AUTHORIZED DOCUMENTATION

Sentinel Link Overview Guide

Novell®
Sentinel Plug-Ins

2011.1r1

October 2011

www.novell.com

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

The *Novell Sentinel Link Overview Guide* helps you understand how to use Sentinel Link to send event data from a Sentinel system to other Sentinel installations.

Audience

This guide is intended for the Sentinel administrator.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please submit all comments and suggestions via the Web form at Collector Request Form (http://support.novell.com/products/sentinel/secure/survey.html).

Documentation Updates

For the most recent version of the *Sentinel Link Overview Guide*, visit the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Additional Documentation

For complete documentation on the Sentinel products, see the following Web sites:

- Sentinel 6.1 (http://www.novell.com/documentation/sentinel61)
- Sentinel 6.1 Rapid Deployment (http://www.novell.com/documentation/sentinel61rd)
- Sentinel Log Manager (http://www.novell.com/documentation/novelllogmanager12)
- Sentinel 7.0 (http://www.novell.com/documentation/sentinel70/)

For information on building your own plug-ins, go to the Sentinel SDK Web page (http://developer.novell.com/wiki/index.php/Develop_to_Sentinel.html).

The Sentinel SDK site provides the details about developing Collectors (proprietary or JavaScript*) and JavaScript correlation actions.

Introduction

1

Sentinel Link is a mechanism that provides the ability to hierarchically link multiple Sentinel systems, including Novell Sentinel Log Manager, Novell Sentinel, and Novell Sentinel Rapid Deployment. You can hierarchically link two or more Sentinel systems to forward filtered events from one Sentinel system to another for further evaluation.

1.1 Benefits

- Multiple Sentinel Log Manager servers, local or distributed, can be linked in a hierarchical manner. In this setup, Sentinel Log Manager servers can manage a large volume of data, retaining raw data and event data locally, while forwarding important events to a central Sentinel Log Manager for consolidation.
- One or more Sentinel Log Manager servers can forward important data to either a Sentinel server or a Sentinel Rapid Deployment server. These systems provide real-time visualization of data, advanced correlation and actions, workflow management, and integration with identity management systems.
- Multiple Sentinel or Sentinel Rapid Deployment servers can be hierarchically linked to monitor the consolidated event information.
- One or more Sentinel or Sentinel Rapid Deployment servers can forward important events to a Sentinel Log Manager server for event consolidation.

1.2 Supported Platforms

- Sentinel 6.1 Service Pack 1 Hotfix 2 or later
- Sentinel 6.1 Rapid Deployment Hotfix 2 or later
- Sentinel Log Manager 1.0 Hotfix 1 or later

1.3 Prerequisite

- Before you forward events from the sender machine, ensure that the Sentinel Link server is up and running on the receiver machine.

1.4 Configuring Sentinel Link

In a Sentinel Link setup, the Sentinel system that forwards the events is called the sender and the Sentinel system that receives the events is called the receiver. You can simultaneously link multiple Sentinel systems to a single receiver system.

To configure a Sentinel link, you need to configure at least two systems: the sender machine and the receiver machine. For further details on configuring Sentinel Link, read the following:

- Chapter 3, “Configuring Sentinel Systems for Sending Events,” on page 31
- Chapter 2, “Configuring Sentinel Systems for Receiving Events,” on page 11

Configuring Sentinel Systems for Receiving Events

2

On the receiver system, you must import and configure the Sentinel Link Collector, which generates events from the data received by the Sentinel Link Connector. You must also import the Sentinel Link Connector and configure a Sentinel Link Event Source Server to receive the event data from the sender systems.

NOTE: For more information on Sentinel Link Connector and Collector, see the corresponding plug-in documentation in the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

2.1 Accessing Event Source Management

2.1.1 Sentinel

1. As the Sentinel Administrator User (esecadm), change directory to:

   `$ESEC_HOME/bin`
2. Run the following command:

   `control_center.sh`
3. Specify the administrator username and password, then click *OK*.
4. In the Sentinel Control Center, select *Event Source Management* > *Live View*.

2.1.2 Sentinel Rapid Deployment

1. Open a Web browser to the following URL:

   `https://svrname.example.com: port/sentinel`

   Replace svrname.example.com with the actual DNS name or IP address (such as 192.168.1.1) of the server where Novell Sentinel Rapid Deployment is running.
2. If you are prompted to verify the certificates, review the certificate information, then click *Yes* if it is valid.

3. Specify the username and password for the Sentinel Rapid Deployment account you want to access.
4. Use the *Languages* drop-down list to specify which language you want to use.
5. Click *Sign in*.
6. In the Web interface, select *Applications* from the left panel.
7. In the Application page, click *Launch* to open the Sentinel Control Center.
8. Log in to the Sentinel Control Center as administrator.
9. Select *Event Source Management > Live View*.

2.1.3 Sentinel Log Manager

1. Open a Web browser to the following URL:

   `https://svrname.example.com: port/novelllogmanager`

   Replace svrname.example.com with the actual DNS name or IP address (such as 192.168.1.1) of the server where Novell Sentinel Log Manager is running.
2. If you are prompted to verify the certificates, review the certificate information, then click *Yes* if it is valid.
3. Specify the username and password for the Log Manager account you want to access.
4. Use the *Languages* drop-down list to specify which language you want to use.
5. Click *Sign in*.
6. In the Novell Log Manager Web interface, click *Collection*.
7. In the Collection page, click *Advanced.*
8. In the Advanced page, click *Launch* to open the Event Source Management.

2.1.4 Sentinel 7.0

1. Open a Web browser to the following URL:

   `https://svrname.example.com: port/sentinel`

   Replace svrname.example.com with the actual DNS name or IP address (such as 192.168.1.1) of the server where Sentinel is running.
2. If you are prompted to verify the certificates, review the certificate information, then click *Yes* if it is valid.
3. Specify the username and password for the Sentinel account you want to access.
4. Use the *Languages* drop-down list to specify which language you want to use.
5. Click *Sign in*.
6. In the Sentinel Web interface, click *Collection*.
7. In the Collection page, click *Advanced.*
8. In the Advanced page, click *Launch Control Center* to open the Sentinel Control Center.
9. Log in to the Sentinel Control Center as administrator.
10. Select *Event Source Management > Live View*.

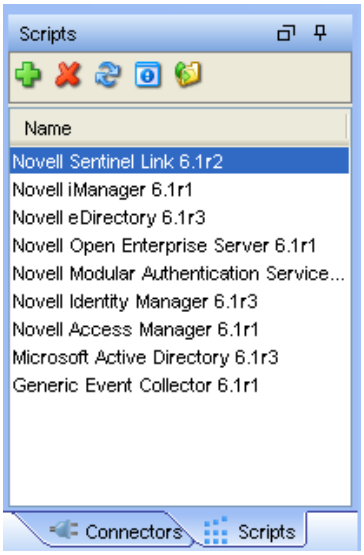
2.2 Importing the Sentinel Link Collector

Install the Collector plug-in to provide data collection services for Novell Sentinel Link.

1. Ensure that you download the Sentinel Link Collector (.zip) file from the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) to the local machine, where Event Source Management is launched.

   NOTE: Always use the latest Sentinel Link plug-ins available from the Sentinel Plug-ins Web site.

2. Launch the Event Source Management (Live View) window. For more information, see Section 2.1, "Accessing Event Source Management," on page 11.
3. Select the Scripts panel, then click the *Add* icon. The Plugin Import Type window is displayed.
4. Browse to select the Novell Sentinel Link Collector file that you downloaded; click Next.
5. Review the summary details, then click *Finish* to import the plug-in.



After the import is complete, the new Collector is displayed in the list of Collectors in the Scripts panel.

2.3 Importing the Sentinel Link Connector

Import and install the Connector plug-in to set up a connection with the event source.

1. Ensure that you download the Sentinel Connector (.zip) file from the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) to the local machine, where Event Source Management is launched.

   NOTE: Always use the latest Sentinel Link plug-ins available from the Sentinel Plug-ins Web site.

2. Launch the Event Source Management (Live View) window. For more information, see Section 2.1, "Accessing Event Source Management," on page 11.

3 Select *Tools* > *Import Plugin*. The Plugin Import Type window displays.

4 In the Plugin Import Type window, select the *Connector plug-in package file (.zip)* option, then click *Next*.

5 In the Choose Plug-in Package File window, locate and select the Sentinel link Connector `.zip` file you just downloaded.

6 Click *Open*.

If another version of this Connector is already in use, click *View Deployed Plugins* to see which Event Source objects use the deployed Connectors.

7 To update the deployed Connectors, select *Update Deployed Plugins*.

8 Click *Finish*.

After the import is complete, the new Connector displays in the list of Connectors in the Event Source Management (Live View) window.

2.4 Setting Up a Sentinel Link Connection

If you wish to manually configure advanced settings such as mutual authentication, refer to the documentation for the Sentinel Link Collector and Connector Plug-ins, available on the Sentinel Plug-ins website.This section describes how to set up the Sentinel Link connection to receive messages from another Sentinel or Sentinel Log Management system, and enable the messages to be processed by a Collector. To set up the Sentinel Link connection, you must, at a minimum, create and configure a Sentinel Link Event Source server. The Sentinel Link Event Source server automatically creates and configures the Connector, the Collector and the Event Source nodes as needed. You can also manually create the Collector, the Connector, and the Event Source nodes. However, it is easier and simpler to allow the Sentinel Link Event Source server auto-create them.

The instructions given in this section use the right-click menu items on the Event Source Management Graph View. However, all the steps described in this section can also be performed through the Event Source Management Table view and the *Connect to Event Source* option on the tool bar.

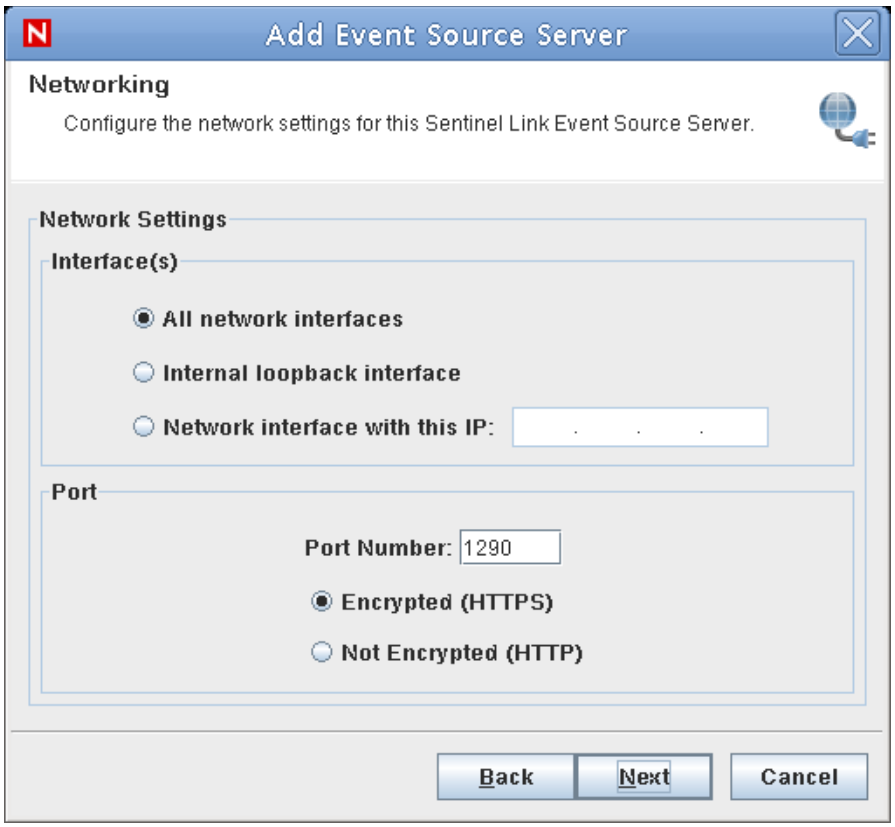
NOTE: These instructions assume that you have already downloaded and installed the Collector to process event data from the Sentinel Link Connector.

2.4.1 Configuring Sentinel Link Event Source Server

Configure a Sentinel Link Event Source server to set up a Sentinel Link connection to start processing the data received from the sender system. After you add a Sentinel Link Event Source server, the required Collector, the Connector, and the Event Source nodes are automatically created and configured when the server receives the events from the sender system. Allowing the Sentinel Link Event Source server to auto-create the nodes is much simpler and is preferred over manual configuration because it ensures that nodes are properly configured and connected so that events are routed to the Sentinel Link Collector.

1 In the Event Source Management view, right-click the Collector Manager, select *Add Event Source Server*, then select *Sentinel Link Connector* and click *Next*.

The Networking window is displayed.

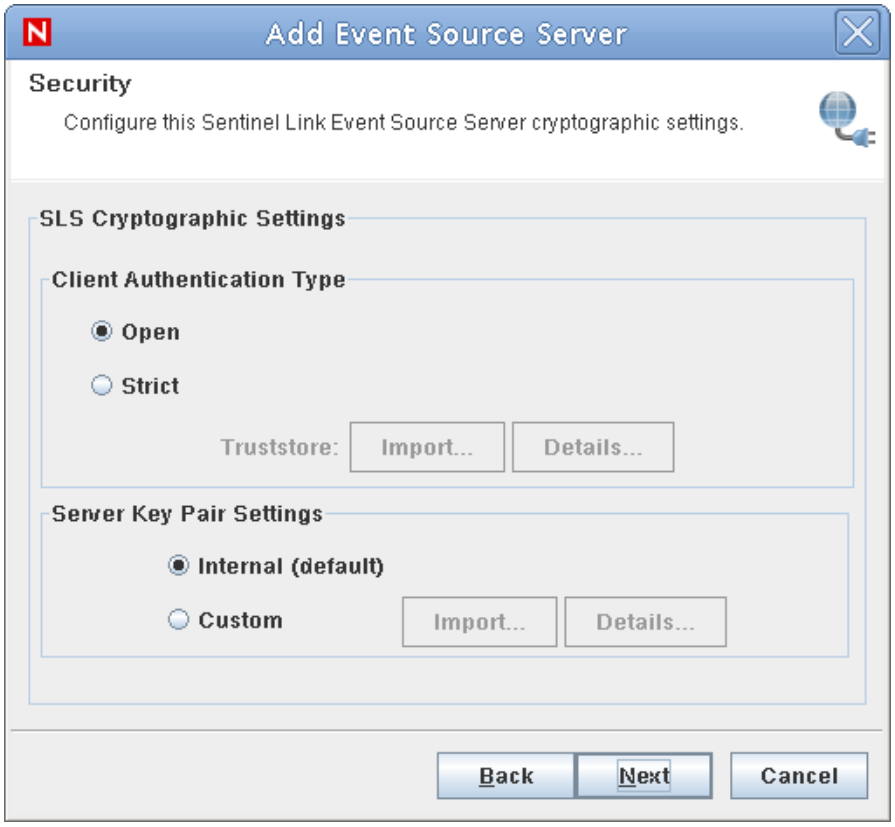


2 Specify the following, then click *Next*.

Options	Description
Interface(s)	Specify any of the following: ◆ **All network interfaces:** Binds the port on all the IP addresses of the machine, including local loopback. ◆ **Internal loopback interface:** Binds the port only to the local loopback address. ◆ **Network interface with this IP:** Allows the port to be bound to one IP address on the machine with multiple IP addresses.
Port Number	Specify the port number. The default port number is 1290. **NOTE:** If the Sentinel Link Event Source Server is running on a Linux/Unix machine, binding to port numbers less than 1024 requires root privileges. Therefore, Novell recommends that you run the server on a port greater than 1024 and change the source devices to send to this new port or use port forwarding.

Options	Description
Encrypted (HTTPS) or *Not Encrypted (HTTP)*	Select either of the following: ◆ **Encrypted (HTTPS):** Allows secure message transport to the Sentinel Link Event Source Server. ◆ **Not Encrypted (HTTP):** Allows insecure message transport to the Sentinel Link Event Source Server.

3 In the Security window for configuring authentication settings on the HTTPS port, specify the following:

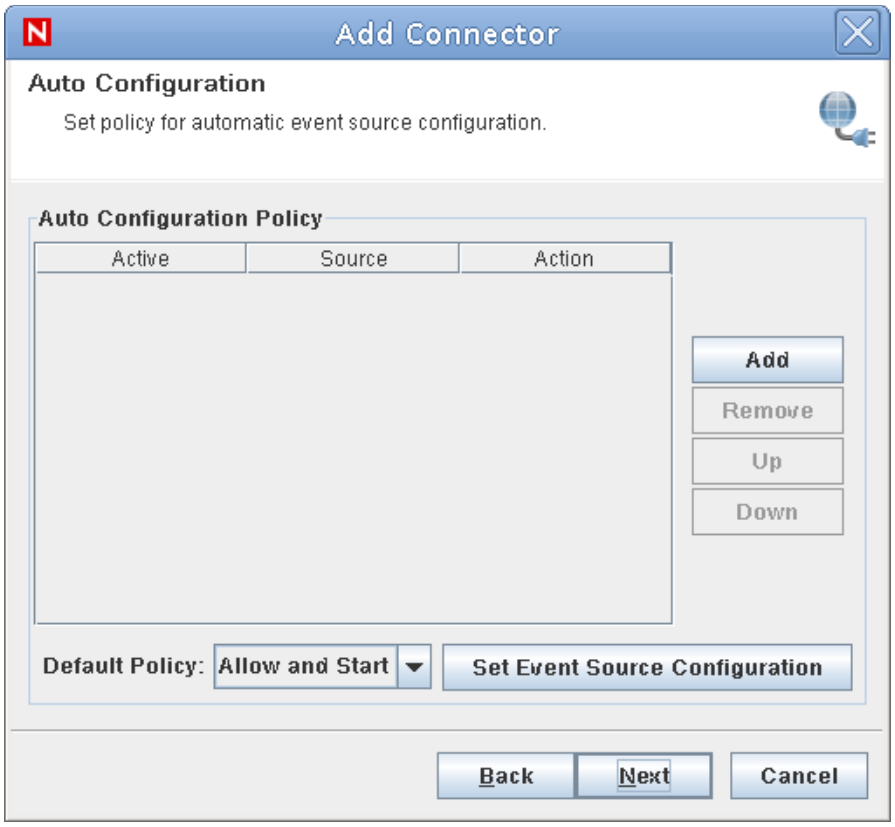


Options	Description
Client Authentication Type	Specify either of the following: ◆ **Open:** Allows HTTPS connections from any sender machines. It does not perform any client certificate validation or authentication. ◆ **Strict:** Validates that the sender's certificate in the trust store and is a valid X.509 certificate. For this option, a truststore needs to be imported. Use the *Import* button to do this. The truststore should have the sender's certificate, which is signed by a CA. Click the *Details* button to display the list of certificates imported from the truststore.
Server Key Pair Settings	Specify either of the following: ◆ **Internal:** The Internal (default) option directs the Sentinel Link Connector to generate a server key pair. ◆ **Custom:** Select this option, then click *Import* to import a server key pair that the embedded tomcat server uses. The imported keystore must contain at least one private/public key pair. If the keystore has more than one, a popup screen allows you to select one of the key pairs. The server key pair *Details* button displays the certificate imported from the keystore.

4 Click *Next*.

The Auto Configuration window is displayed.

In this window, you can create policies to automatically add or exclude individual Sentinel source machines. You can select IP addresses, ranges or subnets to be auto-configured, auto-configured and started, or ignored by the Connector.



The Sentinel Link Event Source Server simplifies Event Source configuration with the option to detect a new source device that is sending data to the Sentinel Link Event Source Server, evaluate its IP address by using a set of user-defined policies, and either ignore the new source device or automatically add it as an Event Source in Event Source Management.

5 Click *Add* if you want to create a new policy.

6 Double-click the *Source* field and enter a source IP address or a range of IP addresses in one of the following formats:

- Specific IP address (such as 10.0.0.1)
- IP address range (such as 10.0.0.1-10.0.0.25)
- IP address with mask (like 10.0.0.1/16)

7 Select an action to associate with the IP address or range of IP addresses:

- The *Allow and Start* action creates and starts Event Source node in the ESM view.
- The *Allow* action auto-creates the Event Source node in the ESM view but does not auto-start the Event Source.

  After the new Event Source node is created, an administrator can review and start it at any time.
- The *Deny* action prevents the auto-creation of an Event Source.

8 Select *Active* to activate the policy.

If there are multiple policies, reorder the order in which they are evaluated by using the *Up* and *Down* buttons.

9 Set the Default Policy, which applies to all sources that do not meet any of the criteria defined by the policies above.

10 To set the filtering and configuration settings for all automatically-created Event Sources, click the *Set Event Source Configuration* button. For more information on these options, see "Adding Event Sources" on page 25.

TIP: Auto-configured Event Sources should not be manually deleted in the Event Source Management interface because they are auto-configured again when the Connector restarts. To block a particular source device, add a Deny policy in Auto Configuration.

---

11 Click *Next* to display the General properties window.

12 Select *Run* to run the Sentinel Link Server automatically whenever the Collector Manager is restarted.

13 Click *Finish* to complete the configuration of the Sentinel Link Event Source Server.

2.4.2 Manually Setting Up the Sentinel Link Connection

Although the Event Source server is capable of auto-creating the needed Collector, Connector, and Event Source nodes, you might also want to manually create the Collector, the Connector, and the Event Source nodes.

Regardless of which way you choose, you must configure an Event Source server. For more information, see Section 2.4.1, "Configuring Sentinel Link Event Source Server," on page 14. This section assumes that you have already configured an Event Source server.

NOTE:

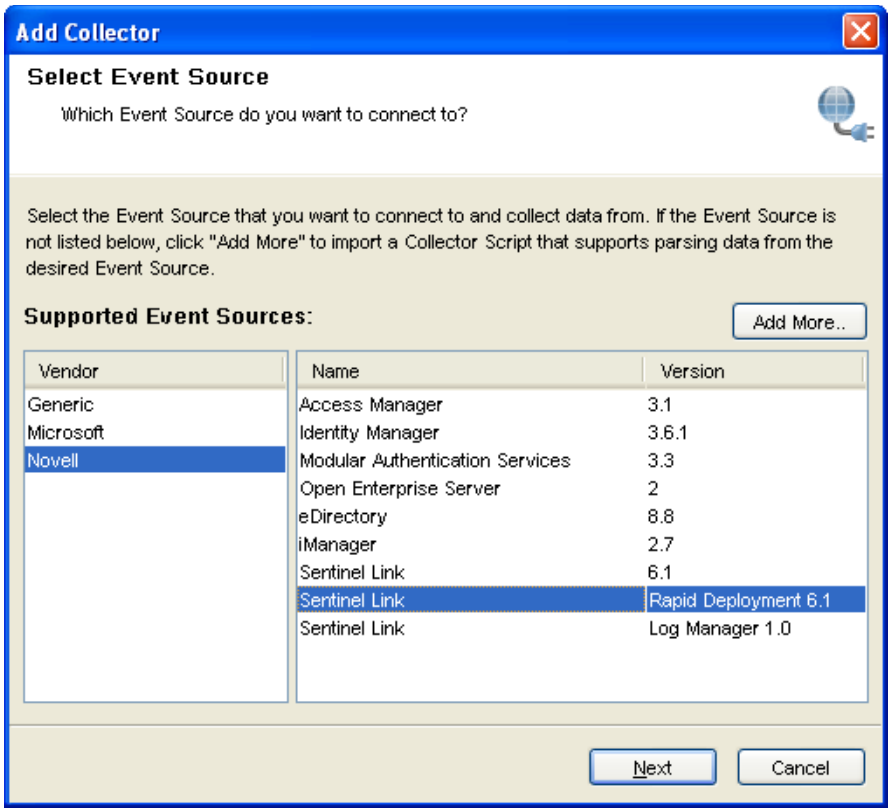
- If you have not created an Event Source server, you are given the option to do so during the configuration of Connector nodes.
- The plug-in versions shown in the images are just examples. When you set up Sentinel Link, the current version of the plug-in is displayed.

- "Adding a Collector" on page 19
- "Adding a Connector" on page 21
- "Adding Event Sources" on page 25

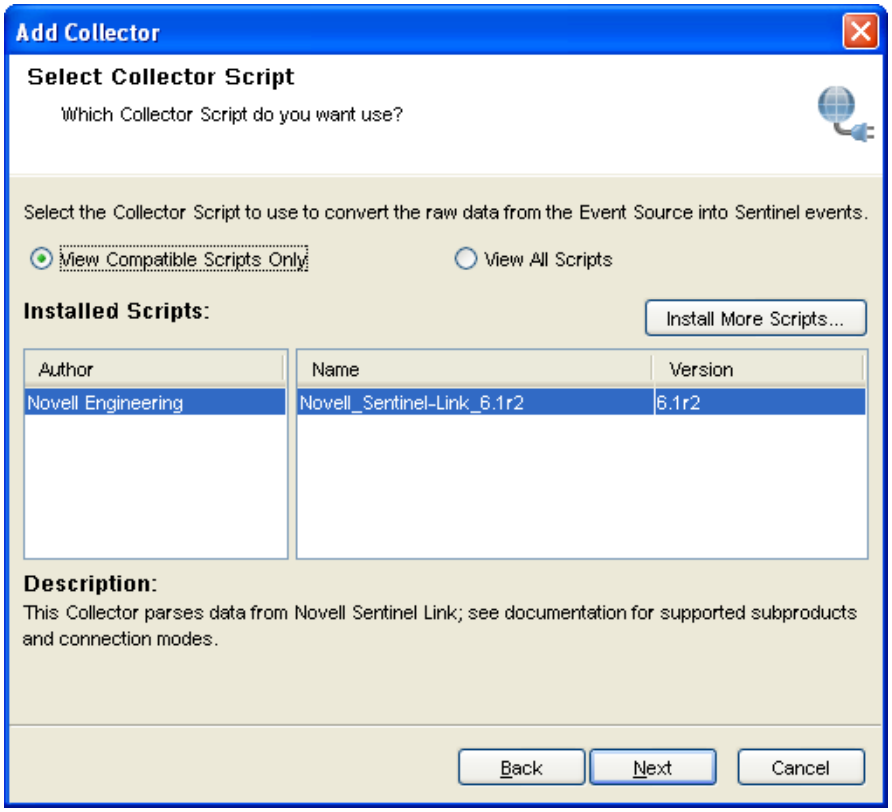
Adding a Collector

1 In the Event Source Management (Live View), right-click the Collector Manager node, then select *Add Collector*.

2 Select *Novell* from the list of vendors from the left panel, then select the desired Sentinel Link version from the list of supported event sources, and click *Next*.



3 Select the Novell Sentinel Link Collector, then click *Next*.



4 Click *Next* to accept the default Collector properties.

   For more information on Collector properties, see the Sentinel Link Collector documentation.

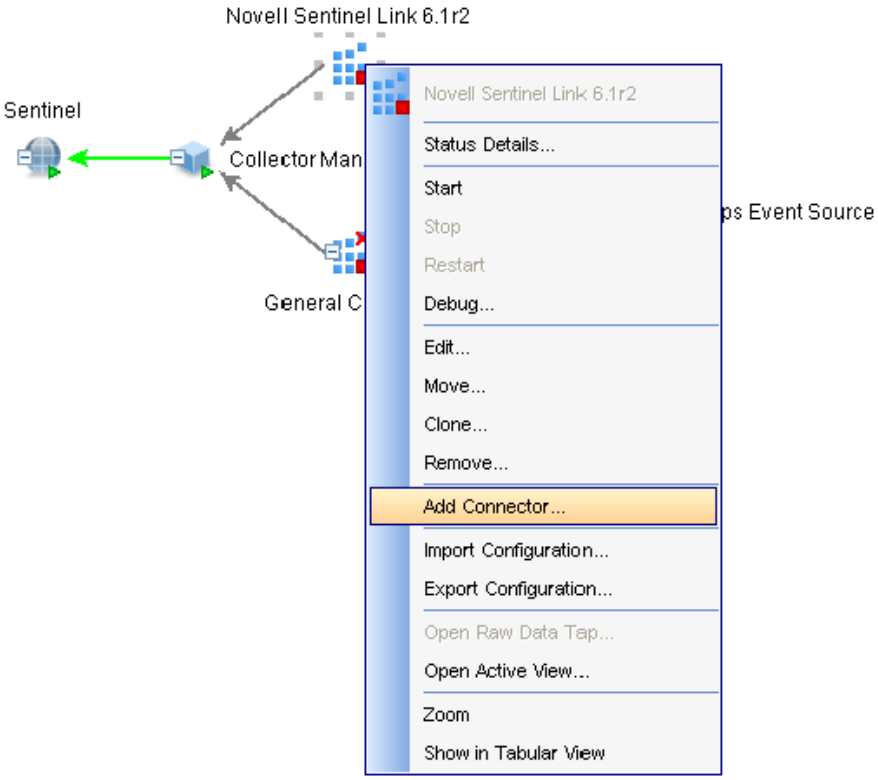
5 Accept the default Collector configuration, then click *Finish* to complete the configuration.

6 Continue with "Adding a Connector" on page 21.

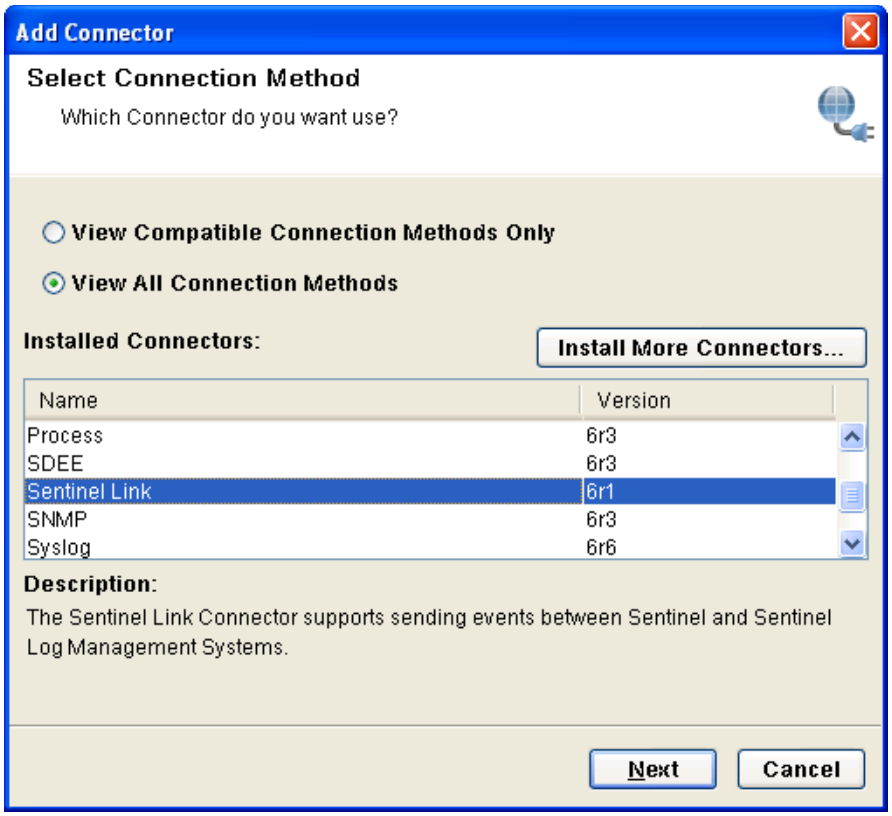
Adding a Connector

In addition to the typical Collector Manager > Collector > Connector > Event Source hierarchy, the Sentinel Link Connector also requires a Sentinel Link Event Source Server.

1 In the Event Source Management (Live View), right-click the Collector node that should process the data retrieved from the Sentinel Link Connector, then select *Add Connector*.



2 In the Select Connection Method window, select *Sentinel Link* from the list of plug-ins, then click *Next*.

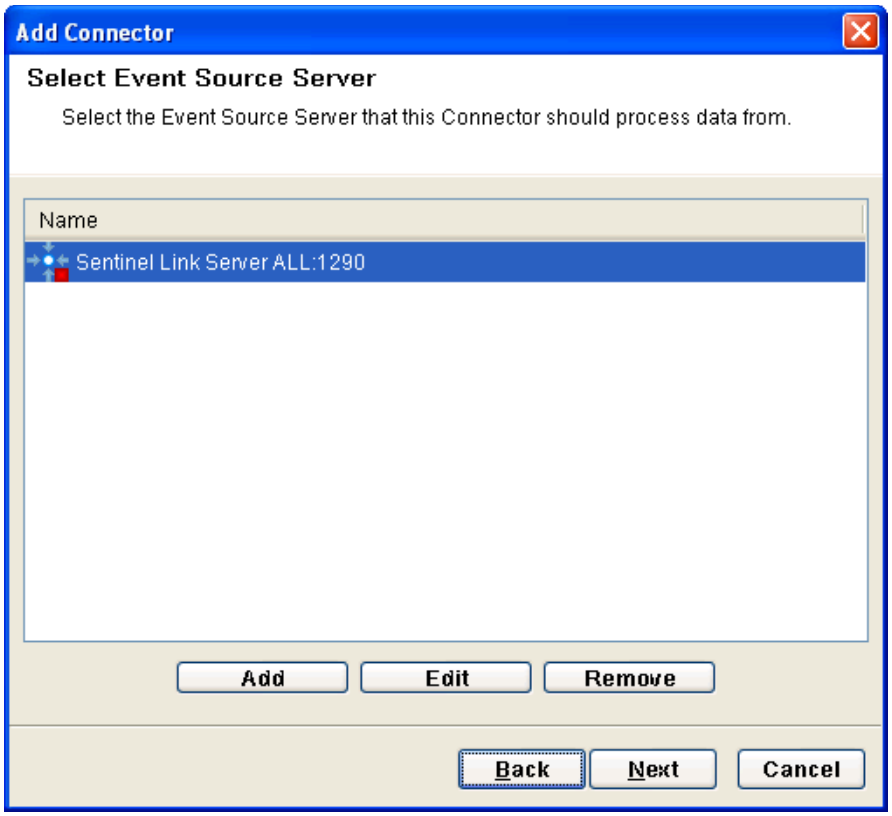


If you don't see the Sentinel Link Connector in the list, use the instructions Section 2.3, "Importing the Sentinel Link Connector," on page 13 to install it.

3 In the Select Event Source Server window, select the Event Source Server from the list of configured Event Source Servers.

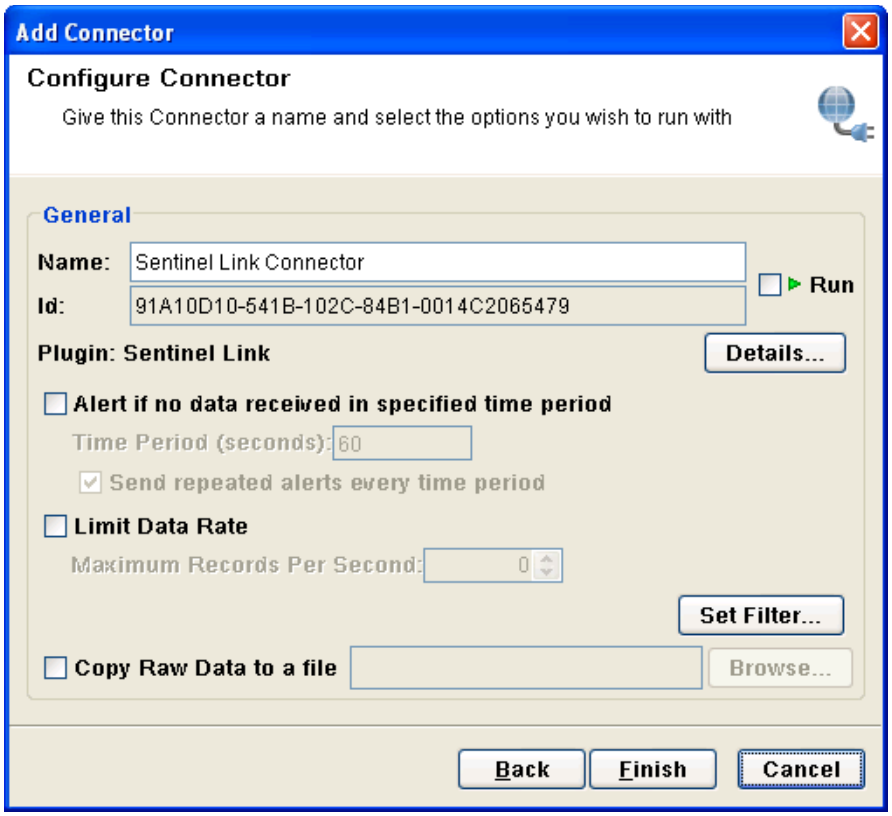
If no Event Source Servers are configured, the following message displays:

```
There are no Event Source Servers configured on this Collector Manager
that match the connection method selected. Please add an Event Source
Server with a matching connection method or choose a different connection
method.
```



4 Click *Add*, then create an Event Source Server. For more information on creating an Event Source server, see Step 2 through Step 13 in the Section 2.4.1, “Configuring Sentinel Link Event Source Server,” on page 14.

5 Click *Next* to open the Configure Connector window.



6 In the Configure Connector window, specify the following:

Options	Description
Name	The name by which you want to identify this Connector.
Id	The Id of the Connector. You cannot change this value.
Details	Click *Details* if you want to open the Plugin Details window.
Run	(Optional) Select this option if you want to specify that the Connector should by default be started whenever the Collector Manager is started.
Alert if no data received in specified time period	(Optional) Select this option to send *No Data Alert* event to Sentinel if no data is received by the Connector in the specified time period. You also have an option, *Send repeated alerts every time period*, to resend the alert if multiple time periods consecutively pass without receiving data from the Connector. Specify the time in seconds. By default the value is 60 seconds.
Limit Data Rate	(Optional) You can set a maximum limit on the rate of data the Connector can send to Sentinel. If the data rate limit is reached, Sentinel begins to throttle back on the source to limit the flow.
Set Filter	(Optional) You can specify a filter for the raw data that passes through this Connector.
Copy Raw Data to a file	(Optional) You can copy the raw data, which passes through this Connector, to a file for further analysis. To save the raw data, click the *Browse* button to specify a location to save the data.

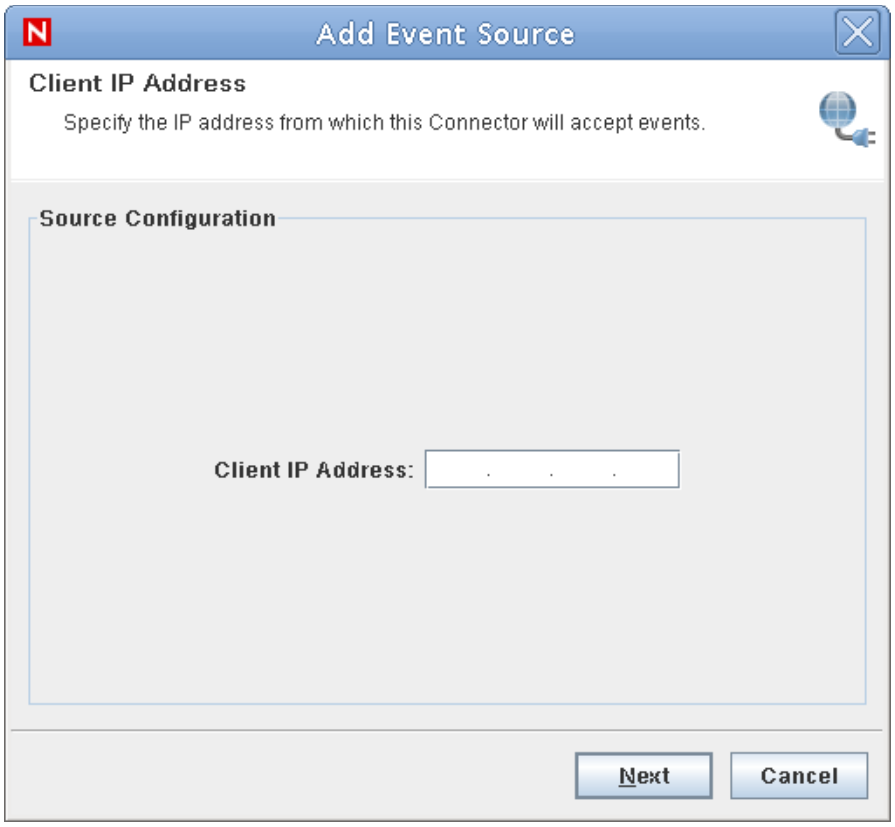
7 Click *Finish* to confirm adding the Connector to the Event Source Management view.

Adding Event Sources

Sentinel Link Event Sources can be automatically detected and added according to user-configured rules, or they can be added manually.

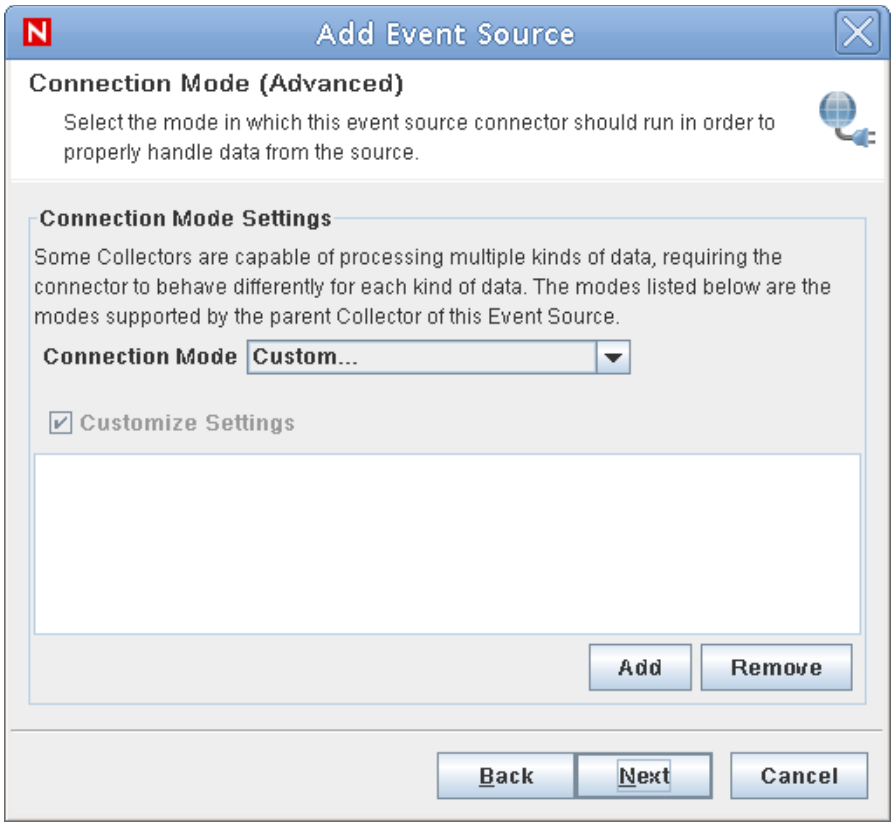
1 In Event Source Management, right-click the Sentinel Link Connector, then select *Add Event Source*.

The Client IP Address window displays.



2 Specify the IP address of the sender machine, which the Sentinel Link event source receives the messages from.

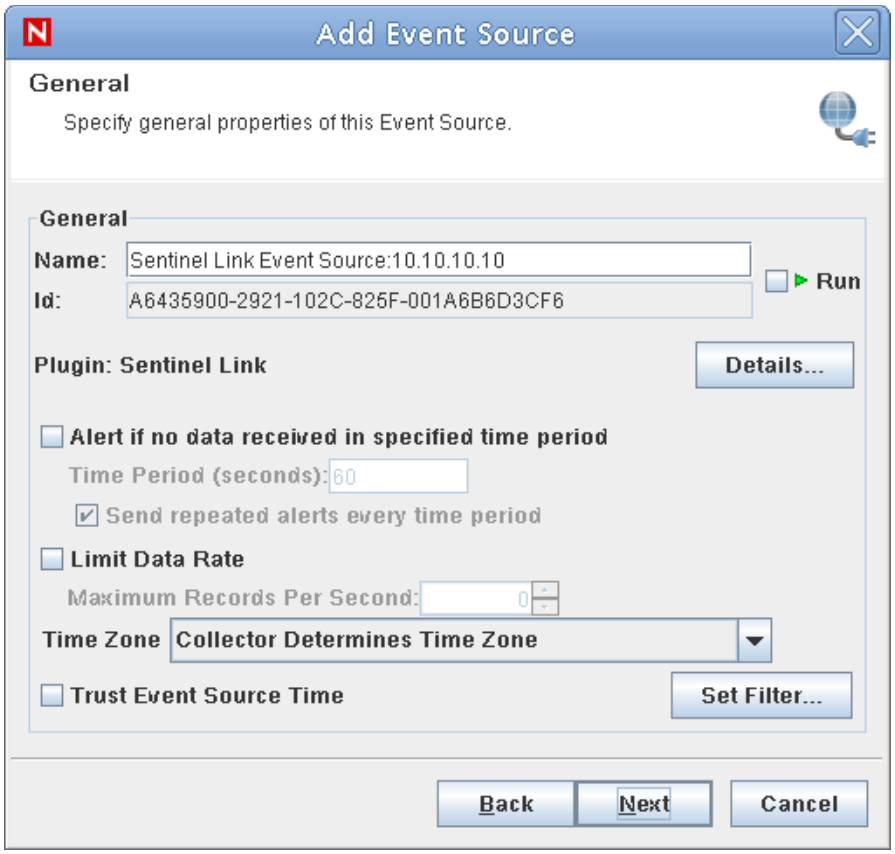
3 Click *Next*.



The Connection Mode (Advanced) window displays and shows all preset connection modes that are supported by the Collector. Each connection mode sends the data in a different format. For the Novell Collectors, which support more than one connection mode for different data formats, see the Collector-specific documentation for information about which mode is appropriate for your particular Event Source.

4 Select a Connection Mode.

5 Click *Next*. The General window displays.



6 Specify the General settings for the Sentinel Link Connector:

Options	Description
Name	The name by which you want to identify this Event Source.
Id	Specifies the Id of the Event Source.
Details	Click *Details* to display the Plugin Details window.
Run	(Optional) Select this option to specify that this event source should by default be started whenever the Collector Manager is started.
Alert if no data received in specified time period	(Optional) Select this option to send *No Data Alert* event to Sentinel, if no data is received by the event source in the specified time period.
Limit Data Rate	(Optional) Set a limit for the rate of data this event source can send to Sentinel. If the maximum rate limit is reached, Sentinel begins to throttle back on the source to limit the flow.
Timezone	Specify the time zone for the event source. **NOTE:** This setting is not currently used by a Sentinel Link event source.

Options	Description
Trust Event Source Time	(Optional) Select this option to have the event time set to the time the event occurred rather than the time Sentinel received the data.
Set Filter	(Optional) Specify a filter on the raw data passing through this event source.

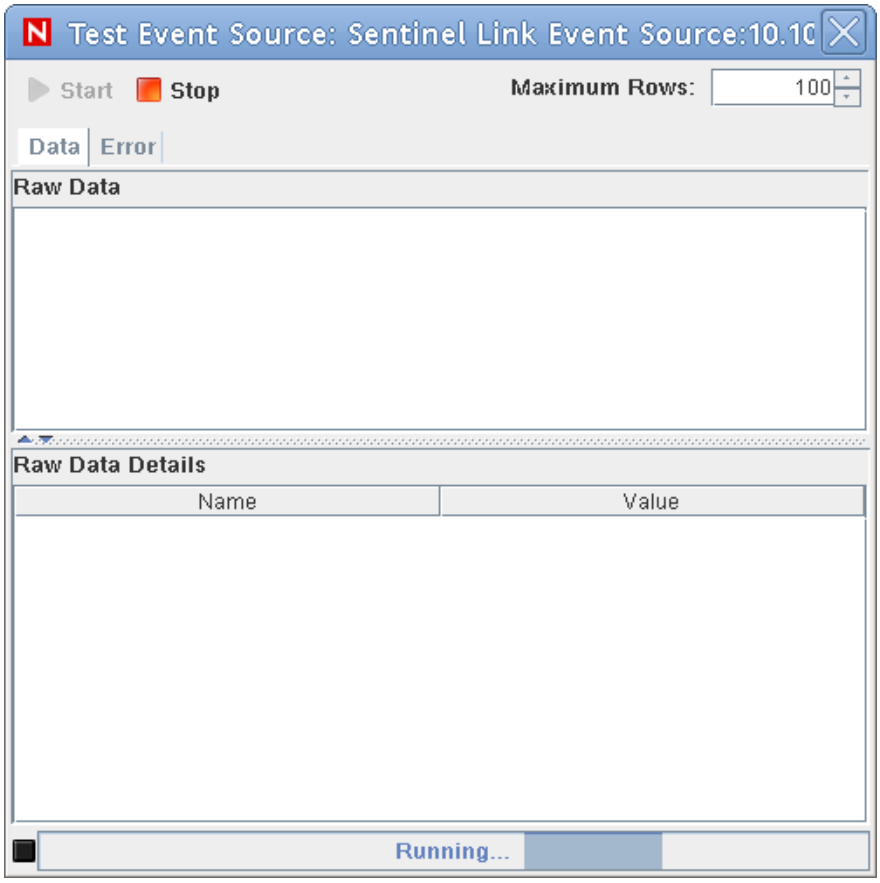
7 Click *Next*.

The Summary window is displayed.

8 To test the configuration, click *Test Connection*.

NOTE: The Sentinel Link Event Source Server and Connector must be running to list the messages in the Test Connection window.

The Test Connection window is displayed with *Data* and *Error* tabs.



8a On the *Data* tab, specify the maximum number of rows of data to be displayed in the Test Connection window at one time.

8b Click *Start* to start the connection test.

The *Data* tab displays the events generated on successful connection with the Event Source.

If there are errors, click the *Error* tab to display any errors in the event source configuration.

8c Click the *Stop* button to stop the connection test.

8d Close the Test Connection window.

9 Click *Finish* to add the Event Source to the Event Source Management view.

Configuring Sentinel Systems for Sending Events

3

You can configure Novell Sentinel Log Manager, Sentinel, or Sentinel Rapid Deployment to forward events to another Sentinel system.

3.1 Configuring Sentinel or Sentinel Rapid Deployment System as a Sender

If Sentinel or Sentinel Rapid Deployment is the sender, you must import and configure Sentinel Link Integrator plug-in and Sentinel Link Action plug-in to create a Sentinel Link configuration. You also need to create an action that forwards the selected events to the receiver system. To filter the events, set a correlation rule by using the Correlation Manager. After creating the rule, associate the action to it, and deploy the rule. You can also use Global Filters to filter the events and forward them to the receiver system.

NOTE: For more information on Sentinel Link Integrator and Action, see the corresponding plug-in documentation in the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html).

Follow the instructions given below to configure Sentinel or Sentinel Rapid Deployment server for sending the events:

3.1.1 Configuring the Integrator Plug-In

The Sentinel Link Integrator allows you to forward the events to another Sentinel system.

Installing the Integrator Plug-In

1. Ensure that you download the Sentinel Link Integrator (.zip) file from the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) to the local machine, where Novell Sentinel Control Center is launched.

NOTE: Always use the latest Sentinel Link plug-ins available from the Sentinel Plug-ins Web site.

2. In the Novell Sentinel Control Center, select *Tools* > *Integrator Manager*. The Integrator Manager window displays.

   (Conditional) If you are working with Sentinel 7.0, click the Configuration tab and select Integrator Manager. The Integrator Manager window displays.

3. Click *Manage Plug-Ins*.

   The Integrator Plugin Manager window displays.You use this window to add, delete, refresh, view Integration plug-in details, configure Integrators, and add auxiliary files.

4. Click *Import*  icon in the Integrator Plugin Manager window.

   The Plugin Import Type window displays.

5. Select *Import an Integrator plugin file (.zip)*, then click *Next*.

   The Choose Plugin Package File window displays.

6. Click *Browse* to locate an Integrator file to import to the plug-in repository.

7. Select a zip file, then click *Open*.

8. (Conditional) If you have selected an Integrator file that already exists, then the Replace Existing Plugin? window displays. Click *Next* if you want to replace the existing plug-in.

9. Click *Next*.

   The details of the plug-in to be imported are displayed in the Plugin Details window.

10. (Conditional) If you want to deploy the plug-in after importing the Integrator plug-in, select the *Launch Integrator Configuration Wizard* check box.

11. Click *Finish*.

    For more information, see the Sentinel product documentation:

    - **Sentinel 6.x:** “Sentinel User Guide” (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/).
    - **Sentinel 6.1 Rapid Deployment:** “Sentinel 6.1 Rapid Deployment User Guide” (http://www.novell.com/documentation/sentinel61rd/s61rd_user/?page=/documentation/sentinel61rd/s61rd_user/data/).
    - **Sentinel 7.0:** “Sentinel 7.0 Administration Guide” (http://www.novell.com/documentation/sentinel70/s70_admin/index.html?page=/documentation/sentinel70/s70_admin/data/bookinfo.html).

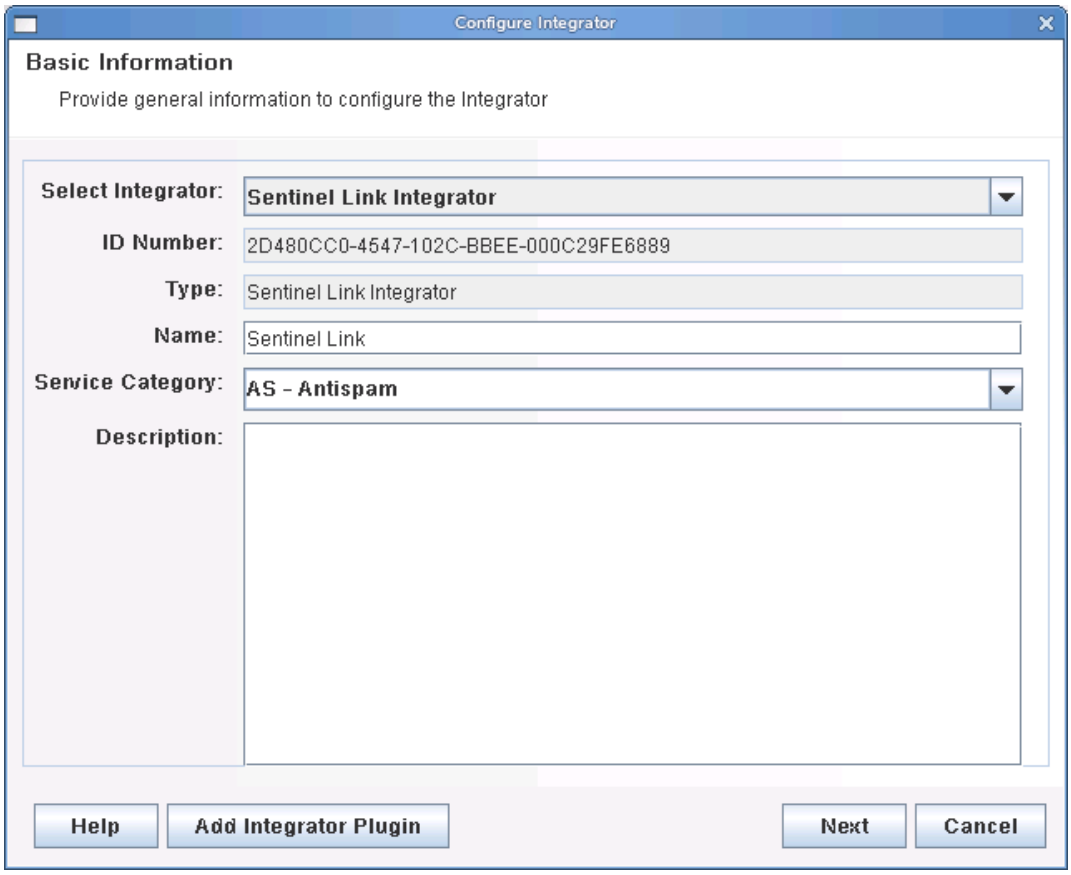
Configuring the Integrator Plug-In

To use an Integrator plug-in, one or more Integrator instances must be configured with valid connection information.

1. Log in to the Novell Sentinel Control Center as an administrator.
2. Select *Tools* > *Integrator Manager*. The Integrator Manager window displays.

   (Conditional) If you are working with Sentinel 7.0, click the Configuration tab and select Integrator Manager. The Integrator Manager window displays.

3. Click the *Add Integrator* icon in the bottom left corner. The Basic Information window displays.



4 Select *Sentinel Link Integrator* from the *Select Integrator* drop-down list.

5 Click *Add Integrator Plugin* to import Integrator plug-in, if the Integrator plug-in is not already available. For more information on importing the Integrator plug-in, see Section 3.1.1, "Configuring the Integrator Plug-In," on page 31.

The *ID Number* is the system-generated ID for the Integrator configuration and cannot be edited.

Type represents the type of Integrator plug-in selected from the drop-down.

6 Specify a name for the integrator in the *Name* field.

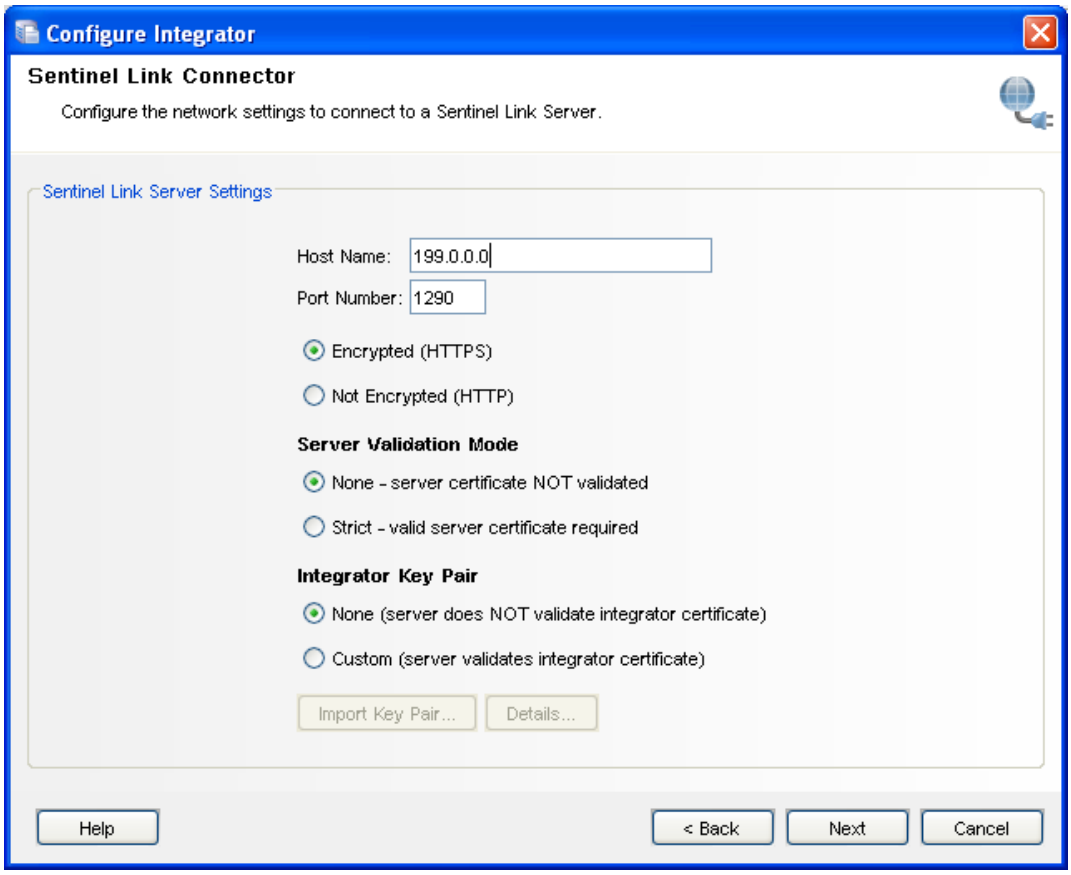
7 Specify a description for the integrator in the *Description* field.

8 Select an Integrator Service category from the *Service Category* drop-down list, or type a name in the field to create a custom service type. These services are used to group similar Integrator instances. The following table list of the Integrator Service categories:

Integrator Service Category	Description
AS	Antispam
AV	Antivirus
BM	Business Management
CM	Configuration Management
DB	Database

Integrator Service Category	Description
EML	E-Mail System
FIN	Financial Application
FW	Network Firewall
HFW	Host-based Firewall
HR	HR Application
IDM	Identity Management
IDS	Intrusion Detection/Prevention System
INCM	Incident Management
NETD	Network Router/Switch
OS	Operating System
PROX	Proxy
STO	Storage
VPN	Virtual Private Network
VULN	Vulnerability Scanner
WEB	Web Server

9 Click *Next*. The Sentinel Link Server Settings window displays.



10 Specify the IP address or hostname of the Sentinel Link server, where the Sentinel Link Connector is running.

11 Specify the port number for the sentinel system. The default port is 1290.

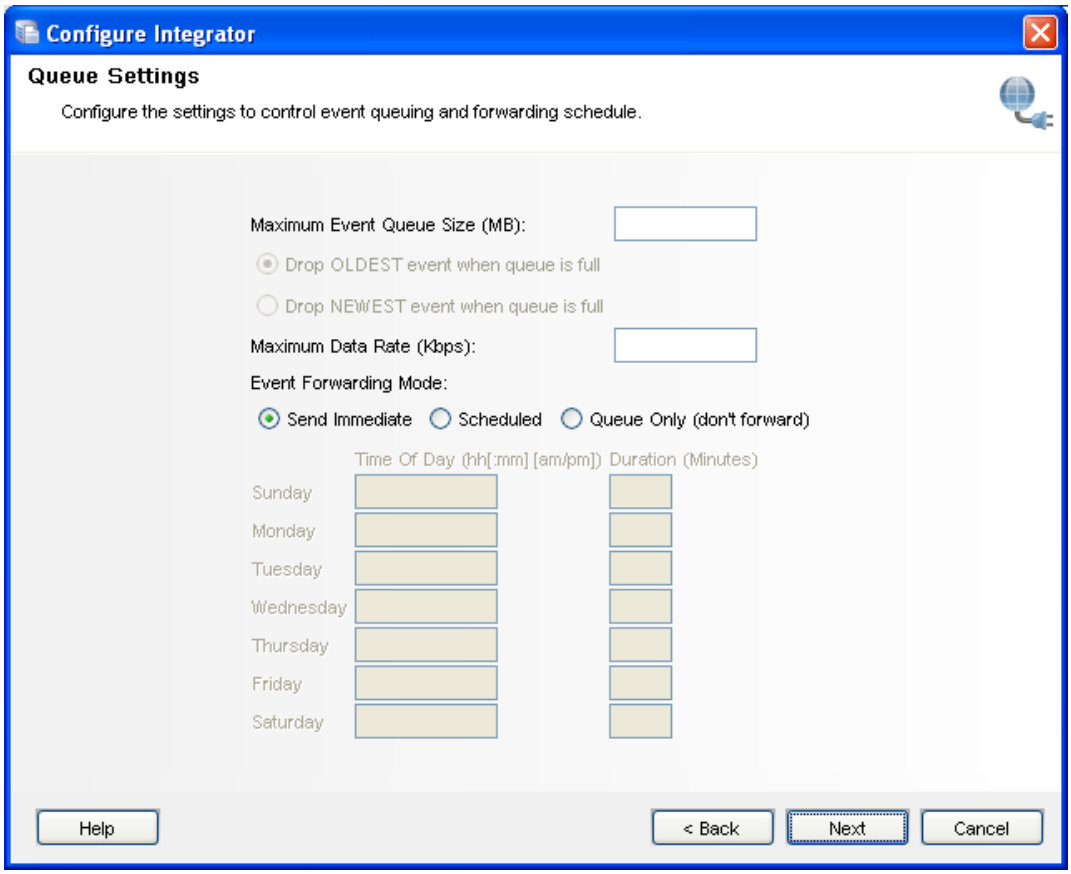
12 Select either of the following:

- **Not Encrypted (HTTP):** Establish an unsecured connection.

- **Encrypted (HTTPS):** Establish a secured connection. If you select the encrypted (HTTPS) option, you are optionally allowed to specify a Server validation mode and an Integrator key pair.

Field	Description
Server Validation Mode	Select either of the following: ◆ **None- server certificate NOT validated:** The Integrator does not validate the receiver's certificate. ◆ **Strict - valid server certificate required:** The Integrator always verifies the receiver's certificate when connecting to the receiver. If this option is selected, the Integrator immediately attempts to retrieve the receiver's certificate over the network and validate that it is issued by an authorized CA. If the certificate is not validated for some reason, it is still presented to the user to accept or reject. The certificate is considered to be valid if the user accepts it. When a validated certificate is acquired, it is stored in the Integrator's configuration. Henceforth, the Integrator allows communication only with a receiver that provides that certificate during the initial connection setup.
Integrator Key Pair	Select either of the following: ◆ **None (server does not validate integrator certificate):** The receiver system does not validate the sender certificates. Select this option if the receiver's client authentication type is configured to *Open*. ◆ **Custom (server validates integrator certificate):** The receiver system validates the sender certificates. Select this option if the receiver's client authentication type is configured to *Strict*. If the receiver system performs a strict validation, it imports a trust store, which contains all the sender certificates that it trusts. After selecting this option, click the *Import Key Pair* button to import a key pair. The key pair you import must match one of the certificates that is included in the trust store, which is imported by the receiver system.

13 Click *Next*. The Queue Settings window displays.

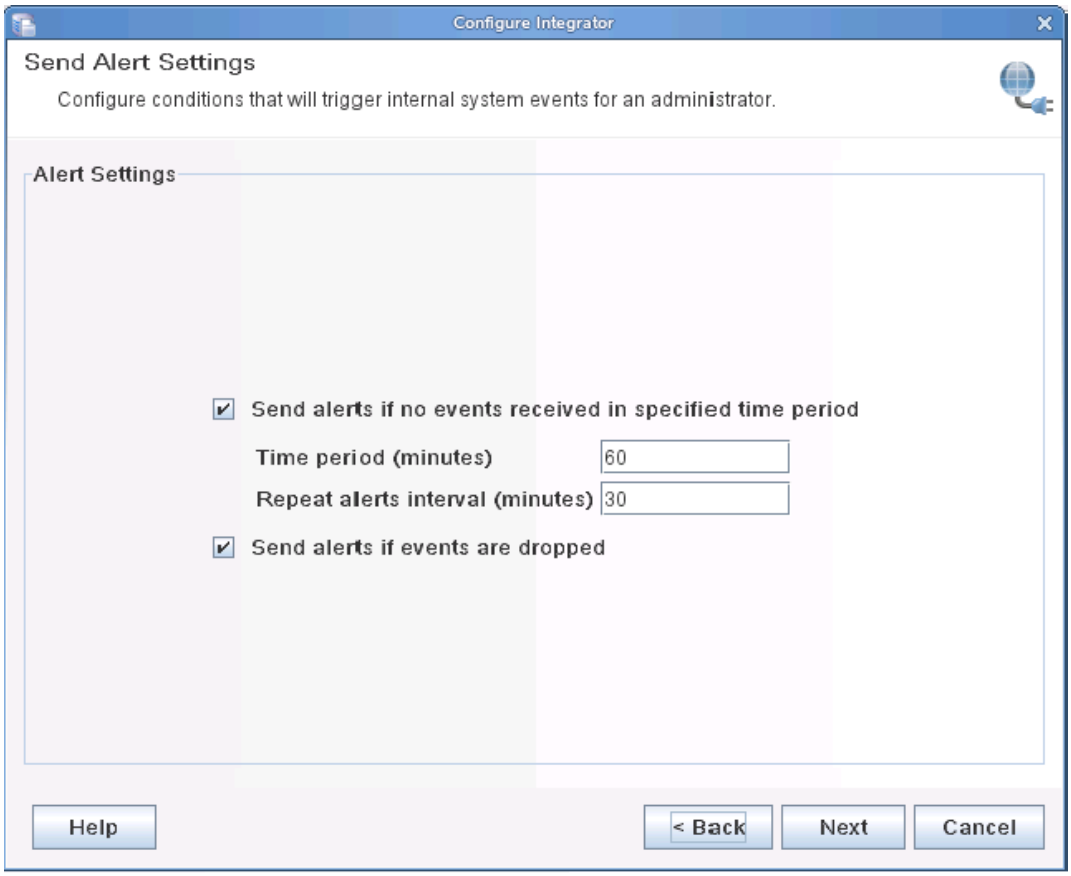


14 Specify the following:

Options	Description
Maximum Event Queue Size (MB)	Specify the maximum event queue size value in megabytes. The value must be between 0 and 2147483647. The following options are enabled only when you specify a value in the *Maximum Event Queue Size (MB)* field. ◆ **Drop OLDEST event when queue is full:** Select this option to drop the oldest events in the event queue when the value specified in the *Maximum Event Queue Size (MB)* field exceeds the limit. ◆ **Drop NEWEST event when queue is full:** Select this option to drop the newest event when the value specified in the *Maximum Event Queue Size (MB)* field exceeds the limit.
Maximum Data Rate (Kbps)	Specify the maximum data rate value in kilobytes per second. The value must be between 0 and 2147483647.

Options	Description
Event Forwarding Mode	Select one of the following options to specify the Event Forwarding Mode: ◆ **Send Immediately:** Select this option to forward the events immediately to the receiver. ◆ **Scheduled:** Select this option to schedule event forwarding. You can specify *Time Of Day* and *Duration* (in minutes) for each day of the week. The valid format for *Time Of Day* is hh:[mm] [am|pm]. The duration must be between 1 and 1440 minutes. If you do not specify time or duration for any of the days in the week, the schedule is considered to be 24 hours a day, seven days a week. It is equivalent to the *Forward Events Immediately* option. ◆ **Queue Only (don't forward):** Select this option to stop forwarding the events to the receiver system. However, the integrator stores the events it receives in its queue unless the queue has a size limit and has reached its maximum capacity. This mode is useful if the receiver is down for maintenance or any network problems persist in communicating with the receiver system that might not be fixed immediately. In such situations, rather than continually trying to forward events, you can select this option to temporarily stop forwarding messages. After the problems are resolved, you can re-enable event forwarding by selecting the *Forward Events Immediately* or *Scheduled Events Forwarding* options.

15 Click *Next*. The *Alert Settings* window is displayed.



The Send Alert Setting allows a user to configure under what conditions the Integrator generates alerts (internal events) that can be monitored by a system administrator. There are two types of alerts, which can be enabled by selecting one of the following options:

- **Send alerts if no events are received in specified time period:** These alerts are generated when the integrator has not received any events for a specified time period. The internal event type for this alert is `NoEventsReceived`.

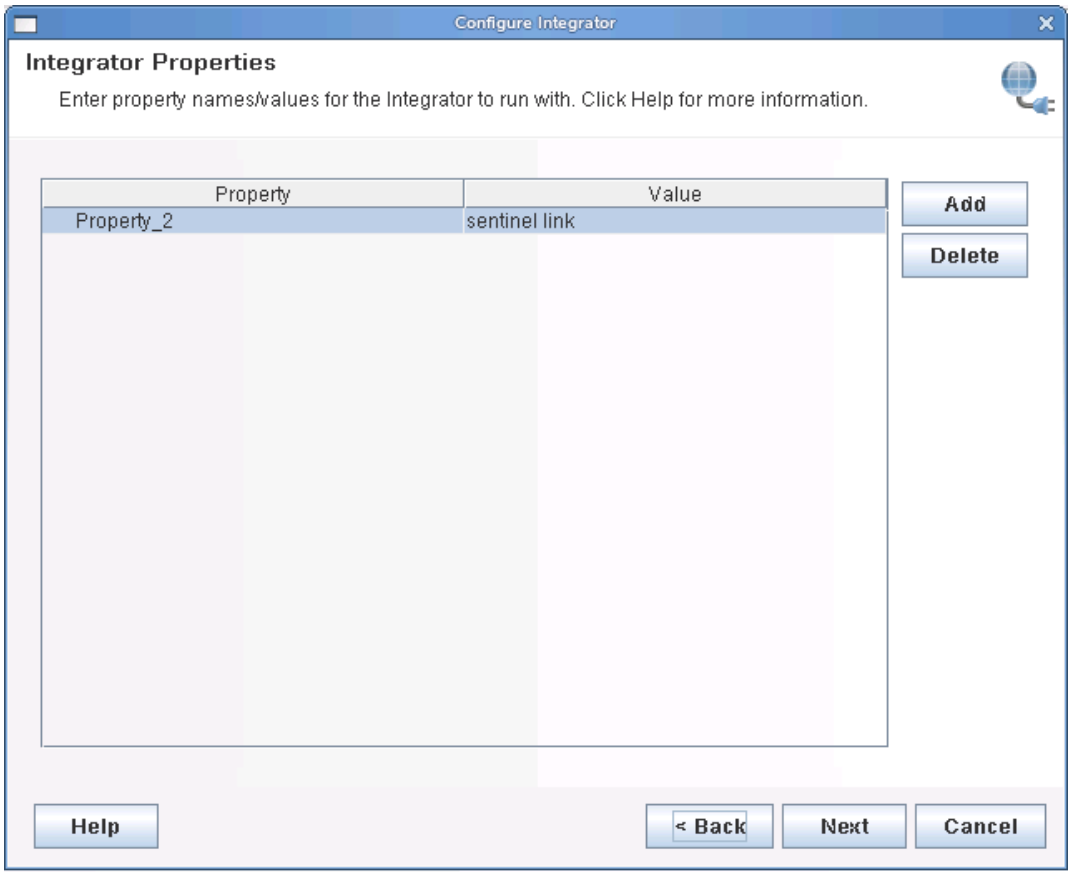
  If the *Send alerts if no events are received in specified time period* option is enabled, the user is allowed to specify two additional parameters:

  Time period (minutes): The time period is the number of minutes that must elapse without receiving an event before the integrator will generate the `NoEventsReceived` alert.

  Repeat alerts interval (minutes): The repeat alert interval is the number of minutes between repeating the `NoEventsReceived` alert. The alert is sent repeatedly at this interval until integrator starts receiving the events again.

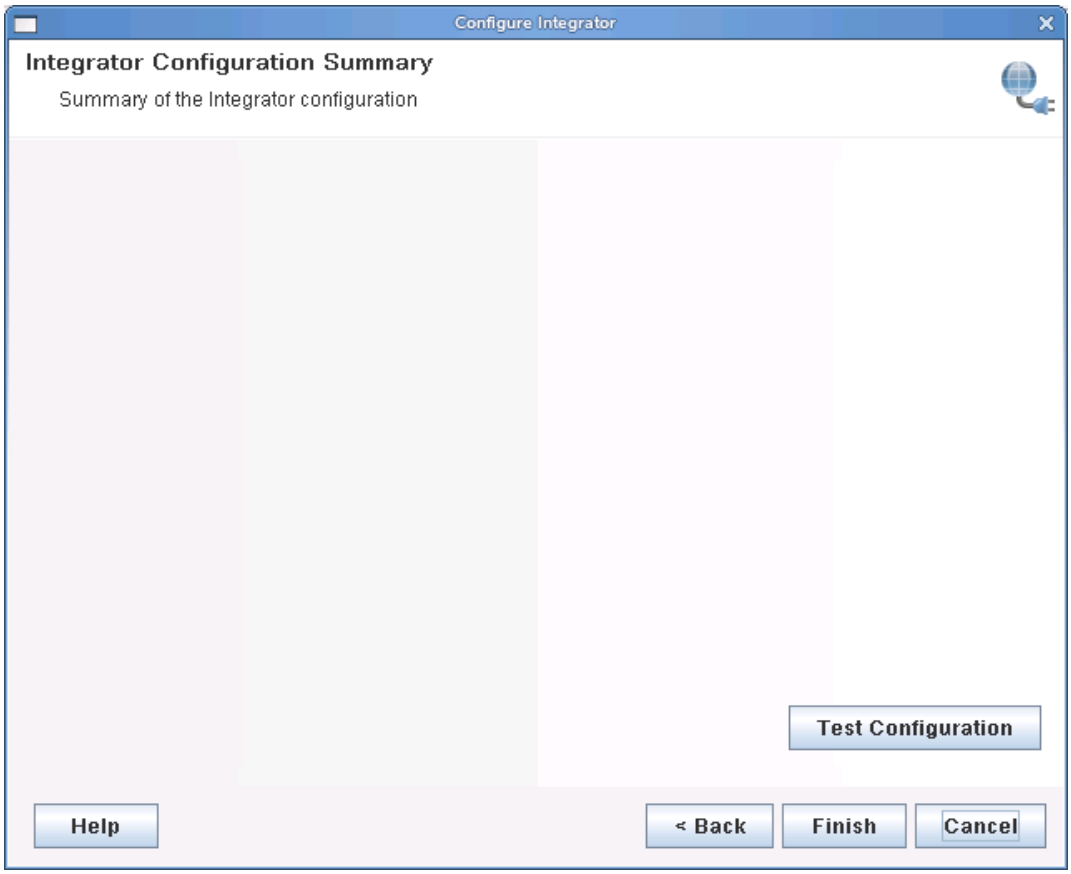
- **Send alerts if events are dropped:** These alerts are generated when the integrator drops the received events because its queue is full. The internal event type for this alert is `DroppedEvents`.

16 Click *Next*. The Integrator Properties window is displayed.



If the connection for your Sentinel Link server requires additional properties to establish a connection other than the fields provided, you can use the *Add* button to add properties. Specify the Property Name and Value. Press Enter. The Property is added to the Properties list in the Integrator Properties window. You can edit the property values if required. Repeat the steps to add more properties.

17 Click *Next*. The Integrator Configuration Summary window is displayed.



18 Click *Finish* to confirm configuring the Sentinel Link Integrator.

19 (Conditional) Click *Revert* to revert unsaved Integrator settings.

20 (Optional) To test the connection of the configured Sentinel Link Integrator, perform the following:

20a In the Integrator Manager window, select the Sentinel Link Integrator that you have configured.

20b Click *Test* to test the configuration.

A message is displayed stating that the `Integrator test was successful`, then click *OK*.

NOTE: This method tests the connection without actually sending any events to the Sentinel Link server. It does not update any statistics for the Integrator.

3.1.2 Importing and Configuring the Action Plug-In

1 Ensure that you download the Sentinel Link Action (.zip) file from the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) to the local machine, where Novell Sentinel Control Center is launched.

NOTE: Always use the latest Sentinel Link plug-ins available from the Sentinel Plug-ins Web site.

---

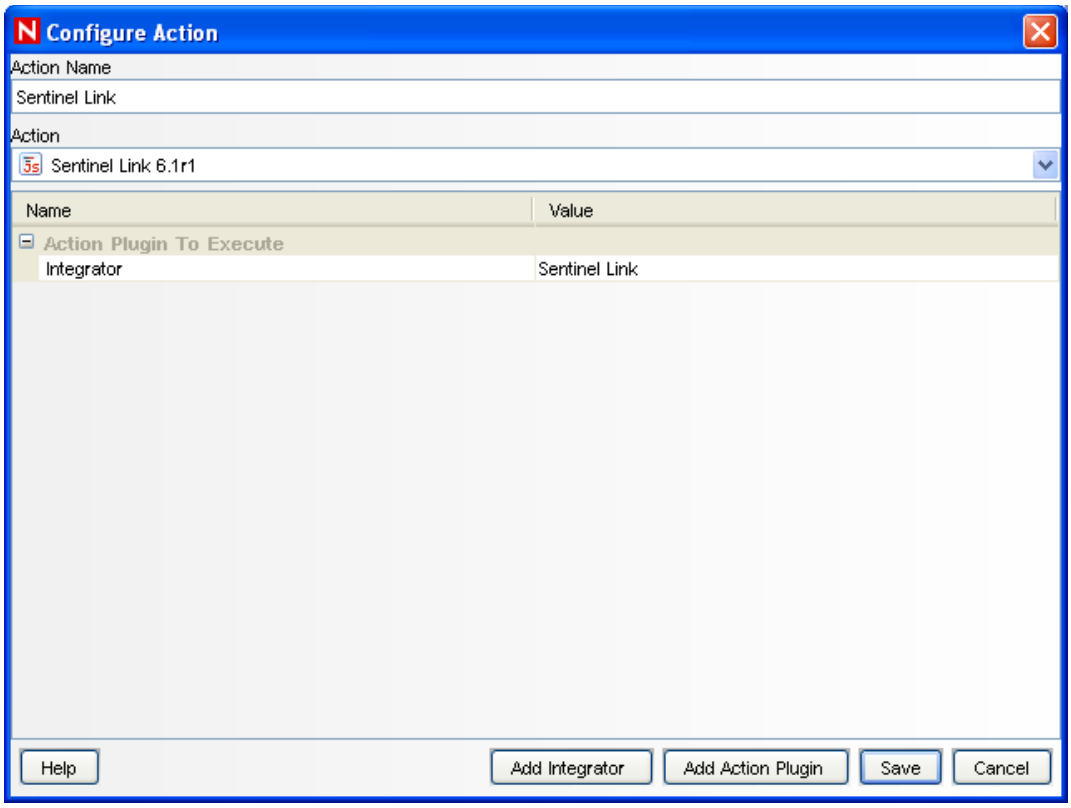
2. Log in to the Sentinel Control Center system as the administrator.
3. Select *Tools* > *Action Manager*.

   (Conditional) If you are working with Sentinel 7.0, click the Configuration tab and select Action Manager. The Action Manager window displays.
4. In the Action Manager window, click *Manage Plugin*s.

   The Action Plugin Manager window is displayed. In this window, you can add, delete, refresh, view Action plug-in details, configure and add auxiliary files.
5. In the Action Plugin Manager, click the Import  icon.
6. In the Import Plugin wizard, select *Import an Action plugin file (.zip)*, then click *Next*.
7. Click *Browse* to locate an Action file to import to the plug-in repository, select the zip file, then click *Open*.

   If you have selected an Action file which already exists, the Replace Existing Plugin? window displays. Click *Next* if you want to replace the existing plug-in.
8. Click *Next* to display the Plugin Details window.

   The details of the plug-in to be imported are displayed.
9. Click *Finish*.
10. Open the Action Configuration wizard, click *Add*, then specify the following:
    - **Action Name:** Specify a name for the action. For example, Sentinel Link.
    - **Action:** Select *Sentinel Link* from the drop-down.
    - **Integrator:** Select *Sentinel Link* from the drop-down.



11 Click *Save*.

3.1.3 Automatically Forwarding Events to the Receiver

To select events that you want to automatically forward to a receiver system, you need some filtering mechanism. Use Correlation rules or Global Filters to filter the desired events and associate the Sentinel Link Action to forward to the receiver system.

NOTE: To forward events to another Sentinel or Sentinel Log Manager system based on simple filtering conditions, use Sentinel Link with Global Filters.

Sentinel Link can also be used wherever else a javascript action can be executed in Sentinel such as Correlation, Incidents, and Event right-click. However, while event forwarding, the same event is likely to be forwarded more than once with these mechanisms. For example, using Correlation, you can have filter(1=1) and filter(e.sev>=3) configured, and launch Sentinel Link action to forward the events to the same receiver. When the action is triggered, the receiver gets duplicated events. Therefore, use them only when simple filtering conditions are not enough.

Note that some field values of the events are changed during event forwarding. For example, the event id is changed, but, the event name is preserved when you forward an event.

Another advantage of Global Filters over Correlation rule is that the events are sent in batches of 500 events to the receiver system. With Correlation rule, each event is forwarded to the receiver system as soon as an event is generated.

Using Correlation Rules to Forward Events to the Receiver

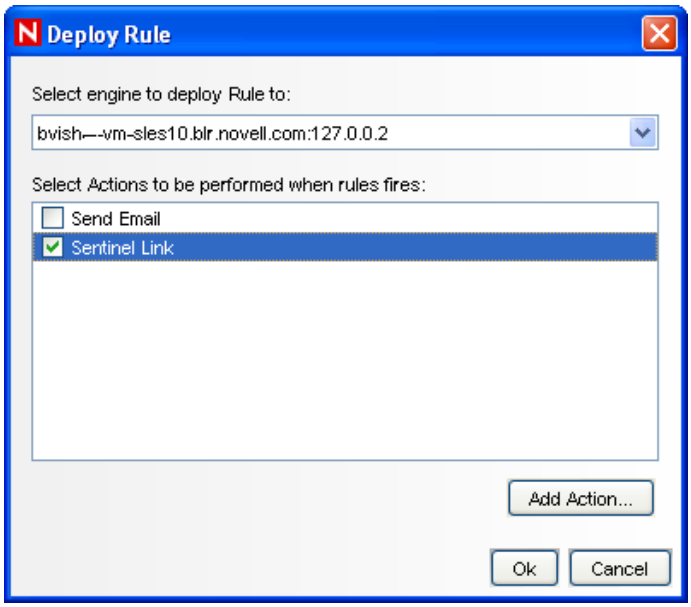
You can create Correlation rules that filter the desired events for forwarding to the receiver system. After creating a rule, associate the Sentinel Link Action while deploying the rule.

Sentinel 6.x and Sentinel Rapid Deployment

In the following example, a simple rule is created that forwards events with severity greater than 3.

1. In the Sentinel Control Center, select *Correlation Rule Manager*.
2. Click *Add*.

   The Correlation Rule wizard is displayed.
3. Click *Simple*. The Simple Rule windows is displayed.
4. Use the drop-down menus to set the criteria to `Severity>3`, then click *Next*. The Update Criteria window displays.
5. Select *Do not perform actions every time this rule fires* and use the drop-down menu to set the time period to 1 minute. Click *Next*. The General Description window displays.
6. Name the rule as *Sev4Rule*, provide a description, and click *Next*.
7. Select *No, do not create another rule* and click *Nex*t.
8. Click *Save*.
9. Select the Correlation Rule Manager window.
10. Select *Sev4Rule* and click *Deploy Rules* link. The Deploy Rule window displays.
11. In the Deploy Rule window, select the Engine to deploy the rule.



12 Select *Sentinel Link*, then click *OK*.

Sentinel 7.0

In the following example, a simple rule is created that forwards events with severity greater than 3.

1 Log in to the Sentinel Web interface as a user with the Manage Correlation Engine and Rules permission.

2 In the navigation panel, click *Correlation*.

The Correlation panel is displayed.

3 Click *Create*.

The Correlation Rule Builder is displayed.

4 In the Subrule window, click *Create a new expression*.

The Expression Builder is displayed.

5 Select the criteria to set it to `Severity>3`, then click *OK*.

The specified criteria are displayed in the subrule window.

6 To associate one or more actions to the rule, in the Actions panel, click  .

The list of Actions is displayed.

7 Select *Send Events via Sentinel Link* action.

8 Click *OK*.

9 Click *Save As*.

10 Specify an intuitive name, for example, *Sev4Rule* for the rule and an optional description, then click *OK*.

11 Double-click the rule that you want to deploy.

12 In the Deploy/Undeploy section, select the engine to which you want to deploy the rule, then click *Deploy*.

NOTE: You can also deploy a rule from the Correlation dashboard. In the Correlation panel, click the engine to which you want to deploy rules. The Correlation Engine dashboard is displayed. In the Available rules section, select the rule or rules that you want to deploy, then click *Deploy*.

Using Global Filters to Forward Events to the Receiver

You can use Global Filters to filter the desired events for forwarding to the receiver system.

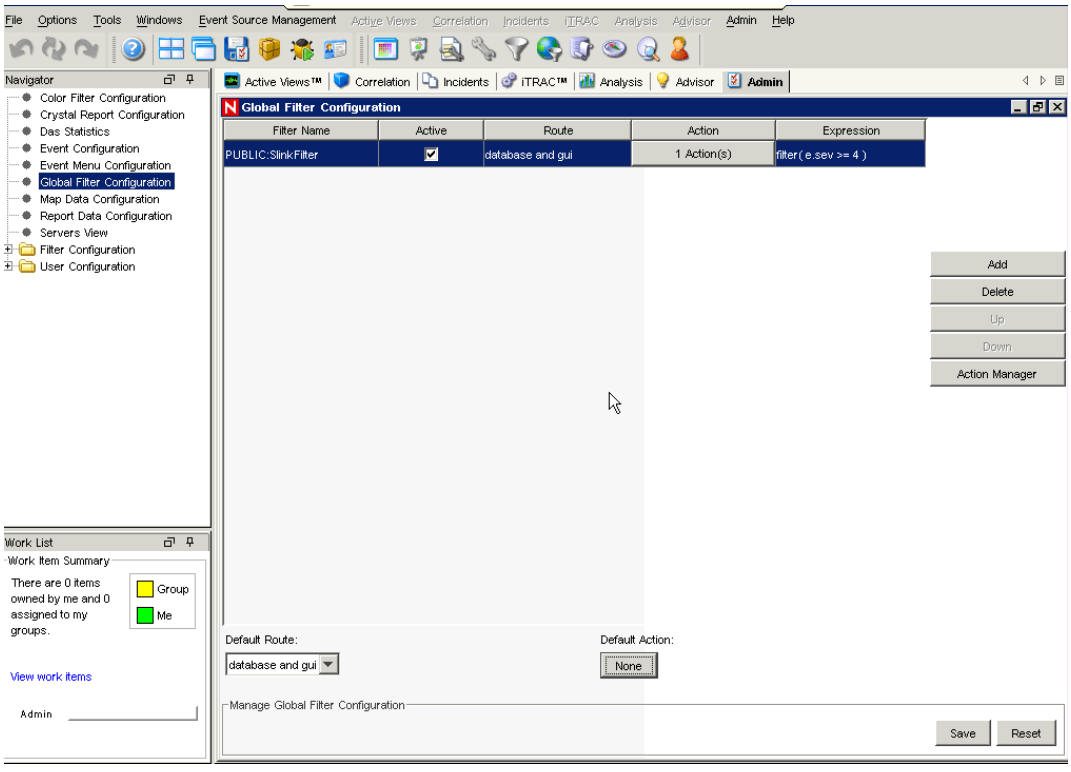
- "Sentinel 6.x and Sentinel Rapid Deployment" on page 46
- "Sentinel 7.0" on page 48

Sentinel 6.x and Sentinel Rapid Deployment

In the Global Filter Configuration window, you can add the Sentinel Link Action, then deploy the rule.

NOTE: This feature is supported only on Sentinel 6.1 SP1 Hotfix 2 or later, and Sentinel 6.1 Rapid Deployment 6.1 Hotfix 2 or later.

1. In the Sentinel Control Center, select the *Admin* Tab.
2. In the left navigation bar, select Global Filter Configuration.



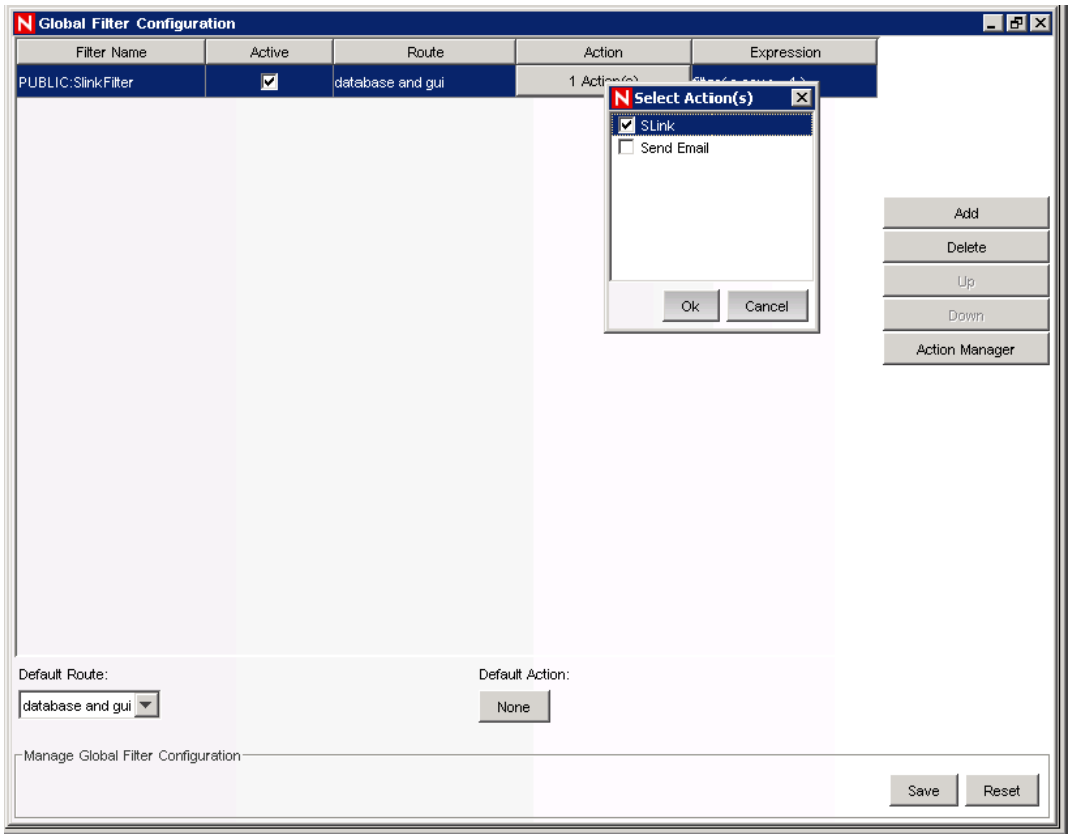
   The Global Filter Configuration window is displayed.
3. Click the *Add* button on the right-side of the window.
4. Click the button below the *Filter Name* field, then click the drop-down to set a filter.
5. Select the *Active* check box.

6 Select a Route from the drop-down:

Based on the selection, the events are either dropped or sent to the selected option.

- drop
- database only
- database and gui
- gui only

7 Click the button below the *Action* field.



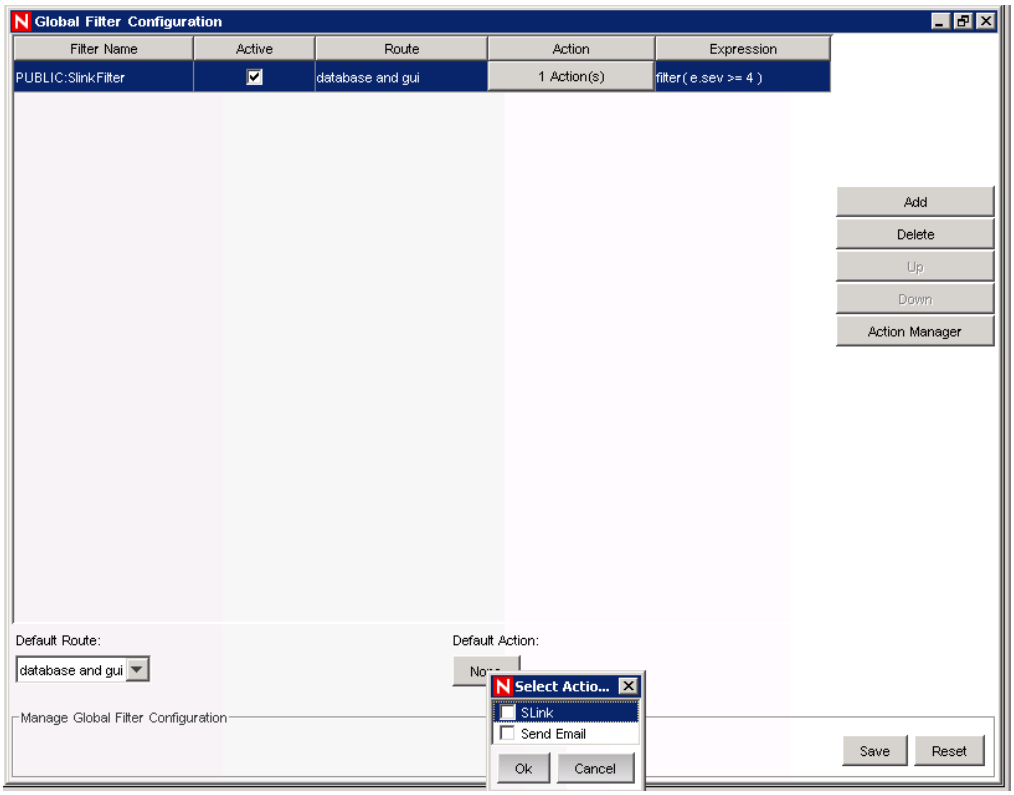
The Select Action window is displayed.

8 Select the Sentinel Link Action you have created, then click *OK*.

If you have not created one, click *Action Manager* button at the right-side of the window, then follow the instructions. For more information, see Section 3.1.1, “Configuring the Integrator Plug-In,” on page 31.

9 Alternatively, you can also add Sentinel Link Action as the default Action.

9a Click the button below the Default Action.



9b Select the Sentinel Link Action, then click *OK*.

10 Click *Save*.

Sentinel 7.0

You must configure and activate the rule to forward events to another Sentinel system.

Configuring the Rule to Forward Events to the Receiver

Sentinel is installed with a rule that forwards events to another Sentinel system.The rule is called *Forward Events to Another Sentinel System*. By default, the *Forward Events To Another Sentinel System* rule is configured to filter out internal system events and events with severity greater than three. This rule filters the following three types of system events:

- Audit (A)
- Performance (P)
- Internal (I)

You can also change the conditions of the rule to filter more events or remove conditions to filter fewer events.

Novell recommends that you configure the rule to forward only those events that you want to store on the Sentinel system for more in-depth reporting and analysis.

Activating the Rule to Forward Events to the Receiver

The *Forward Events To Another Sentinel System* rule is installed with Sentinel, but it is in the inactive (off) state. To forward the events to another Sentinel system, the rule must be activated.

1. Log in to the Sentinel Web UI as an administrator.
2. Click *Routing* in the toolbar.

   The Event Routing Rules screen is displayed.
3. Click *Edit* link next to the *Forward Events To Another Sentinel System* rule.
4. Select *Send Events via Sentinel Link* from the *Perform the following actions:* drop-down list.
5. Click *Save*.

   `Successfully saved rule` message is displayed.
6. Select the check box adjacent to the *Forward Events To Another Sentinel System* rule.

   If the rule is activated, a `Successfully activated the rule` message is displayed.

3.1.4 Manually Forwarding Events to the Receiver

You can forward events to the receiver by manually executing the Sentienl Link Action:

- Executing the Sentienl Link Action on an Incident.
- Executing the Sentienl Link Action on events in Active Views.
- Executing the Sentienl Link Action on events in Search results.

For more information, see the Sentinel product documentation:

- **Sentinel 6.x:** “Sentinel User Guide” (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/).
- **Sentinel 6.1 Rapid Deployment:** “Sentinel 6.1 Rapid Deployment User Guide” (http://www.novell.com/documentation/sentinel61rd/s61rd_user/?page=/documentation/sentinel61rd/s61rd_user/data/bookinfo.html).
- **Sentinel 7.0:** “Sentinel 7.0 User Guide” (http://www.novell.com/documentation/sentinel70/s70_user/index.html?page=/documentation/sentinel70/s70_user/data/bookinfo.html).

3.2 Configuring Sentinel Log Manager as a Sender

In Sentinel Log Manager, the plug-ins and the event forwarding rule by default are installed. You only need to configure the system for Sentinel link and activate the rule for sending the event data.

Follow the instructions below to configure a Sentinel Log Manager for sending the event data:

- Section 3.2.1, “Configuring the Sentinel Link Action,” on page 50
- Section 3.2.2, “Automatically Forwarding Events to the Receiver,” on page 54
- Section 3.2.3, “Manually Forwarding Events to the Receiver,” on page 55

3.2.1 Configuring the Sentinel Link Action

1. Log in to the Sentinel Log Manager Web interface as an administrator.
2. Click *rules* in the upper left corner of the page.

   The *Rules* tab is displayed on the right panel of the page.
3. For Sentinel Log Manager 1.0 Hotfix 3 or earlier, click the Configuration link on the right side of the screen. Scroll through the configuration settings to find the Sentinel Link settings.

   For Sentinel Log Manager 1.0 Hotfix 4 or later, select the *Actions* tab on the right side of the screen. Scroll through the list of Actions to find the *Sentinel Link* Action and click *Edit*.

   The Sentinel Link Action configuration page displays.

Sentinel Link

4 Specify the following Sentinel Link settings, then click *Save*.

Options	Description
Destination	Specify the IP address or hostname of the receiver, where a Sentinel Link Connector is configured.
Port	Specify the port number for the receiver. The default port is 1290. Click *Test* to validate the hostname or IP address and port number.
Encrypted (HTTPS) or Non Encrypted (HTTP)	Specify either of the following: ◆ **Non Encrypted (HTTP):** Provides unsecured connections. ◆ **Encrypted (HTTPS):** Provides secured connections between the Sentinel Link Connector and the Integrator. If you select the encrypted (HTTPS) option, you are allowed to optionally specify a server validation mode and a client key pair. You need to import the client key pair into the Integrator only if the server operates in a mode where it restricts the Integrators it communicates with. The server does this when a client certificate is imported into its trust store. If you import a client key pair into the Integrator, it is assumed that you intend to import the corresponding certificate, which contains the public key, from the client key pair to the trust store of the server. **NOTE:** If the receiver operates in a less restrictive *Open* mode, where it does not validate the sender certificates, it is not necessary to import a key pair into the receiver system. The receiver ignores even if you import one.
Server validation mode	Specify either of the following: ◆ **None - no server certificate required:** Select this option if you do not want to use any server certificate. ◆ **Strict - server certificate required:** Select this option to import a server certificate. The *Import* and *Details* buttons are displayed. If you click *Import*; a dialog box is opened with the following fields: ◆ **Certificate file:** Click *Browse* to add the server certificate file. ◆ **File password:** Specify the password for the certificate file. Click *Import* to import the server certificate. Click *Cancel* to close the Import dialog box.

Options	Description
Client key pair	Select either of the following: ◆ **None - server does not require client certificate:** The receiver system does not validate the sender certificates. Select this option if the server does not require the client key pair. ◆ **Custom - server validates (strict) client certificate:** The receiver system validates the sender certificates. Selecting this option allows you to import a client key pair. The *Import* and *Details* buttons are displayed. Click *Import* to open a dialog box with the following fields: ◆ **Keypair file:** Click *Browse* to import the client keypair file. ◆ **File password:** Specify the password for the client key pair file. Click *Import* to import the client key pair. Click *Cancel* to close the Import dialog box.
Maximum Event Queue Size (MB)	Specify the maximum event queue size value in megabytes. The value must be between 0 and 2147483647.
Maximum Data Rate (Kbps)	The following options are enabled only when you specify a value in the *Maximum Event Queue Size (MB)* field. The value must be between 0 and 2147483647. ◆ **Drop OLDEST event when queue is full:** Select this option to drop the oldest events in the event queue when the value specified in the *Maximum Event Queue Size (MB)* field exceeds the limit. ◆ **Drop NEWEST event when queue is full:** Select this option to drop the newest event when the value specified in the *Maximum Event Queue Size (MB)* field exceeds the limit.

Options	Description
Event Forwarding mode	Select one of the following options to specify the Event Forwarding Mode: ◆ **Forward Events Immediately:** Select this option to forward the events immediately to the receiver. ◆ **Scheduled Event Forwarding:** Select this option to schedule event forwarding. You can specify *Time Of Day* and *Duration* (in minutes) for each day of the week. The valid format for *Time Of Day* is hh:[mm] [am|pm]. The duration must be between 1 and 1440 minutes. If you do not specify time or duration for any of the days in the week, the schedule is considered to be 24 hours a day, seven days a week. It is equivalent to the *Forward Events Immediately* option. ◆ **Queue Events Only (do not forward):** Select this option to stop forwarding events to the receiver system. However, the integrator stores events it receives in its queue unless the queue has a size limit and has reached its capacity. This mode is useful if the receiver is down for maintenance or any network problems persist in communicating with the receiver system that might not be fixed immediately. In such situations, rather than continually trying to forward events, you can select this option to temporarily stop forwarding messages. After the problems are resolved, you can re-enable event forwarding by selecting the *Forward Events Immediately* or *Scheduled Events Forwarding* options.

3.2.2 Automatically Forwarding Events to the Receiver

Configuring the Rule to Forward Events to the Receiver

The Sentinel Log Manager is installed with a rule that forwards events to another sentinel system.The rule is called Forward Events to Another Sentinel System. By default, the Forward Events To Another Sentinel System rule is configured to filter out internal system events and events with severity greater than three. This rule filters the following three types of system events:

- Audit (A)
- Performance (P)
- Internal (I)

You can also change the conditions of the rule to filter more events or remove conditions to filter fewer events.

Novell recommends that you configure the rule to forward only those events that you want to store on the Sentinel system for more in-depth reporting and analysis.

Activating the Rule to Forward Events to the Receiver

The Forward Events To Another Sentinel System rule is installed with Log Manager, but it is in the inactive (off) state. To forward the events to another Sentinel system, the rule must be activated.

1. Log in to the Log Manager Web interface as an administrator.
2. Click *rules* in the upper left corner of the page.
3. The *Rules* tab displays on the right panel of the page.

   The Forward Events To Another Sentinel System rule displays under the *Rules* tab.
4. To activate the Forward Events To Another Sentinel System rule, click the check box next to the rule.

   If the rule is activated, a `Successfully activated the rule` message is displayed.

3.2.3 Manually Forwarding Events to the Receiver

You can forward events to the receiver by manually executing the Sentienl Link Action on events in Search results.

For more information see the "Sentinel Log Manager Administration Guide" (http://www.novell.com/documentation/novelllogmanager12/log_manager_admin/?page=/documentation/novelllogmanager12/log_manager_admin/data/).

Verifying a Sentinel Link

4

In this example, a Sentinel Rapid Deployment machine is used as the sender and a Novell Sentinel Log Manager machine is used as the receiver.

1. Configure a Sentinel Rapid Deployment machine for sending events.

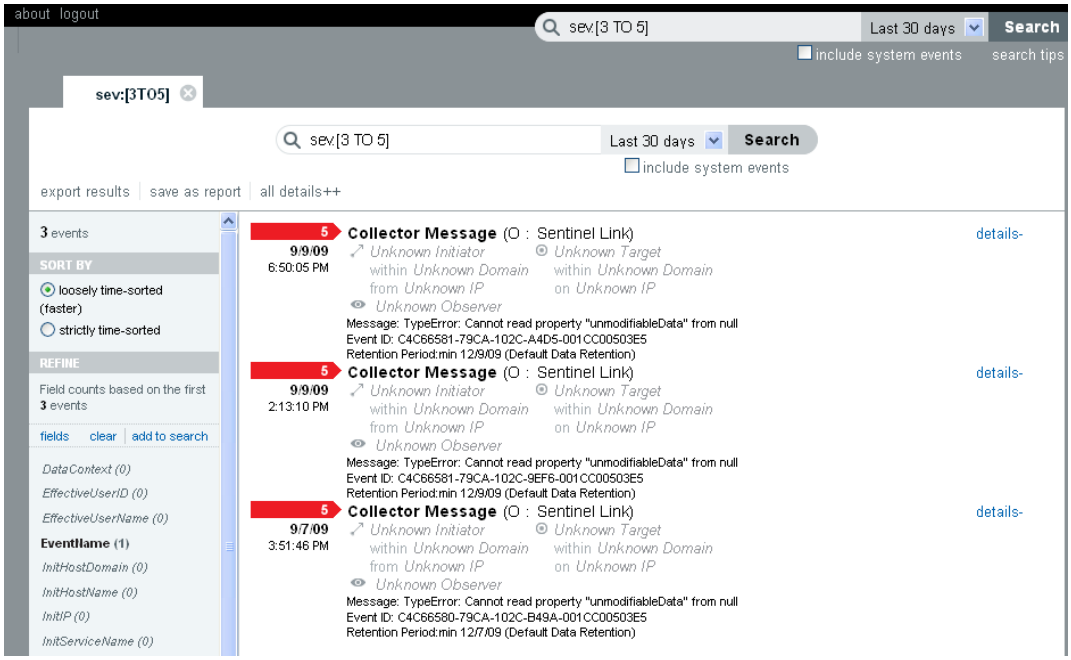
   For detailed instructions, see Section 3.1, “Configuring Sentinel or Sentinel Rapid Deployment System as a Sender,” on page 31.

2. Configure a Novell Log Manager machine for receiving the events.

   For detailed instructions, see Chapter 2, “Configuring Sentinel Systems for Receiving Events,” on page 11.

3. On the sender machine, generate an event with severity greater than 3, such as a failed login.

4. To view that event, go to the Novell Log Manager Web interface, then search for events with sev:[3 TO 5].



Known Issues

A

Refer to the known issues section of the respective documents of Sentinel Link Collector, Connector, Integrator, and Action.

Revision History

B

B.1 Rev: 2011.1r1

The updates include bug fixes to Sentinel Link Collector, Connector, Integrator, and Action. Refer to the revision history of the respective documents for specific bug fixes.

B.2 Rev: 6.1r5

Sentinel Link now supports IBM JRE 1.6 or later.

B.3 Rev: 6.1r4

Sentinel Link is now supported on Sentinel Log Manager 1.1.

In Sentinel Link Integrator, a new Alert Settings window is added that allows you to configure the conditions for the Integrator to generate alerts (internal events), while configuring the Sentinel Link Integrator. For more information about setting Alerts, refer to the *Sentinel Link Integrator* document.

Table B-1 *Bugs Fixed*

Bug Number	Resolution
596479	The `.JSON` file is now created with the correct name when the Sentinel Link Collector runs in the debug execution mode.
582547	In Sentinel Link Collector, the `DeviceEventTimeString` field is now set to the correct value.
536119	In Sentinel Link Collector, the values of the incoming event fields are now preserved by the Collector except for RV 21 - RV 25, which are overwritten to track the ESM nodes that parsed the event.
529913	The Sentinel Link Connector now does not allow you to run two Sentinel Link Event Source servers on the same port, and displays an error message indicating that ‘Port is already in use’.
531859 and 535964	Log message errors are fixed.
541101, 536115, and 541272	A number of event message handling errors are fixed.

Bug Number	Resolution
539925	Sentinel Link Integrator is now supported on Sentinel 6.1.1.2 and later.
603050	In Sentinel Link Integrator, the logging level of some chatty messages is now changed from `INFO` to `FINE` so that they do not show up in the log unless specifically requested.

B.4 Rev: 6.1r3

Table B-2 *Bugs Fixed*

Bug Number	Resolution
561424	Issue: The Sentinel Link showed the `PermGen Space OutofMemory` error when run on the Sentinel RD Hotfix 2 platform. However, sending of events continued without any problem. Fixed: The incorrect occurrence of PermGen memory exception is resolved in the Sentinel RD SP1 platform.

B.5 Rev: 6.1r2

Table B-3 *Bugs Fixed*

Bug Number	Description
558091	Issue: DeviceEventTime is not displayed same as the DeviceEventTime that is displayed on running the original Collector on Sentinel. For example, on running the original collector on Sentinel, for a particular log line, device event time is displayed as 2/22/03 1:23:08 p.m. but when the same event is forwarded from Sentinel Log manager to Sentinel Link Collector has the device event time as 2/22/03 11:53:08 p.m. Fixed: Now the same DeviceEventTime is getting displayed when event is forwarded from one sentinel system to another sentinel system(s).
548654	Issue: The `Plugin.pdf` file is not available with the Sentinel Link Action 6.1r1. Fixed: The `Plugin.pdf` file is now packaged with Sentinel Link Action 6.1r2.
540856	Issue: Sentinel Link count log messages are very chatty as the logging level for the log message was set to `INFO`, which is the default logging level. Fixed: Now the logging level for the Sentinel Link count log message is set to `FINE`, so that messages will be logged when the user sets the logging level to `FINE`.

B.6 Rev: 6.1r1

New Sentinel Link OverviewGuide.