NetWitness® Platform XDR

Jamf Protect Event Source Log Configuration Guide

NETWITNESS

Platform XDR

Jamf Protect

Event Source Product Information:

Vendor: Jamf

Event Source: jamf protect

Versions: API v1.0

NetWitness Product Information:

Supported On: NetWitness Platform XDR 11.7 or later

> **Note:** Jamf Protect is supported from NetWitness Platform XDR 11.5 or later. However, NetWitness recommends you to update NetWitness Platform XDR to the latest version.

Event Source Log Parser: jamf

> **Note:** The jamf parser parses this event source as **device.type=jamf**.

Collection Method: Plugin Framework

Event Source Class.Subclass: Host.Cloud

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

November, 2022

Contents

Collecting Jamf Protect Events in NetWitness Platform XDR 5

Configure the Jamf Protect Event Source 6

Set Up the Jamf Protect Event Source in NetWitness Platform XDR 7

- Deploy the Jamf Protect Files from NetWitness Live 7
- Configure the Event Source 7

Jamf Protect Collection Configuration Parameters 10

- Advanced Parameters 11

Getting Help with NetWitness Platform XDR 13

- Self-Help Resources 13
- Contact NetWitness Support 13
- Feedback on Product Documentation 13

Collecting Jamf Protect Events in NetWitness Platform XDR

Apple builds one of the most secure out-of-the-box platforms in the information technology domain. Apple's macOS and iOS are best among the market competitors in the OS domain. Jamf Protect enhances Apple's built-in security features by increasing visibility, preventions, controls and remediation capabilities. For more information, see https://www.jamf.com/products/jamf-protect/.

In NetWitness Platform XDR, we collect logs with the help of Jamf Protect using either the Jamf Protect GraphQL API or the AWS S3 bucket storage facility. We collect events such as Jamf alerts, audit, computer lists, or telemetry. NetWitness helps you to do the security investigation by fine parsing these collected events.

The following sections describe the configuration of the Jamf Protect as an event source in Netwitness Platform XDR using the Jamf Protect GraphQL API.

- Configure the Jamf Protect Event Source
- Set Up the Jamf Protect Event Source in NetWitness Platform XDR
- Jamf Protect Collection Configuration Parameters.

Configure the Jamf Protect Event Source

The Jamf Protect plugin forwards all the events to both Jamf Protect GraphQL API and AWS S3 storage. The information in the following table helps you to select the NetWitness plugin collection method to collect particular event type. If you want to collect Jamf Protect events from AWS S3 bucket, follow the instructions provided in S3 Universal Connector Event Source Log Configuration Guide and skip using this document.

Jamf Protect Event Types	Jamf Protect GraphQL API	AWS S3 Bucket Forwarding
Alerts	Allowed	Allowed
Audit	Allowed	Not Allowed
Computer List	Allowed	Not Allowed
Telemetry	Not Allowed	Allowed

As of now, NetWitness supports only the above listed Jamf protect security events. If you want to collect any other Jamf protect event type, we request you to raise a customer ticket, see Getting Help with NetWitness Platform XDR. For more information on Jamf Protect events, see Jamf Protect API.

Perform the following tasks in your Jamf Protect account to receive events through the Jamf Protect GraphQL API:

1. Generate a client ID and password by creating a Jamf Protect API client in your Jamf Protect Account. For the information to create the Jamf Protect API client, see Creating an API Client in Jamf Protect.

   > **IMPORTANT:** You need client ID and password when you configure Jamf Protect event source plugin in NetWitness Platform XDR. Please keep them securely because the password is displayed only once when you create the API client.

2. Save your organization tenant value from the API client that you have created. When you click on the API client that you have created, the Token and API endpoints information is displayed. The API Endpoint URL should look like, ***https://<your organisation-tenant>.protect.jamfcloud.com/graphql***. Please get the organization tenant from API Endpoint URL as you need it when you configure the Jamf Protect plugin.

For more information on Jamf Graph QL Queries that we use to collect events from Jamf protect, see Queries and Mutations.

> **Note:** Please make sure that below URLs are allowed to open in your network firewalls/proxies as we use them for event collection.
> - https://<your-organization-tenant>.protect.jamfcloud.com/token
> - https://<your-organization-tenant>.protect.jamfcloud.com/graphql.

Set Up the Jamf Protect Event Source in NetWitness Platform XDR

In NetWitness Platform XDR, perform the following tasks:

i. Deploy the Jamf Protect Files from NetWitness Live

ii. Configure the Event Source

Deploy the Jamf Protect Files from NetWitness Live

Jamf Protect event source require resources available in NetWitness Live to collect logs. Jamf Protect uses the jamf json parser to parse the logs.

To deploy the Jamf Protect content from Live:

1. In the NetWitness Platform XDR menu, select **(Configure)** .
2. Browse Live for the **jamf** parser using RSA Log Device as the Resource Type.
   Select **jamf** parser from the list.
3. Click **Deploy** to deploy the jamf parser to the appropriate Log Decoders using the Deployment Wizard.
4. You should also deploy the Jamf Protect log collection package. Browse Live for Jamf Protect log collector content by typing

   jamf_protect in the search text box and click **Search**.
5. Select the item returned from the search and click **Deploy** to deploy to the appropriate Log Collectors.

   > **Note:** On a hybrid installation, you should deploy the package on both the Virtual Log Collector (VLC) and the Log Collector (LC). If you deploy the package on the LC, you should restart the log decoder and log collector services, otherwise logs will not be collected.
6. Restart the `nwlogcollector` service.

For more details, see the Add or Update Supported Event Source Log Parsers topic, or the *Live Resource Guide* on NetWitness Link.

Configure the Event Source

This section contains details on setting up the event source in NetWitness Platform XDR. In addition to the procedure, the Jamf Protect Collection Configuration Parameters are described.

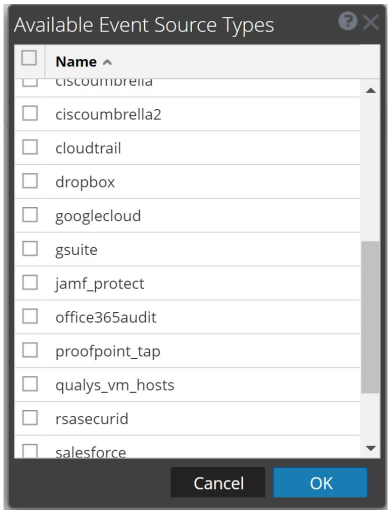
To configure the Jamf Protect Event Source:

1. In the NetWitness Platform XDR menu, select 🛠 (Admin) > **Services**.
2. In the **Services grid**, select a Log Collector service, and from the **Actions** menu, choose **View** > **Config**.
3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

   The **Event Categories** panel displays the File event sources that are configured, if any.

4. In the **Event Categories** panel toolbar, click +.

   The **Available Event Source Types** dialog is displayed.



Available Event Source Types

□ Name ^

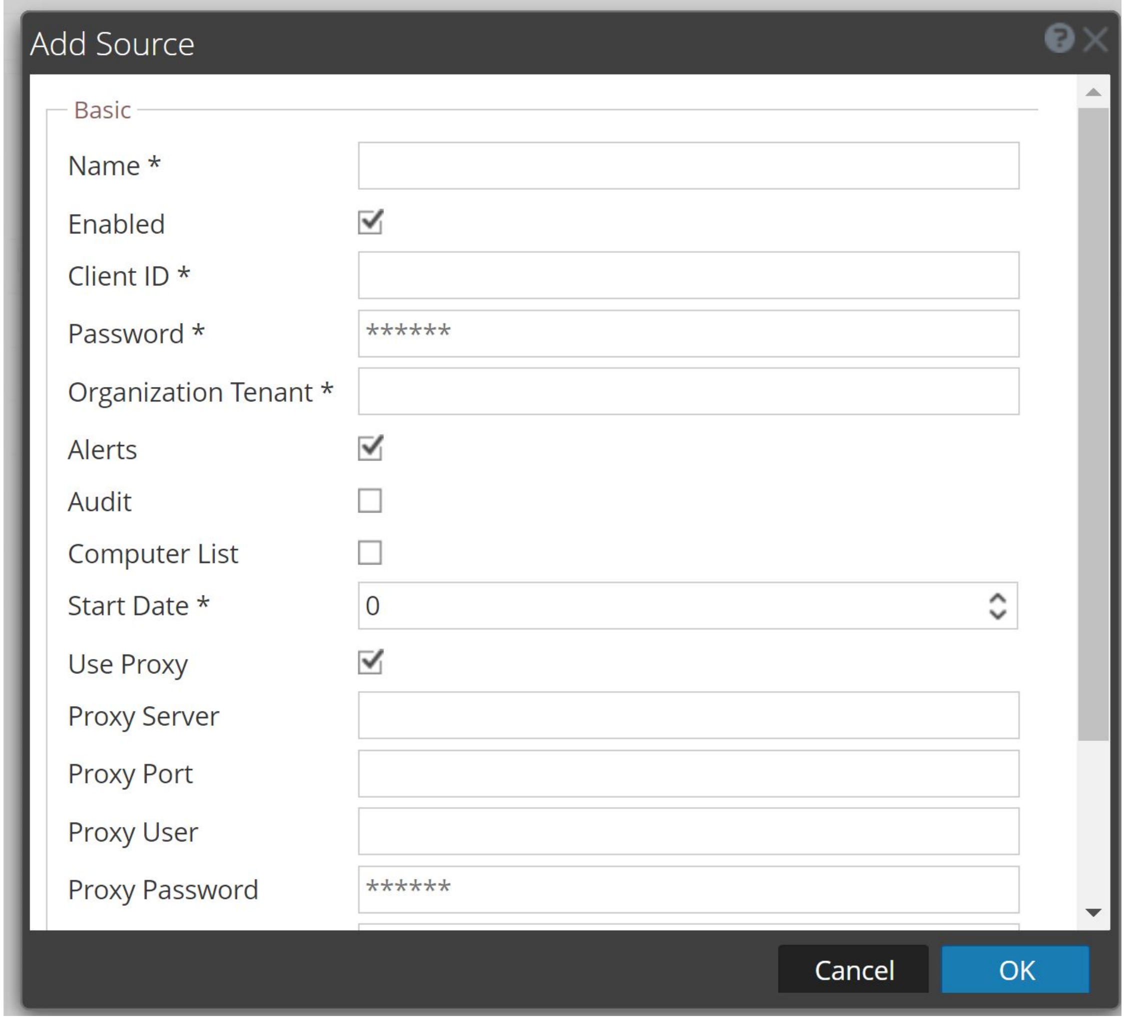
□ ciscoumbrella
□ ciscoumbrella2
□ cloudtrail
□ dropbox
□ googlecloud
□ gsuite
□ jamf_protect
□ office365audit
□ proofpoint_tap
□ qualys_vm_hosts
□ rsasecurid
□ salesforce

5. Select **jamf_protect** from the list, and click **OK**.

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

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

   The **Add Source** dialog is displayed.



Add Source

Basic

Name *	
Enabled	☑
Client ID *	
Password *	******
Organization Tenant *	
Alerts	☑
Audit	□
Computer List	□
Start Date *	0
Use Proxy	☑
Proxy Server	
Proxy Port	
Proxy User	
Proxy Password	******

7. Define parameter values, as described in Jamf Protect Collection Configuration Parameters.
8. Click **Test Connection**.

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

   > **Note:** The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and NetWitness Platform XDR displays an error message.

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

   The new event source is displayed in the Sources panel.

Jamf Protect Collection Configuration Parameters

The following table describes the configuration parameter for the Jamf Protect integration with NetWitness Platform XDR. Fields marked with an asterisk (*) are required.

> **Note:** When run from behind an SSL proxy, if certificate verification needs to be disabled, uncheck the **SSL Enable** checkbox in the **Advanced** section.

Name	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the box to enable the event source configuration to start collection. The box is selected by default.
Client ID *	The Client ID (or client key) is found in the Jamf Protect API client page. Please refer step 1 in Configure the Jamf Protect Event Source.
Password *	The password that is received after API Client creation. Please refer step 1 in Configure the Jamf Protect Event Source.
Organization Tenant *	Organization Tenant value. Please refer step 2 in Configure the Jamf Protect Event Source
Tick any one of the checkboxes to proceed with collection*	• Alerts: Select the checkbox if you want to collect Jamf protect alert events. • Audit: Select the checkbox if you want to collect Jamf protect audit events. • Computer List: Select the checkbox if you want to collect Jamf protect computer list events.
Start Date *	Choose the date from which to start collecting. This parameter defaults to the current date, i.e, 0 and logs will be collected from last 60 mins. The Maximum value is 60 and logs will be collected from last 60 days in that case.
Use Proxy	Uncheck to disable proxy configuration. This is enabled by default.
Proxy Server	If you are using a proxy in your environment, enter the proxy server address.
Proxy Port	Enter the proxy port.
Proxy User	Username for the proxy (leave empty if using anonymous proxy).

Name	Description
Proxy Password	Password for the proxy (leave empty if using anonymous proxy).
Source Address	A custom value chosen to represent the hostname for the Jamf Protect Event Source in the customer environment and the value should be in IPV4 format. The value of this parameter is captured by the **device.ip** meta key.

Advanced Parameters

Click **Advanced** to view and edit the advanced parameters.

Name	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is 180. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy.
Max Duration Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. The default is set to 600.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).
Max Idle Time Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Command Args	Optional arguments to be added to the script invocation.
Debug Caution	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread

	information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.
SSL Enable	Uncheck to disable certificate verification. This is enabled by default.

Getting Help with NetWitness Platform XDR

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions.
- See the NetWitness Knowledge Base: https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base.
- See Troubleshooting section in the guides.
- See also NetWitness® Platform Blog Posts.
- If you need further assistance, Contact NetWitness Support.

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform XDR or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click **Support > Case Portal > View My Cases**.
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.