you what to check in Security Analytics to verify that you have configured File Collection correctly.

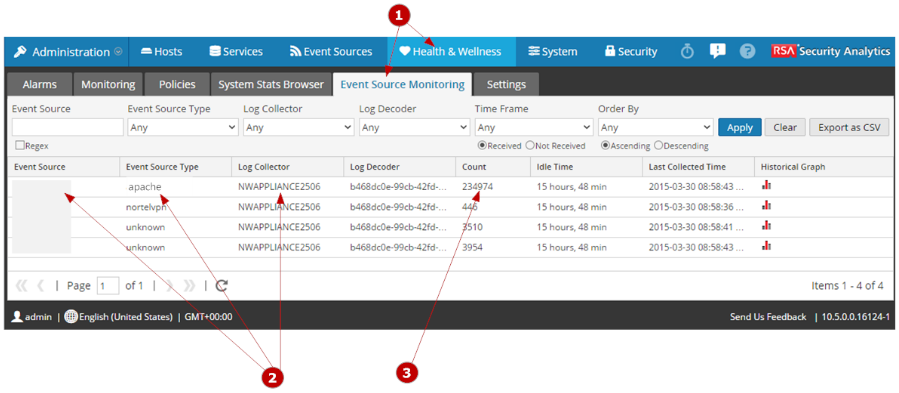
Return to Procedures

Context

You need to verify that File Collection has been configured correctly, in order to ensure that it works.

Procedure

The following figure illustrates how you can verify that File collection is working from the **Administration > Health & Wellness > Event Source Monitoring** tab.



Event Source:
Event Source Type: Any
Log Collector: Any
Log Decoder: Any
Time Frame: Any
Order By: Any
□ Regex
● Received ○ Not Received
● Ascending ○ Descending

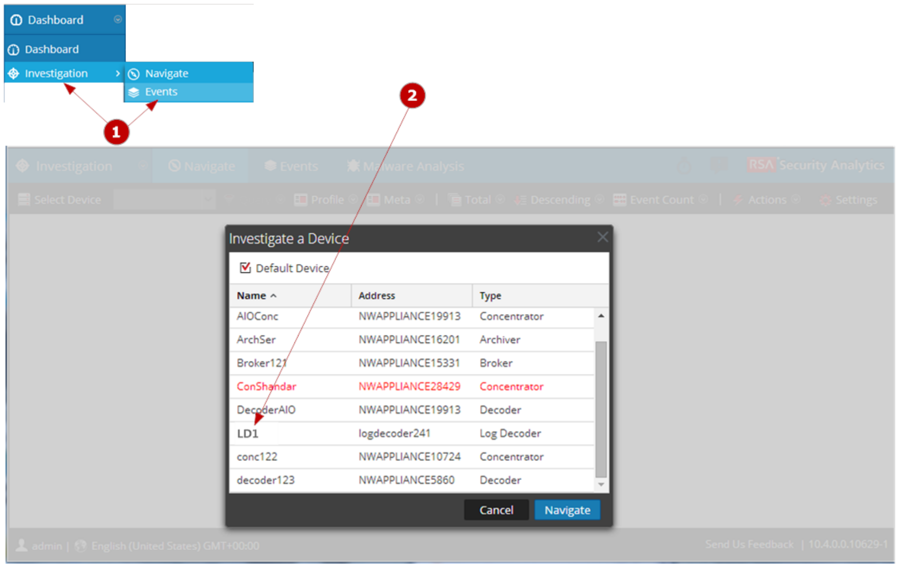
Event Source	Event Source Type	Log Collector	Log Decoder	Count	Idle Time	Last Collected Time	Historical Graph
	apache	NWAPPLIANCE2506	b468dc0e-99cb-42fd-...	234974	15 hours, 48 min	2015-03-30 08:58:43 ...	
	nortelvpn	NWAPPLIANCE2506	b468dc0e-99cb-42fd-...	446	15 hours, 48 min	2015-03-30 08:58:36 ...	
	unknown	NWAPPLIANCE2506	b468dc0e-99cb-42fd-...	3510	15 hours, 48 min	2015-03-30 08:58:41 ...	
	unknown	NWAPPLIANCE2506	b468dc0e-99cb-42fd-...	3954	15 hours, 48 min	2015-03-30 08:58:43 ...	

1 Access the **Event Source Monitoring** tab from the **Administration > Health & Wellness** view.

2 Find the Log Decoder, Event Source, and Event Source Type (for example, **apache**).

3 Look for activity in the **Count** column to verify that File collection is accepting events.

The following figure illustrates how you can verify that File collection is working from the **Investigation> Events >** view.



Investigate a Device

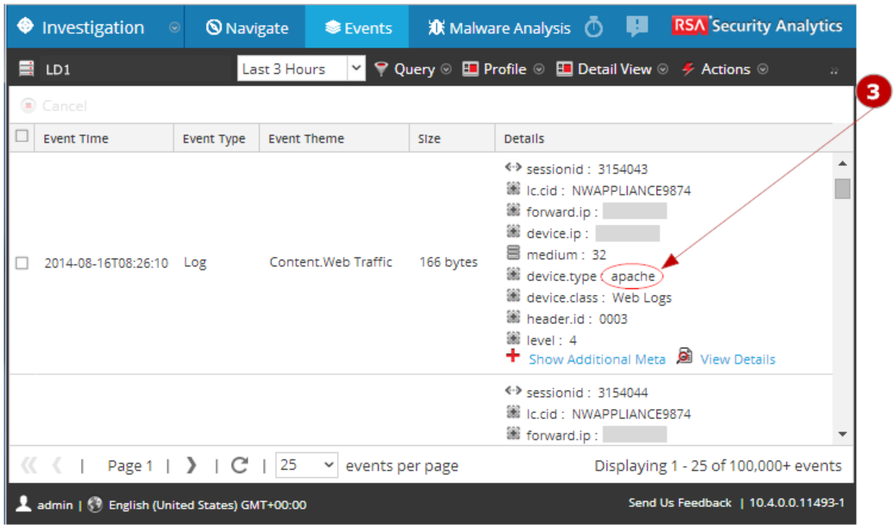
☑ Default Device

Name ^	Address	Type
AIOConc	NWAPPLIANCE19913	Concentrator
ArchSer	NWAPPLIANCE16201	Archiver
Broker121	NWAPPLIANCE15331	Broker
ConShandar	NWAPPLIANCE28429	Concentrator
DecoderAIO	NWAPPLIANCE19913	Decoder
LD1	logdecoder241	Log Decoder
conc122	NWAPPLIANCE10724	Concentrator
decoder123	NWAPPLIANCE5860	Decoder

Cancel Navigate

1. Access the **Investigation > Events** view.

2. Select the Log Decoder (for example, **LD1**) collecting File events in the **Investigate a Device** dialog.



□	Event Time	Event Type	Event Theme	Size	Details
□	2014-08-16T08:26:10	Log	Content.Web Traffic	166 bytes	sessionid : 3154043 lc.cid : NWAPPLIANCE9874 forward.ip : [redacted] device.ip : [redacted] medium : 32 device.type : apache device.class : Web Logs header.id : 0003 level : 4 Show Additional Meta View Details
					sessionid : 3154044 lc.cid : NWAPPLIANCE9874 forward.ip : [redacted]

Page 1 | 25 events per page Displaying 1 - 25 of 100,000+ events

3. Look for a File event source parser (for example, **apache**) in the **Device Type** column to verify that File collection is accepting events.

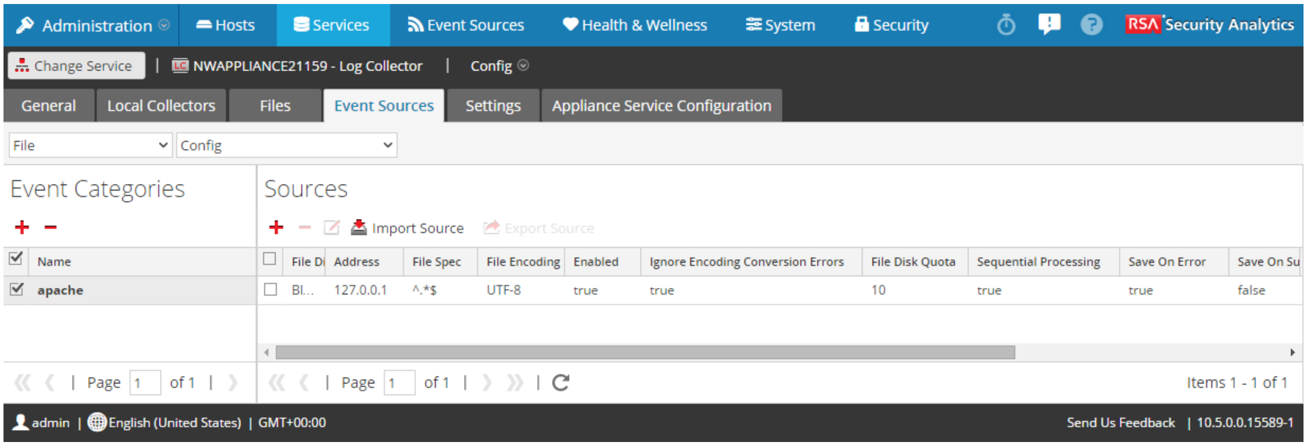
File Collection: Configuration Parameters

This topic describes the user interface for configuring File Collection.

Use this section when you are looking for descriptions of the File Collection user interface and definitions of the features of the user interface.

To access the File Collection Configuration Parameters:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ ⌄ under **Actions** and select **View** > **Config**.
4. In the **Log Collector Event Sources** tab, select **File/Config** from the drop-down menu.



☑	Name
☑	apache

□	File Di	Address	File Spec	File Encoding	Enabled	Ignore Encoding Conversion Errors	File Disk Quota	Sequential Processing	Save On Error	Save On Su
□	Bl...	127.0.0.1	^.*$	UTF-8	true	true	10	true	true	false

The File/Config view in the Event Sources tab has two panels: Event Categories and Sources.

Event Categories Panel

In the Event Categories panel, you can add or delete the appropriate event source types.

Feature	Description
+	Displays the Available Event Source Types dialog from which you select the event source type for which you want to define parameters.
−	Deletes the selected event source types from the Event Categories panel.
□	Selects event source types.
Name	Displays the name of the event source types that you have added.

Available Event Sources Types Dialog

The Available Event Source Types dialog displays the list of supported event source types.

Feature	Description
□	Selects the event source type that you want to add.
Type	Display the event source types that are available to add.
Cancel	Closes the dialog without adding an event source type.
OK	Adds the selected event source type to the Event Categories panel.

Note: The Available Event Source Types dialog displays the list of supported event source types downloaded from the Generic File Reader Type Specification (GFTS) file. If you do not see any event source types in this list, you did not load the content available with Log Collector upgrade to this release.

Sources Panel

Use this panel to review, add, modify, and delete event source file directories and their parameters for the event source type you selected in the Event Categories panel.

Toolbar

The following table provides descriptions of the toolbar options.

Feature	Description
+	Displays the Add Source dialog in which you define the parameters for a Firewall host.
−	Deletes the host that you selected.
✎	Opens the Edit Source dialog, in which you edit the parameters for the selected event source. Select multiple event sources and click ✎ to open the Bulk Edit Source dialog in which you can edit the parameters values for the selected event sources. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.

Feature	Description
Import Source	Opens the Bulk Add Option dialog in which you can import hosts in bulk from a comma-separated values (CSV) file. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.
Export Source	Creates a .csv file that contains the parameters for the selected hosts. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.

Add or Modify Source Dialog

In this dialog, you add or modify a file directory for the selected event source.

Feature	Description
Netflow Source Parameters	Lists the Netflow event source parameters populated with the default values. Enter or modify the appropriate values.
Cancel	Closes the dialog without adding a file directory or saving the parameter values for the selected file directory.
OK	In the Add Source dialog, adds the file directory and its parameters. In the Edit Source dialog, applies the parameter value changes for the selected file directory.

File Directory Parameters

The following table provides descriptions of the source parameters.

Name	Description
Basic	

Name	Description
File Directory*	Collection directory (for example, **Eur_London100**) into which the File event source places its files. Valid value is a character string that is conforms to the following regular expression: **[_a-zA-Z][_a-zA-Z0-9]*** This means that the file directory must start with a letter followed by numbers, letters, and underscores. Do not modify this parameter after you start collecting event data. After you create the collection, the Log Collector creates the work, save, and error sub-directories under the collection directory.
Address*	IP address of the event source. Valid value is an **IPv4 address**, **IPv6 address**, or a **hostname** including a fully-qualified domain name.
File Spec	Regular expression. For example, **^.*$** = process everything.
File Encoding	Internationalization file encoding. Enter the File Encoding method, the following strings are examples of valid methods: • UTF-8 (default) • UCS-16LE • UCS-16BE • UCS-32LE • UCS-32BE • SHIFT-JIS • EBCDIC-US
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
Advanced	
Ignore Encoding Conversion Errors	Select the check box to ignore encoding conversion errors and ignore invalid data. The check box is selected by default. **Caution:** This may cause parsing and transformation errors.

Name	Description
File Disk Quota	Determines when to stop saving files regardless of the **Save On Error** and **Save On Success** parameter settings. For example, a value of 10 indicates that when there is less than 10% available disk left, the Log Collector stops saving files to reserve enough space for your estimated normal collection processing. **Caution:** Available disk refers to a partition where the base collection directory is mounted. If the Log Decoder server has a 10TB disk size and 2TB is allocated to base collection directory, then setting this value to 10 causes log collection to stop when less than 0.2TB (10% of 2TB) of space is left. It does not mean 10% of 10TB. Valid value is a number in the **0** to **100** range. **10** is the default.
Sequential Processing	Sequential processing flag: • Select the check box (default) to process event source files in collection order. • Do not select the checkbox to process event source files in parallel.
Save On Error	Save on error flag. Check the checkbox to retain the **eventsource collection** file when the Log Collector it encounters an error. The check box is selected by default.
Save On Success	Save **eventsource collection** file after processing flag. Select to save the event-source collection file after processing it. The check box is not selected by default.
Eventsource SSH Key	SSH public key used to upload files for this event source. Please refer to Generate Key Pair on Event Source and Import Public Key to Log Collector for instructions on generating keys. **Note:** If File collection is stopped, Security Analytics does not update the authorized_keys file with the SSH public key that you add or modify in this parameter. You must restart File collection to update the public key. You can add or modify the value of the public key in this parameter in multiple File event sources without File collection running, but Security Analytics will not update the **authorized_keys** file until File collection is restarted.

Name	Description
Manage Error Files	By default, the Log Collector uses the **File Disk Quota** parameter to ensure that the disk does not fill up with error files. If you set this parameter to **true**, you can specify one of these: • Maximum space allotted to error files in the **Error Files Size** parameter. • Maximum number of error files allowed in **Error Files Count** parameter. A reduction percent is also specified, which tells the system how much to reduce when the maximum is reached. Select the check box to manage error files. The check box is not selected by default.
Error Files Size	Only valid if the **Manage Error Files** and **Save On Error** parameters are set to true. Specifies to what extent Security Analytics saves error files. The value that you specify is the maximum total size of all the files in the error directory. Valid value is a number in **0** to **281474976710655** range. You specify these values in either **Kilobytes**, **Megabytes**, or **Gigabytes**. **100 Megabytes** is the default. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.
Error Files Count	Only valid if the **Manage Error Files** and **Save On Error** parameters are set to true. Maximum number of error files allowed in the error directory. Valid value is a number in **0** to **65536** range. **65536** is the default. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.
Error Files Reduction %	Percent amount by size or count of the error files that the Log Collector service removes when the maximum size or count has been reached. The service removes the oldest files first. Valid value is a number in the **0** to **100** range. **10** is the default.

Name	Description
Manage Saved Files	Select the check box to manage saved files. The check box is not selected by default. By default, the Log Collector uses the **File Disk Quota** parameter to ensure that the disk does not fill up with saved files. If check this check box, you can specify one of these: • Maximum space allotted to saved files in the **Saved Files Size** parameter. • Maximum number of saved files allowed in **Saved Files Count** parameter. A reduction percent is also specified, which tells the system how much to reduce when the maximum is reached.
Saved Files Size	Only valid if the **Manage Saved Files** and **Save On Success** parameters are set to true. Maximum total size of all the files in the save directory. Valid value is a number in the **0** to **281474976710655** range. You specify these values in either **Kilobytes**, **Megabytes**, or **Gigabytes**. **100 Megabytes** is the default. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.
Saved Files Count	Only valid if the **Manage Saved Files** and **Save On Success** parameters are set to true. Maximum number of saved files in the save directory. Valid value is a number in **0** to **65536** range. **65536** is the default. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.
Saved File Reduction %	Percent amount by size or count of the saved files that the Log Collector service removes when the maximum size or count has been reached. The service removes the oldest files first. Valid value is a number in the **0** to **100** range. **10** is the default.

Name	Description
Debug	**Caution:** Only enable debugging (set this parameter to **On** or **Verbose**) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables/disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
Cancel	Closes the dialog without making adding an event source type.
OK	Adds the parameters for the event source.

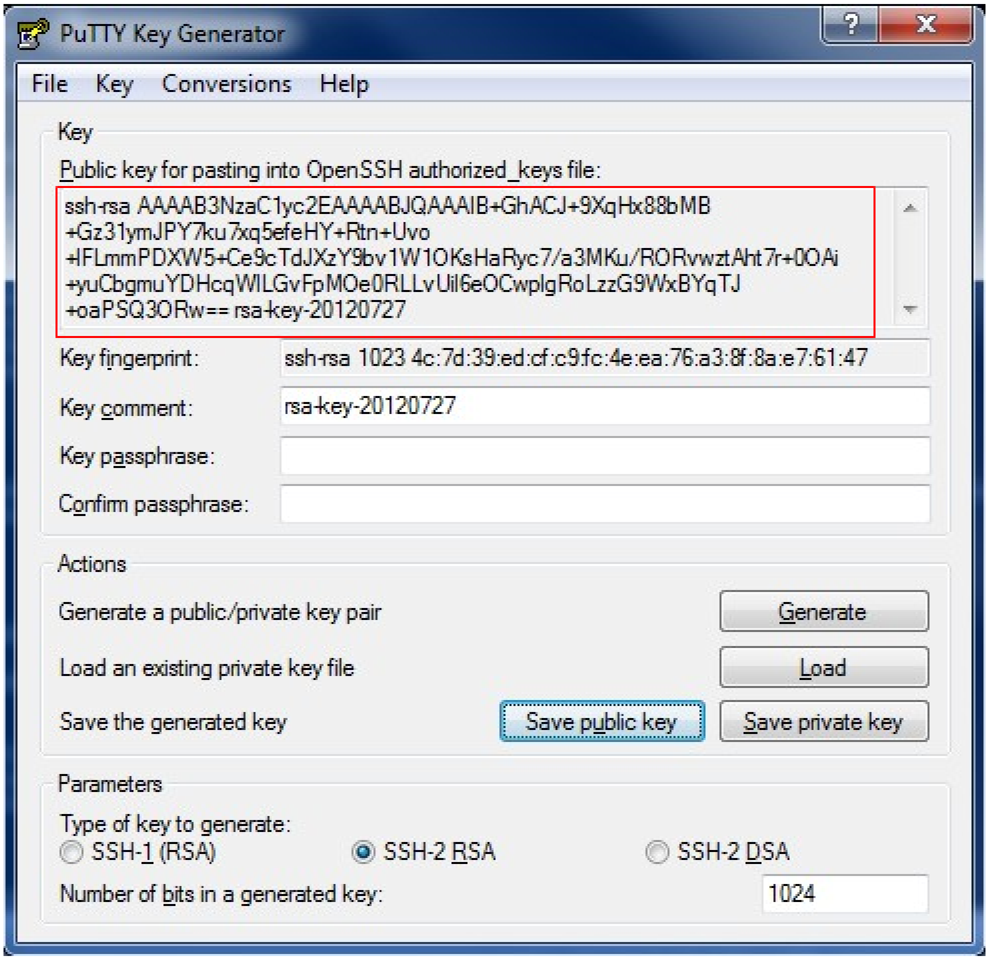
Generate Key Pair on Event Source and Import Public Key to Log Collector

To generate the key pair on the event source and import the public key to Log Collector:

1. Double-click **puttygen.exe** in the **C:\sasftpagent** directory. The PuTTY Key Generator starts.
2. Select **SSH2 RSA** as the type of key to generate.
3. Click **Generate** and move the mouse in the PuTTY Key Generator window until the key is generated.
4. Save the private key:
   a. Click **Save private key**.
   b. Select **Yes** to not use a passphrase.
   c. Save the file as **private.ppk** in the **C:\sasftpagent** directory.
5. Add the public key to the Log Collector:

a. Copy the public key into your buffer so that you can paste it into the parameter in Security Analytics as described in step 5b.

In the following example, the public key is enclosed in a red box.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAIB+GhACJ+9XqHx88bMB
+Gz31ymJPY7ku7xq5efeHY+Rtn+Uvo
+IFLmmPDXW5+Ce9cTdJXzY9bv1W1OKsHaRyc7/a3MKu/RORvwztAht7r+0OAi
+yuCbgmuYDHcqWILGvFpMOe0RLLvUil6eOCwplgRoLzzG9WxBYqTJ
+oaPSQ3ORw== rsa-key-20120727
```

Key fingerprint: ssh-rsa 1023 4c:7d:39:ed:cf:c9:fc:4e:ea:76:a3:8f:8a:e7:61:47

Key comment: rsa-key-20120727

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 1024

b. Paste the public key from your buffer into the Eventsource SSH Key parameter in Security Analytics. For details, see the **Configure File Event Sources** topic in the *RSA Security Analytics Log Collection Guide*.

6. Close the **puttygen**.

Tasks:

Step 1. Configure File Event Sources in Security Analytics

Step 2. Configure File Event Sources to Send Events to Security Analytics

File Collection: Troubleshoot

Security Analytics informs you of Log Collector problems or potential problems in the following two ways.

- Log files.
- Health and Wellness Monitoring views.

Log Files

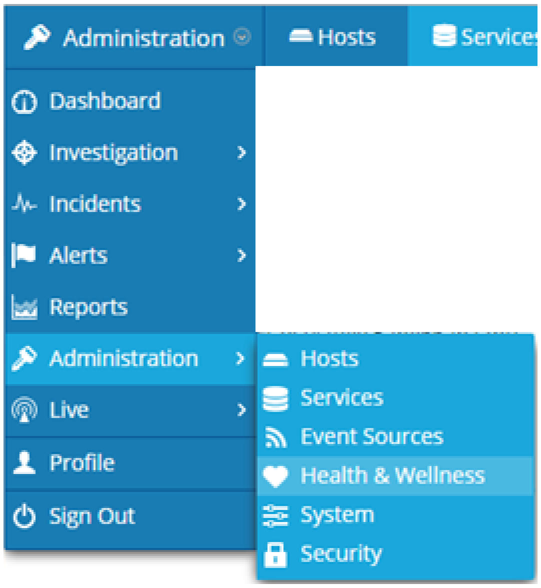
If you have an issue with a particular event source collection protocol, you can review debug log s to investigate this issue. Each event source has a Debug parameter that you can enable (set parameter to On or Verbose) to capture these logs.

Only enable debugging if you have a problem with this event source and you need to investigate this problem. If you have Debug enabled all the time it will adversely affect the performance of the Log Collector.

Security Analytics has a set of error messages associated with Log Collection that it includes in log files. To access these files:

Health and Wellness Monitoring

Health and Wellness monitoring makes you aware of potential hardware and software problems in a timely manner so that you can avoid to outages. RSA recommends that you monitor the Log Collector statistical fields to make sure that the service is operating efficiently and is not at or near the maximum values you have configured. You can monitor the following statistics (Stats) described in the **Administration** > **Health & Wellness** view.



Netflow Collection Configuration Guide

This guide tells you how to configure the Netflow collection protocol. This protocol collects events from Netflow v5 and Netflow v9.

You must deploy Log Collection before you can configure the Netflow collection protocol.

For deployment instructions, see Log Collection Deployment Guide.

The Basics

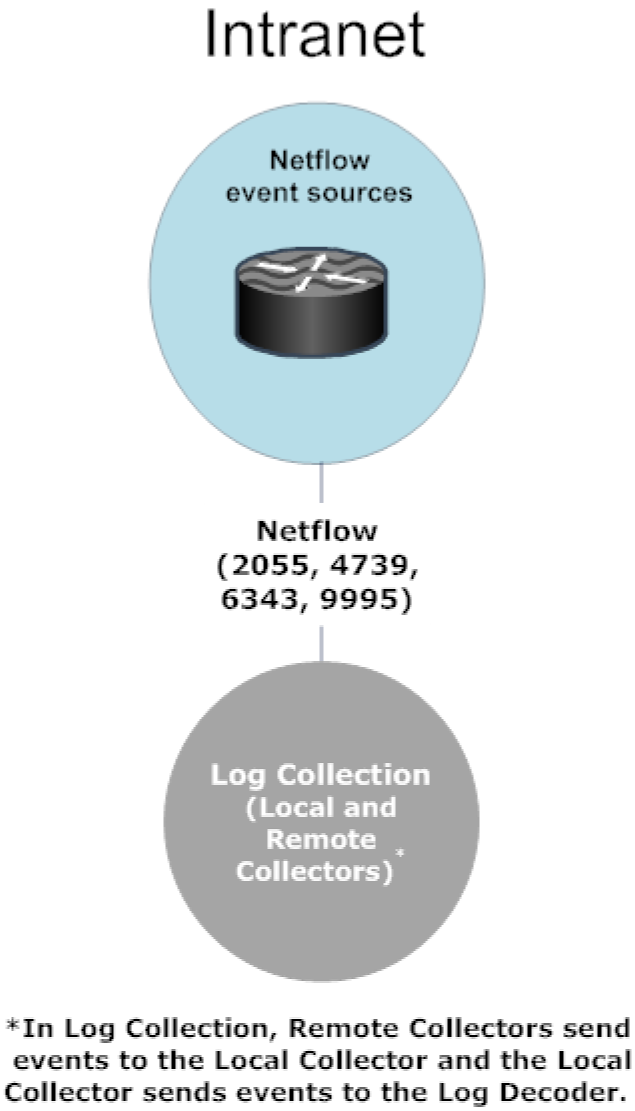
This guide tells you how to configure Netflow collection protocol which accepts events from Netflow v5 and Netflow v9. You use this protocol to accept events for security purposes, not for network performance purposes. This means that you should choose to accept events from select key strategic points in your network only (not everywhere).

How Netflow Collection Works

The Log Collector service collects events from Netflow v5 and Netflow v9.

Deployment Scenario

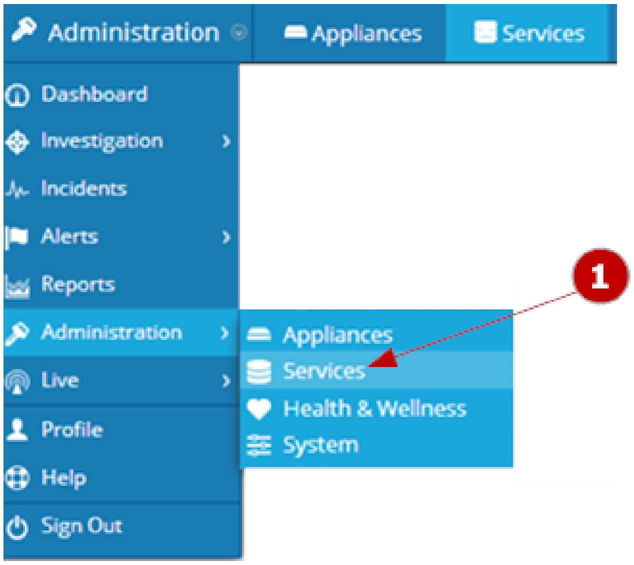
The following figure illustrates how you deploy the Netflow Collection Protocol in Security Analytics.


Intranet
Netflow event sources
Netflow (2055, 4739, 6343, 9995)
Log Collection (Local and Remote Collectors)*
*In Log Collection, Remote Collectors send events to the Local Collector and the Local Collector sends events to the Log Decoder.

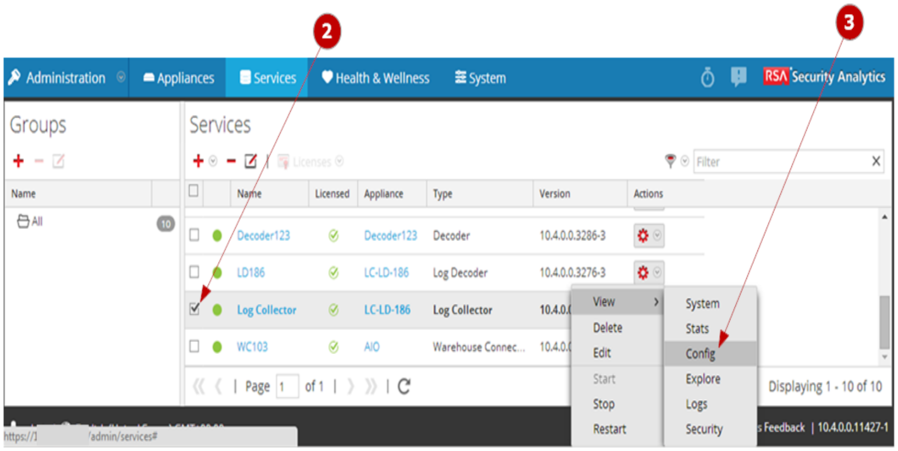
Configure Netflow Collection Protocol in Security Analytics

You configure to the Log Collector to use Netflow collection for an event source in the event Source tab of the Log Collector parameter view. The following figure the basic workflow for configuring an event source for Netflow Collection in Security Analytics. Please refer to:

- Step 1. Configure Netflow Event Sources in Security Analytics for step-by-step instructions on how to configure events sources in Security Analytics that use the Netflow Collection protocol.
- References - Netflow Collection Configuration Parameters for a detailed description of each Netflow Collection Protocol parameter.



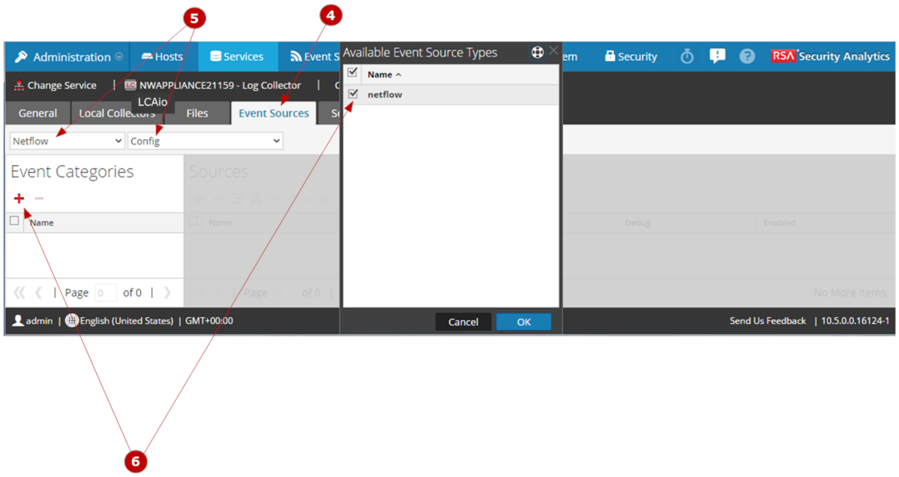
1 Access the **Services** view.



☐		Name	Licensed	Appliance	Type	Version	Actions
☐	●	Decoder123	✓	Decoder123	Decoder	10.4.0.0.3286-3	⚙
☐	●	LD186	✓	LC-LD-186	Log Decoder	10.4.0.0.3276-3	⚙
☑	●	Log Collector	✓	LC-LD-186	Log Collector	10.4.0.	
☐	●	WC103	✓	AIO	Warehouse Connec...	10.4.0.	

2 Select a **Log Collection** service.

3 Click ⌄ under **Actions** and select **View > Config** to display the **Log Collection Configuration Parameter** tabs.

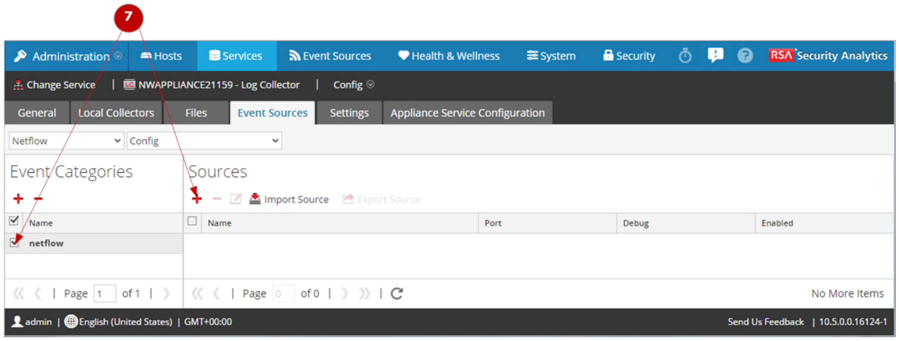


4 Click the **Event Sources** tab.

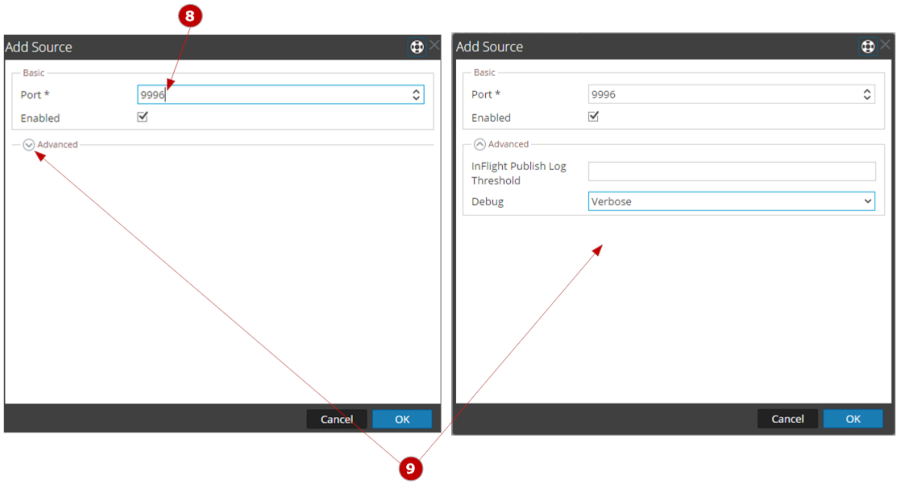
5 Select **Netflow** as the collection protocol and select **Config**.

6 Click + and select **netflow** as the event source category.

The event source category is part of the content you downloaded from LIVE.



7 Select **netflow** as the category and click +.



Add Source

Basic

Port * 9996

Enabled ☑

Advanced

Add Source

Basic

Port * 9996

Enabled ☑

Advanced

InFlight Publish Log Threshold

Debug Verbose

8 Specify the basic parameters required for the Netflow event source.

9 Click ⌄ and specify additional parameters that enhance how the Netflow protocol handles event collection for the event source.

Configure Event Sources to Use Netflow Collection Protocol

You need to configure each event source that uses the Netflow Collection protocol to communicate with Security Analytics (see Step 2. Configure Netflow Event Sources to Send Events to Security Analytics).

Procedures

This topic provides an overview of the end-to-end sequential configuration procedure for the Netflow Collection protocol with a checklist that contains each configuration step.

Configuration steps for the Netflow collection protocol must occur in the specific sequence listed in the table below.

Netflow Collection Configuration Checklist

Note: The steps in this list are in the order in which you must complete them.

Step	Description	√
1	Configure Netflow Event Sources in Security Analytics.	
2	Configure Netflow Event Sources to Send Events to Security Analytics.	
3	Start service for configured Netflow collection protocol.	
4	Verify that Netflow Collection is working.	

Step 1. Configure Netflow Event Sources in Security Analytics

This topic tells you how to configure Netflow event source sources for the Log Collector.

After completing this procedure, you will have...

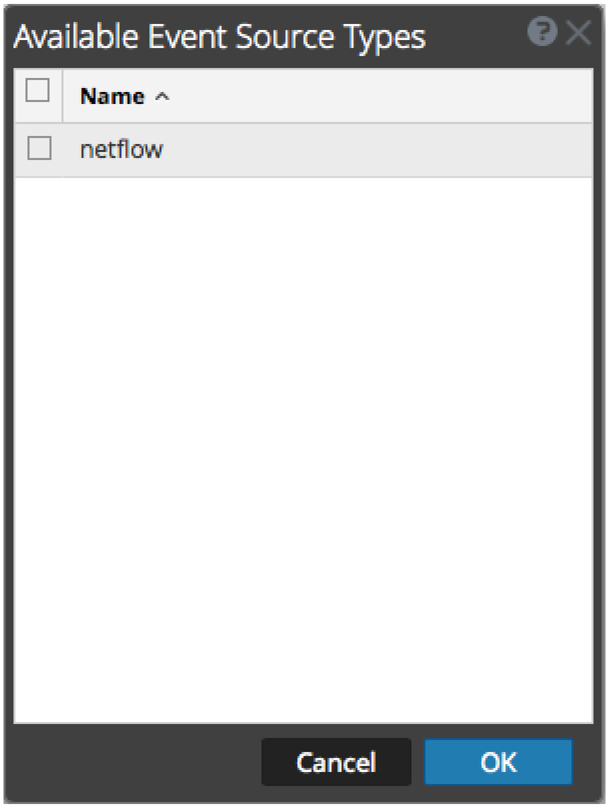
- Configured a Netflow event source.
- Modified a Netflow event source.

Return to Procedures

Procedures

Step 1. Configure Netflow Event Sources in Security Analytics

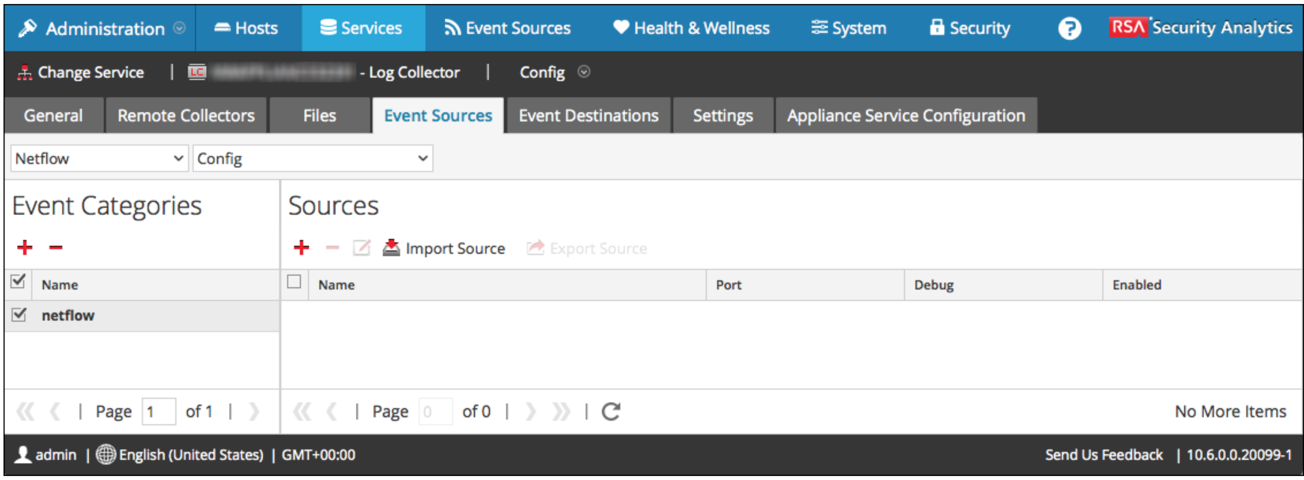
1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Log Collector Event Sources** tab, select **Netflow/Config** from the drop-down menus.
5. In the **Event Categories** panel toolbar, click **+**.



□	Name ^
□	netflow

6. Select an event source type (for example, netflow) and click **OK**.

   The newly added event source type is displayed in the **Event Categories** panel.

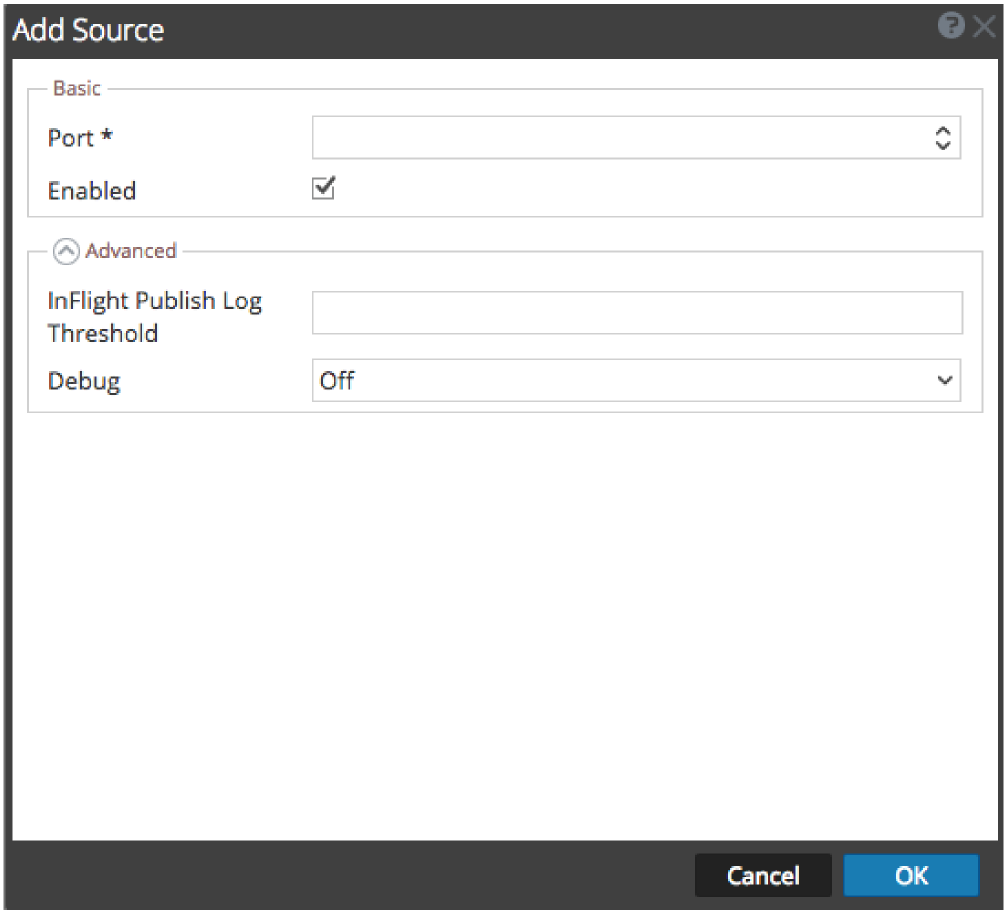


7. Select the new type in the **Event Categories** panel and click + in the **Sources** toolbar.

   The **Add Source** dialog is displayed.

8. Specify the port, modify any other parameters that require changes, and click **OK**.

   > **Note:** Security Analytics opens the 2055, 4739, 6343, and 9995 ports on the firewall by default. You can open other ports for Netflow if required.



Add Source

Basic

Port *

Enabled ☑

Advanced

InFlight Publish Log Threshold

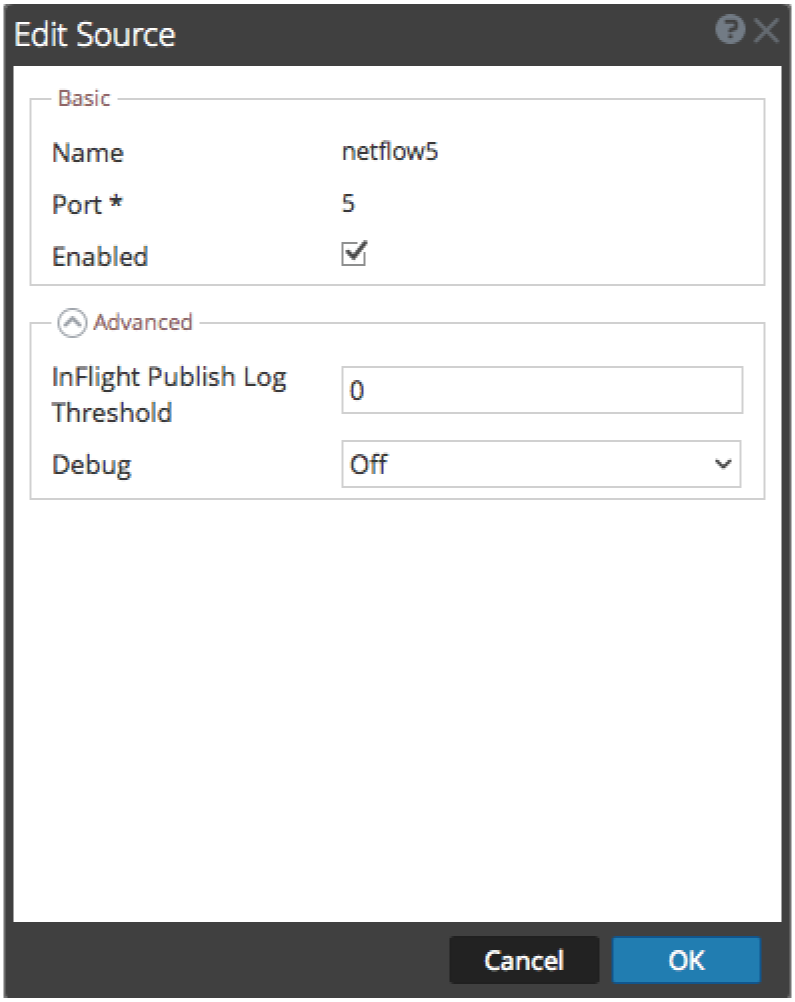
Debug: Off

The new event source is displayed in the list.

Modify a Netflow Event Source

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Log Collector Event Sources** tab, select **Netflow/Config** from the drop-down menu.
5. Select **netflow** for the event source type from the **Event Categories** panel and click **OK**.
6. In the **Sources** panel, select an event source and click ✎.

   The **Edit Source** dialog is displayed.
7. Modify the parameters that require changes and click **OK**.



Edit Source

Basic

Name netflow5

Port * 5

Enabled ☑

Advanced

InFlight Publish Log Threshold 0

Debug Off

Security Analytics applies the parameter changes to the selected event source.

Parameters:

References - Netflow Collection Configuration Parameters

Step 2. Configure Netflow Event Sources to Send Events to Security Analytics

Download and configure the rsaflow or cef parser from Live.

Verify that you downloaded the rsaflow or cef parser from LIVE to the Log Decoder and enabled it.

Procedure

1. In the **Security Analytics** menu, go to **Administration** > **Services**.
2. Select a **Log Decoder** service and select ⚙ ⌄ > **View** > **Config**.

3. In the **General** tab, under the **Service Parsers Configuration** panel, verify that the **rsaflow** option is checked.

Step 3. Start Service for Configured Netflow Collection Protocol

This topic tells you how to start a stopped NetFlow collection service.

Return to Procedures

Context

This topic tells you how to start a collection service. See the *Log Collection Configuration Guide* topic **Enable Automatic Start of Individual Services** if you want the service to start automatically.

Procedure

To start a stopped Netflow collection service:

1. In the **Security Analytics** menu, go to **Administration > Services**.
2. Select a **Log Collector** and select ⚙ ⌄ > **View** > **System**.
3. Click **Collection** > **Netflow** > **Start**.

Step 4. Verify That Netflow Collection Is Working

This topic tells you what to check in Security Analytics to verify that you have configured Netflow Collection correctly.

Return to Procedures

Context

You can verify that Netflow collection is working from the Administration > Health & Wellness > Event Source Monitoring tab.

Procedure

To verify that Netflow collection is working:

1. In the **Security Analytics** menu, select **Administration > Health & Wellness**
2. Click the **Event Source Monitoring** tab.

3. In the grid, find the **Log Decoder**, **Event Source**, and **Event Source Type** (that is, **rsaflow**).
4. Look for activity in the **Count** column to verify that Netflow collection is accepting events.

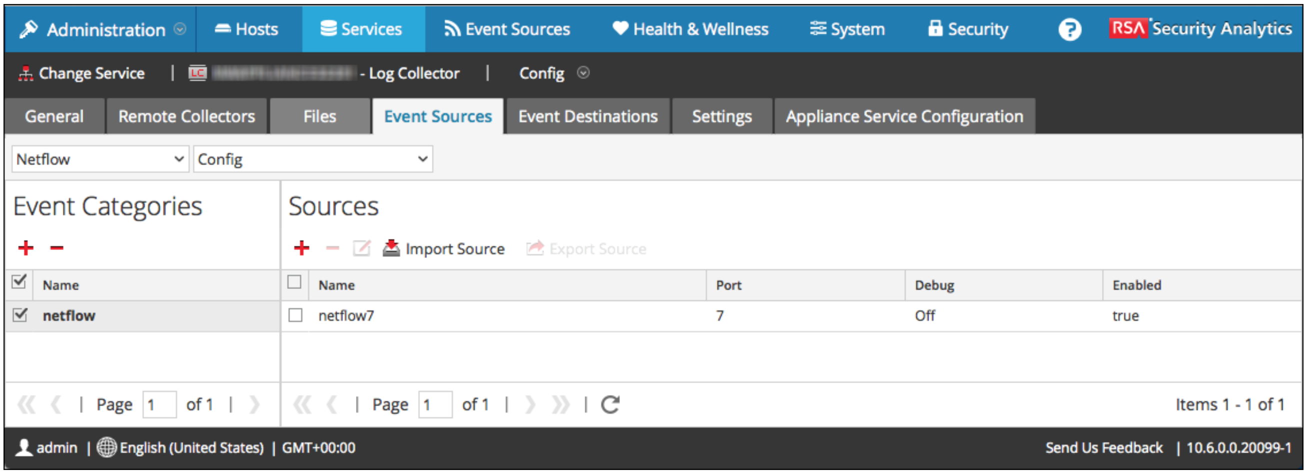
References - Netflow Collection Configuration Parameters

This topic describes the user interface for configuring Netflow Configuration.

Use this section when you are looking for descriptions of the Netflow Collection user interface and definitions of the features of the user interface.

To access the Netflow Collection Configuration Parameters:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.
4. In the **Log Collector Event Sources** tab, select **Netflow/Config** from the drop-down menu.



Netflow | Config

☑	Name
☑	**netflow**

□	Name	Port	Debug	Enabled
□	netflow7	7	Off	true

The Netflow/Config view in the Event Sources tab has two panels: Event Categories and Sources.

Event Categories Panel

In the Event Categories panel, you can add or delete the appropriate event source types.

Feature	Description
+	Displays the Available Event Source Types dialog from which you select the event source type for which you want to define parameters.
−	Deletes the selected event source types from the Event Categories panel.
□	Selects event source types.
Name	Displays the name of the event source types that you have added.

Available Event Sources Types Dialog

The Available Event Source Types dialog displays the list of supported event source types.

Feature	Description
□	Selects the event source type that you want to add.
Type	Display the event source types that are available to add.
Cancel	Closes the dialog without adding an event source type.
OK	Adds the selected event source type to the Event Categories panel.

Sources Panel

Use this panel to review, add, modify, and delete event source parameters for the event source type you selected in the Event Categories panel.

Toolbar

The following table provides descriptions of the toolbar options.

Option	Description
+	Opens the Add Source dialog in which you add a file directory for the event source type that you selected in the Event Categories panel.
−	Deletes the selected file directories.

Option	Description
✎	Opens the Edit Source dialog in which you modify the configuration parameters for the selected file directory. When you select multiple event sources, opens the Bulk Edit Source dialog in which you can edit the parameters values for the selected file directories. Refer to the *Log Collection Configuration Guide* for detailed steps on how to import, export, and edit event sources in bulk.
Import Source	Opens the Bulk Add Option dialog in which you can import event source file directory parameters in bulk from a comma-separated values (CSV) file. Refer to the *Log Collection Configuration Guide* for detailed steps on how to import, export, and edit event sources in bulk.
Export Source	Creates a **.csv** file that contains the parameters for the selected file directories. Refer to the **Log Collection Configuration Guide** for detailed steps on how to import, export, and edit event sources in bulk.

Add or Modify Source Dialog

In this dialog, you add or modify a file directory for the selected event source.

Feature	Description
Netflow Source Parameters	Lists the Netflow event source parameters populated with the default values. Enter or modify the appropriate values.
Cancel	Closes the dialog without adding a file directory or saving the parameter values for the selected file directory.
OK	In the Add Source dialog, adds the file directory and its parameters. In the Edit Source dialog, applies the parameter value changes for the selected file directory.

Netflow Source Parameters

The following table provides descriptions of the source parameters.

Name	Description
Basic	
Port	Specify the port number configured for the Netflow event source. Security Analytics opens the 2055, 4739, 6343, and 9995 ports for Netflow by default. You can open other ports for Netflow if required.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
Advanced	
InFlight Publish Log Threshold	Establishes a threshold that, when reached, Security Analytics generates a log message to help you resolve event flow issues. The Threshold is the size of the netflow event messages currently flowing from the event source to Security Analytics. Valid values are: • **0 (default)** - disables the log message. • **100-100000000** - generates a log message when this log collector has processed the specified number of netflow events. For example, if you set this value to 100, Security Analytics generates a log message when 100 netflow events of the specific netflow version (v5 or v9) have been processed.

Name	Description
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables/disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).
Cancel	Closes the dialog without making adding an event source type.
OK	Adds the parameters for the event source.

Tasks:

Step 1. Configure Netflow Event Sources in Security Analytics

Step 2. Configure Netflow Event Sources to Send Events to Security Analytics

Troubleshoot Netflow Collection

This topic highlights possible problems that you may encounter with Netflow Collection and provides suggested solutions to these problems.

Troubleshoot Netflow Collection Issues

In general, you receive more robust log messages by disabling SSL.

Log Message/ Problem	Log Collector is not receiving Netflow traffic.

Possible Cause	Configured the wrong port.
Solution	Make sure that you configured the correct firewall port (that is, 2055, 4739, 6343, or 9995).
Log Message/ Problem	Log Collector issues log messages that tell you there was an incompatible or mismatched header or version number.
Possible Cause	Netflow v10 event information was sent to log collector.
Solution	Ignore - Netflow v10 is not supported in Security Analytics 10.4. Netflow Collection only accepts events from Netflow v5 and Netflow v9.

ODBC Collection Configuration Guide

This guide tells you how to configure the ODBC collection protocol. This protocol collects events from event sources that store audit data in a database using the Open Database Connectivity (ODBC) software interface.

You must deploy Log Collection before you can configure the ODBC collection protocol.

For deployment instructions, see Log Collection Deployment Guide.

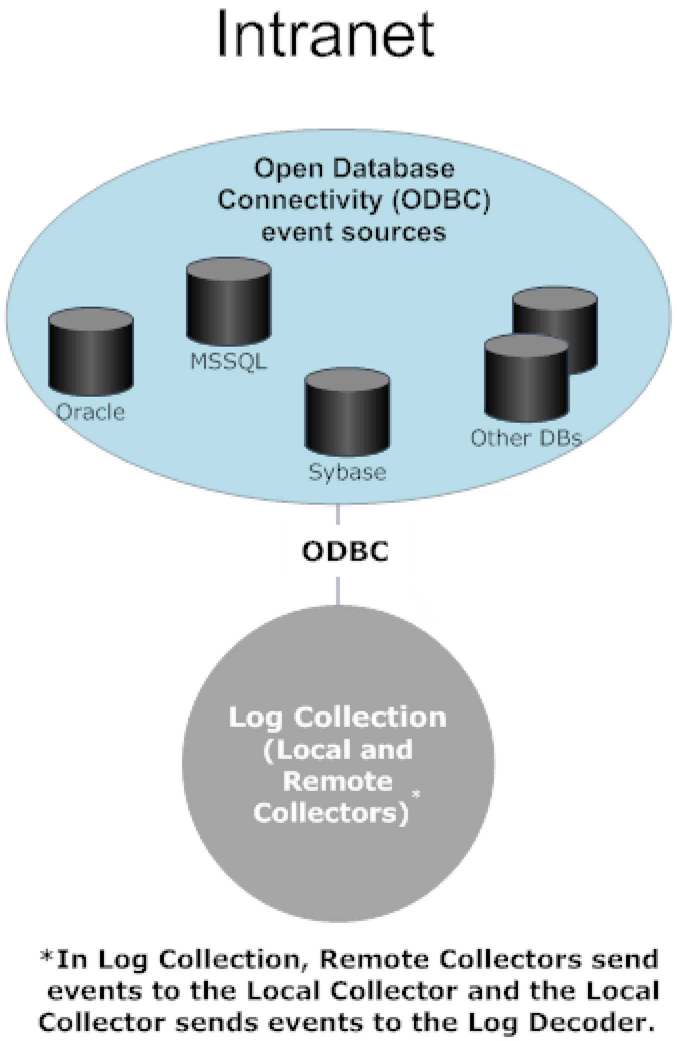
The Basics

Overview

This guide tells you how to configure ODBC collection protocol which collects events from event sources that store audit data in a database using the Open Database Connectivity (ODBC) software interface.

Deployment Scenario

The following figure illustrates how you deploy the ODBC Collection Protocol in Security Analytics.


Intranet
Open Database Connectivity (ODBC) event sources
MSSQL
Oracle
Sybase
Other DBs
ODBC
Log Collection (Local and Remote Collectors)*
*In Log Collection, Remote Collectors send events to the Local Collector and the Local Collector sends events to the Log Decoder.

Procedures

Configure ODBC Collection Protocol in Security Analytics

You configure the Log Collector to use ODBC collection for an event source in the event Source tab of the Log Collector parameter view. The following procedure explains the basic workflow for configuring an event source for ODBC Collection in Security Analytics. Please refer to:

- Step 1. Configure ODBC Event Sources in Security Analytics for step-by-step instructions on how to configure events sources in Security Analytics that use the ODBC Collection protocol.
- ODBC Event Source Configuration Parameters for a detailed description of each ODBC Collection Protocol parameter.

To configure the Log Collector to use ODBC collection protocol:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collection** service.
3. Select⚙ ⌄ > **View** > **Config** to display the Log Collection configuration parameter tabs.
4. In the **Event Sources** tab, select **ODBC** as the collection protocol and select **Config**.
5. Click + and select an event source category (for example, **mssql**).
6. The event source category is part of the content you downloaded from LIVE.
7. Select **DSNs** from the drop-down and click + .
8. Select a DSN value pair template, enter a DSN name, and add or delete value pairs if required.

   If required, click ☑ Manage Templates to add or delete DSN templates.
9. Select **Config**.
10. Select the **ODBC** category and click + in the **Sources** panel.
11. Specify the basic parameters required for the ODBC event source.
12. Click ⌄ and specify additional parameters that enhance how the ODBC protocol handles event collection for the event source.

Configure Event Sources to Use ODBC Collection Protocol

You need to configure each event source that uses the ODBC Collection protocol to communicate with Security Analytics (see Step 2. Configure ODBC Event Sources to Send Events to Security Analytics).

Procedures

This topic provides an overview of the end-to-end sequential configuration procedure for the ODBC Collection protocol with a checklist that contains each configuration step.

Configuration steps for the ODBC collection protocol must occur in the specific sequence listed in the table below.

ODBC Collection Configuration Checklist

> **Note:** The steps in this list are in the order in which you must complete them.

Step	Description	√
1	Configure ODBC Event Sources in Security Analytics.	
2	Configure ODBC Event Sources to Send Events to Security Analytics.	
3	Start service for configured ODBC collection protocol.	
4	Verify that ODBC Collection is working.	

Step 1. Configure ODBC Event Sources in Security Analytics

This topic tells you how to configure ODBC event source sources for the Log Collector.

After completing this procedure, you will have...

- Configured an ODBC event source.
- Modified an ODBC event source

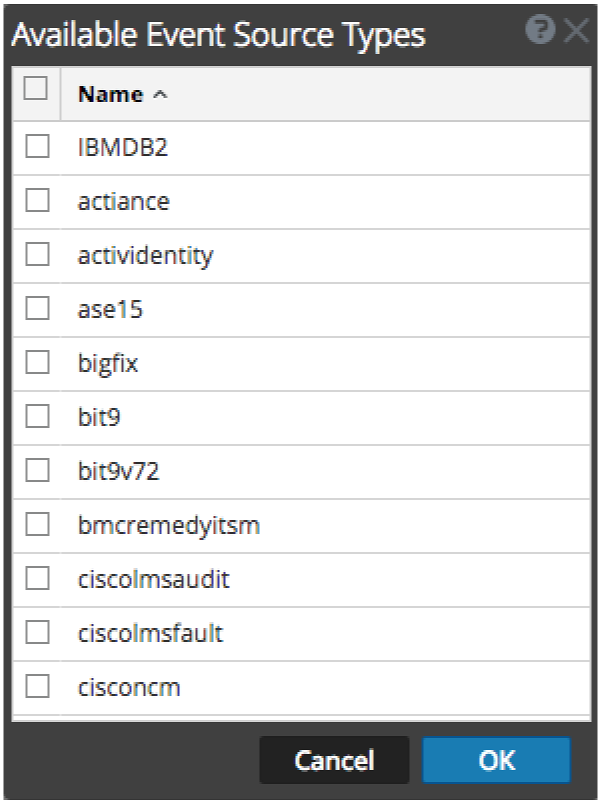
Return to Procedures

Procedures

Configure an ODBC Event Source

1. Make sure that you have configured the DSN/value pairs combination (see Step 1. Configure ODBC Event Sources in Security Analytics) for the ODBC Event Categories that you want to configure.

2. In the **Security Analytics** menu, select **Administration > Services**.
3. In the **Services** grid, select a **Log Collector** service.
4. Click ⚙ ⌄ under **Actions** and select **View > Config**.
5. In the **Log Collector Event Sources** tab, select **ODBC/Config** from the drop-down menu.
   The **Event Categories Panel** displays the ODBC event sources that are configured, if any.
6. Click ✚.
   The **Available Event Source Types** dialog is displayed.

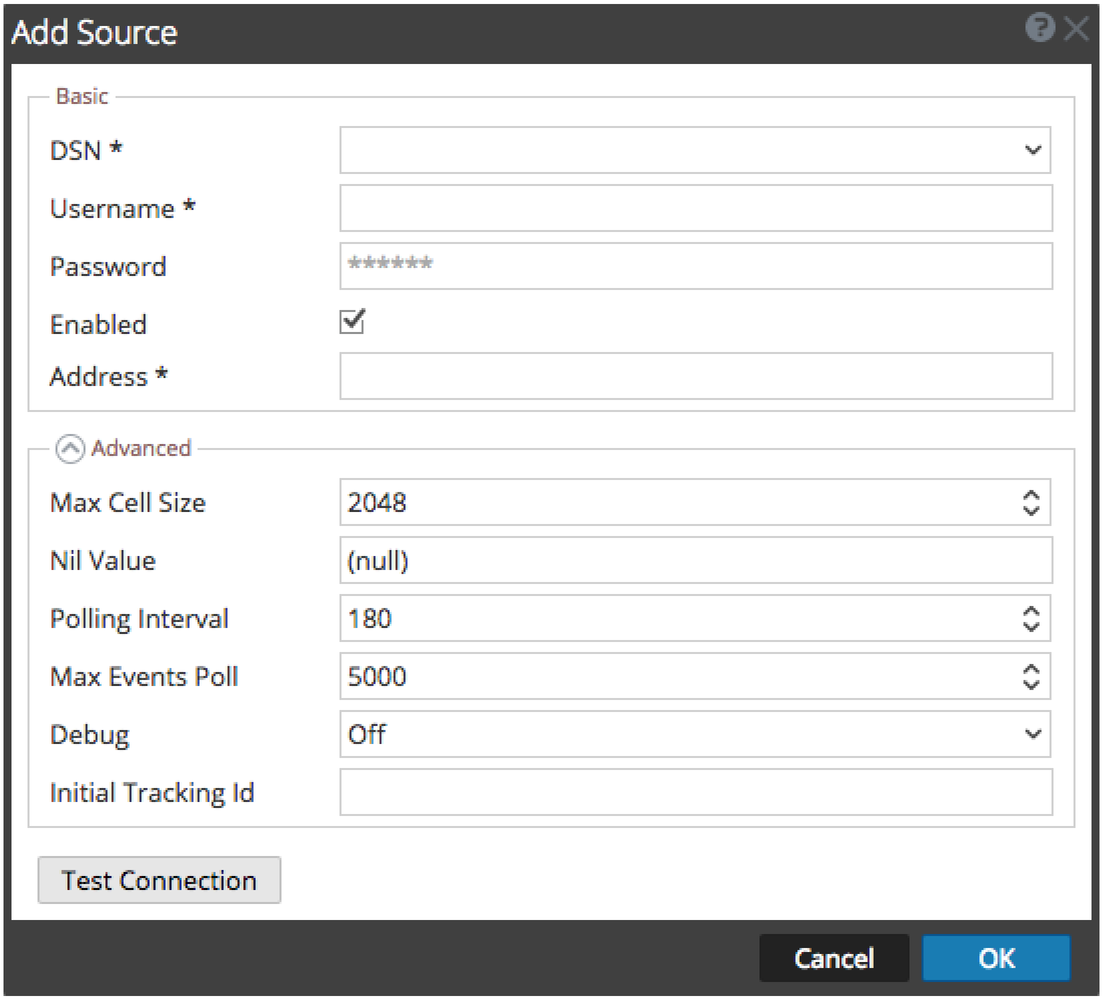


Available Event Source Types

□	**Name** ^
□	IBMDB2
□	actiance
□	actividentity
□	ase15
□	bigfix
□	bit9
□	bit9v72
□	bmcremedyitsm
□	ciscolmsaudit
□	ciscolmsfault
□	cisconcm

7. Select an event source type (for example, **mssql**) and click **OK**.
   The newly added ODBC event source type is displayed in the **Event Categories** panel.
8. Select the new type in the **Event Categories Panel** and click ✚ in the **DSNs List** panel toolbar.
   The **Add DSN** dialog is displayed.
9. Select a DSN from the drop down list, specify or modify the other parameters as required, and click **OK**.
   You defined the DSN names in the drop down list in step 4 that identify the DSN/value pairs

combinations.



DSN *	
Username *	
Password	******
Enabled	☑
Address *	
Max Cell Size	2048
Nil Value	(null)
Polling Interval	180
Max Events Poll	5000
Debug	Off
Initial Tracking Id	

10. Click **Test Connection**.
    The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the DSN information and retry.
    Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and the Security Analytics server displays an error message.

11. If the test is successful, click **OK**.
    The newly defined DSN is displayed in the **Sources** panel.

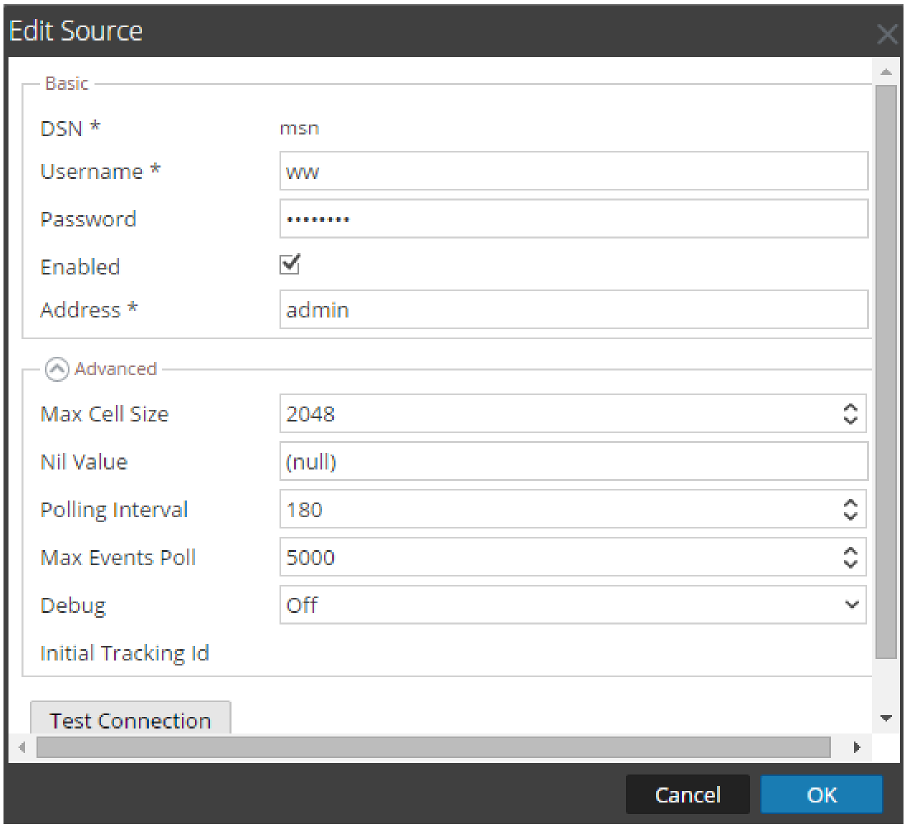
Modify an ODBC Event Source

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ ⌄ under **Actions** and select **View** > **Config**.

4. In the **Log Collector Event Sources** tab, select **ODBC/Config** from the drop-down menu.

5. In the **Sources** panel, select an event source and click ✎.

   The **Edit DSN** dialog is displayed



Edit Source

Basic

DSN *	msn
Username *	ww
Password	••••••••
Enabled	☑
Address *	admin

Advanced

Max Cell Size	2048
Nil Value	(null)
Polling Interval	180
Max Events Poll	5000
Debug	Off
Initial Tracking Id	

6. Modify the parameters that require changes.

7. Click **Test Connection**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the DSN information and retry.

   Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and the Security Analytics displays an error message.

8. If the test is successful, click **OK**.

   Security Analytics applies the parameter changes to selected DSN.

Parameters

References - ODBC Collection Configuration Parameters

ODBC DSNs Event Source Configuration Parameters

Configure Data Source Names (DSNs)

Overview

This topic tells you how to create and maintain DSNs for ODBC Collection.

Context

Open Database Connectivity (ODBC) event sources require Data Source Names (DSNs) so you need to define DSNs with their associate value pairs for ODBC event source configuration.

After completing this procedure, you will have..

- Added a DSN template.
- Added a DSN.
- Edited a DSN.

Return to Procedures

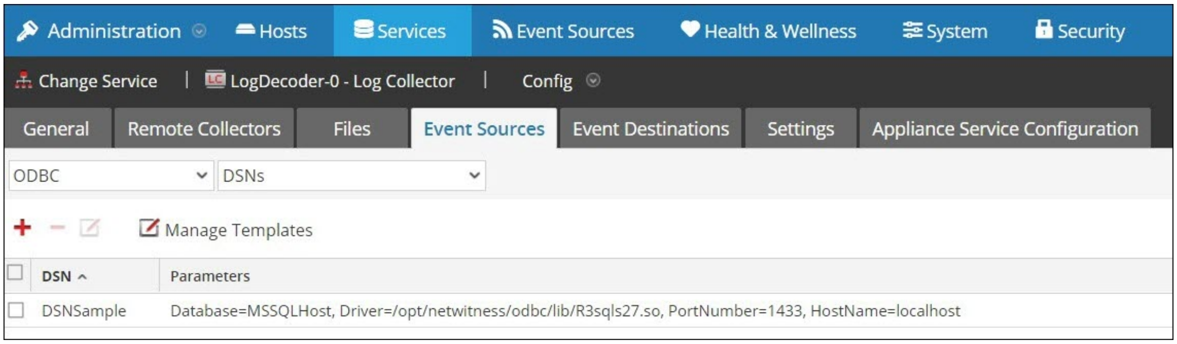
Procedures

Add a DSN Template

You can add DSN templates to use it the next time you add a DSN.

To add a DSN template:

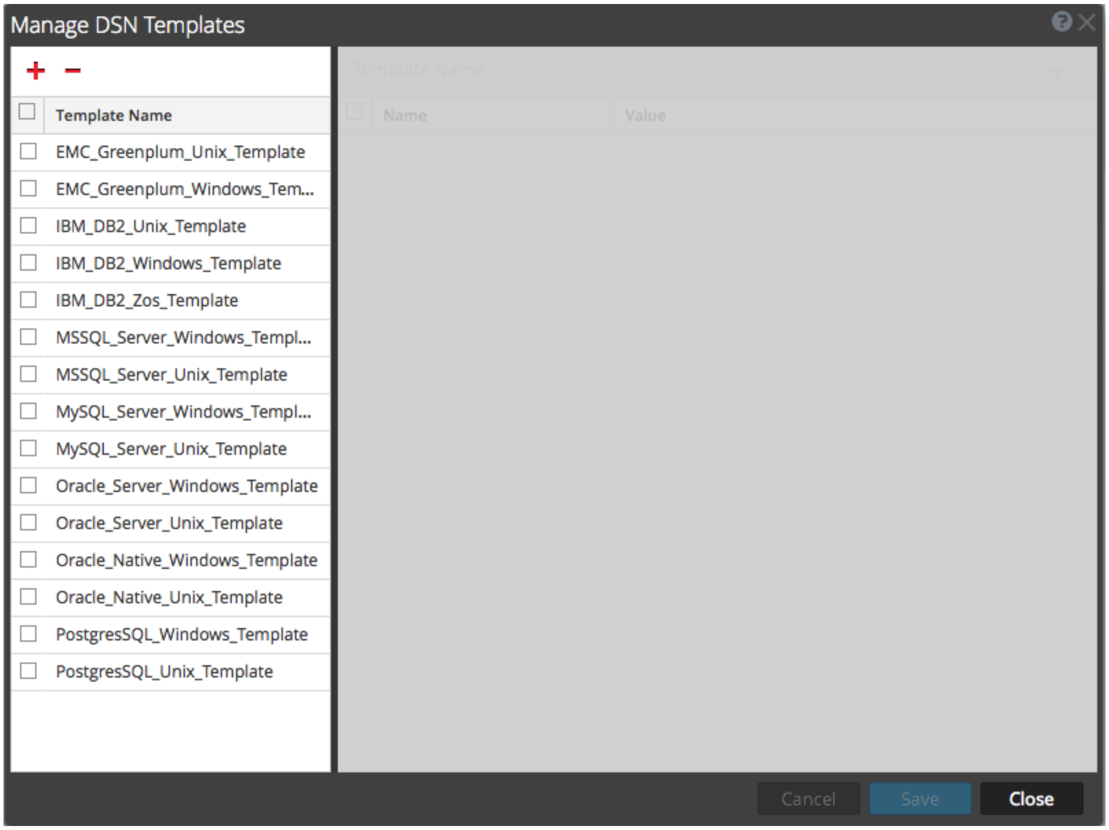
1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ ⌄ under **Actions** and select **View** > **Config**.
4. In the **Log Collector Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.
   The **DSNs** panel is displayed with the DSNs that are added, if any.



□	DSN ^	Parameters
□	DSNSample	Database=MSSQLHost, Driver=/opt/netwitness/odbc/lib/R3sqls27.so, PortNumber=1433, HostName=localhost

5. Click Manage Templates

   The **Manage DSN Templates** dialog is displayed.



□	Template Name
□	EMC_Greenplum_Unix_Template
□	EMC_Greenplum_Windows_Tem...
□	IBM_DB2_Unix_Template
□	IBM_DB2_Windows_Template
□	IBM_DB2_Zos_Template
□	MSSQL_Server_Windows_Templ...
□	MSSQL_Server_Unix_Template
□	MySQL_Server_Windows_Templ...
□	MySQL_Server_Unix_Template
□	Oracle_Server_Windows_Template
□	Oracle_Server_Unix_Template
□	Oracle_Native_Windows_Template
□	Oracle_Native_Unix_Template
□	PostgresSQL_Windows_Template
□	PostgresSQL_Unix_Template

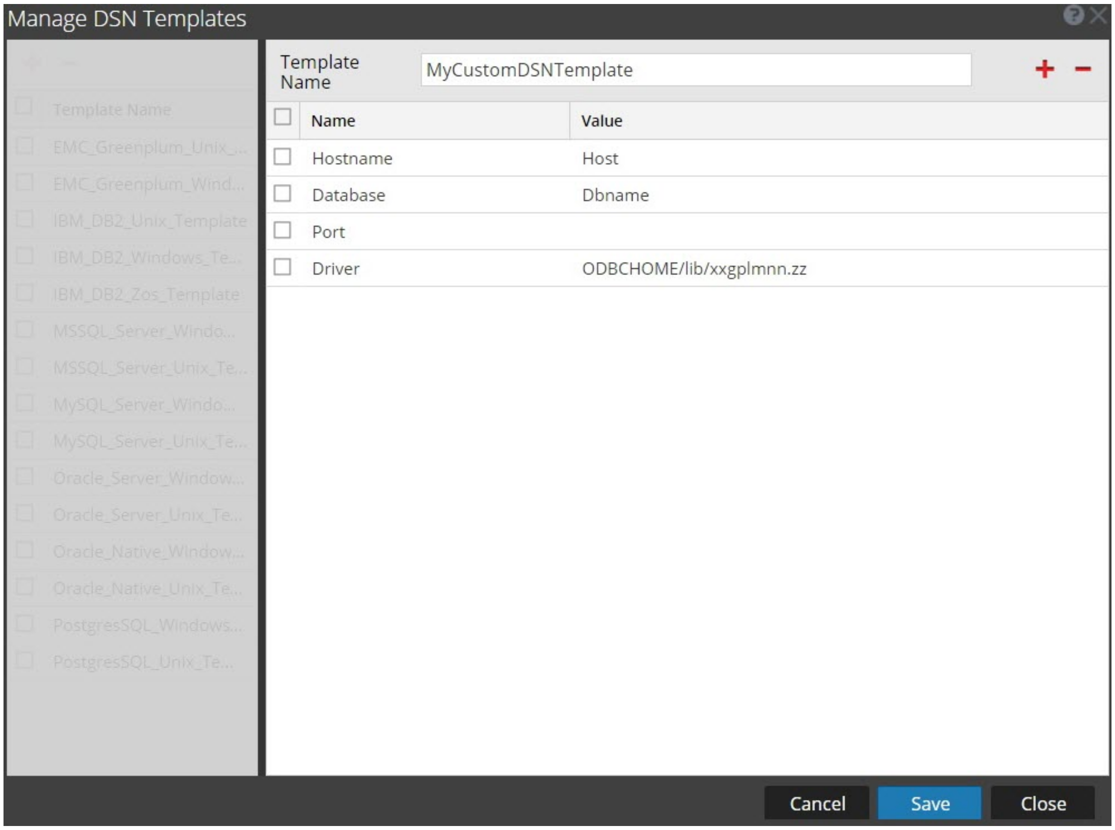
Note: RSA provides default templates on the left side panel that you can use while adding a new DSN.

6. Click +.

   The right panel is activated.

7. Specify a template name and click + on the right panel to add parameters.

8. Specify the parameters. Click **Save**.



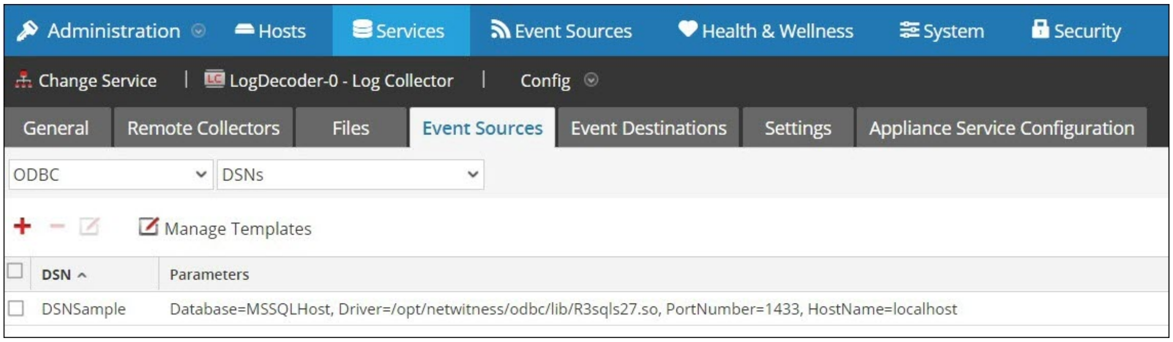
Template Name: MyCustomDSNTemplate

Name	Value
Hostname	Host
Database	Dbname
Port	
Driver	ODBCHOME/lib/xxgplmnn.zz

The new DSN template is added in the **Manage DSN Templates** list.

Add a DSN

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ under **Actions** and select **View > Config**.
4. In the **Log Collector Event Sources** tab, select **ODBC/DSNs** from the drop-down menus. The **DSNs** panel is displayed with the DSNs that are added, if any.

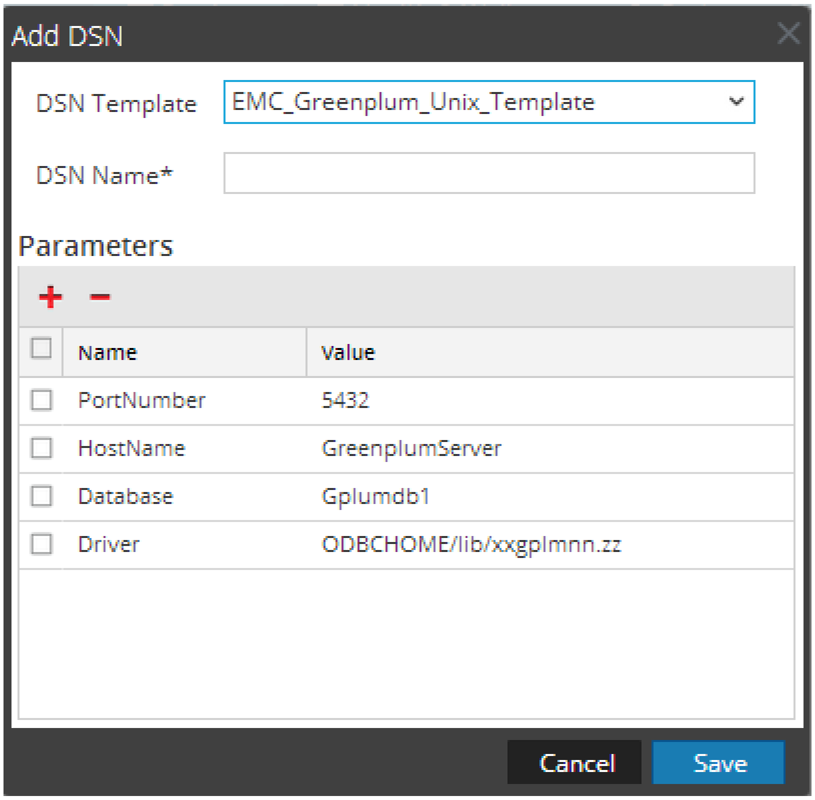


DSN	Parameters
DSNSample	Database=MSSQLHost, Driver=/opt/netwitness/odbc/lib/R3sqls27.so, PortNumber=1433, HostName=localhost

5. Click +.

- Using the DSN Template

   a. Select a DSN template from the drop down in **DSN Template** field. The default parameters are displayed.



DSN Template: EMC_Greenplum_Unix_Template

DSN Name*:

□	Name	Value
□	PortNumber	5432
□	HostName	GreenplumServer
□	Database	Gplumdb1
□	Driver	ODBCHOME/lib/xxgplmnn.zz

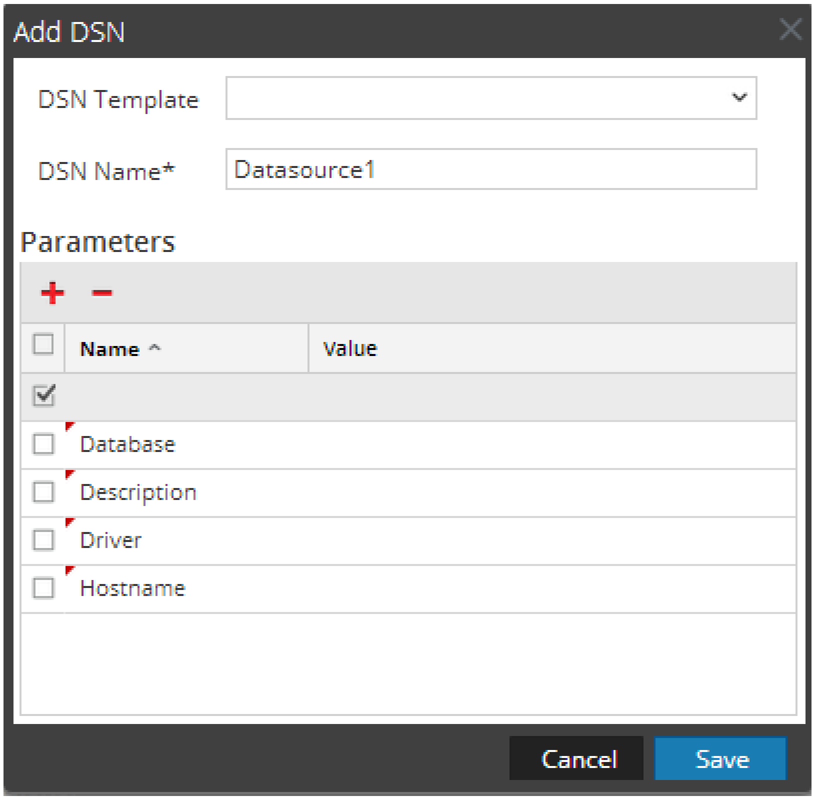
   b. Specify a name in the **DSN Name** field,

   c. Add, delete or edit the default parameters and click **Save**.The newly added DSN and its name-value pairs are displayed in the DSNs panel.

- Adding Parameters Manually

   a. Specify a name in the **DSN Name** field.

b. Click + to add parameters.



Add DSN

DSN Template:

DSN Name*: Datasource1

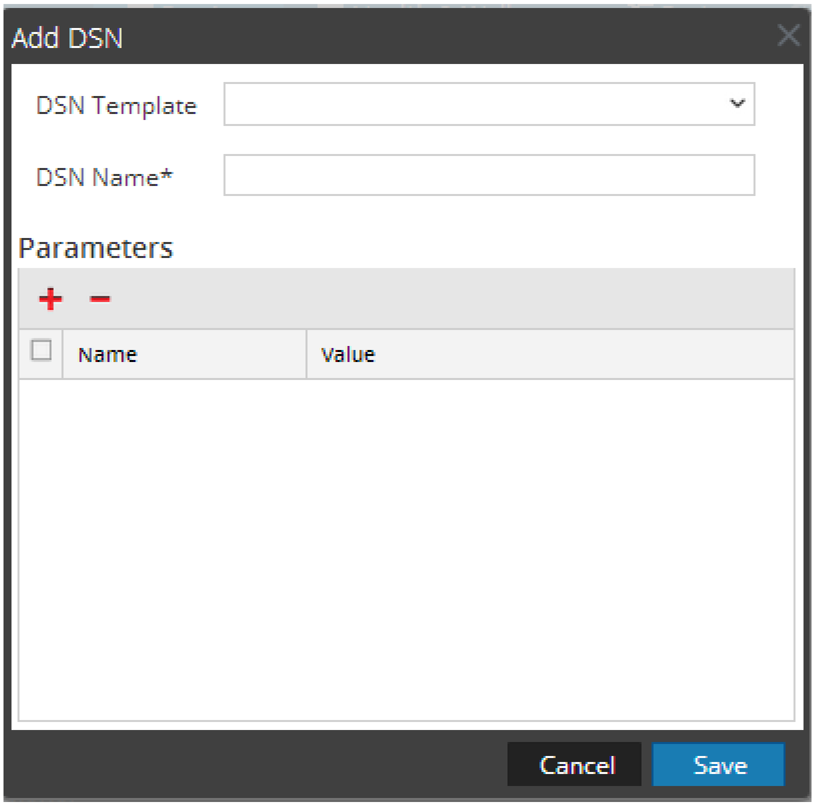
Parameters

☐	Name ^	Value
☑		
☐	Database	
☐	Description	
☐	Driver	
☐	Hostname	

c. Specify the value pairs in the dialog and click **Save**.

The newly added DSN and its name-value pairs are displayed in the **DSNs** panel.

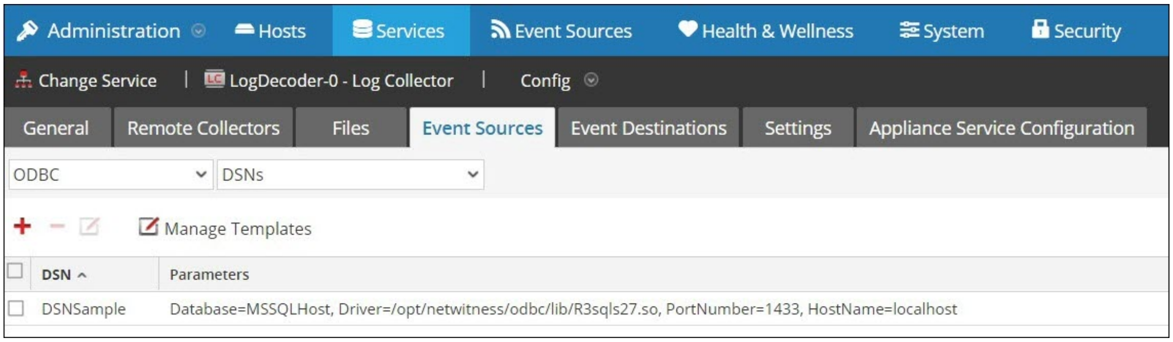
6. The **Add DSN** dialog is displayed.



You can add a DSN in two ways:

Edit a DSN

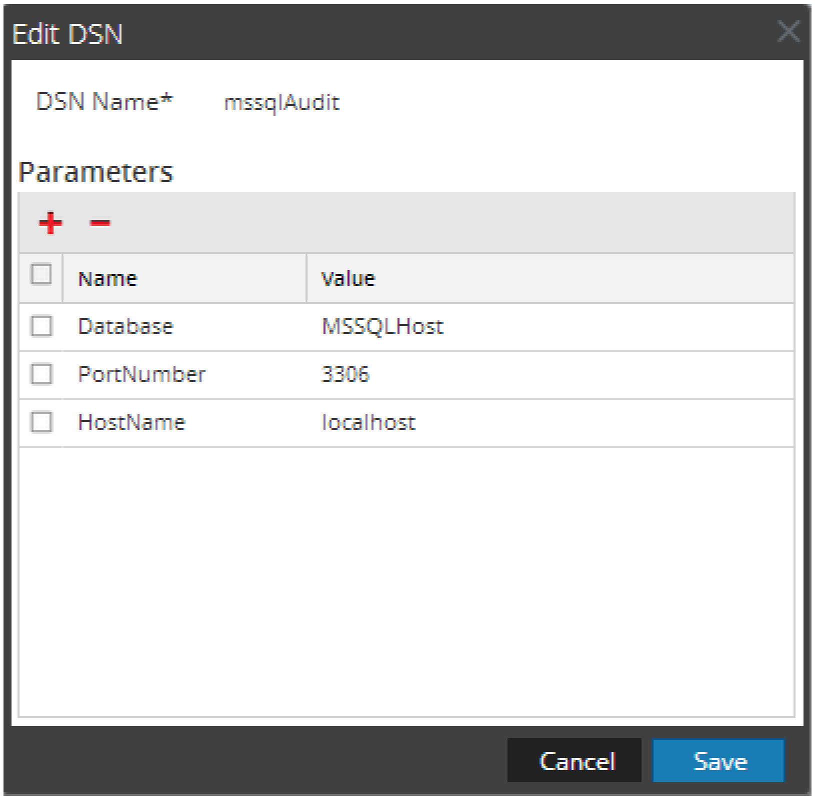
1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⚙ under **Actions** and select **View > Config**.
4. In the **Log Collector Event Sources** tab, select **ODBC/DSNs** from the drop-down menus. The **DSNs** panel is displayed with the DSNs that are added, if any



	DSN	Parameters
□	DSNSample	Database=MSSQLHost, Driver=/opt/netwitness/odbc/lib/R3sqls27.so, PortNumber=1433, HostName=localhost

5. Select a DSN.
6. Click ✎.

   The **Edit DSN** dialog is displayed.
7. Modify the parameters that require changes and click **Save**.



DSN Name* mssqlAudit

Parameters

□	Name	Value
□	Database	MSSQLHost
□	PortNumber	3306
□	HostName	localhost

The modified name-value pairs are displayed in the **DSNs** panel.

Parameters

ODBC DSNs Event Source Configuration Parameters

ODBC Event Source Configuration Parameters

Create Custom Typespec for ODBC Collection

This topic tells you how to create a custom typespec for the Log Collector. The topic includes:

- Create Custom typespec procedure
- ODBC Collection typespec syntax
- Sample ODBC Collection typespec files

Create Custom Typespec

To create a custom typespec file:

1. Open an SFTP client (for example, WinSCP) and connect to a Log Collector or remote Log Collector.
2. Navigate to **/etc/netwitness/ng/logcollection/content/collection/odbc**, and copy an existing file, for example **bit9.xml**.
3. Modify the file according to your requirements. See ODBC Collection Typespec Syntax for details.
4. Rename and save the file to the same directory.
5. Restart the Log Collector.

Note: You will not be able to see new Event Source type in Security Analytics until you restart the Log Collector.

ODBC Collection Typespec Syntax

The following table describes the typespec parameters.

Parameter	Description
name	The display name of your ODBC event source (for example, **activeidentity**). Security Analytics displays this name in the **Sources** panel of the **View > Config > Events Sources** tab. Valid value is an alphanumeric string. You cannot use - (dashes), _ (underscores), or spaces . The name must be unique across all typespec files in the folder.
type	Event source type: **odbc**. Do not modify this line.
prettyName	User-defined name for the event source. You can use the same value as name (for example, apache) or use a more descriptive name.
version	Version of this typespec file. Default value is 1.0.
author	Person who created the typespec file. Replace author-name with your name.
description	Formal description of the event source. Replace formal-description with your description of the event source.
<device> Section	

Parameter	Description
parser	**This *optional* parameter applies to Security Analytics 10.6.1 and newer.** This parameter contains the name of the log parser. This value forces the Log Decoder to use the specified log parser when parsing logs from this event source. **Note:** Please leave the field blank when unsure of the log parser to be used.
name	Name your ODBC event source (for example, **ActivIdentity ActivCard AAA Server**).
maxVersion	The version number of the event source (for example, **6.4.1**).
description	Description of the event source.
	<collection> Section
odbc	The syntax under `<odbc>` is used for event collection and processing. You can provide multiple queries for the same event source type by adding `<query>` tags.
query	This section contains the details of the query used to collect information from the event source.
tag	The prefix tag you want to add to events during transformation (for example **ActivIdentity**).
outputDelimiter	Specify the delimiter to use to separate fields. Specify any of the following values: • || (piping) • ^ (caret) • **,** (comma) • **:** (colon) • **0x20** (to represent a space)
interval	Specify the number of seconds between events. Default value is **60**.

Parameter	Description
dataQuery	Specify the query to fetch data from the ODBC eventsource database for SQL-syntax. For example: `SELECT acceptedrejected, servername, serveripa, sdate, millisecond, suid, groupname, ipa, reason, info1, info2, threadid FROM A_AHLOG WHERE sdate > '%TRACKING%' ORDER BY sdate`
maxTrackingQuery	The query used on the initial pull of events to identify the starting point within the data set to begin pulling logs from. After the initial pull, this query is no longer used, unless the **maxTracking** value has been reset or altered. For example: `SELECT MAX(Event_Id) from ExEvents`
trackingColumn	The tracking column value used when the ODBC collector pulls a new set of events.

Sample ODBC Collection Typespec Files

The following sample is the typespec file for the IBM ISS SiteProtector event source.

```
<?xml version="1.0" encoding="UTF-8"?>
<typespec>

   <name>siteprotector4_x</name>
   <type>odbc</type>
   <prettyName>SITEPROTECTOR4_X</prettyName>
   <version>1.0</version>
   <author>Administrator</author>
   <description>Collects events from SiteProtector</description>

   <device>
      <name>Internet Security Systems, Inc. RealSecure SiteProtector v 2.0</name>
      <maxVersion>2.0</maxVersion>
      <description></description>
      <parser>iss</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <odbc>
```

```
         <query>
            <tag></tag>
            <outputDelimiter></outputDelimiter>
            <interval></interval>
            <dataQuery></dataQuery>
            <maxTrackingQuery></maxTrackingQuery>
            <trackingColumn></trackingColumn>
            <levelColumn></levelColumn>
            <eventIdColumn></eventIdColumn>
            <addressColumn></addressColumn>
         </query>
      </odbc>
   </collection>
</typespec>
```

The following sample is the typespec file for the Bit9 Security Platform event source.

```
<?xml version="1.0" encoding="UTF-8"?>
<typespec>

   <name>bit9</name>
   <type>odbc</type>
   <prettyName>BIT9</prettyName>
   <version>1.0</version>
   <author>Administrator</author>
   <description>Bit9 Events</description>

   <device>
      <name>Bit9</name>
      <parser>bit9</parser>
   </device>

   <configuration>
   </configuration>

   <collection>
      <odbc>
         <query>
            <tag>BIT9</tag>
            <outputDelimiter>||</outputDelimiter>
            <interval>10</interval>
            <dataQuery>
            SELECT
            Timestamp,
            Event_Id,
            Computer_Id,
            File_Catalog_Id,
            Root_File_Catalog_Id,
            Priority,
            Type,
            Subtype,
            IP_Address,
            User_Name,
            Process,
            Description
            FROM
            ExEvents
            WHERE
            Event_Id > '%TRACKING%'
            </dataQuery>
            <trackingColumn>Event_Id</trackingColumn>
            <maxTrackingQuery>SELECT MAX(Event_Id) from ExEvent-
s</maxTrackingQuery>
            <eventIdColumn></eventIdColumn>
         </query>
      </odbc>
   </collection>
</typespec>
```

Step 2. Configure ODBC Event Sources to Send Events to Security Analytics

This topic tells you where to find the event sources currently supported for ODBC collection and the available configuration instructions for each event source.

You may need to view the event sources currently supported for ODBC collection, as well as the available configuration instructions for each event source. The Supported Event Sources list provides information on which event sources are currently available for ODBC collection.

Procedure

Return to Procedures

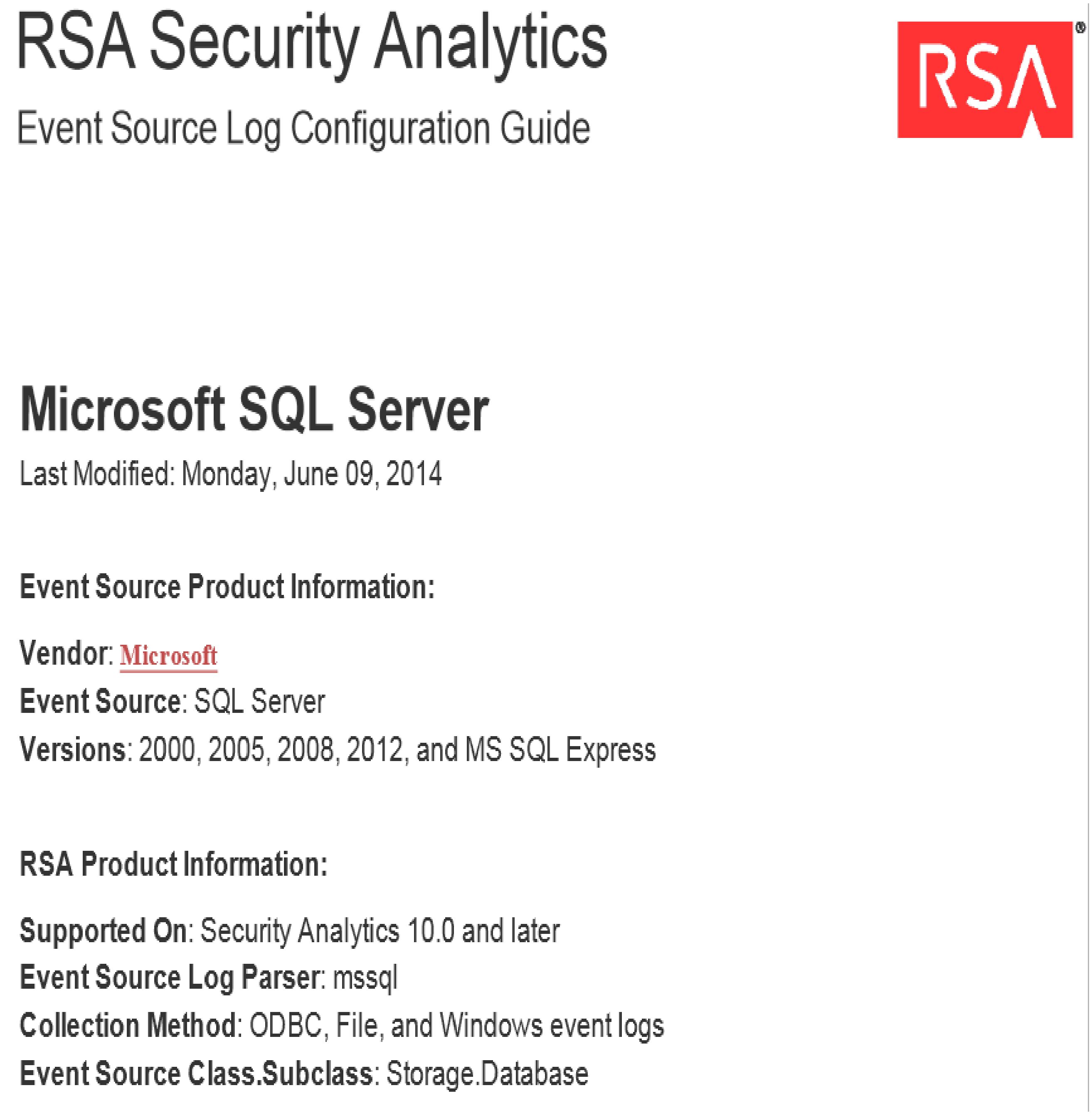
The list of RSA Supported Event Sources is an alphabetized of all the event sources currently supported by Security Analytics that identifies which event sources you can use with ODBC Collection. To verify that the event source is supported:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a Log Decoder and click ⚙ > **View** > **Config**.

   The **Services Config** view is displayed with the **General** tab open.
3. In the **General** tab, under the **Service Parsers Configuration** panel, find the name of the event source.
4. Verify that it is supported by the ODBC Collection protocol. Click on 📒 in the **Supported Event Sources** list to display the configuration instructions for the event source.
5. Verify that you downloaded the correct event source parser (for example, **mssql**) from Live to the Log Decoder and enabled it.

Sample Configuration Instructions

The following illustration is taken from the ODBC Security Suite, IPS-1 configuration instructions.



RSA Security Analytics

Event Source Log Configuration Guide

RSA

Microsoft SQL Server

Last Modified: Monday, June 09, 2014

Event Source Product Information:

Vendor: Microsoft
Event Source: SQL Server
Versions: 2000, 2005, 2008, 2012, and MS SQL Express

RSA Product Information:

Supported On: Security Analytics 10.0 and later
Event Source Log Parser: mssql
Collection Method: ODBC, File, and Windows event logs
Event Source Class.Subclass: Storage.Database

Step 3. Start Service for Configured ODBC Collection Protocol

This topic tells you how to start a stopped ODBC collection service.

If an ODBC collection service stops, you need to start it again to get it working. You can also enable the automatic start of individual services if you want the service to start automatically.

Procedure

Return to Procedures

The following procedure explains how to start a collection service. See the **Enable Automatic Start of Individual Services** topic in the *Log Collection Configuration Guide* if you want the service to start automatically.

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a Log Collector and select ⚙ ⌄ **> View > System**.

   The Services System view is displayed.
3. Select **Collection > ODBC > Start**.

Step 4. Verify That ODBC Collection Is Working

This topic tells you what to check in Security Analytics to verify that you have configured ODBC Collection correctly

You need to verify the ODBC Collection is configured correctly, otherwise it will not work.

Procedure

Return to Procedures

The following procedure explains how you can verify that ODBC collection is working from the **Administration** > **Health & Wellness** > **Event Source Monitoring** tab.

1. In the **Security Analytics** menu, select **Administration** > **Health & Wellness**.

   The **Health & Wellness** view is displayed with the **Monitoring** tab open.
2. In the **Event Source Monitoring** tab, find an ODBC event source type (for example, **msql**) in the **Event Source Type** column.
3. Look for activity in the **Count** column to verify that ODBC collection is accepting events.

References - ODBC Collection Configuration Parameters

This topic describes the ODBC event source configuration parameters.

ODBC event source parameters have two parts and separate view, ODBC and DSN parameters.

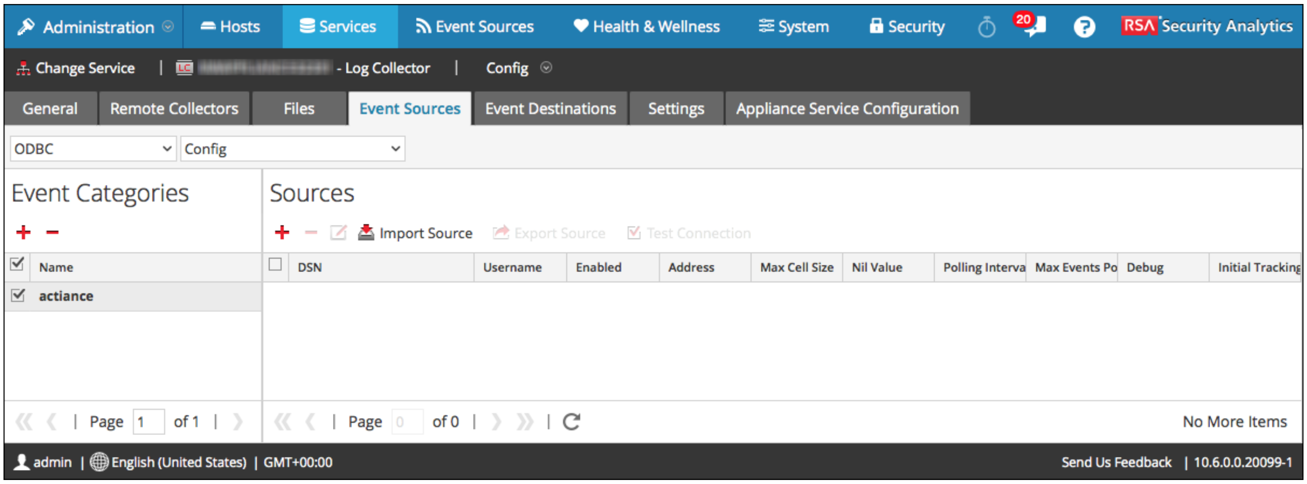
ODBC Event Source Configuration Parameters

This topic describes the ODBC event source configuration parameters.

To access the ODBC Event Source Configuration Parameters:

1. In the **Security Analytics** menu, select **Administration** >**Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.

   The **Service Config** view is displayed with the Log Collector **General** tab open.
4. In the **Log Collector Event Sources** tab, select **ODBC/Config** from the drop-down menu.



Features

The ODBC/Config view in the Event Sources tab has two panels: Event Categories and Sources.

Event Categories Panel

The Event Categories panel provides a way to add or delete event source types.

Feature	Description
+	Displays the Available Event Source Types dialog from which you select the event source type for which you want to define parameters.
−	Deletes the selected event source types from the Event Categories panel.
□	Selects event source types.
Name	Displays the name of the event source types that you have added.

Available Event Sources Types Dialog

In this dialog, you select the event source type for which you want to define parameters.

This dialog contains the list of event source types downloaded from the list of event source types in the Generic ODBC Type Specification (GOTS) file. If you do not see any event source types in this list, you did not load the content available with Log Collector upgrade to this release.

Feature	Description
□	Selects the event source type that you want to add.
Type	Displays the event source types that are available to add.
Cancel	Closes the dialog without adding an event source type.
OK	Adds the selected event source type to the Event Categories Panel.

Sources Panel

Use the Sources panel to review, add, modify, and delete Data Source Name (DSN) parameters.

An ODBC DSN tells the Log Collector how to reach an ODBC endpoint. You refer to an ODBC DSN when you configure a data source name with information such as which ODBC driver to use or the host name and port of the ODBC endpoint.

An ODBC DSN is a sequence of name -value pairs. For information about the valid names for a given ODBC data source type, such as Sybase, Microsoft SQL Server, or Oracle, please download the *DataDirect Connect Series for ODBC User's Guide and DataDirect Connect Series for ODBC User's Guide* in the Progress DataDirect Documentation Library.

Toolbar

The following table provides descriptions of the toolbar options.

Option	Description
+	Opens the Add DSN dialog in which you add an event source for the event source type you selected in the Event Categories panel.
−	Deletes the selected event sources.

✎	Opens the Edit DSN dialog in which you modify the configuration parameters for the selected event source. When you select multiple event sources, this option opens the Bulk Edit Source dialog in which you can edit the parameters values for the selected file directories. Refer to the *Log Collection Configuration Guide*for detailed steps on how to import, export, and edit event sources in bulk.
Import DSN	Opens the Bulk Add Option dialog in which you can import DSN parameters in bulk from a comma-separated values (CSV) file. The Bulk Add Option dialog has the following two options. Refer to the *Log Collection Configuration Guide*for detailed steps on how to import, export, and edit event sources in bulk.
Export DSN	Creates a **.csv** file that contains the parameters for the selected DSNs. Refer to the *Log Collection Configuration Guide*for detailed steps on how to import, export, and edit event sources in bulk.
☑ Test Connection	Validates the configuration parameters for the selected ODBC database. Refer to the *Log Collection Configuration Guide*for detailed steps on how to test event source connections in bulk.

Add or Edit DSN Dialog

In this dialog, you add or modify an event source for the selected event source.

Name	Description
Basic	

DSN*	The data source name (DSN) that defines the database from which to collect events. Select an existing DSN from the drop-down list. The values in this list are maintained in the ODBC DSNs Event Source Configuration Parameters.
Username*	User name that the data source name uses to connect to the database. You must specify a user name when you create the event source.
Password	Password that the data source name uses to connect to the database. **Caution:** The password is encrypted internally and is displayed in its encrypted form.
Enabled	Select the checkbox to enable the event source configuration to start collection. The checkbox is selected by default.
Address*	For ODBC, this field is not used. The Log Collector uses the address in the **ODBC.ini** file.
Advanced	
Max Cell Size	Maximum size in bytes of the data that the Log Collector can pull from one cell in the database. The default value is **2048**.
Nil Value	Character string that the Log Collector displays when NIL is returned for a cell in the database. Default value: **“”** (null).
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).

Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.
Initial Tracking Id	Initial identification code that the Log Collector assigns to this event source if collection is not started. If there is no value for this parameter, the Log Collector starts at the end of the table and only pulls rows after the end of the table as they are added. The default value is **“”** (null).
Filename	For Microsoft SQL Server Event Sources only, the location of the trace files directory (for example, **C:\MyTraceFiles**). Please refer to the RSA Microsoft SQL Server Event Source Configuration Guide, located on RSA Secure Care Online (SCOL) for detailed information on how to create this directory with the correct permissions.
Test Connection	Checks the configuration parameters specified in this dialog to make sure they are correct.
Cancel	Closes the dialog without adding or modifying DSN parameters.
OK	Adds or modifies the parameters for the DSN.

Tasks

Step 1. Configure ODBC Event Sources in Security Analytics

ODBC DSNs Event Source Configuration Parameters

This topic describes the Data Source Names DSNs configuration parameters.

Open Database Connectivity (ODBC) event sources require Data Source Names (DSNs) so you need to define DSNs with their associate value pairs for ODBC event source configuration. This topic describes the DSN configuration parameters.

To access the ODBC DSNs Event Source Configuration Parameters:

1. In the **Security Analytics** menu, select **Administration** >**Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. From the **Event Sources** tab, select **ODBC/DSNs** from the drop-down menus.

Features

The ODBC/DSNs view in Event Sources has one panel: the DSN panel.

DSN Panel

In the DSNs panel, you can add, delete, or edit DSNs and the DSN name -value pairs for ODBC Event sources.

Feature	Description
+	Displays the Add DSN dialog in which you define a DSN and its parameters.
−	Deletes the selected DSNs.
✎	Displays the Edit DSN dialog in which you edit the name-value pairs for the selected DSN.
✎ Manage Templates	Displays the Manage DSN Templates dialog in which you can add or delete DSN name-value pair templates.
□	Selects DSNs.
DSN	Name of the DSN that you added.
Parameters	**<name-value for="" p="" pairs="" the=""> </name-value>**

Add or Edit DSN Dialog

In this dialog, you add or modify a file directory for the selected event source.

Feature	Description
DSN Template	Select a predefined DSN value name-value pairs template for the DSN.
DSN Name*	Add the name of the DSN. You cannot edit a DSN name after you add it. This value must correspond with a DSN entry in the ODBC.ini file. Valid value is a character string that is restricted to the following characters: `[_a-zA-Z][_a-zA-Z0-9]*` This means that the file directory must start with a letter followed by numbers, letters, and underscores (for example, oracle_executive_compensation).
Parameters	+ Adds a row in which you can define a parameter name-value pair. − Deletes the selected parameter name-value pair. ☐ Selects parameter name-value pairs. Name - Enter or modify the parameter name. Value - Enter or modify the value associated with the parameter name.
Cancel	Closes the dialog without adding the DSN and its name-value pairs or saving modifications to the name-value pairs.
Save	Adds the DSN and its name-value pairs or saves modifications to the name-value pairs.

Manage DSN Templates Dialog

In this dialog, you can add or delete DSN name-value pair templates.

Feature	Description
Template Selection Panel	
+	Opens the Add Template panel in which you can add a DSN name-value pair template.

Feature	Description
−	Deletes the selected template.
☐	Selects a template for deletion or modification.
Add Template Panel	
+	Adds a value pair row.
−	Deletes a value pair row.
☐	Selects a value pair row.
Name	Enter the parameter name.
Value	Enter the value associated with the parameter name.
Cancel	Cancels any changes you made in the dialog.
Save	Adds the DSN and its name-value pairs or saves modifications to the name-value pairs.
Close	Closes the dialog without adding the DSN and its name-value pairs or saving modifications to the name-value pairs.

Task

Step 1. Configure ODBC Event Sources in Security Analytics

Troubleshoot ODBC Collection

This topic suggests how to resolve problems you may encounter with the ODBC collection protocol.

Troubleshoot ODBC Collection Issues

You can troubleshoot problems and monitor ODBC collection by reviewing the ODBC collector log informational, warning, and error messages to during execution of collection.

Each ODBC log messages includes the:

- Timestamp
- Category: debug, info, warning, or failure
- collection method = OdbcCollection
- ODBC event source type (GOTS-name) = Generic ODBC Type Specification name that you configured for the event source.
- collection function completed or attempted (for example, [processing])
- ODBC event source name (DSN-name) = Data Source Name that you configured for the event source.
- description (for example, how many events the Log Collector collected)
- tracking ID = the Log Collector position in the target database table.

The following example illustrates the message you would receive upon successful collection of an ODBC event:

```
2014-July-25 17:21:25 info (OdbcCollection) : [event-source]
[processing] [event-source] Published 100 ODBC events: last
tracking id: 2014-July-25 13:22:00.280
```

The following example illustrates a message you may receive upon unsuccessful collection of an ODBC event:

Log Message	timestamp failure (OdbcCollection: [event-source] [processing][event-source-type] Failed during doWork: Unable to prepare statement: state: S0002; error-code:208; description: [RSA] [ODBC-driver][event-source-type]Invalid object name 'object-name'.
Possible Cause	ODBC collection failed while accessing the ODBC Driver or the target database.
Solutions	Validate the DSN value pairs for the events source.

SDEE Collection Configuration Guide

This guide tells you how to configure the SDEE collection protocol. This protocol collects events from Intrusion Detection System (IDS) and Intrusion Prevention Service (IPS) messages.

You must deploy Log Collection before you can configure the SDEE collection protocol.

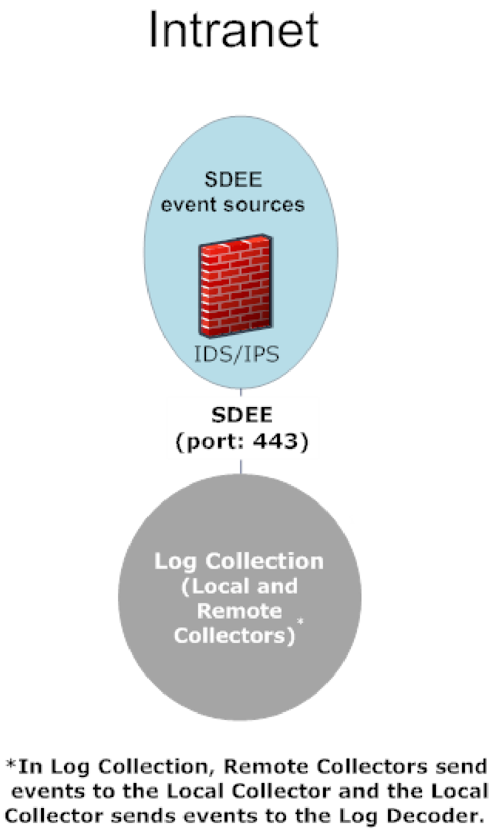
For deployment instructions, see Log Collection Deployment Guide.

The Basics

This guide tells you how to configure the SDEE collection protocol which collects events from Intrusion Detection System (IDS) and Intrusion Prevention Service (IPS) messages.

Deployment Scenario

The following figure illustrates how you deploy the SDEE Collection Protocol in Security Analytics.

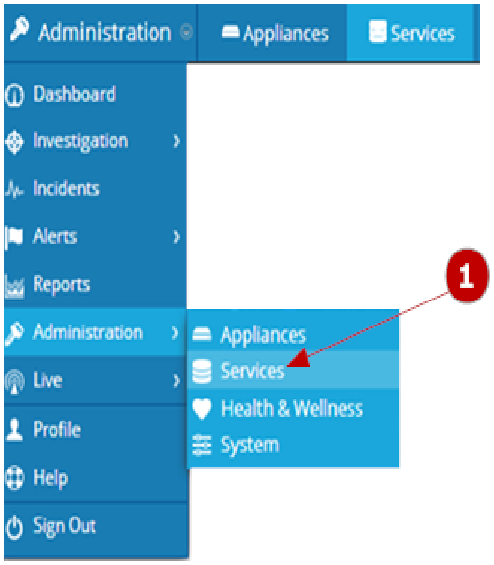

Intranet
SDEE
event sources
IDS/IPS
SDEE
(port: 443)
Log Collection
(Local and
Remote
Collectors)*
*In Log Collection, Remote Collectors send events to the Local Collector and the Local Collector sends events to the Log Decoder.

Procedures

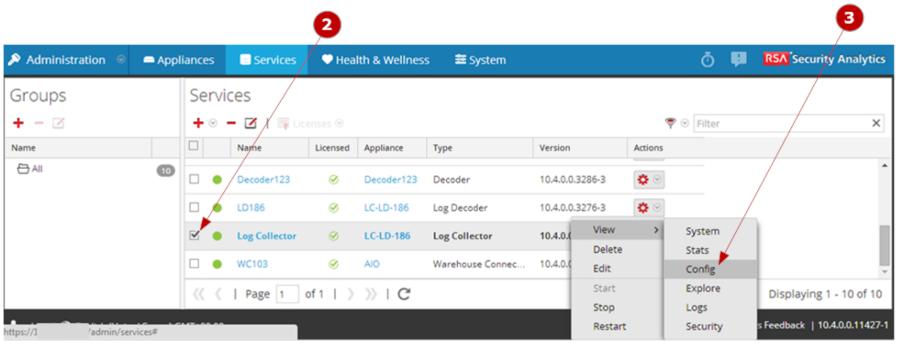
Configure SDEE Collection Protocol in Security Analytics

You configure to the Log Collector to use SDEE collection for an event source in the event Source tab of the Log Collector parameter view. The following figure the basic workflow for configuring an event source for SDEE Collection in Security Analytics. Please refer to:

- Step 1. Configure SDEE Event Sources in Security Analyticsfor step-by-step instructions on how to configure events sources in Security Analytics tht use the SDEE Collection protocol.
- Reference - SDEE Event Source Configuration Parameters for a detailed description of each SDEE Collection Protocol parameter.



1 Access the **Services** view.



☐		Name	Licensed	Appliance	Type	Version	Actions
☐	●	Decoder123	✓	Decoder123	Decoder	10.4.0.0.3286-3	
☐	●	LD186	✓	LC-LD-186	Log Decoder	10.4.0.0.3276-3	
☑	●	Log Collector	✓	LC-LD-186	Log Collector	10.4.0.(	
☐	●	WC103	✓	AIO	Warehouse Connec...	10.4.0.(	

Page 1 of 1

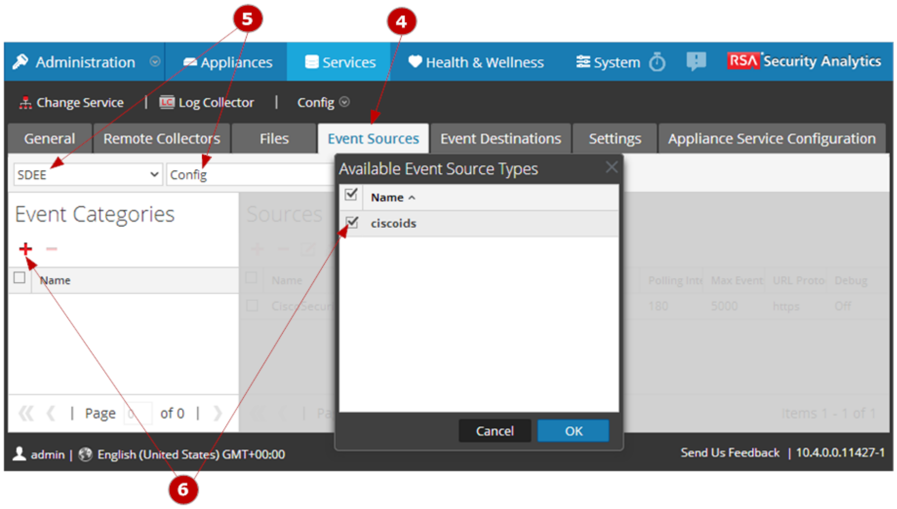
Displaying 1 - 10 of 10

https://1[redacted]/admin/services#

s Feedback | 10.4.0.0.11427-1

2 Select a **Log Collection** service.

3 Click ⌄ under **Actions** and select **View > Config** to display the **Log Collection** configuration parameter tabs.

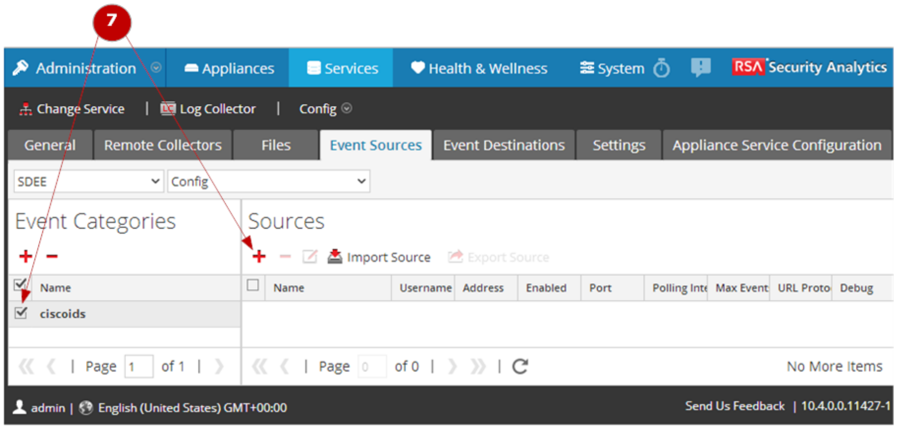


4 Click the **Event Sources** tab.

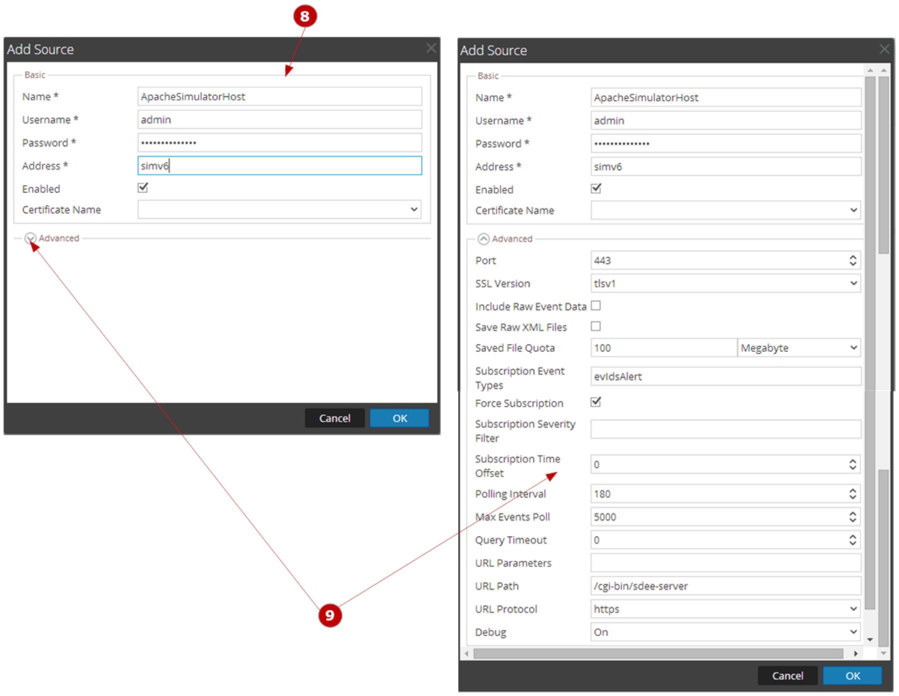
5 Select **SDEE** as the collection protocol and select **Config**.

6 Click + and select **SDEE** as the event source category.

The event source category is part of the content you downloaded from LIVE.



7 Select the **SDEE** category and click + .



Add Source

Basic

Name * ApacheSimulatorHost

Username * admin

Password * •••••••••••••••

Address * simv6

Enabled ☑

Certificate Name

Advanced

Add Source

Basic

Name * ApacheSimulatorHost

Username * admin

Password * •••••••••••••••

Address * simv6

Enabled ☑

Certificate Name

Advanced

Port 443

SSL Version tlsv1

Include Raw Event Data □

Save Raw XML Files □

Saved File Quota 100 Megabyte

Subscription Event Types evIdsAlert

Force Subscription ☑

Subscription Severity Filter

Subscription Time Offset 0

Polling Interval 180

Max Events Poll 5000

Query Timeout 0

URL Parameters

URL Path /cgi-bin/sdee-server

URL Protocol https

Debug On

8 Specify the basic parameters required for the SDEE event source.

9 Click ⌄ and specify additional parameters that enhance how the SDEE protocol handles event collection for the event source.

Configure Event Sources to Use SDEE Collection Protocol

You need to configure each event source that uses the SDEE Collection protocol to communicate with Security Analytics (see Step 2. Configure SDEE Event Sources to Send Events to Security Analytics).

Procedures

This topic provides an overview of the end-to-end sequential configuration procedure for the SDEE Collection protocol with a checklist that contains each configuration step

Configuration steps for the SDEE collection protocol must occur in the specific sequence listed in the table below.

SDEE Collection Configuration Checklist

Note: The steps in this list are in the order in which you must complete them.

Step	Description	√
1	Configure SDEE Event Sources in Security Analytics.	
2	Configure SDEE Event Sources to Send Events to Security Analytics.	
3	Start service for configured SDEE collection protocol.	
4	Verify that SDEE Collection is working.	

Step 1. Configure SDEE Event Sources in Security Analytics

This topic tells you how to configure SDEE event sources for the Log Collector.

After completing this procedure, you will have...

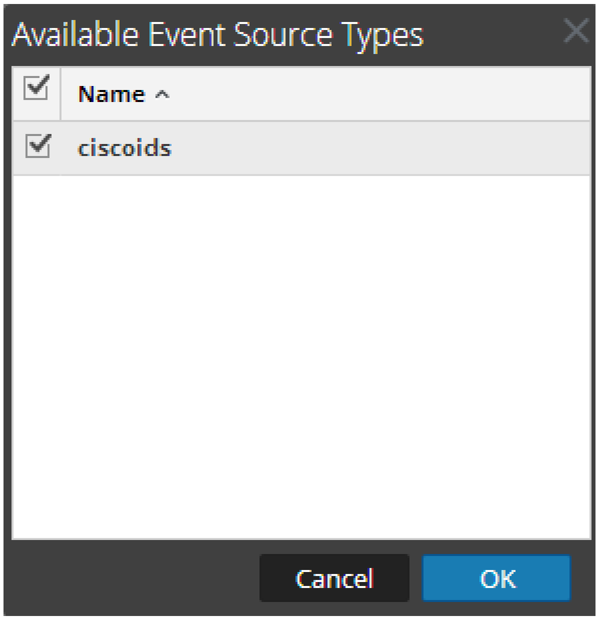
- Configured an SDEE event source.
- Modified an SDEE event source.

Return to Procedures

Procedures

Configure an SDEE Event Source

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Event Sources** tab, select **SDEE/Config** from the drop-down menu.
   The **Event Categories** panel displays the SDEE event sources that are configured, if any.
5. In the **Event Categories** panel toolbar, click ✚.

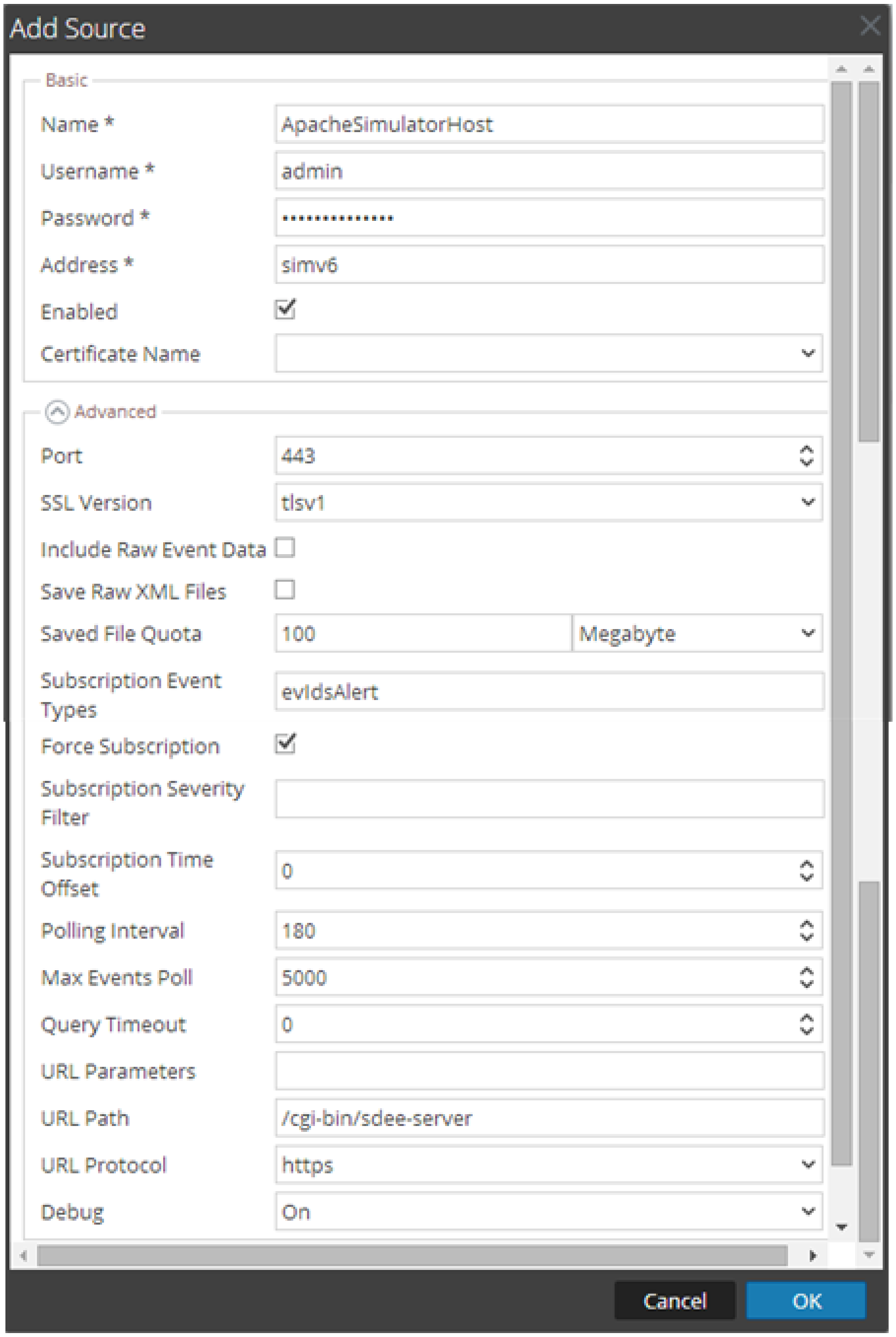


If you do not see any event source types in this list, you did not load the content that you get from Customer Care as part of the Log Collector upgrade to this release.

6. Select an event source type (for example, **ciscoids**) and click **OK**.
   The newly added event source type is displayed in the **Event Categories** panel.

7. Select the new type in the **Event Categories** panel and click + in the Sources toolbar.
   The **Add Source** dialog is displayed.

8. Add a **Name**, **Username**, **Address**, and **Password**, and modify any other parameters that require changes, and click **OK**.



Add Source

Basic

Name *	ApacheSimulatorHost
Username *	admin
Password *	•••••••••••••••
Address *	simv6
Enabled	☑
Certificate Name	

Advanced

Port	443
SSL Version	tlsv1
Include Raw Event Data	□
Save Raw XML Files	□
Saved File Quota	100 Megabyte
Subscription Event Types	evIdsAlert
Force Subscription	☑
Subscription Severity Filter	
Subscription Time Offset	0
Polling Interval	180
Max Events Poll	5000
Query Timeout	0
URL Parameters	
URL Path	/cgi-bin/sdee-server
URL Protocol	https
Debug	On

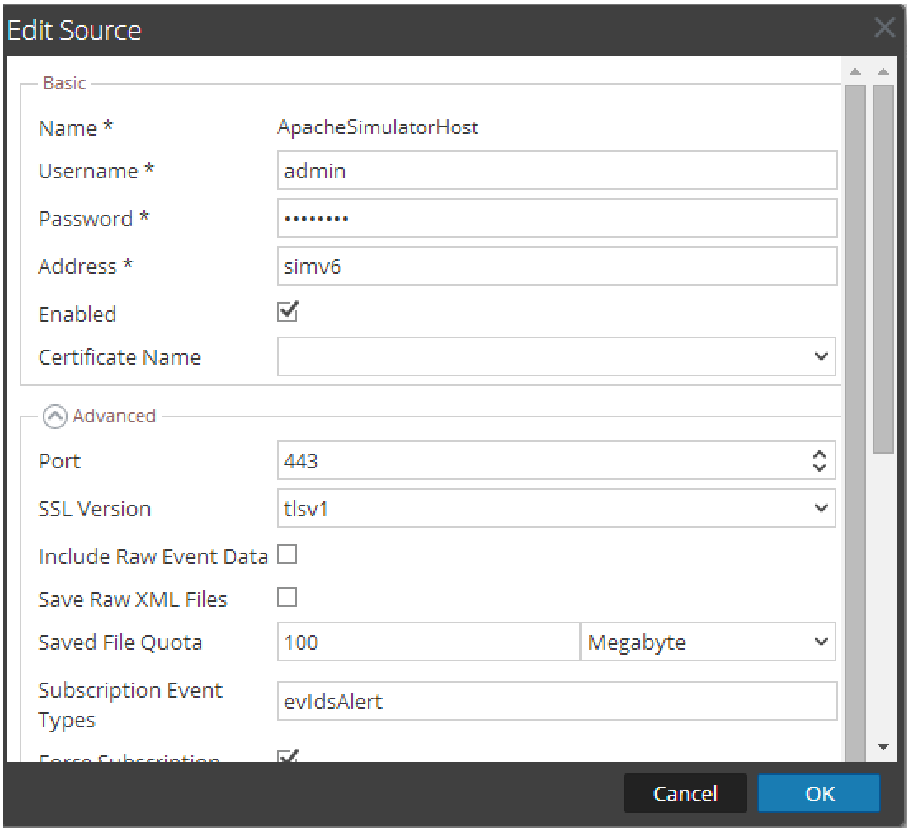
The new event source is displayed in the list.

Modify an SDEE Event Source

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.

4. In the **Event Sources** tab, select **SDEE/Config** from the drop-down menu.
5. Select an event source type in the Event Categories panel.
6. In the **Sources** panel, select an event source and click ✎.

   The **Edit Source** dialog is displayed.



Name * ApacheSimulatorHost

Username * admin

Password * ••••••••

Address * simv6

Enabled ☑

Certificate Name

Port 443

SSL Version tlsv1

Include Raw Event Data ☐

Save Raw XML Files ☐

Saved File Quota 100 Megabyte

Subscription Event Types evIdsAlert

Force Subscription ☑

7. Modify the parameters that require changes and click **OK**.
8. Security Analytics applies the parameter changes to the selected event source.

Parameters

Reference - SDEE Event Source Configuration Parameters

Step 2. Configure SDEE Event Sources to Send Events to Security Analytics

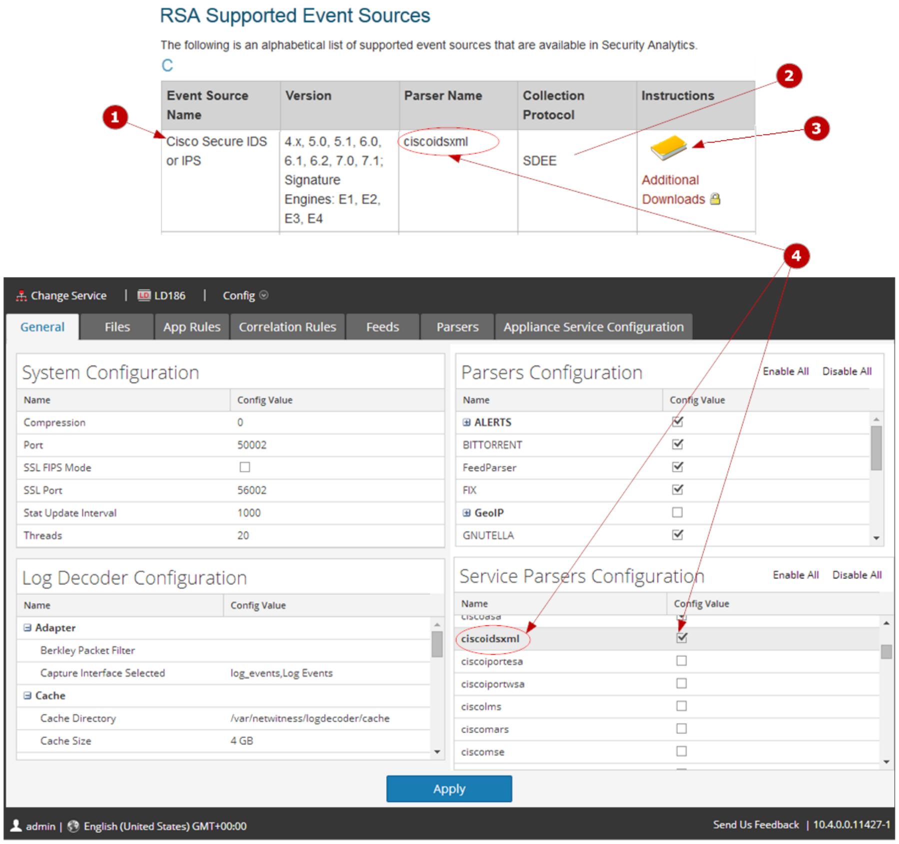
This topic tells you where to find the event sources currently supported for SDEE collection and the available configuration instructions for each event source.

Return to Procedures

The event sources currently supported for SDEE collection are available in the Supported Event Sources list.

Procedure

The list of RSA Supported Event Sources is an alphabetized of all the event sources currently supported by Security Analytics that identifies which event sources you can use with SDEE Collection.



RSA Supported Event Sources

The following is an alphabetical list of supported event sources that are available in Security Analytics.

C

Event Source Name	Version	Parser Name	Collection Protocol	Instructions
Cisco Secure IDS or IPS	4.x, 5.0, 5.1, 6.0, 6.1, 6.2, 7.0, 7.1; Signature Engines: E1, E2, E3, E4	ciscoidsxml	SDEE	📒 Additional Downloads 🔒

System Configuration

Name	Config Value
Compression	0
Port	50002
SSL FIPS Mode	□
SSL Port	56002
Stat Update Interval	1000
Threads	20

Log Decoder Configuration

Name	Config Value
⊟ Adapter	
Berkley Packet Filter	
Capture Interface Selected	log_events,Log Events
⊟ Cache	
Cache Directory	/var/netwitness/logdecoder/cache
Cache Size	4 GB

Parsers Configuration

Name	Config Value
⊞ ALERTS	☑
BITTORRENT	☑
FeedParser	☑
FIX	☑
⊞ GeoIP	□
GNUTELLA	☑

Service Parsers Configuration

Name	Config Value
ciscoasa	☑
ciscoidsxml	☑
ciscoiportesa	□
ciscoiportwsa	□
ciscolms	□
ciscomars	□
ciscomse	□

1 Find the name of the event source.

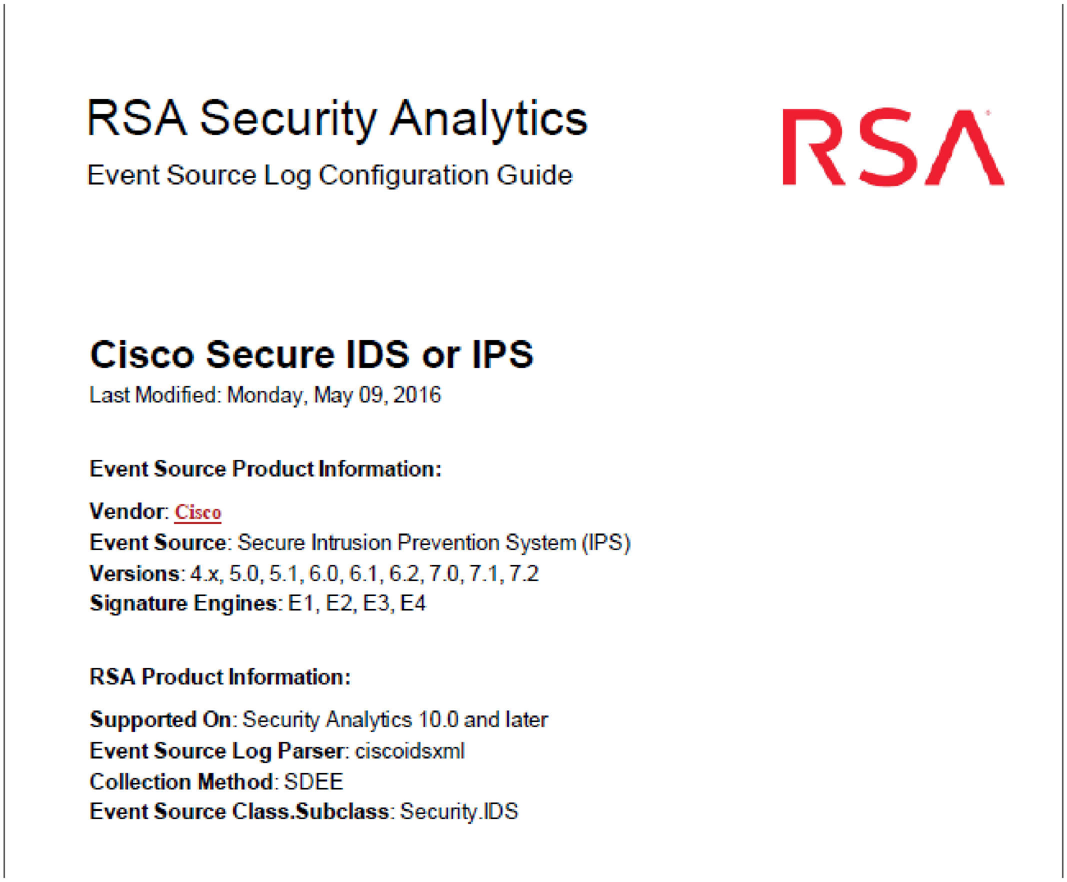
2 Verify that it is supported by the SDEE Collection Protocol.

3 Click on 📒 to retrieve the configuration instructions for the event source.

4 Verify that you downloaded the correct event source parser (for example, **ciscoidsxml**) from LIVE to the Log Decoder and enabled it.

Sample Configuration Instructions

The following illustration is taken from the Cisco Secure IDS or IPS configuration instructions.



RSA Security Analytics

Event Source Log Configuration Guide

Cisco Secure IDS or IPS

Last Modified: Monday, May 09, 2016

Event Source Product Information:

Vendor: Cisco
Event Source: Secure Intrusion Prevention System (IPS)
Versions: 4.x, 5.0, 5.1, 6.0, 6.1, 6.2, 7.0, 7.1, 7.2
Signature Engines: E1, E2, E3, E4

RSA Product Information:

Supported On: Security Analytics 10.0 and later
Event Source Log Parser: ciscoidsxml
Collection Method: SDEE
Event Source Class.Subclass: Security.IDS

Step 3. Start Service for Configured SDEE Collection Protocol

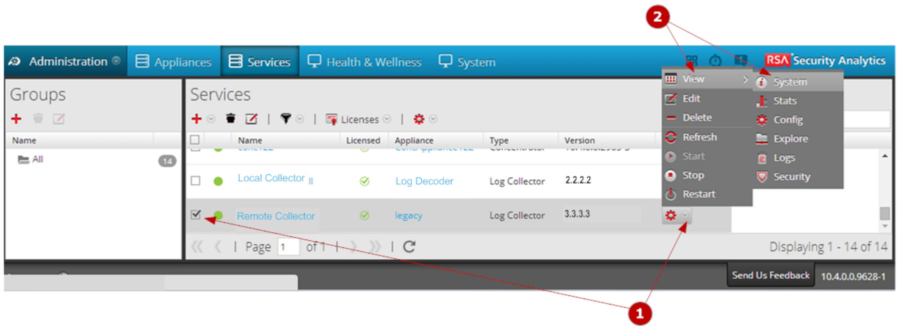
This topic tells you how to start a stopped SDEE collection service.

Return to Procedures

If an SDEE collection service has stopped, you may need to restart it or enable the automatic start of an individual service

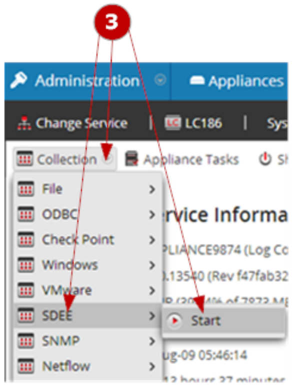
Procedure

The following figure shows you how to start a collection service. See the **Enable Automatic Start of Individual Services** topic in the *Log Collection Configuration Guide* if you want the service to start automatically.



1 Select a **Log Collector** service and click ⌄ under **Actions**.

2 Click **View** > **System**.



3 Click **Collection** > **SDEE** and click **Start**.

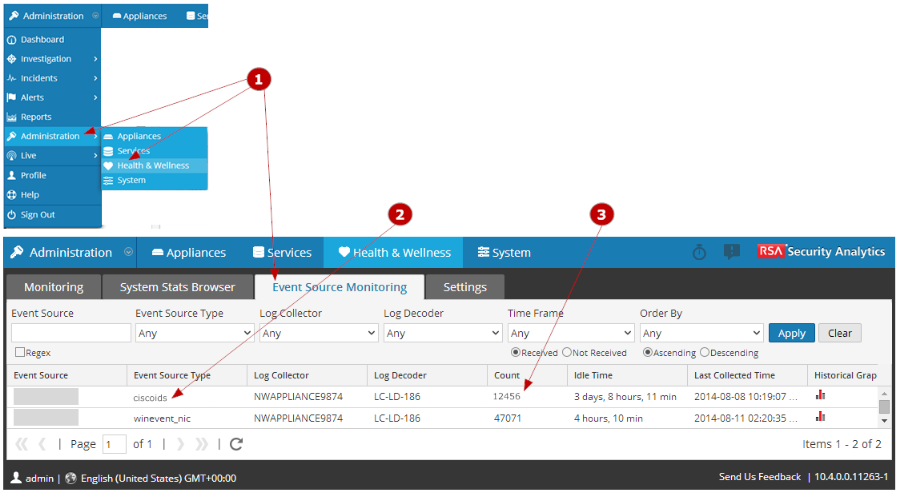
Step 4. Verify That SDEE Collection Is Working

This topic tells you what to check in Security Analytics to verify that you have configured SDEE Collection correctly. You need to verify that SDEE collection is configured correctly, otherwise it will not work.

Return to Procedures

Procedure

The following figure illustrates how you can verify that SDEE collection is working from the **Administration** > **Health & Wellness** > **Event Source Monitoring** tab.



Event Source	Event Source Type	Log Collector	Log Decoder	Time Frame	Order By
	Any	Any	Any	Any	Any
□ Regex				● Received ○ Not Received	● Ascending ○ Descending

Event Source	Event Source Type	Log Collector	Log Decoder	Count	Idle Time	Last Collected Time	Historical Grap
[redacted]	ciscoids	NWAPPLIANCE9874	LC-LD-186	12456	3 days, 8 hours, 11 min	2014-08-08 10:19:07 ...	
[redacted]	winevent_nic	NWAPPLIANCE9874	LC-LD-186	47071	4 hours, 10 min	2014-08-11 02:20:35 ...	

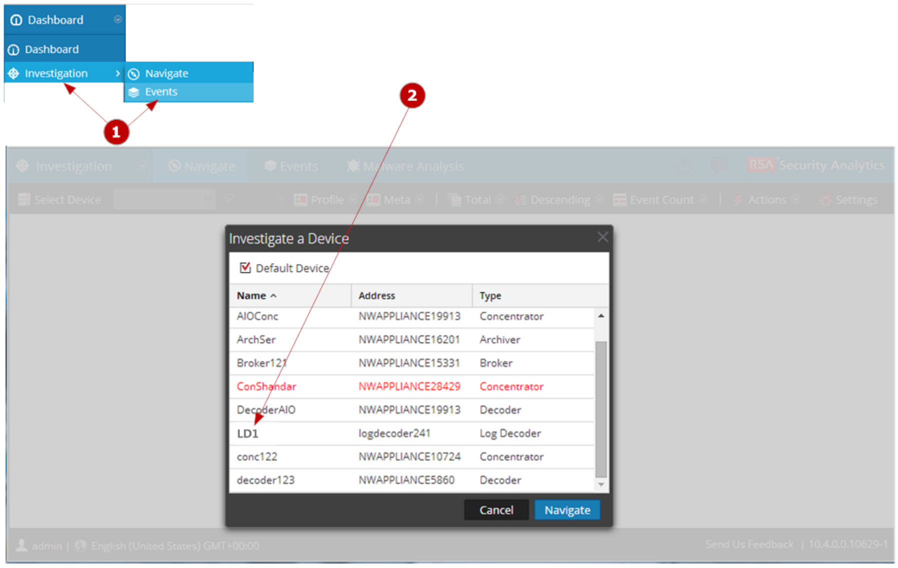
Page 1 of 1 | Items 1 - 2 of 2

1 Access the **Event Source Monitoring** tab from the **Administration** > **Health & Wellness** view.

2 Find an SDEE event source type (for example, **ciscoids**) in the **Event Source Type** column.

3 Look for activity in the **Count** column to verify that SDEE collection is accepting events.

The following figure illustrates how you can verify that SDEE collection is working from the **Investigation** > **Events** > view.



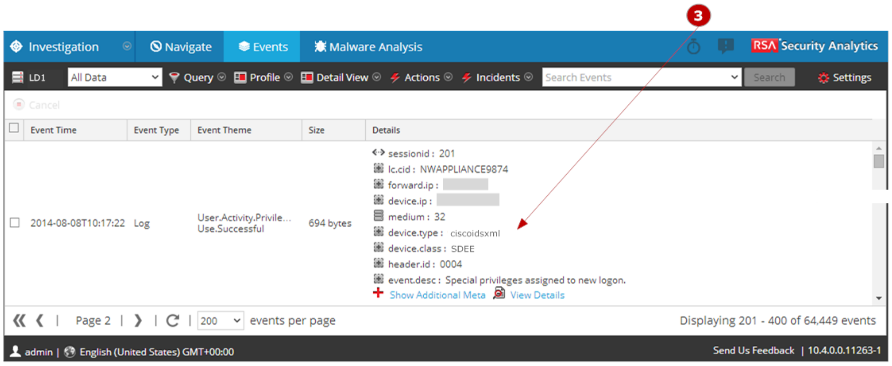
Investigate a Device

☑ Default Device

Name ^	Address	Type
AIOConc	NWAPPLIANCE19913	Concentrator
ArchSer	NWAPPLIANCE16201	Archiver
Broker121	NWAPPLIANCE15331	Broker
ConShandar	NWAPPLIANCE28429	Concentrator
DecoderAIO	NWAPPLIANCE19913	Decoder
LD1	logdecoder241	Log Decoder
conc122	NWAPPLIANCE10724	Concentrator
decoder123	NWAPPLIANCE5860	Decoder

1 Access the **Investigation > Events** view.

2 Select the Log Decoder (for example, **LD1**) collecting SDEE events in the **Investigate a Device** dialog.



☐	Event Time	Event Type	Event Theme	Size	Details
☐	2014-08-08T10:17:22	Log	User.Activity.Privile... Use.Successful	694 bytes	sessionid : 201 lc.cid : NWAPPLIANCE9874 forward.ip : [redacted] device.ip : [redacted] medium : 32 device.type : ciscoidsxml device.class : SDEE header.id : 0004 event.desc : Special privileges assigned to new logon. Show Additional Meta View Details

Page 2
200
events per page
Displaying 201 - 400 of 64,449 events
admin | English (United States) GMT+00:00
Send Us Feedback | 10.4.0.0.11263-1

3 Look for an SDEE event source parser (for example, **ciscoidsxml**) in the **Device Type** column to verify that SDEE collection is accepting events.

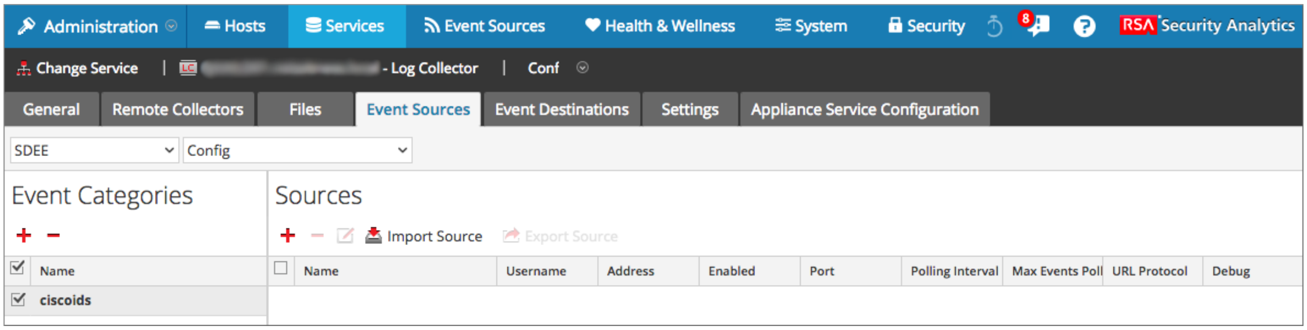
Reference - SDEE Event Source Configuration Parameters

This topic describes the Security service Event Exchange (SDEE) event source parameters.

Use the SDEE option on the Log Collector Config View Event Sources tab to add and maintain configuration parameters for collecting Intrusion Detection System (IDS) data (for example, Cisco Secure IDS messages) formatted under the SDEE standard.

To access the SDEE Event Source Configuration Parameters:

1. In the **Security Analytics** menu, select **Administration > Services.**
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⊙ under **Actions** and select **View > Config**.
4. In the **Event Sources** tab, select **SDEE/Config** from the drop-down menu.



SDEE | Config

Event Categories

☑	Name
☑	ciscoids

Sources

☐	Name	Username	Address	Enabled	Port	Polling Interval	Max Events Poll	URL Protocol	Debug

The SDEE/Config view in the Event Sources tab has two panels: Event Categories and Sources.

Event Categories Panel

In the Event Categories panel, you can add or delete the appropriate event source types.

Feature	Description
+	Displays the Available Event Source Types dialog from which you select the event source type for which you want to define parameters.
−	Deletes the selected event source types from the Event Categories panel.
□	Selects event source types.
Name	Displays the name of the event source types that you have added.

Available Event Sources Types Dialog

The Available Event Source Types dialog displays the list of supported event source types.

Feature	Description
□	Selects the event source type that you want to add.
Type	Display the event source types that are available to add.
Cancel	Closes the dialog without adding an event source type.
OK	Adds the selected event source type to the Event Categories panel.

Sources Panel

Use this panel to review, add, modify, and delete event sources.

Toolbar

The following table provides descriptions of the toolbar options.

Feature	Description
+	Displays the Add Source dialog in which you define the parameters for a Firewall host.

Feature	Description
−	Deletes the host that you selected.
✎	Opens the Edit Source dialog, in which you edit the parameters for the selected event source. Select multiple event sources and click ✎ to open the Bulk Edit Source dialog in which you can edit the parameters values for the selected event sources. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.
Import Source	Opens the Bulk Add Option dialog in which you can import hosts in bulk from a comma-separated values (CSV) file. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.
Export Source	Creates a .csv file that contains the parameters for the selected hosts. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.

Add or Modify Source Dialog

In this dialog, you add or modify a file directory for the selected event source.

Feature	Description
Source Parameters	Lists the parameters populated with the default values. Enter or modify the appropriate values.
Cancel	Closes the dialog without adding a file directory or saving the parameter values for the selected event sources.
OK	In the Add Source dialog, adds the file directory and its parameters. In the Modify Sources dialog, applies the parameter value changes for the selected event source.

Add or Edit Source Parameters

The following table provides descriptions of the source parameters.

Name	Description

Name	Description
Basic	
Name *	Name of the event source.
Username *	User name to authenticate with the event source.
Password *	Password to authenticate with the event source. **Caution:** The password is encrypted internally and is displayed in its encrypted form.
Address *	IP Address for the event source that is the IDS Sensor.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
Certificate Name	Certificate name for secure connections to use when the transport mode is https. Valid values are the certificates currently existing in your trust store that you created using the Settings tab. **Note:** If you leave this field blank, Security Analytics does not perform validation.
Advanced	
Port	Port number. A valid port number is any number within the 1 through 65535 range (443 default value).
SSL Version	Version of SSL through which the event source is configured to communicate. Valid values are: • tlsv1 (default) • sslv2 • sslv3 • sslv2
Include Raw Event Data	Select the checkbox to include the raw XML data for the event returned by the SDEE event source in the event data sent to the Log Decoder. The check box is not selected by default. **Note:** This parameter is only supported for content 3.0 data.

Name	Description
Save Raw XML Files	Select the check box to send raw data to **/var/netwitness/logcollector/runtime/sdee/saved_raw_events**. The check box is not selected by default.
Saved File Quota	Amount of space available for saved XML files. Valid value is the number of Megabytes, Kilobytes, or Gigabytes of space that you want to allocate. Security Analytics defaults to **100** Megabytes.
Subscription Event Types	(Only applies when you make initial subscription request.) Filters events for the specified Subscription event types (for example, IDS alerts). Default is **evIdsAlert**.
Force Subscription	(Only applies when you make initial subscription request.) Select the checkbox if you want the SDEE server to create a subscription even when maximum number of subscriptions are open. The checkbox is selected by default. **Note:** The server closes the existing subscription to accommodate new one.
Subscription Severity Filter	(Only applies when you make initial subscription request.) All events generated by an SDEE event source have a severity level assigned to them. Use this parameter to filter event messages by severity. If you leave this field blank, Security Analytics collects all the events regardless of severity level. For example, if you wanted to collected events with medium and high severity levels exclusively, you would specify the following character string in this parameter: **medium+high**
Subscription Time Offset	(Only applies when you make initial subscription request.) Default (time of subscription on). This parameter allows you to specify how far back in time (in seconds) to start pulling events.

Name	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify **180**, the collector schedules a polling of the event source every **180** seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. If you have a large number of event sources that you are polling, it may take longer than **180** seconds for the polling to start because the threads are busy.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Query Timeout	Value (in seconds) passed to the SDEE event source that instructs the server on how long to wait when there is no data.
URL Parameters	Appends parameters to the url string (for example, **/cgi-bin/sdee-server.cgi**).
URL Path	URL path for the SDEE server.
URL Protocol	Valid values are: • **http** • **https**

Name	Description
Debug	**Caution:** Only enable debugging (set this parameter to "On" or "Verbose") if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.

Tasks

Step 1. Configure SDEE Event Sources in Security Analytics

Troubleshoot SDEE Collection

This topic highlights possible problems that you may encounter with SDEE Collection and suggested solutions to these problems.

Troubleshoot SDEE Collection Issues

In general, you receive more robust log messages by disabling SSL.

You can select the Save Raw XML Files configuration parameter to save the raw XML files from the server to **/var/netwitness/logcollector/runtime/sdee/saved_sdee_files** to further investigate SDEE issues. The file name for these file contains the event source name and a timestamp. You can control the the amount of files (data) Security Analytics stores with the Saved File Quota configuration parameter. The value that you enter for the quota is the number of bytes Security Analytics stores, in kilobytes, megabytes, or gigabytes.

SNMP Collection Configuration Guide

This guide tells you how configure the SNMP collection protocol. This protocol accepts SNMP traps.

You must deploy Log Collection before you can configure the Check Point collection protocol.

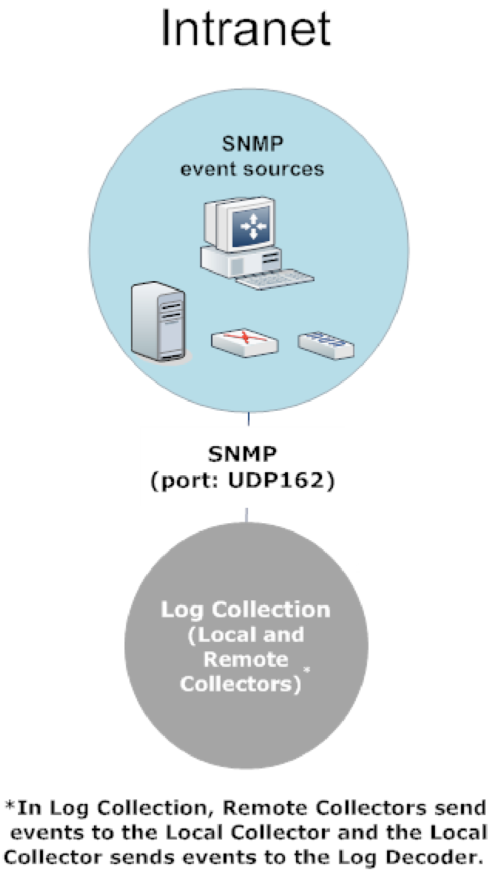
For deployment instructions, see Log Collection Deployment Guide.

The Basics

This guide tells you how to configure SNMP collection protocol which accepts SNMP traps.

Deployment Scenario

The following figure illustrates how you deploy the SNMP Collection Protocol in Security Analytics.


Intranet
SNMP
event sources
SNMP
(port: UDP162)
Log Collection
(Local and
Remote
Collectors)*
*In Log Collection, Remote Collectors send events to the Local Collector and the Local Collector sends events to the Log Decoder.

Procedures

Configure SNMP Collection Protocol in Security Analytics

You configure the Log Collector to use SNMP collection for an event source in the Event Source tab of the Log Collector parameter view. The following figure the basic workflow for configuring an event source for SNMP Collection in Security Analytics. Please refer to:

- Step 1. Configure SNMP Event Sources in Security Analyticsfor step-by-step instructions on how to configure events sources in Security Analytics tht use the SNMP Collection protocol.
- References - SNMP Collection Configuration Parametersfor a detailed description of each SNMP Collection Protocol parameter.

1. In the **Security Analytics** menu, select **Administration > Services.**
2. In the **Services** grid, select a **Log Collection** service.
3. Select ⚙ ⌄ > **View** > **Config** to display the **Log Collection** configuration parameter tabs.
4. Click the **Event Sources** tab.
5. Select **SNMP** as the collection protocol and select **Config**.
6. Click ✚ and select **SNMP** as the event source category.

   The event source category is part of the content you downloaded from Live.
7. Select **SNMP** as the collection protocol and select **SNMP v3 User Manager**.
8. Click ✚ to display the **Add SNMP User** dialog.
9. Define the **SNMP User** parameters and click **Save**

Configure Event Sources to Use SNMP Collection Protocol

You need to configure each event source that uses the SNMP Collection protocol to communicate with Security Analytics (see Step 2. Configure SNMP Event Sources to Send Events to Security Analytics).

Procedures

This topic provides an overview of the end-to-end sequential configuration procedure for the SNMP Collection protocol with a checklist that contains each configuration step.

Configuration steps for the SNMP collection protocol must occur in the specific sequence listed in which the procedures are presented.

SNMP Collection Configuration Checklist

Note: The steps in this list are in the order in which you must complete them.

Step	Description	√
1	Configure SNMP Event Sources in Security Analytics.	
2	Configure SNMP Event Sources to Send Events to Security Analytics.	
3	Start service for configured SNMP collection protocol.	
4	Verify that SDEE Collection is working.	

Step 1. Configure SNMP Event Sources in Security Analytics

This topic tells you how to configure SNMP event sources for the Log Collector.

After completing this procedure, you will have...

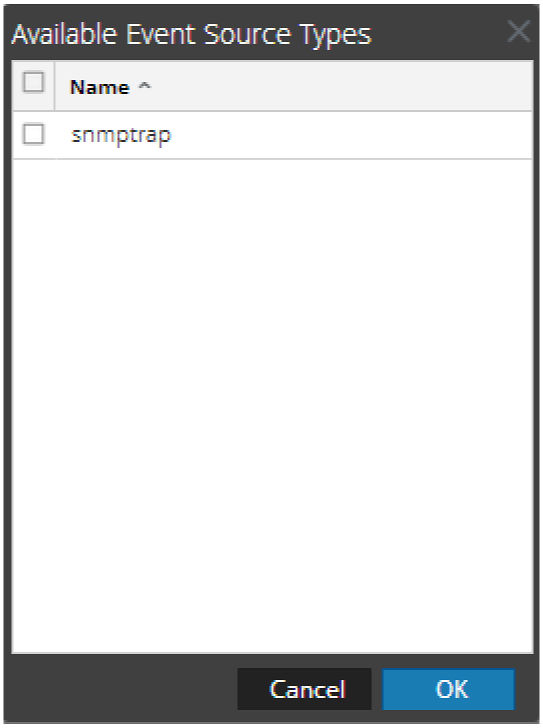
- Configured an SNMP event source.
- Modified an SNMP event source.

Return to Procedures

Procedures

Configure an SNMP Event Source

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config** >.
4. In the **Event Sources** tab, select **SNMP/Config** from the drop-down menu.
   The **Event Categories** panel displays the SNMP event sources that are configured, if any.
5. In the **Event Categories** panel toolbar, click ✚.
   The **Available Event Source Types** dialog is displayed.



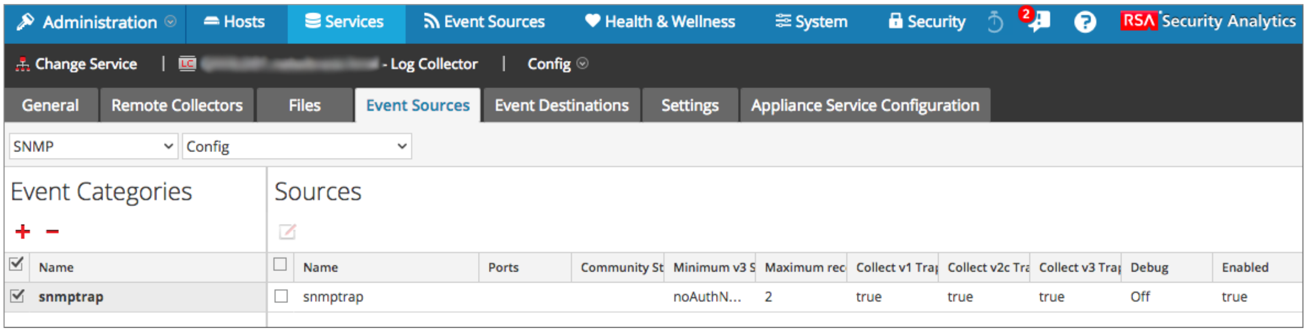
□	Name ^
□	snmptrap

6. Select an event source type (for example, **snmptrap**) and click **OK**.

   The newly added event source type is displayed in the **Event Categories** panel.

7. Select the new type in the **Event Categories** panel

   The new SNMP source dialog is displayed in the **Sources** panel.



☑	Name
☑	**snmptrap**

□	Name	Ports	Community St	Minimum v3 S	Maximum rec	Collect v1 Tra	Collect v2c Tra	Collect v3 Tra	Debug	Enabled
□	snmptrap			noAuthN...	2	true	true	true	Off	true

Modify an SNMP Event Source

1. In the **Security Analytics** menu, select **Administration > Services.**

2. In the **Services** grid, select a **Log Collector** service.

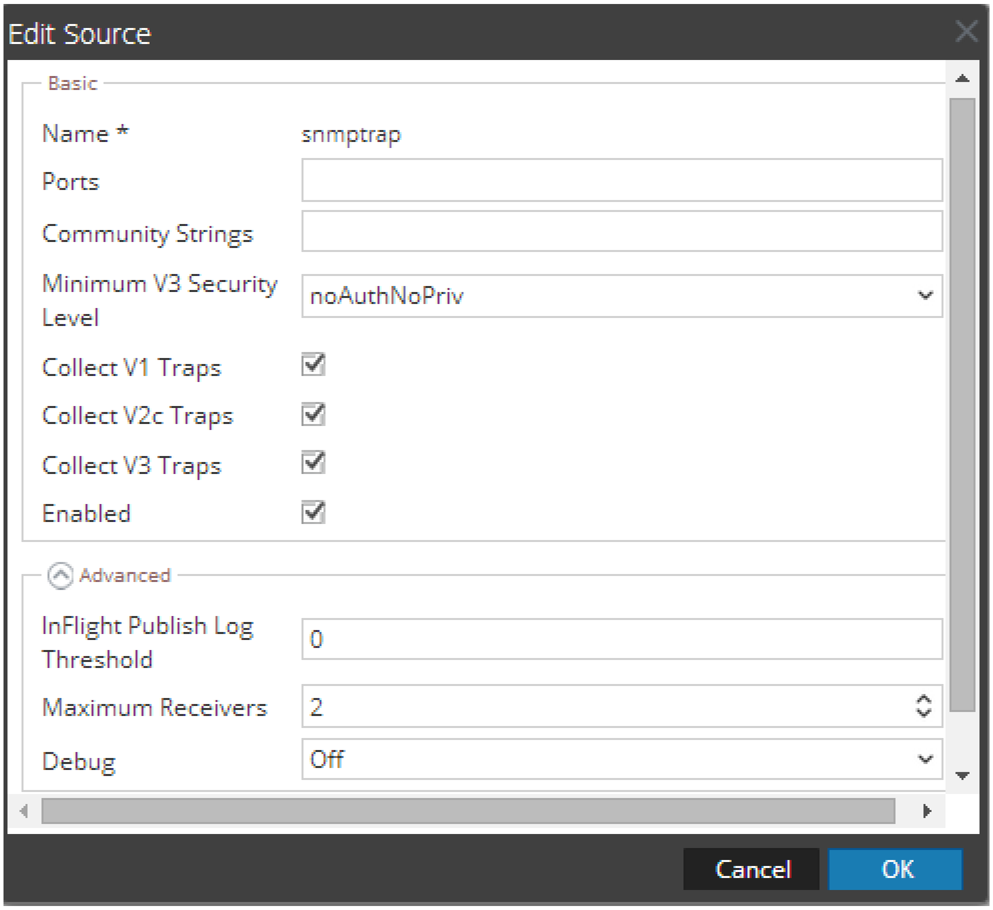
3. Click ⌄ under **Actions** and select **View > Config >**.

4. In **Event Sources** tab, select **SNMP/Config** from the drop-down menu.

5. Select an event source type (for example, **snmptrap**) from the **Event Categories** panel and click **OK**.

6. In the **Source** panel, select an event source and click ✎.

   The **Edit Source** dialog is displayed.



Basic

Name *	snmptrap
Ports	
Community Strings	
Minimum V3 Security Level	noAuthNoPriv
Collect V1 Traps	☑
Collect V2c Traps	☑
Collect V3 Traps	☑
Enabled	☑

Advanced

InFlight Publish Log Threshold	0
Maximum Receivers	2
Debug	Off

7. Modify the parameters that require changes and click **OK**.

   Security Analytics applies the parameter changes to the selected event source.

Parameters

Step 1. Configure SNMP Event Sources in Security Analytics

SNMP v3 User Manager Configuration Parameters

Step 2. Configure SNMP Event Sources to Send Events to Security Analytics

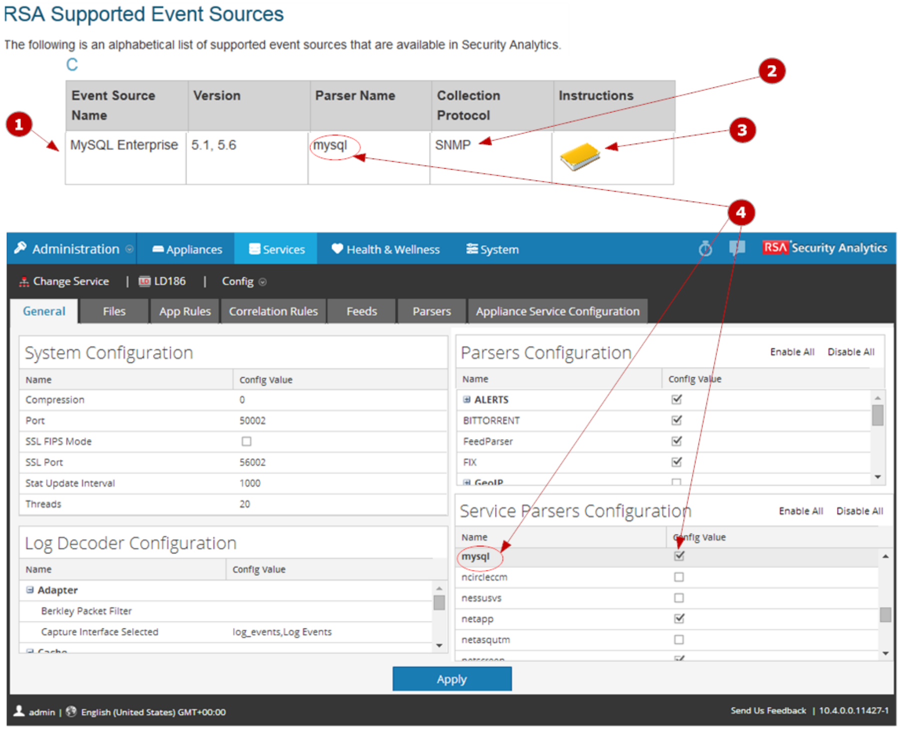
This topic tells you where to find the event sources currently supported for SNMP collection and the available configuration instructions for each event source.

To find the event sources currently supported for SNMP collection, see the Supported Event Sources list. Sample configuration instructions are provided below.

Procedure

Return to Procedures

The list of RSA Supported Event Sources is an alphabetized list of all the event sources currently supported by Security Analytics that identifies which event sources you can use with SNMP Collection.



RSA Supported Event Sources

The following is an alphabetical list of supported event sources that are available in Security Analytics.

C

Event Source Name	Version	Parser Name	Collection Protocol	Instructions
MySQL Enterprise	5.1, 5.6	mysql	SNMP	

System Configuration

Name	Config Value
Compression	0
Port	50002
SSL FIPS Mode	□
SSL Port	56002
Stat Update Interval	1000
Threads	20

Log Decoder Configuration

Name	Config Value
⊟ Adapter	
Berkley Packet Filter	
Capture Interface Selected	log_events,Log Events

Parsers Configuration

Name	Config Value
⊞ ALERTS	☑
BITTORRENT	☑
FeedParser	☑
FIX	☑
⊞ GeoIP	□

Service Parsers Configuration

Name	Config Value
mysql	☑
ncircleccm	□
nessusvs	□
netapp	☑
netasqutm	□

1 Find the name of the event source.

2 Verify that it is supported by the SNMP Collection Protocol.

3 Click on 📒 to display the configuration instructions for the event source.

4 Verify that you downloaded the correct event source parser (for example, **mysql)** from LIVE to the Log Decoder and enabled it.

Sample Configuration Instructions

The following illustration is taken from the MySQL Enterprise configuration instructions.

RSA Security Analytics

Event Source Log Configuration Guide

MySQL Enterprise

Last Modified: Monday, June 09, 2014

Event Source Product Information:

Vendor: MySQL
Event Source: MySQL Enterprise
Versions: 5.1 and 5.6

RSA Product Information:

Supported On: Security Analytics 10.0 and later
Event Source Log Parser: mysql
Collection Method: SNMP
Event Source Class.Subclass: Storage.Database

Step 3. Start Service for Configured SNMP Collection Protocol

This topic tells you how to start a stopped SNMP collection service.

You need to start a stopped SNMP collection service in order to make it work again. You also have the option to enable the automatic start of individual protocols if want the protocols to begin automatically.

Procedure

Return to Procedures

The following procedure tells you how to start a collection protocol. See the **Enable Automatic Start of Individual Protocols** topic in the *Log Collection Configuration Guide* if you want the protocol to start automatically.

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service and select ⚙ ⌄ > **View** > **System**.

   The **Services System** view is displayed.
3. Click **Collection** > **SNMP** > **Start**.

Step 4. Verify That SNMP Collection Is Working

This topic tells you what to check in Security Analytics to verify that you have configured SNMP Collection correctly.

Return to Procedures

You need to verify that SNMP Collection is configured correctly, otherwise the collection will not work.

Procedure

The following procedure tell you how you can verify that SNMP collection is working from the **Administration** > **Health & Wellness** > **Event Source Monitoring** tab.

1. In the **Security Analytics** menu, select **Administration** > **Health & Wellness**
2. Click the **Event Source Monitoring** tab.
3. Find **SNMP** in the **Event Source Type** column.
4. Look for activity in the **Count** column to verify that SNMP collection is accepting events.

References - SNMP Collection Configuration Parameters

This topic describes the SNMP event source configuration parameters.

SNMP collection event source configuration parameters have two parts each with a separate view, SNMP and SNMP v3 User Manager parameters.

- SNMP Event Source Configuration Parameters
- SNMP v3 User Manager Configuration Parameters

SNMP Event Source Configuration Parameters

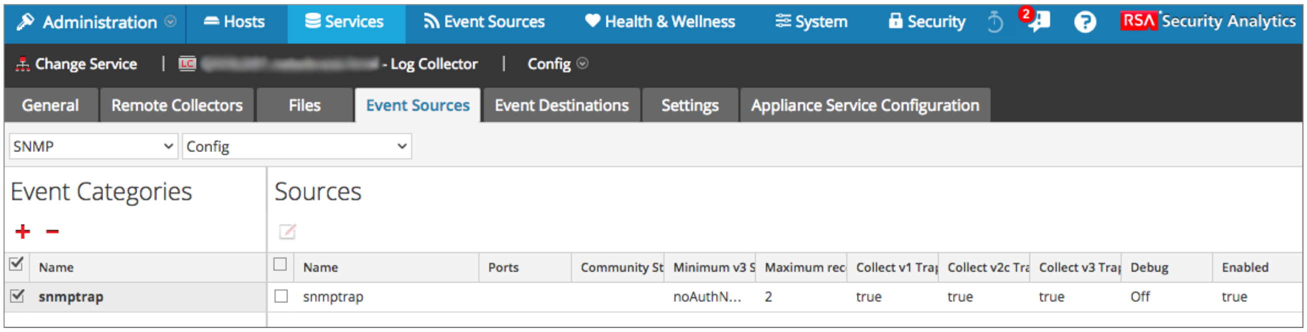
This topic describes the Simple Network Management Protocol (SNMP) event source parameters.

Simple Network Management Protocol (SNMP) is a set of internet standards for management of network services. SNMP includes a protocol, a schema for defining data, and data sets known as Management Information Bases (MIBs). MIBs include Internet standards and standards specific to vendors/services. SNMP entities include agents and managers. Agents are managed services that instrument various MIBs and make the data available to managers. Managers can retrieve the data from the managed services. The managed services can also notify managers asynchronously through a trap.

There are three versions of SNMP in widespread use: version 1, version 2c and version 3. Version 3 includes security and access control features.

To access the SNMP Event Source Configuration Parameters:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Event Sources** tab, select **SNMP/Config** from the drop-down menu.



☑	Name
☑	snmptrap

□	Name	Ports	Community St	Minimum v3 S	Maximum rec	Collect v1 Tra|	Collect v2c Tra	Collect v3 Tra|	Debug	Enabled
□	snmptrap			noAuthN...	2	true	true	true	Off	true

Features

The SNMP/Config view in the Event Sources tab has two panels: Event Categories and Sources.

Event Categories Panel

In the Event Categories panel, you can add or delete SNMP event source types.

Feature	Description
+	Displays the Available Event Source Types dialog from which you select the event source type for which you want to define parameters. **Note:** Security Analytics only supports a single event source, that is snmptrap, and adds snmptrap automatically when you add the event source type is added.
−	Deletes the selected event source types from the Event Categories panel.
✎	Selects event source types.
Name	Displays the name of the event source types that you have added.

Available Event Source Types Dialog

SNMP has a single event source type (category) called snmptrap. After you add snmptrap to the Event Categories panel, Security Analytics generates an event source called snmptrap to the Sources panel as well. Only a single event source is supported. You cannot add or delete it. Only the event source type (or category) can be added or deleted.

Feature	Description
□	Selects the event source type that you want to add.
Type	Displays the event source types that are available to add.
Cancel	Closes the dialog without adding an event source type.
OK	Adds the selected event source type to the Event Categories panel.

Sources Panel

Use this panel to review, add, modify, and delete event sources and their parameters for the event source type you selected in Event Sources.

Toolbar

The following table provides descriptions of the toolbar options.

Option	Description
✎	Opens the Modify Source dialog in which you modify the configuration parameters for the selected event source. When you select multiple event sources, opens the Bulk Edit Source dialog in which you can edit the parameters values for the selected event sources. After you save changes to the SNMP event source, Security Analytics prompts you to restart SNMP collection. When you restart SNMP collection, Security Analytics uses the changed parameter values
□	Selects event source type that you want to edit.

Edit Source Dialog

In this dialog, you add or modify an event source for the selected event source.

Feature	Description
SNMP Source Parameters	Lists the parameters populated with the default values. Enter or modify the appropriate values.

Feature	Description
Cancel	Closes the dialog without adding an event source or saving the parameter values for the selected event source.
OK	In the Add Sources dialog, adds the event source and its parameters. In the Modify Sources dialog, applies the parameter value changes for the selected event source.

SNMP Source Parameters

The following table provides descriptions of the SNMP source parameters.

Option	Description
Basic	
Name *	The name of the SNMP source (for example, snmptrap).
Ports *	The UDP and UDP/IPv6 port numbers. A valid port number is any number within the 1 through 65535 range with 162 as the default port. You can enter multiple ports by separating each with a comma. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.
Minimum v3 Security Level	The minimum required security level in v3 traps received. Valid values are: • **noAuthNoPriv** - no authentication and no privacy. • **authNoPriv** - authentication but no privacy. Security Analytics ignores any traps with a security level of noAuthNoPriv. • **authPriv** - authentication and privacy. Security Analytics ignores any traps with a security level of noAuthNoPriv or authNoPriv.
Collect v1 Traps	Select the check box to collect SNMP version 1 traps. The check box is selected by default. If you do not select this parameter, Security Analytics ignores SNMP v1 traps.

Collect v2c Traps	Select the check box to collect SNMP version 2c traps. The check box is selected by default. If you do not select this parameter, Security Analytics ignores SNMP v2c traps.
Collect v3 Traps	Select the check box to collect SNMP version 3 traps. The check box is selected by default. If you do not select this parameter, Security Analytics ignores SNMP v3 traps.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
Community Strings	Comma separated list of community strings. This parameter contains no values by default. • **no values specified -** Security Analytics collects all SNMP traps. • **values specified** - if the community string in the received trap is not in the list specified, Security Analytics ignores the trap.
Advanced	
Maximum receivers	Maximum number of receiver resources in the 1 to 50 range. The default value is conditional based on the SNMP type(category) and defaults to 2 for the snmp type. If you change this parameter, the change does not take effect until you restart collection or restart the Log Collector service.
InFlight Publish Log Threshold	The threshold value in published events at which Security Analytics creates an informational message. Valid values are: • **0** = disable the message • **100-100000000** = published event threshold

Debug	**Caution:** Only enable debugging (set this parameter to "On" or "Verbose") if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables/disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. The debug logging is verbose, so limit the number of event sources to minimize performance impact. If you change this value, the change takes effect immediately (no restart required).

Tasks

Step 1. Configure SNMP Event Sources in Security Analytics

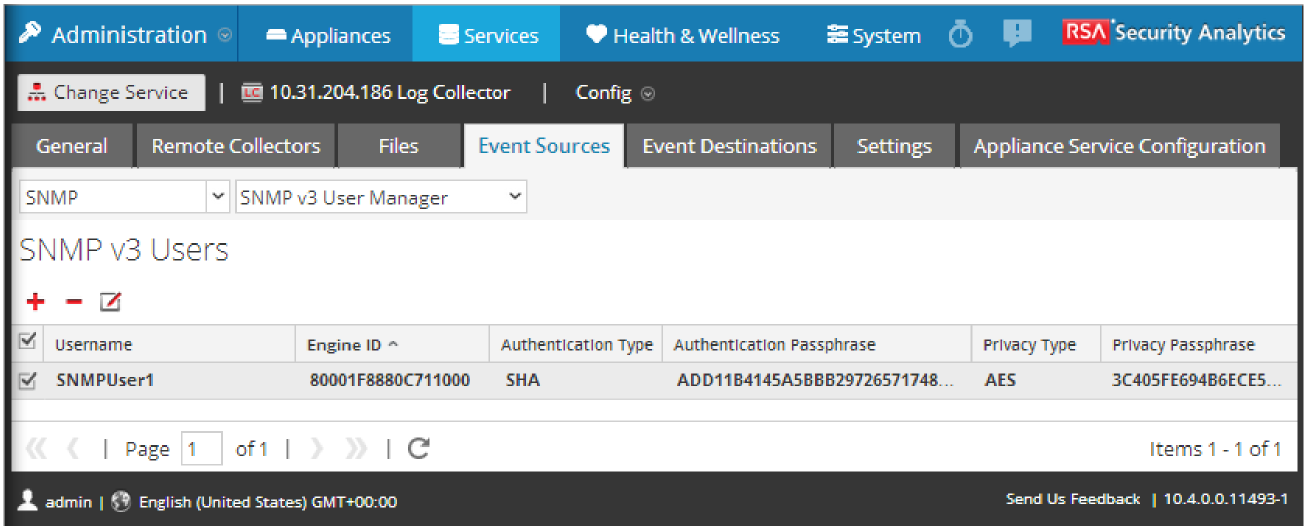
SNMP v3 User Manager Configuration Parameters

This topic describes the SNMP v3 User Manager configuration parameters.

To access the SNMP v3 User Manager Configuration Parameters:

1. In the **Security Analytics** menu, select **Administration >Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View > Config**.

4. In the **Event Sources** tab, select **SNMP/SNMP v3User Manager** from the drop-down menu.



SNMP | SNMP v3 User Manager

SNMP v3 Users

☑	Username	Engine ID ^	Authentication Type	Authentication Passphrase	Privacy Type	Privacy Passphrase
☑	SNMPUser1	80001F8880C711000	SHA	ADD11B4145A5BBB29726571748...	AES	3C405FE694B6ECE5...

The SNMP/SNMP v3 User Manager view in the Event Sources tab has one panel: SNMP v3 Users.

SNMP v3 Users

In the SNMP v3 Users panel, you can add, delete, or edit SNMP v3 users.

Feature	Description
+	Displays the Add SNMP dialog in which you define an SNMP v3 user parameters.
−	Deletes the selected SNMP v3 users.
✎	Displays the Edit SNMP dialog in which you edit SNMP v3 user parameters. After you save changes to the SNMP user configuration, the Security Analytics prompts to restart SNMP collection. When you restart SNMP collection, Security Analytics uses the changed parameter values.
☐	Selects SNMP v3 users.
SNMP v3 User Parameters	Displays the each SNMP v3 user that you have added with its parameters.

Add or Edit SNMP User Dialog

In this dialog, you add or modify SNMP v3 user parameters.

Feature	Description
Username *	User name (or more accurately in SNMP terminology, security name). Security Analytics uses this parameter and the Engine ID parameter to create a user entry in the SNMP engine of the collection service. The Username and Engine ID combination must be unique (for example, **logcollector**).
Engine ID	(Optional) Engine ID of the event source. For all event sources sending SNMP v3 traps to this collection service, you must add the username and engine id of the sending event source. For all event sources sending SNMPv3 informs, you must add just the username with a blank engine id." For example, **Username = logcollector** and **Engine ID = 80001F8880C71100000410449510000**.
Authentication Type	(Optional) Authentication protocol. Valid values are: • **None (default)** - only security level of noAuthNoPriv can be used for traps sent to this service • **SHA** - Secure Hash Algorithm • **MD5** - Message Digest Algorithm
Authentication Passphrase	Optional if you do not have the Authentication Type set. Authentication passphrase.
Privacy Type	(Optional) Privacy protocol. You can only set this parameter if Authentication Type parameter is set. Valid values are: • **None (default)** • **AES** - Advanced Encryption Standard • **DES** - Data Encryption Standard
Privacy Passphrase	Optional if you do not have the PrivacyType set. Privacy passphrase
Close	Closes the dialog without adding the SNMP v3 user or saving modifications to the parameters.
Save	Adds the SNMP v3 user parameters or saves modifications to the parameters.

Tasks

Configure SNMP v3 Users

Troubleshoot SNMP Collection

This topic highlights possible problems that you may encounter with SNMP Collection and suggested solutions to these problems.

Troubleshoot SNMP Collection Issues

To retrieve events from SNMP, you must configure the parameters so that they verify and decrypt SNMPv3 Traps and Inform messages from the event sources.

- For Inform messages, you must specify the user (security name, in SNMPv3 terminology) without an Engine ID.
- For Trap messages, you must specify the user with the Engine ID of the event sender.

You must set the Debug parameter to **Verbose** to receive invalid Trap and Inform log messages.

Security Analytics returns the following types of error messages in the log files for the SNMP collection protocol.

Log Messages	(d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: snmpv3_parse: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: msgMaxSize 65507 received (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing begun... (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: Unknown Engine ID. (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing has begun (offset 55) (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: getting user (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing completed. (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: snmpv3_parse: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: msgMaxSize 65507 received (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing begun... (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: Unknown User(logcollector) (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing has begun (offset 55) (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: getting user logcollector (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 13:43:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing completed.
Possible Cause	Missing Username or Engine ID for SNMP trap
Solutions	Make sure that the event source sends the Username and Engine ID that you configured for the event source in the SNMP v3 User Manager Configuration Parameters.

Log Messages	(d) 2013-May-02 16:47:26 [SnmpTrapCollection(TraceLog)] Net-SNMP: snmptrapd: (d) 2013-May-02 16:47:26 [SnmpTrapCollection(TraceLog)] Net-SNMP: Running global handlers (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: snmpv3_parse: (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: msgMaxSize 65507 received (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing begun... (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: match on user logcollector (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: Verification succeeded. (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: usm: (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: USM processing completed. (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: snmp_parse: (d) 2013-May-02 16:47:38 [SnmpTrapCollection(TraceLog)] Net-SNMP: Parsed SNMPv3 message (secName:logcollector, secLevel:authPriv): ASN.1 parse error in message
Possible Cause	The Authentication Type and or Passphrase used by the event source was different from the values you configured.
Solutions	Make sure that Authentication Type and the Authentication Passphrase sent by the event source matches parameters you configured for the event source in the SNMP v3 User Manager Configuration Parameters.

VMware Collection Configuration Guide

This guide tells you how to configure the VMware collection protocol. This protocol collects events from a VMware virtual infrastructure.

You must deploy Log Collection before you can configure the Check Point collection protocol.

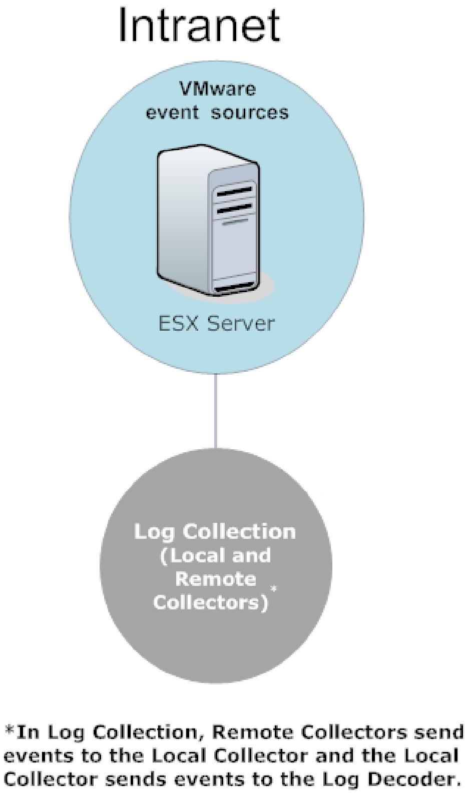
For deployment instructions, see Log Collection Deployment Guide.

The Basics

This guide tells you how to configure VMware collection protocol which collects events from a VMware virtual infrastructure.

Deployment Scenario

The following figure illustrates how you deploy the VMware Collection Protocol in Security Analytics.


Intranet
VMware event sources
ESX Server
Log Collection (Local and Remote Collectors)*
*In Log Collection, Remote Collectors send events to the Local Collector and the Local Collector sends events to the Log Decoder.

Procedures

Configure VMware Collection Protocol in Security Analytics

You configure the Log Collector to use VMware collection for an event source in the event Source tab of the Log Collector parameter view. The following procedure explains the basic workflow for configuring an event source for VMware Collection in Security Analytics. Please refer to:

- Step 1. Configure VMware Event Sources in Security Analytics for step-by-step instructions on how to configure event sources in Security Analytics that use the VMware Collection protocol.
- References - VMware Event Source Configuration Parameters for a detailed description of each VMware Collection Protocol parameter.

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a Log Collection service.
3. Click ⌄ under **Actions** and select **View > Config**.

   The **Log Collector Config** view is displayed.
4. Click the **Event Sources** tab.
5. Select **VMware** as the collection protocol, and select **Config**.
6. Click + and select the event source category name (for example, **vmware-events**). The event source category is part of the content you downloaded from LIVE.
7. Select a category and click + in the **Sources** panel toolbar.
8. Specify the basic parameters required for the VMware event source.
9. Click ⌄ and specify additional parameters that enhance how the VMware protocol handles event collection for the event source.

Configure Event Sources to Use VMware Collection Protocol

You need to configure each event source that uses the VMware Collection protocol to communicate with Security Analytics (see Step 2. Configure VMware Event Sources to Send Events to Security Analytics).

Procedures

This topic provides an overview of the end-to-end sequential configuration procedure for the VMware Collection protocol with a checklist that contains each configuration step.

Configuration steps for the VMware collection protocol must occur in the specific sequence listed in the table below.

VMware Collection Configuration Checklist

Note: The steps in this list are in the order in which you must complete them.

Step	Description
1	Configure VMware Event Sources in Security Analytics.
2	Configure VMware Event Sources to Send Events to Security Analytics.
3	Start service for configured VMware collection protocol.
4	Verify that VMware Collection is working.

Step 1. Configure VMware Event Sources in Security Analytics

This topic tells you how to configure VMware event sources for the Log Collector.

After completing this procedure, you will have...

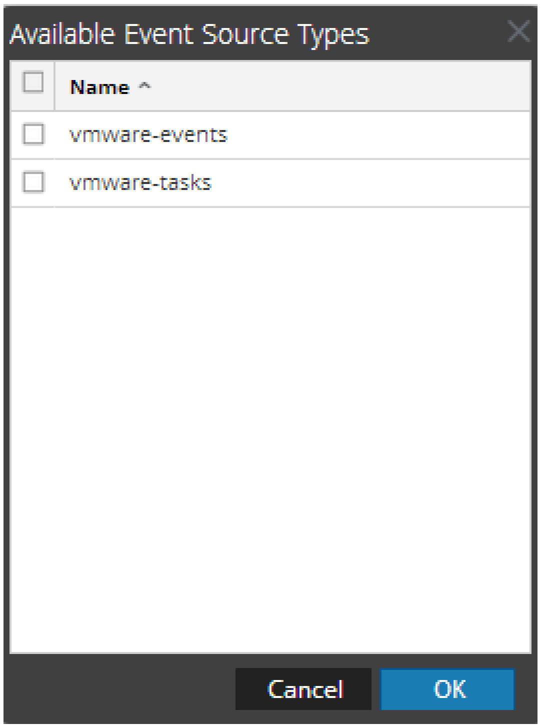
- Configured a VMware event source.
- Modified a VMware event source.

Return to Procedures

Procedures

Configure a VMware Event Source

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. In the **Event Sources** tab, select **VMware/Config** from the drop-down menu.
   The **Event Categories** panel displays the VMware event sources that are configured, if any.
5. In the **Event Categories** panel toolbar, click ✚.



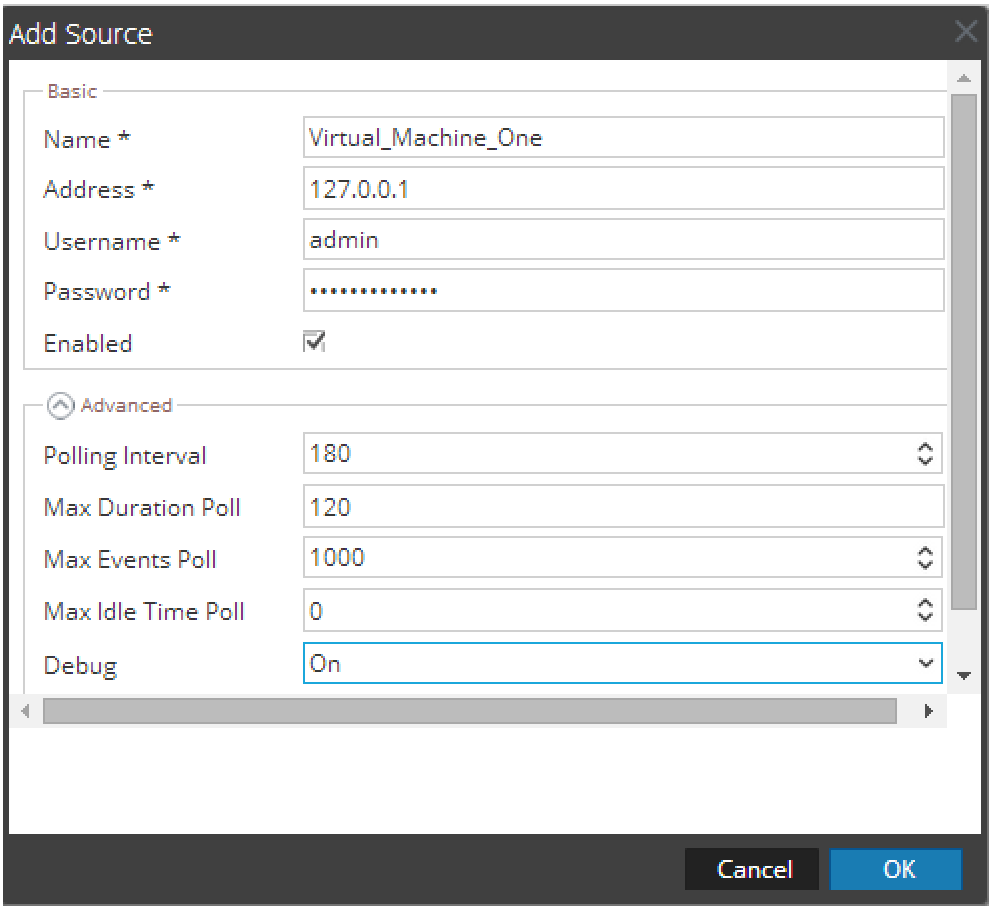
The newly added event source type is displayed in the **Event Categories** panel.

6. Select the new type in the **Event Categories** panel and click ✚ in the **Sources** toolbar.

   The **Add Source** dialog is displayed.

7. Add a **Name**, **Username** and **Password**, modify any other parameters that require changes, and click **OK**.

   > **Caution:** If you need to enter the domain name as part of the Username, you must use a double-backslash as a separator. For example, if the domain|username is corp\smithj, you must specify corp\\smithj.



Add Source

Basic

Name * Virtual_Machine_One

Address * 127.0.0.1

Username * admin

Password * ••••••••••••••

Enabled ☑

Advanced

Polling Interval 180

Max Duration Poll 120

Max Events Poll 1000

Max Idle Time Poll 0

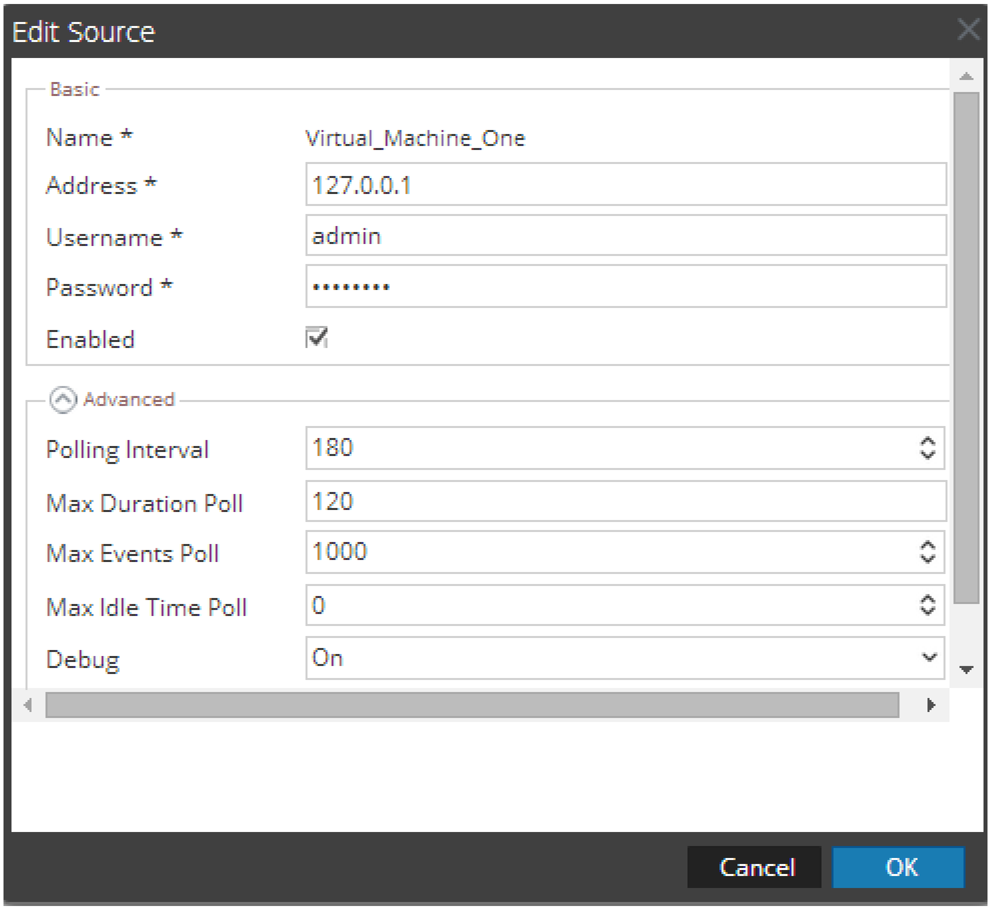
Debug On

The new event source is displayed in the list.

Modify a VMware Event Source

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.
4. Select **VMware/Config** from the drop-down menu.
5. In the **Event Source** list, select an event source and click ✎.

   The **Edit Source** dialog is displayed.



Name * Virtual_Machine_One

Address * 127.0.0.1

Username * admin

Password * ••••••••

Enabled ☑

Polling Interval 180

Max Duration Poll 120

Max Events Poll 1000

Max Idle Time Poll 0

Debug On

6. Modify the parameters that require changes and click **OK**.

   Security Analytics applies the parameter changes to the selected event source.

Parameters

References - VMware Event Source Configuration Parameters

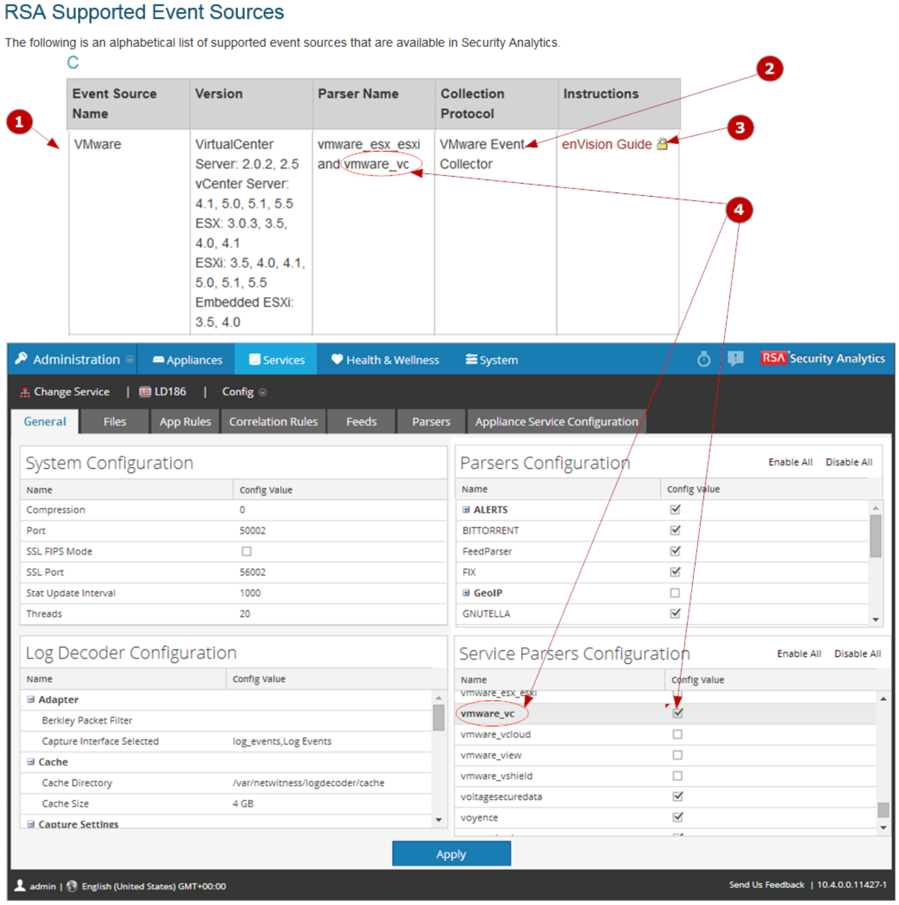
Step 2. Configure VMware Event Sources to Send Events to Security Analytics

This topic tells you where to find the event sources currently supported for VMware collection and the available configuration instructions for each event source.

Supported Event Sources List

Return to Procedures

The list of RSA Supported Event Sources is an alphabetized of all the event sources currently supported by Security Analytics that identifies which event sources you can use with VMware Collection.



RSA Supported Event Sources

The following is an alphabetical list of supported event sources that are available in Security Analytics.

C

Event Source Name	Version	Parser Name	Collection Protocol	Instructions
VMware	VirtualCenter Server: 2.0.2, 2.5 vCenter Server: 4.1, 5.0, 5.1, 5.5 ESX: 3.0.3, 3.5, 4.0, 4.1 ESXi: 3.5, 4.0, 4.1, 5.0, 5.1, 5.5 Embedded ESXi: 3.5, 4.0	vmware_esx_esxi and vmware_vc	VMware Event Collector	enVision Guide

System Configuration

Name	Config Value
Compression	0
Port	50002
SSL FIPS Mode	□
SSL Port	56002
Stat Update Interval	1000
Threads	20

Log Decoder Configuration

Name	Config Value
⊟ **Adapter**	
Berkley Packet Filter	
Capture Interface Selected	log_events,Log Events
⊟ **Cache**	
Cache Directory	/var/netwitness/logdecoder/cache
Cache Size	4 GB
⊟ **Capture Settings**	

Parsers Configuration

Name	Config Value
⊞ **ALERTS**	☑
BITTORRENT	☑
FeedParser	☑
FIX	☑
⊞ **GeoIP**	□
GNUTELLA	☑

Service Parsers Configuration

Name	Config Value
vmware_esx_esxi	□
vmware_vc	☑
vmware_vcloud	□
vmware_view	□
vmware_vshield	□
voltagesecuredata	☑
voyence	☑

1 Find the name of the event source.

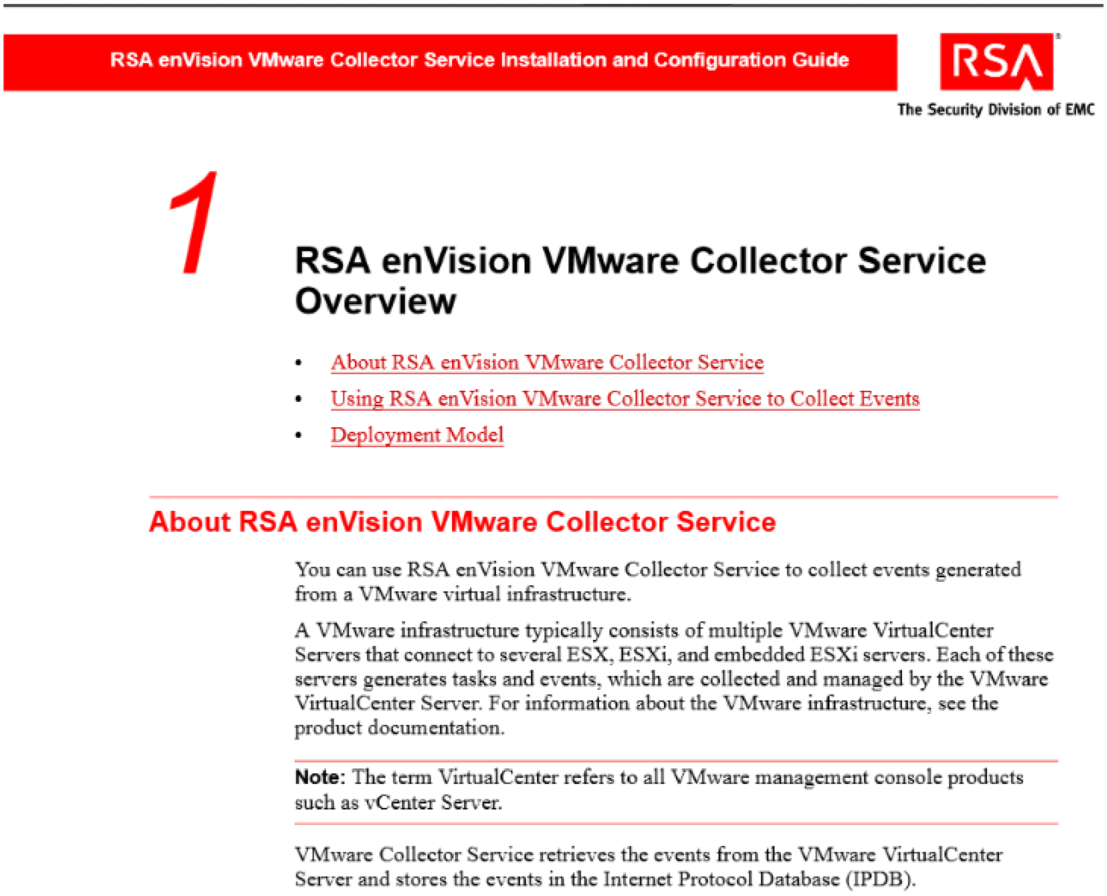
2 Verify that it is supported by the VMware Collection Protocol.

3 Click on 🔒 to retrieve the configuration instructions for the event source.

4 Verify that you downloaded the correct event source parser (for example, **vmare_vc**) from LIVE to the Log Decoder and enabled it.

Sample Configuration Instructions

The following illustration is taken from the VMware Collector Service configuration instructions.



RSA enVision VMware Collector Service Installation and Configuration Guide

RSA The Security Division of EMC

1

RSA enVision VMware Collector Service Overview

- About RSA enVision VMware Collector Service
- Using RSA enVision VMware Collector Service to Collect Events
- Deployment Model

About RSA enVision VMware Collector Service

You can use RSA enVision VMware Collector Service to collect events generated from a VMware virtual infrastructure.

A VMware infrastructure typically consists of multiple VMware VirtualCenter Servers that connect to several ESX, ESXi, and embedded ESXi servers. Each of these servers generates tasks and events, which are collected and managed by the VMware VirtualCenter Server. For information about the VMware infrastructure, see the product documentation.

Note: The term VirtualCenter refers to all VMware management console products such as vCenter Server.

VMware Collector Service retrieves the events from the VMware VirtualCenter Server and stores the events in the Internet Protocol Database (IPDB).

Step 3. Start Service for Configured VMware Collection Protocol

This topic tells you how to start a stopped VMware collection service.

If a VMware collection service has stopped, you will need to start it again in order to make it work. You can also refer to the Enable Automatic Start of Individual Services topic in the Log Collection Configuration Guide if you want the service to start automatically.

Procedure

To start a collection service:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. Select a Log Collector service and, in the **Actions** column, click ⌄ > **View** > **System**.

   The **Services System** view is displayed.
3. In the toolbar, click **Collection** > **VMware** and click **Start**.

Step 4. Verify That VMware Collection Is Working

This topic tells you what to check in Security Analytics to verify that you have configured VMware Collection correctly.

If VMware Collection is not configured correctly, it does not work. You can verify that it works in the Health & Wellness view.

Procedure

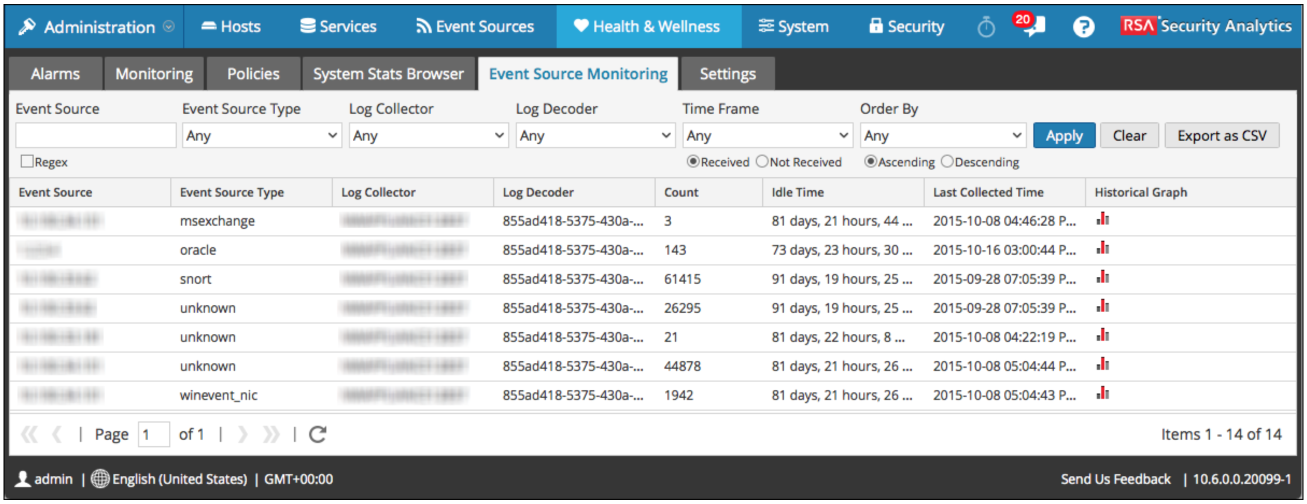
Return to Procedures

To verify that VMware Collection is working:

1. In the **Security Analytics** menu, select **Administration** > **Health & Wellness**.

   The **Health & Wellness** view is displayed with the **Alarms** tab open.

2. Click the **Event Source Monitoring** tab.



Event Source: (blank) □Regex
Event Source Type: Any
Log Collector: Any
Log Decoder: Any
Time Frame: Any ●Received ○Not Received
Order By: Any ●Ascending ○Descending

Event Source	Event Source Type	Log Collector	Log Decoder	Count	Idle Time	Last Collected Time	Historical Graph
[redacted]	msexchange	[redacted]	855ad418-5375-430a-...	3	81 days, 21 hours, 44 ...	2015-10-08 04:46:28 P...	
[redacted]	oracle	[redacted]	855ad418-5375-430a-...	143	73 days, 23 hours, 30 ...	2015-10-16 03:00:44 P...	
[redacted]	snort	[redacted]	855ad418-5375-430a-...	61415	91 days, 19 hours, 25 ...	2015-09-28 07:05:39 P...	
[redacted]	unknown	[redacted]	855ad418-5375-430a-...	26295	91 days, 19 hours, 25 ...	2015-09-28 07:05:39 P...	
[redacted]	unknown	[redacted]	855ad418-5375-430a-...	21	81 days, 22 hours, 8 ...	2015-10-08 04:22:19 P...	
[redacted]	unknown	[redacted]	855ad418-5375-430a-...	44878	81 days, 21 hours, 26 ...	2015-10-08 05:04:44 P...	
[redacted]	winevent_nic	[redacted]	855ad418-5375-430a-...	1942	81 days, 21 hours, 26 ...	2015-10-08 05:04:43 P...	

Page 1 of 1 Items 1 - 14 of 14

3. Find a VMware event source (for example, **vmware_vc**) in the **Event Source Type** column.

4. Look for activity in the **Count** column to verify that VMware collection is accepting events.

References - VMware Event Source Configuration Parameters

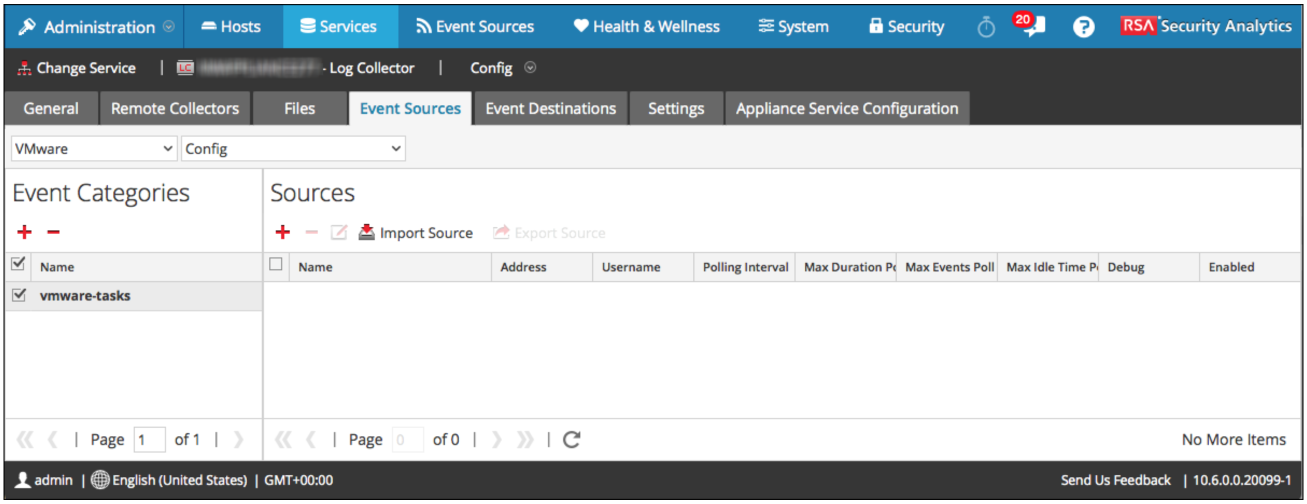
This topic describes the VMware event source parameters.

You use the VMware option on the Log Collector Config View Event Sources tab to add and maintain configuration parameters for VMware event sources. These event sources generate events from a VMware virtual infrastructure. The infrastructure typically consists of multiple VMware vCenter Servers that connect to several ESX, ESXi, and embedded ESXi servers. Each of the vCenter servers collects and manages tasks and events. Events can be any message generated by a VMware event source (for example, an alarm). Tasks are jobs that you schedule to perform.

To access the VMware Event Source Configuration Parameters:

1. In the **Security Analytics** menu, select **Administration > Services**
2. In the **Services** grid, select a Log Collector service.
3. Click ⌄ under **Actions** and select **View > Config**.

   The **Service Config** view is displayed with the **General** tab open.
4. Click the **Event Sources** tab.
5. Select VMware from the drop-down menu.



Event Categories

☑	Name
☑	vmware-tasks

Sources

□	Name	Address	Username	Polling Interval	Max Duration P	Max Events Poll	Max Idle Time P	Debug	Enabled

The VMware view in the Event Sources tab has two panels: Event Categories and Sources.

Event Categories Panel

In the Event Categories panel, you can add or delete the appropriate event source types.

Feature	Description
+	Displays the Available Event Source Types dialog from which you select the event source type for which you want to define parameters.
−	Deletes the selected event source types from the Event Categories panel.
□	Selects event source types.
Name	Displays the name of the event source types that you have added.

Available Event Sources Types Dialog

The Available Event Source Types dialog displays the list of supported event source types.

Feature	Description
□	Selects the event source type that you want to add.
Type	Display the event source types that are available to add.
Cancel	Closes the dialog without adding an event source type.

Feature	Description
OK	Adds the selected event source type to the Event Categories panel.

Sources Panel

Use this panel to review, add, modify, and delete event sources and their parameters for the event source type you selected in the Event Categories panel.

Caution: For VMware event collection, Security Analytics pulls all the currently existing events the first time that you start collecting VMware events.

Toolbar

The following table provides descriptions of the toolbar options.

Feature	Description
+	Displays the Add Source dialog in which you define the parameters for a Firewall host.
−	Deletes the host that you selected.
✎	Opens the Edit Source dialog, in which you edit the parameters for the selected event source. Select multiple event sources and click ✎ to open the Bulk Edit Source dialog in which you can edit the parameters values for the selected event sources. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.
Import Source	Opens the Bulk Add Option dialog in which you can import hosts in bulk from a comma-separated values (CSV) file. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.
Export Source	Creates a .csv file that contains the parameters for the selected hosts. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.

Add or Modify Sources Dialog

In this dialog, you add or modify an event source for the selected event source.

Feature	Description
Source Parameters	Lists the parameters populated with the default values. Enter or modify the appropriate values.
Cancel	Closes the dialog without adding an event source or saving the parameter values for the selected event source.
OK	In the **Add Sources** dialog, adds the event source and its parameters. In the **Modify Sources** dialog, applies the parameter value changes for the selected event source.

Source Parameters

The following table provides descriptions of the source parameters.

Name	Description
	Basic
Name *	Name of the server on which VMware is running.
Address *	IP Address of the VMware server. (127.0.0.1 is the default value).
Username *	User name that the Log Collector uses to connect to the VMware server. You must specify a user name when you create the event source. **Caution:** If you need to enter the domain name as part of the Username, you must use a backslash as a separator For example, if the **domain\username** is **corp\smithj** , you must specify **corp\\smithj**.
Password *	Password that the Log Collector uses to connect to the VMware server. **Caution:** The password is encrypted internally and is displayed in its encrypted form.
Enabled	Select the check box to enable the event source configuration to start collection. The check box is selected by default.
	Advanced

Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify **180**, the collector schedules a polling of the event source every **180** seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. If you have a large number of event sources that you are polling, it may take longer than **180** seconds for the polling to start because the threads are busy.
Max Duration Poll	The maximum duration of polling cycle (how long the cycle lasts) in seconds.
Max Idle Time Poll	Maximum idle time, in seconds, of a polling cycle. **0** indicates no limit. **300** is the default value.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Debug	**Caution:** Only enable debugging (set this parameter to "On" or "Verbose") if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.
Cancel	Closes the dialog without adding an event source type.
OK	Adds the parameters for the event source.

Tasks

Step 2. Configure VMware Event Sources to Send Events to Security Analytics

Troubleshoot VMware Collection

This topic suggests how to resolve problems you may encounter with the VMware collection protocol.

Security Analytics informs you of Log Collector problems or potential problems in the following two ways:

- Log files.
- Health and Wellness Monitoring view

Log Files

If you have an issue with a particular event source collection protocol, you can review debug logs to investigate this issue. Each event source has a Debug parameter that you can enable (set parameter to On or Verbose) to capture these logs.

Only enable debugging if you have a problem with this event source and you need to investigate this problem. If you have Debug enabled all the time it will adversely affect the performance of the Log Collector.

Security Analytics has a set of error messages associated with Log Collection that it includes in log files. To access these files:

Health and Wellness Monitoring

Health and Wellness monitoring makes you aware of potential hardware and software problems in a timely manner so that you can avoid to outages. RSA recommends that you monitor the Log Collector statistical fields to make sure that the service is
operating efficiently and is not at or near the maximum values you have configured. You can monitor the statistics (Stats) described in the **Administration > Health & Wellness** view.

Windows Collection Configuration Guide

This guide tells you how configure the Windows collection protocol. This protocol collects events from Windows machines that support the Microsoft Windows model.

You must deploy Log Collection before you can configure the Windows collection protocol.

For deployment instructions, see Log Collection Deployment Guide.

The Basics

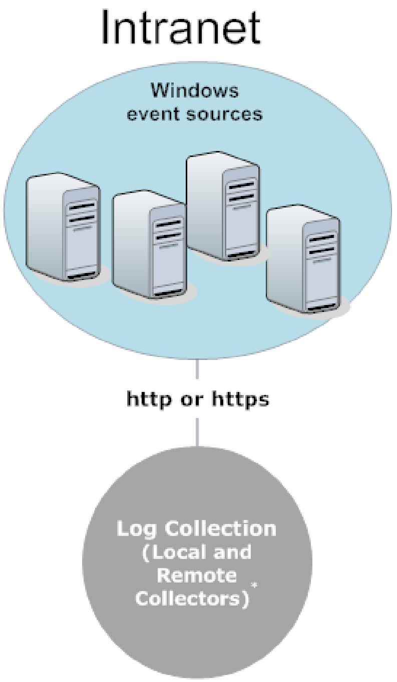
This guide tells you how to configure Windows collection protocol which collects events from Windows machines that support the Microsoft Windows model. Windows 6.0 is an event logging and tracing framework included in the operating system beginning with Microsoft Windows Vista and Windows Server 2008.

How Windows Collection Works

The Log Collector service collects events from Microsoft Windows event sources.

Deployment Scenario

The following figure illustrates how you deploy the Windows Collection Protocol in Security Analytics.



*In Log Collection, Remote Collectors send events to the Local Collector and the Local Collector sends events to the Log Decoder.

Procedures

Configure Windows Collection Protocol in Security Analytics

You configure to the Log Collector to use Windows collection for an event source in the Event Source tab of the Log Collector parameter view. The following procedure explains the basic workflow for configuring an event source for Windows Collection in Security Analytics. Please refer to:

- Step 1. Configure Windows Event Sources in Security Analyticsfor step-by-step instructions on how to configure events sources in Security Analytics that use the Windows Collection protocol.
- Windows Event Source Configuration Parameters for a detailed description of each Windows Collection Protocol parameter.

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. Select a **Log Collection** service.
3. Click ⚙ ⌄ > **View** > **Config**.

   The Log Collection configuration parameter tabs are displayed.

4. Click the **Event Sources** tab.
5. Select **Windows** as the collection protocol and select **Config**.
6. Click + and define a Windows alias (**Add Source**).
7. Select the alias and click +.
8. Define a Windows host.
9. Click **Test Connection** to validate connection with Windows event source.

Configure Event Sources to Use Windows Collection Protocol

You need to configure each event source that uses the Windows Collection protocol to communicate with Security Analytics (see Step 2. Configure Windows Event Sources to Send Events to Security Analytics).

Procedures

This topic provides an overview of the end-to-end sequential configuration procedure for the Windows Collection protocol with a checklist that contains each configuration step.

Configuration steps for the Windows collection protocol must occur in the specific sequence listed in the table below.

Windows Collection Configuration Checklist

Note: The steps in this list are in the order in which you must complete them.

Step	Description	√
1	Configure Windows Event Sources in Security Analytics.	
2	Configure Windows Event Sources to Send Events to Security Analytics.	

Step	Description	√
3	Start service for configured Windows collection protocol.	
4	Verify that Windows Collection is working.	

Step 1. Configure Windows Event Sources in Security Analytics

This topic tells you how to configure Windows event sources for the Log Collector.

After completing this procedure, you will have:

- Configured a Windows event source.
- Modified a Windows event source.
- Determined the channel name and add It to a Windows event source.

Return to Procedures

Procedures

Configure a Windows Event Source

Add Windows Event Source

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click ⌄ under **Actions** and select **View** > **Config**.

4. In the **Event Sources** tab, select **Windows/Config** from the drop-down menu.

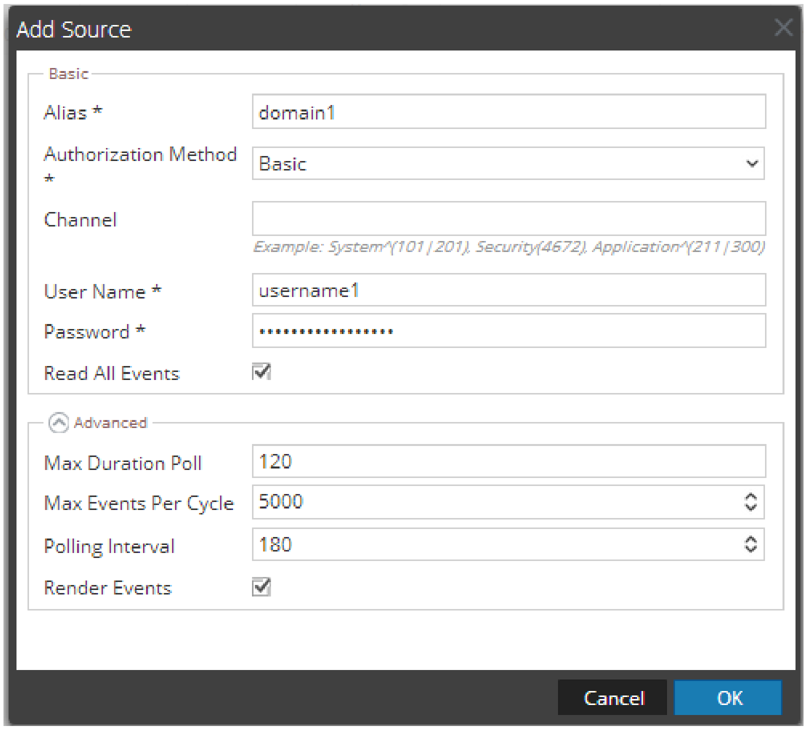
   The **Event Categories** panel is displayed with the Windows event sources that are configured, if any.

Configure Event Source (Alias)

1. Click + in the **Event Categories** panel toolbar.

   The **Add Event Source** dialog is displayed.

2. Specify values for the parameters and click **OK**.



Add Source

Basic

Alias *	domain1
Authorization Method *	Basic
Channel	Example: System^(101|201), Security(4672), Application^(211|300)
User Name *	username1
Password *	•••••••••••••••••
Read All Events	☑

Advanced

Max Duration Poll	120
Max Events Per Cycle	5000
Polling Interval	180
Render Events	☑

The newly added Windows event source is displayed in the **Event Categories** panel.

Add Event Source Host

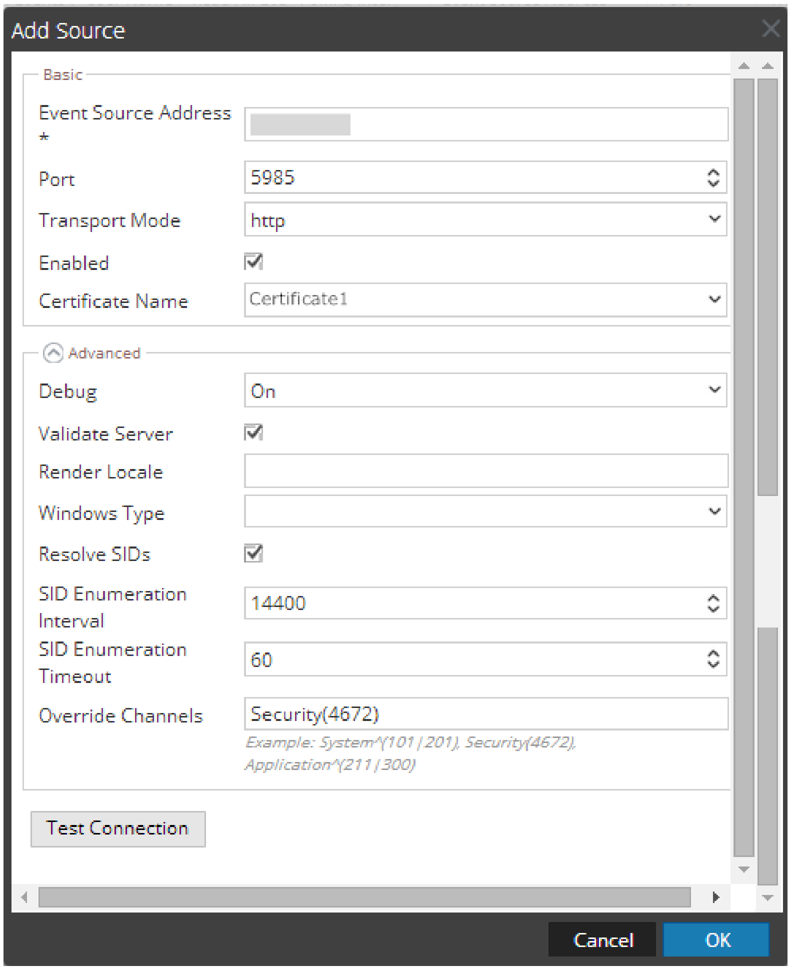
1. Select the new event source (alias) in the **Event Categories** panel.

   The **Hosts** panel is activated.

2. Click + in the **Hosts** panel toolbar.

   The **Add Source** dialog is displayed.

3. Specify values for the **Host** parameters.



Event Source Address *	[redacted]
Port	5985
Transport Mode	http
Enabled	☑
Certificate Name	Certificate1
Debug	On
Validate Server	☑
Render Locale	
Windows Type	
Resolve SIDs	☑
SID Enumeration Interval	14400
SID Enumeration Timeout	60
Override Channels	Security(4672) *Example: System^(101 | 201), Security(4672), Application^(211 | 300)*

4. Click **Test Connection**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

   > **Note:** Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and the Security Analytics displays an error message.

5. If the test is successful, click **OK**. The newly added host is displayed in the **Hosts** panel.

Modify a Windows Event Source

To modify a Windows event source:

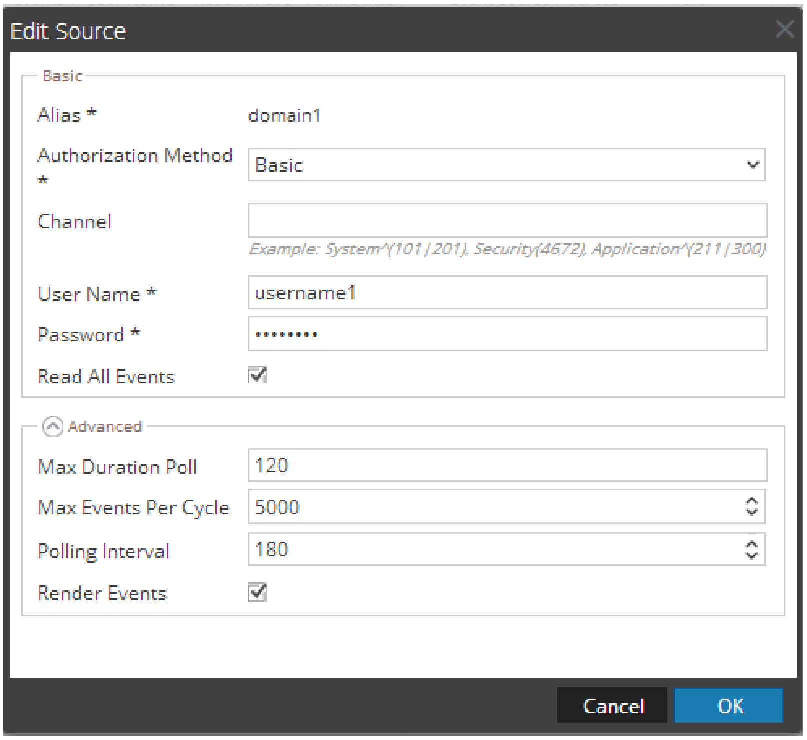
1. In the **Security Analytics** menu, select **Administration** > **Services**.

2. In the **Services** grid, select a **Log Collector** service.

3. Click under **Actions** and select **View > Config.**
4. In the **Event Sources** tab, select **Windows/Config** from the drop-down menu.
5. Modify the source parameters.
   a. In the **Event Categories** panel, select a source and click .

      The **Edit Source** dialog is displayed.

   b. Modify the source parameters that require changes and click **OK**.



Edit Source

Basic

Alias * domain1

Authorization Method * Basic

Channel

Example: System^(101|201), Security(4672), Application^(211|300)

User Name * username1

Password * ••••••••

Read All Events ☑

Advanced

Max Duration Poll 120

Max Events Per Cycle 5000

Polling Interval 180

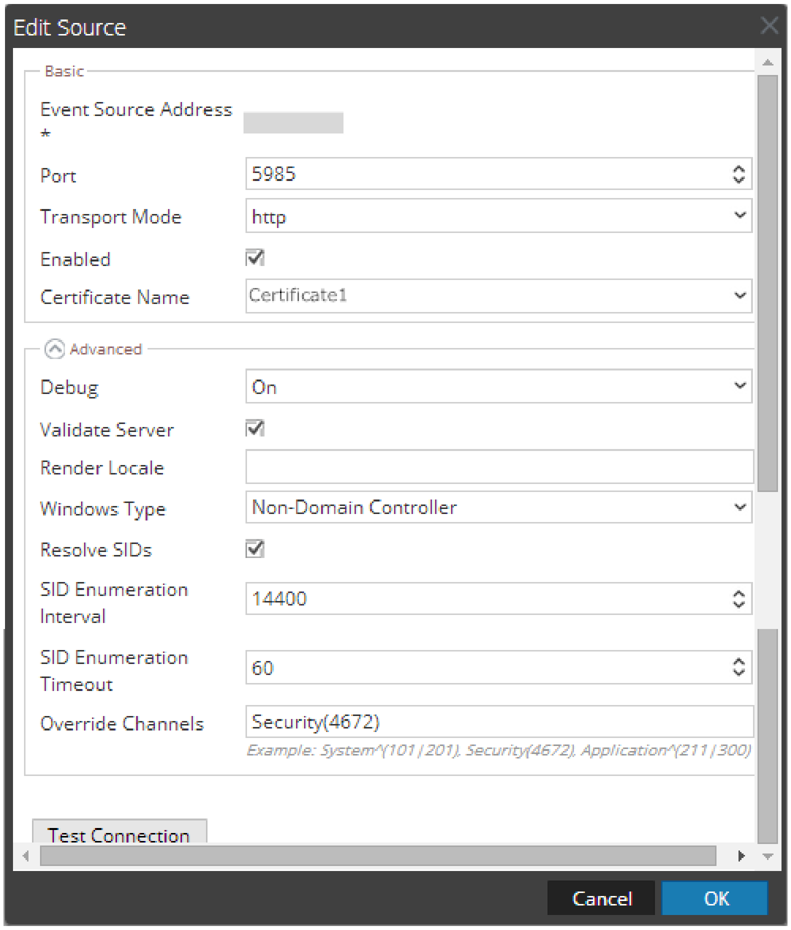
Render Events ☑

Security Analytics applies the parameter changes to the selected source.

6. Modify the event source host:
   a. In the **Hosts** panel, select a host and click .

      The **Edit Source** dialog is displayed.

   b. Modify the host parameters that require changes and click **OK**.



Edit Source

Basic

Event Source Address *	
Port	5985
Transport Mode	http
Enabled	☑
Certificate Name	Certificate1

Advanced

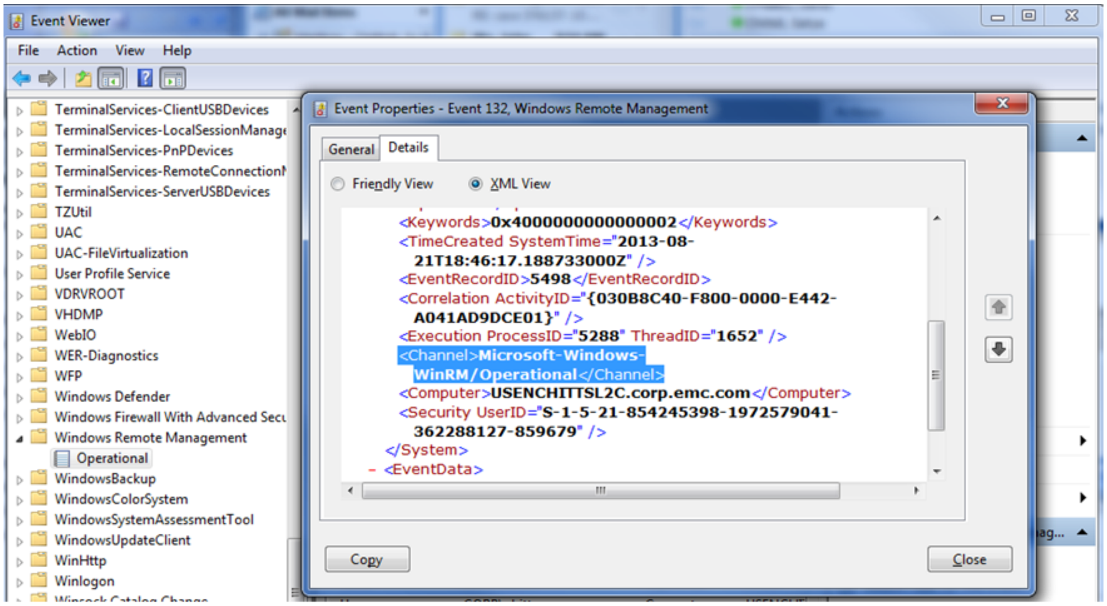
Debug	On
Validate Server	☑
Render Locale	
Windows Type	Non-Domain Controller
Resolve SIDs	☑
SID Enumeration Interval	14400
SID Enumeration Timeout	60
Override Channels	Security(4672) *Example: System^(101 | 201), Security(4672), Application^(211 | 300)*

Security Analytics applies the parameter changes to selected host.

Determine the Channel Name and Add It to a Windows Event Source

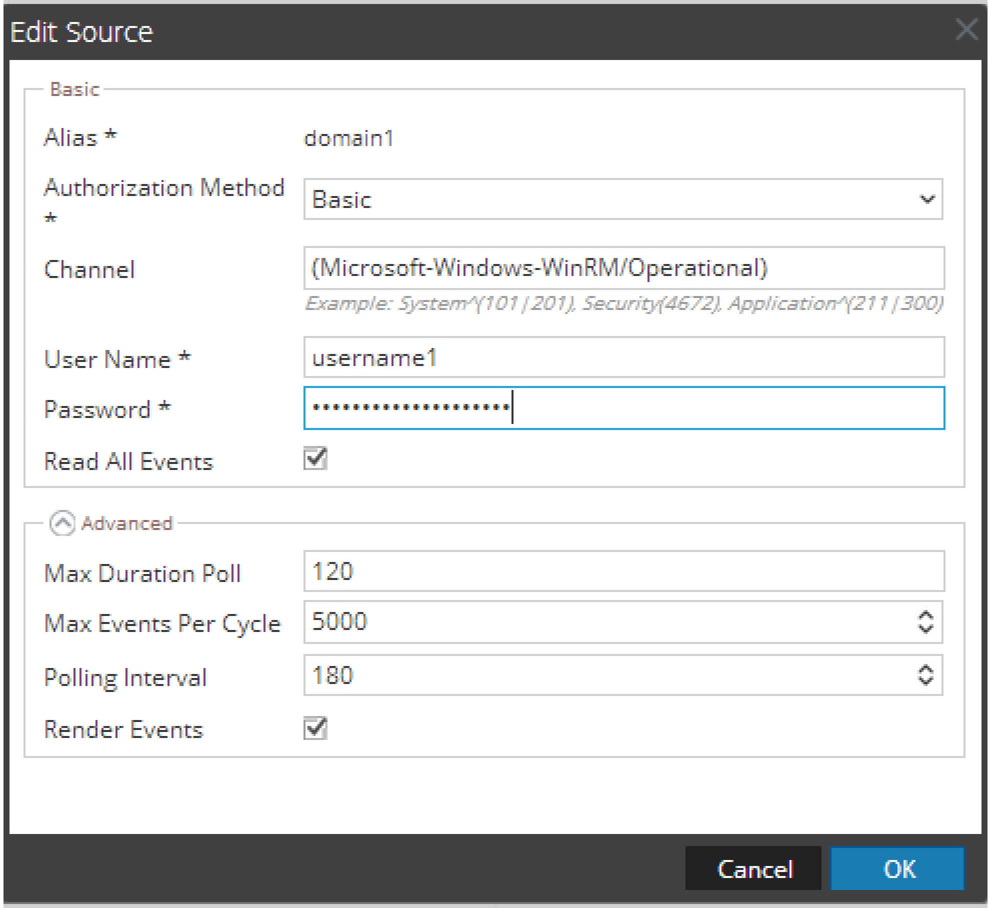
To find an unknown channel name and add it to a Windows event source:

1. On the Windows event source, select the channel that you want.
2. Click **Details** tab and find the channel field and that is the channel name (for example, **Microsoft-Windows-WinRM/Operational**).


Event Viewer
File Action View Help
TerminalServices-ClientUSBDevices
TerminalServices-LocalSessionManage
TerminalServices-PnPDevices
TerminalServices-RemoteConnection
TerminalServices-ServerUSBDevices
TZUtil
UAC
UAC-FileVirtualization
User Profile Service
VDRVROOT
VHDMP
WebIO
WER-Diagnostics
WFP
Windows Defender
Windows Firewall With Advanced Secu
Windows Remote Management
Operational
WindowsBackup
WindowsColorSystem
WindowsSystemAssessmentTool
WindowsUpdateClient
WinHttp
Winlogon
Event Properties - Event 132, Windows Remote Management
General
Details
○ Friendly View
● XML View
Copy
Close

```
    <Keywords>0x4000000000000002</Keywords>
    <TimeCreated SystemTime="2013-08-
      21T18:46:17.188733000Z" />
    <EventRecordID>5498</EventRecordID>
    <Correlation ActivityID="{030B8C40-F800-0000-E442-
      A041AD9DCE01}" />
    <Execution ProcessID="5288" ThreadID="1652" />
    <Channel>Microsoft-Windows-
      WinRM/Operational</Channel>
    <Computer>USENCHITTSL2C.corp.emc.com</Computer>
    <Security UserID="S-1-5-21-854245398-1972579041-
      362288127-859679" />
  </System>
- <EventData>
```

3. Edit the Event Source in Security Analytics, add channel to the **Channel** parameter, and click **OK**. For example:



Alias *	domain1
Authorization Method *	Basic
Channel	(Microsoft-Windows-WinRM/Operational) *Example: System^(101|201), Security(4672), Application^(211|300)*
User Name *	username1
Password *	•••••••••••••••••••
Read All Events	☑
Max Duration Poll	120
Max Events Per Cycle	5000
Polling Interval	180
Render Events	☑

Parameters

Windows Event Source Configuration Parameters

Configure Kerberos Realm

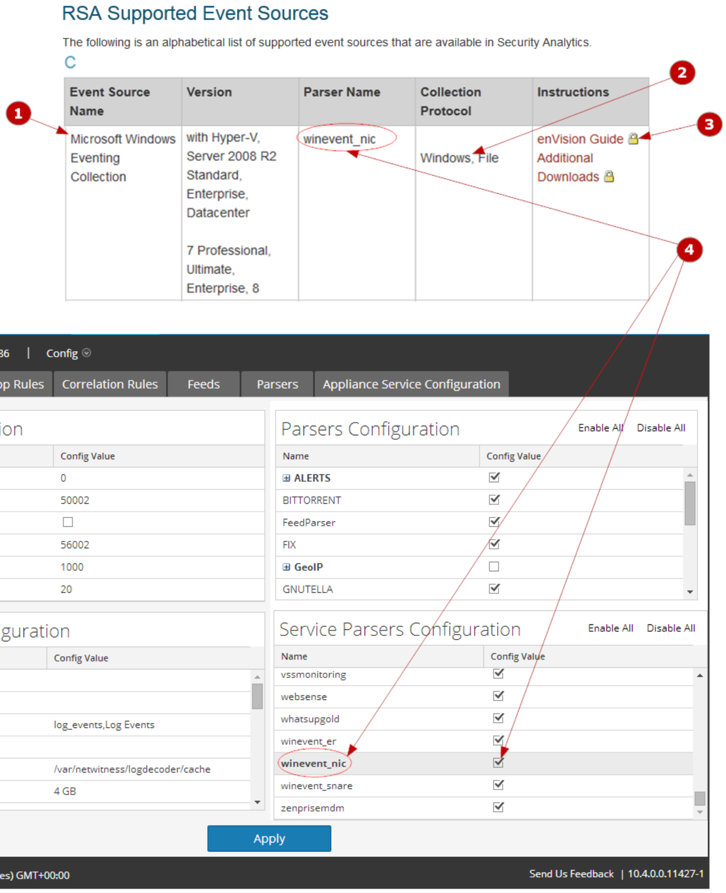
Step 2. Configure Windows Event Sources to Send Events to Security Analytics

This topic tells you where to find the event sources currently supported for Windows collection and the available configuration instructions for each event source.

Supported Event Sources List

Return to Procedures

The list of RSA Supported Event Sources is an alphabetized list of all the event sources currently supported by Security Analytics that identifies which event sources you can use with Windows Collection.



RSA Supported Event Sources

The following is an alphabetical list of supported event sources that are available in Security Analytics.

C

Event Source Name	Version	Parser Name	Collection Protocol	Instructions
Microsoft Windows Eventing Collection	with Hyper-V, Server 2008 R2 Standard, Enterprise, Datacenter 7 Professional, Ultimate, Enterprise, 8	winevent_nic	Windows, File	enVision Guide Additional Downloads

System Configuration

Name	Config Value
Compression	0
Port	50002
SSL FIPS Mode	□
SSL Port	56002
Stat Update Interval	1000
Threads	20

Log Decoder Configuration

Name	Config Value
⊟ Adapter	
Berkley Packet Filter	
Capture Interface Selected	log_events,Log Events
⊟ Cache	
Cache Directory	/var/netwitness/logdecoder/cache
Cache Size	4 GB

Parsers Configuration

Name	Config Value
⊞ ALERTS	☑
BITTORRENT	☑
FeedParser	☑
FIX	☑
⊞ GeoIP	□
GNUTELLA	☑

Service Parsers Configuration

Name	Config Value
vssmonitoring	☑
websense	☑
whatsupgold	☑
winevent_er	☑
winevent_nic	☑
winevent_snare	☑
zenprisemdm	☑

1 Find the name of the event source.

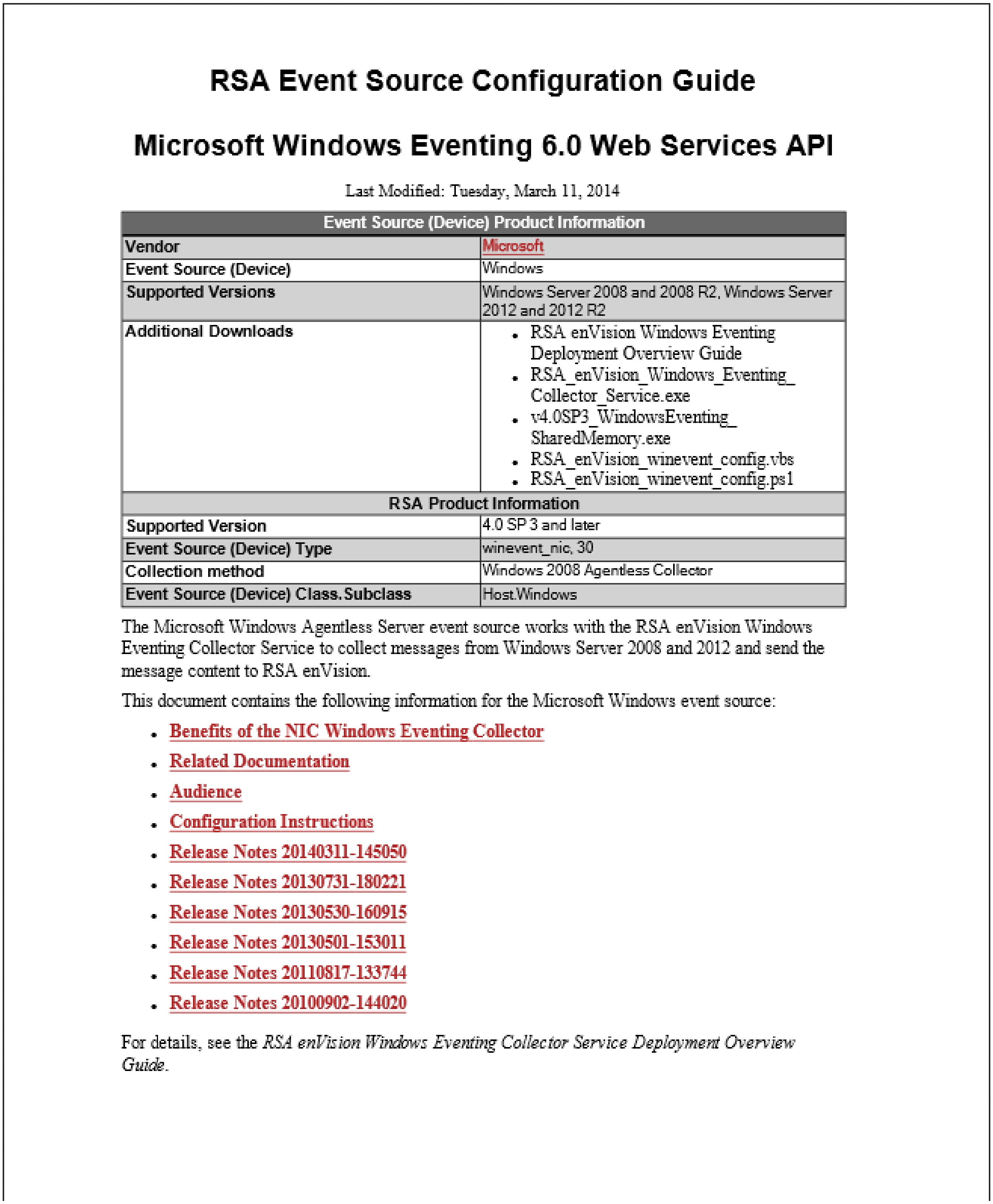
2 Verify that it is supported by the Windows Collection Protocol.

3 Click on 🔒 to retrieve the configuration instructions for the event source.

4 Verify that you downloaded the correct event source parser (for example, **winevent_nic**) from LIVE to the Log Decoder and enabled it.

Sample Configuration Instructions

The following illustration is taken from the Microsoft Windows Eventing 6.0 Web Services API configuration instructions.



RSA Event Source Configuration Guide

Microsoft Windows Eventing 6.0 Web Services API

Last Modified: Tuesday, March 11, 2014

Event Source (Device) Product Information	
Vendor	Microsoft
Event Source (Device)	Windows
Supported Versions	Windows Server 2008 and 2008 R2, Windows Server 2012 and 2012 R2
Additional Downloads	• RSA enVision Windows Eventing Deployment Overview Guide • RSA_enVision_Windows_Eventing_Collector_Service.exe • v4.0SP3_WindowsEventing_SharedMemory.exe • RSA_enVision_winevent_config.vbs • RSA_enVision_winevent_config.ps1
RSA Product Information	
Supported Version	4.0 SP 3 and later
Event Source (Device) Type	winevent_nic, 30
Collection method	Windows 2008 Agentless Collector
Event Source (Device) Class.Subclass	Host.Windows

The Microsoft Windows Agentless Server event source works with the RSA enVision Windows Eventing Collector Service to collect messages from Windows Server 2008 and 2012 and send the message content to RSA enVision.

This document contains the following information for the Microsoft Windows event source:

- Benefits of the NIC Windows Eventing Collector
- Related Documentation
- Audience
- Configuration Instructions
- Release Notes 20140311-145050
- Release Notes 20130731-180221
- Release Notes 20130530-160915
- Release Notes 20130501-153011
- Release Notes 20110817-133744
- Release Notes 20100902-144020

For details, see the *RSA enVision Windows Eventing Collector Service Deployment Overview Guide*.

Step 3. Start Service for Configured Windows Collection Protocol

This topic tells you how to start a stopped Windows collection service.

If a Windows collection service stops, you will need to start it again in order to make it work. You can also refer to the topic **Enable Automatic Start of Individual Services** in the *Log Collection Configuration Guide* if you want the service to start automatically.

Procedure

Return to Procedures

1. To start a collection service:
2. In the **Security Analytics** menu, select **Administration** > **Services**.
3. Select a Log Collector service and select ⌄ > **View** > **System**.

   The **Services System** view is displayed.
4. Click **Collection** > **Windows** > **Start** in the toolbar.

Step 4. Verify That Windows Collection Is Working

This topic tells you what to check in Security Analytics to verify that you have configured Windows Collection correctly.

If the Windows collection is not configured correctly, it will not work. You can check if it is working from the Health & Wellness view or the Investigation view.

Procedure

Return to Procedures

To verify that the Windows collection is working:

1. In the **Security Analytics** menu, select **Administration** > **Health & Wellness**
2. In the **Event Source Monitoring** tab, find a Windows event source type (for example, **winevent_nic**) in the **Event Source Type** column.
3. Look for activity in the **Count** column to verify that Windows collection is accepting events.

The following figure illustrates how you can verify that Windows collection is working from the **Investigation**> **Events** > view.

1. In the **Security Analytics** menu, select **Investigation** > **Events**.
2. Select the Log Decoder collecting **Windows** events in the **Investigate a Service**dialog.
3. Look for a Windows service type in the **Details** column to verify that Windows collection is accepting events.

References - Windows Collection Configuration Parameters

This topic describes the Windows event source configuration parameters.

Windows collection event source configuration parameters have two views: **Windows** and **Kerberos Realm** parameters.

- Windows Event Source Configuration Parameters
- Windows Kerberos Configuration Parameters

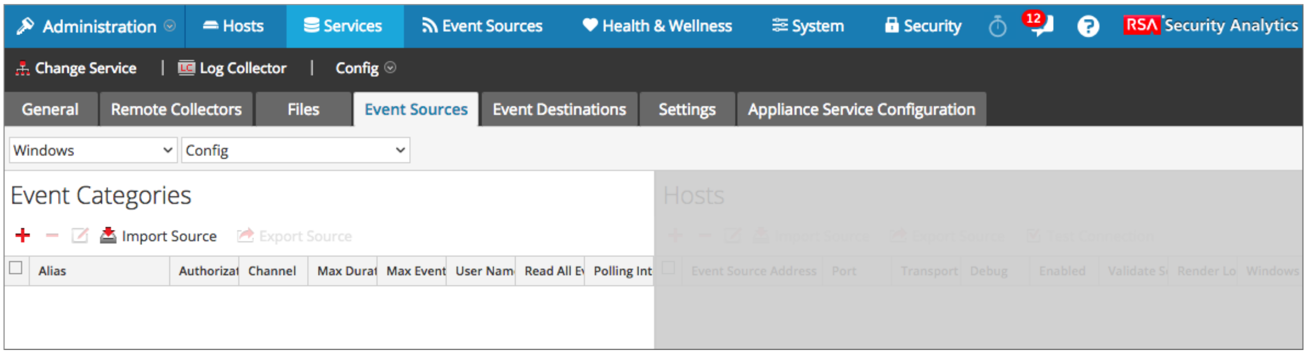
Windows Event Source Configuration Parameters

This topic tells you how to configure Windows event sources for the Log Collector.

The Windows/Config option on the Log Collector service Config View > Event Sources tab displays the parameters that you specify to configure Windows event sources.

To access the Windows Event Source configuration parameters:

1. In the **Security Analytics** menu, select **Administration >Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. In the **Actions** column, select ⚙ > **View** > **Config**.
4. In the **Event Sources** tab, select **Windows/Config** from the drop-down menus.



Note: For data encryption during communication between Security Analytics Windows Collection and Windows event source, use Kerberos Authentication with HTTPS mode in WinRM.

Features

The Windows/Config view of the Event Sources tab has two panels: Event Categories and Hosts.

Event Categories Panel

The Event Categories panel provides a list of existing Windows event source aliases. Use this section to add or delete Windows event source aliases.

The windows domain, referred to as alias, is the configuration parameter that the Log Collector uses to group event sources. Most often, the alias defines a single domain because credentials (that is username, and password), and channels are domain -wide. Occasionally, you need to define multiple alias entries for the same domain if you need to customize the settings for different groups of event sources.

Toolbar

The following table provides descriptions of the toolbar options.

Option	Description
➕	Displays the **Add Event Source** dialog in which you define the parameters for a new Windows event source.
➖	Deletes the Windows event source aliases that you selected.
✎	Displays the **Edit Event Source** dialog in which you edit the parameters for the selected Windows event source. When multiple event sources are selected, opens the **Bulk Edit Source** dialog in which you can edit the parameters values for the selected event sources. Refer to import, export, and edit event sources in bulk in the *Log Collection Configuration Guide* for detailed steps on how to use this function.
Import Source	Opens the **Bulk Add Option** dialog in which you can import event source host parameters in bulk from a comma-separated values (CSV) file. Refer to import, export, and edit event sources in bulk in the Log Collection Configuration Guide for detailed steps on how to use this function.

Export Source	Creates a **.csv** file that contains the parameters for the selected hosts. Refer to import, export, and edit event sources in bulk in the *Log Collection Configuration Guide* for detailed steps on how to use this function.
Test Connection	Validates the configuration parameters for the selected hosts. Refer to the *Log Collection Configuration Guide*for detailed steps on how to test event source connections in bulk.

Add Event Source Dialog

In this dialog, you define parameters for a new Windows event source.

Feature	Description
Basic	
Alias*	The windows domain, referred to as Alias, is the configuration parameter that the Log Collector uses to group event sources. These event source type groups (for example, **domain2**, **domain3**, and **domain4**) categorize the event sources you have configured.
Authorization Method*	The authentication method. Valid values are: • Basic (default) • Negotiate - Negotiates authentication between Kerberos and NTLM (Microsoft Windows NT LAN Manager). For security reasons, Security Analytics supports Kerberos exclusively.

Feature	Description
Channel	A comma-separated list of channels from which Security Analytics collects events. System, Application, Security is the default value for this parameter. Please refer to "Determine the Channel Name on the Windows Event Source" in Step 1. Configure Windows Event Sources in Security Analytics to find the appropriate channel names to use to define this parameter. You can use parentheses to include and exclude event IDs. The exclude filter must have a ^ between the channel name and the event ID. You must separate event IDs with a |. For example, **Application^(211|300), System (1010|1012)** excludes the 211 and 300 Application events and includes the 1010 and 1012 System events. A channel is a named stream of events that transports them from an event publisher to an event log file. There are many predefined Windows channels. The following are examples of some of these channels: **System** - applications that run under system service accounts (installed system services), drivers, or a component or application that has events that relate to the health of the system. **Application** - all user -level applications. This channel is unsecured and it is open to any application. If an application has extensive information, you should define an application -specific channel for it. **Security** - the Windows Audit Log (event log) used exclusively for the Windows Local Security Authority. Please refer to http://msdn.microsoft.com/en-us/subscriptions/aa385225(v=vs.85).aspx for additional information on windows channels.
User Name *	Event source username. For negotiate authentication, this must be the Kerberos principal name in the name@kerberosdomain format. For example, **logcollector@LAB30.LOCAL**.
Password *	Event source password. The password is encrypted internally and is displayed in its encrypted form.

Feature	Description
Read All Events	Select this checkbox to read all historical event data from a channel. Valid values are: • **Checked** - Log Collector collects from all historical event data from a specified channel. • **Unchecked (default)** - Log Collector does not collect from all historical event data for a specified channel.
Advanced	
Max Duration Poll	The maximum duration of polling cycle (how long the cycle lasts) in seconds.
Max Events Per Cycle	The maximum number of events per polling cycle (how many events collected per polling cycle).
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Render Events	Select this checkbox to request rendered events from the event source. • **Checked (default)** - Log Collector requests rendered events from the event source. • **Unchecked** - Log Collector does not request rendered events from the event source.
Cancel	Closes the dialog without adding the Windows event source.
OK	Adds the current parameter values as a new event source.

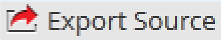
Hosts Panel

The Hosts panel displays a list of existing Windows event source hosts. Use this section to add or delete Windows event source hosts (that is the windows event source address and associated communication parameters).

Toolbar

The following table provides descriptions of the toolbar options.

Option	Description
+	Displays the Add Host dialog in which you define the parameters for a host for the event source that you select in the Event Categories panel.
−	Deletes the event source host that you selected.
✎	Displays the Edit Host dialog in which you edit the parameters for the selected Windows event source. When multiple event sources are selected, opens the Bulk Edit Source dialog in which you can edit the parameters values for the selected hosts. Refer to import, export, and edit event sources in bulk in the *Log Collection Configuration Guide* for detailed steps on how to use this function.
Import Source	Opens the Bulk Add Option dialog in which you can import event sources in bulk from a comma-separated values (CSV) file. The Bulk Add Option dialog has the following two options. Refer to import, export, and edit event sources in bulk in the *Log Collection Configuration Guide* for detailed steps on how to use this function.

 Export Source	Creates a **.csv** file that contains the parameters for the selected event sources. Refer to import, export, and edit event sources in bulk in the *Log Collection Configuration Guide* for detailed steps on how to use this function.
Test Connection	Validates the Event Source Address for the selected hosts.

Add Host Dialog

The following table provides descriptions of the Add Host dialog features.

Column	Description
Basic	
Event Source Address*	IP address of the event source. Valid value is an IPv4 address, IPv6 address, or a hostname including a fully qualified domain name. Log Collector converts the hostname to lower-case letters to prevent duplicate entries.
Port	Port number. A valid port number is any number within the 1 through 65535 range. • WinRM 2.0 (Vista and later) uses ports 5985 for http and 5986 for https as the default ports. • WinRM 1.1 (Windows 2003) uses ports 80 for http and 443 for https as the default ports.
Transport Mode	transport-mode [for example, http (default)]. Valid transport modes are: • **http** (default) - non-secure connection • **https** - secure connection
Enabled	Select this checkbox to collect from this event source. If you do not check this checkbox, the Log Collector does not collect events from this event source.
Certificate Name	Name of the certificate to use when the transport mode is https. If set, the certificate must exist in the certificate trust store. You add certificates to the trust store in the Certificates panel of the **Settings** tab.

Advanced	
Debug	**Caution:** Only enable debugging (set this parameter to **On** or **Verbose**) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). Limit the number of event sources for which you use Verbose debugging to minimize performance impact.
Validate Server	Select this check box to validate the Subject in the server certificate. The Subject of the server certificate must match the event source address.
Render Locale	Specify the location in which the events are rendered. If you do not specify a value, the event source uses its default locale. In most cases the default locale is en-US. The event source ignores an unsupported locale and the subscription fails if the locale is invalid.
Windows Type	(Optional setting) Indicates whether or not the event source you configured and are collecting from is a Domain controller. Security Analytics uses this parameter to determine if it should send the information to the Identity Event Processor (IDEP) or not. If you do not specify this parameter, all the data is sent to the IDEP. Valid values are: • **not set** - send all data to the IDEP • **Non-Domain Controller** - the event source you configured and are collecting from is a non-domain controller. • **Domain Controller** - the event source you configured and are collecting from is a domain controller.

Resolve SIDs	Resolve System Identification Codes (SIDs) Select this check box to resolve account SIDs in relevant attributes in the collected events into the account names. This check box is selected by default.
SID Enumeration Interval	Interval in seconds at which each event source enumerates account SIDs. Valid value is in the **0 - 86400** range. **14400** is the default value.
SID Enumeration Timeout	Enter the time in seconds for SID enumeration operations. Valid value is in the **10 - 600** range. **60** is the default value.

Override Channels	This parameter overrides the alias's Channel parameter that you set up in the **Add Source** dialog for all the hosts defined for a Windows alias (event source). If you leave the parameter blank, Security Analytics uses the alias' **Channel** parameter. A comma-separated list of channels from which Security Analytics collects events. **System**, **Application**, **Security** is the default value for this parameter. Please refer to "Determine the Channel Name on the Windows Event Source" in Step 1. Configure Windows Event Sources in Security Analyticsto find the appropriate channel names to use to define this parameter. You can use parentheses to include and exclude event IDs. The exclude filter must have a ^ between the channel name and the event ID. You must separate event IDs with a |. For example, **Application^(211|300), System(1010|1012)** excludes the 211 and 300 Application events and includes the 1010 and 1012 System events. A channel is named stream of events that transports them from an event publisher to an event log file. There are many predefined Windows channels. The following are examples of some of these channels: **System** - applications that run under system service accounts (installed system services), drivers, or a component or application that has events that relate to the health of the system. **Application** - all user -level applications. This channel is unsecured and it is open to any application. If an application has extensive information, you should define an application -specific channel for it. **Security** - the Windows Audit Log (event log) used exclusively for the Windows Local Security Authority.
Test Connection	Validates the connection to Event Source Address.
Cancel	Closes the dialog without adding the Windows event source.
OK	Saves the current parameter values as a new event source.

Tasks

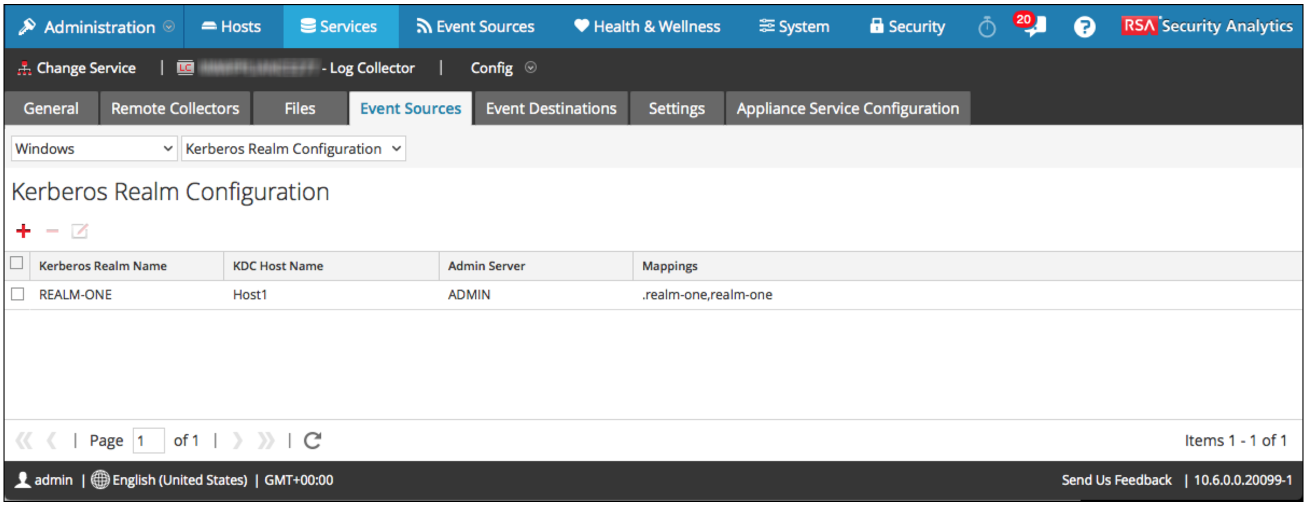
Step 1. Configure Windows Event Sources in Security Analytics

Windows Kerberos Configuration Parameters

Windows Kerberos Configuration Parameters

This topic covers the Kerberos Realm configuration parameters for Windows Kerberos Authentication.

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. In the toolbar, select **View > Config > Event Sources**.
4. In the **Event Sources** tab, select **Windows/Kerberos Realm Configuration** from the drop-down menu.



Kerberos Realm Configuration

□	Kerberos Realm Name	KDC Host Name	Admin Server	Mappings
□	REALM-ONE	Host1	ADMIN	.realm-one,realm-one

Features

The Windows/Kerberos Realm Configuration view in the Event Sources tab has one panel: Kerberos Realm Configuration.

Kerberos Realm Configuration Panel

In the **Kerberos Realm Configuration** panel, you can **add**, **delete**, or **edit** Kerberos realms.

Note: Security Analytics pre-fills the Mappings parameter based on the the Kerberos Realm Name parameter values that you enter.

Feature	Description
+	Displays the **Add Kerberos Realm** dialog in which you define Kerberos realm parameters.
−	Deletes the selected Kerberos realms.
✎	Displays the **Edit Kerberos Domain** dialog in which you edit Kerberos realm parameters.
□	Selects Kerberos realms.
Kerberos realm parameters	Displays the realms that you have added with its parameters.

Add or Edit Kerberos Domain Dialog

In this dialog, you add or modify Kerberos realm parameters.

Feature	Description
Kerberos Realm Name *	Kerberos realm name. Valid value is a name that is in all upper case letters and is in Fully-Qualified Domain Name (FQDN) format.
KDC Host Name *	A Key Distribution Center name. Valid value is a name that is in **.domain-name** format. If multiple KDCs are available, you can enter them using comma as a separator.
Admin Server	(Optional) The name of the Kerberos Administration Server in **FQDN** format.

Feature	Description
Mappings	Mappings from hosts to Kerberos realms. **.domain,domain** is the default value where domain is the Windows domain. If your deployment requires additional mappings, you can enter them using comma as a separator. **Note:** Security Analytics pre-fills the Mappings parameter based on the the Kerberos Realm Name parameter values that you entered.
Close	Closes the dialog without adding the realm or saving modifications to the parameters.
Save	Adds the Kerberos realm parameters or saves modifications to the parameters.

Tasks

Windows Kerberos Configuration Parameters

Windows Event Source Configuration Parameters

Troubleshoot Windows Collection

This topic highlights possible problems that you may encounter with Windows Collection and suggested solutions to these problems.

Troubleshoot Windows Collection Issues

In general, you receive more robust log messages by disabling SSL.

Security Analytics returns the following types of error messages in the log files.

Log Messages	(i) 2013-Nov-21 14:47:06 [WindowsCollection] [LAB30.bad-host_lab30_local] [processing] [LAB30.bad-host_lab30_local] Starting work (F) 2013-Nov-21 14:47:06 [WindowsCollection] [LAB30.bad-host_lab30_local] Error subscribing. Transport error code = 6/Could not resolve host (F) 2013-Nov-21 14:47:06 [WindowsCollection] [LAB30.bad-host_lab30_local] [processing] [LAB30.bad-host_lab30_local] Unable to subscribe for events with Windows event source bad-host.lab30.local: Could not resolve host Possible causes: - DNS resolution failed or name/address (bad-host.lab30.local) incorrect. (i) 2013-Nov-21 14:47:06 [WindowsCollection] [LAB30.bad-host_lab30_local] [processing] [LAB30.bad-host_lab30_local] Finished work (F) 2013-Nov-21 14:47:06 [WindowsCollection] [LAB30.bad-host_lab30_local] [processing] [LAB30.bad-host_lab30_local] windows:WrkUnit[1] Processing failed. (i) 2013-Nov-21 14:47:06 [WindowsCollection] [LAB30.10_100_33_179] [processing] [LAB30.10_100_33_179] Starting work (i) 2013-Nov-21 14:47:06[WindowsCollection] [LAB30.10_100_33_179] [processing] [LAB30.10_100_33_179] Enumerating SID information (F) 2013-Nov-21 14:47:09 [WindowsCollection] [LAB30.10_100_33_179] Error enumerating for account SIDs. Transport error code = 7/Could not connect (F) 2013-Nov-21 14:47:09 [WindowsCollection] [LAB30.10_100_33_179] [processing] [LAB30.10_100_33_179] Error enumerating for SID information: Could not connect

	(F) 2013-Nov-21 14:47:12 [WindowsCollection] [LAB30.10_100_33_179] Error subscribing. Transport error code = 7/Could not connect (F) 2013-Nov-21 14:47:12 [WindowsCollection] [LAB30.10_100_33_179] [processing] [LAB30.10_100_33_179] Unable to subscribe for events with Windows event source 10.100.33.179: Could not connect Possible causes: - Event source not configured for collection with http. - Event source currently down. (i) 2013-Nov-21 14:47:12 [WindowsCollection] [LAB30.10_100_33_179] [processing] [LAB30.10_100_33_179] Finished work (F) 2013-Nov-21 14:47:12 [WindowsCollection] [LAB30.10_100_33_179] [processing] [LAB30.10_100_33_179] windows:WrkUnit[2] Processing failed.
Possible Cause	Windows collection cannot connect to WinRM.
Solutions	Windows collection connects to the WinRM service on the Windows event source. You must configure the Windows event source to allow events to be collected. You can do this manually using the **winrm** command on the event source or you can create a Group Policy and push it to all event sources in a domain. This configuration creates a WinRM listener on the event source. You also configure the firewall on the event source to allow connections to it. By default, WinRM listens on port 5985 for HTTP connections and port 5986 for HTTPS connections. Please refer to **Supported Event Sources** in the *Live Resources Management Guide* for documentation on how to configure event sources.

Windows Legacy and NetApp Collection Configuration Guide

This guide tells you how to configure Windows Legacy and NetApp using the **Windows Legacy** collection protocol.

This protocol collects events from Windows Legacy (Windows 2003 or earlier event sources) and CIFS Auditing events from NetApp ONTAP event sources.

You must deploy Log Collection, that is set up a Local Collector and Windows Legacy Remote Collector, before you can configure the Windows Legacy collection protocol.

For deployment instructions, see Log Collection Deployment Guide.

The Basics

This topic tells you how the Windows Legacy collection protocol works, how you deploy it, and gives you a high-level description of how you configure this protocol.

How Legacy Windows and NetApp Collection Works

You use the Windows Legacy collection protocol to configure Security Analytics to collection events from:

- Legacy Microsoft Windows event sources (Window 2003 and earlier event sources)
- NetApp event sources

Window 2003 and Earlier Event Sources

Legacy Windows event sources are older Windows versions (such as Windows 2000 and Window 2003). The Windows Legacy collection protocol collects from Windows event sources that are already configured for enVision collection without having to reconfigure them. You set up these event sources under the windows event source type.

NetApp Event Sources

NetApp appliances running Data ONTAP support a native auditing framework that is similar to Windows Servers. When configured, this auditing framework generates and saves audit events in Windows .evt file format. The Windows Legacy collection protocol supports collection of events from such NetApp .evt files. You set up these event sources under the netapp_evt event source type.

The NetApp Data ONTAP appliance is configured to generate CIFS Auditing events and save them periodically as .evt files in a format that includes the timestamp in the filename. Refer to the NetApp Event Source configuration documentation on SecurCare Online (SCOL) for details. The collection protocol saves the timestamp of the last processed .evt filename to keep track of collection status

Net App Specific Parameters

Most of the parameters that you maintain in Add/Edit Source dialog apply to both Windows Legacy and Net App events sources.

The following two parameters are unique to NetApp event sources.

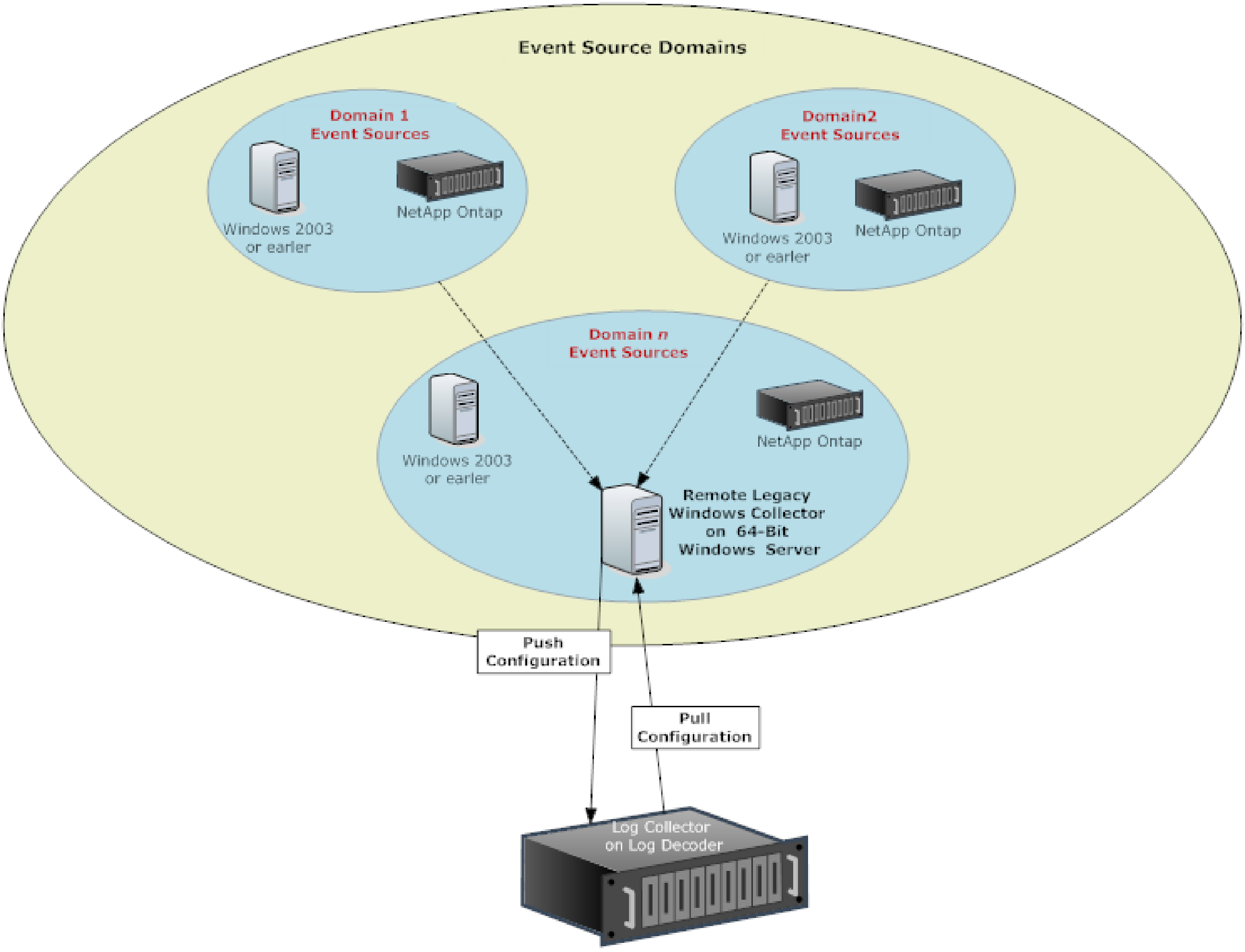
- **Event Directory Path -** The NetApp appliance generates event data and saves it in .evt files in a shareable directory on the NetApp appliance. Security Analytics requires you to specify this directory path in the Event Directory Path parameter
- **Event File Prefix -** Similar to the Event Directory Path, Security Analytics requires you to specify the prefix (for example, adtlog.) of the event data .evt files so that Security Analytics can process this data.

In each polling cycle, Security Analytics browses the configured NetApp shared path for the **.evt** files that you identified with the Event Directory Path and Event File Prefix parameters. Security Analytics:

- Sorts Files matching the event-file-prefix.YYMMDDhhmmss.evt format in ascending order.
- Uses the timestamp of the last file processed to determine the files that still need processing. If Security Analytics finds a partially processed file, it skips the events already processed.

Deployment Scenario

The Windows Legacy collection protocol collects event data from Windows 2003 or earlier, and NetApp ONTAP appliance, event sources. The Windows Legacy Remote Collector is the SA Legacy Windows Collector installed on physical or virtual Windows 2008 64-bit server in your event source domain.



Configure Windows Legacy Collection Protocol in Security Analytics

You configure to the Log Collector to use Windows Legacy collection for an event source in the event Source tab of the Log Collector parameter view. The following figure the basic workflow for configuring an event source for Windows Legacy Collection in Security Analytics. Please refer to:

- Step 2. Configure Windows Legacy and NetApp Event Sources in Security Analyticsfor step-by-step instructions on how to configure events sources in Security Analytics that use the File Collection protocol.
- Windows Event Source Configuration Parameters for a detailed description of each File Collection Protocol parameter.

Procedures

This topic provides an overview of the end-to-end sequential configuration procedure for Windows Legacy Collection protocol with a checklist that contains each configuration step.

Configuration steps for the Log Collector must occur in the specific sequence listed in the table below.

Windows Legacy and NetApp Configuration Checklist

Note: You install the Security Analytics Windows Legacy Collector on a physical or virtual Windows 2008 R2 SP1 64-Bit server using the **SALegacyWindowsCollector-*version-number.exe*.** You download the **SALegacyWindowsCollector-*version-number.exe*** from SCOL [please refer to the SA-v10.6 Legacy Windows Upgrade and Installation Instructions on SCOL (https://knowledge.rsasecurity.com/)].

The steps in this list are in the order in which you must complete them.

Step	Description	√
1	Set up your Windows Legacy collector.	
2	Configure Windows Legacy Event Sources in Security Analytics.	
3	Start service for configured Windows Legacy protocol.	
4	Verify that Windows Legacy Collection is working.	

Step 1. Set Up Windows Legacy Collector

This topic tells you where to find the executable and instructions required to install or upgrade the Windows Legacy collector in your Windows Legacy domain or domains.

Return to Procedures

You install the Security Analytics Windows Legacy collector on a physical or virtual Windows 2008 R2 SP1 64-Bit server using the **SALegacyWindowsCollector-10.6.*version-number.exe***. You download the **SALegacyWindowsCollector-10.6.*version-number.exe*** from SCOL. Please refer to the *SA v10.6 Windows Legacy Collection Upgrade & Installation Instructions* on SCOL (https://knowledge.rsasecurity.com) for the details on how to install or upgrade Windows Legacy collection.

Note: The Microsoft Management Console (MMC) should be closed during the installation process.

Step 2. Configure Windows Legacy and NetApp Event Sources in Security Analytics

This topic tells you how to configure Windows Legacy event sources in Security Analytics.

The Windows Legacy collection protocol collects event data from Windows 2003 or earlier event sources, and from NetApp event sources.

After completing this procedure, you will have:

- Configured a Windows Legacy event source.
- Modified a Windows Legacy event source.

Return to Procedures

Prerequisites

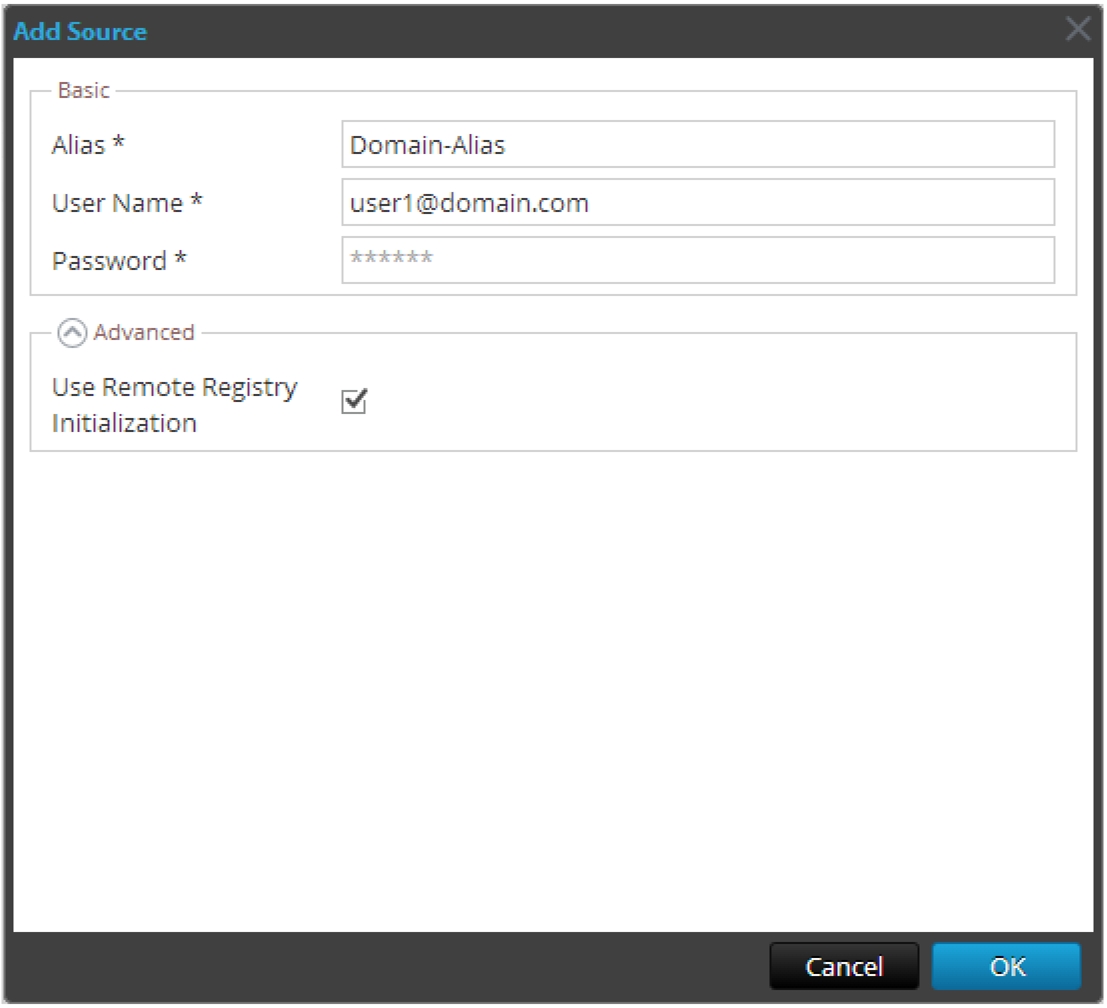
Before you configure a Windows Legacy event source, make sure that you have:

1. Installed the Security Analytics Windows Legacy Remote Collector on a physical or virtual Windows 2008 64-bit server.
2. Added this Windows Legacy Remote Collector to Security Analytics.

Procedures

Add a Windows Legacy Event Source

1. In the **Security Analytics** menu, select **Administration > Services.**
2. In the **Services** grid, select a **Windows Legacy Log Collector** service.
3. In the toolbar, select **View > Config > Event Sources.**
4. In the **Event Sources** tab, select one of the following options from the drop-down menu.
    - Windows Legacy/Windows.
    - Windows Legacy/NetApp.
5. Configure the alias:
    a. Click + in the **Event Categories** panel toolbar.
       The **Add Source** dialog is displayed.
    b. Specify values for the parameters and click **OK**.


Add Source

Basic

Alias * Domain-Alias

User Name * user1@domain.com

Password * ******

Advanced

Use Remote Registry Initialization ☑

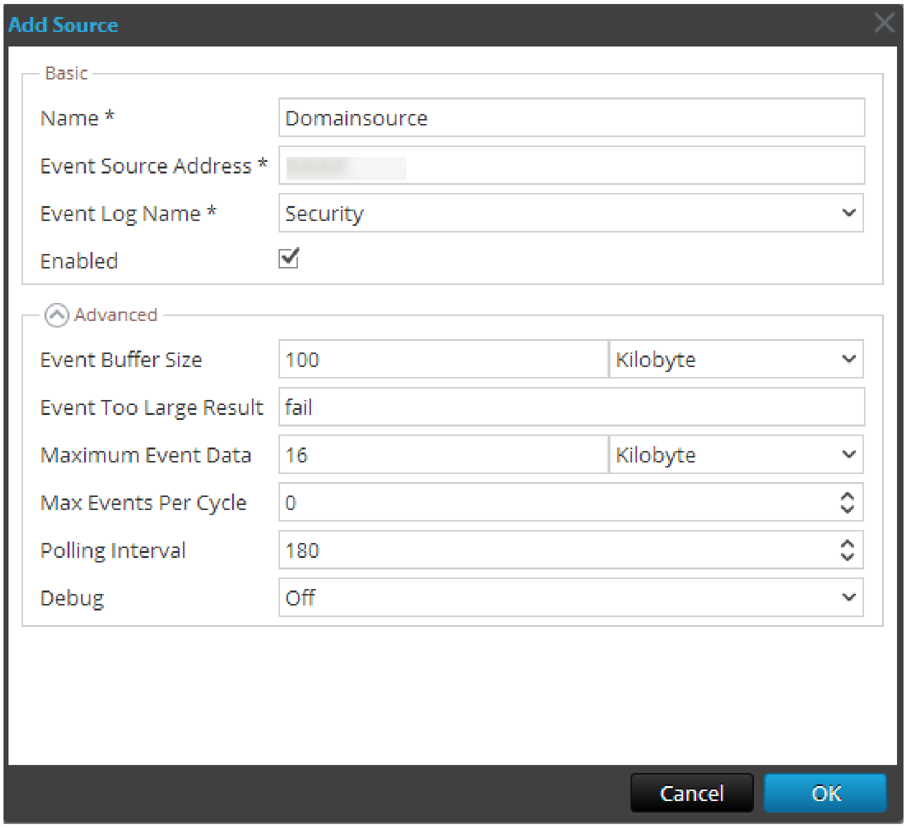
The newly added windows event source type is displayed in the **Event Categories** panel.

6. Add the event source:

   a. Select the new alias in the **Event Categories** panel and click + in the **Source** panel toolbar.

      The **Add Source** dialog is displayed.

   b. Specify values for the event source parameters and click **OK**.



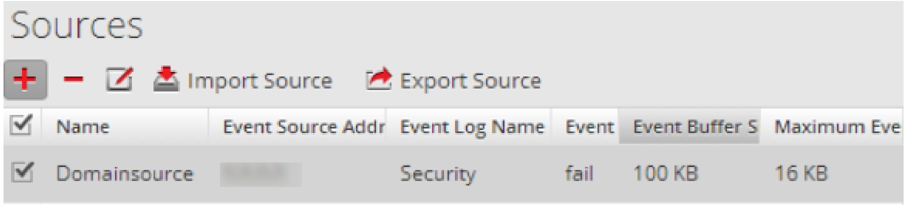
Basic

Name *	Domainsource
Event Source Address *	[redacted]
Event Log Name *	Security
Enabled	☑

Advanced

Event Buffer Size	100	Kilobyte
Event Too Large Result	fail	
Maximum Event Data	16	Kilobyte
Max Events Per Cycle	0	
Polling Interval	180	
Debug	Off	

The newly added Windows event source is displayed in the **Event Categories** panel.



☑	Name	Event Source Addr	Event Log Name	Event	Event Buffer S	Maximum Eve
☑	Domainsource	[redacted]	Security	fail	100 KB	16 KB

Modify a Windows Legacy Event Source

1. In the **Security Analytics** menu, select **Administration** > **Services.**

2. In the **Services** grid, select a **Log Collector** service.

3. In the **Actions** drop-down, select **View** > **Config**.

4. In the **Event Sources** tab, select one of the following options from the drop-down menu.

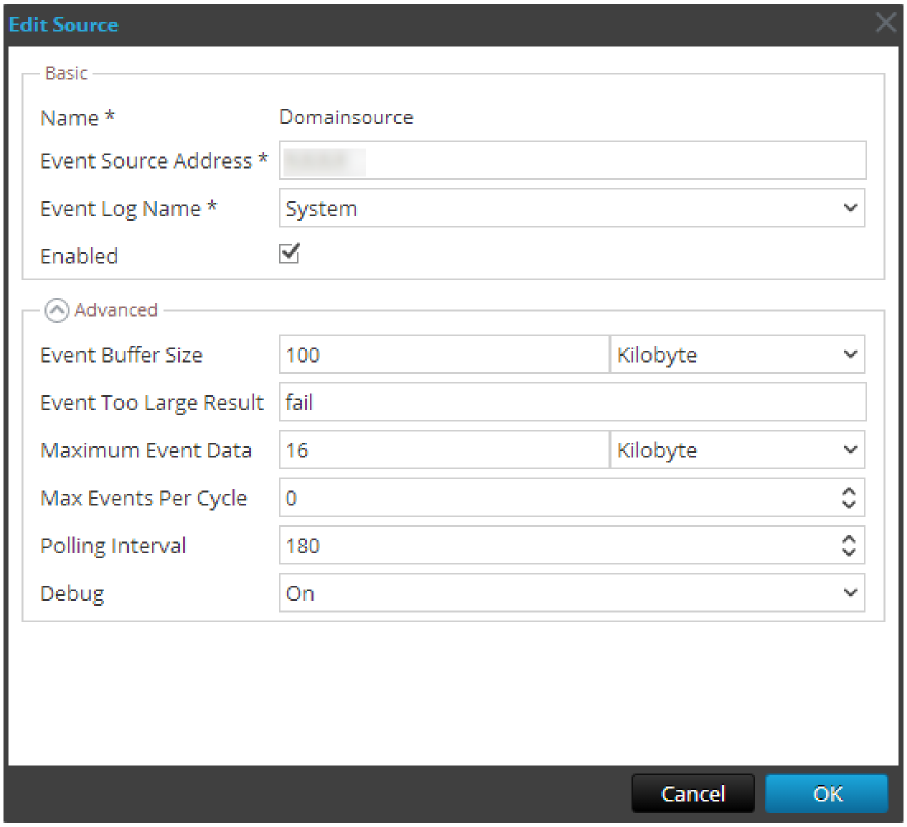
   - Windows Legacy/Windows.
   - Windows Legacy/NetApp

5. Modify the source parameters.

   a. In the **Event Categories** panel, select a source and click ✎.

      The **Edit Domain** dialog is displayed.

   b. Modify the source parameters that require changes and click **Save**.



Name * Domainsource

Event Source Address * [redacted]

Event Log Name * System

Enabled ☑

Event Buffer Size 100 Kilobyte

Event Too Large Result fail

Maximum Event Data 16 Kilobyte

Max Events Per Cycle 0

Polling Interval 180

Debug On

6. Modify the event source parameters.

   a. In the **Source** panel, select an event source and click ✎.

      The **Edit Source** dialog is displayed.

   b. Modify the event source parameters that require changes and click **Save**.

      Security Analytics applies the parameter changes to selected host

Parameters

References - Windows Legacy and NetApp Collection Configuration Parameters

Configure Remote Registry Access

This topic describes the procedure to enable Remote Registry Access method for collecting data from event sources.

Return to Procedures

Windows Legacy Collector performs an initial verification of the event source before collecting data. By default, Windows Legacy Collector uses Windows Management Instrumentation (WMI) method to perform this initial verification. If you enable Remote registry access method, Windows Legacy Collector performs a remote registry query to verify the event source.

> **Note:** Customers who have upgraded from RSA enVision can select the Remote Registry Access method so as to use the existing domain collection user without having to enable WMI permission.

Procedure

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a Windows Legacy Log Collector service.
3. In the **toolbar**, select **View > Config** > **Event Sources**.
4. In the **Event Sources** tab, select **Windows Legacy**/**Windows** from the drop-down menu.
5. Configure the alias:
   a. Click + in the **Event Categories** panel toolbar.
      The **Add Source** dialog is displayed.
   b. Make sure that the **Use Remote Registry Initialization** checkbox is checked (it is checked by default) and click **OK**.

Result

Remote Registry Access method is enabled.

Configure Windows Legacy Collector Events Filters

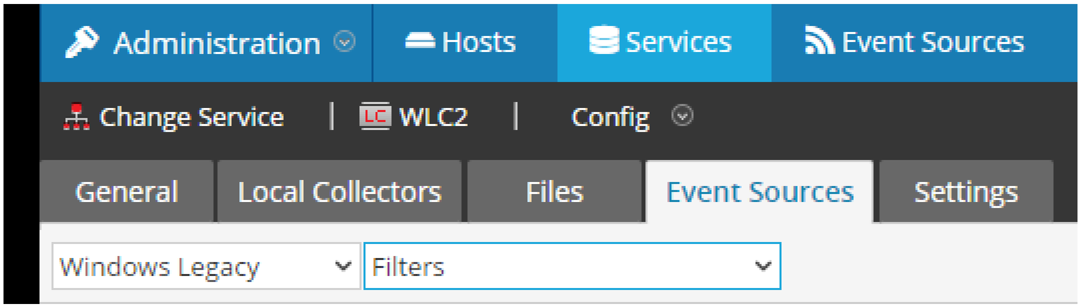
You can filter specific types of events in the Windows Legacy Collector. For example, if your system collects a large number of events, and a large percentage of them come from Windows firewalls, you can filter those events out so that you can track other events that are occurring. This can be useful if your Log Decoders are under a heavy load and you want to process only those events that are meaningful.

Procedure

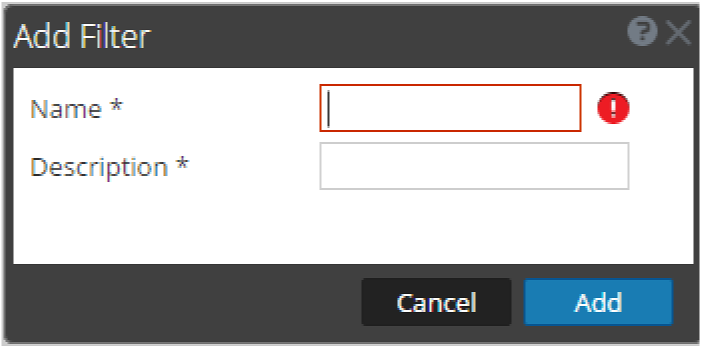
To configure a Windows Legacy Collector events filter:

1. In the Security Analytics menu, select **Administration** > **Services**.
2. Under **Services**, select a Windows Log Collector service.
3. In the Windows Log Collector service row, click the down arrow under **Actions** and select **View** > **Config**.

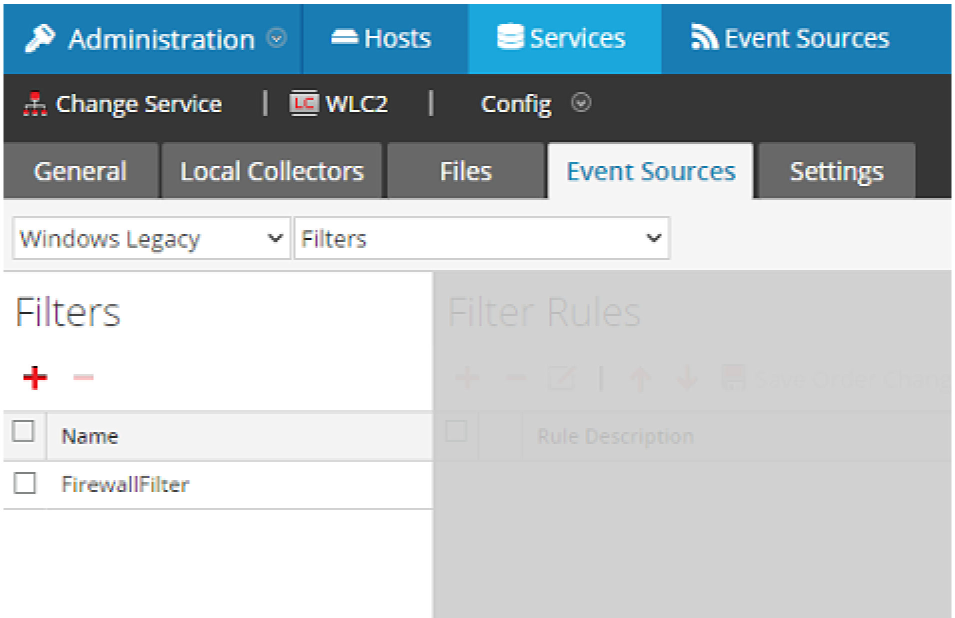
4. Select the Event Sources tab. Windows Legacy is displayed at the top of the page on the left. In the Windows drop-down menu, select **Filters**.



5. In the Filters panel, click +.
   The Add Filter dialog is displayed.



6. Type a name and description for the new filter and click **Add**.
   The new filter is displayed in the **Filter** panel (in this example, FirewallFilter).

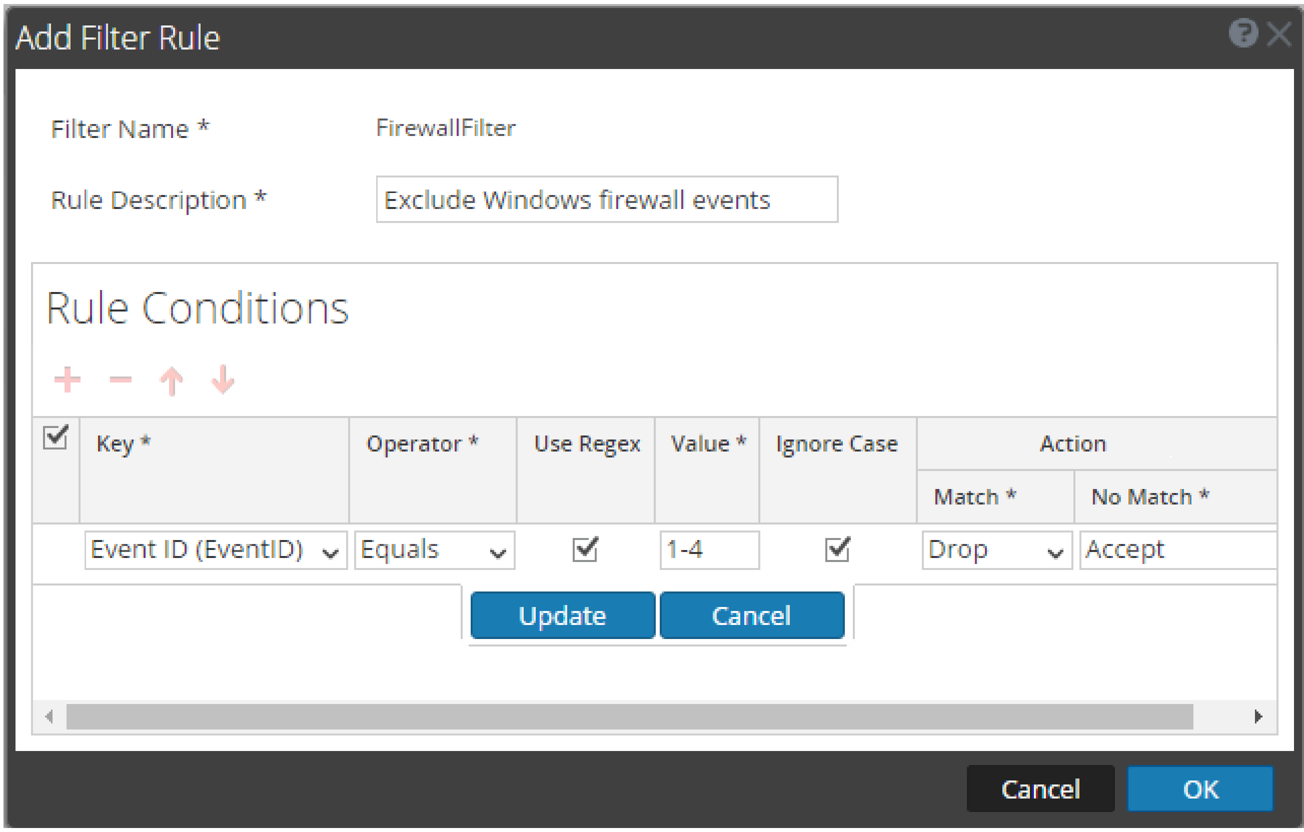


7. Select the new filter in the **Filters** panel, and in the Filter Rules panel toolbar, click ✚. The Add Filter Rule dialog is displayed.

8. Under **Rule Conditions**, click ✚ and add the parameters for this rule. The following table describes the parameter options.

Field	Description
Key	The only valid value is Event ID (EventID).
Operator	Valid values are: • Contains • Equals
Use Regex	Optional
Value	Alphanumeric characters that describe the event IDs for the events to filter.
Ignore case	Optional
Action	If there is a match you can choose from the following actions: • Accept: events that match the IDs provided will be included in event logs, and will display in the Systems Analytics UI. • Drop: events that match the IDs provided will not be included in event logs and will not display in the UI. • Next condition: the filter will ignore events with IDs that match, and will move on to the next rule condition. • Next rule: the filter will ignore events with IDs that match, and will move on to the next rule.

The following image shows an example of a rule condition for the FirewallFilter:



Add Filter Rule

Filter Name * FirewallFilter

Rule Description * Exclude Windows firewall events

Rule Conditions

☑	Key *	Operator *	Use Regex	Value *	Ignore Case	Action	
						Match *	No Match *
	Event ID (EventID)	Equals	☑	1-4	☑	Drop	Accept

9. Click **Update**, and then click **OK**. Security Analytics updates the filter with the rule that you defined.

Step 3. Start Service for Configured Windows Legacy Collection Protocol

This topic tells you how to start a stopped Windows Legacy collection service.

If a Windows Legacy collection service stops, you may need to start it again.

Procedure

Return to Procedures

The following procedure shows you how to start a collection service. See the **Enable Automatic Start of Individual Services** topic in the *Log Collection Configuration Guide* if you want the service to start automatically.

1. In the **Security Analytics** menu, select **Administration > Services**.
2. Select a **Windows Legacy Log Collector** and, in the **Actions** column, select ⚙ > **View > System**.

   The **Services System** view is displayed.
3. Click **Collection > Windows Legacy > Start**.

Step 4. Verify That Windows Legacy Collection Is Working

This topic tells you what to check in Security Analytics to verify that you have configured Windows Legacy Collection correctly.

This procedure is useful for verifying that you have configured Windows Legacy Collection correctly. If it is not configured correctly, it cannot work the way it should.

Procedure

Return to Procedures

The following procedure explains how you can verify that Windows Legacy collection is working from the **Administration** > **Health & Wellness** > **Event Source Monitoring** tab.

1. In the **Security Analytics** menu, select **Administration** > **Health & Wellness**.
2. Click the **Event Source Monitoring** tab.
3. In the grid row for the Windows Legacy event source type, look for activity in the **Count** column to verify that Windows Legacy collection is accepting events.

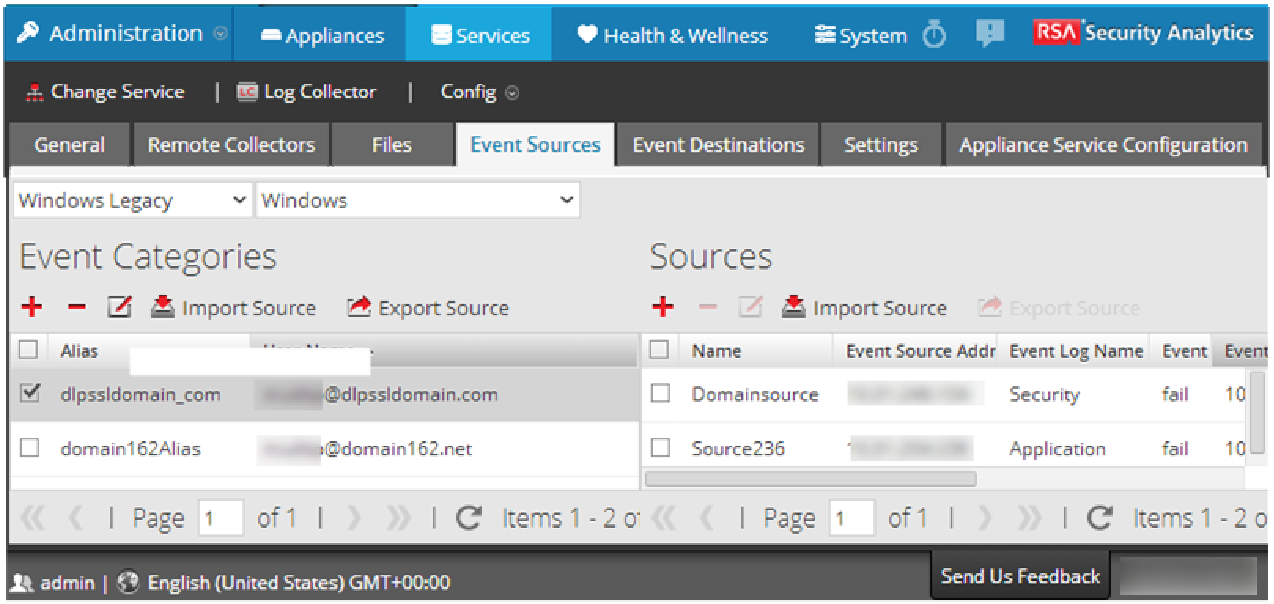
References - Windows Legacy and NetApp Collection Configuration Parameters

This topic describes the user interface for Configuring Windows Legacy Collection.

The **Windows Legacy/Windows** or **Windows Legacy/NetApp** options on the Log Collector service **Config View** > **Event Sources** tab displays the parameters that you specify to configure Windows Legacy event sources.

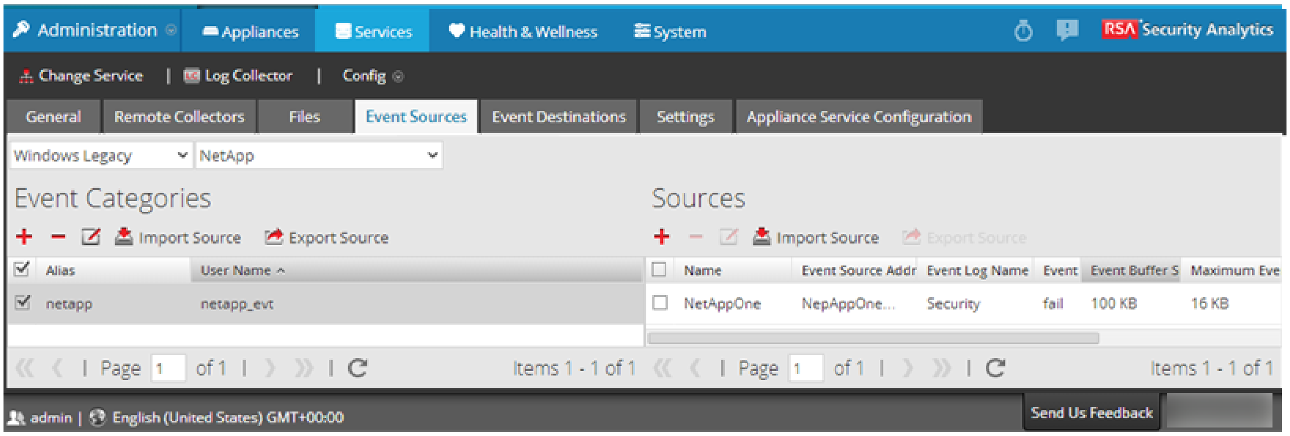
To access the Windows Legacy and NetApp Collection Configuration Parameters:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. In the **Actions** column, select ⚙ ⌄ > **View** > **Config**, then click the **Event Sources** tab.
4. In the **Event Sources** tab, select one of the following options from the drop-down menu
   - **Windows Legacy/Windows**
   - **Windows Legacy/NetApp**



☐	Alias	[redacted]
☑	dlpssldomain_com	[redacted]@dlpssldomain.com
☐	domain162Alias	[redacted]@domain162.net

☐	Name	Event Source Addr	Event Log Name	Event	Event
☐	Domainsource	[redacted]	Security	fail	10
☐	Source236	[redacted]	Application	fail	10



☑	Alias	User Name ^
☑	netapp	netapp_evt

☐	Name	Event Source Addr	Event Log Name	Event	Event Buffer S	Maximum Eve
☐	NetAppOne	NepAppOne...	Security	fail	100 KB	16 KB

Features

The Event Sources tab for Windows Legacy/Windows and Windows Legacy/NetApp has two panels: Event Categories and Sources.

Event Categories Panel

The Event Categories panel lists existing Windows Legacy event source aliases. Use this section to add or delete Windows Legacy event source aliases.

The windows domain, referred to as alias, is the configuration parameter that the Log Collector uses to group event sources. Most often, the alias defines a single domain because credentials (that is username, and password), and event log name are domain -wide. Occasionally, you need to define multiple alias entries for the same domain if you need to customize the settings for different groups of event sources.

Sources Panel

The Sources panel displays a list of existing Windows Legacy event sources. Use this section to add or delete Windows Legacy event sources (that is the windows event source address and associated communication parameters).

Toolbar

The following table provides descriptions of the toolbar options.

Feature	Description
+	Displays the Add Source dialog in which you define the parameters for a Firewall host.
−	Deletes the host that you selected.
✎	Opens the Edit Source dialog, in which you edit the parameters for the selected event source. Select multiple event sources and click ✎ to open the Bulk Edit Source dialog in which you can edit the parameters values for the selected event sources. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.
Import Source	Opens the Bulk Add Option dialog in which you can import hosts in bulk from a comma-separated values (CSV) file. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.
Export Source	Creates a .csv file that contains the parameters for the selected hosts. Refer to the Log Collection Configuration Guide for detailed information on how to import, export, and edit event sources in bulk.

Add Source Dialog

In this dialog, you define parameters for a new Windows Legacy event source.

Feature	Description
	Basic
Name*	The name of the event source. Valid value is a name in the **[_a-zA-Z] [_a-zA-Z0-9]*** range. You can use a dash "**-**" as part of the name.

Feature	Description
Event Source Address*	IP address of the event source. Valid value is an IPv4 address, IPv6 address, or a hostname including a fully qualified domain name. Security Analytics defaults to **127.0.0.1**. Log Collector converts the hostname to lower-case letters to prevent duplicate entries.
Event Log Name	The name of the event log from which to collect event data (for example, **System**, **Application**, or **Security**). The following are examples of some of these channels: • **System** - applications that run under system service accounts (installed system services), drivers, or a component or application that has events that relate to the health of the system. • **Application** - all user -level applications. This channel is unsecured and it is open to any application. If an application has extensive information, you should define an application -specific channel for it. • **Security** - the Windows Audit Log (event log) used exclusively for the Windows Local Security Authority.
Enabled	Select this checkbox to collect from this event source. If you do not check this checkbox, the Log Collector does not collect events from this event source.

Feature	Description
Event Directory Path	NetApp **.evt or .evtx** files directory path. This must be the UNC path. The NetApp generates event data and saves it in .evt or .evtx files in a shareable directory on the NetApp appliance. • In each polling cycle, Log Collector browses the configured NetApp shared path for the .evt files that you identified with the **Event Directory Path** and **Event File Prefix parameters**. Log Collector: ○ sorts files that match the **event-file-prefix.YYMMDDhhmmss.evt** format in ascending order. ○ uses the timestamp of the last file processed to determine the files that still need processing. If Log Collector finds a partially processed file, it skips the events already processed. • In each polling cycle, Log Collector browses the configured NetApp shared path for the **.evtx** files that you identified with the **Event Directory Path** and **Event File Prefix parameters**. Log Collector: ○ sorts files that match the **event-file-prefix.YYMMDDhhmmssms.evtx** format in ascending order. ○ uses the timestamp of the last file processed to determine the files that still need processing. If Log Collector finds a partially processed file, it skips the events already processed.
Event File Prefix	Prefix of the **.evt** files (for example, **adtlog.**) saved in the **Event Directory Path**.
Advanced	
Event Buffer Size	Maximum size of the data the Log Collector pulls from the event source for each request. Valid value is a number in **0** to **511** Kilobytes range. You specify this value in **Kilobytes**.
Event Too Large Result	Tells Log Collector what to do if an event is too large for the event buffer.

Feature	Description
Maximum Event Data	Maximum size of event data to include in the output. Valid value is a number in **0** to **511Kilobytes** range. You specify this value in **Kilobytes** or **Megabytes**. • 1 Kilobyte - 100 Megabytes • 0 = do not include event data in the output.
Max Events Per Cycle	The maximum number of events per polling cycle (how many events collected per polling cycle).
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, it will wait for it to finish that cycle. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). Limit the number of event sources for which you use Verbose debugging to minimize performance impact.
Cancel	Closes the dialog without adding the Windows Legacy event source.
OK	Adds the current parameter values as a new event source

Troubleshoot Windows Legacy and NetApp Collection

This topic highlights possible problems that you may encounter with Windows Legacy Collection (LWC) and suggested solutions to these problems.

Troubleshoot Windows Legacy and NetApp Collection Issues

In general, you receive more robust log messages by disabling SSL.

Protocol Restart Problems

Problem	Possible Causes	Solutions
You restart the Legacy Windows collection protocol, but Security Analytics is not receiving events.	The logcollector service is stopped.	Restart the **logcollector** service. 1. Log on to the **Windows Legacy Remote Collector**. 2. Go to **Start > Administrative Tools > Task Scheduler** and click on **Task Scheduler Library**. 3. In the right panel, look for the **restartnwlogcollector** task and make sure that it is running. 4. If this is not the case, right-click **restartnwlogcollector** and select **Run**.

Installation Problems

If you see any of the following messages in the **MessageBroker.log**, you may have issues.

Log Messages	Any message that contains "rabbitmq"
Possible Cause	RabbitMQ service may not be running. Port **5671** may not be opened.

Solutions	Make sure that the RabbitMQ service is running. Make sure that port **5671** is open.
Log Messages	Error: Adding logcollector user account. Error: Adding administrator tag to logcollector account. Error: Adding Adding logcollection vhost. Error: Setting permissions to logcollector account in all vhosts.
Possible Cause	**rabbitmq-server** was not running when installer tried to create users and vhosts.

Solutions	Make sure that the **RabbitMQ** service is running and run below commands manually.
	`rabbitmqctl -q add_user logcollector netwitness`
	`rabbitmqctl -q set_user_tags logcollector administrator`
	`rabbitmqctl -q add_vhost logcollection`
	`rabbitmqctl -q set_permissions -p / logcollector ".*" ".*" ".*"`
	` rabbitmqctl -q set_permissions -p logcollection logcollector ".*" ".*" ".*"`

Windows Legacy Federation Script Issues

If you see any of the following messages in the federation script log, you may have issues.

Problem	Possible Symptoms	Solutions
Federation script started, but the LWC service went down.	Security Analytics log shows connection failure exceptions with Windows Legacy Collector.	This issue is fixed automatically after restarting the Windows Legacy service.

LWC is running, but RabbitMQ service is down or restarting.	Federation log file at Windows Legacy side displays an error message about RabbitMQ service being down.
	The log file to look at is: **C:\NetWitness\ng\logcollector**
	The following error message is logged in case RabbitMQ is not running:
	`"Unable to connect to node logcollector@localhost: nodedown"`
	The following diagnostics messages are displayed:
	`attempted to contact: [logcollector@localhost]`
	`logcollector@localhost:`
	`* connected to epmd (port 4369) on localhost`
	`* epmd reports: node 'logcollector' not running at all other nodes on localhost: ['rabbitmqctl-4084']`
	`* suggestion: start the node`
		Run the **federation.bat** script manually at LWC.
		To run the **federate.bat** script manually, perform the following steps:
		1. Go to folder C**:\Program Files\NwLogCollector** where the Windows Legacy instance is installed.
		2. Locate the file **federate.bat i**n this folder. Select the file and right click.
		3. Select **Run as Administrator**.
		4. To monitor the log file, navigate to **C:\NetWitness\ng\logcollector\federate.log** while the **federate.bat** script is being executed.
		Note: Make sure the log file does not show any errors while the script is being executed.

RabbitMQ service is down on Security Analytics side.	Security Analytics User Interface pages do not work.	Restart RabbitMQ service.

No Health & Wellness stats are displayed in Security Analytics User Interface.	Puppet agent is not running, or is taking a while to publish the exchanged certificates.	Restart Puppet agent, or wait a few several minutes to finish exchanging the certificates.
Customer receives a Health and Wellness notification, or the following Health and Wellness Alarm is displayed: "Communication failure between Master Security Analytics Host and a Remote Host" with LWC Host as the Remote IP.	1. **Federate.bat** script failed to run successfully. 2. Puppet agent has not run after the **federate.bat** script ran successfully.	1. If the **federate.bat** script did not run correctly, run it manually as described previously. 2. If the **federate.bat** script ran correctly and the puppet agent has not performed its scheduled run, run the puppet agent manually using the following command on your Security Analytics server: **puppet agent -t**