January 2022

Absolute SIEM Connector Install Guide

IMPORTANT The Classic SIEM Connector is no longer available for download, but it is still supported. If the Connector is already installed and configured, it will continue to send alert events to your SIEM solution. To configure a new SIEM integration, install the Absolute 7 SIEM Connector. For more information, see SIEM Integration in the Help.

This guide provides information about integrating Absolute with a Security Information and Event Management (SIEM) solution. The purpose of this integration is to send alert events from Absolute to a SIEM solution, such as RSA® Security Analytics, HP ArcSight, or Splunk®. The alert events are transmitted using the syslog protocol.

If you are using a SIEM application and you want the ability to view and analyze Absolute alert events in your SIEM application, along with events from other sources, follow the steps presented in this guide.

This guide includes information about the following topics and tasks:

NOTE This guide describes how to install and manage the Classic version of the Absolute SIEM Connector. If you are currently using the Absolute 7 SIEM Connector to send events to your SIEM application, you do not need to disable that Connector to use the Classic SIEM Connector. The events sent by the Absolute 7 version are different from the events sent by the Classic version, so the two versions can run in parallel. For information about the Absolute 7 SIEM Connector, see *SIEM Integration* in the Help.

Overview

Security information and event management (SIEM) solutions collect logged events from multiple software programs and store them in a central repository for consolidated reporting and analysis. Organizations can then monitor security events across their system for incident response, forensics, and regulatory compliance.

Absolute's SIEM integration enables alert events logged in Absolute to be sent to your SIEM application. The alert events are sent in messages that use the syslog protocol, which allows event data from different types of systems to be transmitted in a standardized format to a central repository.

This section includes the following topics:

Role of the Absolute SIEM Connector

Absolute's SIEM integration is created by installing the Absolute SIEM Connector on a computer within your network. The SIEM Connector configures a Windows service that sends SOAP requests to the Absolute Gateway Server to retrieve alert event data from the Absolute database. The alert events are then transmitted in syslog messages to your SIEM's Syslog server to allow SIEM users to view, analyze, and report on these events, along with other events within your system.

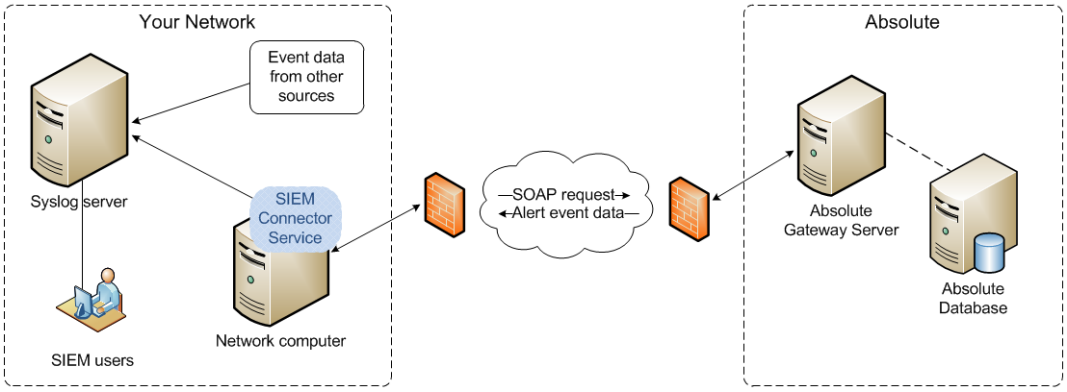

Figure 1: *Network configuration of standard SIEM integration with Absolute SIEM Connector*

After you install the Absolute SIEM Connector, it retrieves all Absolute alert events logged within the past 24 hours and sends them to the Syslog server. Going forward, the SIEM Connector retrieves new alert events at the interval set in SIEM Connector configurations. You can set the interval to any value between two minutes and 24 hours; the default value is 60 minutes.

NOTE To view alert event data that was triggered *prior* to the installation of the SIEM Connector, log in to the Absolute console and on the navigation bar click **Policies** > **Rules**. At the bottom of the page, click **Go to the Classic Alerts Page** link. On the Classic Alerts page, click **Alert Events**.

Alert event data retrieved

The Absolute SIEM Connector retrieves the following alert event data from Absolute:

- Information about the device that triggered the alert event, including:
  - **Identifier**: unique electronic serial number (ESN) assigned to the agent installed on the device
  - **Device Name**: name assigned to the device
  - **Serial Number**: serial number of the device
- **Alert Name**: name assigned to the alert
- **Event Date/Time**: date and time (UTC) when the alert event was triggered

NOTE When Absolute is integrated with RSA Security Analytics, HP ArcSight, or Splunk, additional alert event data is retrieved and the SIEM integration is enhanced. For more information, see Enhanced SIEM integrations.

System requirements

The Absolute SIEM Connector can be installed on a computer running any of the following operating systems:

- Windows Server®:
  - Windows Server 2019
  - Windows Server 2016
  - Windows Server 2012
  - Windows Server 2008 R2
- Windows (64- or 32-bit):
  - Windows 10
  - Windows 8 or 8.1
  - Windows 7

NOTE .NET Framework 4.0 or higher is also required.

Prerequisites

The following prerequisites need to be met before you install the Absolute SIEM Connector:

- One or more alerts are activated in Absolute. For more information about activating predefined alerts and creating custom alerts, see "Alerts" in the *Absolute User Guide*.
- The Syslog server and the computer on which you intend to install the SIEM Connector reside within the same network.
- An Internet connection is available.

Installing the Absolute SIEM Connector

NOTE This section only applies if you downloaded the SIEM Connector before the release of Absolute 7.19 in February 2022. The SIEM Connector is no longer available for download from the Absolute console.

The SIEM Connector is a Windows service that transmits Alert events from Absolute to your SIEM application using syslog messages.

Installation of the SIEM Connector consists of the following tasks, which are described in this section:

- Pre-installation steps
- Installing the Absolute SIEM Connector
- Verifying installation of the Absolute SIEM Connector

IMPORTANT If Single Sign-On is enabled for your Absolute account, contact Absolute Technical Support before proceeding with the tasks described in this guide. Technical Support will assist you with the installation of the SIEM Connector.

Pre-installation steps

Before you install the SIEM Connector, it is best practice to create a Absolute user to be used exclusively for the SIEM integration. You will enter the credentials for this user when you install the SIEM Connector.

1. Create a generic email address in your corporate email system. For example, create `SIEM_Admin@<domain>` where `<domain>` is your corporate domain.

   NOTE You may want to consider adding an email alias to the generic email address to ensure that any system notifications are sent to the IT administrator who is administering your SIEM application.

2. Log in to the Absolute console as a System Administrator.
3. On the quick access toolbar, click ⊕ > **Users**.
4. Create a user using the generic email address you created in step 1. Assign the System Administrator role to the user.

   NOTE If desired, you can downgrade this user to the Administrator, Power User, or Guest User role after you complete step 6.

5. Click **Invite User** to send an email to the generic email address you entered in step 1.
6. Follow the instructions in the email to create a password.

Installing the Absolute SIEM Connector

The installation package includes a setup wizard to help you install and configure the SIEM Connector service.

➔ **To install the SIEM Connector:**

1. Navigate to the location where you downloaded the `Absolute SIEM Connector <version>.msi` file from the Absolute console and double-click the file.
2. On the Welcome page of the Absolute SIEM Connector Setup Wizard click **Next**.
3. Review and accept the terms and conditions of the End-User Service Agreement and click **Next**.
4. On the Destination Folder page do one of the following:
   - To install to the default folder shown in the field, click **Next**.
   - To install to a different folder:
     a. Click **Change**.
     b. Navigate to the applicable folder on your local drive, select it, and click **OK**.
     c. On the Destination Folder page click **Next**.
5. On the configuration page:
   a. Enter the **Username** and **Password** of the Absolute user you created for the SIEM integration.
   b. In the **Update Interval** field, enter how frequently you want the SIEM Connector service to check for new alert events in Absolute. You can set the interval to any value between two minutes and

1440 minutes (one day). The default interval is 60 minutes.

c. Click **Next**. The system verifies that the Username and Password you entered are valid.

6. On the Syslog server configuration page:
   a. Enter the **Hostname** of the Syslog server.
   b. Enter the **Port** number for syslog messages.
   c. Select the **TCP** or **UDP** protocol.
   d. Click the **Target SIEM platform** field and from the list select the SIEM application that you want to integrate with:
      - **RSA Security Analytics**
      - **HP ArcSight**
      - **Splunk**
      - **Other (supports standard syslog format)**

      NOTE If you select this option and your target SIEM application supports Common Event Format (CEF), alert event data may not be presented as expected in your SIEM application.

      NOTE For more information about integrating with RSA Security Analytics, HP ArcSight, or Splunk, see Enhanced SIEM integrations.

   e. Click **Next**.
7. On the Ready to install Absolute SIEM Connector page click **Install** and wait for the installation to finish.
8. On the Completed the Absolute SIEM Connector Setup Wizard page click **Finish**. The SIEM Connector is installed.

Verifying installation of the Absolute SIEM Connector

After you install the SIEM Connector you may want to check that its Windows service is running.

➔ **To verify that the SIEM Connector service is running:**

1. Right-click the task bar and click **Start Task Manager**.
2. In Windows Task Manager click the **Services** tab.
3. Click the **Services** button.
4. On the Services dialog, verify that **Absolute SIEM Connector Service** is **Started**.
5. Close the Services dialog and the Windows Task Manager dialog.

Managing the Absolute SIEM Connector

This section includes the following topics:

- Changing Absolute SIEM Connector settings
- Viewing the Windows event log for the Absolute SIEM Connector

- Uninstalling the Absolute SIEM Connector

Changing Absolute SIEM Connector settings

From time to time you may need to update the Absolute console or Syslog server configurations for the SIEM Connector. For example, if you may want to change the frequency at which the Windows service checks for new alert events in Absolute.

➔ To change the settings for the SIEM Connector:

1. Open Programs and Features. For example, on a Windows 10 operating system:
   a. Click **Start** and type `Control Panel` in the **Search** field.
   b. Click **Control Panel**.
   c. Click **Programs** > **Programs and Features**.
2. Select **Absolute SIEM Connector** and click **Change**.
3. On the Absolute SIEM Connector Setup Wizard Welcome page click **Next**.
4. On the Change, repair or remove installation page click **Change**.
5. On the configuration page:
   a. Update the **Username** and **Password** of the Absolute SIEM user, if required.
   b. In the **Update Interval** field, enter how frequently you want the SIEM Connector service to check Absolute for new alert events. You can set the interval to any value between two minutes and 1440 minutes (one day). The default interval is 60 minutes.
   c. Click **Next**.
6. On the Syslog server configuration page:
   a. Update the **Hostname** of the Syslog server, if required.
   b. Update the **Port** number for syslog messages.
   c. Select the **TCP** or **UDP** protocol.
   d. Click the **Target SIEM platform** field and select an option from the list.
   e. Click **Next**.
7. On the Ready to change Absolute SIEM Connector page, click **Change**.
8. On the Completed the Absolute SIEM Connector Setup Wizard page click **Finish**. The SIEM Connector settings are updated.

Viewing the Windows event log for the Absolute SIEM Connector

You can monitor the SIEM Connector and troubleshoot issues by viewing the event log in the Windows Event Viewer.

➔ **To view the Windows event log:**

1. Open the Windows Event Viewer. For example, on a Windows 10 operating system:
   a. Click the **Start** icon and type `Event Viewer` in the **Search** field.
   b. Click **Event Viewer**.

   Alternatively, open a Command Prompt windows and type `eventvwr`.
2. In Event Viewer, click **Windows Logs** > **Application**.
3. From the list of logged events, review the events for the SIEM Connector.

   For more information about viewing event logs and troubleshooting issues, see the Microsoft Management Console Help.

Uninstalling the Absolute SIEM Connector

➔ **To uninstall the SIEM Connector:**

1. Open Programs and Features. For example, on a Windows 10 operating system:
   a. Click **Start** and type `Control Panel` in the **Search** field.
   b. Click **Control Panel**.
   c. Click **Programs** > **Programs and Features**.
2. Select **Absolute SIEM Connector** and click **Uninstall**.
3. Follow the on-screen instructions to uninstall the SIEM Connector.

   The SIEM Connector is uninstalled.

Enhanced SIEM integrations

This section contains additional information about integrating Absolute with specific SIEM applications.

This section includes the following topics:

Integrating with RSA Security Analytics

If you are using RSA® Security Analytics, Absolute's SIEM integration is enhanced. In addition to the alert event data listed in Alert event data retrieved, the SIEM Connector also retrieves the following information about each alert:

- **Alert ID**: unique identifier assigned to the alert in Absolute
- **Condition**: alert condition that triggered the alert in Absolute

The alert event data sent to RSA Security Analytics maps to the following RSA meta keys:

RSA meta key	Absolute field name or "value"
device.type	"absolutesiemconnectorpe"
device class	"Analysis"
event.source	Identifier
serial.number	Serial Number
subject	Alert Name
event.time.str	Event Date/Time
operation.id	Alert ID
event.desc	Condition
event.computer	Device Name
email	User Email Address

Integrating with HP ArcSight

If you are using HP ArcSight, Absolute's SIEM integration is enhanced. In addition to the alert event data listed in Alert event data retrieved, the SIEM Connector also retrieves the following information about each alert:

- **Alert ID**: unique identifier assigned to the alert in Absolute
- **Condition**: alert condition that triggered the alert in Absolute

All syslog messages sent to ArcSight support Common Event Format (CEF), which enables the alert event data to map directly to the following fields in ArcSight:

ArcSight field name	Absolute field name or "value"
Device External Id	Serial Number
Device Host Name	Device Name
Device Vendor	"Absolute"
Device Product	"AbsoluteSiemConnector"
Device Version	The version number of the SIEM Connector, for example "1.4"
Name	Alert Name
Destination User ID	Email
Device Custom String 1 Label	"ESN"
Device Custom String 1	Identifier
Device Receipt Time	Event Date/Time
Device Custom Number 1 Label	"Alert ID"
Device Custom Number 1	Alert ID
Message	Condition
Source User Name	Email

Device, device action, and application-related events

ArcSight field name	Absolute field name or "value"
Device External Id	Serial Number
Device Host Name	Device Name
Device Custom String 1 Label	"ESN"
Device Custom String 1	Identifier
Device Receipt Time	Event Date/Time
act/Name	Event Name
Message	Event Details
Source User Name	Email

Authentication events

ArcSight field name	Absolute Event History field name or "value"
Source User Name	Email
Name	Event
Message	Event Details

ArcSight field name	Absolute Event History field name or "value"
End Time	Date
Destination Service Name	destination (for example, "Absolute IdP")
Source Service Name	Source

Integrating with Splunk

If you are using any of the following versions of Splunk, Absolute's SIEM integration is enhanced:

- Splunk Enterprise
- Splunk Cloud
- Splunk Light

In addition to the alert event data listed in Alert event data retrieved, the SIEM Connector also retrieves the following information about each alert:

- **Alert ID**: unique identifier assigned to the alert in Absolute
- **Condition**: alert condition that triggered the alert in Absolute

All syslog messages sent to Splunk support Common Event Format (CEF), which enables the alert event data to map directly to the following Report fields in Splunk:

Splunk field name	Absolute field name
DDS_AlertCondition	Condition
DDS_AlertID	Alert ID
DDS_AlertName	Alert Name
DDS_AlertTime	Event Date/Time
DDS_ComputerName	Device Name
DDS_Identifier	Identifier
DDS_SerialNumber	Serial Number

This section includes the following topics:

Integration requirements

To successfully integrate the SIEM Connector with Splunk, ensure that the following requirements are met, as they pertain to the version of Splunk you are using:

- For Splunk Cloud and Splunk Light Cloud Service:
  - You have the appropriate user permissions to manage your Splunk Cloud instance
  - The Splunk Universal Forwarder is downloaded, installed, and deployed on a network computer

- The Universal Forwarder is configured to listen on the applicable TCP or UDP port for incoming syslog messages
- The SIEM Connector is installed on a network computer.

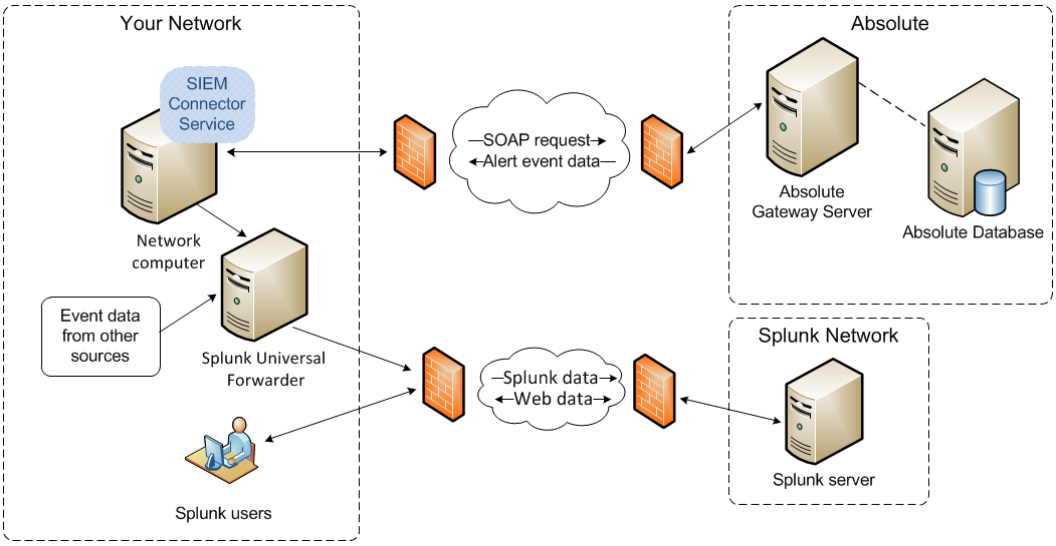

Figure 2: *Network configuration for Splunk Cloud or Splunk Light Cloud Service*

For more information about working with the Splunk Universal Forwarder and about using Splunk Cloud or Splunk Light Cloud Service, refer to Splunk documentation.

- For Splunk Enterprise or Splunk Light Software (with a Splunk Universal Forwarder):
  - You have the appropriate user permissions to manage Splunk Enterprise
  - The Splunk Universal Forwarder is downloaded, installed, and deployed on a network computer
  - The Universal Forwarder is configured to listen on the applicable TCP or UDP port for incoming syslog messages
  - The SIEM Connector is installed on a network computer.

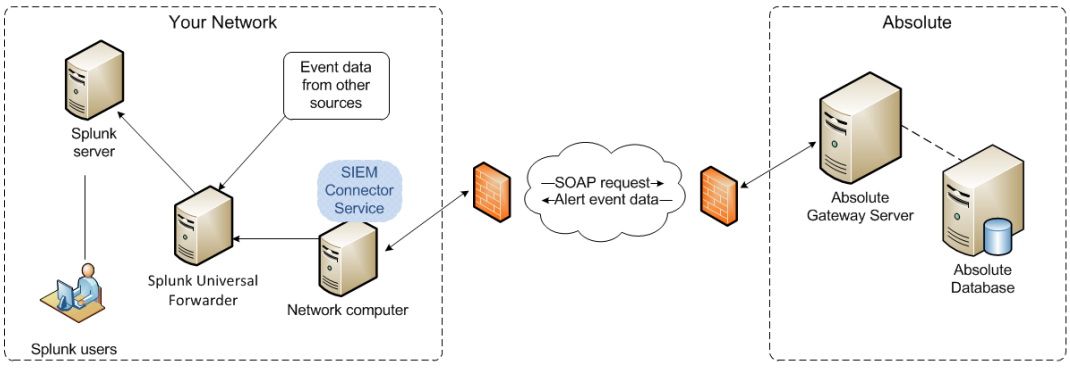

Figure 3: *Network configuration for Splunk Enterprise or Splunk Light Software (Universal Forwarder)*

For more information about working with the Splunk Universal Forwarder and about using Splunk Enterprise or Splunk Light Software, refer to Splunk documentation.

- For Splunk Enterprise or Splunk Light Software (without a Splunk Universal Forwarder):
  - You have the appropriate user permissions to manage Splunk Enterprise
  - A new TCP or UDP Data Input has been added to Splunk Enterprise
  - The new TCP or UDP Data Input is configured to listen on the appropriate port for incoming syslog messages
  - The SIEM Connector is installed on a network computer.

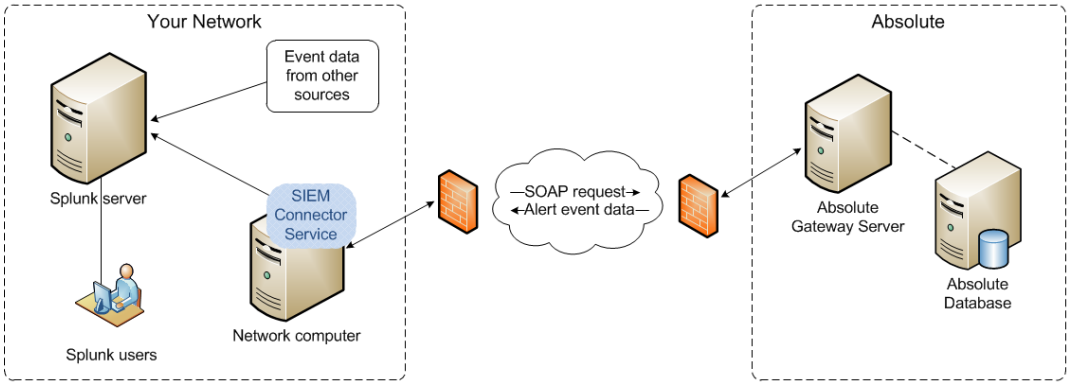

Figure 4: *Network configuration for Splunk Enterprise or Splunk Light Software (no Universal Forwarder)*

For more information about installing Splunk Enterprise or Splunk Light Software and configuring Data Inputs, refer to Splunk documentation.

Absolute DDS App for Splunk

If you are using *Splunk Cloud* or *Splunk Enterprise*, your Splunk integration with Absolute can be further enhanced by installing the Absolute Data & Device Security (DDS) App for Splunk. This app lets you view the alert events logged in Absolute in a format that enhances readability and analysis. After Splunk indexes the alert events, you can work with the event data using the Absolute DDS Alerts report or any of the four predefined Splunk dashboards included with the app.

You can also access Absolute Device Freeze directly from Splunk to freeze devices that you determine are at-risk, based on a triggered alert.

NOTE The Absolute Data & Device Security (DDS) App for Splunk is not available in Splunk Light.

This section includes the following topics:

- Installing the Absolute DDS App for Splunk
- Viewing alert events in the Absolute DDS Alerts report
- Viewing alert events using the Absolute DDS dashboards
- Freezing at-risk devices from Splunk

Installing the Absolute DDS App for Splunk

After you've installed the SIEM Connector on a network computer, log in to Splunk and add the Absolute DDS App for Splunk to your Splunk account.

➔ **To install the Absolute DDS App for Splunk:**

1. From the home page in Splunk Cloud or Splunk Enterprise, click the  icon next to **Apps** in the left navigation bar. The Apps page opens.
2. Click **Browse more apps**. The Browse More Apps page opens.
3. In the search field on the left navigation bar, type **Absolute** and press `Enter`.

   NOTE If you are working in Splunk Enterprise and can't find the Absolute DDS app for Splunk in Browse More Apps, you may need to follow an alternate workflow to download the app. For details, refer to Splunk Enterprise documentation.
4. In the app description for the Absolute Data & Device Security (DDS) App for Splunk, click **Install**.
5. In the Login dialog, do the following:
   a. Type your Splunk **Username** and **Password**.
   b. Select the check box to acknowledge the license terms and conditions and then click **Login and Install**.
6. In the Complete dialog click **Done**.

Viewing alert events in the Absolute DDS Alerts report

➔ **To view alert events in the Absolute DDS Alerts report:**

1. From the home page in Splunk Cloud or Splunk Enterprise, click **Absolute Data & Device Security (DDS) App for Splunk** in the left navigation bar.
2. On the toolbar click **Reports**.
3. On the Reports page click **Absolute DDS Alerts** to open the default report included in the Absolute DDS App for Splunk.
4. Review the list of alert events. To view details about an event, in the event's **i** column, click the **>** icon to expand the section.
5. By default, the alert event data shown in the report includes all events triggered since the SIEM Connector was installed. To show events during a specific time period, click **All time** and select an option from the time range picker.

NOTE For more information about viewing events in Splunk reports, refer to Splunk documentation.

Viewing alert events using the dashboards

➔ **To view alert events in the predefined dashboards:**

1. From the home page in Splunk Cloud or Splunk Enterprise, click **Absolute Data & Device Security (DDS) App for Splunk** in the left navigation bar.
2. On the toolbar, click **Dashboards**.
3. On the Dashboards page, click the link for one of the following predefined dashboards included with the Absolute DDS App for Splunk:

Dashboard	Details
Alert Events by Alert Name	Shows all triggered Absolute alert events for all devices. Click a device's Identifier to view all triggered alert events for a particular device. The events are grouped into columns by Alert Name. Click the linked numeral in a column to view the details about each triggered event for the associated alert.
Alert Events by Alert Name (pie chart)	Shows a pie chart of all Absolute alert events triggered for all devices. The events are grouped into pie slices by Alert Name. ➔ **To view alert event data:** a. Hover over a slice to view the following details: • Alert Name • Number of triggered events • Number of triggered events as a percentage of total triggered events b. Click a slice to view the details about each triggered event for the associated alert.
Alert Events by Condition Name	Shows all triggered Absolute alert events for each device. Click a device's Identifier to view all triggered alert events for a particular device. The events are grouped into columns by the Condition assigned to the alert. Click the linked numeral in a column to view the details about each triggered event for the associated Condition.
Alert Events by Condition Name (pie chart)	Shows a pie chart of all triggered Absolute alert events for all devices. The events are grouped into pie slices by Condition. ➔ **To view alert event data:** a. Hover over a slice to view the following details: • Condition Name • Number of triggered events • Number of triggered events as a percentage of total triggered events b. Click a slice to view the details about each triggered event for the associated Condition.

4. By default, the alert event data shown in the dashboards includes all events triggered since the SIEM Connector was installed. To show events during a specific time period, click **All time** and select an option from the time range picker.

NOTE For more information about viewing events using Splunk dashboards, refer to Splunk documentation.

Freezing at-risk devices from Splunk

After reviewing the triggered alert events, you may find that you want to freeze a device that may be at risk.

➔ **To freeze a device in Absolute from Splunk:**

1. From the home page in Splunk Cloud or Splunk Enterprise, click **Absolute Data & Device Security (DDS) App for Splunk** in the left navigation bar.

2. Do one of the following:
   - To freeze a device from the Absolute DDS Alerts report:
     a. On the toolbar click **Reports**.
     b. Click **Absolute DDS Alerts** to open the report.
   - To freeze a device from a dashboard:
     a. On the toolbar, click **Dashboards**.
     b. Click a link to open a dashboard.
     c. Depending on the dashboard you opened, click a device Identifier or a pie slice to view the triggered alert events.
3. In the **i** column for the device you want to freeze, click the **>** icon to expand the section.
4. Click **Event Actions** > **Request Device Freeze**.
5. On the Absolute Login page, enter your credentials to log in to the Absolute console. The Request Device Freeze page opens.

   NOTE You must log in as a Security Administrator or Security Power User to submit a Device Freeze request.
6. Enter the required information to submit a Device Freeze request. For more information, see *Freezing devices* in the Absolute Help.

Contacting Technical Support

If you have difficulty installing the Absolute SIEM Connector, contact Absolute Technical Support. We welcome your questions, comments, and feature requests. Visit us at www.absolute.com/en/support and follow the instructions on the page to contact technical support in your region.

Copyright Information